



Ressources**informatiques**

Windows 11

Installation et configuration

Yann BARDOT



Windows 11

Installation et configuration

Ce livre sur Windows 11 (rédigé sur la version 21H2 build 22000.100 et supérieure) s'adresse à des **administrateurs et techniciens réseau** qui évoluent dans un environnement d'entreprise avec des postes clients Windows 11.

Il a été conçu pour permettre au lecteur de maîtriser toutes les spécificités du système d'exploitation client Microsoft : l'**installation** et la **configuration** de l'OS, la **personnalisation de l'interface**, le **partitionnement** des disques et la gestion des **pilotes de périphériques**, la gestion des **clients Windows** (accès à distance, imprimantes, BranchCache...), les fonctionnalités liées à la **sécurité** avec entre autres EFS, BitLocker et AppLocker, ainsi que la **protection** et la **récupération du système**.

L'objectif de ce livre est de **rendre le lecteur autonome** en termes de **maintenance** du système, de **surveillance** et d'**optimisation des performances**. Chaque sujet est approfondi et détaillé : tous les concepts sont illustrés par des manipulations afin de bien en assimiler les mécanismes.

Auteur(s)

Article I. Yann BARDOT

Formateur et technicien informatique freelance, **Yann BARDOT** est spécialisé dans les infrastructures Windows. Développeur à ses débuts, il s'est ensuite tourné vers l'administration de systèmes d'exploitation et le support technique. Il accompagne ses clients dans les domaines de la maintenance, de l'installation de serveurs et dans la formation (prise en main d'un PC, bureautique).

À propos de cet ouvrage

- Ce livre vous fournit les connaissances nécessaires pour installer et configurer le système d'exploitation Windows 11 chez vous ou dans un environnement d'entreprise.
- À destination des professionnels de l'informatique comme des consultants, techniciens de support, administrateurs ou architectes, les prérequis suivants sont nécessaires à la bonne compréhension de cet ouvrage :
 - Expérience dans l'installation et la configuration de postes de travail Microsoft.
 - Connaissances sommaires d'un environnement Active Directory.
 - Maîtrise des notions fondamentales concernant les réseaux (TCP/IP et DNS).
- À la lecture de cet ouvrage, vous adopterez de bonnes pratiques autour des manipulations initiales comme des manipulations les plus avancées.
- Le cheminement se veut didactique et progressif : chaque sujet traité est suivi d'un exemple détaillé.
- Les environnements utilisés dans les exemples sont principalement basés sur Windows 11 Professionnel, Entreprise et Windows Server 2019.
- Idéalement, vous installerez Windows 11 Professionnel sur une machine virtuelle, afin de pouvoir, sans impact, effectuer les actions décrites dans les travaux dirigés.
- Ce livre étant le vôtre, vous pouvez participer à son amélioration ; si vous avez des questions, des critiques ou des suggestions, n'hésitez pas à contacter son auteur : ybardot@yahoo.fr

Remerciements

- Je tiens à remercier les Éditions ENI qui m'ont permis de concrétiser ce projet d'écriture et toute l'équipe pour l'aide apportée tout au long de la rédaction.

Installation du Windows 11

Introduction



- Windows 11 est le successeur du système d'exploitation Windows 10. Destiné aux particuliers et aux entreprises, c'est un système client aussi bien orienté tablette tactile, poste de travail pourvu d'un clavier et d'une souris, ou encore - officieusement - smartphone.
- Il succède à Windows 10 après plus de six ans de bons et loyaux services (commercialisation débutée le 29 juillet 2015).
- À l'heure où nous écrivons cet ouvrage, la date de commercialisation annoncée par Microsoft est celle du 5 octobre 2021. Celle-ci concerne principalement les nouvelles machines. Les fabricants pourront ainsi intégrer le nouveau système d'exploitation aux machines vendues en fin d'année. La mise à jour gratuite des anciennes machines fonctionnant sous Windows 10 interviendra progressivement à partir de cette date. Le déploiement sur les machines compatibles s'effectuera donc graduellement et s'étendra probablement jusqu'au premier semestre 2022.
- Microsoft a conçu ce nouveau système en reprenant la puissance et la sécurité de Windows 10, tout en ajoutant de nouvelles fonctionnalités. Les performances et l'ergonomie ont été améliorées, l'expérience utilisateur a été repensée, offrant un style plus moderne. Le noyau évolue sensiblement et passe ainsi en version 11. Cela signifie que les applications compatibles avec Windows 10 le seront également avec Windows 11. Le système promet d'améliorer la productivité avec une expérience utilisateur flexible et fluide, de prendre en charge les systèmes hybrides et de favoriser la connectivité. Les applications en arrière-plan consomment moins de ressources au profit des applications de premier plan. La sortie du mode veille a été accélérée en optimisant le réveil du SSD ou de la carte réseau.
- Cet ouvrage est basé sur la version 21H2 de Windows 11, build 22000.100 et supérieure, dont le nom de code a été longtemps Sun Valley. Cette version, prévue pour les *Windows Insiders*, n'est pas une version finale, c'est-à-dire commerciale, et donc pourra présenter des différences minimes avec le système que vous installerez.

- Vous noterez au passage le changement d'appellation des mises à jour ou versions Windows depuis l'année 2020. Jusqu'au premier semestre 2020, les mises à jour semi-annuelles étaient estampillées avec l'année et le mois de livraison. Par exemple 2004 (20 pour l'année 2020 et 04 pour le mois d'avril) pour la première mise à jour de 2020. À partir des versions suivantes, Microsoft a modifié cette appellation en 20H2 (20 pour l'année 2020 et H2 pour le 2^e semestre, *half-year* en anglais).
- Il est d'ailleurs intéressant de noter que le nom de la première version de Windows 11 (21H2) correspond à celui d'une mise à jour Windows 10, montrant clairement la filiation entre Windows 10 et Windows 11. La mise à jour 21H2 est en réalité une mise à niveau, un changement de version de Windows. Cela démontre également la volonté de Microsoft d'inciter les utilisateurs de son système d'exploitation à migrer vers cette nouvelle version de Windows en toute transparence.
- Microsoft avait annoncé que Windows 10 serait son dernier système d'exploitation et que celui-ci serait amélioré via des mises à jour semi-annuelles. Il apparaît donc que la société a changé son fusil d'épaule, préférant rompre avec le numéro de version actuel et mettre en avant une nouvelle version. Qui sait si la pandémie de covid-19 et le recours au télétravail n'y seraient pas pour quelque chose...

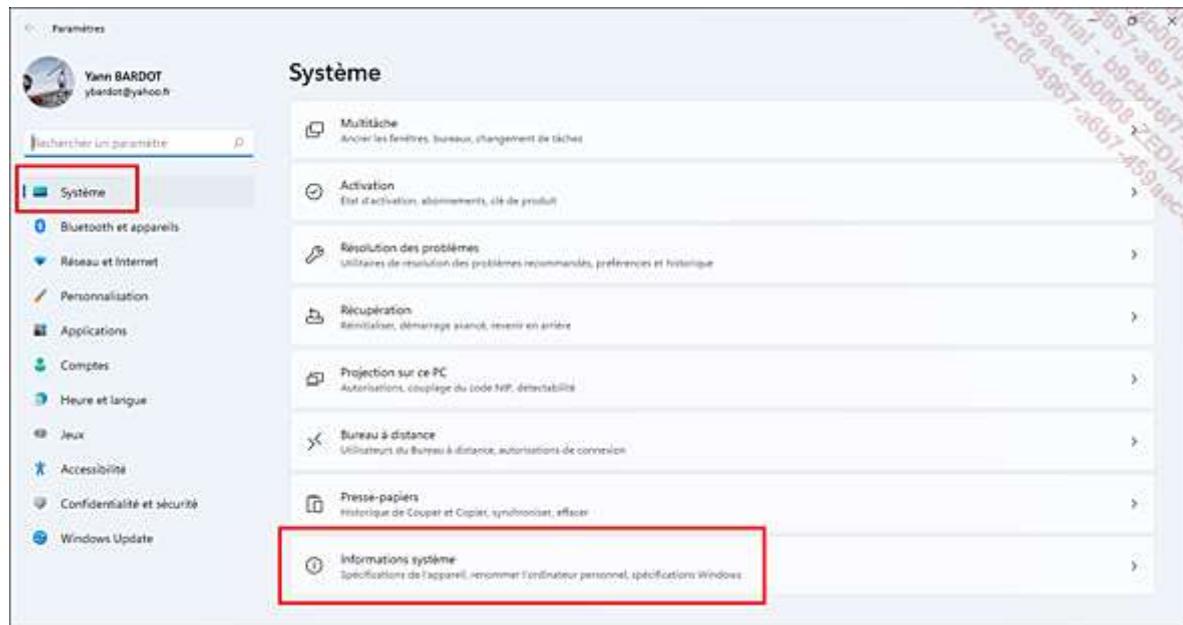
Comment savoir quelle version vous utilisez ? En bas au milieu de votre écran (la barre des tâches est centrée sur cette nouvelle version, il s'agit d'une des nouveautés de Windows 11), cliquez avec le bouton gauche sur

l'icône de l'**Ecran de démarrage** (nouveau nom du menu **Démarrer** ), puis sur l'icône des



paramètres . Dans la colonne de gauche, cliquez sur **Système**, puis dans la colonne de droite sur **Informations système**.

Dans la suite de cet ouvrage, par mesure de simplicité nous utiliserons généralement les termes menu **Démarrer** ou bouton **Démarrer**, plus connus des utilisateurs.



- La fenêtre suivante apparaît :

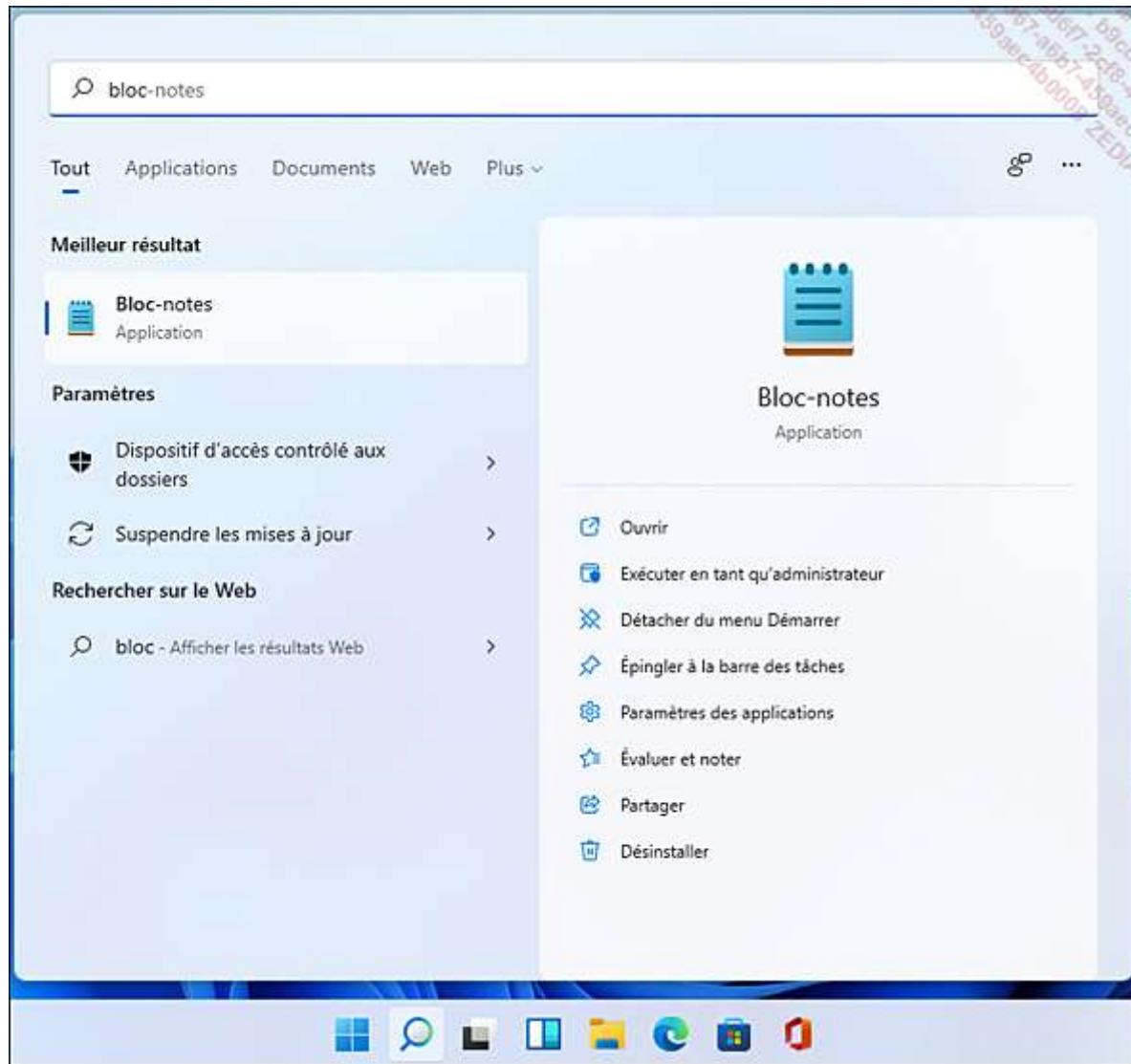
The screenshot shows the Windows System Information window. On the left, a sidebar lists various system settings like Système, Bluetooth et appareils, Réseau et Internet, Personnalisation, Applications, Comptes, Heure et langue, Jeux, Accessibilité, Confidentialité et sécurité, and Windows Update. The main pane is titled "Système > Informations système". It displays general system information such as Manufacturer (Yann BARDOT), Product ID (4A4C358E-4F1A-495A-A1C9-77B8552B332C), and System Type (Système d'exploitation 64 bits, processeur x64). A note states that touch input is not available if a stylus is not supported by the screen. Below this, there are tabs for Liens connexes, Domaine ou groupe de travail, Protection du système, and Paramètres avancés du système. The "Spécifications de Windows" tab is selected, showing detailed system specifications. The "Edition" is listed as Windows 11 Professionnel, "Version" as 21H2, "Installé le" as 03/07/2021, and "Build du système d'exploitation" as 22000.100. The "Expérience" section indicates Windows Feature Experience Pack 42138901.0. Under "Paramètres associés", there is a link to "Clé de produit et activation" and "Bureau à distance".

- Vérifiez la version dans le champ **Version**. Dans l'exemple ci-dessus, il s'agit de la version 21H2, build 22000.100. Votre machine affichera probablement le même numéro de version, mais un numéro de build supérieur.
- Si la présentation des menus diffère de la capture ci-dessus, vous utilisez probablement encore une version de Windows 10. Sachez qu'il est possible de la mettre à niveau vers Windows 11. Cette partie sera abordée un peu plus loin dans cet ouvrage.
- Avant de commencer à utiliser Windows 11, il est important de se familiariser avec la nouvelle interface, largement inspirée de celle de Windows 10X (le projet de système d'exploitation prévu pour concurrencer le système Chrome OS), afin de réaliser des tâches basiques mais néanmoins indispensables :
 - Exécution d'applications : comme signalé précédemment, premier grand changement visuel : le menu **Démarrer** ou **Ecran de démarrage** est désormais situé au centre de la barre des tâches, représenté par l'icône . La touche Windows de votre clavier (si présente) () affiche également ce menu.

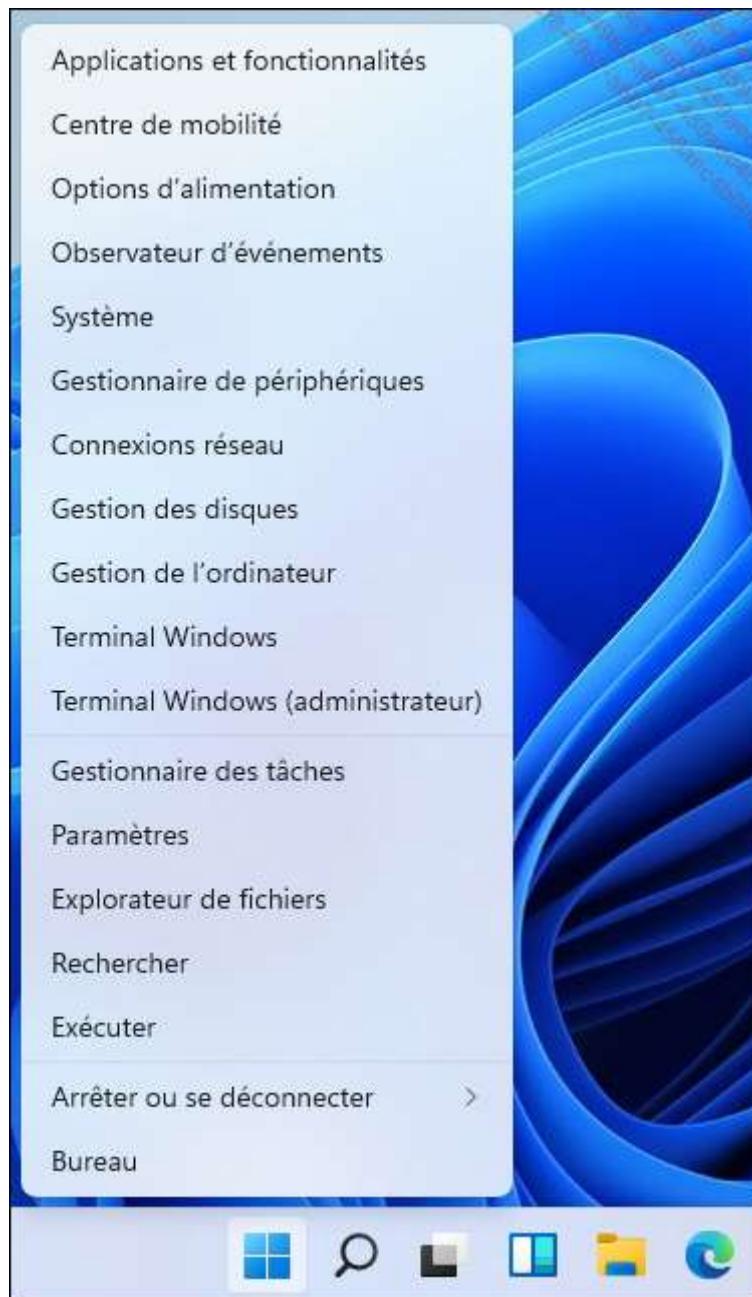
Le menu est désormais flottant et permet d'accéder aux applications en cliquant ensuite sur **Toutes les applications**.



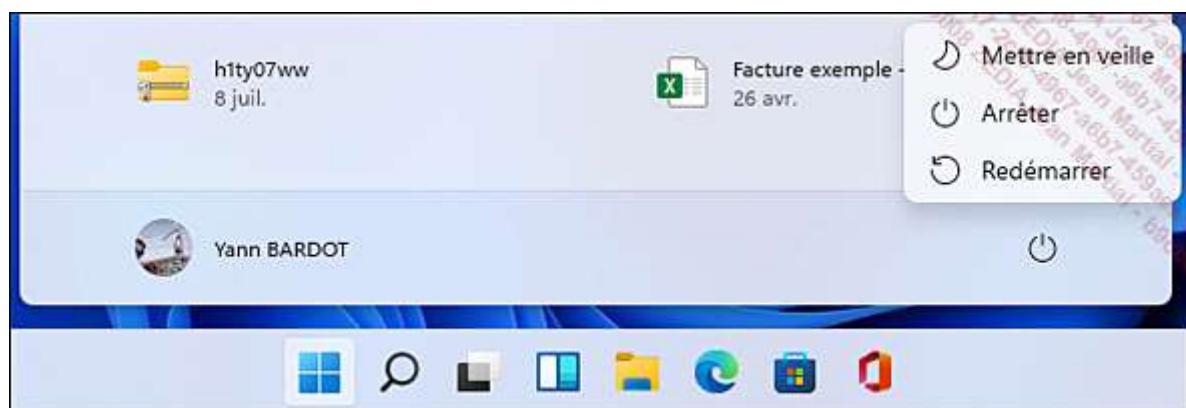
Ce menu permet également à l'utilisateur de trouver et exécuter une application en saisissant les premières lettres, soit en tapant directement dans le menu, soit en plaçant le curseur de la souris dans le champ nommé **Taper ici pour effectuer une recherche**. Ainsi, en saisissant les premières lettres de l'application **Bloc-notes**, celle-ci est proposée pour exécution.



- Notez qu'en cliquant avec le bouton droit sur le menu **Ecran de démarrage**, certaines fonctionnalités très utiles aux administrateurs sont accessibles, comme l'accès à l'**Explorateur de fichiers**, au **Gestionnaire de périphériques**, à la **gestion des disques**, au **Terminal Windows** (l'invite de commandes **Windows PowerShell**), au **Gestionnaire des tâches**, etc.

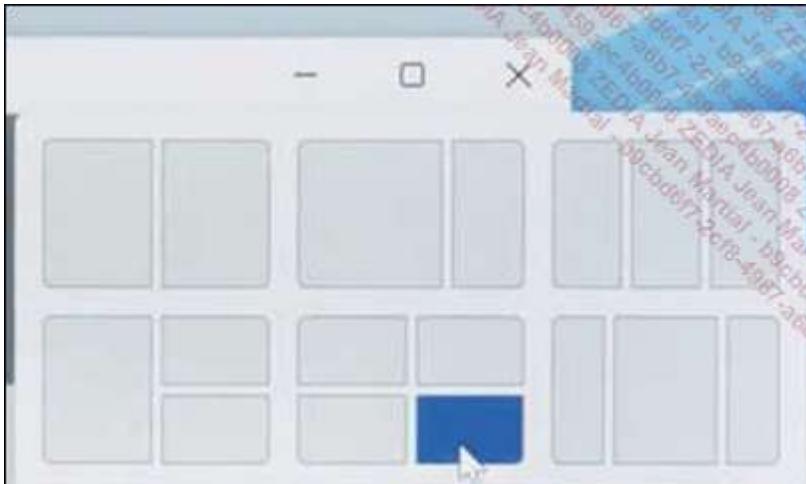


- Arrêt de l'ordinateur : pour éteindre ou redémarrer votre ordinateur, il suffit de cliquer sur le menu **Ecran de démarrage** (anciennement **Démarrer**) avec le bouton gauche de la souris, puis sur le bouton **Marche/Arrêt**  et sur **Arrêter**.



Fonctionnalités nouvelles et améliorées

- Windows 11 apporte peu de nouvelles fonctionnalités mais a été conçu selon trois axes :
 - Moderniser l'interface utilisateur, de manière à la rendre plus ergonomique et plus cohérente.
 - Favoriser la productivité.
 - Faciliter la communication en rendant Windows plus ouvert.
- Cela se traduit par les nouveautés suivantes :
 - Interface utilisateur : Microsoft a repensé l'interaction homme/machine sur son système ainsi que la gestion des applications.
 - L'apparence du système a été entièrement repensée, en reprenant le cahier des charges du projet Windows 10X : transparence plus poussée, fenêtres aux coins arrondis, effets d'ombre projetée, animations fluides et soignées (icônes qui se réduisent lorsque l'on clique dessus...).
 - Le logo Windows est passé du carré vu en perspective au carré vu de face.
 - Les icônes des applications et des paramètres Windows, datant pour certaines de Windows XP, se sont elles aussi modernisées.
 - L'Explorateur de fichiers évolue lui aussi pour se calquer sur cette nouvelle apparence : menus généraux et contextuels simplifiés et remaniés.
 - La barre des tâches est désormais centrée et épurée. Elle simplifie grandement son menu contextuel mais reste personnalisable, notamment au niveau de sa position (centrée ou à gauche) ou des icônes pouvant apparaître à son extrémité droite.
 - Le nouveau menu **Démarrer (Ecran de démarrage)** est désormais centré et flotte au-dessus de la barre des tâches. Il permet toujours d'accéder aux applications, mais propose une section **Nos recommandations** qui regroupe les derniers fichiers utilisés. Il est paramétrable, c'est-à-dire qu'il est possible d'épingler les applications les plus utilisées pour y accéder très rapidement sans avoir à rechercher dans la liste de toutes les applications. Il est également possible d'épingler certains dossiers. Enfin, dans sa partie haute, il propose un champ de recherche.
 - Le panneau de gestion des paramètres est entièrement nouveau : l'interface a été modernisée, les menus remaniés. Par exemple la gestion du téléphone s'effectue dans **Bluetooth et appareils**.
 - Système de disposition automatique des fenêtres (*Snap Layout* et *Snap groups*) : cette fonctionnalité, héritière directe des *Fancy Zones* (fonctionnalité disponible dans les PowerToys Microsoft), permet de définir et mémoriser un agencement personnalisé des fenêtres dans chaque bureau virtuel et pour chaque écran connecté. Des zones sont prédéfinies en fonction de la taille de votre écran (largeur minimum de 1920 pixels pour un affichage sur trois colonnes) ; il suffit de passer votre souris sur l'icône d'agrandissement de la fenêtre de votre application, puis de sélectionner la zone où l'on souhaite positionner la fenêtre pour que cette dernière s'y dirige, le tout en un seul clic. Le fait de reconnecter un écran externe permettra aux fenêtres précédemment paramétrées de s'y placer automatiquement.



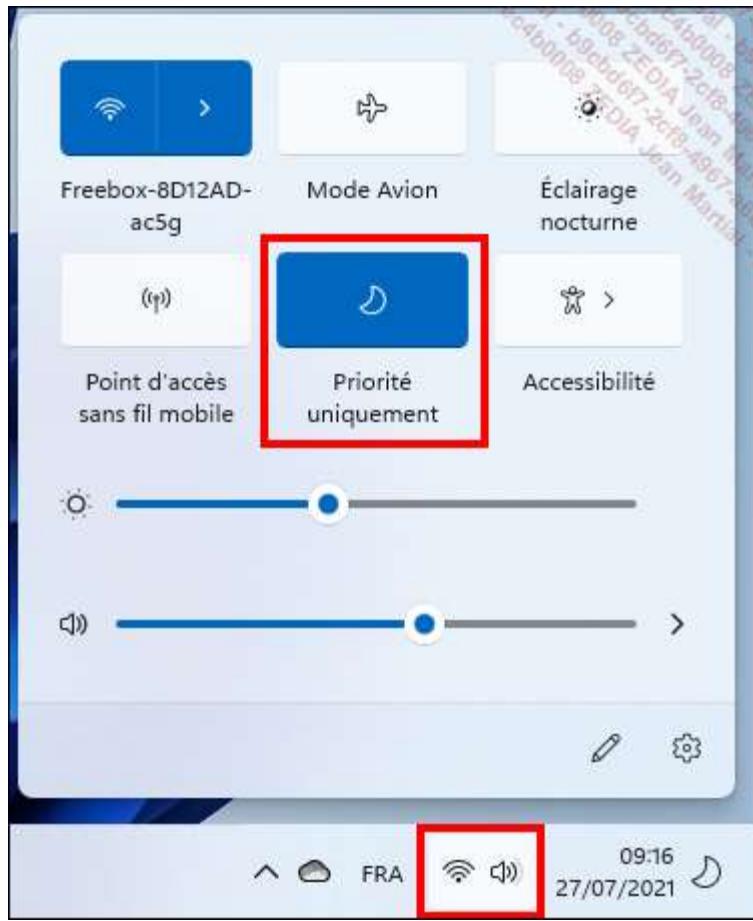
- Widgets : un nouveau panneau latéral, accessible directement depuis la barre des tâches, permet d'accéder aux widgets que vous aurez choisis : météo, dernières news... Il permet également de faire des recherches sur Internet via le moteur de recherche Bing.
- Microsoft Store : Windows 11 est compatible Android ! Outre une interface revue, le magasin d'applications devient universel et inclut désormais les applications Android, via le magasin d'applications d'Amazon. Cela signifie qu'il est possible d'exécuter des applications Android de manière native, sans avoir à recourir à un émulateur tiers. Pour ce faire, Windows 11 utilise la technologie WSA (*Windows Subsystem for Android*), qui elle-même utilise la technologie Intel Bridge, cette dernière permettant à des applications Android de fonctionner sur des plateformes Intel ou AMD. De plus, le magasin d'applications de Windows 11 s'ouvre aux différents formats : PWA, Win32, UWP, facilitant ainsi la mise à disposition du travail des développeurs.

À l'heure où cet ouvrage est rédigé, cette nouvelle fonctionnalité n'est pas encore disponible et ne le sera pas pour la sortie de Windows 11. Microsoft annonce une disponibilité courant 2022.

- Gamers : quelques nouvelles fonctionnalités font leur apparition : l'HDR automatique (HDRa) qui rend les couleurs encore plus réelles et plus vives, l'API DirectStorage (déjà exploitée par la console Xbox Series X) qui permet d'améliorer les temps de chargement en donnant au GPU l'accès au stockage, WDDM 3.0 qui permet de choisir quelle carte graphique utiliser selon le programme exécuté. Sur les machines compatibles, un mode automatique (DRR pour *Dynamic Refresh Rate*) permet de sélectionner la fréquence d'actualisation de l'affichage en fonction de vos actions (écriture ou utilisation de la roulette) pour favoriser la fluidité de l'affichage ou optimiser la consommation d'énergie.
- Communication : pour se connecter au monde extérieur, Skype laisse la place à Teams Chat appelé également Conversation. L'outil s'intègre directement dans la barre des tâches de Windows 11 et devient même accessible avec un raccourci-clavier (+ C). Il permet de lancer rapidement une conversation ou une réunion avec ses contacts. Microsoft confirme ainsi sa volonté d'en faire l'outil de communication multiplateforme universel.
- Processeurs : Windows 11 a été optimisé pour tirer pleinement profit des architectures de processeurs mixant des cœurs performants à des cœurs économies. En plus des plateformes Intel et AMD, il supporte les plateformes ARM.
- Tactile : le fonctionnement du stylet et de l'écran tactile est ici optimisé pour permettre l'utilisation des mêmes gestes que depuis le trackpad. Il offre également des transitions plus douces entre le mode PC et le mode tablette.
- Comme toute nouvelle version d'un système d'exploitation, certaines fonctionnalités disparaissent définitivement :

- Le menu **Démarrer** perd ses tuiles dynamiques. Il ne permet plus de créer des groupes ou des dossiers d'applications.
- La barre des tâches n'est plus aussi personnalisable : il est désormais impossible de la déplacer sur un des côtés de votre bureau. Les **Actualités et champs d'intérêt** ont migré vers les **Widgets**.
- La fonction **Chronologie (Timeline)** disparaît complètement de cette nouvelle version. Seul l'**Affichage des tâches** survit à cette mise à niveau.
- Le mode Tablette disparaît également de cette nouvelle version. Le passage du mode PC au mode tablette (clavier détaché ou replié) se fait naturellement ; les icônes de la barre des tâches et de l'explorateur s'écartent les unes des autres pour faciliter l'appui avec le doigt, des cases à cocher apparaissent dans l'Explorateur, le clavier virtuel est automatiquement proposé...
- Le mode S, limitant les installations d'applications au magasin d'applications Microsoft, ne sera disponible que pour l'édition Famille de Windows 11.
- Internet Explorer n'est plus présent. Edge propose néanmoins un mode IE, activable via une stratégie (GPO), pour les utilisateurs et entreprises ayant besoin de ce navigateur.
- Cortana n'apparaît plus lors de la configuration de la machine (Expérience du premier démarrage) et n'est plus présente sur la barre des tâches. L'assistante virtuelle se réserve maintenant au monde des entreprises. Elle reste néanmoins activable à la demande.
- Certaines applications intégrées dans Windows 10 ne le sont plus dans Windows 11, mais restent néanmoins téléchargeables : OneNote, Paint 3D, Skype, la Visionneuse 3D.
- La synchronisation de fond d'écran entre appareils connectés à un même compte Microsoft est supprimée.
- Il est également important de noter l'indisponibilité d'une version 32 bits de ce système d'exploitation.
- Bien entendu, de nombreuses fonctionnalités déjà présentes avec Windows 10 perdurent dans cette nouvelle version :
 - Bureau virtuel : simulation de plusieurs écrans afin par exemple que l'utilisateur puisse exécuter ses applications professionnelles dans un bureau virtuel et ses applications personnelles dans un autre. Celui-ci devient accessible directement depuis la barre des tâches en cliquant sur le bouton 
 - Navigateur Edge : Internet Explorer étant abandonné, Microsoft intègre dorénavant un navigateur plus rapide et permettant par exemple d'annoter les pages internet.
 - Recherche : la recherche et la visualisation des informations sont améliorées à l'aide de la recherche unifiée. Les résultats d'une recherche prennent en compte les données issues de l'ordinateur, de ses applications ou du moteur de recherche Bing.
 - Dossiers de travail : synchronisation des fichiers entre plusieurs ordinateurs ou appareils appartenant à un même utilisateur, qu'il s'agisse de systèmes joints à un domaine Active Directory ou membres d'un groupe de travail.
 - OneDrive : fonctionnalité intégrée totalement au système d'exploitation, les données sont stockées dans le cloud et synchronisées sur les ordinateurs et tablettes Windows 11.
 - DirectAccess : connexion distante d'un utilisateur au réseau de son entreprise sans aucune intervention manuelle de celui-ci.
 - BranchCache : technologie de mise en cache des données distantes sur des clients du même réseau.
 - Gestionnaire de connexions : une seule interface gère toutes les connexions distantes (Wi-Fi, Bluetooth, 3G/4G, etc.).

- IPv6 : gestion du protocole IPv6 lors des connexions internet.
- Presse-papiers : le Presse-papiers permet, comme dans les anciennes versions, de sauvegarder des contenus, textes et images (via copier-coller, touches [Ctrl] + C/[Ctrl] + V), mais aussi de les synchroniser entre différents terminaux Windows 10. De plus, en pressant les touches  + V, l'utilisateur aura la possibilité d'utiliser l'historique du Presse-papiers en cliquant sur le bouton **Activer**.
- Votre téléphone : l'application mobile, disponible sur Android et iPhone, synchronise les photos prises par l'utilisateur via son smartphone sur son ordinateur ou sa tablette Windows et permet d'afficher et envoyer des SMS à partir de son ordinateur, de passer et recevoir des appels et même, si vous disposez d'Android 11, d'exécuter des applications de votre téléphone depuis votre ordinateur.
- SwiftKey : le système de saisie tactile par *swipe* (balayage des doigts sur l'écran) de Microsoft, déjà disponible pour Android et iOS, est intégré à Windows 11. Pour le paramétrier, il suffit de cliquer sur le menu **Démarrer** puis **Paramètres, Heure et langue, Saisie** et enfin **Clavier tactile**.
- Un moteur de recherche enrichi grâce à un mode de prévisualisation des résultats.
- eSIM : Windows 11 prend en charge les cartes SIM des opérateurs préintégrées au matériel.
- Eye Control : le système intègre une fonctionnalité de contrôle par suivi des yeux.
- Exploit Protection : module centré sur la lutte contre le piratage.
- Microsoft Edge : possibilité du contrôle du son par onglet, mémorisation des cartes de crédit de manière sécurisée...
- Partage de proximité en Bluetooth ou Wi-Fi de liens web ou de fichiers.
- Assistant de concentration : pour éviter d'être déconcentré par des notifications, un "Assistant de concentration" permet en deux clics depuis l'icône **Notifications** de la barre des tâches de désactiver celles-ci.



- Sécurité : Windows 11 Professionnel améliore les fonctionnalités de sécurité suivantes :
- Device Guard : empêche un utilisateur d'exécuter des applications non approuvées par l'administrateur.
- Windows Defender Antivirus : logiciel permettant de déterminer si un ordinateur est infecté par des programmes malveillants.
- Microsoft Defender Application Guard : offre un conteneur sécurisé pour la navigation internet.
- Protection des données d'entreprise : en cas de vol de matériel, les données sont effacées à distance sur le poste de travail de l'utilisateur. La protection contre la fuite de données est renforcée.
- Cartes à puce virtuelles : émulation des fonctionnalités des cartes à puce en utilisant les puces TPM (*Trusted Platform Module*).
- Authentification mot de passe image : possibilité d'ouvrir une session grâce à une image choisie et sur laquelle l'utilisateur doit effectuer une série de trois gestes, avec des cercles, lignes droites et/ou points.
- Reconnaissance biométrique : authentifie l'accès aux ordinateurs par l'intermédiaire de capteurs d'empreinte digitale. L'ouverture d'un document via cette méthode est également implémentée.
- Pare-feu Windows avec sécurité avancée : filtrage dans les deux sens des flux transitant.
- BitLocker : chiffrement des disques durs et des mémoires flash USB. Support de la fonctionnalité Full Disk Encryption.
- Windows Hello : permet de se connecter aux appareils Windows 11 de façon plus sécurisée, en utilisant le procédé de reconnaissance d'iris ou du visage du propriétaire de l'ordinateur.
- Déploiement : Windows 11 est basé sur une image aisément modifiable et dont le processus d'installation peut être automatisé à l'aide d'un fichier de réponses. De nouvelles méthodes permettent de déployer un poste de travail :

- Installation du système depuis une mémoire flash USB.
 - Démarrage de Windows 11 depuis un disque virtuel VHD.
 - Secure Boot : fonction utilisant l'UEFI pour vérifier les signatures du gestionnaire de démarrage Windows 11 garantissant ainsi un démarrage sécurisé de l'ordinateur. Cette fonctionnalité est désormais un prérequis pour installer le système d'exploitation.
 - Activation basée sur l'Active Directory : un administrateur peut gérer simplement les activations des systèmes joints à un domaine Active Directory dont il a la charge.
 - Maintenance : Microsoft propose une gestion simplifiée des postes de travail ainsi que de nouveaux outils d'aide à la résolution des problèmes :
 - InstantGo : permet de quitter instantanément le mode veille, applications et données étant à jour.
 - Windows PowerShell : exécution des scripts pour automatiser certaines tâches d'administration.
 - Accès attribué : un utilisateur ne peut exécuter qu'une seule application en plein écran sur l'ordinateur, réduisant celui-ci à une borne d'accès.
 - Start Screen Control : l'administrateur peut configurer l'environnement de travail de l'utilisateur, comme la position des vignettes, grâce à une stratégie de groupe.
 - Packs de résolution des problèmes : enregistrement des actions utilisateur, site internet Microsoft Fix it.
 - AppLocker : contrôle des applications qui peuvent être installées et exécutées par les utilisateurs.
 - Compatibilité des applications : la virtualisation devient un composant essentiel du système d'exploitation.
 - Client Hyper-V : virtualisation d'un système d'exploitation depuis l'hyperviseur Windows 11.
 - Application Compatibility Toolkit : utilitaire aidant à la résolution des problèmes de compatibilité des applications.
 - Périphériques : la gestion des appareils est améliorée, de nouvelles fonctionnalités sont supportées.
 - Impression 3D : intégration du pilote d'une imprimante 3D et support de son format de fichier.
 - Wi-Fi Tethering : connexion internet partagée grâce à un réseau sans fil diffusé entre différents ordinateurs.
 - Miracast : partage du son et de la vidéo d'un appareil mobile vers un moniteur ou une télévision via une connexion sans fil.
 - Wi-Fi Direct wireless printing : impression directe de documents sur une imprimante Wi-Fi sans nécessiter d'ajouter des pilotes ou logiciels tiers.
- Le tableau ci-dessous liste la disponibilité des fonctionnalités prisées par les entreprises, comme AppLocker, BitLocker ou Hyper-V, en fonction de la version de Windows 11 choisie :

	Famille	Pro	Entreprise	Education	Chapitre
AppLocker			X	X	Configuration de la sécurité Windows
BitLocker et BitLocker To Go		X	X	X	Configuration de la sécurité Windows
BranchCache			X	X	Gestion des clients Windows

	Famille	Pro	Entreprise	Education	Chapitre
Bureaux virtuels	X	X	X	X	Interface et applications
Business Store		X	X	X	
Chiffrement EFS		X	X		Configuration de la sécurité Windows
Client Hyper-V		X	X	X	Conception d'une image de déploiement
Cortana	X	X	X	X	Interface et applications
Credential Guard et Device Guard			X	X	Configuration de la sécurité Windows
Démarrage natif VHD		X	X		Installation du client Windows 11
Démarrage sécurisé	X	X	X	X	Installation du client Windows 11
DirectAccess			X	X	Gestion des clients Windows
Espaces de stockage	X	X	X		Gestion des disques et des pilotes
Fonctionnalité RemoteFX			X		Gestion des clients Windows
Historique des fichiers	X	X	X	X	Protection et récupération du système
Impression 3D	X	X	X	X	Gestion des clients Windows
Interface tactile	X	X	X	X	Interface et applications
Jonction à un domaine		X	X	X	
Microsoft Edge	X	X	X	X	Interface et applications
Microsoft Passport	X	X	X	X	Configuration de la sécurité Windows
Miracast	X	X	X	X	Connectivité réseau
Accès attribué (mode kiosque)		X	X	X	Installation du client Windows 11
Mode PC Partagé		X	X		Gestion des clients Windows
OneDrive	X	X	X	X	Gestion des disques et des pilotes

	Famille	Pro	Entreprise	Education	Chapitre
Protection des données d'entreprise		X	X	X	Configuration de la sécurité Windows
Réinitialiser/Actualiser	X	X	X	X	Protection et récupération du système
Traitement des objets stratégie de groupe		X	X	X	
Upgrade Readiness		X	X		Conception d'une image de déploiement
Wi-Fi Direct wireless printing	X	X	X	X	Gestion des clients Windows
Wi-Fi Sense	X	X	X	X	Connectivité réseau
Wi-Fi Tethering	X	X	X	X	Connectivité réseau
Windows Hello	X	X	X	X	Installation du client Windows 11
Windows Information Protection		X	X		Configuration de la sécurité Windows
Windows Update for Business		X	X	X	Configuration de la sécurité Windows
Work folders	X	X	X	X	Gestion des clients Windows
Workplace join	X	X	X	X	Gestion des clients Windows

Préparation à l'installation

Avant d'installer Windows 11, il est nécessaire de vérifier que l'ordinateur de destination supporte les prérequis du système. L'administrateur devra choisir la version qui correspond à ses besoins et s'assurer que ses applications seront compatibles.

1. Prérequis minimaux

Windows 11 étant un système d'exploitation hybride, il peut aussi bien fonctionner sur une tablette tactile que sur un ordinateur portable ou de bureau. Ce nouveau système d'exploitation nécessite une configuration matérielle supérieure à celle demandée pour Windows 10. Voici les prérequis minimaux :

- Processeur 1 GHz ou plus rapide avec au moins deux cœurs, sur une architecture 64 bits. Une liste des processeurs compatibles est disponible sur le site de Microsoft : <http://aka.ms/CPUList>
- 4 Go de RAM.
- Stockage de 64 Go minimum.
- Microprogramme UEFI compatible avec le démarrage sécurisé (*Secure Boot*).

- Module de plateforme sécurisé (TPM) version 2.0 minimum.
- Carte graphique (GPU pour *Graphics Processing Unit*) supportant DirectX 12 ou supérieur avec pilote WDDM 2.0. Ce type de carte graphique permettra une prise en charge efficace de l'interface Windows 11.
- Écran haute définition (720p) avec une diagonale supérieure à 9 pouces.
- Lecteur DVD-ROM ou périphérique flash USB. En cas de déploiement de Windows 11 depuis un réseau, il est nécessaire que la carte réseau de l'ordinateur soit compatible PXE.

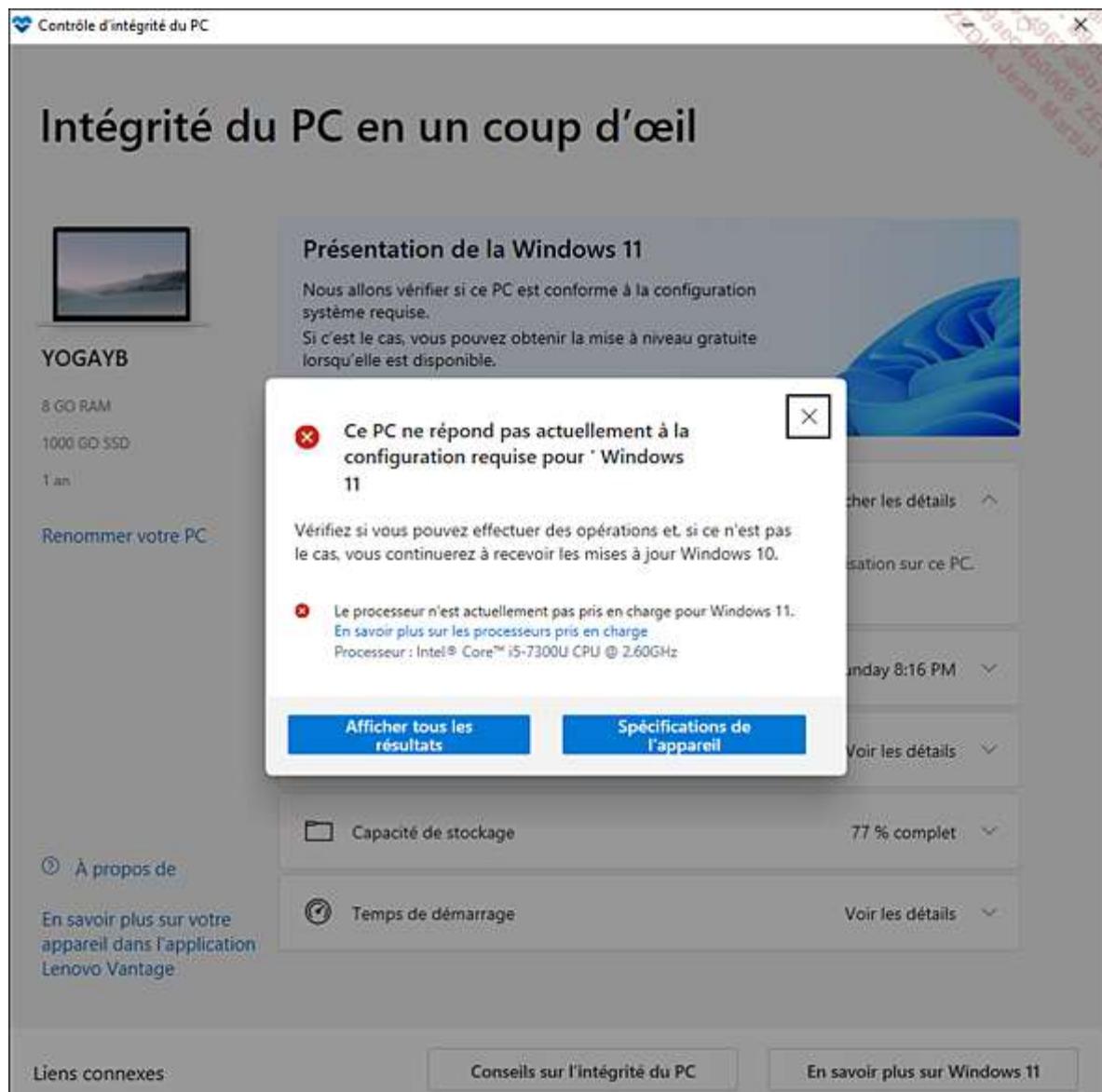
Depuis la version 2004 de Windows 10, seule la version 64 bits est disponible. Windows 11 poursuit logiquement ce choix, les équipements informatiques vendus actuellement disposant tous d'une architecture 64 bits.

À l'heure où cet ouvrage est rédigé, seuls les processeurs Intel de 8^e génération et supérieurs (quelques processeurs de 7^e génération sont néanmoins dans la liste), les processeurs AMD Ryzen ou Epyc de 2^e génération ou supérieurs et Qualcomm 7 et 8 sont compatibles. Microsoft envisage d'identifier (par l'intermédiaire du programme *Windows Insiders*) des processeurs Intel de 7^e génération et des AMD Zen1 qui répondront également aux prérequis.

Microsoft a mis en ligne un outil, Contrôle d'intégrité du PC (*PC Health Check*), permettant de vérifier la compatibilité de son système avec Windows 11. Vous le trouverez ici : <https://aka.ms/GetPCHealthCheckApp>

The screenshot shows the Windows PC Health Check application window. At the top left is the title "Contrôle d'intégrité du PC". Below it, the main heading is "PC Health en un coup d'œil". On the left side, there's a summary of system components: "YOGAYB" (laptop model), "8 GO RAM", "1000 GO SSD", and "Moins d'un an" (less than a year old). Below this, there's a "Renommer votre PC" section. The central area features a large blue banner with the text "Présentation de la Windows 11" and a "Vérifier maintenant" button. To the right of the banner, there's a "Sauvegarde et synchronisation" section with a "Se connecter à un compte Microsoft pour commencer" button and a "Connecté" status indicator. Further down, there are sections for "Mémoriser mes préférences" (Activé), "Synchronisation du dossier OneDrive" (Gérer), "Windows Update" (Dernière vérification : Monday 10:30 AM), and "Capacité de la batterie" (Voir les détails). At the bottom, there are "Liens connexes", "Conseils sur PC Health", and "En savoir plus sur Windows 11".

Pour confirmer la compatibilité de votre machine, cliquez sur le bouton **Vérifier maintenant**. Si votre machine n'est pas compatible, le message suivant s'affichera :



Il est alors possible de continuer à utiliser Windows 10. Ce système est pris en charge jusqu'au 14 octobre 2025, c'est-à-dire qu'il continue de recevoir des mises à jour de sécurité régulièrement jusqu'à cette date.

Les produits vendus en fin d'année 2021 mentionnent "Mise à niveau gratuite vers Windows 11" s'ils sont compatibles Windows 11.

Certaines fonctionnalités spécifiques peuvent nécessiter la présence ou l'ajout de matériel supplémentaire :

- BitLocker To Go nécessite un périphérique flash USB.
- DirectStorage réclame un SSD de type NVMe.
- La fonctionnalité InstantGo requiert une prise en charge matérielle de la veille connectée.
- Le client Hyper-V nécessite une architecture 64 bits avec des fonctions de traduction d'adresses de second niveau (SLAT) et 2 Go de RAM supplémentaires (Windows 11 Professionnel et Windows 11 Entreprise).

La configuration matérielle recommandée dépend également de ce que souhaite faire l'utilisateur. En effet, un ordinateur dédié aux jeux nécessite une carte graphique performante, mais pas nécessairement un stockage vaste.

Dans le même ordre d'idée, une personne souhaitant effectuer du traitement d'image privilégiera un processeur rapide et une grande quantité de mémoire.

a. Démarrage Secure Boot

Un logiciel malveillant, comme un "rootkit", peut dans certains cas s'exécuter avant le lancement du système d'exploitation, créant ainsi une faille de sécurité importante. Face à ce type de menace, Microsoft propose la fonctionnalité Secure Boot basée sur la norme UEFI (*Unified Extensible Firmware Interface*), successeur du BIOS.

L'UEFI offre des fonctionnalités réseau intégrées, l'affranchissement de la limite de démarrage des disques de 2,2 To ou encore la gestion des mises à jour du micrologiciel grâce à Internet.

La fonction Secure Boot utilise l'UEFI version 2.3.1 Errata B ou supérieur pour vérifier les signatures du gestionnaire de démarrage Windows 11, les micrologiciels implantés ainsi que les pilotes UEFI, garantissant ainsi un démarrage sécurisé de l'ordinateur. Secure Boot gère également une base de données des signatures révoquées, empêchant ainsi un code malveillant de s'exécuter.

Cette fonctionnalité fait partie des prérequis pour pouvoir installer Windows 11. Néanmoins, les utilisateurs et fabricants peuvent l'avoir désactivée sur leurs ordinateurs. Il est possible de la réactiver manuellement en modifiant les paramètres de l'UEFI.

b. Appareils non supportés

Comme précisé précédemment, Windows 11 nécessite une configuration matérielle relativement récente (généralement moins de quatre ans) pour fonctionner. Cependant, les machines ne disposant pas des prérequis minimaux ne sont pas automatiquement dans l'impossibilité d'installer cette nouvelle version.

Microsoft tolère l'installation de Windows 11 sur une machine non compatible avec cependant quelques mises en garde :

- L'expérience utilisateur sera inconfortable : écrans bleus (BSOD : *Blue Screen Of Death*), gels ou crashes d'applications surviendraient de manière plus fréquente (de l'ordre de 17 à 52 %).
- Pas d'installation possible depuis les mises à jour Windows. Il faudra donc télécharger et utiliser l'image ISO.
- Limitation ou absence de mises à jour. La machine ne recevra donc probablement pas les nouvelles fonctionnalités, mais surtout ne pourra pas profiter des corrections de bugs et mises à jour de sécurité.

Ces avertissements n'empêchent pas d'installer le nouveau système d'exploitation sur une machine non officiellement supportée mais permettent à l'utilisateur d'être prévenu afin qu'il installe Windows 11 en toute connaissance de cause. La procédure à suivre est disponible sur la page suivante : <https://support.microsoft.com/fr-fr/windows/m%C3%A9thodes-d-installation-de-windows-11-e0edbbfb-cfc5-4011-868b-2ce77ac7c70e>

2. Choix d'une version

Quatre éditions de Windows 11 sont principalement disponibles à destination des particuliers et des professionnels. Chacune possède ses propres fonctionnalités et limitations, mais toutes nécessitent une partition NTFS (*New Technology File System*) pour s'installer.

Le détail de chaque version principale est présenté ci-après.

a. Windows 11 Famille

Cette édition est destinée aux particuliers. Elle inclut les principales nouveautés, comme le système de réorganisation des fenêtres, mais aussi :

- bureau virtuel,
- un passage simplifié du mode bureau au mode tablette,
- Microsoft Edge, le nouveau navigateur de Microsoft,

- chiffrement de l'appareil,
- le mode S (applications en provenance du Microsoft Store uniquement) est intégré à cette version. Si vous souhaitez sortir de ce mode, l'opération sera gratuite mais irréversible.

Le support est désormais de 24 mois à compter de la date de publication de la mise à jour (*release*).

Notez que l'édition Windows 11 Famille nécessite un accès internet et un compte Microsoft pour configurer l'appareil lors de la première utilisation. De même, pour sortir Windows 11 Famille du mode S, une connexion internet sera nécessaire.

b. Windows 11 Professionnel

Édition à destination des petites et moyennes entreprises possédant un domaine Active Directory et nécessitant une sécurité accrue, cette version comprend les fonctionnalités de Windows 11 Famille, ainsi que les suivantes :

- jonction à un domaine et application des stratégies de groupe,
- chiffrement des volumes grâce à BitLocker,
- virtualisation de systèmes d'exploitation et d'applications via Hyper-V,
- gestion centralisée des postes de travail et accès Bureau à distance,
- accès attribué pour ne pouvoir exécuter qu'une application sur une borne,
- association avec Azure Active Directory, avec authentification unique pour les applications hébergées sur le cloud Microsoft Azure,
- Windows Update for Business pour bénéficier d'un client Windows 11 toujours à jour, que ce soit au niveau des fonctionnalités ou de la sécurité, sur l'ensemble des terminaux de l'entreprise.

Windows 10 Professionnel pourra être mis à niveau vers Windows 11 Professionnel. Si la machine dispose d'une version S de Windows 10 Professionnel, elle devra tout d'abord sortir de ce mode pour ensuite pouvoir être mise à jour.

Le support est désormais de 24 mois à compter de la date de publication de la mise à jour (*release*).

Windows Media Center, logiciel regroupant des services multimédias (lire des fichiers son, image, jouer à un jeu vidéo, regarder la télévision...), n'est plus fourni avec ces éditions depuis Windows 10.

c. Windows 11 Entreprise

Destinée aux grandes entreprises, cette édition est disponible uniquement lorsqu'une société souscrit un contrat de maintenance Software Assurance auprès de Microsoft. Le programme Software Assurance propose aux entreprises un support 24/7, une aide au déploiement ou encore la mise à jour automatique vers les dernières versions des produits Microsoft.

Windows 11 Entreprise propose les mêmes fonctionnalités que Windows 11 Professionnel, auxquelles s'ajoutent les suivantes :

- DirectAccess propose de connecter automatiquement l'utilisateur itinérant au réseau de l'entreprise mais sans connexion VPN.
- AppLocker restreint l'exécution et l'installation des logiciels définies depuis un serveur Windows Server sur des clients Microsoft Windows 7 et supérieur.
- BranchCache permet à un client Windows 11 de mettre en cache les données auxquelles il a accédé (pages internet ou dossiers partagés) auprès d'une succursale, pour les rendre disponibles plus rapidement aux ordinateurs de son propre réseau.
- DeviceGuard est un ensemble de fonctionnalités de sécurité matérielle et logicielle qui, lorsqu'elles sont utilisées conjointement, verrouillent un appareil Windows 10 et supérieur afin qu'il puisse uniquement exécuter des applications approuvées par l'administrateur de l'entreprise.

- Credential Guard utilise une technologie de sécurité liée à la virtualisation pour isoler des "secrets" afin que seul l'environnement système puisse y accéder.
- Long Term Servicing Channel (LTSC, le successeur de LTSB depuis 2018) offre aux entreprises la possibilité de faire évoluer les fonctionnalités et correctifs de sécurité de Windows 11 au fil du temps via un contrat liant Microsoft et l'entreprise.

Le support est désormais de 36 mois à compter de la date de publication de la mise à jour (*release*).

d. Windows 11 Education

Windows 11 Education est une version conçue spécialement pour le monde de l'éducation et reprend l'essentiel des fonctionnalités de Windows 11 Entreprise.

Le support est désormais de 36 mois à compter de la date de publication de la mise à jour (*release*).

À noter que le mode de licence LTSC n'est pas disponible dans cette édition.

3. Vérification de la compatibilité

Afin de préparer au mieux l'installation de Windows 11, il est nécessaire de vérifier que le matériel utilisé (carte graphique, scanner, etc.) est pleinement compatible.

Lorsqu'un utilisateur achète un ordinateur équipé de Windows 11, une mention des éditions supportées est apposée sur le matériel. Celle-ci garantit que le constructeur a respecté les exigences de Microsoft. Le kit d'évaluation de matériel en laboratoire Windows (HLK) pour Windows 11 regroupe un ensemble d'outils pour vérifier que les composants de l'ordinateur sont compatibles avec le système de Microsoft. Il peut être téléchargé gratuitement depuis l'adresse : <https://docs.microsoft.com/fr-fr/windows-hardware/test/hlk/windows-hardware-lab-kit> ou directement ici : <https://go.microsoft.com/fwlink/?linkid=2166382>

Un logiciel compatible signifie que l'éditeur affirme que son produit est compatible avec Windows 11.

Installation du client Windows 11

Cette procédure consiste en une installation complète de Windows 11 dans une nouvelle partition sur un ordinateur généralement dépourvu de système d'exploitation antérieur. Depuis Windows 10, Microsoft a réduit le temps nécessaire à l'installation du produit, en comparaison des anciens systèmes, tels que Windows Vista ou Windows 7.

Cinq méthodes sont à la disposition de l'utilisateur pour effectuer cette action :

- L'installation à partir du DVD : cette méthode permet d'installer et de réparer le système d'exploitation Windows 11 en ayant inséré le média d'installation. L'utilisateur devra au préalable configurer l'UEFI pour que l'ordinateur démarre en priorité depuis le lecteur DVD.
- L'installation depuis une clé USB : depuis Windows 98, les versions des systèmes d'exploitation Microsoft sont commercialisées sur un support optique (CD ou DVD). Si vous possédez un ordinateur portable dépourvu de lecteur optique, vous pourrez utiliser un support extrêmement répandu, la clé USB, qui contiendra les fichiers d'installation de Windows 11.
- L'utilisation d'un disque virtuel avec démarrage natif : le démarrage natif permet à un disque dur virtuel contenant Windows 11 de s'exécuter sur un ordinateur physique sans hyperviseur tel qu'Hyper-V ou un produit tiers.
- Le déploiement d'une image par le réseau : à l'aide des services de déploiement Microsoft (WDS), il est possible de déployer une image au format WIM de Windows 11, au travers d'un réseau d'entreprise. Cette méthode est détaillée dans le chapitre Conception d'une image de déploiement section Format de fichier WIM.

- L'exécution de l'installation depuis un partage réseau : en exécutant le fichier setup.exe, stocké avec le contenu du DVD d'installation dans un dossier partagé sur le réseau, l'utilisateur exécutera une nouvelle installation de Windows 11. Au préalable, il est nécessaire de démarrer l'ordinateur à l'aide de Windows PE (*Preinstallation Environment*) pour accéder à une invite de commandes.

La fonctionnalité Windows sur clé USB (Windows To Go) a été supprimée des systèmes d'exploitation depuis Windows 10, version 2004 car elle ne prenait pas en charge les mises à jour de fonctionnalités du système. De plus, elle nécessitait un type de port USB spécifique qui n'est plus pris en charge par la plupart des fabricants d'ordinateurs.

1. Création du média d'installation

La première étape consiste à télécharger le fichier ISO de la version de Windows 11 que vous souhaitez installer et à créer le média d'installation, que ce soit sur DVD ou clé USB. Microsoft a simplifié la procédure en fournissant un outil qui vous charge automatiquement la dernière version majeure.

Depuis un poste de travail Windows 7 (32 ou 64 bits) ou une version supérieure, rendez-vous sur la page de téléchargement de l'outil de création du support Windows 11, en saisissant l'adresse suivante dans votre navigateur internet : <http://www.microsoft.com/fr-fr/software-download/windows11>

Dans la section Crédation d'un support d'installation de Windows 11, cliquez sur le bouton **Télécharger**. Le téléchargement du fichier MediaCreationToolW11.exe débute (il est possible que le nom du fichier soit différent).

Exécutez le fichier précédemment téléchargé. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît. Lisez les termes du contrat de licence puis cliquez sur le bouton **Accepter**.

Microsoft propose désormais un fichier ISO multiversion (familiale, professionnelle...) qui utilise la clé produit (licence) pour déverrouiller la bonne version. Il n'est donc plus nécessaire de sélectionner son édition Windows au préalable. Cliquez seulement sur le bouton **Suivant**. Néanmoins, si vous désirez modifier la langue, décochez la case **Utilisez les options recommandées pour ce PC** et choisissez la langue adaptée, puis cliquez sur le bouton **Suivant**.

Les versions destinées aux entreprises ne sont pas disponibles via cet outil et nécessitent une connexion au Centre de gestion des licences en volume.

Les possibilités de mise à niveau sont détaillées dans le tableau ci-dessous :

• Votre édition actuelle de Windows	• Édition de Windows 11
1 Windows 7 Édition Starter	15 Windows 11
2 Windows 7 Édition Familiale Basique	
3 Windows 7 Édition Familiale Premium	
4 Windows 7 Professionnel	
5 Windows 7 Édition Intégrale	
6 Windows 8/8.1	
7 Windows 8.1 avec Bing	
8 Windows 8 Professionnel	
9 Windows 8.1 Professionnel	
10 Windows 8/8.1 Professionnel avec Media Center	
11 Windows 8/8.1 Unilingue	
12 Windows 8 Unilingue avec Bing	
13 Windows 10 Famille	

• Votre édition actuelle de Windows	• Édition de Windows 11
14 Windows 10 Professionnel	
16 Windows 8/8.1 Édition en chinois	18 Windows 11 Famille Chine
17 Windows 8 Édition en chinois avec Bing	

Deux options sont possibles :

- Si vous souhaitez créer une clé USB amorçable, cochez l'option **Disque mémoire flash USB** puis cliquez sur le bouton **Suivant**. Branchez votre mémoire flash USB d'une capacité d'au moins 8 Go, et cliquez sur le bouton **Suivant**.
- Si vous souhaitez graver le fichier ISO sur un DVD ultérieurement via le programme d'installation, cochez la case **Fichier ISO**. Choisissez l'emplacement où enregistrer le fichier, donnez-lui un nom et cliquez sur **Enregistrer**.

Dans les deux cas, le fichier est téléchargé puis, soit la clé USB amorçable est créée, soit le fichier ISO est enregistré. Dans ce dernier cas, il faudra le graver sur un DVD de manière à en faire un DVD amorçable, ou bien le mettre à disposition sur un serveur.

2. Installation

L'installation de Windows 11 depuis le DVD ou la clé USB s'effectue désormais avec un nombre limité d'étapes, Microsoft ayant simplifié cette procédure par rapport à Windows 7 :

Démarrez la machine à partir du DVD ou de la clé USB. Il vous faudra peut-être modifier les paramètres de l'UEFI pour autoriser le démarrage à partir d'une clé USB.

À l'invite, appuyez sur une touche du clavier pour lancer l'installation.

Sélectionnez la **Langue à installer**, le **Format horaire et monétaire** ainsi que la langue du **Clavier**.



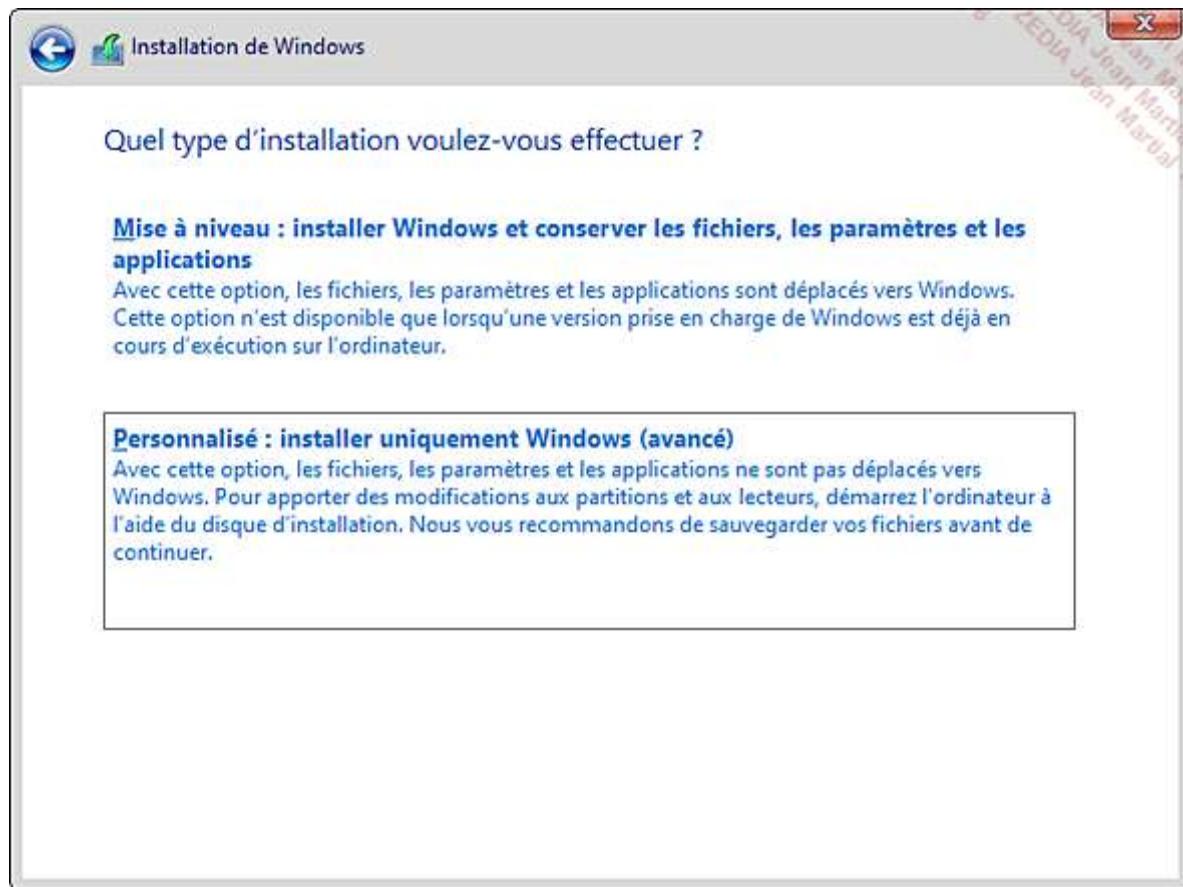
Cliquez sur le bouton **Suivant**.

Cliquez ensuite sur **Installer maintenant**. Entrez la clé de produit sans spécifier les tirets "-" séparateurs, puis cliquez sur le bouton **Suivant**.

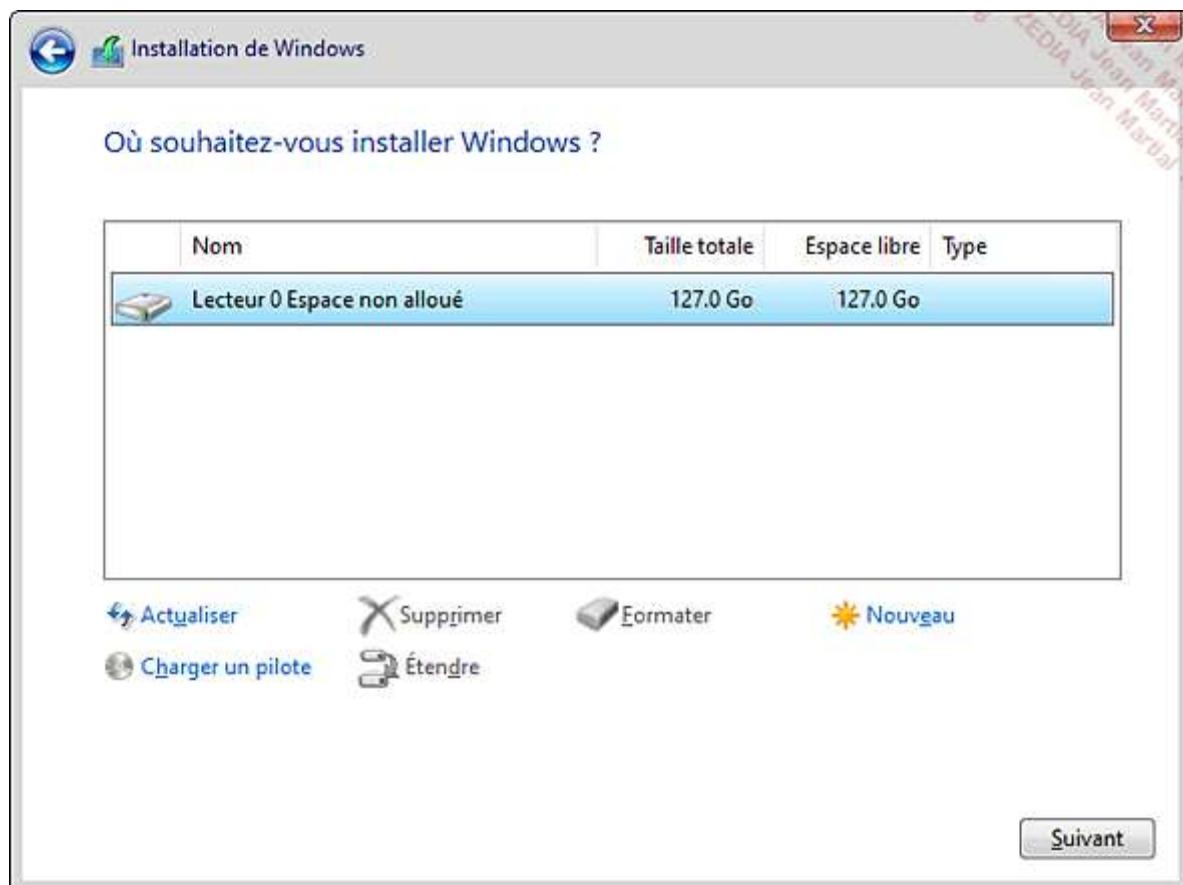
Si vous disposez d'un support multiversion, sélectionnez le système d'exploitation à installer, puis cliquez sur le bouton **Suivant**.

Cochez la case **J'accepte les termes du contrat de licence** puis validez par **Suivant**.

Dans la fenêtre du choix du type d'installation, cliquez sur **Personnalisé : installer uniquement Windows (avancé)** afin d'exécuter une installation du système Windows 11 sur un ordinateur dépourvu de tout système d'exploitation. L'option **Mise à niveau** n'est réalisable qu'en exécutant l'installation depuis l'ancien système d'exploitation.

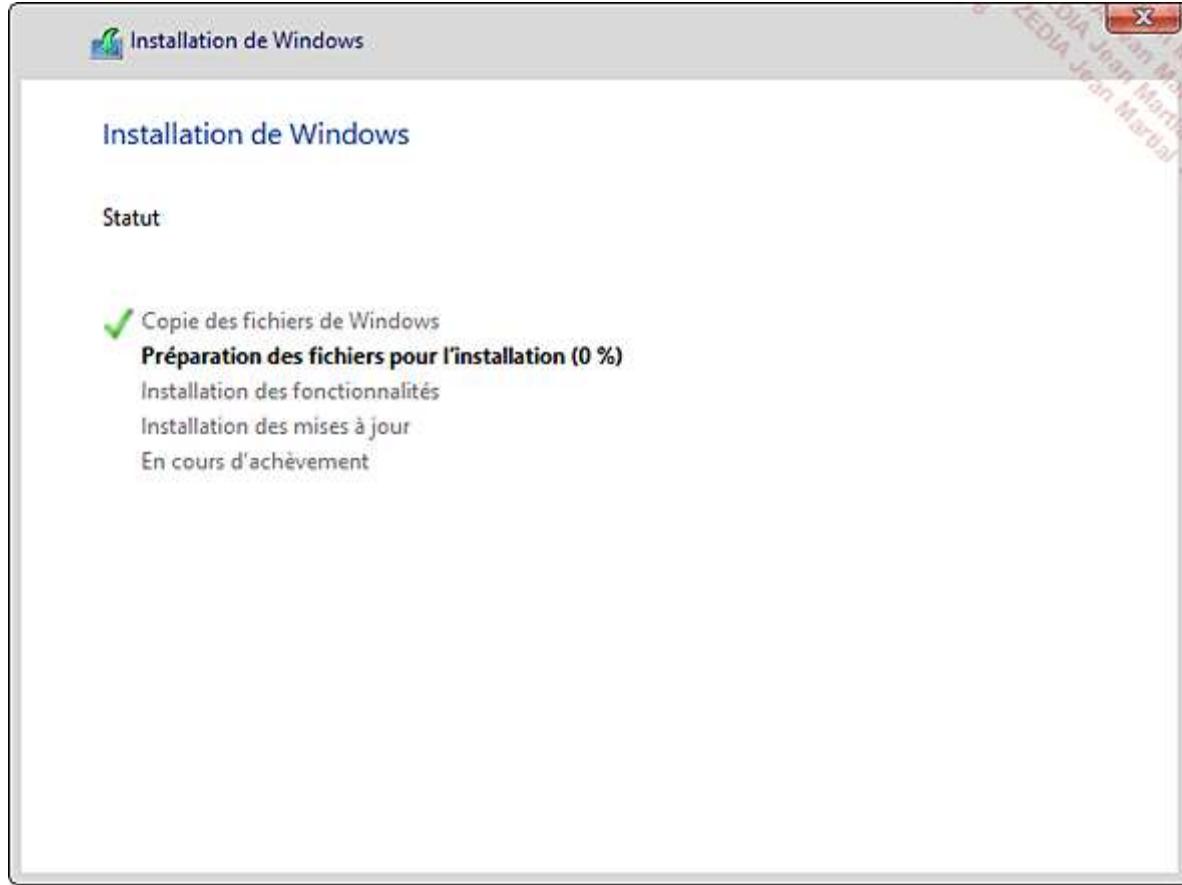


L'écran suivant propose de partitionner les disques durs présents dans l'ordinateur. Si vous n'avez pas de besoins particuliers, laissez le système créer automatiquement les partitions.

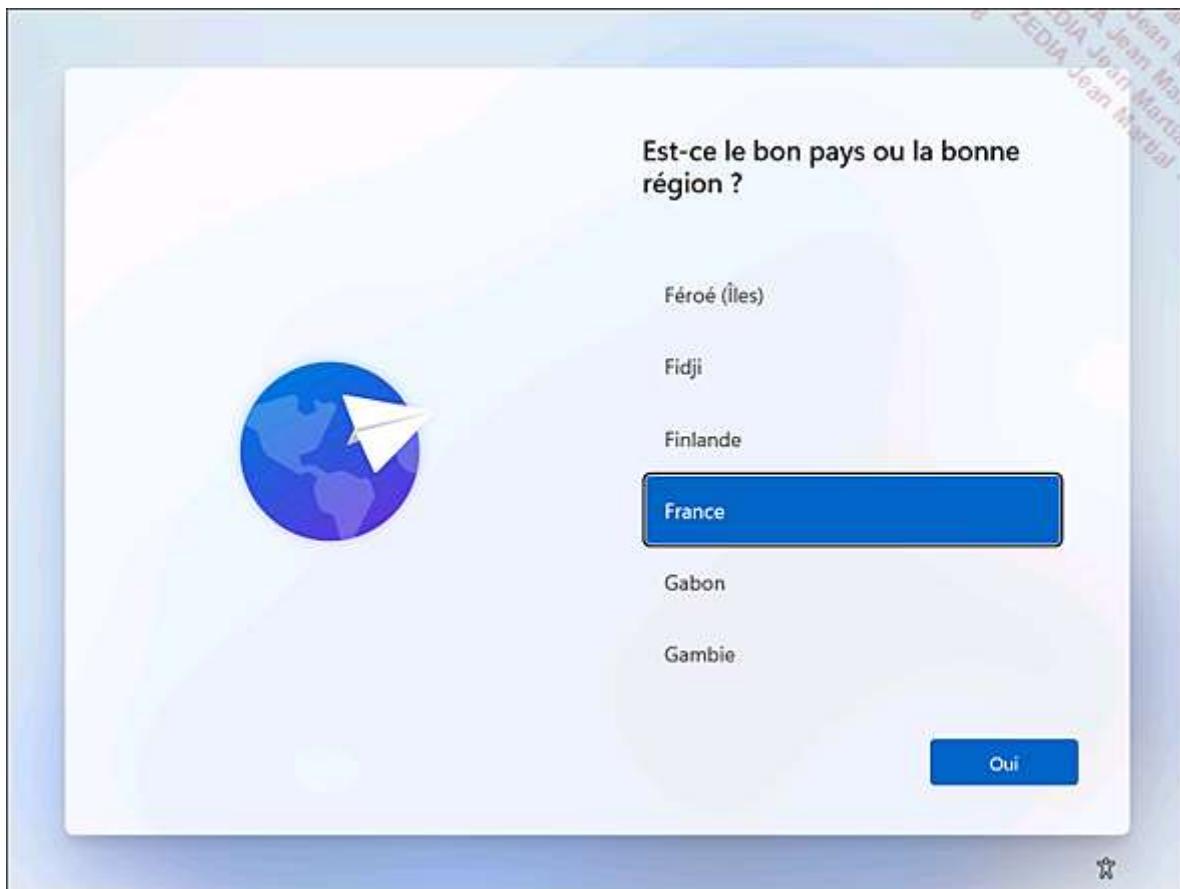


Vous pouvez **Charger un pilote tiers** et **Étendre, Supprimer ou Formater** une partition. Windows 11 nécessite un espace disque disponible d'au moins 64 Go. Une fois les opérations effectuées, sélectionnez la partition de destination puis cliquez sur le bouton **Suivant**.

19 Windows 11 copie les fichiers nécessaires à son fonctionnement puis installe les fonctionnalités du système.

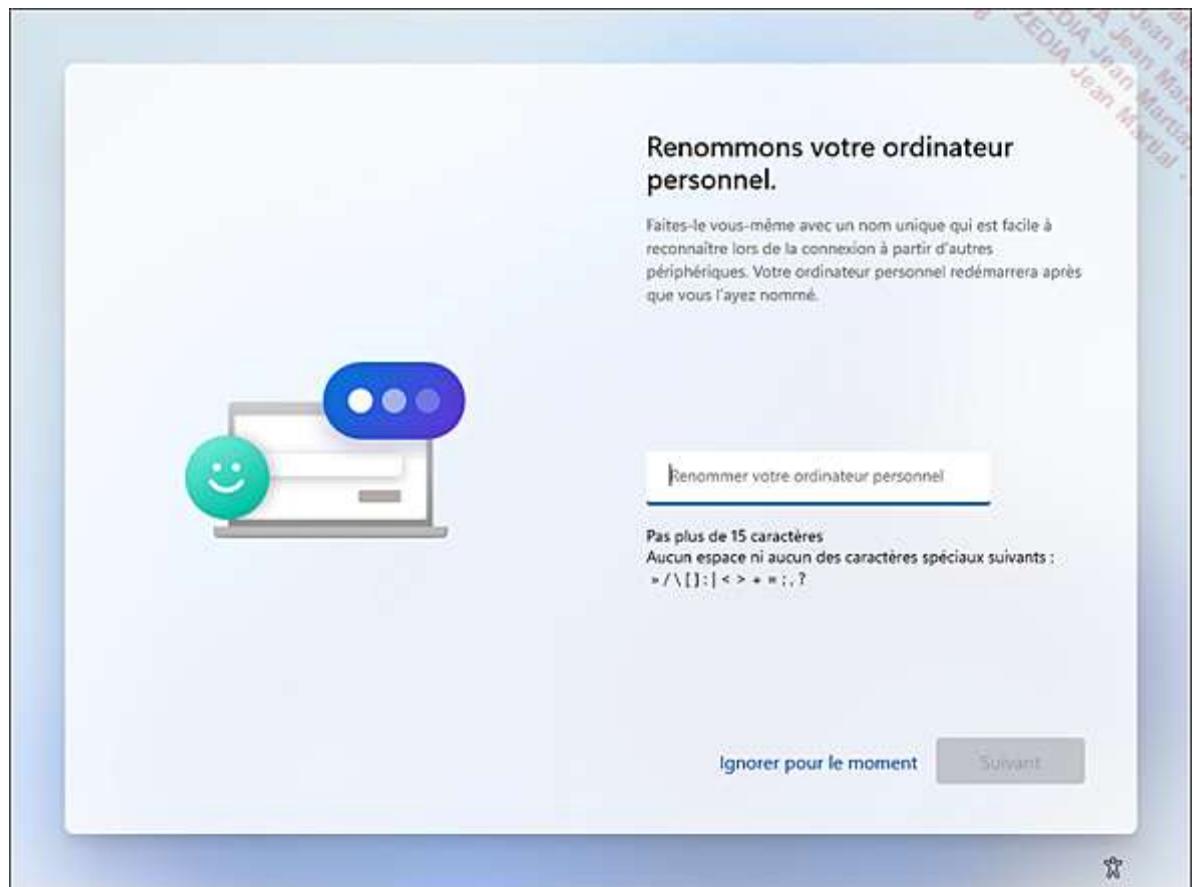


Après le redémarrage automatique de Windows 11, sélectionnez le pays ou la région dans laquelle vous vous trouvez, puis validez en cliquant sur le bouton **Oui**.



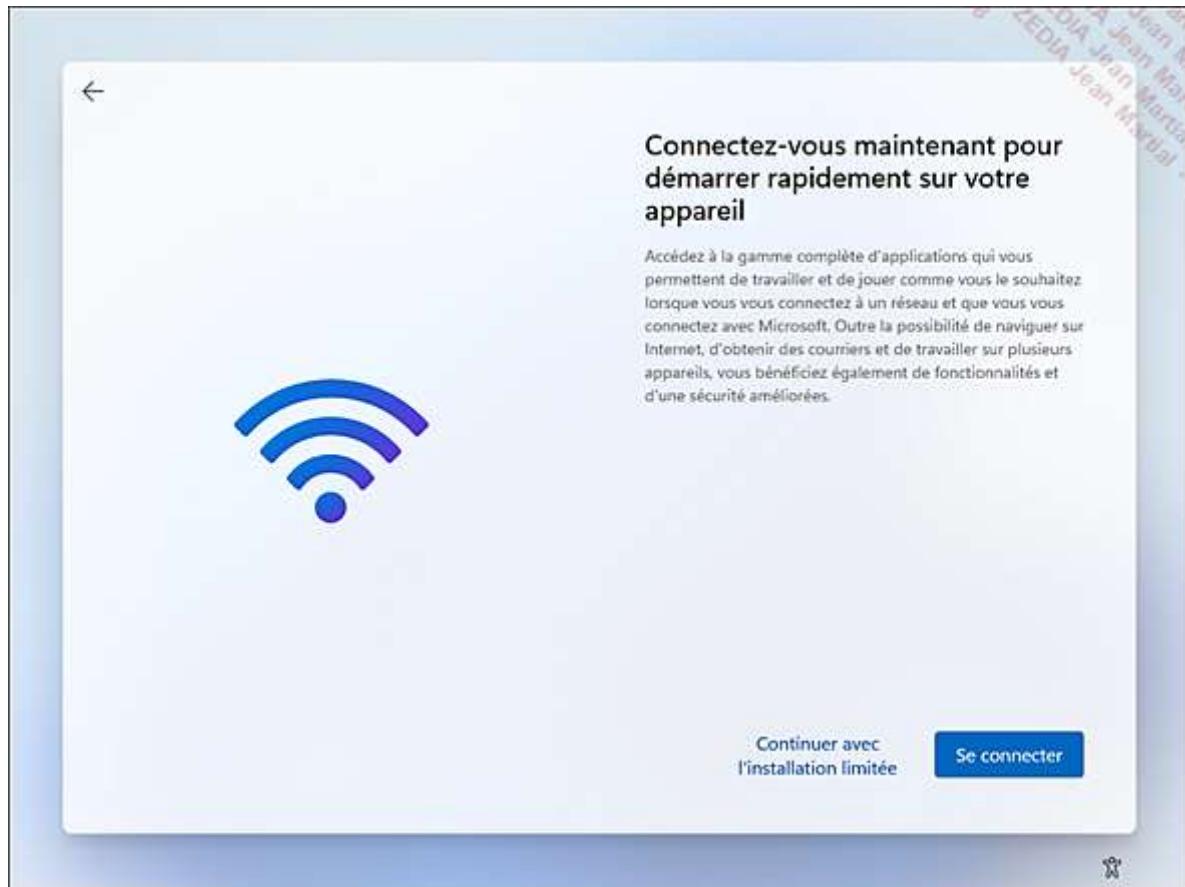
Selectionnez ensuite la disposition du clavier puis cliquez une nouvelle fois sur le bouton **Oui**. Si vous souhaitez ajouter une deuxième langue à votre ordinateur, cliquez sur le bouton **Ajouter une disposition**, sinon passez cette étape en cliquant sur le bouton **Ignorer**.

L'assistant vérifie la présence de mises à jour, propose de renommer votre machine, puis redémarre lorsque vous cliquez sur le bouton **Suivant** :

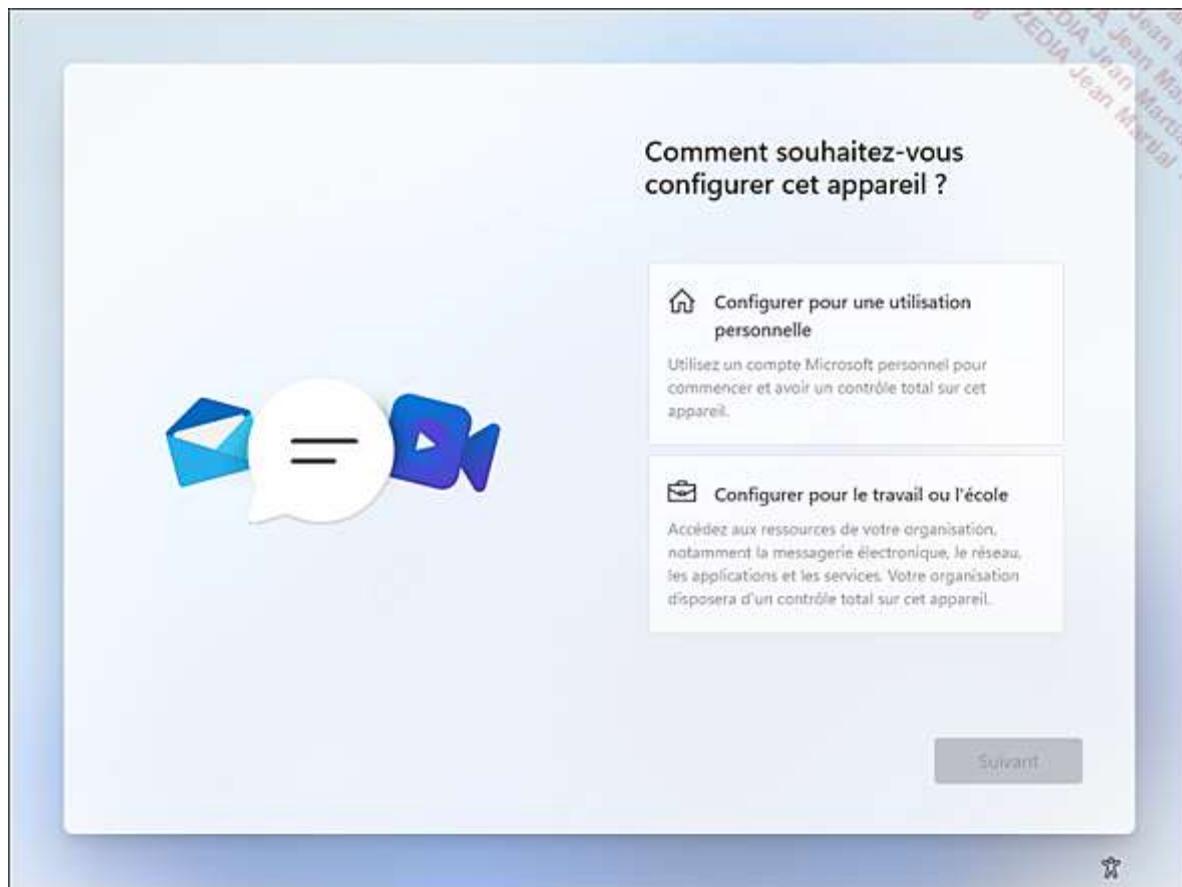


Si aucun réseau n'est détecté, l'assistant vous propose de vous connecter. Si vous n'avez pas de connexion à Internet, cliquez sur le lien **Je n'ai pas Internet**. L'installation va se poursuivre avec la création d'un compte local.

Cliquez sur **Continuer avec l'installation limitée** :

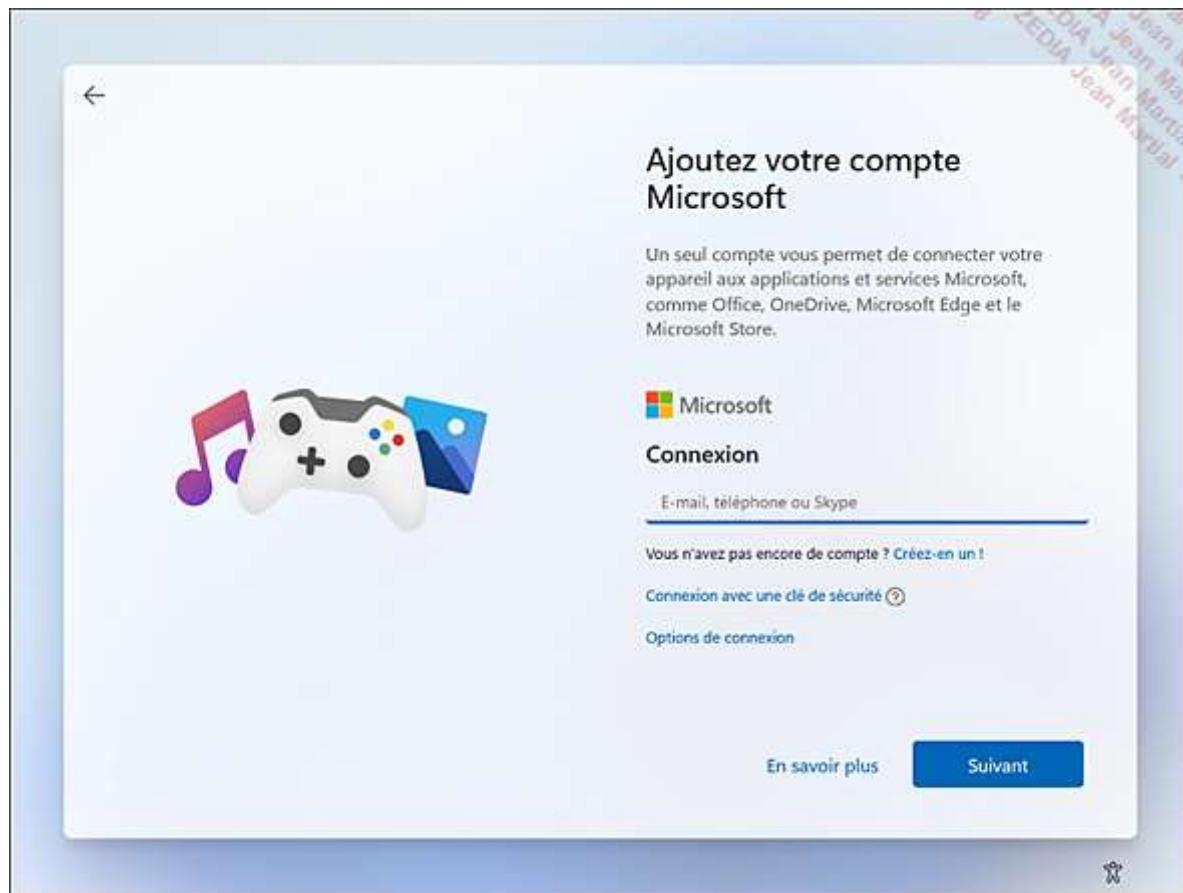


Dans l'autre cas, si une connexion internet est présente, il est ensuite possible de paramétrier votre machine, soit avec votre compte personnel Microsoft, soit avec un compte utilisateur en joignant votre machine à un domaine (uniquement pour les éditions Professionnel, Entreprise ou Education).

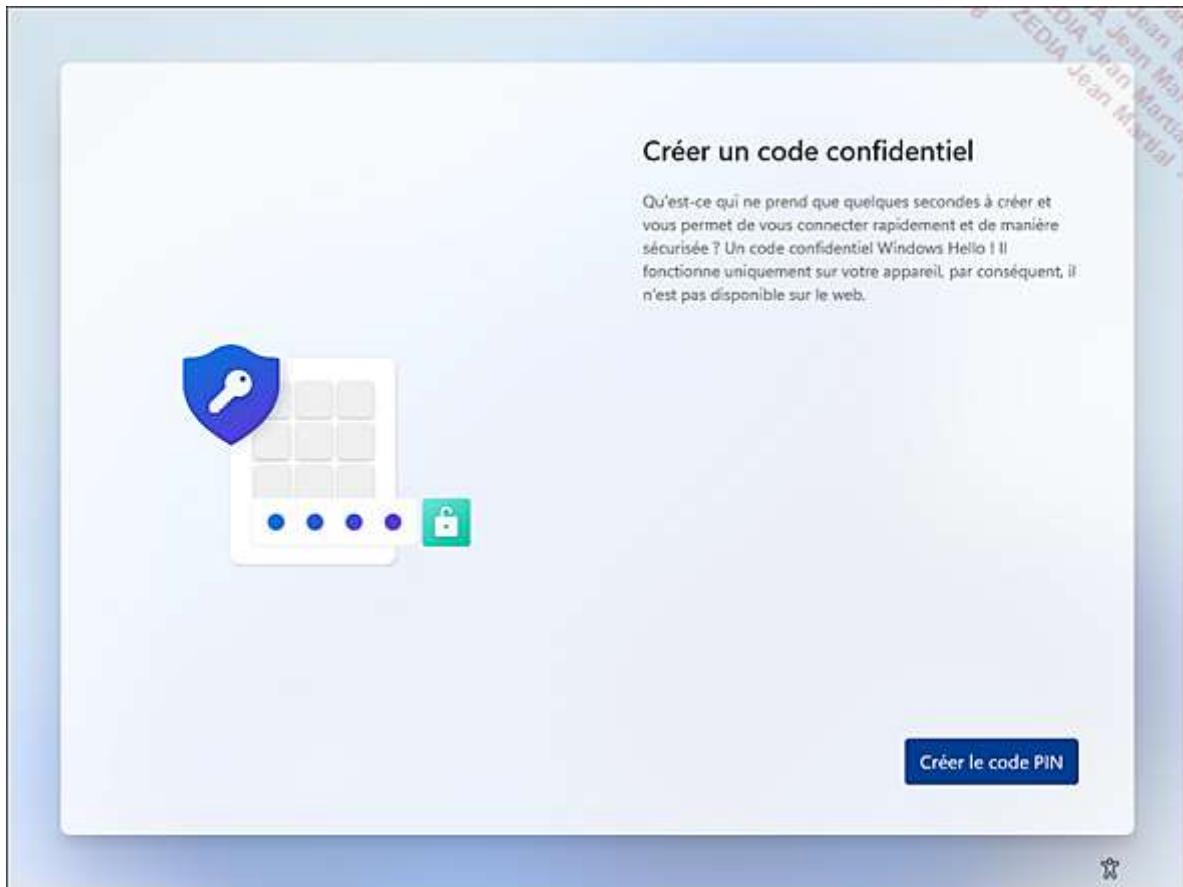


Si vous ne possédez aucun compte de domaine, sélectionnez **Configurer pour une utilisation personnelle** pour que Windows 11 puisse vous proposer d'utiliser un compte personnel Microsoft :

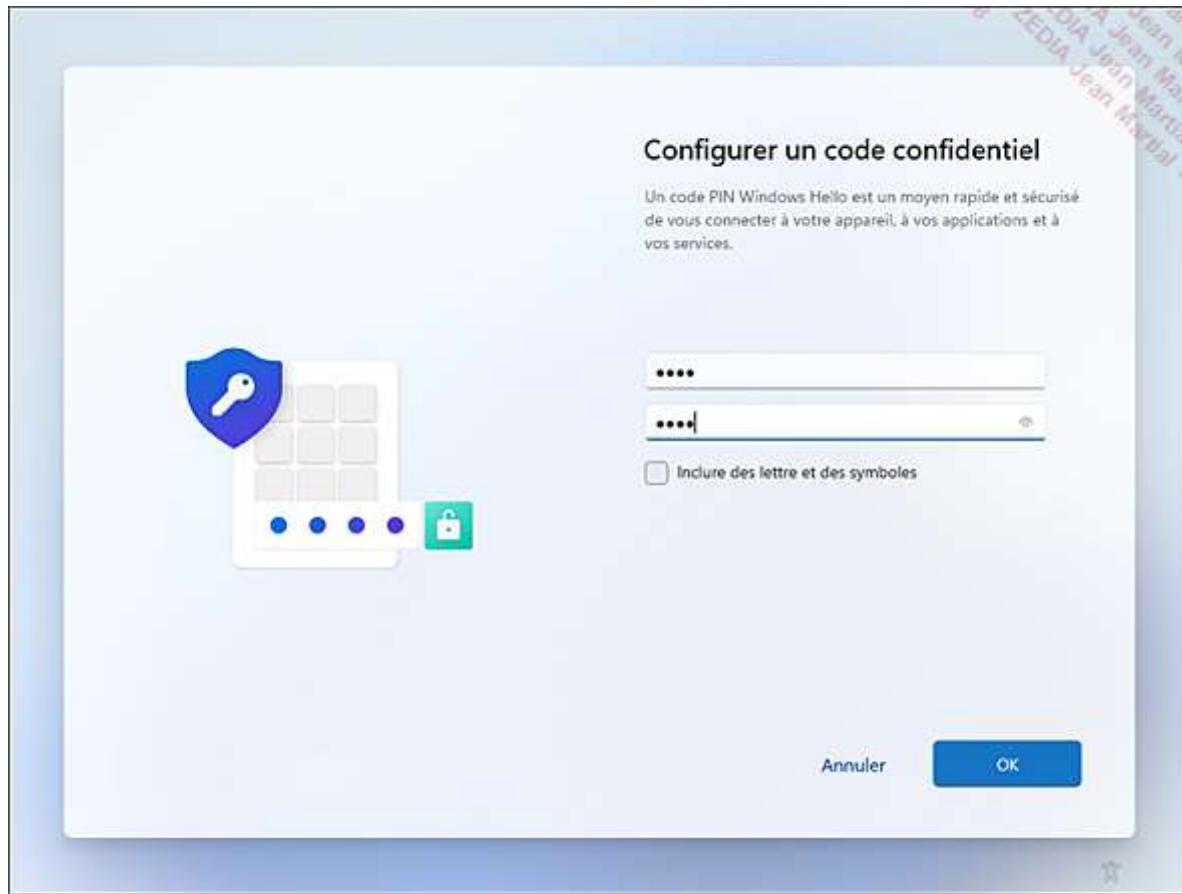
- L'assistant propose maintenant d'utiliser votre compte Microsoft pour vous connecter à la machine. Saisissez l'adresse électronique de la personne qui sera amenée à utiliser la machine et cliquez sur le bouton **Suivant**. Saisissez ensuite le mot de passe associé au compte en cours de création, puis cliquez sur le bouton **Suivant**.



- En plus du mot de passe créé précédemment, l'écran suivant propose de créer un code confidentiel Windows Hello pour se connecter rapidement. Cliquez sur le bouton **Créer le code PIN**.



- Vous avez la possibilité de créer un code PIN numérique ou bien composé de chiffres, lettres et symboles. Pour cela, il suffit de cocher l'option **Inclure des lettres et des symboles**. Saisissez votre code PIN, confirmez-le puis validez avec le bouton **OK**.



Si vous êtes connecté à un domaine, sélectionnez **Configurer pour le travail ou l'école**. C'est cette option que nous allons sélectionner. Cliquez ensuite sur le bouton **Suivant**.

- Entrez votre adresse de messagerie professionnelle et cliquez sur le bouton **Suivant**. Pour les versions Professionnel et Entreprise, le compte Microsoft n'est pas requis, puisque la machine sera potentiellement liée à un domaine Active Directory.
- En cliquant sur **Options de connexion**, il est possible de configurer un compte local (cas où la machine n'est pas connectée au réseau) en cliquant sur **Joindre le domaine à la place**. Le processus de personnalisation est donc quelque peu différent : il est demandé un nom d'utilisateur, un mot de passe et la configuration de trois questions de sécurité.

Microsoft vous propose ensuite de personnaliser votre expérience en définissant vos préférences (emplacement, localisation...). À chaque écran, sélectionnez l'option que vous souhaitez et validez avec le bouton **Accepter**.

Cliquez sur **Non** afin de refuser que Microsoft et les applications installées puissent utiliser votre emplacement pour vous proposer un contenu précis (prévisions météo, itinéraires, etc.). Validez en cliquant sur le bouton **Accepter**.

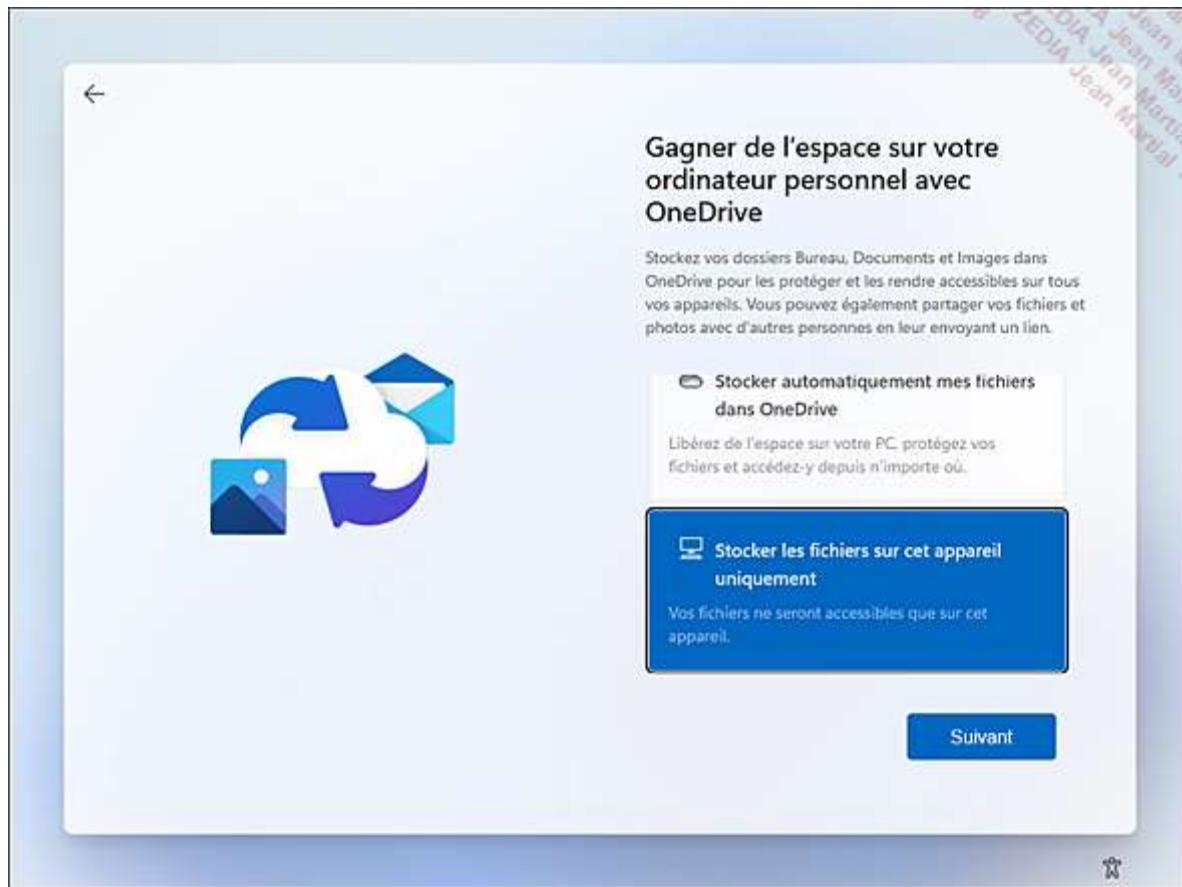
Afin de pallier la perte ou le vol de l'ordinateur, le système propose d'utiliser un composant GPS pour localiser l'ordinateur portable. Cliquez sur **Non** puis sur le bouton **Accepter**.

Cliquez sur **Basique** pour limiter les informations sur votre système envoyées à Microsoft. Validez en cliquant sur le bouton **Accepter**.

Cliquez sur le bouton **Non** pour empêcher Windows 11 d'utiliser vos données pour améliorer la reconnaissance linguistique et les fonctionnalités de suggestions, puis cliquez sur le bouton **Accepter**.

Cliquez sur **Non** pour empêcher les applications d'utiliser l'identifiant de publicité pour afficher des publicités personnalisées. Validez en cliquant sur le bouton **Accepter**.

Si vous avez un accès réseau, Microsoft propose de stocker vos dossiers en ligne avec son service OneDrive. Choisissez l'option de stocker uniquement sur l'appareil et validez avec le bouton **Suivant**.

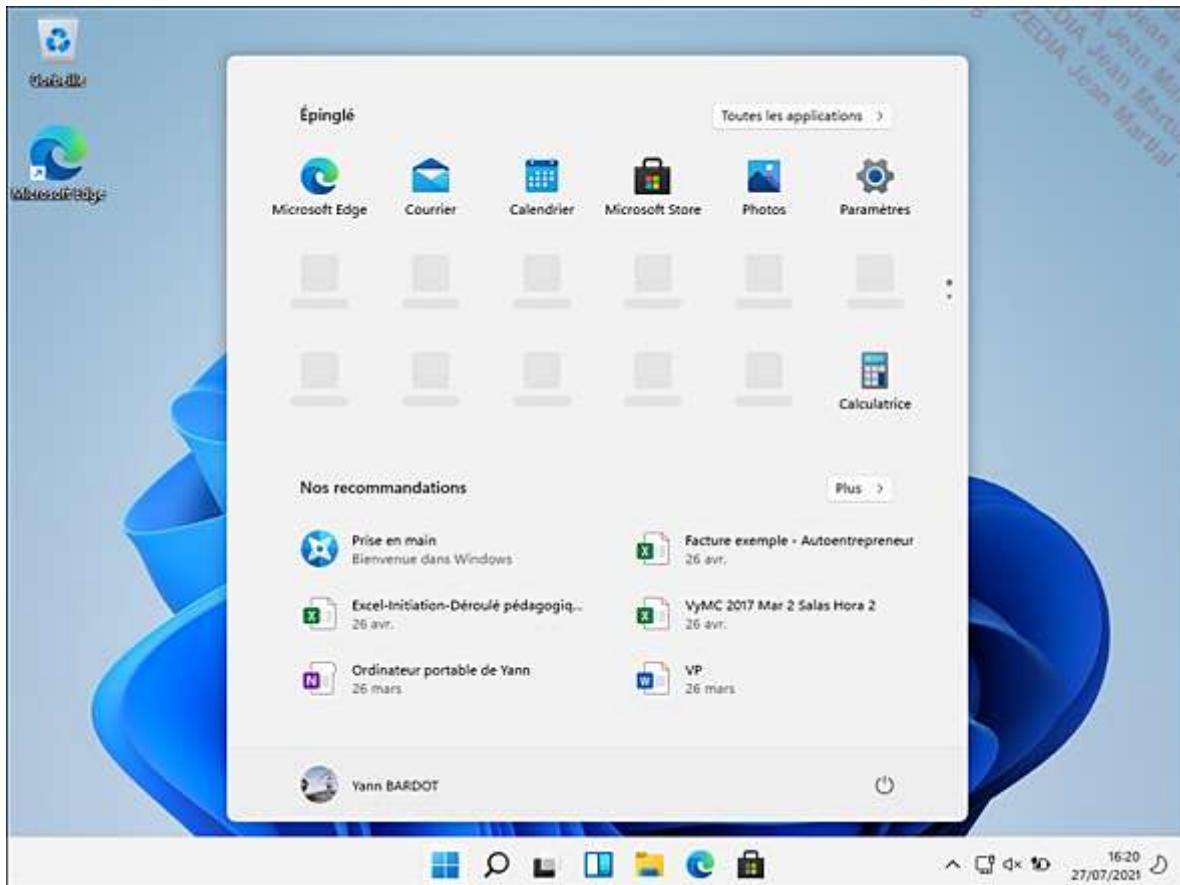


À la proposition d'essai d'Office 365, cliquez sur **Non merci**, sauf si vous possédez déjà une licence.

Si vous le souhaitez, vous pouvez associer votre smartphone Android ou Apple à votre PC. Cliquez sur **Plus tard**.

Windows 11 installe ensuite les applications par défaut du nouveau système.

Une fois ces actions effectuées, la première ouverture de session s'effectue, affichant la nouvelle interface du système.



3. Disque virtuel avec démarrage natif

Un disque virtuel est un fichier contenant les données d'un autre système d'exploitation. Il permet de simuler la présence d'un autre volume physique (disque), tout en ayant les avantages d'un fichier (déplacement, copie, suppression... facilités). Microsoft utilise un fichier au format VHD (*Virtual Hard Disk*) ou VHDX, stocké sur un des volumes de la machine (disque physique, clé USB). Cette fonctionnalité permet de tester un nouveau système sans mettre à jour le système actuel.

Le démarrage natif permet à un disque dur virtuel de s'exécuter sur un ordinateur physique sans hyperviseur tel qu'Hyper-V ou un produit tiers.

Windows 11 Professionnel et Windows 11 Entreprise supportent cette fonctionnalité qui permet donc de disposer de plusieurs systèmes d'exploitation sur son ordinateur, sans nécessairement posséder de système parent.

Microsoft utilise dans cette mouture un format de disque virtuel qui supprime la limite de 2 To proposée initialement par un fichier VHD : c'est le format VHDX, qui prend en charge jusqu'à 64 To par disque virtuel tout en assurant une tolérance de panne. Un disque VHDX n'est compatible qu'avec les systèmes d'exploitation Windows 8.1, Windows Server 2012 ainsi que les versions supérieures.

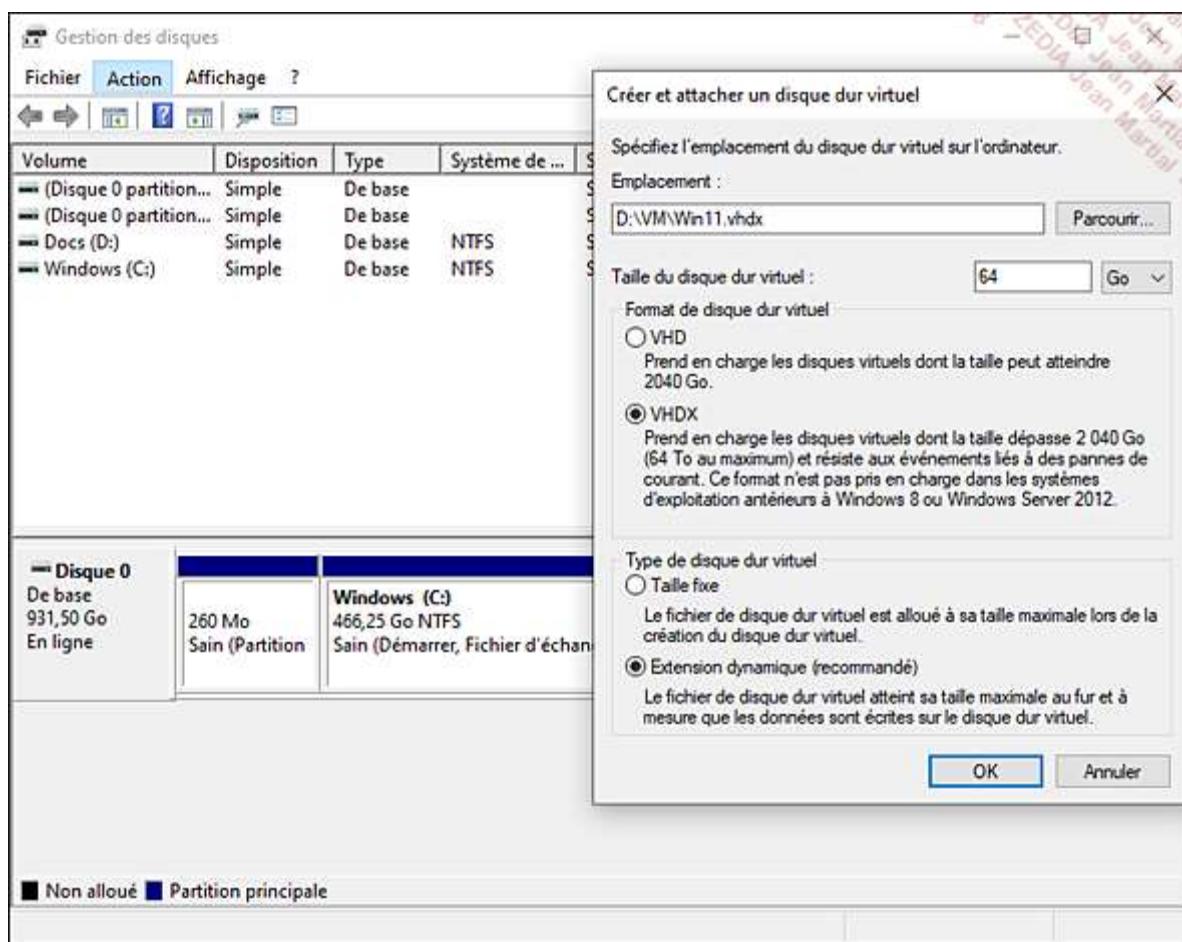
Il est conseillé de définir une taille fixe lors de la création d'un fichier VHD, et de définir une taille dynamique pour un fichier VHDX (format plus efficace pour la gestion des disques de grande capacité).

Pour créer un disque dur virtuel VHDX, il est nécessaire d'utiliser la console **Gestion des disques** :

Depuis le champ de recherche situé dans la barre des tâches de Windows 11, saisissez gestion des disques et sélectionnez **Créer et formater des partitions de disque dur**.

Dans la console MMC (*Microsoft Management Console*) **Gestion des disques**, cliquez sur le menu **Action**, puis sur **Créer un disque virtuel**.

Spécifiez ensuite l'emplacement de stockage du fichier VHDX sur le disque dur, ainsi que la taille allouée (fixe ou dynamique). Dans notre exemple, nous choisissons une taille dynamique de **64 Go** pour le fichier de disque dur virtuel VHDX situé dans le dossier **d:\VM** (ce dossier doit être préalablement créé).



20 Le fichier VHDX est désormais visible comme n'importe quel disque dur physique dans la console **Gestion des disques** ou depuis une invite de commandes, grâce à l'utilitaire **DiskPart** (cf. chapitre Gestion des disques et des pilotes section Partitionnement et gestion des fichiers). À l'aide de ce dernier, tapez les commandes suivantes :

diskpart

puis

list vdisk

```
PS C:\WINDOWS\system32> diskpart
Microsoft DiskPart version 10.0.19041.964
Copyright (C) Microsoft Corporation.
Sur l'ordinateur : YOGAYB
DISKPART> list vdisk
VDisk ###  Disque ###  État          Type      Fichier
VDisk 0   Disque 1   Attaché, non ouvert  Extensible D:\VM\Win11.vhdx
DISKPART>
```

Une fois le disque virtuel VHDX créé, il est nécessaire d'y installer Windows 11 :

Redémarrez l'ordinateur à l'aide du support d'installation Windows 11 (DVD-ROM ou mémoire flash USB), puis lorsque l'écran de partitionnement des disques apparaît, pressez les touches [Shift]+[F10] afin d'exécuter une invite de commandes.

Ouvrez l'utilitaire de gestion des disques. Sélectionnez le fichier VHDX à l'aide de la commande diskpart.

Puis, sélectionnez le disque virtuel à utiliser, X étant la lettre de lecteur contenant le fichier VHDX précédemment créé : select vdisk file=X:\VM\FICHIER.VHDX

Attachez ensuite le disque dur virtuel : attach vdisk.

Fermez l'invite de commandes en tapant exit puis validez par la touche [Entrée].

Cliquez sur **Actualiser** dans l'interface de partitionnement des disques et sélectionnez le disque virtuel VHDX possédant la lettre X, puis continuez la procédure d'installation du système d'exploitation Windows 11.

Une fois l'installation terminée, votre ordinateur démarrera depuis un fichier virtuel VHDX en mode natif.

En sélectionnant le disque virtuel Windows 11 nouvellement créé, puis en cliquant sur le menu **Action - Détacher un disque virtuel**, l'utilisateur peut copier le fichier VHDX sur un autre ordinateur (par exemple Windows Server 2019) pourvu d'Hyper-V et ainsi importer l'ordinateur virtuel.

Mise à niveau vers Windows 11

La mise à niveau consiste à installer Windows 11 sur une version plus ancienne, afin de remplacer cette dernière sans devoir réinstaller les applications, l'environnement de l'utilisateur ou encore restaurer ses données. Elle est gratuite pour les utilisateurs possédant une licence Windows 7, 8.1 et 10.

L'utilisateur peut être contraint d'effectuer une mise à niveau, par exemple si le volume des données à sauvegarder est trop important par rapport au support de sauvegarde disponible.

La mise à niveau vers Windows 11 est possible depuis Windows 10 (20H1), 8.1 (build 9600) et Windows 7. Bien entendu, la configuration matérielle doit également le permettre. De plus, le microprogramme doit être UEFI, le Secure Boot doit être activé. Si besoin, le disque sera converti au format GPT.

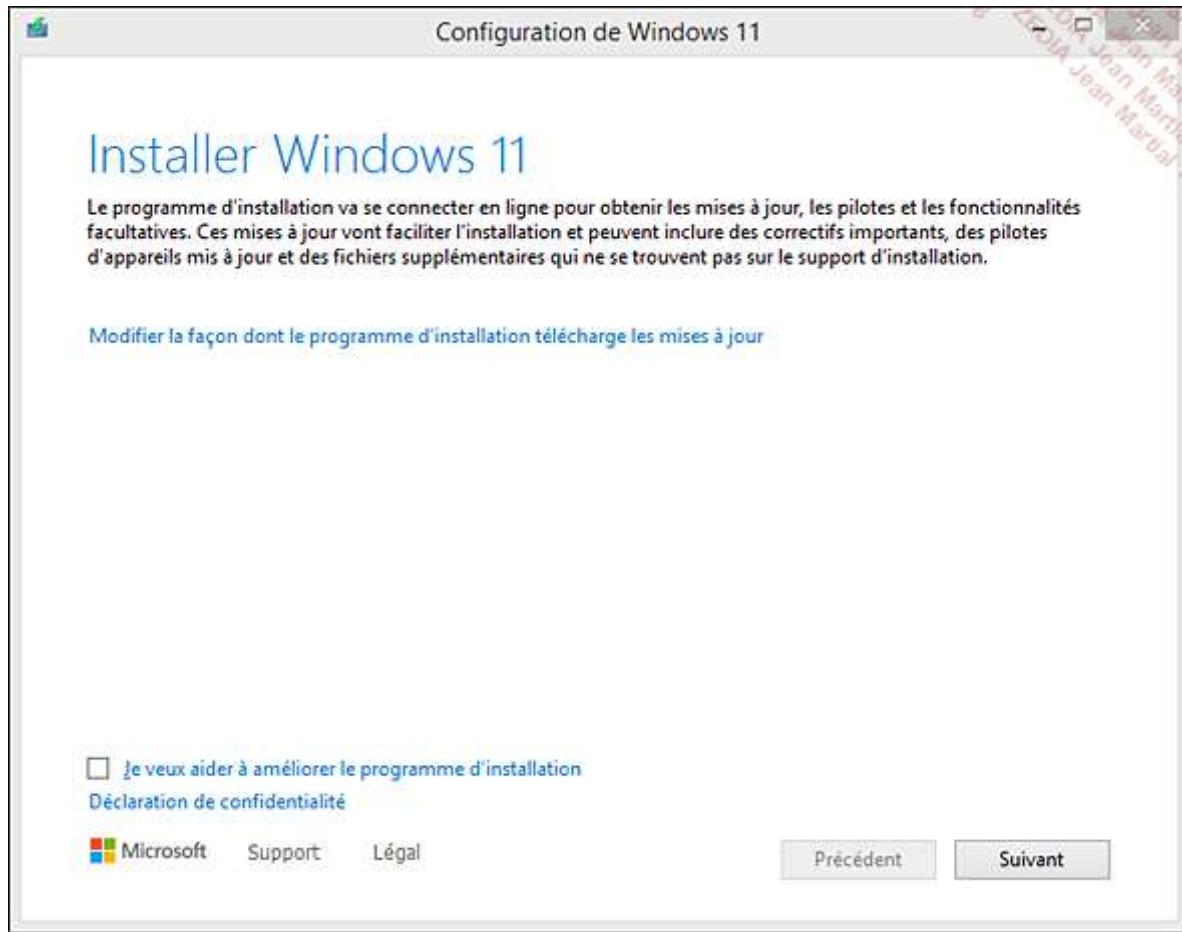
Sur un poste disposant de Windows 10, le plus simple consiste à utiliser la fonctionnalité **Windows Update** disponible depuis **Paramètres, Mises à jour et sécurité** grâce au bouton **Recherchez des mises à jour**. Microsoft a, en effet, intégré le processus de vérification dans Windows Update. Si la mise à jour vers Windows 11 est disponible et votre ordinateur compatible, elle sera proposée.

Le déploiement mondial de la nouvelle version se faisant progressivement, il ne sera pas forcément possible d'actualiser son ordinateur dans l'immédiat. Vous pourrez alors soit patienter jusqu'à ce que la mise à jour vous soit proposée, soit utiliser la méthode présentée ci-après.

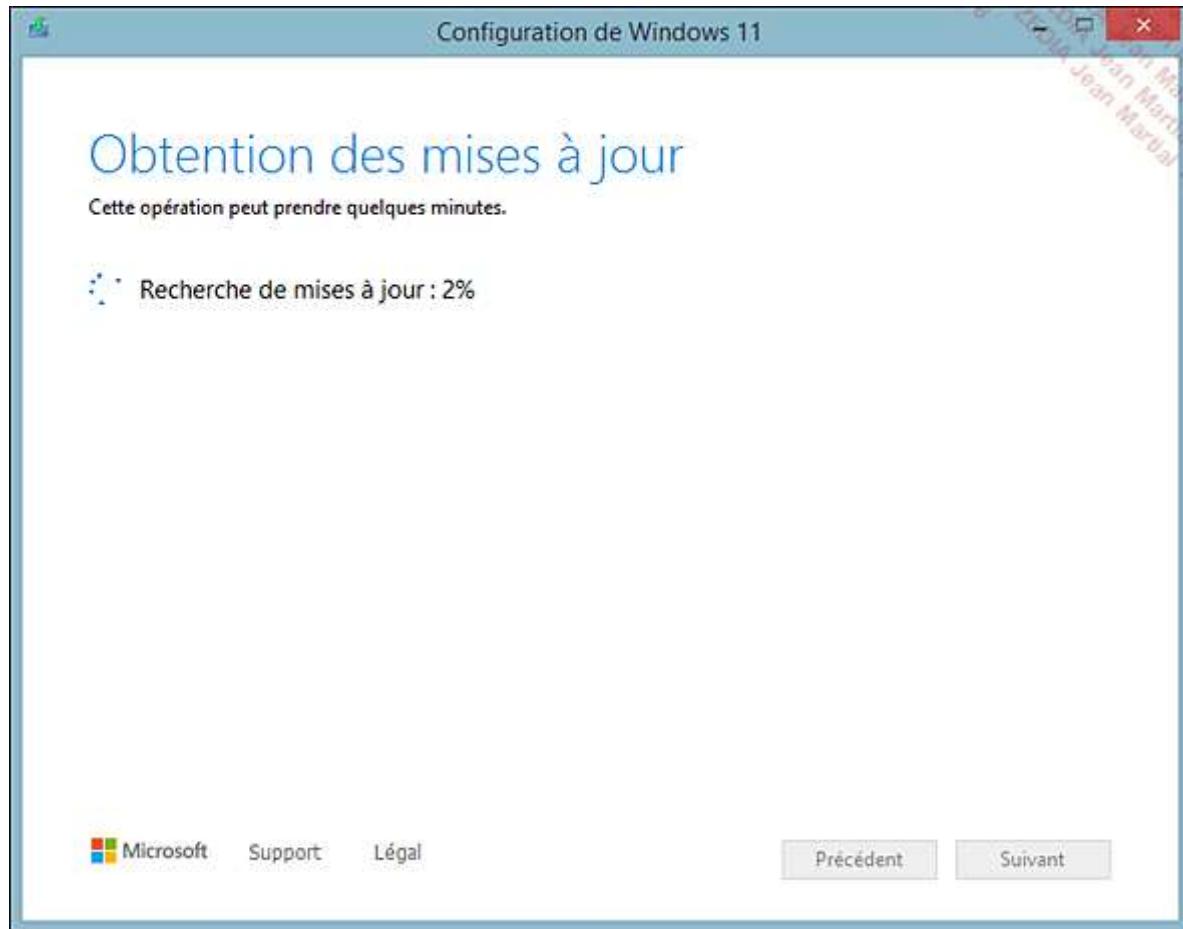
Une autre manière de procéder est d'utiliser le média d'installation. La procédure est la suivante :

Démarrez le poste et connectez-vous au système, puis insérez le média d'installation préalablement créé (DVD, clé USB, fichier ISO).

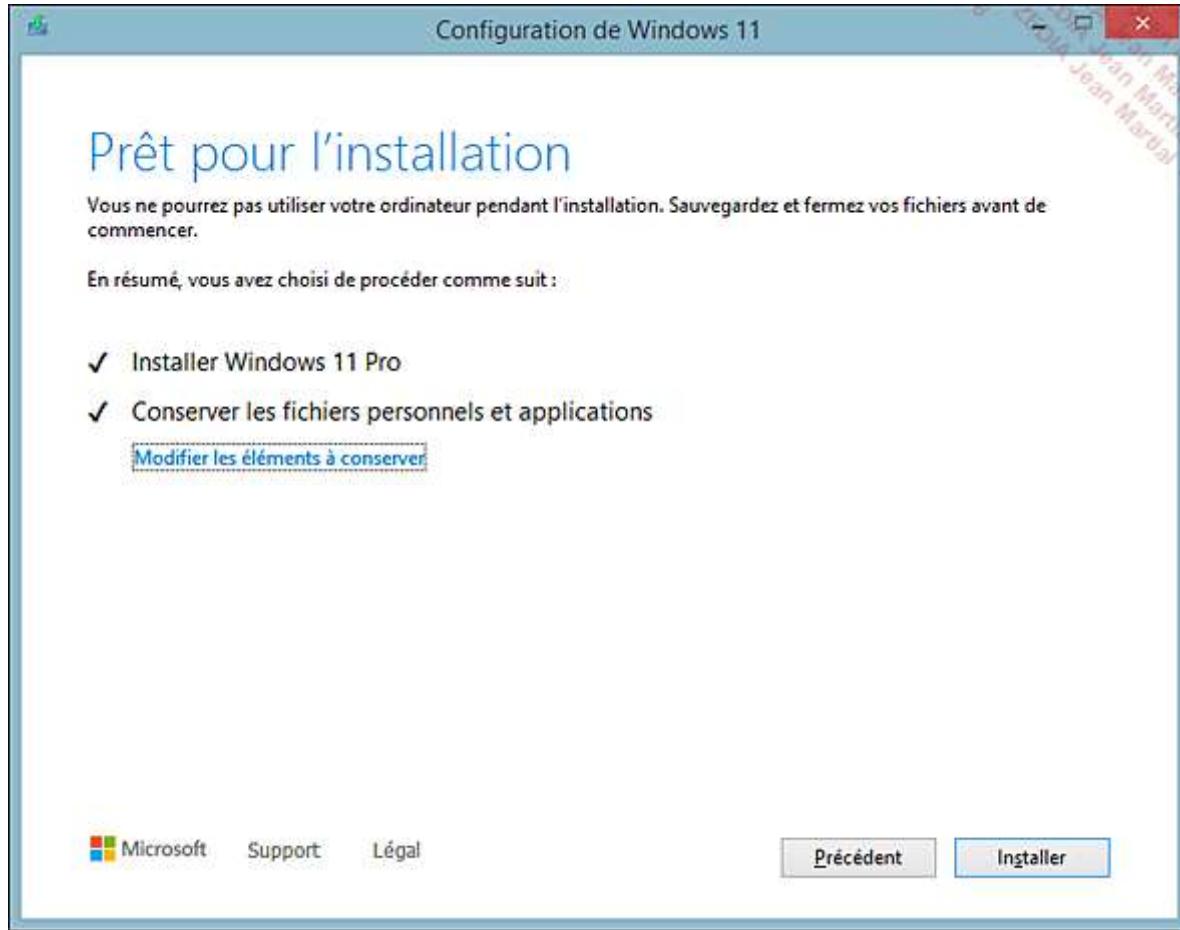
Depuis l'**Explorateur de fichiers**, développez le lecteur du média et double cliquez sur le fichier **setup.exe**. Le programme d'installation s'exécute. Cliquez sur le bouton **Suivant**.



Acceptez les avis et conditions du contrat de licence en cliquant sur le bouton **Accepter**. L'assistant téléchargera ensuite les mises à jour, puis vérifie que la machine est prête à effectuer l'installation.



Une fois les mises à jour téléchargées, cliquez sur le bouton **Installer**. L'installation démarre. La machine va redémarrer à plusieurs reprises.



En cliquant sur le lien **Modifier les éléments à conserver**, vous avez la possibilité de personnaliser votre installation :

- **Conserver les fichiers personnels et applications** permet de garder vos documents et applications.
- **Conserver uniquement les fichiers personnels** conserve uniquement vos documents personnels.
- **Rien** : permet de partir de profils vierges.

Dans certains cas, il est possible que l'option **Conserver les fichiers personnels et applications** ne soit pas proposée ; par conséquent, seules les données personnelles pourront être conservées.

Ce procédé d'installation est idéal pour les petites entreprises, mais la migration avec transfert des paramètres utilisateur et des données sera privilégiée dans les grands groupes.

Si vos périphériques fonctionnaient avec Windows 10, Microsoft assure leur compatibilité avec Windows 11. Il n'y a donc aucun souci à avoir.

Notez qu'il est possible de rétrograder vers Windows 10 dans un délai de 10 jours après la mise à niveau. Passé cette période, l'unique moyen de retrouver un environnement Windows 10 sera de passer par une réinstallation totale du système.

1. Mise à jour d'une ancienne version de Windows 10

À la date d'écriture de cet ouvrage, Windows 10 21H1 est la dernière version du système d'exploitation client proposé par Microsoft. Plusieurs fois par an, une nouvelle mise à jour du système est proposée aux utilisateurs.

Pour connaître la version actuelle de votre système d'exploitation, cliquez sur le bouton du menu **Démarrer** situé en bas à gauche, puis sur le bouton **Paramètres**.

Cliquez ensuite sur **Système**, puis sur **À propos de**.

The screenshot shows the Windows Settings interface under the 'Système' (System) category. On the left, a sidebar lists various system settings like Affichage (Display), Son (Sound), Notifications et actions (Notifications and actions), Assistant de concentration (Concentration Assistant), Alimentation et mise en veille (Power and sleep), Batterie (Battery), Stockage (Storage), Tablette (Tablet), Multitâche (Multitasking), Projection sur ce PC (Project to this PC), Expériences partagées (Shared experiences), Presse-papiers (Clipboard), Bureau à distance (Remote Desktop), and À propos de (About). The 'À propos de' item is currently selected. The main pane displays the following information:

À propos de

Votre ordinateur est surveillé et protégé.
Voir les détails dans la sécurité Windows

Spécifications de l'appareil

Thinkpad YOGA 370 Signature Edition

Nom de l'appareil	YOGAYB
Processeur	Intel(R) Core(TM) i5-7300U CPU @ 2.60GHz 2.71 GHz
Mémoire RAM installée	8.00 Go (7.84 Go utilisable)
ID de périphérique	69423584-9D9B-48FA-A38E-E8D4D2F57176
ID de produit	00330-80000-00000-AA714
Type du système	Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile	Prise en charge du stylet et de la fonction tactile avec 10 points de contact

Copier

Renommer ce PC

Spécifications de Windows

Édition	Windows 10 Professionnel
Version	21H1
Installé le	16/01/2021
Build du système d'exploitation	19043.1149
Numéro de série	MP1CBEPA
Expérience	Windows Feature Experience Pack 120.2212.3920.0

Pour mettre à jour Windows 10 vers la dernière version disponible du système d'exploitation :

Exécutez un navigateur internet puis ouvrez la page suivante : <https://www.microsoft.com/fr-fr/software-download/windows10>

Téléchargez le fichier **Windows10Upgrade9252.exe** en cliquant sur le bouton **Mettre à jour maintenant**. Exécutez le fichier. L'écran de mise à niveau apparaît.



Cliquez sur le bouton **Mettre à jour maintenant**. L'assistant vérifie les prérequis nécessaires à la mise à niveau, tels que l'espace disque disponible sur le disque C:, la puissance du processeur, la quantité de mémoire vive...

Une fois la mise à jour effectuée, vous bénéficierez des dernières fonctionnalités proposées par Microsoft avec Windows 10.

Il est nécessaire d'effectuer la procédure ci-dessus car la mise à niveau vers Windows 11 n'est possible que depuis la version 20H1 ou ultérieure de Windows 10.

L'assistant de mise à jour n'est pas disponible avec l'édition Entreprise de Windows 10. Dans ce cas, il sera nécessaire d'utiliser un fichier ISO ou d'adhérer au programme Insider Preview.

2. Mise à niveau vers Windows 10

Dans certains cas, il est possible que la mise à niveau depuis Windows 7 ou 8.1 ne fonctionne pas. Il faut alors procéder par étapes :

Mettre à niveau le système d'exploitation vers Windows 10.

Puis vers Windows 11.

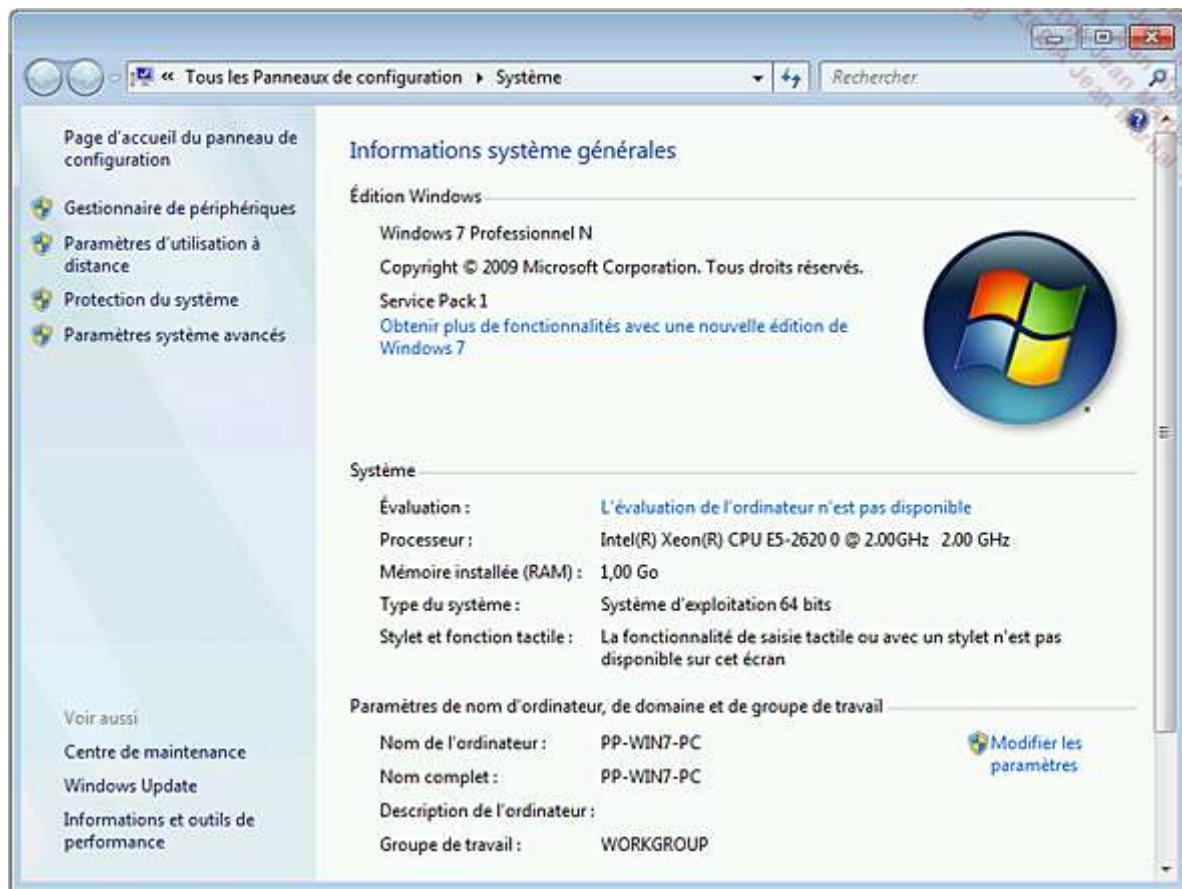
L'étape de mise à niveau vers Windows 11 ayant été vue précédemment dans ce chapitre, cette partie traitera uniquement de la mise à niveau vers Windows 10.

Pour effectuer la mise à niveau vers Windows 10, assurez-vous tout d'abord de disposer d'un support d'installation (DVD ou clé USB) de Windows 10 version 20H1 ou ultérieure. Cela vous évitera de devoir ensuite faire une mise à jour de Windows 10 vers la dernière version de celui-ci.

Branchez sur le secteur vos périphériques, tels que des imprimantes et des moniteurs, et connectez-les à votre ordinateur avant d'exécuter l'Assistant Mise à niveau, afin de vérifier s'ils fonctionneront avec Windows 10.

Pour connaître la version exacte de Windows 7 utilisée, suivez la procédure ci-dessous :

Depuis votre poste de travail, cliquez sur le menu **Démarrer** puis effectuez un clic avec le bouton droit sur **Ordinateur** et sélectionnez **Propriétés**. Dans la fenêtre qui apparaît, notez la version de l'édition Windows.



Avant d'effectuer une mise à niveau, notez que ce procédé ne prend pas en charge le passage d'une architecture 32 bits vers 64 bits, et inversement.

Le processus de mise à niveau s'effectue de deux manières au choix : depuis le support d'installation (DVD, périphérique USB) ou depuis le réseau internet.

a. Mise à niveau depuis le support d'installation

Si vous disposez du support DVD ou de la clé USB contenant les dernières sources de Windows 10, démarrez le poste à mettre à niveau, puis insérez le support. Si le processus d'installation ne se lance pas automatiquement, exécutez le fichier **setup.exe**.

Cliquez sur le bouton **Suivant** et suivez la procédure d'installation. Le poste redémarrera automatiquement.

b. Mise à niveau depuis Internet

Si vous ne disposez pas du média d'installation, vous pouvez utiliser les outils mis en ligne par Microsoft pour mettre à niveau Windows 7 ou 8.1 vers la dernière version disponible de Windows 10. Les deux options à suivre s'offrent à vous.

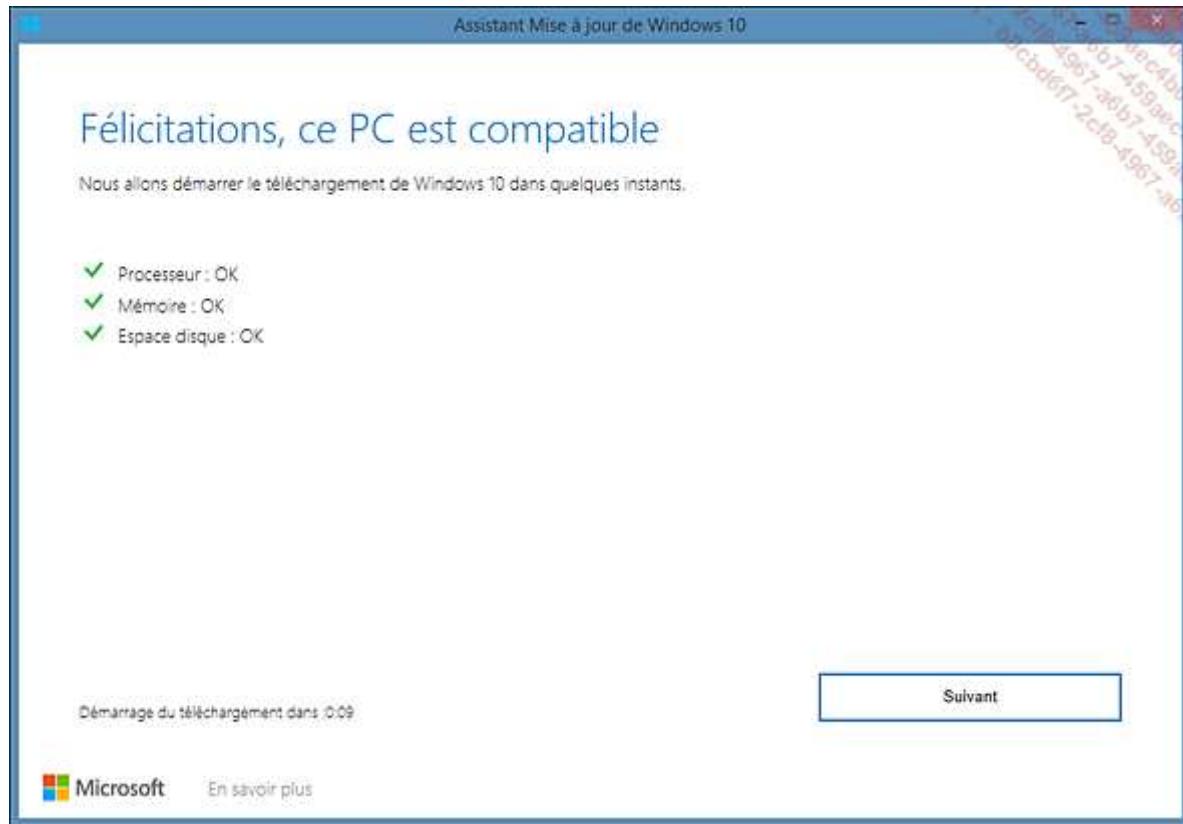
Outil de mise à jour Windows 10

Depuis un poste disposant de Windows 10, ouvrez un navigateur internet et rendez-vous à l'adresse suivante : <https://www.microsoft.com/fr-fr/software-download/windows10>

Téléchargez le fichier **Windows10Upgrade9252.exe** en cliquant sur le bouton **Mettre à jour maintenant**.

Copiez ce fichier sur le poste à mettre à niveau et exécutez le fichier.

Acceptez le contrat de licence, l'écran de mise à niveau apparaît. L'assistant commence par vérifier les prérequis nécessaires à la mise à niveau, tels que l'espace disque disponible sur le disque C:, la puissance du processeur, la quantité de mémoire vive... Si le système est compatible, le téléchargement des données commence et la procédure se poursuit automatiquement.



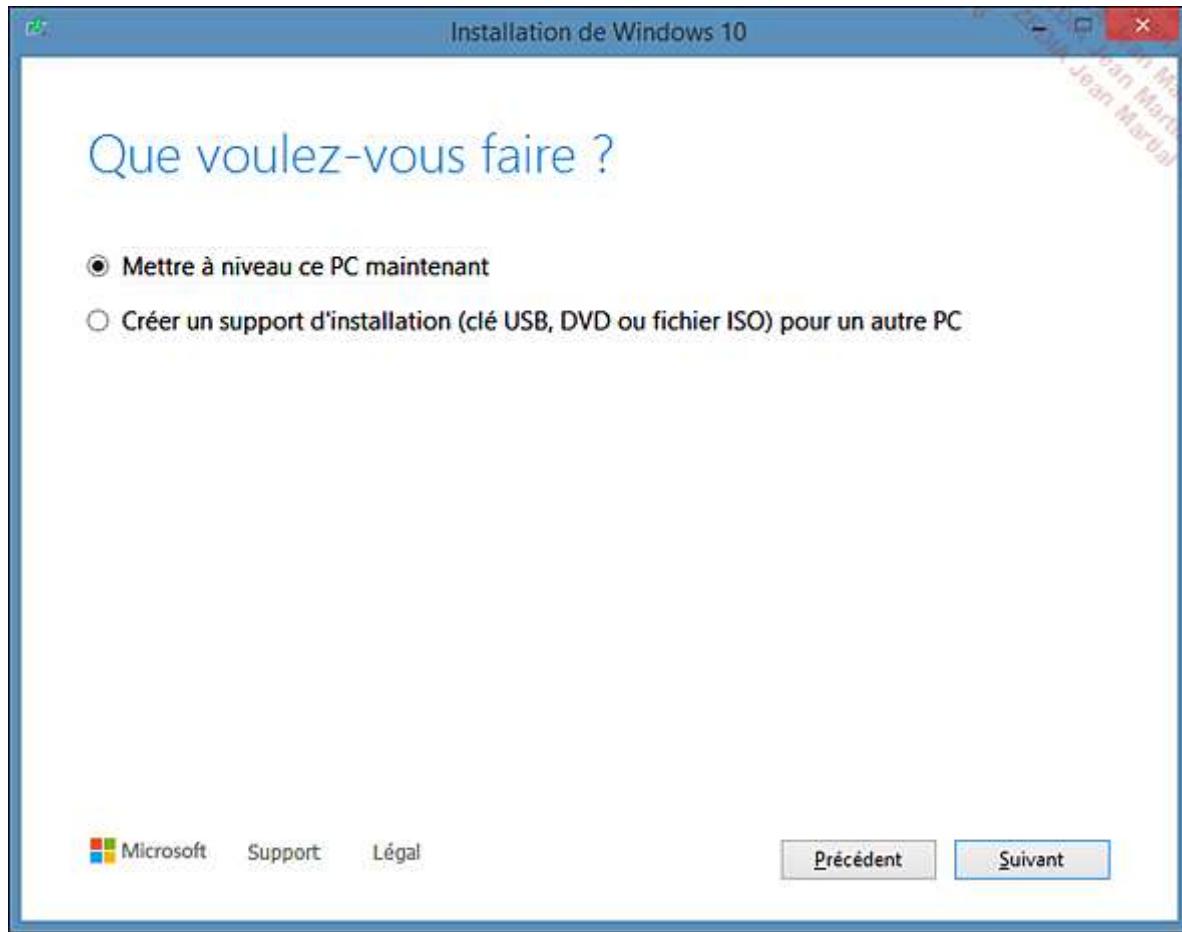
Une fois la mise à jour effectuée, vous bénéficieriez de la dernière version de Windows 10 et pourrez ensuite la mettre à niveau vers Windows 11.

Outil de création de support

Depuis le poste à mettre à niveau, ouvrez un navigateur internet et rendez-vous à l'adresse suivante : <https://www.microsoft.com/fr-fr/software-download/windows10>

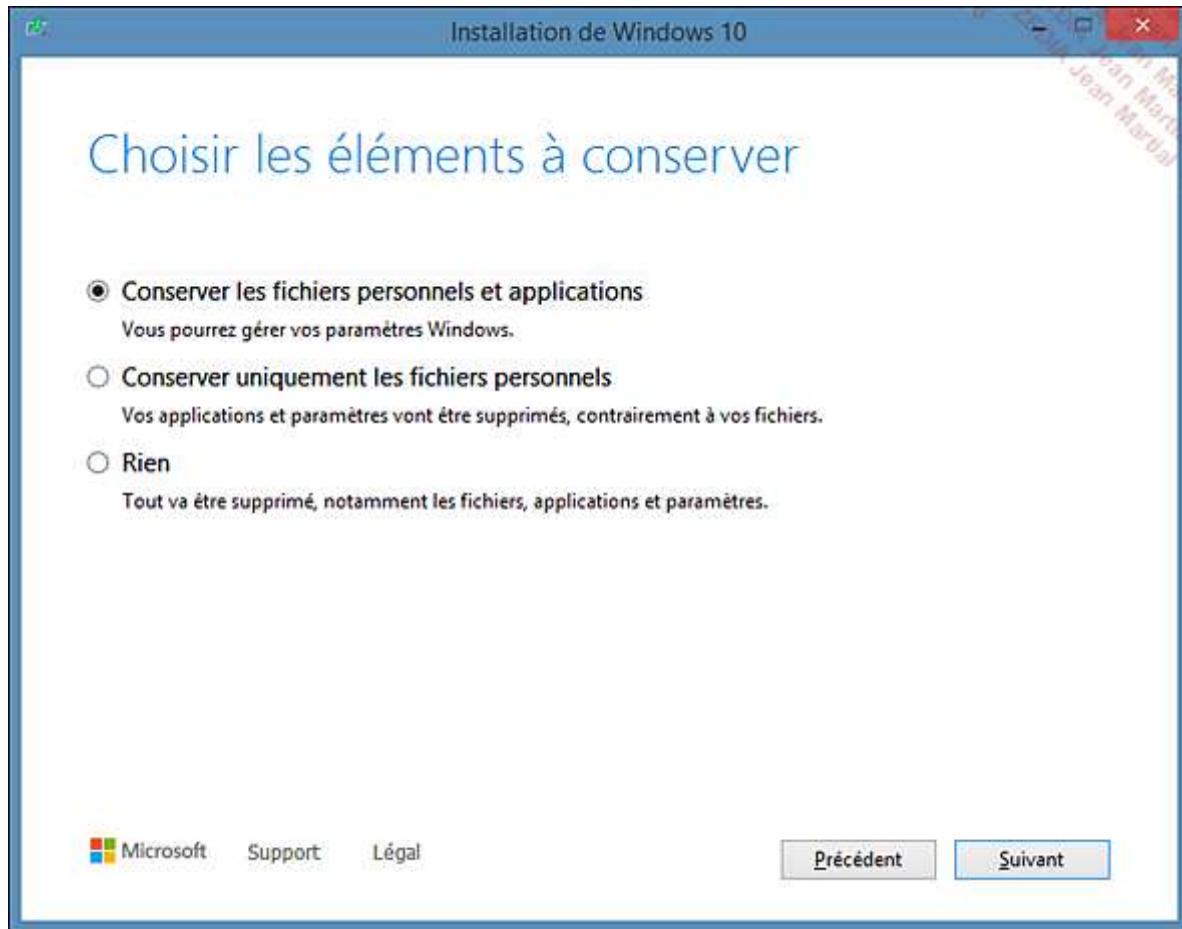
Téléchargez le fichier **MediaCreationTool21H1.exe** en cliquant sur le bouton **Télécharger maintenant l'outil**.

Exécutez le fichier et acceptez le contrat de licence. L'écran de mise à niveau apparaît.



Sélectionnez **Mettre à niveau ce PC maintenant** et cliquez sur le bouton **Suivant**. Le téléchargement de Windows 10 commence...

Acceptez de nouveau le contrat de licence puis sélectionnez les éléments à conserver, généralement **Conserver les fichiers personnels et applications**.



La procédure se poursuit automatiquement.

Microsoft conseille d'exécuter une mise à niveau depuis un système parent plutôt que de démarrer l'ordinateur depuis le DVD d'installation Windows 10, ceci afin de conserver toutes les données, programmes et paramètres de l'utilisateur.

Migration vers Windows 11

Il est parfois préférable de partir sur une installation vierge de Windows 11, tout en conservant les données personnelles. Dans ce cas, il est nécessaire de sauvegarder les données des utilisateurs (outils **Transfert de fichiers et paramètres** ou USMT), d'effacer l'ancien système d'exploitation et enfin d'installer Windows 11 : c'est le processus de migration.

Le principal inconvénient est la nécessité de réinstaller les applications et les pilotes, et surtout de restaurer les données. Ce procédé garantit néanmoins que tous les ordinateurs migrés démarreront avec les mêmes paramètres et applications, puisqu'il est basé sur une nouvelle installation.

Avant chaque migration, il est nécessaire d'identifier les composants à migrer :

- Comptes d'utilisateurs : doit-on migrer tous les comptes locaux, ou bien uniquement ceux des utilisateurs réguliers ?
- Paramètres de logiciel et du système d'exploitation : apparence des fenêtres, polices, comptes de messagerie...
- Fichiers et dossiers : quels fichiers et dossiers doivent être sauvegardés ? De quels types (documents, vidéos, images, etc.) ? Sur quelle partition ?

1. Sauvegarder et restaurer Windows

Pour procéder à la migration, Microsoft propose un outil nommé **Sauvegarder et restaurer (Windows 7)**, idéal pour migrer un petit nombre d'ordinateurs. La sauvegarde peut être effectuée vers un partage réseau, une partition de données ou un périphérique externe puis être restaurée sur le système Windows 11 fraîchement déployé. Cet utilitaire est détaillé dans le chapitre Protection et récupération du système.

Dans le cas où la migration s'effectuerait sur un grand nombre de postes, préférez l'outil de migration utilisateur USMT (*User State Migration Tool*).

2. USMT

USMT pour Windows 11 est un outil en ligne de commande scriptable permettant de migrer l'environnement de travail des utilisateurs à grande échelle. En utilisant conjointement USMT et les services de déploiement Windows Deployment Server, il est possible de migrer des postes sans aucune intervention, en insérant les commandes USMT dans un script d'ouverture de session.

USMT est livré avec le kit Windows ADK (cf. chapitre Conception d'une image de déploiement, section Création d'une installation de référence).

Deux composants sont utilisés pour migrer efficacement l'environnement des utilisateurs :

- **ScanState** : la commande analyse l'ordinateur source, sauvegarde les fichiers et les paramètres en les compressant puis crée un magasin. Sa syntaxe est la suivante :
 - `scanstate [Chemindestockageréseau] [/i:[cheminverslesfichiersxml]]`

[Options]

- Parmi les nouveautés liées à cette nouvelle version d'USMT, signalons les paramètres **/apps /ppkg /drivers** permettant de sauvegarder les pilotes de périphériques installés sur une machine et de sauvegarder l'état des applications pour un déploiement ultérieur.
- Par exemple, pour créer ou recréer (/o) un magasin dans un dossier réseau, selon les règles définies dans les fichiers de configuration xml, avec un niveau de log maximal (/v:13), on utilisera la commande :

```
scanstate \\server\share\mondossiermigration /i:MigApp.xml
```

```
/i:MigDocs.xml /o /config:config.xml /v:13
```

- **LoadState** : migre les fichiers et les paramètres du magasin créé avec ScanState vers l'ordinateur de destination. Il est nécessaire d'installer les applications sur l'ordinateur de destination avant de restaurer les données, garantissant ainsi la conservation des paramètres des programmes du système source. Voici la syntaxe d'utilisation de LoadState, sensiblement identique à celle de ScanState :
 - `loadstate [Chemindestockageréseau] [/i:[cheminverslesfichiersxml]]`

[Options]

- Pour charger la configuration préalablement sauvegardée, on utilisera la commande suivante :

```
loadstate \\server\share\mondossiermigration /i:MigApp.xml
```

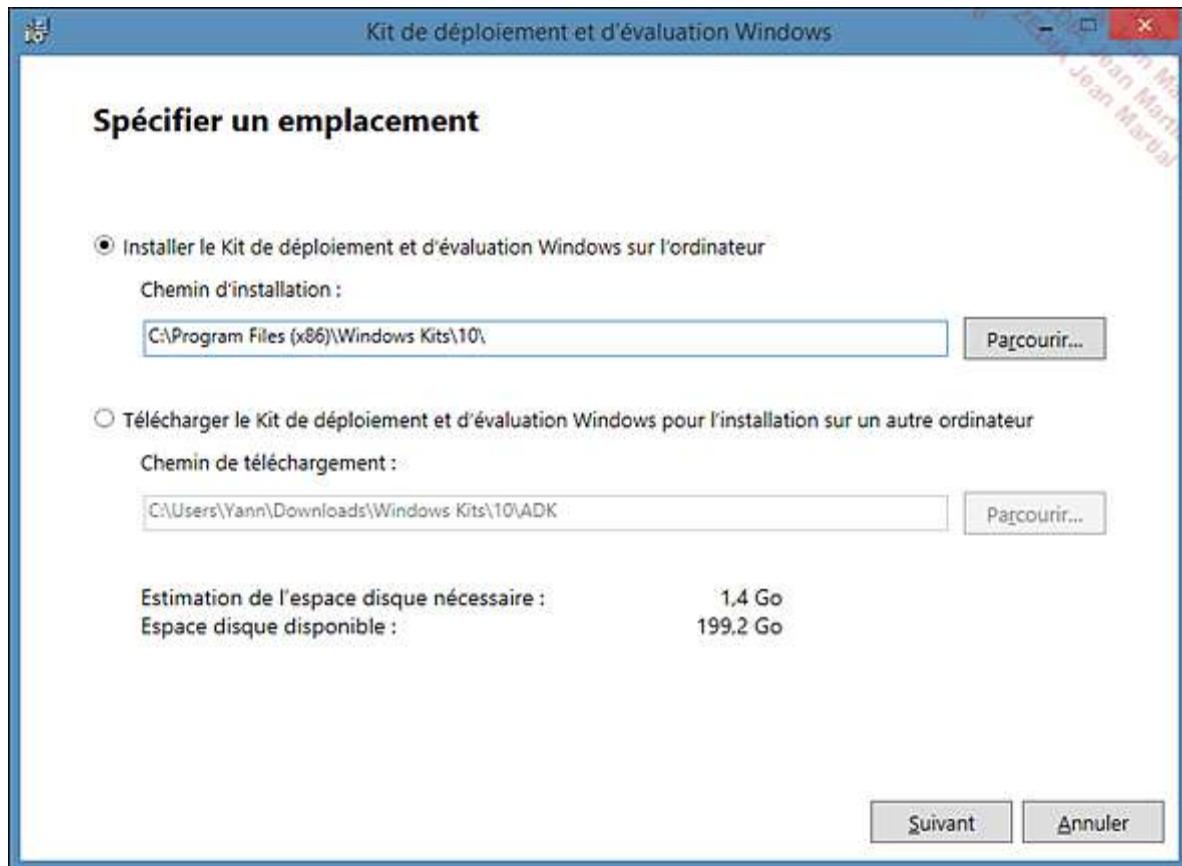
```
/i:MigDocs.xml /o /config:config.xml /v:13
```

Les commandes scanstate et loadstate nécessitent d'être exécutées en tant qu'administrateur depuis les ordinateurs source et destination afin de migrer l'ensemble des comptes. Dans le cas contraire, seul l'utilisateur courant sera migré.

Par exemple, pour sauvegarder les paramètres des utilisateurs depuis un ordinateur source Windows 8.1 vers un poste de travail Windows 11, voici la procédure.

La première étape est l'installation de l'outil USMT depuis le kit Windows ADK sur le poste de travail.

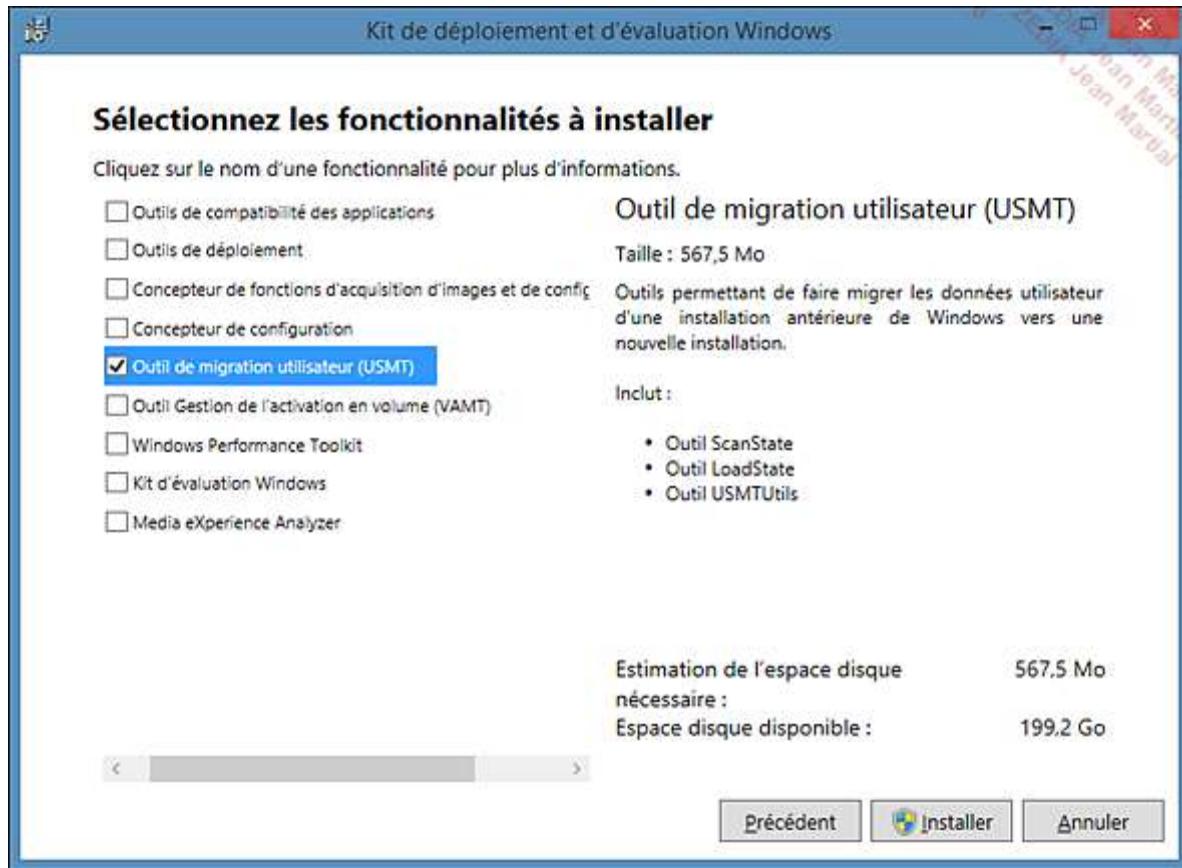
Ouvrez une session sur l'ordinateur Windows 8.1 en tant qu'administrateur. Exécutez un navigateur internet et rendez-vous à l'adresse <https://docs.microsoft.com/fr-fr/windowshardware/get-started/adk-install>. Dans la section Télécharger le kit ADK pour Windows 11 cliquez sur Télécharger Windows ADK. Une fois le fichier ADKsetup.exe récupéré, exécutez-le. Définissez ensuite un dossier d'installation.



Cliquez sur le bouton **Suivant** et une nouvelle fois sur **Suivant**. Validez le contrat de licence en cliquant sur **Accepter**.

La fenêtre **Sélectionnez les fonctionnalités à installer** apparaît.

Cochez la case **Outil de migration utilisateur (USMT)**, décochez les autres cases.



Cliquez sur le bouton **Installer**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

Maintenant que le kit ADK est installé, nous allons sauvegarder les données des utilisateurs du poste Windows 8.1 :

Cliquez avec le bouton droit sur le menu **Démarrer** situé en bas à gauche de la barre des tâches du bureau, puis sélectionnez **Windows PowerShell (admin)**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

Positionnez-vous sur le répertoire USMT qui correspond à l'architecture de votre ordinateur source (32 ou 64 bits). Par défaut sur un système 64 bits : C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\User State Migration Tool\amd64 ; sur un système 32 bits : C:\Program Files\Windows Kits\10\Assessment and Deployment Kit\User State Migration Tool\x86.

Saisissez .\scanstate c:\sauvegarde /c et validez par [Entrée].

Notez l'utilisation de .\ lors de l'exécution de cette commande dans une fenêtre Windows PowerShell. Dans une invite de commandes, seule la saisie de la commande scanstate aurait été nécessaire.

Le fichier généré se nomme par défaut USMT.MIG dans le dossier USMT.

Les données des comptes présents sur le poste Windows 8.1 sont sauvegardées dans le dossier C:\sauvegarde. Copiez celui-ci dans le même dossier sur le poste de travail cible Windows 11.

Pour appliquer les données et paramètres capturés au nouvel ordinateur Windows 11, voici la procédure (notez qu'au préalable, le kit Windows ADK doit être installé sur le poste Windows 11) :

Dans une invite de commandes exécutée en tant qu'administrateur, positionnez-vous dans le répertoire USMT correspondant à l'architecture de votre ordinateur de destination (64 bits). Par défaut : C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\User State Migration Tool\amd64.

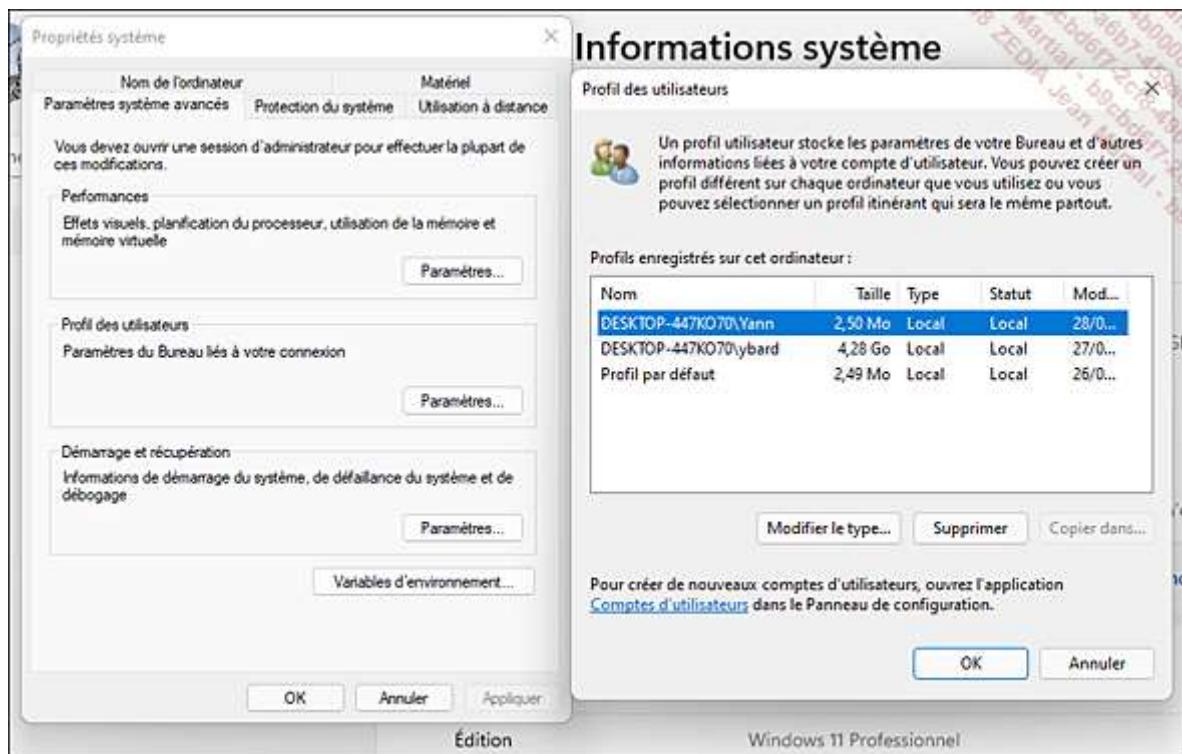
Assurez-vous que le fichier USMT.MIG préalablement généré est disponible dans le dossier C:\sauvegarde.

Saisissez la commande loadstate c:\sauvegarde puis validez par [Entrée].

Il sera peut-être nécessaire de rajouter le commutateur /lac pour autoriser la création de comptes locaux.

Les profils des utilisateurs sont désormais transférés. Pour vérifier l'application des paramètres utilisateur sur l'ordinateur de destination Windows 11, procédez comme suit :

Depuis le champ de recherche situé dans la barre des tâches, saisissez **Système**. Le panneau des paramètres s'ouvre alors. Cliquez sur **Système** et sur **Paramètres avancés du système**. Ensuite, dans la section **Profil des utilisateurs**, cliquez sur le bouton **Paramètres**. La liste des profils actuels et migrés s'affiche.



Fermez les fenêtres en cliquant sur le bouton **OK**.

Les versions 7, 8, 10 et 11 de Windows sont compatibles avec USMT version 10.0. Par contre, la migration depuis une version serveur de Windows, telle que Windows Server 2019 ou depuis Windows NT, n'est plus supportée.

Le transfert des données d'un système d'exploitation 32 bits vers un système 64 bits est possible, mais l'inverse n'est pas vrai.

Authentification

L'authentification est l'étape qui permet de vérifier l'identité d'une entité (personne, ordinateur, etc.) afin de lui donner accès à des ressources (fichiers, applications, etc.).

La phase de vérification fait intervenir un protocole d'authentification, comme Kerberos.

Il existe trois types d'authentification gérés par Windows 11 :

- L'authentification simple : un seul élément (exemple : mot de passe) est pris en compte lors du processus.
- L'authentification forte : repose sur au moins deux facteurs parmi ceux-ci :
 - Ce que l'utilisateur sait (mot de passe, code PIN, etc.).
 - Ce qu'il possède (carte à puce, smartphone, mémoire flash USB, etc.).
 - Ce qu'il est (empreinte, visage, etc.).
 - Ce qu'il sait faire (mouvement).
- L'authentification SSO (*Single Sign-On*) : une seule authentification est nécessaire pour accéder à plusieurs logiciels, grâce aux composants AD FS (*Active Directory Federation Services*) ou l'authentification directe Azure Active Directory.

Windows 11 Professionnel propose donc l'authentification basée non seulement sur le savoir, mais également sur le savoir-faire : par exemple, il est possible de demander à l'utilisateur d'effectuer une série de gestes sur une image sélectionnée pour ouvrir une session.

1. Mot de passe image

Le mot de passe image nécessite idéalement un écran tactile afin de créer une combinaison de cercles, points et lignes droites.

Cette fonctionnalité est optionnelle et devient une alternative pratique, mais non dénuée de failles de sécurité, dont :

- sensibilité à l'enregistrement vidéo (ou visuel) des gestes de l'utilisateur,
- observation des traces de doigt sur l'écran, aisément contournable en le nettoyant régulièrement.

Un mot de passe composé de trois mouvements est facilement mémorisable et rapide à exécuter.

Si l'utilisateur se trompe cinq fois de mouvement lors de l'authentification, la fonctionnalité est désactivée jusqu'à ce qu'il entre son mot de passe principal. De plus, lors d'un accès réseau à l'aide du compte utilisateur supportant le mot de passe image, cette méthode n'est pas disponible.

Utiliser un mot de passe image pour l'utilisateur courant s'effectue en suivant la procédure ci-dessous :

Cliquez sur le menu **Démarrer**, puis sur **Paramètres** et sur **Comptes**.

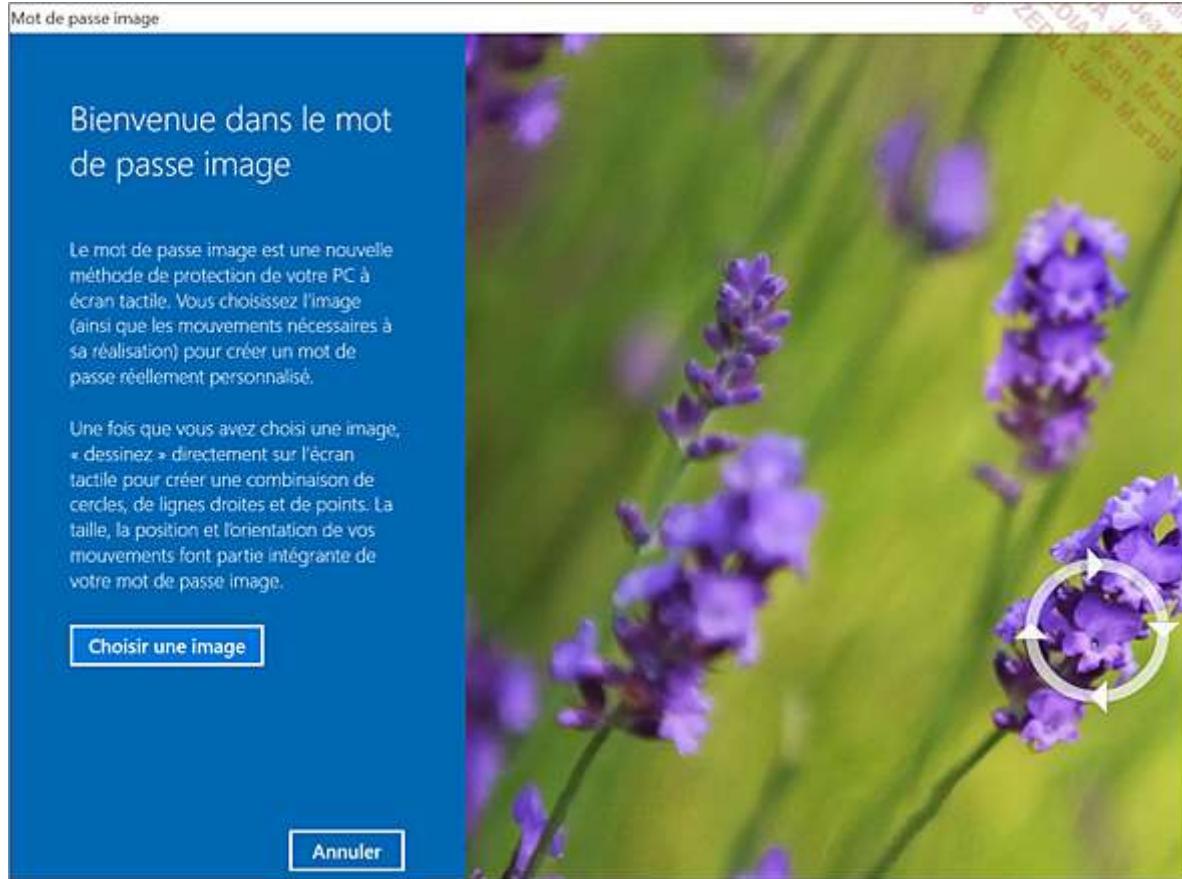
Dans la section **Options de connexion**, cliquez sur le bouton **Ajouter** du champ **Mot de passe image**.

The screenshot shows the Windows Settings interface under 'Comptes > Options de connexion'. On the left, a sidebar lists various settings categories like Système, Réseau et Internet, Personnalisation, Applications, Comptes (which is selected and highlighted in grey), Heure et langue, Jeux, Accessibilité, Confidentialité et sécurité, and Windows Update. A search bar at the top says 'Rechercher un paramètre'. The main pane displays two connection methods: 'Mot de passe' (Password) and 'Mot de passe image' (Password image). The 'Mot de passe image' section includes a note about using a favorite photo to unlock the device. Below these options is a button labeled 'Ajouter' (Add). Underneath the options, there's a section titled 'Paramètres supplémentaires' (Additional settings) with three items: 'Pour plus de sécurité, autorisez uniquement la connexion à Windows Hello pour les comptes Microsoft sur cet appareil (recommandé)' (For security, allow only Windows Hello connections for Microsoft accounts on this device (recommended)), which has an 'Activé' (Enabled) toggle switch; 'Verrouillage dynamique' (Dynamic lock), which has a note about automatically locking the device when you're away, and an 'Enregistrer automatiquement mes applications redémarrables et les redémarrer lorsque je me reconnecte' (Automatically save my restartable apps and restart them when I reconnect) setting, which has a 'Désactivé' (Disabled) toggle switch.

Avant d'activer la fonctionnalité, le système vous demande de confirmer votre mot de passe actuel puis de valider par **OK**.

- Si le compte visé ne possède pas de mot de passe, vous devrez en créer un.

Cliquez sur le bouton **Choisir une image** puis sélectionnez l'image que vous utiliserez pour vous authentifier et validez par **Ouvrir**.



Cliquez sur **Utiliser cette image** puis créez des mouvements (cercles, lignes ou points) sur celle-ci, renouvez l'opération une seconde fois. Cliquez sur le bouton **Terminer**.

L'authentification par mot de passe image fonctionne aussi sans écran tactile, à l'aide d'une souris, en cliquant avec le bouton gauche pour créer des points et en maintenant la touche pressée pour créer un cercle ou une ligne.

Lors de l'ouverture de session, vous aurez désormais le choix entre taper un mot de passe ou effectuer une série de gestes sur l'image sélectionnée :



- Grâce à un objet de stratégie de groupe, l'administrateur peut interdire l'utilisation de cette fonctionnalité. C'est le paramètre **Désactiver la connexion par mot de passe image** du nœud **Configuration ordinateur\Stratégies\Modèles d'administration\Système\Ouverture de session**.

2. Windows Hello

La biométrie est une technologie de plus en plus courante qui permet d'accéder facilement à des systèmes, des services et des ressources. Elle consiste à mesurer une caractéristique physique inaltérable d'une personne pour identifier celle-ci de façon unique. Les empreintes digitales font partie des caractéristiques biométriques les plus utilisées, notamment avec les millions de lecteurs d'empreintes digitales intégrés aux ordinateurs personnels et aux périphériques.

Malheureusement, cette fonctionnalité nécessite un matériel bien précis : une caméra infrarouge active spécifique pour la reconnaissance faciale ou de l'iris, et un lecteur d'empreintes digitales compatible avec Windows Biometric Framework.

Windows Hello vous permet ainsi de vous connecter à vos appareils Windows 11 de façon plus sécurisée, en utilisant la biométrie.

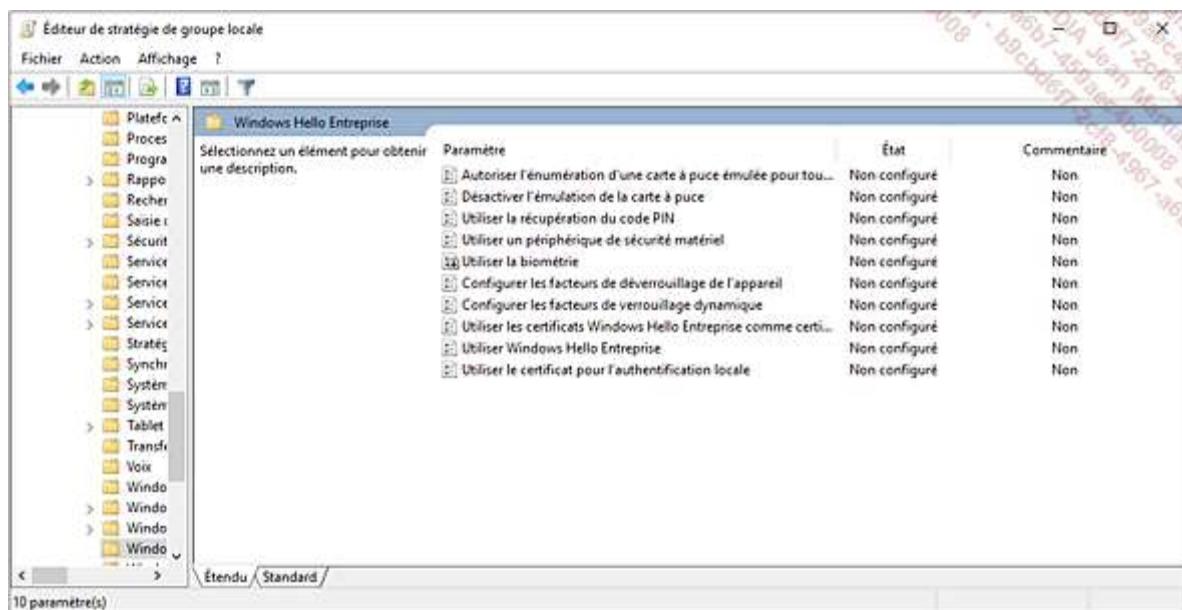
La fonctionnalité est disponible lors d'une authentification via un compte Microsoft Active Directory ou Microsoft Azure Active Directory (Azure AD). En outre, des services de fournisseur d'identité tiers qui prennent en charge l'authentification FIDO (*Fast ID Online*) v2.0 peuvent être utilisés.

Depuis Windows 10 version Creators Update, Microsoft a introduit Windows Hello Entreprise, qui permet d'authentifier un utilisateur via une paire de clés asymétriques ou un certificat. Ces clés peuvent être générées à l'aide d'une puce TPM ou via un logiciel spécialement conçu. L'authentification forte à 2 facteurs utilise donc une clé ou un certificat lié à un appareil ainsi qu'un élément détenu par l'utilisateur (code PIN) ou propre à ce dernier (Windows Hello).

L'activation de la fonctionnalité s'effectue via un objet de stratégie de groupe depuis le nœud Windows Hello Entreprise. Pour y accéder depuis l'éditeur de stratégie de groupe (gpedit.msc) suivez ces étapes :

Ouvrez l'arborescence **Configuration utilisateur** ou **Configuration ordinateur - Modèles d'administration - Composants Windows**.

Double cliquez sur le paramètre **Utiliser Windows Hello Entreprise** et cliquez sur la case d'option **Activé**.



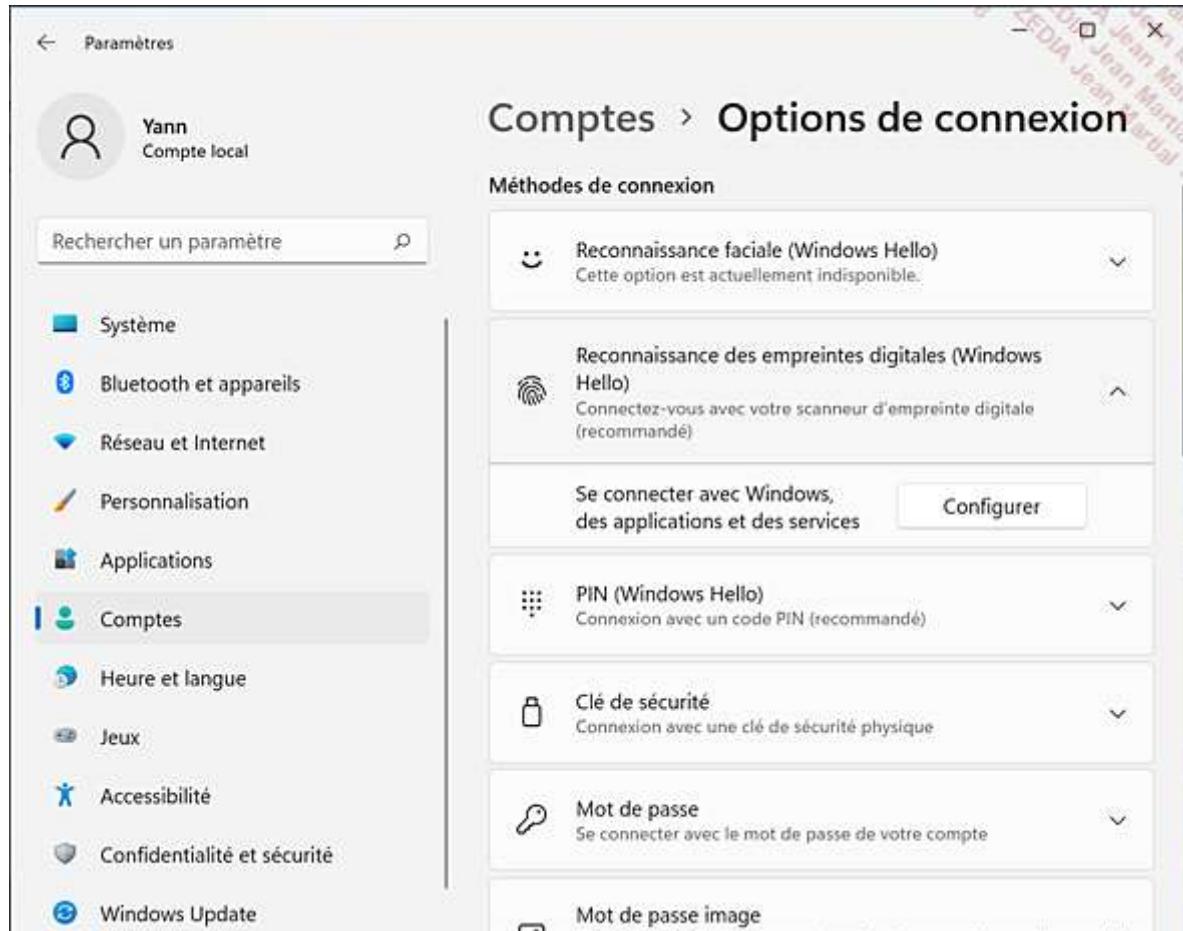
a. Empreintes digitales

Windows 11 intègre les pilotes et applicatifs nécessaires à la gestion des empreintes digitales, afin d'offrir à l'utilisateur un moyen simple, rapide et sécurisé de s'authentifier localement ou via l'intermédiaire d'un domaine Active Directory.

Pour configurer cette fonctionnalité, assurez-vous au préalable qu'un lecteur d'empreinte est connecté à votre ordinateur :

Cliquez sur le menu **Démarrer**, puis sur **Paramètres** et sur **Comptes**.

Dans la section **Options de connexion**, déroulez la section **Reconnaissance des empreintes digitales (Windows Hello)**, puis cliquez sur le bouton **Configurer**.



Cliquez sur le bouton **Démarrer** dans la fenêtre de configuration de Windows Hello. Confirmez votre identité en saisissant votre mot de passe, puis commencez la lecture de l'empreinte en touchant le lecteur.



Renouvez cette action jusqu'à ce que l'empreinte soit complète. Il vous faudra également modifier l'angle de touche.

Une fois l'enregistrement de l'empreinte complété, vous avez la possibilité d'en ajouter une autre ou bien de terminer la configuration en cliquant sur le bouton **Fermer**.

Lors de l'achat d'une App sur le magasin Microsoft Store, l'utilisateur peut désormais authentifier son compte grâce à ses empreintes.

- Grâce à un objet de stratégie de groupe, l'administrateur peut interdire l'utilisation de cette fonctionnalité, via le paramètre **Autoriser l'utilisation de la biométrie** du nœud **Configuration ordinateur - Stratégies - Modèles d'administration - Composants Windows - Biométrie**.

b. Reconnaissance du visage ou de l'iris

Windows Hello permet également de se connecter aux appareils Windows 11 de façon plus sécurisée, en utilisant le procédé de reconnaissance d'iris ou du visage du propriétaire de l'ordinateur. Ainsi, l'utilisation d'un mot de passe, bien souvent peu sécurisé, n'est plus un prérequis à l'authentification.

L'iris est la partie colorée visible de l'œil qui contient des informations uniques permettant de reconnaître son propriétaire.

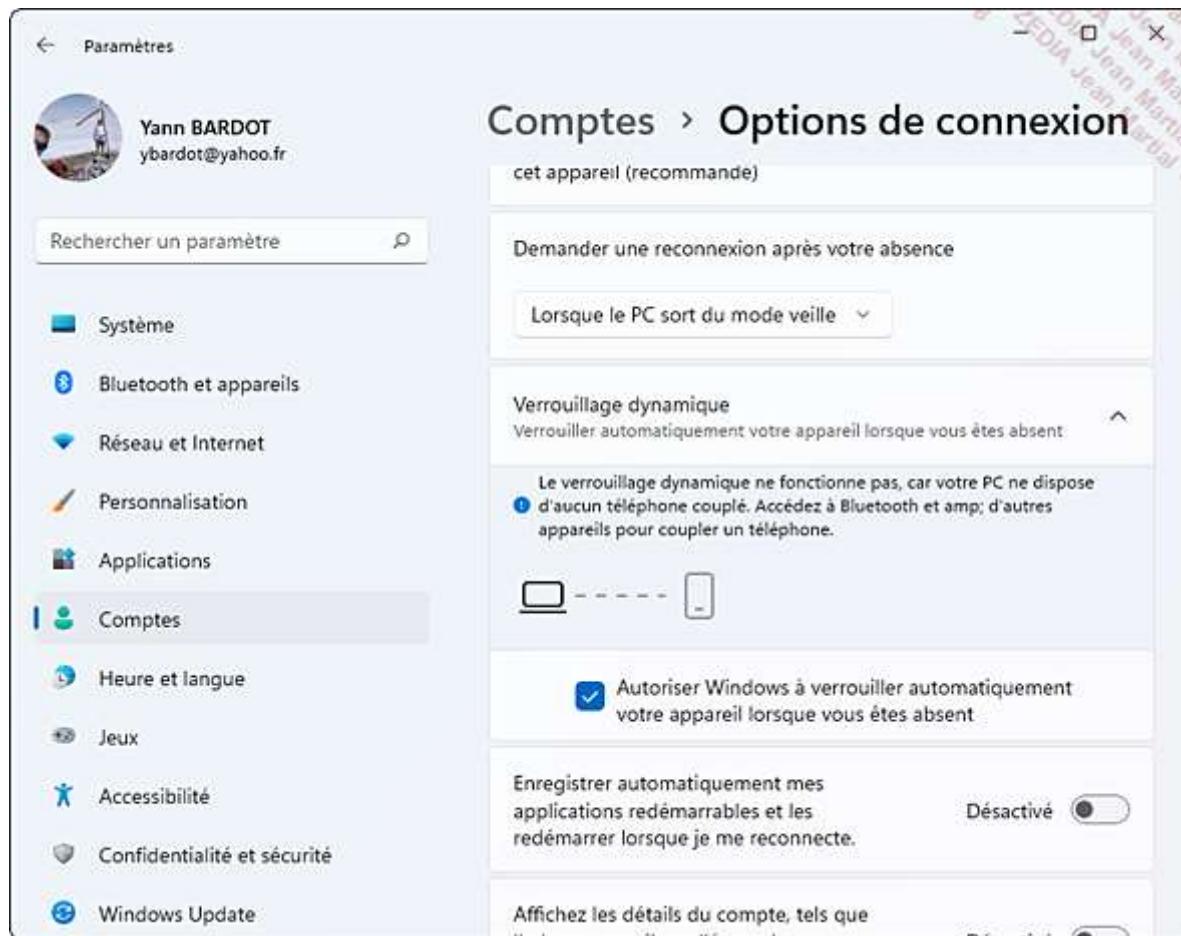
Pour configurer celle-ci, suivez la procédure ci-dessous (assurez-vous au préalable que le matériel compatible mentionné plus haut est connecté à votre ordinateur) :

Cliquez sur le menu **Démarrer**, puis sur **Paramètres, Comptes et Options de connexion**. Choisissez l'option correspondant à la reconnaissance du visage ou à celle de l'iris.

3. Verrouillage dynamique

Windows 11 peut verrouiller automatiquement l'ordinateur quand un appareil, tel qu'un smartphone, n'est plus à portée via le réseau Bluetooth. Ce procédé nécessite l'activation du Bluetooth sur le système et le couplage d'un appareil.

Cliquez sur le menu **Démarrer**, puis sur **Paramètres**, **Comptes**, **Options de connexion**. Déroulez la section **Verrouillage dynamique**, et cochez la case **Autoriser Windows à verrouiller automatiquement votre appareil lorsque vous êtes absent**.



4. Accès attribué

La fonctionnalité Accès attribué (encore appelée Accès affecté ou mode kiosque) permet de limiter des utilisateurs spécifiques à n'utiliser qu'une seule application du Microsoft Store, et ceci en plein écran. Comparable à une borne d'arcade, un enfant ne peut jouer qu'à un seul jeu éducatif sur sa tablette. Une entreprise peut aussi fournir un accès à son application sous forme de borne cloisonnée.

Cette technologie nécessite l'utilisation d'un compte Microsoft ayant ouvert au moins une fois une session sur le poste de travail Windows 11.

Pour configurer ce type d'accès, voici la procédure :

Cliquez sur le menu **Démarrer**, **Paramètres** puis **Comptes**.



Dans la section **Configurer un mode plein écran**, cliquez sur le bouton **Prise en main** pour créer un compte local, seulement autorisé à exécuter une application.

Choisissez le nom du compte pour en créer un nouveau, ou sélectionnez un compte existant et cliquez sur **Suivant**.

Puis choisissez l'application cible (dans notre exemple **Alarmes et horloge**) parmi les applications du Windows Store, via la liste affichée et cliquez sur **Suivant** :



L'utilisateur défini ne pourra désormais exécuter que l'application sélectionnée en plein écran lors de l'ouverture de sa session.

Vous pouvez faire l'essai en vous connectant avec ce compte. La fermeture de session s'effectue en pressant [Ctrl]+[Alt]+[Suppr].

5. Code PIN

À l'aide d'un code d'au minimum quatre chiffres, l'utilisateur peut ouvrir une session rapidement. Il n'est malheureusement pas possible avec cette méthode de combiner les facteurs d'authentification (mot de passe ou mot de passe image) afin d'améliorer la sécurité du poste de travail.

Le clavier numérique étant facilement accessible depuis une tablette ou un clavier, cette méthode d'ouverture de session est simple d'usage mais pas exempte de faiblesses importantes :

- Faiblesse du nombre de combinaisons : code confidentiel dont les valeurs sont comprises entre 0000 et 9999, soit 10 000 combinaisons possibles.
- Code confidentiel trivial : l'utilisateur a tendance à employer un code facilement mémorisable comme sa date de naissance, qui peut donc être rapidement deviné.
- Trainée du code confidentiel : l'usure des touches du clavier peut donner une indication sur les quatre chiffres utilisés, ce qui limite le nombre de combinaisons possibles à 24.

Le code confidentiel peut également inclure des lettres et des symboles, le rendant ainsi proche du mot de passe. Il doit comporter au moins 4 caractères (jusqu'à 124) et ne pas correspondre à un modèle de numéro (123456, par exemple).

Créer un code confidentiel comme méthode d'authentification s'effectue simplement :

Cliquez sur le menu **Démarrer**, puis sur **Paramètres**, **Comptes** et **Options de connexion**.

Déroulez la section **PIN (Windows Hello)** et cliquez sur le bouton **Configurer**.

Paramètres

Comptes > Options de connexion

Méthodes de connexion

- Reconnaissance faciale (Windows Hello)
Cette option est actuellement indisponible.
- Reconnaissance des empreintes digitales (Windows Hello)
Connectez-vous avec votre scanner d'empreinte digitale (recommandé)
- PIN (Windows Hello)
Connexion avec un code PIN (recommandé)
- Utiliser un code PIN pour vous connecter à Windows, aux applications et aux services
Configurer
- Liens connexes
- Clé de sécurité
Connexion avec une clé de sécurité physique
- Mot de passe
Se connecter avec le mot de passe de votre compte

Rechercher un paramètre

- Système
- Bluetooth et appareils
- Réseau et Internet
- Personnalisation
- Applications
- Comptes
- Heure et langue
- Jeux
- Accessibilité
- Confidentialité et sécurité
- Windows Update

Confirmez votre identité en saisissant votre mot de passe, puis saisissez un code confidentiel et confirmez-le. Celui-ci doit contenir au minimum quatre caractères. Si vous le souhaitez, vous pouvez le complexifier en incluant des lettres et des symboles. Pour ce faire, cochez la case **Inclure des lettres et des symboles**. Validez la saisie en cliquant sur le bouton **OK**.

Sécurité Windows

Configurer un code confidentiel

Un code PIN Windows Hello est un moyen rapide et sécurisé de vous connecter à votre appareil, à vos applications et à vos services.

Nouveau code confidentiel

Confirmmer le code confidentiel

Inclure des lettres et des symboles

OK **Annuler**

- Plus le code PIN aura une longueur importante, plus l'authentification de l'utilisateur sera sécurisée.

Lors de la phase d'authentification, l'utilisateur peut entrer son code confidentiel, l'icône le symbolisant est un clavier numérique :



- Grâce à un objet de stratégie de groupe, l'administrateur peut interdire l'utilisation de cette fonctionnalité, via le paramètre **Activer la connexion par le code PIN d'usage** du nœud **Configuration ordinateur - Modèles d'administration - Système - Ouverture de session**.

6. Contrôle visuel

Le contrôle visuel permet d'utiliser la technologie de suivi oculaire pour contrôler le mouvement du pointeur de la souris, mais aussi pour saisir du texte grâce au clavier visuel, et enfin communiquer avec des personnes à l'aide de la conversion de texte par synthèse vocale (*speech to text*). Cette fonctionnalité est très utile aux personnes en situation de handicap.

Pour activer le contrôle visuel, depuis un poste de travail Windows 11 pourvu d'un système de suivi oculaire, cliquez sur le menu **Démarrer** puis **Paramètres, Accessibilité** et **Contrôle visuel**.

Cliquez sur l'option **Activer**. Un menu LaunchPad apparaîtra sur votre écran, proposant les fonctions suivantes :



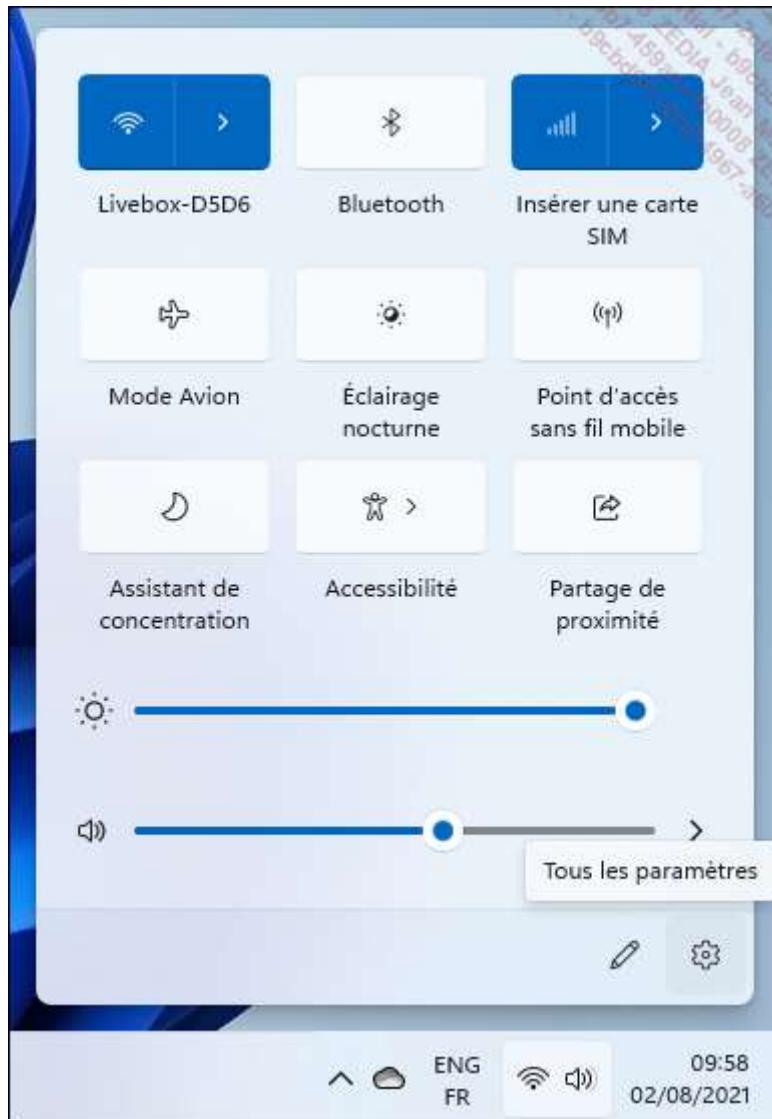
21 Image issue du site : <https://support.microsoft.com/fr-fr/windows/notions-de-base-sur-le-controle-visuel-dans-windows-10-97d68837-b993-8462-1f9d-3c957117b1cf>

7. Utilisateurs et groupes locaux

Tout comme les anciennes versions clientes des systèmes Microsoft, Windows 11 possède une base de données des comptes et groupes locaux, nommée SAM (*Security Account Manager*) située dans le dossier %systemroot%\System32\Config. Avec les outils adéquats, l'administrateur peut définir des autorisations et des droits à un compte d'utilisateur ou à un groupe local sur un ordinateur précis.

Pour gérer les utilisateurs et groupes locaux créés sur un poste de travail, plusieurs méthodes existent :

- Depuis la console **Gestion de l'ordinateur** accessible en pressant les touches  et X, développez le nœud **Utilisateurs et groupes locaux**. Cette console est également accessible en saisissant **compmgmt.msc** depuis la barre de recherche.
- Depuis les paramètres du PC accessibles de trois manières :
 - Cliquez sur le menu **Démarrer**, puis sur **Paramètres** et sur **Comptes**.
 - Cliquez sur l'icône **Paramètres rapides** depuis le coin droit de la barre des tâches, puis sur **Paramètres et Comptes**.

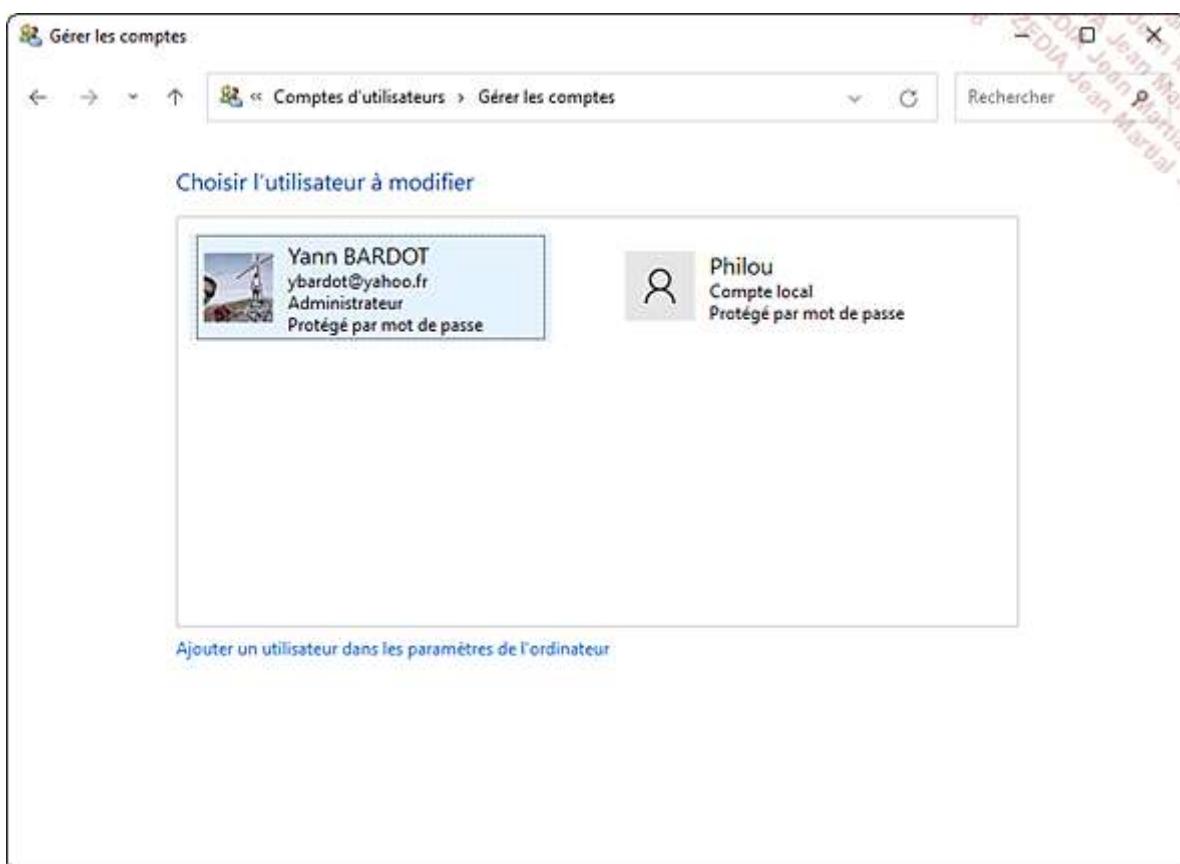


Ou bien pressez les touches  + i.

- L'ancienne méthode, depuis le panneau de configuration : saisissez **Panneau de configuration** depuis le champ de recherche de la barre des tâches.
- Dans le cadre des démonstrations proposées dans ce livre, l'auteur utilisera l'affichage par petites icônes, afin d'accéder plus rapidement à l'ensemble des fonctionnalités proposées par le panneau de configuration.



Cliquez ensuite sur **Comptes d'utilisateurs** dans la fenêtre **Tous les Panneaux de configuration**, puis **Gérer un autre compte**.



Trois comptes sont créés et désactivés par défaut. Ils ne sont visibles que depuis la fenêtre **Gestion de l'ordinateur** (première méthode), console plutôt réservée aux utilisateurs avertis :

- Administrateur : ce compte possède le contrôle total du système et peut définir des autorisations supplémentaires aux utilisateurs. Il est conseillé de le renommer. Lors de l'ouverture d'une session en mode sans échec, même désactivé, ce compte peut être utilisé. Il ne peut pas être supprimé.
- Invité : ce compte est souvent utilisé par des personnes ne possédant aucun compte sur l'ordinateur. Il a un rayon d'action limité.
- DefaultAccount : compte utilisateur géré par le système.

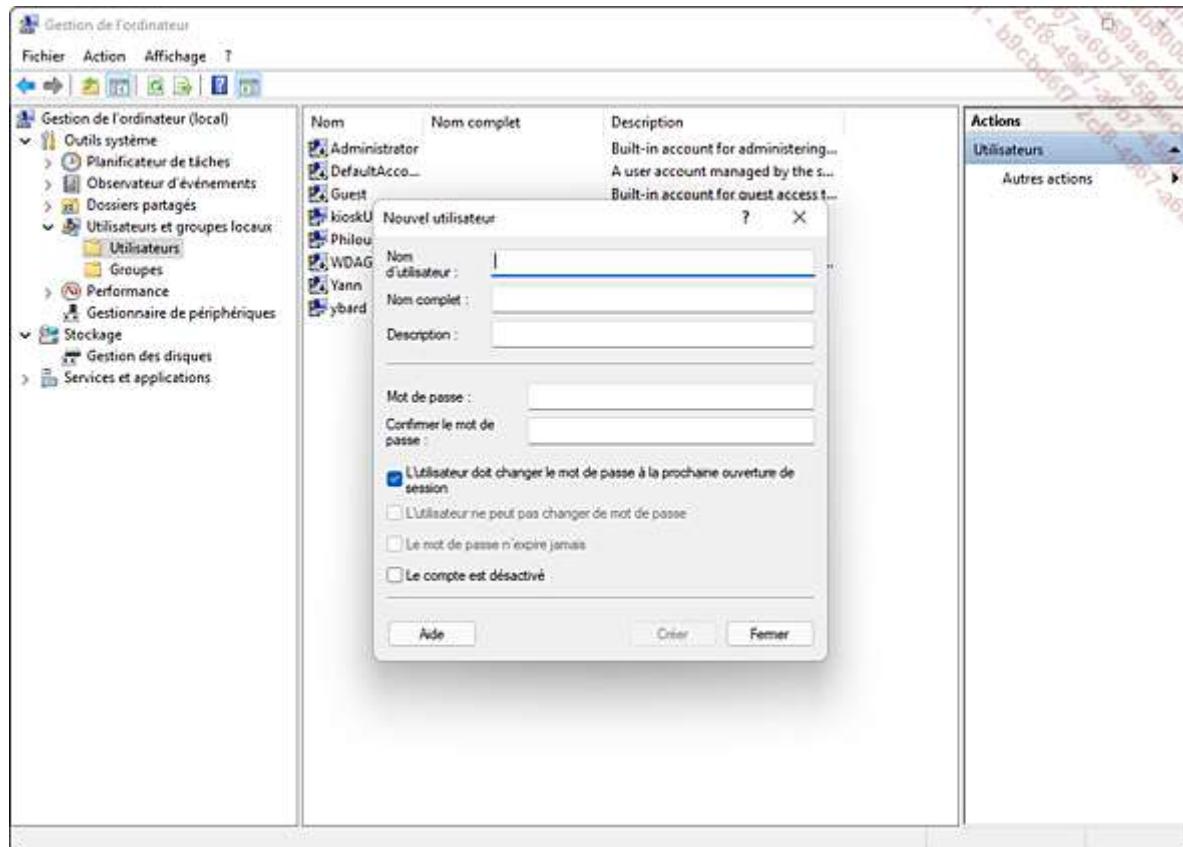
Les groupes suivants sont créés à l'installation de Windows 11 et permettent à ses membres d'effectuer des actions spécifiques :

- Administrateurs : contient les utilisateurs ayant des priviléges administrateur.
- Administrateurs Hyper-V : accès complet aux fonctions de virtualisation de Windows 11.
- Duplateurs : gestion de la réPLICATION des fichiers lorsque le poste est membre d'un domaine.

- IIS_IUSRS : est utilisé par le serveur web Microsoft IIS.
- Invités : contient les utilisateurs ayant des priviléges limités.
- Lecteurs des journaux d'événements : autorisation d'afficher en lecture les journaux des événements.
- Opérateurs d'assistance de contrôle d'accès : possibilité d'interroger à distance les attributs d'autorisation et les autorisations des ressources.
- Opérateurs de chiffrement : autorisation de chiffrer les données.
- Opérateurs de configuration réseau : gestion de la configuration TCP/IPv4 et TCIP/IPv6.
- Opérateurs de sauvegarde : permission de sauvegarder et restaurer des données sur l'ordinateur.
- System Managed Accounts Group : les membres de ce groupe sont gérés par le système.
- Utilisateurs : ce type de compte ne possède que des actions limitées, comme l'exécution de programmes ou l'impression depuis une imprimante locale.
- Utilisateurs avec pouvoir : octroie des droits d'administration limités.
- Utilisateurs de gestion à distance : accès aux ressources WMI via des protocoles de gestion.
- Utilisateurs de l'Analyseur de performances : autorisation de visualiser les compteurs.
- Utilisateurs du Bureau à distance : les membres ont la possibilité de se connecter à distance à l'ordinateur à l'aide du client Bureau à distance.
- Utilisateurs du journal de performances : permission de configurer les compteurs de performances et les journaux.
- Utilisateurs du modèle COM distribué : comptes autorisés à exécuter et gérer les objets DCOM.

La création de comptes utilisateurs locaux est possible en utilisant n'importe laquelle des trois méthodes précédemment évoquées. Notez que l'utilisation du panneau de configuration vous renverra sur le panneau **Paramètres**.

Depuis la console **Gestion de l'ordinateur**, développez **Utilisateurs et groupes locaux**, puis **Utilisateurs** : Cliquez avec le bouton droit sur **Utilisateurs** et choisissez **Nouvel utilisateur**.



Remplissez les champs **Nom d'utilisateur**, **Mot de passe**, **Confirmer le mot de passe**.

Au besoin, cochez les options permettant de forcer l'utilisateur à changer son mot de passe ou non, de définir un délai d'expiration et validez en cliquant sur le bouton **Créer**.

Le nouveau compte est créé et placé dans le groupe **Utilisateurs**.

Depuis l'écran **Paramètres, Comptes** :

Cliquez sur **Famille et autres utilisateurs**.

Dans la section **Autres utilisateurs**, cliquez sur **Ajouter un compte**. Par défaut, Microsoft propose de créer ou de connecter un compte Microsoft à la machine. Il est néanmoins possible de créer un compte purement local.

The screenshot shows the Windows Control Panel under 'Paramètres' (Settings). The left sidebar lists various categories: Système, Bluetooth et appareils, Réseau et Internet, Personnalisation, Applications, Comptes (selected), Heure et langue, Jeux, Accessibilité, Confidentialité et sécurité, and Windows Update. The main content area is titled 'Famille et autres utilisateurs'. It includes sections for 'Votre famille' (Your family), 'Autres utilisateurs' (Other users), and 'Configurer un mode plein écran' (Configure full screen mode). A sidebar on the right lists user accounts: Yann Bardot, Philou, and others.

Votre famille

Autoriser les membres de la famille à se connecter à ce PC : les organisateurs peuvent contribuer à la sécurité des membres en ligne grâce aux paramètres de sécurité [En savoir plus sur le Contrôle parental](#)

Ajouter un membre à la famille [Ajouter un compte](#)

Autres utilisateurs

Ajouter un autre utilisateur [Ajouter un compte](#)

Philou
Compte local

Configurer un mode plein écran

Plein écran
Transformer cet appareil en kiosque pour l'utiliser en tant que signature numérique, affichage interactif ou autre chose [Actif](#)

Dans la fenêtre **Compte Microsoft**, au lieu de saisir l'adresse électronique, cliquez sur le lien **Je ne dispose pas des informations de connexion de cette personne**.

Puis cliquez sur **Ajouter un utilisateur sans compte Microsoft**.

Saisissez le nom, le mot de passe et confirmez-le, choisissez et répondez aux trois questions de sécurité, puis cliquez sur le bouton **Suivant**.

Compte Microsoft

Créer un utilisateur pour ce PC

Si ce compte est destiné à un enfant ou à un adolescent, songez à sélectionner **Retour** puis à créer un compte Microsoft. Quand des membres jeunes d'une famille se connectent avec un compte Microsoft, leurs données personnelles bénéficient de protections adaptées à leur âge.

Si vous souhaitez utiliser un mot de passe, choisissez une expression facile à retenir, mais difficile à deviner.

Qui sera amené à utiliser ce PC ?

Sécurisez votre mot passe.

Au cas où vous auriez oublié votre mot de passe

Ce champ est obligatoire

Suivant **Précédent**

The screenshot shows the 'Create a user account for this PC' step of the Windows User Account Creation Wizard. It includes fields for the user's name ('Yann'), password ('*****'), and a security question ('Question de sécurité 1'). A note at the top right suggests creating a Microsoft account for children or teenagers. At the bottom are 'Next' and 'Previous' buttons.

Le nouveau compte local est créé et placé dans le groupe **Utilisateurs**.

Lorsqu'un utilisateur ouvre une session avec un compte possédant des droits limités, il peut utiliser la commande runas (exécuter en tant que) pour temporairement éléver son niveau de privilège administratif et ainsi accéder à une ressource précise. Des informations d'identification lui seront demandées.

Le paramètre /profile couplé à la commande runas permet de charger le profil de l'utilisateur spécifié. Pour ne pas le charger et ainsi exécuter l'application plus rapidement, utilisez le paramètre /noprofile.

Deux méthodes permettent d'exécuter une fonctionnalité avec des droits plus élevés, l'une depuis l'interface utilisateur et l'autre à l'aide de la commande précitée. Ci-après, un exemple d'utilisation de cette dernière.

Créez un compte d'utilisateur standard puis ouvrez une session avec celui-ci :

Cliquez sur le menu **Démarrer** avec le bouton droit de la souris puis sur **Windows PowerShell (admin)**. Cliquez sur le bouton **Oui** lorsque la fenêtre de contrôle de compte utilisateur apparaît.

La fenêtre **Windows PowerShell** s'exécute avec des privilèges élevés.

Saisissez la commande : runas /user:votreloginadministrateur explorer.exe
puis entrez le mot de passe lié au compte administrateur.

L'Explorateur Windows est désormais accessible en tant qu'administrateur.

Notez qu'à l'aide de la commande winrs.exe, l'administrateur peut exécuter une commande sur un ordinateur distant Windows 11. Celui-ci doit autoriser le protocole WS-Management en créant une exception dans le pare-feu, à l'aide de la commande winrm quickconfig.

Par exemple, pour exécuter la commande ipconfig sur un ordinateur distant : winrs -r:ORDINATEURDISTANT ipconfig

8. Compte Microsoft

Grâce à son compte Microsoft (messagerie Hotmail, par exemple), l'utilisateur va ouvrir une session et retrouver ses paramètres et applications, ainsi que ses documents, depuis n'importe quel ordinateur pourvu de Windows. Cette possibilité est offerte via un service cloud (dans le "nuage"), accessible à la demande et utilisant des serveurs virtualisés et mutualisés disponibles depuis le réseau internet.

- L'emplacement des données de l'utilisateur dans le "nuage" n'est pas connu de celui-ci.

L'authentification grâce à un compte Microsoft, synchronise les éléments suivants :

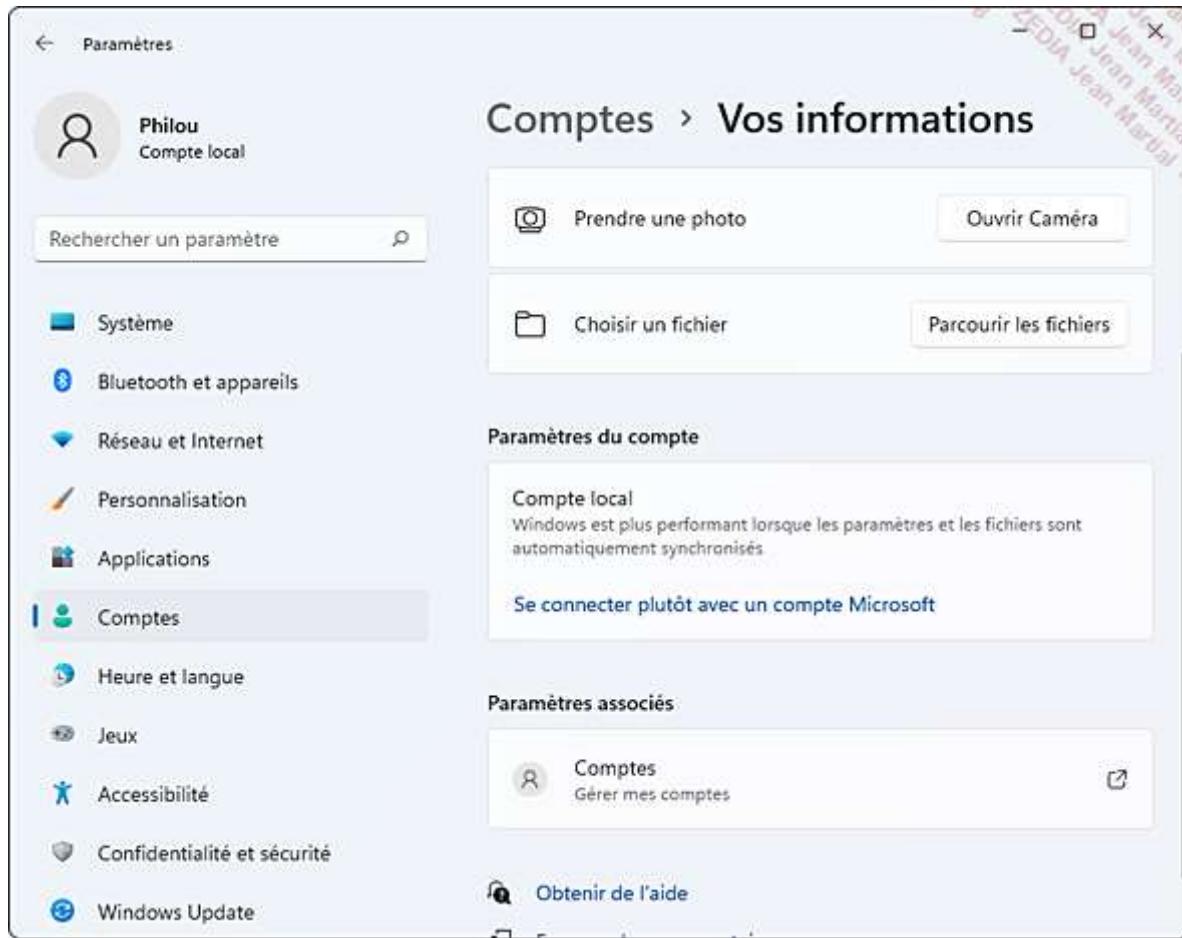
- Applications téléchargées depuis Microsoft Store.
- Favoris, thèmes, préférences linguistiques.
- Mise à jour de votre réseau social Facebook, Hotmail, Twitter, etc.
- Photos et autres fichiers stockés sur des services tels que OneDrive, Flickr, etc.

La création et la configuration du compte Microsoft peuvent être initiées lors de la phase d'installation de Windows 11 (cf. section Installation de ce chapitre), sous réserve d'une connexion active au réseau internet.

L'utilisateur peut néanmoins utiliser ce service après l'installation du système, en suivant la procédure suivante :

Cliquez sur le menu **Démarrer**, puis sur **Paramètres** et sur **Comptes**.

Cliquez sur **Vos informations**, et dans la section **Paramètres du compte**, cliquez sur le lien **Se connecter plutôt avec un compte Microsoft**.



L'utilisateur est invité à entrer son adresse de messagerie Microsoft, ou à en créer une. Une connexion au réseau internet est requise.

9. Contrôle parental

De plus en plus d'enfants utilisent un ordinateur pour jouer et apprendre, mais aussi discuter grâce aux réseaux sociaux. Les parents, soucieux d'assurer la protection de leur progéniture, cherchent souvent une solution pour contrôler l'activité internet de celle-ci. Il peut être intéressant d'apporter une réponse pédagogique aux problèmes de sécurité engendrés par Internet, et de placer l'ordinateur familial dans une pièce commune. Néanmoins, la vérification régulière des actions de l'enfant rassurera les parents. Windows 11 fournit la fonctionnalité **Contrôle parental**, qui s'appuie sur un compte Microsoft pour suivre l'activité de l'enfant, quelle que soit la machine utilisée pour ouvrir une session. Cette fonctionnalité est désormais intégrée à Windows Defender Antivirus.

Des rapports hebdomadaires sur son activité sont générés, puis envoyés par courriel à l'adresse des parents. Chaque modification de paramètres du contrôle parental est répercutée sur tous les postes, grâce au cloud et au site <http://familysafety.microsoft.com>.

L'enfant doit posséder un compte standard et non administrateur, afin d'éviter qu'il puisse lui-même modifier les paramètres de la fonctionnalité ou installer un logiciel malveillant.

De plus, des heures d'utilisation de l'ordinateur peuvent être définies, en fonction du jour de la semaine.

Pour configurer les paramètres de la fonctionnalité, procédez comme suit :

Ouvrez **Paramètres**, cliquez sur **Confidentialité et sécurité**, puis **Options de contrôle parental**. Cela permet d'accéder au panneau **Sécurité Windows** (anciennement **Windows Defender**).

Dans la section **Contrôle parental**, cliquez sur le lien **Afficher les paramètres du contrôle parental**. Une page internet s'ouvre automatiquement invitant le parent à s'authentifier via son compte Microsoft depuis le lien **Déjà configuré ? Se connecter maintenant**.



Cliquez ensuite sur le bouton **Créer un groupe familial**. Ajoutez l'adresse électronique de l'enfant, puis cliquez sur **Suivant**.

Cliquez sur le bouton **Membre**, puis sur **Suivant**.

Saisissez les caractères affichés à l'écran pour confirmer que vous n'êtes pas un robot, puis cliquez sur le bouton **Inviter**. Le membre de la famille est alors en attente de rattachement. Il recevra un e-mail et devra accepter l'invitation.

Une fois que l'enfant aura validé son rattachement au contrôle parental, le parent pourra définir les critères de restriction de sa vie numérique, tels que fixer les limites de durée d'utilisation, bloquer le contenu inapproprié ou encore éviter les commandes inopinées grâce à l'envoi d'un e-mail lors d'un achat sur le Microsoft Store.

Gestion des licences

Une gestion adéquate des logiciels Microsoft installés dans le réseau d'une entreprise permet de rationaliser les coûts des licences et d'améliorer la sécurité du système d'information.

Une licence vous donne le droit d'utiliser un logiciel en tant qu'utilisateur final, en ayant accès aux dernières mises à jour.

Pour ce faire, il est nécessaire de dresser la liste des logiciels installés sur les ordinateurs clients et serveurs. Vous pouvez l'effectuer manuellement ou en utilisant un logiciel tel que MECM (*Microsoft Endpoint Configuration Manager*).

Une fois l'inventaire dressé, il suffit de le comparer avec le listing des licences acquises. En général, le responsable informatique se rend compte qu'il possède peu de licences pour tel logiciel, rarement l'inverse.

Il existe trois types de licences Microsoft :

- OEM (*Original Equipment Manufacturer*) : un particulier achetant un ordinateur équipé de Windows 11 dans un magasin utilise généralement une licence OEM, non réutilisable en cas de changement d'ordinateur.
- Vente au détail : correspond à l'achat d'un système Windows en magasin donnant droit à une licence individuelle (version boîte). Cette dernière est souvent plus chère qu'une licence OEM.
- Licence en volume : une unique clé permet d'activer un nombre défini de clients.

Chaque licence dispose d'un canal d'obtention spécifique. Par exemple, l'édition Windows 11 Entreprise n'est disponible qu'à travers une licence en volume.

Microsoft propose d'utiliser le programme Volume Activation, solution permettant d'automatiser le processus d'activation des produits.

L'activation est un processus visant à authentifier l'achat d'un logiciel Microsoft, qu'il soit une suite bureautique telle qu'Office, ou bien un système d'exploitation comme Windows 11.

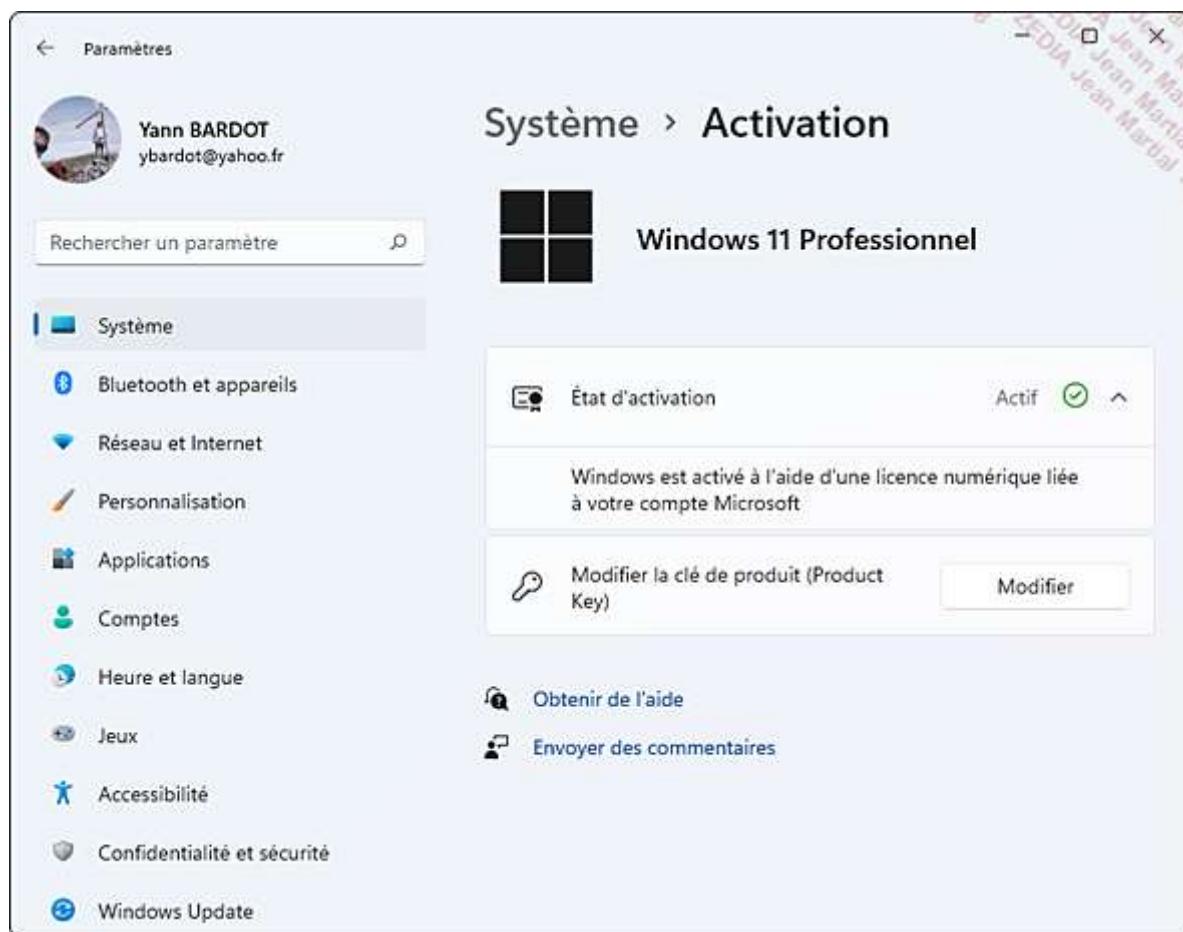
Un des buts du processus d'activation est d'endiguer la propagation de copies illégales de logiciel, entraînant une perte de revenus pour Microsoft. Le piratage d'une licence entraîne une infraction aux règles mentionnées dans le CLUF (Contrat de Licence d'Utilisateur Final) du logiciel.

En ce qui concerne l'utilisateur final, l'activation lui garantit l'authenticité de son achat et lui permet ainsi de bénéficier des mises à jour et du support du produit acheté.

Pour activer manuellement Windows 11, suivez ces étapes :

Cliquez sur le menu **Démarrer, Paramètres et Système**.

Dans le menu de droite, cliquez sur **Activation** puis sur le bouton **Activer**. L'utilisateur peut aussi entrer une nouvelle clé de produit en cliquant sur le bouton **Modifier** de la section **Modifier la clé de produit** ou bien activer sa version de Windows 11 par téléphone.



Notez qu'il ne faut pas nécessairement posséder un compte administrateur pour activer une copie de Windows 11.

Les administrateurs peuvent utiliser trois modes pour activer leurs systèmes Microsoft dans leur environnement d'entreprise :

- Basé sur Active Directory.
- KMS (*Key Management Service*), paramètre défini par défaut sur les clients.
- MAK (*Multiple Activation Key*), paramètre d'activation via un serveur d'activation Microsoft.

La planification de l'activation en volume dans une entreprise doit faire partie intégrante du processus de déploiement de Windows 11.

Les clés de licences en volume ne peuvent pas être utilisées avec des produits achetés en grande distribution ou encore avec un système préinstallé sur une machine (OEM). Elles sont prévues pour des systèmes comme par exemple Windows 11 Entreprise ou Windows Server 2019.

Désormais, la gestion des licences est centralisée grâce au rôle **Services d'activation en volume** d'un ordinateur pourvu de Windows Server 2019 (ou versions antérieures selon les versions des systèmes à activer).

1. Activation basée sur Active Directory

Un administrateur peut gérer les activations des systèmes dont il a la charge grâce à un domaine Active Directory dont le niveau fonctionnel du schéma est défini au moins à Windows Server 2012.

Seul un ordinateur Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 et Windows Server 2019 joint à un domaine peut être activé par cette méthode d'activation basée sur Active Directory. Les anciennes versions de Windows ne sont pas supportées par ce mode.

Lorsque le système client démarre, il tente de s'inscrire auprès d'un contrôleur de domaine, et ce de manière transparente pour l'utilisateur final. Cette activation dispose d'une durée de validité de 180 jours.

Si les informations nécessaires à l'activation du poste membre du domaine ne sont pas trouvées dans les services AD DS (*Active Directory Domain Services*), le client recherchera dans ce cas un serveur KMS référent via le service DNS.

Contrairement au service KMS, aucun port réseau n'est à ouvrir et aucune entrée DNS n'est à créer avec la méthode d'activation basée sur Active Directory.

2. Service de gestion des clés (KMS)

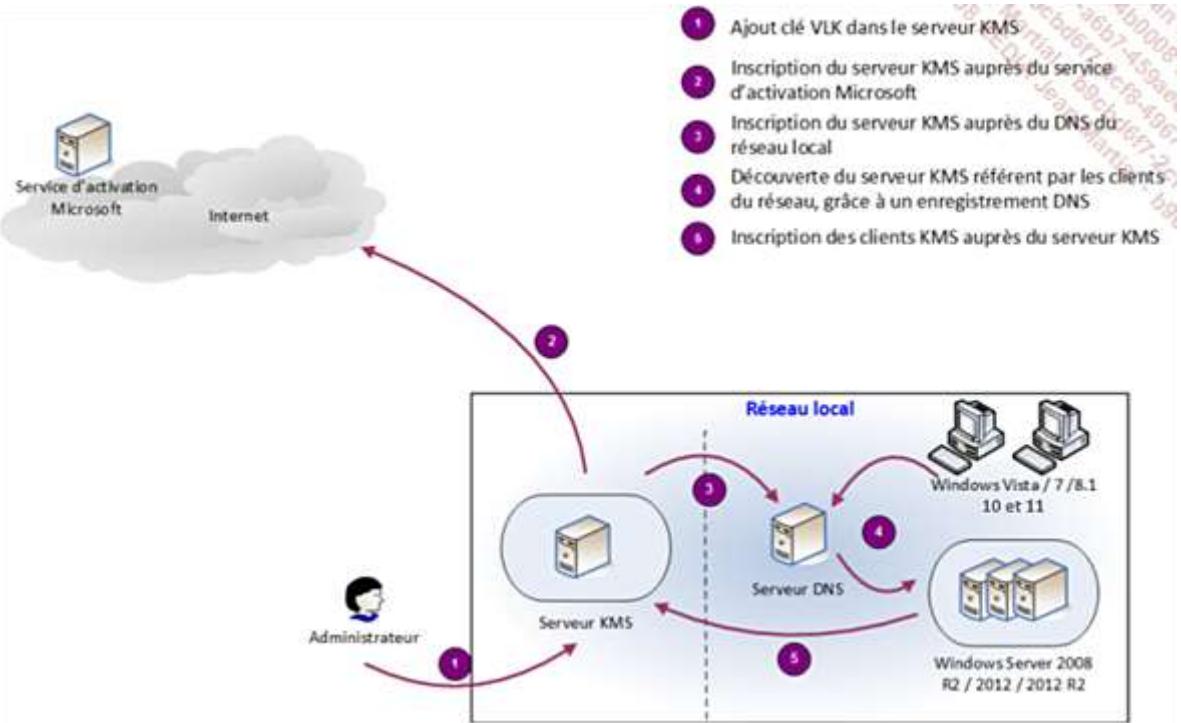
Le service de gestion des clés ou KMS (*Key Management Service*) permet de répondre aux demandes d'activation des clients Microsoft, tels que Windows 7, Windows 8.1, Windows 11, ou encore Windows Server. Aucune clé de licence n'est à entrer sur les clients, et aucune activation n'est confirmée sur le site de Microsoft.

Ainsi, une seule clé (licence en volume) est définie sur le serveur KMS, associée à un nombre de postes défini. Celle-ci est activée une seule fois par Internet. Par la suite, à chaque nouvel ajout d'une clé, il sera nécessaire d'activer celle-ci via Internet. Dès lors, il n'est plus nécessaire de diffuser des clés de licence auprès de tiers, au travers d'un master par exemple.

Le serveur KMS est disponible sur Windows Server 2012 ou versions supérieures. Une fois le service KMS installé sur un serveur, l'administrateur ajoute la clé KMS achetée, puis l'active par l'intermédiaire d'Internet.

Le serveur KMS s'inscrit auprès du serveur DNS principal du réseau en ajoutant un enregistrement de ressources SRV pour que les clients puissent facilement s'activer auprès de lui.

Voici le schéma d'une architecture KMS simple :



La clé VLK est la clé de licence en volume.

À la première installation du système d'exploitation, le client KMS envoie une demande d'activation au serveur KMS sur le port TCP 1688 et la renverra toutes les deux heures jusqu'à obtenir une réponse positive. Une fois validée, le client KMS tentera de se réactiver auprès du serveur KMS tous les sept jours. Il est donc vital que ce dernier soit toujours accessible. Côté serveur, l'activation d'une licence en volume doit être renouvelée tous les 180 jours.

Afin que le serveur KMS commence à activer des clients KMS, un seuil de requête d'activation doit être atteint :

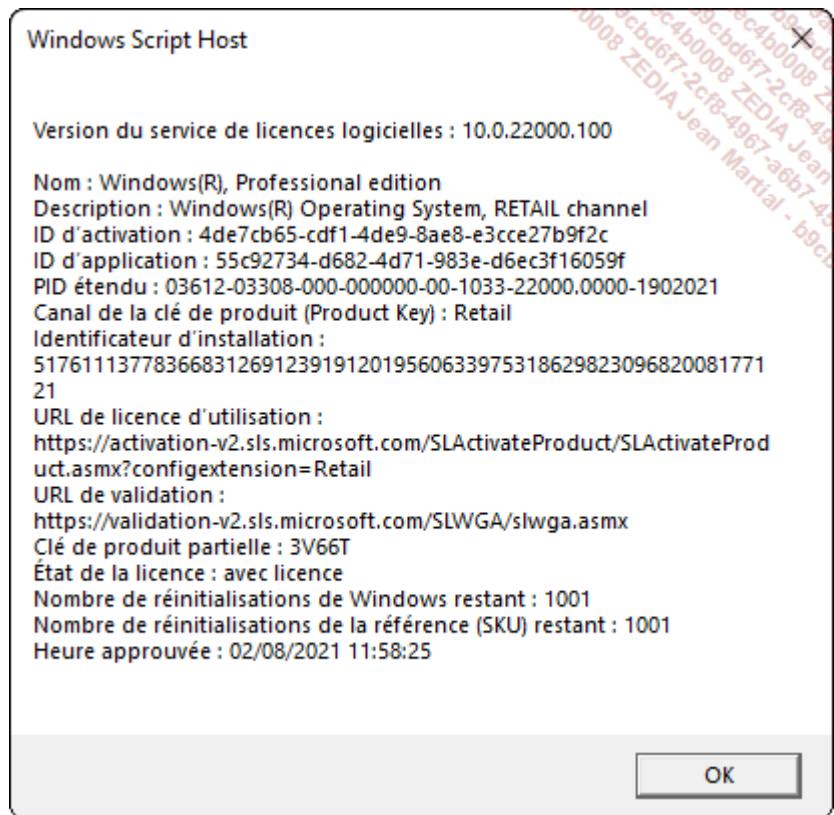
- 5 machines physiques ou virtuelles Windows Server.
- et 25 machines clientes physiques ou virtuelles Windows 11.

Pour installer le service KMS sur un ordinateur Windows 11, il suffit de se munir d'une clé de licence en volume et de respecter la procédure suivante :

Ouvrez une session sur l'ordinateur Windows 11 en tant qu'administrateur. Dans une invite de commandes que vous aurez au préalable exécutée en tant qu'administrateur, exécutez la commande : slmgr.vbs /ipk RWJNJ-2KH4B-XXXXX-XXXXX-XXXXX

Nous devons maintenant activer la clé de licence en volume par Internet : slmgr.vbs /ato. Dans le cas où l'ordinateur Windows 11 n'aurait pas accès à Internet, l'activation est possible par téléphone en tapant la commande slui.exe 4 et en suivant les étapes d'activation.

Pour vérifier l'état actuel de la licence sur le poste Windows 11, exécutez la commande slmgr.vbs /dlv.



3. Clé d'activation multiple (MAK)

a. Principe d'une clé MAK

Une clé MAK (*Multiple Activation Key*) contient un nombre prédéterminé d'activations autorisées, en fonction du contrat de licence en volume acquis par l'entreprise. Chaque activation d'un système d'exploitation Microsoft réduit ainsi le nombre limite d'activations.

Contrairement à l'utilisation du service KMS, l'activation MAK est utilisée une seule fois, n'exigeant ainsi aucun renouvellement auprès des services d'activation Microsoft.

Nous allons voir que l'utilisation d'une clé MAK est recommandée pour les ordinateurs qui se connectent rarement au réseau de l'entreprise mais plutôt au réseau internet : le personnel itinérant, comme les commerciaux, est donc une cible de choix.

En effet, deux options d'activation MAK sont disponibles :

- Activation indépendante MAK : chaque client se connecte par le biais d'Internet au service d'activation de Microsoft et s'active automatiquement. Le processus d'activation est aussi disponible par téléphone. Pour connaître la liste des numéros de téléphone, parfois gratuits, des services téléphoniques par pays, connectez-vous à l'adresse ci-dessous : <https://www.microsoft.com/fr-fr/licensing/existing-customer/activation-centers>
- Activation MAK par proxy : envoi d'une demande d'activation par l'intermédiaire d'une seule connexion, regroupant les demandes de plusieurs ordinateurs. Cette méthode est configurable à l'aide de l'outil gratuit VAMT (*Volume Activation Management Tool*) téléchargeable depuis le kit de déploiement et d'évaluation Windows ADK : <https://go.microsoft.com/fwlink/?linkid=2165884>

b. Volume Activation Management Tool

VAMT est inclus dans le kit Windows ADK et permet d'automatiser l'activation des postes de travail Windows, ainsi que les versions Windows Server et Microsoft Office. L'outil est administré depuis la console MMC (*Microsoft Management Console*) 3.0 et peut être géré à l'aide des commandes Windows PowerShell. Il prend désormais en charge l'activation basée sur Active Directory, ainsi que l'authentification par proxy.

Cet outil, disponible uniquement en version 32 bits et en anglais, gère l'activation en volume, à l'aide de clés MAK, KMS et Active Directory, d'ordinateurs physiques ou virtuels.

Vous pourrez ainsi spécifier un groupe d'ordinateurs à activer dans un domaine, dans un groupe de travail ou au travers d'adresses IP. Une fois que VAMT aura reçu les codes de confirmation d'activation en provenance de Microsoft, il se chargera de les transmettre à chaque ordinateur cible.

Les codes de confirmation étant stockés dans une base de données, vous pourrez réactiver un ordinateur précédemment activé ayant fait l'objet d'une ré-imagerie, sans nécessité de contacter Microsoft par téléphone.

L'utilisation d'une clé MAK prend tout son sens dans le cas où le nombre d'activations est inférieur à celui imposé par le service KMS (25 pour les versions client, 5 pour les éditions serveur).

Une clé MAK peut également être définie sur un ordinateur initialement configuré pour l'utilisation du service d'activation KMS.

L'intégration d'une clé MAK est possible au travers de l'image générée du système cible (cf. chapitre Conception d'une image de déploiement), ou manuellement sur le système cible, ou bien encore dans un fichier de réponses.

Par défaut, Windows 11 est installé en tant que client du service KMS. Pour transformer une activation KMS en activation MAK, il suffit d'installer une clé MAK sur l'ordinateur cible, pendant l'installation de Windows 11, ou bien après celle-ci, en exécutant la commande suivante en tant qu'administrateur local de l'ordinateur Windows 11 : slmgr.vbs /ipk <votrecléMAK>

Si l'installation de la clé se fait au moyen du script slmgr.vbs, le client ne tentera pas de s'activer automatiquement par Internet, contrairement à une installation par l'interface utilisateur.

Lors de la phase d'installation, le système génère un identifiant matériel à partir des composants de l'ordinateur :

- Carte réseau.
- Taille de la mémoire vive.
- Type de processeur et numéro de série associé.
- Carte graphique...

L'identifiant matériel et la clé de produit sont envoyés à Microsoft de manière cryptée ; une réactivation du système d'exploitation peut être nécessaire dans le cas où la configuration matérielle de l'ordinateur changerait de manière majeure.

Résumé du chapitre

- Quatre éditions de Windows 11 sont principalement disponibles : une à destination des particuliers (Famille), deux pour les professionnels (Professionnel et Entreprise) et une dédiée au marché de l'éducation (Education).
- Avant d'installer Windows 11, l'administrateur doit vérifier que son matériel et ses logiciels sont compatibles avec le nouveau système d'exploitation.
- L'utilisateur peut, au choix, créer une nouvelle installation de Windows 11, mettre à niveau depuis Internet un ancien système d'exploitation vers Windows 11, avec une étape intermédiaire vers Windows 10, ou effectuer une migration des données et une installation vierge. L'outil USMT permet de sauvegarder les données des utilisateurs.
- Windows 11 peut s'installer depuis un DVD d'installation, une mémoire flash USB ou un disque virtuel.
- L'utilisateur peut ouvrir une session à l'aide de son compte Microsoft créé sur Internet (messagerie Hotmail par exemple), afin de retrouver son environnement quel que soit le poste sur lequel il se connecte. Plusieurs méthodes d'authentification sont disponibles, en fonction du matériel présent : le mot de passe classique, le mot de passe image, qui implique l'exécution de gestes sur une image, le code confidentiel, qui nécessite un

code PIN, l'authentification biométrique, basée sur les empreintes digitales, l'iris ou le visage de l'utilisateur, via Windows Hello.

- La fonctionnalité Accès attribué (mode kiosque) permet d'imposer l'utilisation d'une seule application du Microsoft Store pour un compte d'utilisateur Microsoft spécifique. Ainsi, une entreprise pourra restreindre un système à n'accéder qu'à son logiciel métier sous forme de borne cloisonnée.
- Windows 11 fournit la fonctionnalité Contrôle parental, qui s'appuie sur un compte Microsoft pour suivre l'activité de l'enfant, quelle que soit la machine sur laquelle il ouvre une session. Des rapports hebdomadaires sur son activité sont générés, puis envoyés par courriel à l'adresse des parents.
- Le service de gestion des clés ou KMS permet de répondre aux demandes d'activation des clients Microsoft. Aucune clé de licence n'est à entrer sur les clients, et aucune activation n'est confirmée sur le site de Microsoft. Une seule clé (licence en volume) est définie sur le serveur KMS, associée à un nombre de postes défini.
- Une clé MAK contient un nombre prédéterminé d'activations autorisées, en fonction du contrat de licence en volume qu'a acquis l'entreprise. Contrairement à l'utilisation du service KMS, l'activation MAK est utilisée une unique fois, n'exigeant ainsi aucun renouvellement auprès des services d'activation Microsoft.
- Un administrateur peut gérer les activations des systèmes dont il a la charge grâce à un domaine Active Directory. Seul un ordinateur membre d'un domaine peut utiliser cette nouvelle méthode d'activation qui ne nécessite aucune intervention manuelle.

Conception d'une image de déploiement

Introduction

- Les services informatiques doivent régulièrement déployer des systèmes d'exploitation clients ou serveurs dans leur entreprise. Les tâches d'administration et de support liées à ces opérations d'installation sont trop souvent réalisées manuellement et donc coûteuses en temps d'intervention.
- Avec Windows 11, le processus de création et de déploiement d'une image est grandement simplifié. Tout ce processus permet de personnaliser l'installation de Windows 11 tout en réduisant le coût de déploiement au minimum.
- Deux méthodes permettent de déployer un poste de travail Windows 11 dans un environnement d'entreprise : **Lite Touch** et **Zero Touch**.
- La méthode Lite Touch nécessite une infrastructure contenant un serveur de stockage des images, un serveur de déploiement (type WDS) et un serveur de données contenant les sauvegardes des utilisateurs dans le cadre d'une migration. Un administrateur devra personnaliser les paramètres de déploiement grâce à un fichier de réponses pour limiter son intervention.
- **Microsoft Deployment Toolkit** (MDT) contient les outils nécessaires à ce type de déploiement.
- Un déploiement Zero Touch ne nécessite aucune intervention humaine, la procédure de déploiement du poste est entièrement automatisée. L'infrastructure nécessaire est décrite ci-dessous :
 - Un serveur Point de distribution des images.
 - Un serveur de données contenant les sauvegardes des utilisateurs.
 - Un serveur d'applications stockant les fichiers d'installation des applications de l'entreprise.
 - Un serveur WDS pour déployer Windows PE.
- Des produits tels que **SCCM** ou **MDT** permettent d'effectuer ce type de déploiement grâce à un séquenceur de tâches qui exécute un assistant de génération des étapes Zero Touch.
- Avant de migrer un parc informatique vers la toute dernière version du client Windows, il est important d'inventorier celui-ci, en listant les applications métiers, les pilotes de périphériques et bien entendu les fonctionnalités Windows 11 vers lesquelles migrer.

Upgrade Readiness

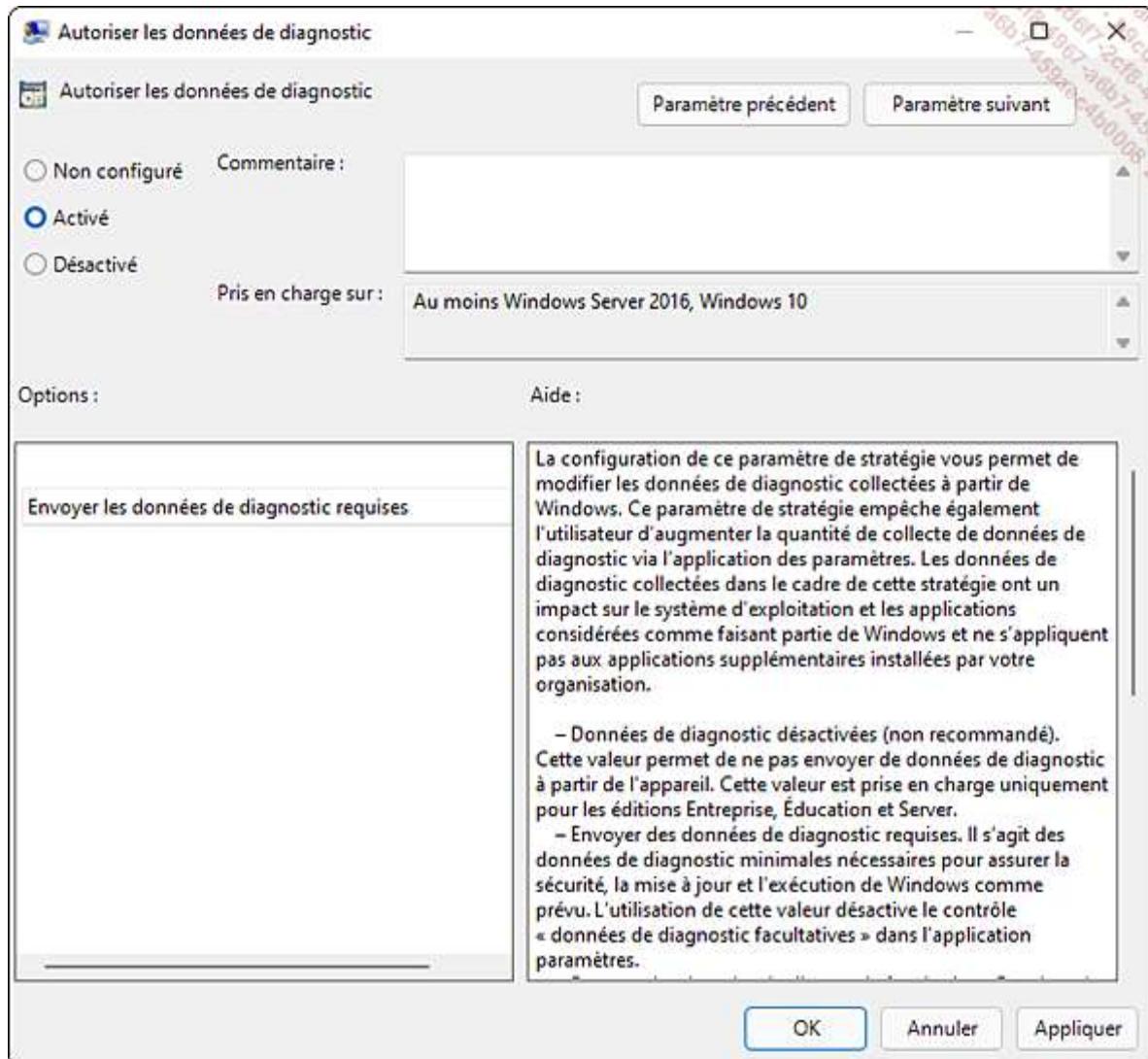
- Upgrade Readiness (anciennement Upgrade Analytics) est un service gratuit intégré à Windows Analytics au sein du modèle cloud Windows as a Service. Un bilan de la compatibilité des systèmes avec un passage vers Windows 11 est proposé sous forme de tableau de bord. Le logiciel évalue l'état de préparation des appareils de votre environnement en vue d'une mise à niveau vers Windows 11. Intégré à Configuration Manager, Upgrade Readiness permet d'accéder aux données de compatibilité de mise à niveau du client.
- Concrètement, le service s'appuie sur la télémétrie du système pour collecter les données système, applicatives et les drivers. Lorsqu'un problème de compatibilité est détecté, un correctif est suggéré (lorsque connu par Microsoft).
- Par exemple, pour activer le niveau de télémétrie depuis un objet stratégie de groupe - dans notre cas, local - suivez la procédure ci-dessous :

Pressez les touches  + R du clavier puis saisissez gpedit.msc et validez via le bouton **OK**.

Dans la fenêtre **Éditeur de stratégie de groupe locale**, développez le nœud **Configuration ordinateur - Modèles d'administration - Composants Windows - Collecte des données et versions d'évaluation Preview**.

Double cliquez sur le paramètre **Autoriser les données de diagnostic**. Sélectionnez l'option **Activé** puis dans le menu déroulant **Options**, cliquez sur **Envoyer les données de diagnostic requises**.

- La première option, **Données de diagnostic désactivées**, empêche l'envoi de données de diagnostic à Microsoft. Cette option est prise en charge uniquement sur les éditions Entreprise, Éducation et Server. L'option suivante, **Envoyer les données de diagnostic requises**, envoie les données de diagnostic minimales pour assurer la sécurité du système. Enfin, la troisième option, **Envoyer des données de diagnostic facultatives**, inclut les données requises en y ajoutant des données sur l'utilisation de Windows, des applications installées, des performances du système, des journaux de diagnostic, des vidages sur incident.



Cliquez sur le bouton **OK**.

- Sur le poste Windows 11 cible, depuis un objet stratégie de groupe (dans notre cas, local), suivez la procédure ci-dessous pour joindre ce dernier à la base de données du service Upgrade Readiness :

Pressez les touches + R du clavier, puis saisissez gpedit.msc et validez via le bouton **OK**.

Dans la fenêtre **Éditeur de stratégie de groupe locale**, développez le nœud **Configuration ordinateur - Modèles d'administration - Composants Windows - Collecte des données et versions d'évaluation Preview**, et double cliquez sur le paramètre **Configurer l'ID commercial**.

Dans le champ **ID commercial**, collez la clé. Cliquez sur le bouton **OK** pour valider l'action.

- Pour connaître toutes les étapes d'implémentation d'Upgrade Readiness dans Configuration Manager, suivez les liens ci-dessous : <https://docs.microsoft.com/fr-fr/mem/configmgr/core/clients/manage/upgrade-readiness>, <https://docs.microsoft.com/fr-fr/mem/configmgr/desktop-analytics/connect-configmgr> et <https://docs.microsoft.com/fr-fr/mem/configmgr/desktop-analytics/overview>.

Format de fichier WIM

- Le format de fichier **WIM** (*Windows Imaging*) a été proposé avec Windows Vista. Il permet à une seule image d'un système Windows d'être déployée et appliquée au travers du réseau sur un ensemble de postes de travail. Windows 11 utilise celui-ci pour s'installer de manière manuelle. Cette image WIM possède de multiples avantages :
 - Indépendance du matériel de destination : une image unique peut donc être appliquée indifféremment sur des matériels de constructeurs différents (HP, Dell...).
 - Indépendance du contenu : un fichier de référence peut contenir de multiples images, chacune contenant des applications différentes. Un même fichier WIM peut donc fournir une image Windows 11 Professionnel avec la suite bureautique Office 2016 et une autre image Windows 11 Entreprise avec la fonctionnalité BitLocker activée.
 - Compression : lors de la génération du fichier WIM, la compression des images permet de réduire considérablement le temps de déploiement par le réseau. Les fichiers communs aux différentes images ne sont stockés qu'une fois.
 - Modification sans recouvrement : une image doit évoluer avec le temps, car de nouvelles vulnérabilités ou applications émergent en permanence. Il est possible de modifier une image hors connexion, en ajoutant/supprimant des fichiers, sans avoir à générer une nouvelle image. De plus, l'application d'une image sur une partition n'efface pas les données (par exemple : documents Word ou classeurs Excel) qu'elle contient.
 - Démarrage Windows PE (*Preinstallation Environment*) : Windows PE, système d'exploitation minimal doté de fonctionnalités limitées, est le successeur de l'environnement MS-DOS de démarrage utilisé avec Microsoft Windows 2000 et Windows XP. Il est contenu dans le fichier **boot.wim** disponible dans le répertoire **Sources** du DVD d'installation Windows 11.
- Les différentes éditions de Windows 11 sont présentes dans le fichier **install.wim** qui est lui aussi stocké dans le dossier **Sources** du support d'installation du produit.

Environnement de préinstallation Windows PE

- Windows PE (version 10) est un système d'exploitation 32 ou 64 bits permettant d'installer une version client (Windows 7, Windows 8 et ultérieur) ou serveur (Windows Server 2012 et ultérieur) d'un produit Microsoft. C'est l'interface d'installation du produit, qui contient aussi un environnement de récupération nommé **Windows RE** (*Recovery Environment*). Pour de plus amples informations sur Windows RE, consultez le chapitre Protection et récupération du système section Dépannage du système.
- Windows PE prend en charge des fonctionnalités telles que la capture d'images, des outils de sécurité (BitLocker et module TPM), ou encore des pilotes génériques. C'est ce système d'exploitation qui permettra à l'administrateur de partitionner son disque dur avant d'installer Windows 11 ou encore de modifier celui-ci lorsqu'il n'est pas en cours d'exécution.
- Windows PE supporte les partitions **NTFS 5**, la gestion du protocole TCP/IP et les pilotes de périphériques 32 bits et 64 bits. De plus, le système peut fonctionner au sein d'un hyperviseur et ainsi gérer les disques virtuels (VHD, VHDX).
- Notez que lors du démarrage, une lettre de lecteur X: est créée, ne correspondant pas au média support.
- Quatre méthodes permettent de démarrer Windows PE sur un ordinateur :
 - CD-ROM ou DVD-ROM.

- Périphérique flash USB.
- Disque dur.
- WDS : nécessite l'utilisation d'un serveur Microsoft Windows Server 2012 ou ultérieur membre d'un domaine et, du côté du client, d'une carte réseau compatible PXE (*Preboot eXecution Environment*).
- L'utilisation d'un disque virtuel permet d'émuler un système de fichiers CD-ROM, c'est pourquoi l'environnement se charge en mémoire vive, permettant ainsi à l'administrateur de retirer le média Windows PE (CD-ROM, mémoire flash USB).
- L'espace de travail par défaut dédié est de 512 Mo pour un ordinateur possédant plus de 1 Go de mémoire vive. Windows PE gère jusqu'à 64 Go de RAM pour une architecture x86, et 4 To pour une architecture x64.
- Windows PE version 32 bits gère les interfaces UEFI 32 bits, BIOS 32 bits ou BIOS 64 bits. La version 64 bits peut démarrer les ordinateurs avec interface UEFI 64 bits ou BIOS 64 bits.
- Néanmoins, ce n'est pas un système d'exploitation à usage général, il ne doit être utilisé que dans une optique de déploiement ou de récupération. Ainsi, après 72 heures d'utilisation continue, l'interpréteur de commandes est automatiquement arrêté. Par défaut, toutes les modifications sont effacées lorsque Windows PE est redémarré.
- Notez que WinPE n'est plus inclus dans le kit d'installation automatisé (ADK) de Windows 11. Il est téléchargeable à l'adresse suivante, sous la forme d'un fichier nommé **adkwinpesetup.exe** : <https://go.microsoft.com/fwlink/?linkid=2166133>

Création d'une installation de référence

Windows 11 offre la possibilité de créer une installation personnalisée du système à des fins de déploiement sur un ou plusieurs ordinateurs du réseau. Pour cela, une panoplie d'outils est mise à disposition gratuitement au travers du kit de déploiement et d'évaluation **Windows ADK**.

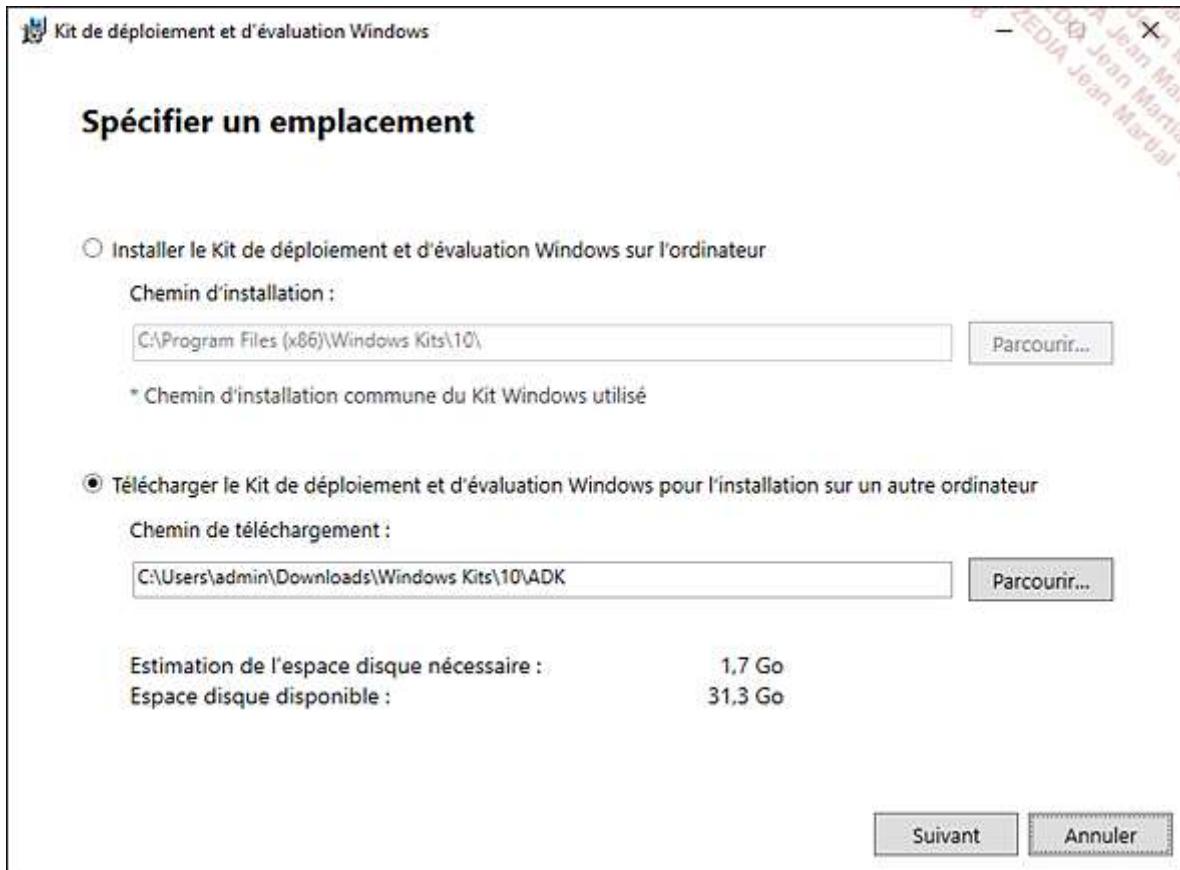
1. Kit d'installation automatisée Windows ADK

Le kit Windows ADK est une collection d'outils, librement téléchargeables depuis le site internet de Microsoft, vous permettant d'industrialiser le processus de déploiement de la famille Windows.

Avant de commencer le processus de création d'une image personnalisée, il faut télécharger le kit à l'adresse internet suivante : <https://go.microsoft.com/fwlink/?linkid=2165884>

Le kit est disponible sous la forme d'un fichier exécutable nommé **adksetup.exe**, qui a la charge de télécharger les outils sélectionnés par l'administrateur, ainsi que .NET Framework, nécessaire à son fonctionnement.

Il est aussi possible de graver sur un DVD une image ISO du kit. Il suffit de cocher l'option **Télécharger le Kit de déploiement et d'évaluation Windows pour l'installation sur un autre ordinateur** durant le processus d'installation.

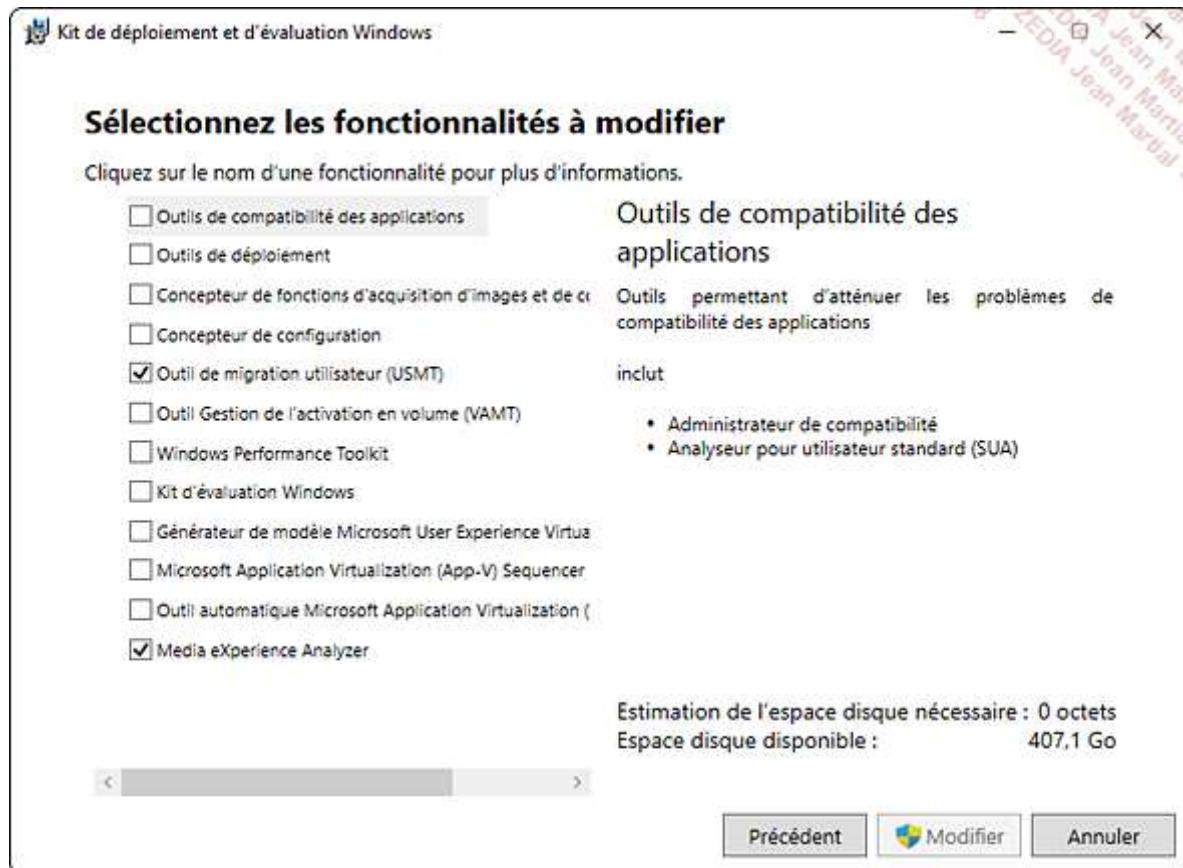


a. Composants du kit Windows ADK

Le kit d'évaluation et de déploiement contient les outils suivants :

- Outils de compatibilité des applications** : permet de créer un inventaire des logiciels installés et de générer des rapports de compatibilité en vue d'une mise à niveau vers Windows 11 (cf. chapitre Interface et applications, section Compatibilité des applications). Inclut **Administrateur de compatibilité** et **Analyseur pour utilisateur standard (SUA)**.
- Outils de déploiement** : gère et maintient les images de déploiement à l'aide de l'utilitaire **DISM** (*Deployment Image Servicing and Management*), **OEM Activation** et l'**Assistant Gestion d'installation (SIM)**, **OSCDIMG**, **BCDBoot**, **DISMAPI**...
- Concepteur de fonctions d'acquisition d'images et de configurations (ICD)** : création des packages de mise en service permettant de configurer un ordinateur ou un téléphone Windows 11 sans avoir à le réinstaller.
- Concepteur de configuration** : création des packages de mise en service permettant de configurer un ordinateur. Cette fonctionnalité est indispensable à la précédente.
- Outil de migration utilisateur (USMT)** : contient les programmes **ScanState** et **LoadState** (cf. chapitre Installation du client Windows 11, section Migration vers Windows 11).
- Outil Gestion de l'activation en volume (VAMT)** : gère l'activation de Windows 11 et d'Office de manière centralisée (cf. chapitre Installation du client Windows 11, section Gestion des licences).
- Windows Performance Toolkit** : enregistre et analyse les événements système. Contient les outils **Enregistreur de performances Windows**, **Analyseur de performance Windows** et **Xperf**.
- Kit d'évaluation Windows** : permet de simuler l'activité d'un utilisateur sur un ordinateur, afin de générer des métriques et ainsi suivre les recommandations en vue d'améliorer les performances du système. Les outils **Console d'évaluation Windows** et **Évaluations** seront installés.

- **Générateur de modèle Microsoft User Experience Virtualization (UE-V)** : capture les paramètres de personnalisation des applications et les met à disposition pour d'autres machines.
- **Microsoft Application Virtualization (App-V) Sequencer** : crée des applications virtuelles à partir d'applications traditionnelles.
- **Outil automatique Microsoft Application Virtualization (App-V) Sequencer** : outil similaire au précédent, mais automatisé.
- **Media eXperience Analyzer** : analyse graphique des performances multimédias. Contient **Auto eXperience Analyzer** et **Media eXperience Analyzer**.



Parmi les nouveautés, notons les fonctionnalités que propose le Concepteur de fonctions et d'acquisition d'images et de configuration (ICD) :

- Création d'un package de mise en service utilisable pour personnaliser le parc informatique Windows 11 de la société (ordinateurs, appareils mobiles, kiosques) sans avoir à réinstaller les cibles.
- Création d'une image Windows personnalisée pour des régions et des segments de marché précis.

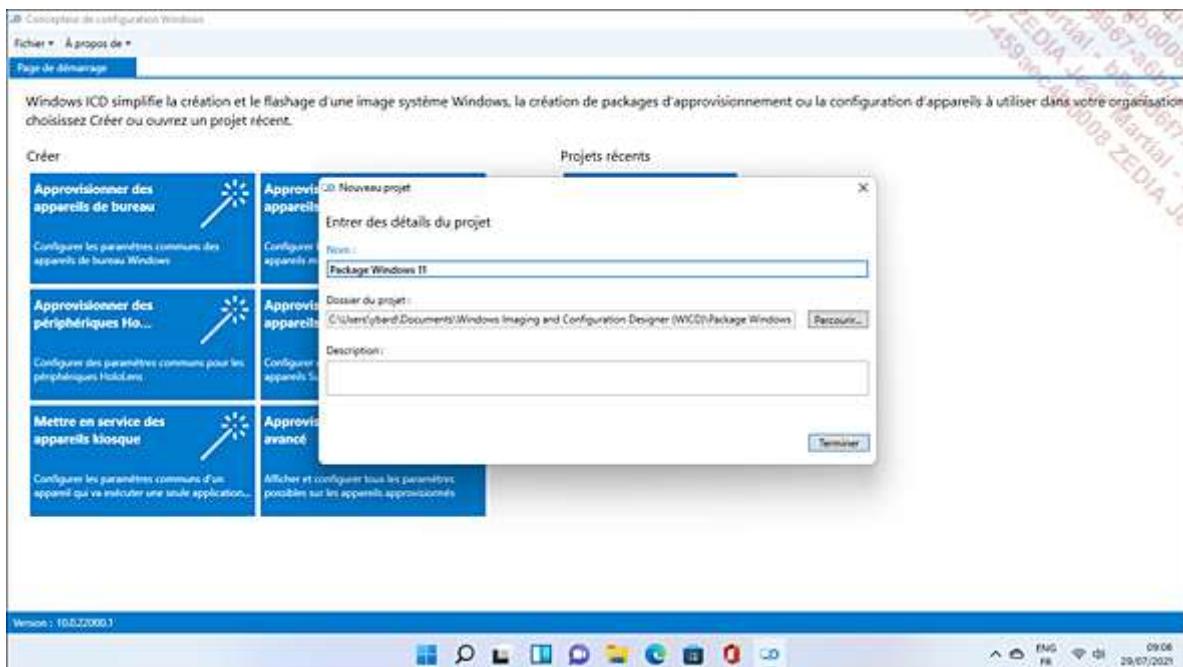
b. ICD

ICD permet donc de créer des packages de mise en service applicable sans destruction sur un ordinateur, nous affranchissant ainsi d'une réinstallation fastidieuse. Cet outil engendre un gain de temps sur la maintenance des ressources de l'entreprise.

Après avoir installé ICD depuis le kit Windows ADK, il est tout d'abord nécessaire de créer un package de mise en service simple. Voici la procédure :

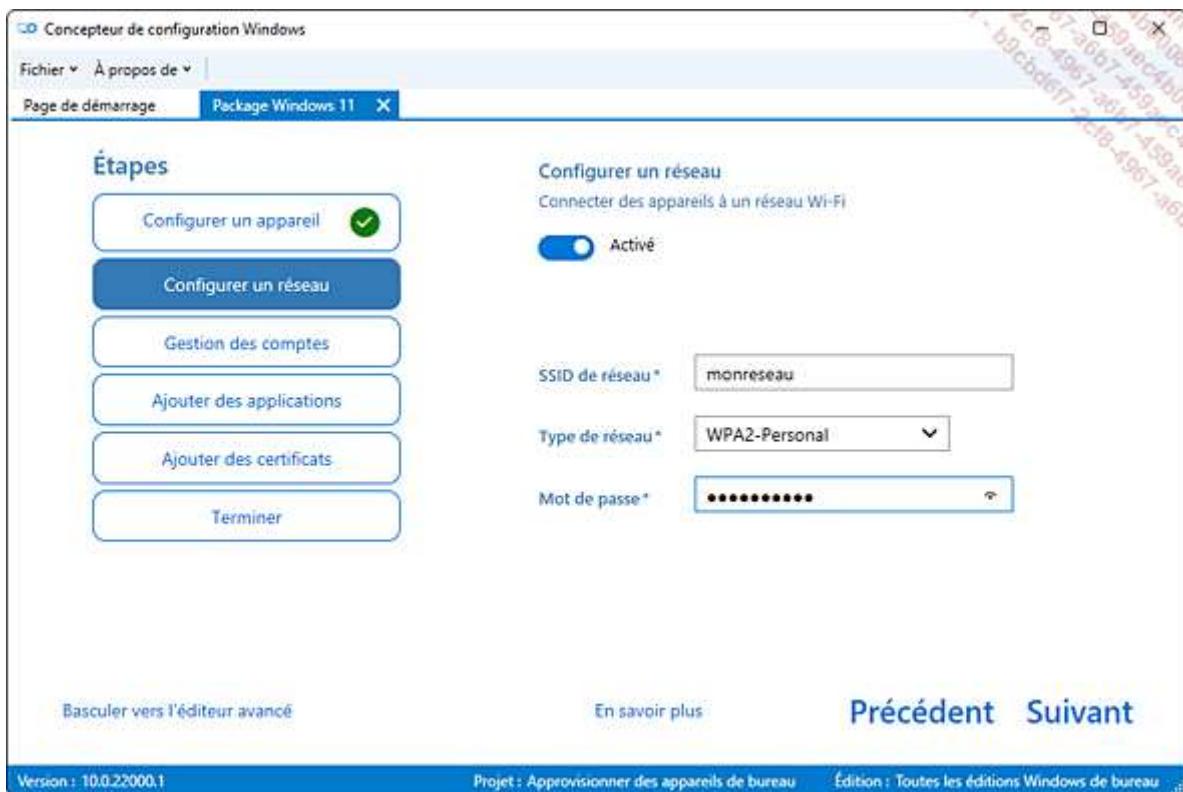
Depuis Windows 11, dans le champ de recherche situé sur la barre des tâches, saisissez **Concepteur de configuration et d'acquisition d'images Windows** (le nom peut être en anglais, **Windows Imaging and Configuration Designer**). Cliquez sur le bouton **Approvisionnement des appareils de bureau**.

Dans le champ **Nom** du projet, saisissez par exemple **Package Windows 11**. Laissez les autres champs par défaut et cliquez sur **Terminer**.



Spécifiez un nom d'appareil, dans notre exemple **nomsociete-%RAND:3%**. Ainsi, trois caractères aléatoires seront insérés dans le nom de l'ordinateur. Si nécessaire, saisissez une clé VLK contenant la licence du système Windows 11. Cliquez sur le bouton **Suivant**.

Saisissez le nom de votre réseau Wi-Fi, ainsi que sa clé WPA associée, puis cliquez sur **Suivant**.



L'étape suivante permet de joindre automatiquement le poste de travail à un domaine Active Directory, Azure ou non, en spécifiant le nom de celui-ci, ainsi qu'un nom d'utilisateur (avec mot de passe) autorisé à faire la jonction. Saisissez enfin le nom d'un compte local administrateur qui sera créé sur le système Windows 11.

Concepteur de configuration Windows

Fichier ▾ À propos de ▾

Page de démarrage Package Windows 11 X

Étapes

- Configurer un appareil ✓
- Configurer un réseau ✓
- Gestion des comptes
- Ajouter des applications
- Ajouter des certificats
- Terminer

Gérer des comptes scolaires/professionnels

Améliorer la sécurité et l'administration à distance en inscrivant des appareils dans Active Directory.

Incrire dans Active Directory

S'inscrire à Azure AD

Administrateur local

Utilisez un compte d'utilisateur moins privilégié pour inscrire des appareils dans Active Directory.

Nom du domaine * mondomaine.fr

Nom de l'utilisateur * mondomaine\Admin

Mot de passe de l'utilisateur ••••••••

Facultatif : créer un compte d'administrateur local

Nom de l'utilisateur adminlocal

Mot de passe ••••••••

Basculer vers l'éditeur avancé En savoir plus Précédent Suivant

Version : 10.0.22000.1 Projet : Approvisionner des appareils de bureau Édition : Toutes les éditions Windows de bureau

Cliquez sur le bouton **Suivant**. Si nécessaire, ajoutez des applications et des certificats.

Cliquez sur le bouton **Créer**.

Vous pouvez désormais appliquer ce package de mise en service à n'importe quel moment, que ce soit au moment du déploiement de l'image Windows 11 ou bien après. Le fichier généré porte l'extension .ppkg. Pour l'installer, double cliquez dessus.

Package Windows 11

Nouveau dossier ▾

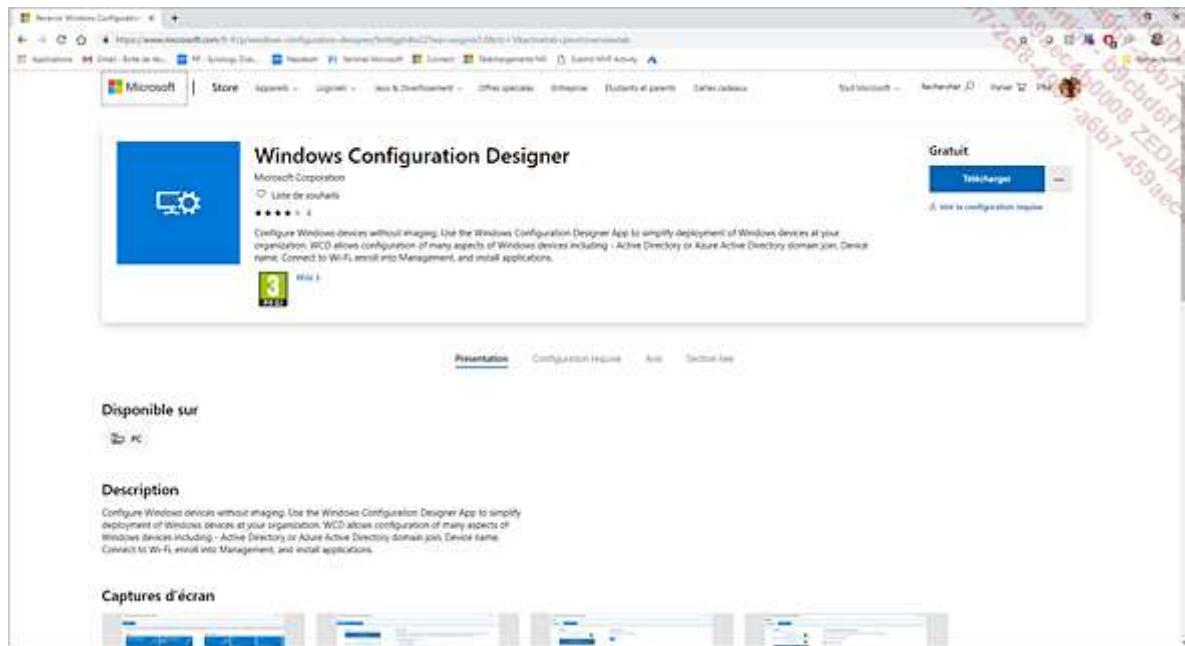
Rechercher dans : Package Windows 11

Nom	Modifié le	Type	Taille
customizations.xml	29/07/2021 09:16	Document XML	2 Ko
ICD.log	29/07/2021 09:09	Document texte	0 Ko
Package Windows 11.cat	29/07/2021 09:16	Catalogue de sécu...	1 Ko
Package Windows 11.jcdproj.xml	29/07/2021 09:16	Document XML	2 Ko
Package Windows 11.ppkg	29/07/2021 09:16	RunTime Provision...	9 Ko
SettingsMetadata.xml	29/07/2021 09:09	Document XML	577 Ko
TemplateState.data	29/07/2021 09:16	Fichier DATA	24 Ko

Documents Images Disque local (C:) Musique System32 Vidéos OneDrive Ce PC Bureau Documents Images Musique Téléchargements

7 élément(s)

Notez que depuis la version Creators Update de Windows 10, l'administrateur peut désormais installer le kit de déploiement depuis le Microsoft Store, en effectuant une recherche sur « Windows Configuration Designer » ou bien en cliquant sur le lien ci-dessous : <https://www.microsoft.com/fr-fr/store/p/windows-configuration-designer/9nblggh4tx22?wa=wsignin1.0&rtc=1>



Parmi les nouveautés apportées par cette version, ICD intègre de nouveaux assistants de création pour des périphériques (Surface Hub, HoloLens, etc.).

Scanstate.exe (cf. chapitre Installation du client Windows 11, section USMT), composant intégré à Windows ADK pour Windows 11, propose une fonctionnalité de sauvegarde de l'état des applications installées au sein d'un package de mise en service. Une fois créé, ce package avec applications peut être importé dans ICD afin de créer un média.

Au lieu d'utiliser **Sysprep** puis de capturer l'image Windows 11, nous utilisons l'outil **ScanState** avec les paramètres **/apps /ppkg** pour capturer les personnalisations des applications.

Sur le poste de travail Windows 11 de référence, assurez-vous que l'utilitaire ScanState est disponible (kit Windows ADK) puis saisissez la commande suivante depuis le dossier **C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\User State Migration Tool\amd64** (ou **x86** en fonction de l'architecture) dans une invite de commandes exécutée en tant qu'administrateur : `scanstate.exe /apps /ppkg C:\Packages\PMSAApps01.ppkg`

Ce n'est pas l'utilitaire **LoadState** qui va gérer l'installation des applications capturées précédemment à l'aide de ScanState, mais bien le fichier d'installation de Windows 11 nommé `setup.exe`. Avant cela, il est nécessaire d'utiliser la commande DISM afin de créer un média d'installation Windows 11 qui contiendra le fichier `ppkg`. Davantage d'informations sur la commande DISM seront données un peu plus loin dans ce chapitre (cf. section Gestion d'images avec DISM).

Voici la procédure à suivre :

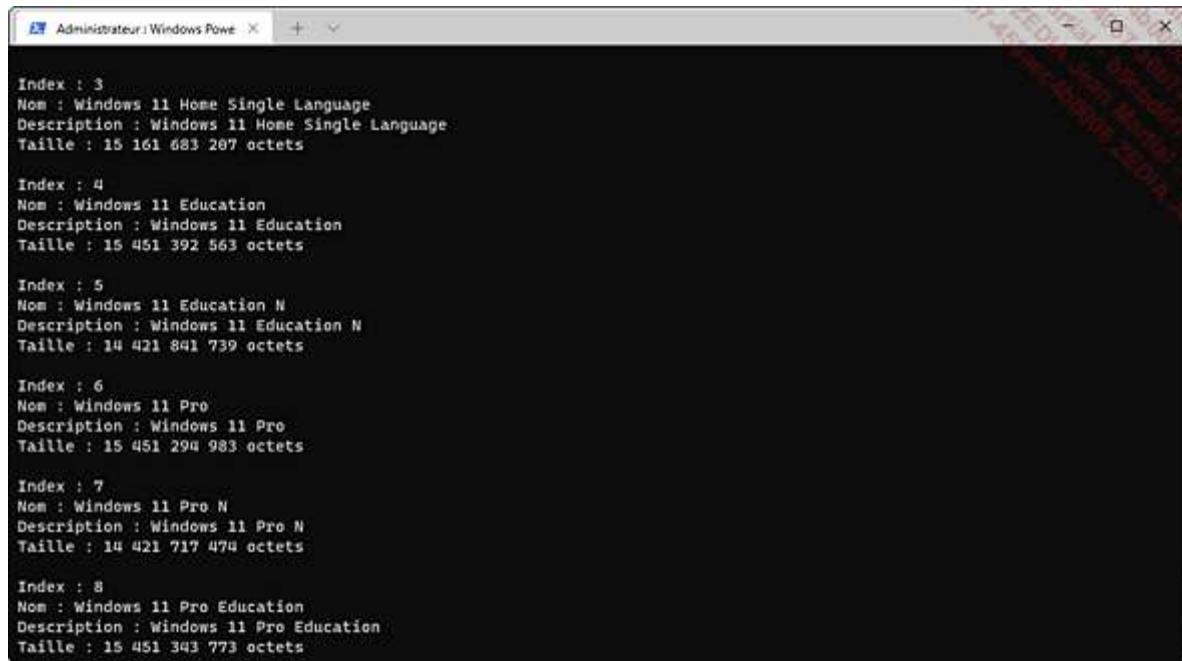
Montez l'image à l'aide de DISM. Si nécessaire, copiez les fichiers sources depuis le DVD ou la clé USB vers un dossier de l'ordinateur qui sert à effectuer la manœuvre.

Ouvrez une invite de commandes et positionnez-vous dans le dossier contenant les sources (les fichiers `.wim`), généralement **Sources**.

Chaque fichier WIN contient en réalité plusieurs éditions du système à installer (Famille, Professionnel, Entreprise...). Récupérez le numéro d'index de l'édition de Windows à modifier avec la commande :

```
22 dism /get-wiminfo /wimfile:.\install.wim
```

Généralement, pour la version Windows 11 Professionnel, l'index est le 6.



```
Index : 3
Nom : Windows 11 Home Single Language
Description : Windows 11 Home Single Language
Taille : 15 161 683 207 octets

Index : 4
Nom : Windows 11 Education
Description : Windows 11 Education
Taille : 15 451 392 563 octets

Index : 5
Nom : Windows 11 Education N
Description : Windows 11 Education N
Taille : 14 421 841 739 octets

Index : 6
Nom : Windows 11 Pro
Description : Windows 11 Pro
Taille : 15 451 294 983 octets

Index : 7
Nom : Windows 11 Pro N
Description : Windows 11 Pro N
Taille : 14 421 717 474 octets

Index : 8
Nom : Windows 11 Pro Education
Description : Windows 11 Pro Education
Taille : 15 451 343 773 octets
```

Montez l'image dans un dossier précédemment créé, ici **c:\mount**, et le numéro de l'index de l'édition de Windows à modifier, avec la commande :

```
dism /mount-wim /wimfile:.\\install.wim /mountdir:c:\\mount /index:6
```

Puisqu'il s'agit d'une opération de décompression d'un fichier de plusieurs gigaoctets, l'exécution peut être relativement longue. Le fichier WIM ne doit pas posséder la propriété lecture seule.

Si l'image est au format esd, il est possible de la convertir avec la commande :

```
dism /export-image /SourceImageFile:.\\install.esd /SourceIndex:6 /
```

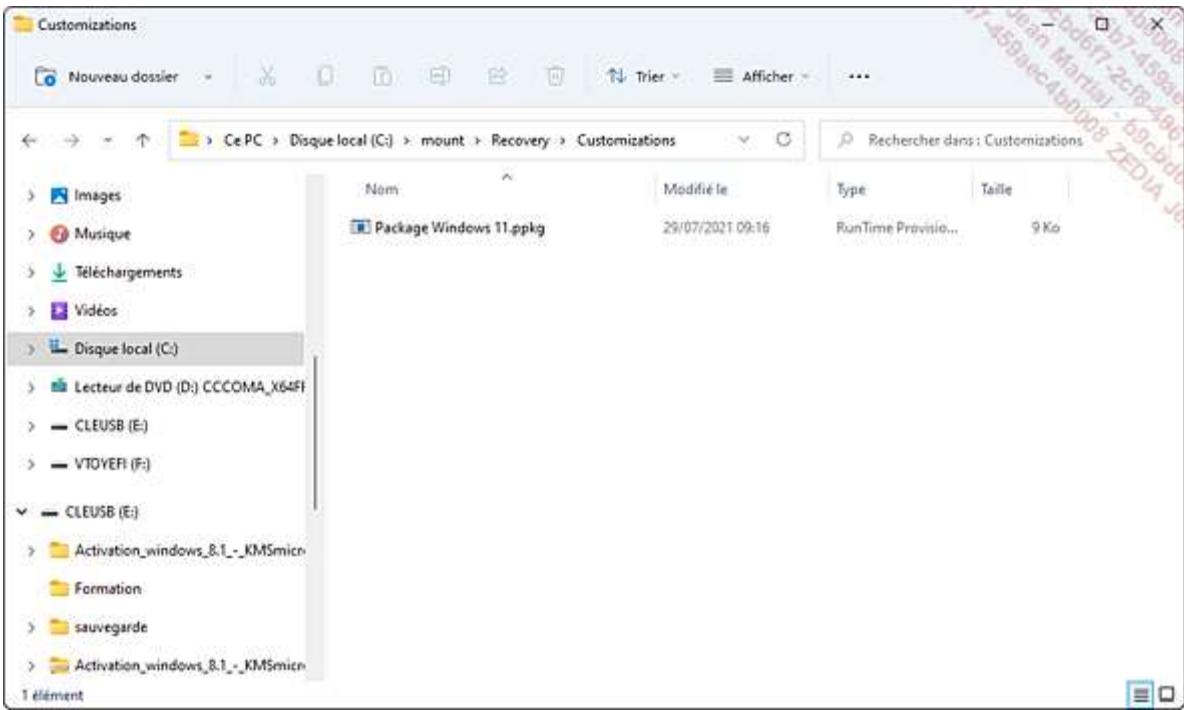
```
DestinationImageFile:c:\\install.wim /Compress:max /checkIntegrity
```

Injectez le package avec la commande :

```
dism /image=c:\\mount /add-provisioningpackage
```

```
/packagepath:c:\\package.ppkg
```

Un dossier **Recovery** a été ajouté à l'image contenant le fichier ppkg. Il est visible depuis le dossier de montage de l'image.



Démontez l'image :

```
dism /unmount-image /mountdir:c:\mount /commit
```

Puisqu'il s'agit d'une opération de compression de fichiers, l'exécution peut prendre plusieurs minutes.

L'image Windows 11 avec les applications personnalisées embarquées est désormais générée dans le fichier `install.wim` et pourra ainsi être déployée, via par exemple les services WDS.

2. Outil sysprep

L'outil sysprep, disponible depuis le répertoire local `%systemroot%\system32\sysprep\`, permet de supprimer toutes les données spécifiques créées lors de l'installation d'un système Windows 11, comme l'ID unique de sécurité. Vous pourrez ainsi capturer une image neutre mais personnalisée avec des applications, afin de la déployer sur des environnements hétérogènes.

Exécutez sysprep uniquement sur une nouvelle installation de Windows. Si l'ordinateur de référence est membre d'un domaine, sysprep le retirera automatiquement de celui-ci.

Voici la liste des options de ligne de commande les plus importantes à connaître lors de la manipulation de l'outil :

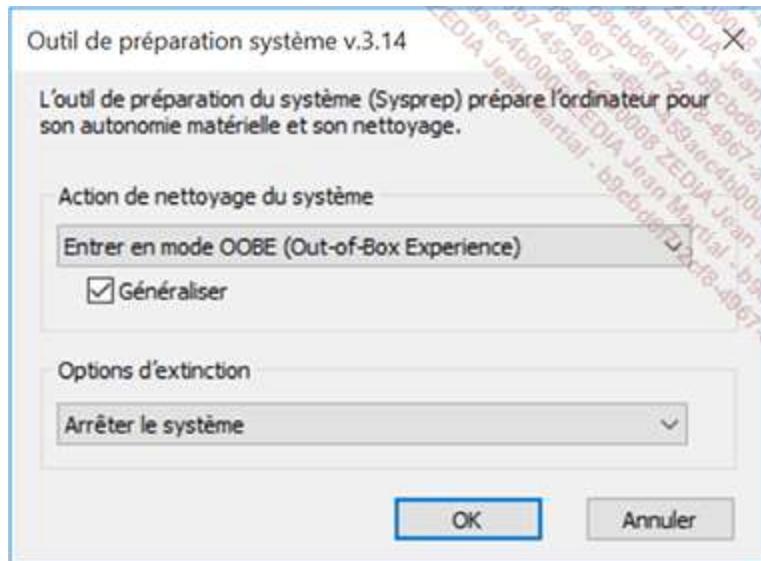
- **/audit** : ajoute des applications et des pilotes de périphériques tiers à votre image avant capture.
- **/generalize** : prépare l'ordinateur de référence à la création de l'image, en supprimant l'ID de sécurité et les points de restauration du système.
- **/oobe** : redémarre l'ordinateur source en affichant l'écran d'accueil Windows pour personnaliser Windows 11, permettant par exemple de créer des comptes d'utilisateur qui seront disponibles sur les installations déployées à partir de l'image.
- **/reboot** : redémarre l'ordinateur à l'issue du processus vous permettant d'auditer le système.

La procédure de préparation via l'interface graphique d'un ordinateur Windows 11 en vue de la création d'une image est la suivante :

Cliquez sur l'**Explorateur de fichiers** situé dans la barre des tâches. Naviguez jusqu'au dossier `C:\Windows\System32\sysprep` et double cliquez sur le fichier `sysprep.exe`.

Dans la zone **Action de nettoyage du système**, cliquez sur **Entrer en mode OOBE (Out-of-Box Experience)**. Cochez la case **Généraliser**.

Dans la zone **Options d'extinction**, cliquez sur **Arrêter le système**.



Validez par **OK**.

L'image Windows 11 est désormais prête à être dupliquée.

3. Gestion d'images avec DISM

DISM (*Deployment Image Servicing and Management*) est un outil disponible en ligne de commande permettant de modifier les images système portant l'extension .wim (install.wim) et les disques durs virtuels (.vhdx et .vhd) en mode hors connexion. Il peut, par exemple, ajouter des pilotes ou des fonctionnalités à ces mêmes images et offre la possibilité de mettre à niveau une image système Windows vers une autre édition. Il est intégré par défaut à Windows 11, vous n'avez donc pas à l'installer depuis le kit Windows ADK. Il peut gérer les images de tous les systèmes Microsoft commercialisés à ce jour pour stations de travail et serveurs. Le système Windows PE peut être aussi administré (fichier boot.wim).

Pour commencer à travailler sur une image WIM, il faut la monter dans un répertoire de travail temporaire, à l'aide de la commande dism.

Assurez-vous que toutes les dépendances du fichier dism.exe sont chargées en mémoire avant d'exécuter des commandes. Sinon, utilisez l'**Invite de commandes des outils de déploiement** disponible avec le kit ADK.

Les commandes DISM de ce chapitre doivent systématiquement être exécutées avec des priviléges élevés.

a. Monter une image

Avant de monter une image, il est nécessaire de choisir l'une des versions de Windows 11 sur laquelle nous travaillerons, définie par un index, un nom, une description et une taille. Le paramètre nous intéressant est principalement le numéro d'index, utilisé dans les futures manipulations.

Au préalable, copiez le fichier install.wim présent dans le dossier **sources** du DVD d'installation dans un dossier temporaire nommé, par exemple **c:\temp** sur l'ordinateur Windows 11. Dans ce même dossier, créez un sous-dossier nommé **offline**.

L'option get-wiminfo permet de lister les versions de Windows 11 contenues dans le fichier install.wim, et ainsi récupérer l'index utilisé :

Cliquez avec le bouton droit sur le menu **Démarrer**, puis sur **Terminal Windows (administrateur)**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît. Saisissez la commande :

```
dism /get-wiminfo /wimfile:c:\temp\install.wim
```

Pour l'exemple, choisissez la version Windows 11 Professionnel correspondant à l'index 6.

```
Index : 3
Nom : Windows 11 Home Single Language
Description : Windows 11 Home Single Language
Taille : 15 161 683 207 octets

Index : 4
Nom : Windows 11 Education
Description : Windows 11 Education
Taille : 15 451 392 563 octets

Index : 5
Nom : Windows 11 Education N
Description : Windows 11 Education N
Taille : 14 421 841 739 octets

Index : 6
Nom : Windows 11 Pro
Description : Windows 11 Pro
Taille : 15 451 294 983 octets

Index : 7
Nom : Windows 11 Pro N
Description : Windows 11 Pro N
Taille : 14 421 717 474 octets

Index : 8
Nom : Windows 11 Pro Education
Description : Windows 11 Pro Education
Taille : 15 451 343 773 octets
```

Montez maintenant l'image :

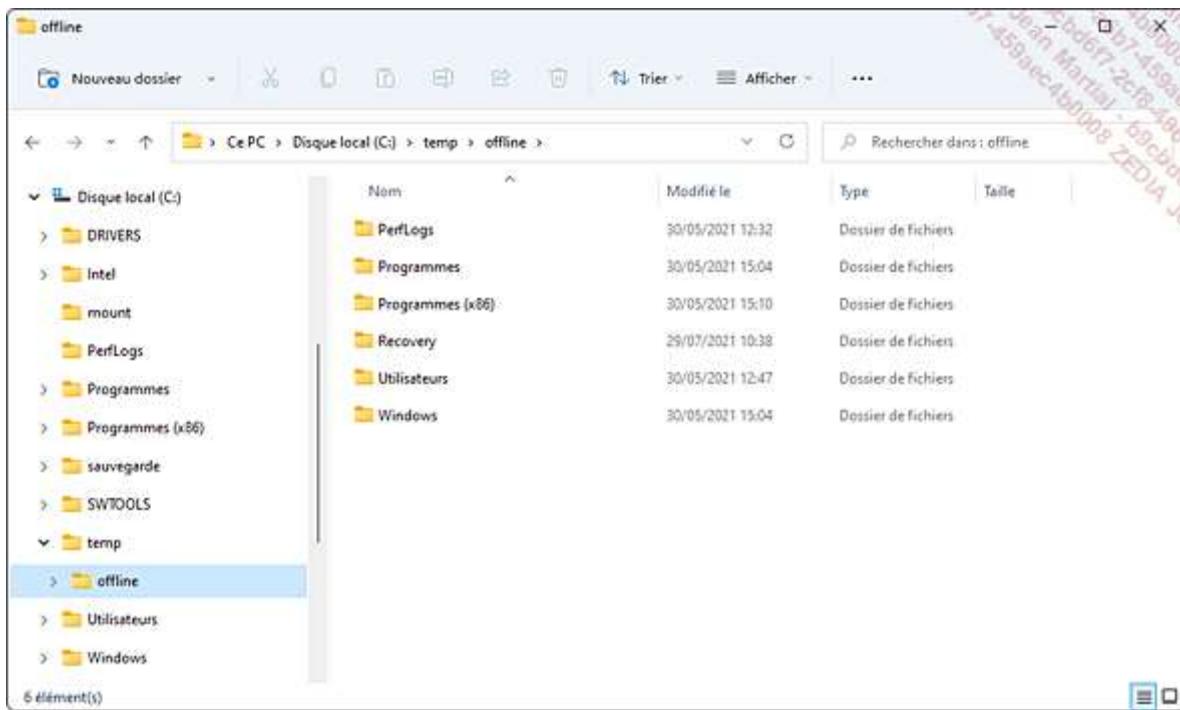
```
dism /Mount-Wim /WimFile:C:\temp\install.wim /index:6
```

```
/MountDir:C:\temp\offline
```

```
PS C:\temp> dism /mount-wim /wimfile:.\install.wim /mountdir:c:\temp\offline /index:6
Outil Gestion et maintenance des images de déploiement
Version : 10.0.22000.1

Montage de l'image
[=====100.0%=====]
L'opération a réussi.
PS C:\temp>
PS C:\temp>
PS C:\temp>
PS C:\temp> |
```

Le contenu du répertoire de l'image hors connexion monté dans le dossier **c:\temp\offline** est le suivant :



DISM supporte un nombre illimité de points de montage. La commande suivante liste les images déjà montées :

```
dism /Get-MountedWimInfo
```

L'image Windows 11 l'étant déjà, il suffit maintenant d'ajouter des composants, tels qu'une fonctionnalité, une mise à jour de sécurité, ou encore un pilote de périphérique.

Pour obtenir la liste des fonctionnalités installables, utilisez la commande :

```
dism /Image:c:\temp\offline /get-features
```

Notez que l'option /get-drivers liste les pilotes tiers disponibles et /get-packages affiche les packages présents.

Le résultat de la commande affichant un grand nombre de fonctionnalités, il peut être utile d'ajouter "pipe more" (| more) pour contrôler le défilement, ou encore de rediriger (>) le résultat dans un fichier.

Voici le résultat de la commande :

```
PS C:\temp> dism /image:c:\temp\offline /get-features

Outil Gestion et maintenance des images de déploiement
Version : 10.0.22000.1

Version de l'image : 10.0.21996.1

Features listing for package : Microsoft-Windows-Foundation-Package~31bf3856ad364e35~amd64~~10.0.21996.1

Feature Name : Windows-Defender-Default-Definitions
State : Enabled

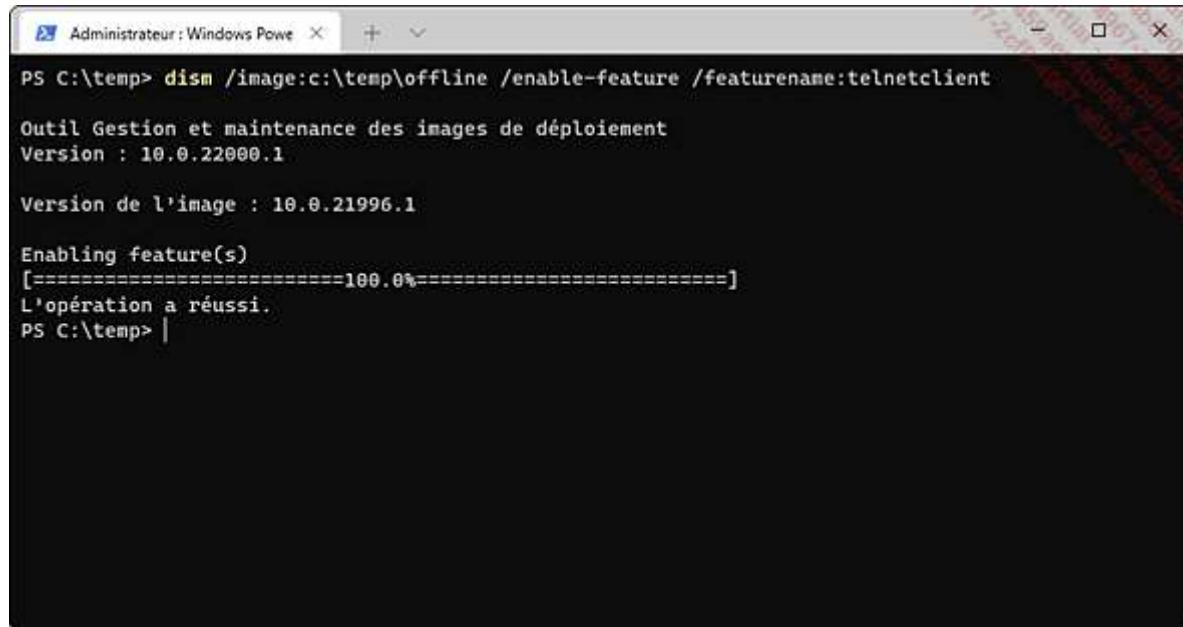
Feature Name : Printing-PrintToPDFServices-Features
State : Enabled

Feature Name : Printing-XPSServices-Features
State : Enabled

Feature Name : SearchEngine-Client-Package
State : Enabled
```

Pour activer le client Telnet, exécutez la commande suivante :

```
dism /image:c:\temp\offline /enable-feature /  
featurename:telnetclient
```



The screenshot shows a Windows PowerShell window titled "Administrateur : Windows Powe". The command entered is "dism /image:c:\temp\offline /enable-feature /featurename:telnetclient". The output shows the tool's version (10.0.22000.1), the image version (10.0.21996.1), and a progress bar indicating the enabling of features at 100.0%. It concludes with the message "L'opération a réussi." (The operation was successful).

La désactivation s'utilise de la même façon, avec le commutateur /disable-feature.

L'ajout d'une clé de produit Windows 11 peut aussi être réalisé à l'aide de la commande :

```
dism /image:c:\temp\offline /Set-ProductKey:VWXYZ-VWXYZ-  
VWXYZ-VWXYZ-VWXYZ
```

Notez que la validité de la clé de produit va être vérifiée par l'utilitaire DISM lors de l'exécution de la commande.

Une fois que l'image WIM a été personnalisée, il est nécessaire d'enregistrer les modifications en démontant l'image :

```
dism /unmount-wim /mountdir:c:\temp\offline /commit
```

Pour annuler les modifications effectuées et démonter l'image :

```
dism /unmount-wim /mountdir:c:\temp\offline /discard
```

Tant que l'image ne sera pas démontée, aucun paramètre modifié ne sera pris en compte.

L'image personnalisée peut désormais être déployée au travers du réseau (service WDS), ou bien depuis un support d'installation.

Une fois que l'ordinateur de référence a été préparé à l'aide de l'utilitaire sysprep, que l'image au format WIM a été modifiée grâce à la commande DISM, il est nécessaire de la capturer puis de l'appliquer à un ordinateur, grâce aux paramètres Capture-Image et Apply-Image.

b. Capturer une image

Capturer une image est relativement simple. Nous supposerons dans notre démonstration qu'un administrateur souhaite créer une image personnalisée d'une partition C: dans un fichier install.wim stocké sur la partition D:.

La commande suivante, exécutée grâce aux options de démarrage avancées (cf. chapitre Protection et récupération du système, section Dépannage du système) fournies par Windows RE, permet d'effectuer cette action :

```
dism /capture-image /imagefile:D:\install.wim
```

```
/capturedir:C:\ /name:"Windows 11 Professionnel"
```

Notez qu'un répertoire vide ne peut être capturé.

Lorsque vous générerez un fichier WIM, celui-ci doit être stocké sur un support, qui peut être un partage réseau, un périphérique de stockage USB ou une autre partition.

c. Créer une partition avec DiskPart

La taille et le format de la partition de destination doivent être créés sur l'ordinateur de destination AVANT l'application de l'image, à l'aide de l'utilitaire DiskPart (cf. chapitre Gestion des disques et des pilotes, section Partitionnement et gestion des fichiers).

Dans l'invite de commandes exécutée depuis Windows PE sur le nouveau système à installer, saisissez les commandes suivantes et validez par la touche [Entrée] après chaque saisie :

Exécutez l'outil diskpart.

Sélectionnez le disque : select disk 0

Supprimez toutes les données du disque : clean

Créez une partition de 64 Go : create partition primary size=64000

Sélectionnez la partition 1 : select partition 1

Formatez la partition au format NTFS (*New Technology File System*) : format fs=ntfs label=PartitionWINDOWS quick

Affectez la lettre C à la partition nouvellement créée et activez-la : assign letter=c

Quittez l'utilitaire DiskPart : exit

d. Appliquer une image

Pour appliquer l'image précédemment créée sur la partition C: de votre nouvel ordinateur, il faut au préalable copier le fichier install.wim sur un emplacement accessible depuis Windows PE. Cela peut être un partage réseau nommé imageswin11 stocké sur un serveur SRV1 par exemple :

```
23 dism /apply-image /imagefile:\\SRV1\imageswin11\install.wim
```

```
24 /index:6/ApplyDir:C:\
```

Pour terminer l'application de l'image, nous devons configurer les fichiers de l'environnement de démarrage sur la partition système Windows 11.

e. Configuration de l'environnement de démarrage

L'outil **bcdboot** (cf. chapitre Protection et récupération du système, section Dépannage du système) configure la partition système, en nous permettant d'effectuer cette modification depuis le répertoire local %systemroot%\system32 du nouvel ordinateur :

Dans une fenêtre de Terminal exécutée en tant qu'administrateur du poste de travail Windows 11, saisissez : bcdboot c:\windows et validez par [Entrée].

Redémarrez l'ordinateur (commande shutdown) pour finaliser l'exécution de Windows 11.

Le système a ainsi été initialisé à l'aide de l'outil sysprep. Une image au format .wim a été créée, modifiée, capturée puis appliquée. Il est désormais possible d'industrialiser le processus en déployant le fichier WIM généré au travers d'un réseau.

Déploiement par le réseau

Le déploiement d'un système d'exploitation grâce au réseau de l'entreprise permet à l'équipe en charge de l'informatique d'économiser du temps, et de s'assurer que l'ensemble des postes de travail aura la même configuration de départ. De plus, ce type de déploiement permet de pallier l'absence de lecteur DVD y compris avec des images contenant des applications métier. Plusieurs produits, payants et gratuits, existent pour installer un système Windows 11 à distance. Nous allons les détailler ci-après.

1. Service de déploiement Windows

WDS est le service de déploiement de systèmes d'exploitation Microsoft. Il permet de déployer dans un réseau d'entreprise des fichiers WIM, VHD et VHDX en démarrant depuis Windows PE, plus précisément depuis le fichier **boot.wim**. Ainsi, un administrateur n'a plus besoin de se déplacer pour installer Windows 11 depuis un support tel qu'un DVD-ROM ou une clé USB.

WDS permet le déploiement de tous les systèmes d'exploitation Microsoft depuis Windows Vista et Windows Server 2008.

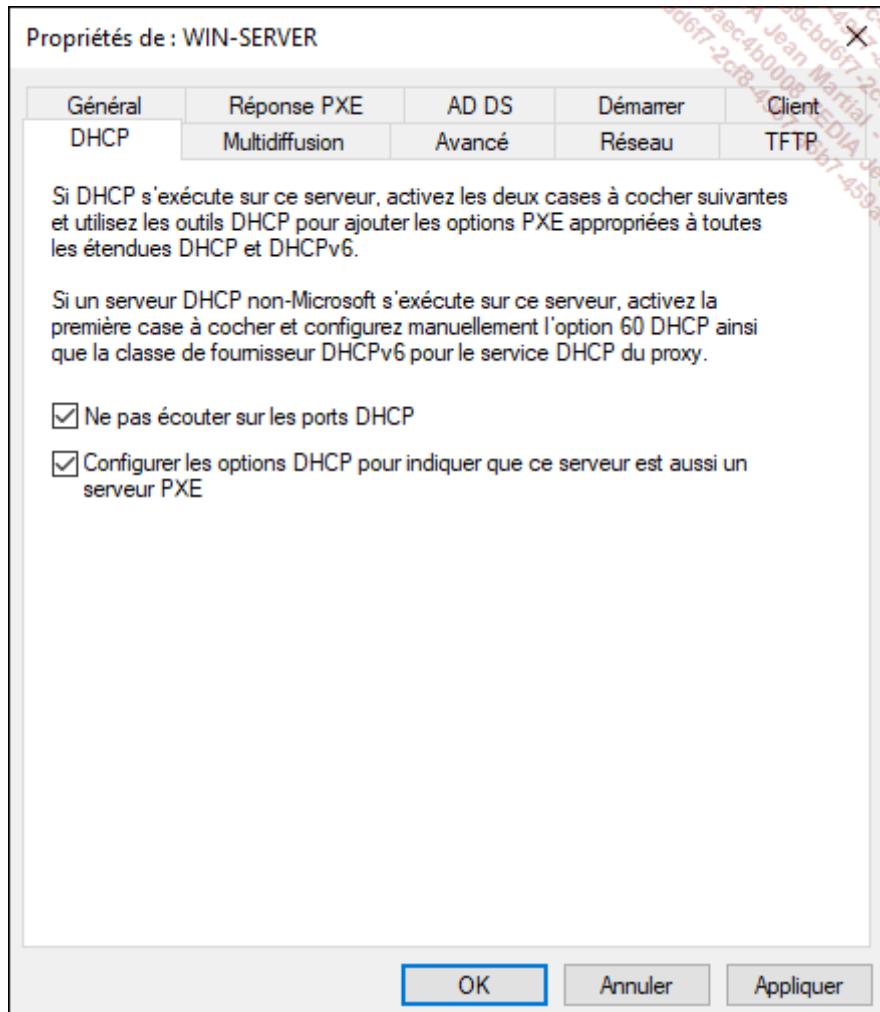
L'administrateur peut désormais créer des images d'un ordinateur de référence à l'aide de l'**Assistant Capture d'image**, remplaçant de l'utilitaire ImageX.

L'ajout de pilotes de périphériques peut être intégré aux images à déployer.

L'utilisation du service de déploiement Windows est soumise à des prérequis importants qu'il est nécessaire de connaître.

Dans un groupe de travail, le déploiement d'un serveur WDS nécessite les éléments suivants :

- Une version serveur de Windows, quelle que soit la version.
- Une partition NTFS : le serveur WDS disposera d'une partition NTFS idéalement distincte de la partition système servant à stocker les images à déployer sur votre réseau.
- Un serveur DNS (*Domain Name System*).
- Un serveur DHCP (*Dynamic Host Configuration Protocol*) autorisé doit être présent sur le réseau. Il peut être installé en tant que service sur le serveur de déploiement, mais dans ce cas, il vous faudra configurer WDS pour qu'il n'écoute pas sur le port 67, afin que les services WDS et DHCP n'entrent pas en conflit. De plus, pour que les clients PXE puissent détecter la présence d'un serveur WDS, il est nécessaire de cocher la case **Configurer les options DHCP pour indiquer que ce serveur est aussi un serveur PXE**. Ces actions s'effectuent dans les propriétés du serveur WDS, depuis l'onglet **DHCP**.



- L'utilisateur chargé d'installer le rôle WDS doit être membre du groupe local Administrateurs du serveur.
- Le client sur lequel vous souhaitez installer l'image doit posséder une carte réseau compatible PXE activée depuis le BIOS. Dans le cas contraire, l'installation devra s'effectuer en démarrant l'ordinateur à partir du DVD Windows 11 et en se connectant à un dossier partagé contenant les sources. Le client doit être autorisé dans la console WDS au travers d'une stratégie de réponse PXE.
- Les ports UDP suivants doivent être ouverts sur le pare-feu du serveur WDS :
 - Port 67 (DHCP).
 - Port 69 (*Trivial File Transfer Protocol*) : le transfert des images du serveur WDS vers les clients s'effectue au travers du protocole TFTP.
 - Port 4011 (PXE).
- À l'installation du rôle Services de déploiement Windows, les règles d'ouverture des ports sont automatiquement créées.

Dans un domaine Active Directory, voici les prérequis :

- Un serveur WDS (n'importe quelle version de serveur) doit être membre d'un domaine Microsoft. Les ordinateurs de destination peuvent faire partie d'un domaine ou d'un groupe de travail.
- L'existence d'un domaine Microsoft Active Directory repose sur un serveur DNS. Il n'est pas obligatoire qu'il soit installé sur le même serveur que WDS.
- Un serveur DHCP autorisé avec les mêmes paramètres de configuration que pour un groupe de travail.

- L'utilisateur chargé d'installer le rôle WDS doit être membre du groupe local Administrateurs et du groupe Utilisateurs du domaine pour initialiser le serveur.
- Une carte réseau compatible PXE.
- L'ouverture des ports : idem que pour le groupe de travail.

WDS comprend deux services de rôle :

- **Serveur de transport** : fournit un sous-ensemble des fonctionnalités des services WDS, comme la transmission de données par multidiffusion.
- **Serveur de déploiement** : comprend toutes les fonctionnalités de déploiement d'images.

La console MMC WDS permet de gérer le rôle WDS depuis une interface graphique. L'administrateur peut aussi utiliser la commande wdsutil pour effectuer des actions, tout en automatisant des tâches à l'aide de scripts.

Deux méthodes permettent de déployer WDS sur un serveur Windows Server 2019.

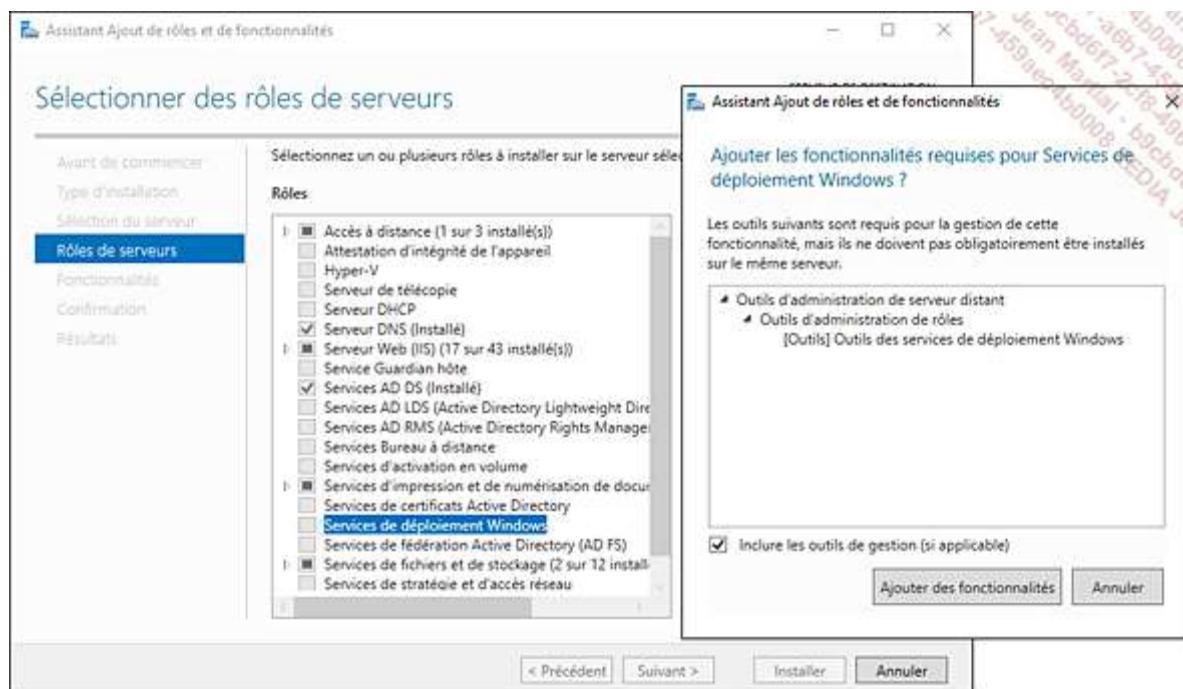
Depuis la console Gestionnaire de serveur

Cliquez sur **Ajouter des rôles et des fonctionnalités**, puis sur le bouton **Suivant**.

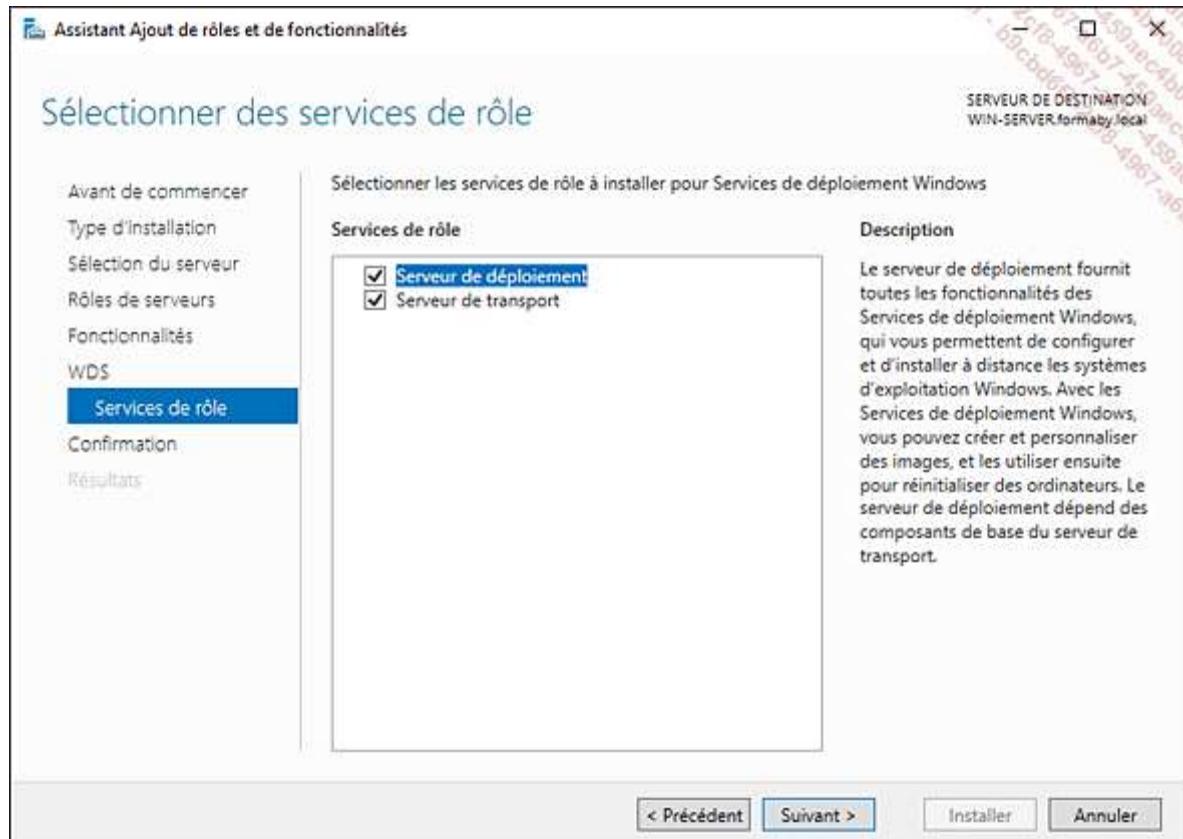
Cochez la case **Installation basée sur un rôle ou une fonctionnalité** puis validez par **Suivant**.

Assurez-vous que le nom de votre serveur est bien sélectionné puis cliquez sur **Suivant**.

Dans **Rôles de serveurs**, cochez la case **Services de déploiement Windows** puis, dans la fenêtre qui apparaît, vérifiez que la case **Inclure les outils de gestion** est bien cochée. Cliquez sur le bouton **Ajouter des fonctionnalités**.



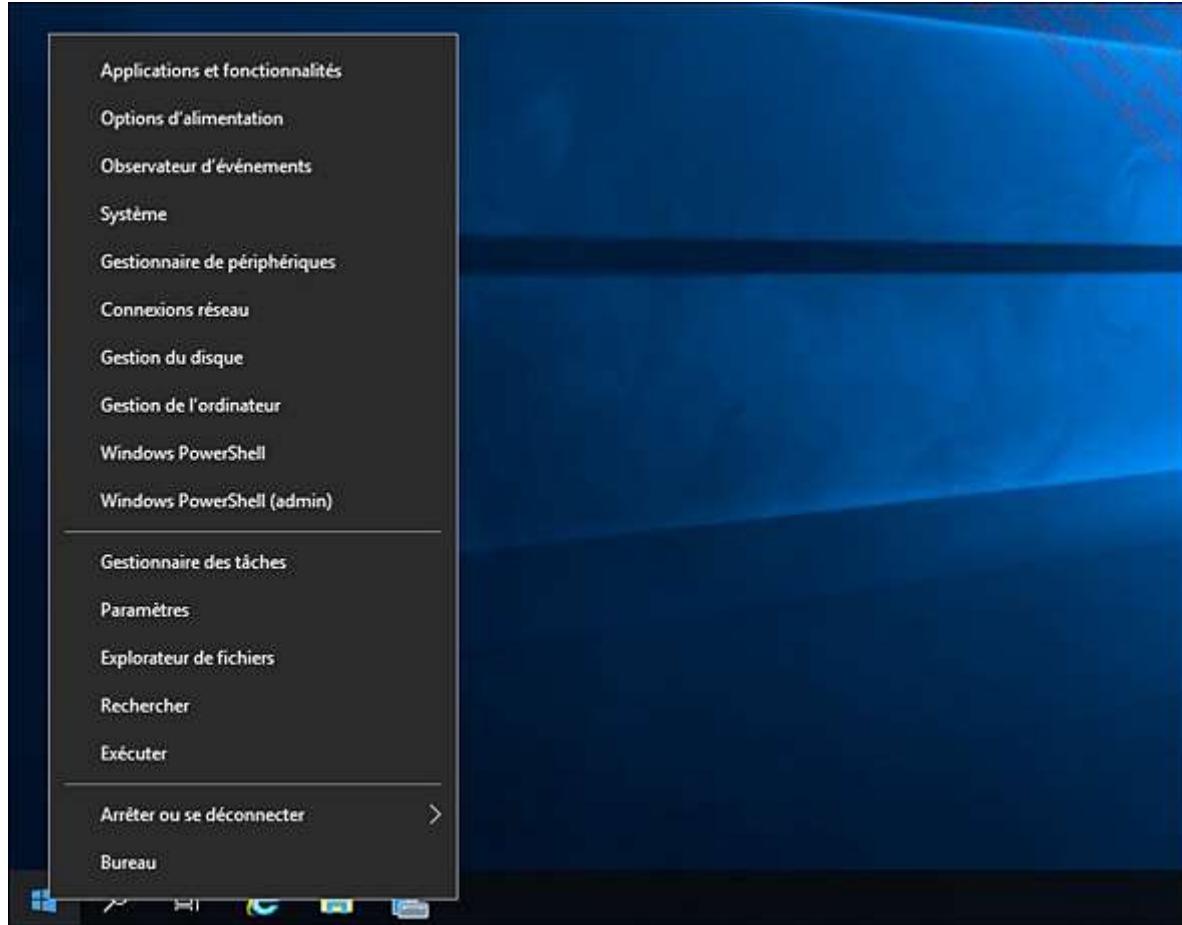
Cliquez trois fois sur le bouton **Suivant**. Dans **Services de rôle**, cochez les cases **Serveur de déploiement** et **Serveur de transport**.



Cliquez sur **Suivant** puis sur le bouton **Installer** pour démarrer l'installation du rôle WDS.

Depuis Windows PowerShell

Sur le bureau du système Windows Server, cliquez avec le bouton droit sur **Démarrer**, puis choisissez **Windows PowerShell (admin)**.



Dans la fenêtre **Administrateur : Windows PowerShell**, saisissez la commande suivante et validez par [Entrée] :

```
Install-WindowsFeature -Name WDS -IncludeManagementTools
```

Vérifiez l'installation du rôle WDS à l'aide de la commande :

```
get-windowsfeature
```

A screenshot of a Windows PowerShell window titled "Administrateur : Windows PowerShell". The window shows the command "Install-WindowsFeature -Name WDS -IncludeManagementTools" being run, followed by the output which indicates success for the WDS role. Below this, the command "get-windowsfeature" is run, displaying a table of installed Windows features. The table has columns for Display Name, Name, and Install State. The "Install State" column shows "Installed" for RemoteAccess and DirectAccess-VPN, and "Available" for Web-Application-Proxy, Routing, DeviceHealthAttestation, Hyper-V, and Fax.

- À noter que vous ne pouvez pas installer les services WDS sur une version minimale (serveur Core) de Windows Server.

Après avoir installé le rôle WDS, il est nécessaire de le configurer. Nous allons supposer que le serveur Windows Server 2019 est membre d'un groupe de travail et qu'un serveur DHCP est disponible dans le réseau :

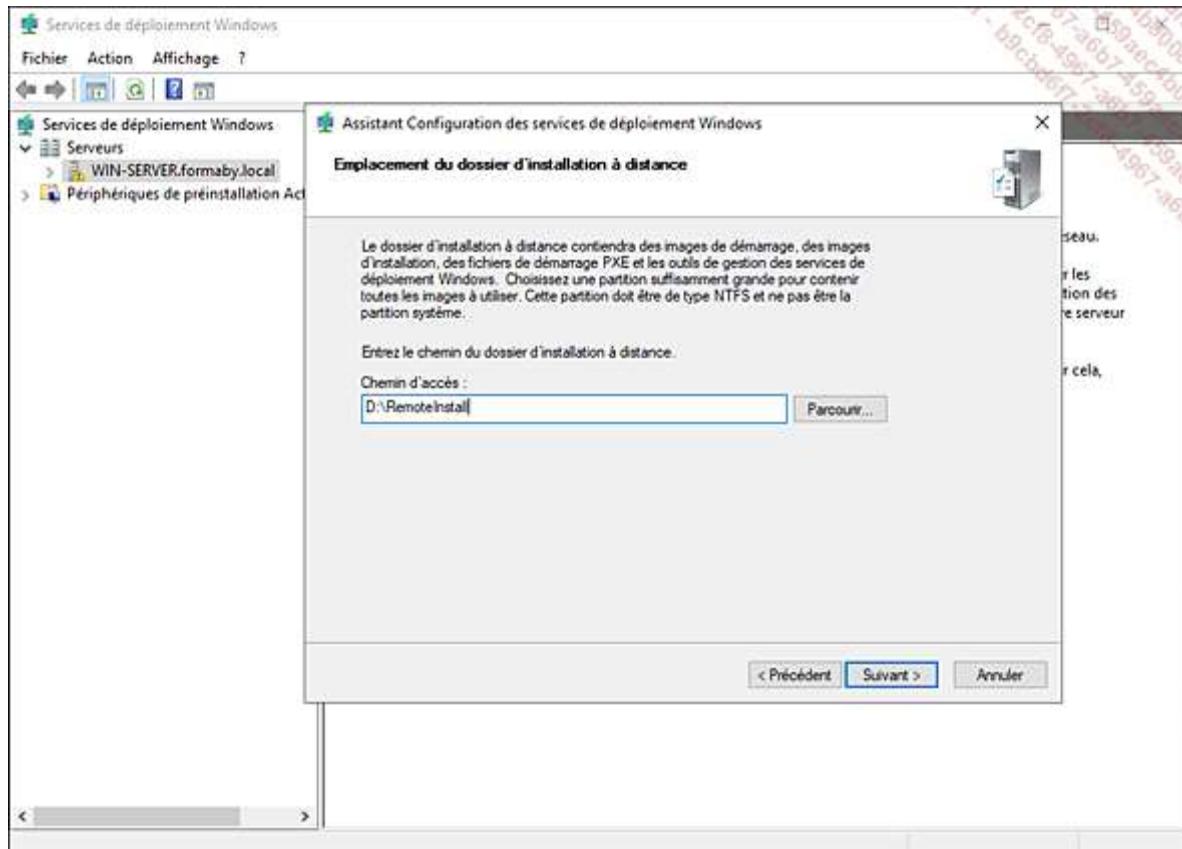
Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils** puis sur **Services de déploiement Windows**.

Développez le nœud **Serveurs**, puis cliquez avec le bouton droit sur le nom de votre serveur et choisissez **Configurer le serveur**.

Dans l'**Assistant Configuration des services de déploiement Windows**, cliquez sur le bouton **Suivant**.

Sélectionnez la case **Serveur autonome** puis **Suivant**.

Saisissez le chemin vers le dossier d'installation qui contiendra les images à déployer, idéalement stocké sur une partition NTFS distincte de la partition système Windows et cliquez sur **Suivant**.



Définissez ensuite la stratégie de réponse à adopter lorsque des clients contacteront le serveur WDS pour obtenir une image d'installation :

- Ne répondre à aucun ordinateur client (option cochée par défaut).
- Répondre uniquement aux ordinateurs clients connus.
- Répondre à tous les ordinateurs clients (connus et inconnus). Vous pouvez aussi exiger l'approbation de l'administrateur pour la validation des clients inconnus en cochant la case correspondante.

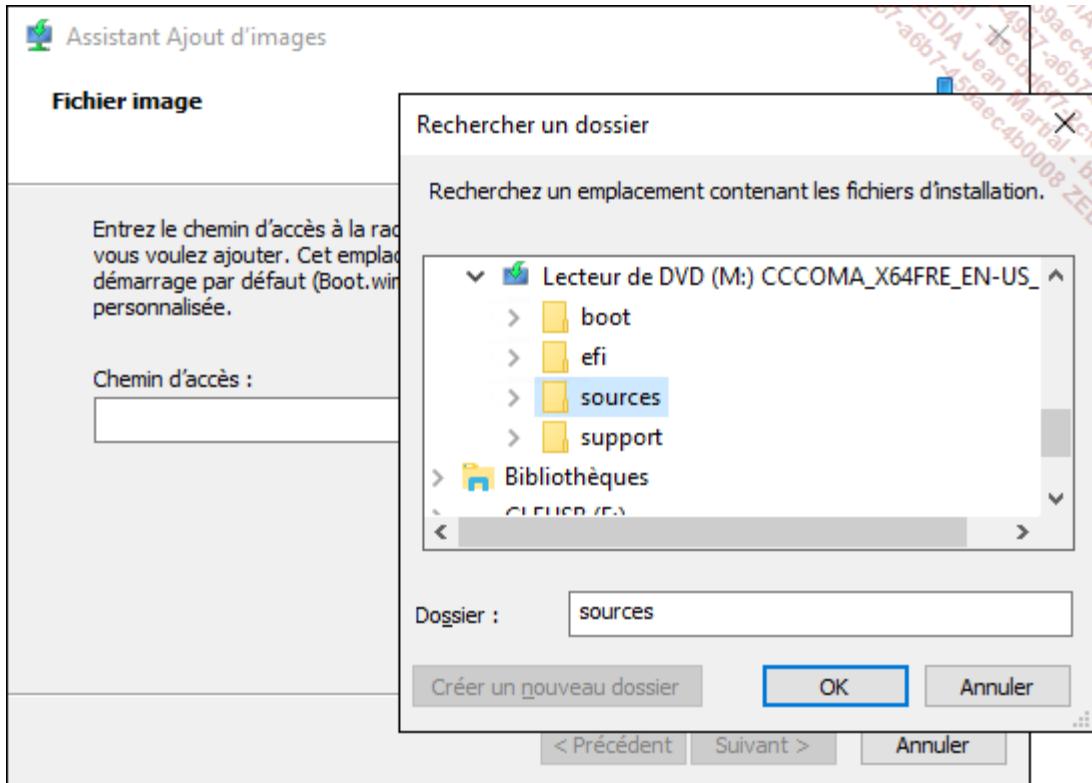
Cliquez sur le bouton **Suivant**.

Assurez-vous que la case **Ajouter les images au serveur maintenant** est cochée puis cliquez sur **Terminer**.

a. Ajout d'images de démarrage et d'installation

Nous allons maintenant ajouter les images de démarrage et d'installation de Windows 11 sur le serveur WDS. L'image de démarrage contient l'environnement de préinstallation Windows PE avec lequel vous allez démarrez votre client avant d'installer le système d'exploitation final. Elle se nomme **boot.wim** et se trouve dans le répertoire **Sources** du DVD d'installation de Windows 11. L'image d'installation est, elle, contenue dans le fichier **install.wim** du même répertoire **Sources**.

Dans l'**Assistant Ajout d'images**, cliquez sur le bouton **Parcourir** puis sélectionnez le dossier **Sources** du DVD d'installation Windows 11 et cliquez sur **Suivant**. Il contient les fichiers **boot.wim** et **install.wim**.



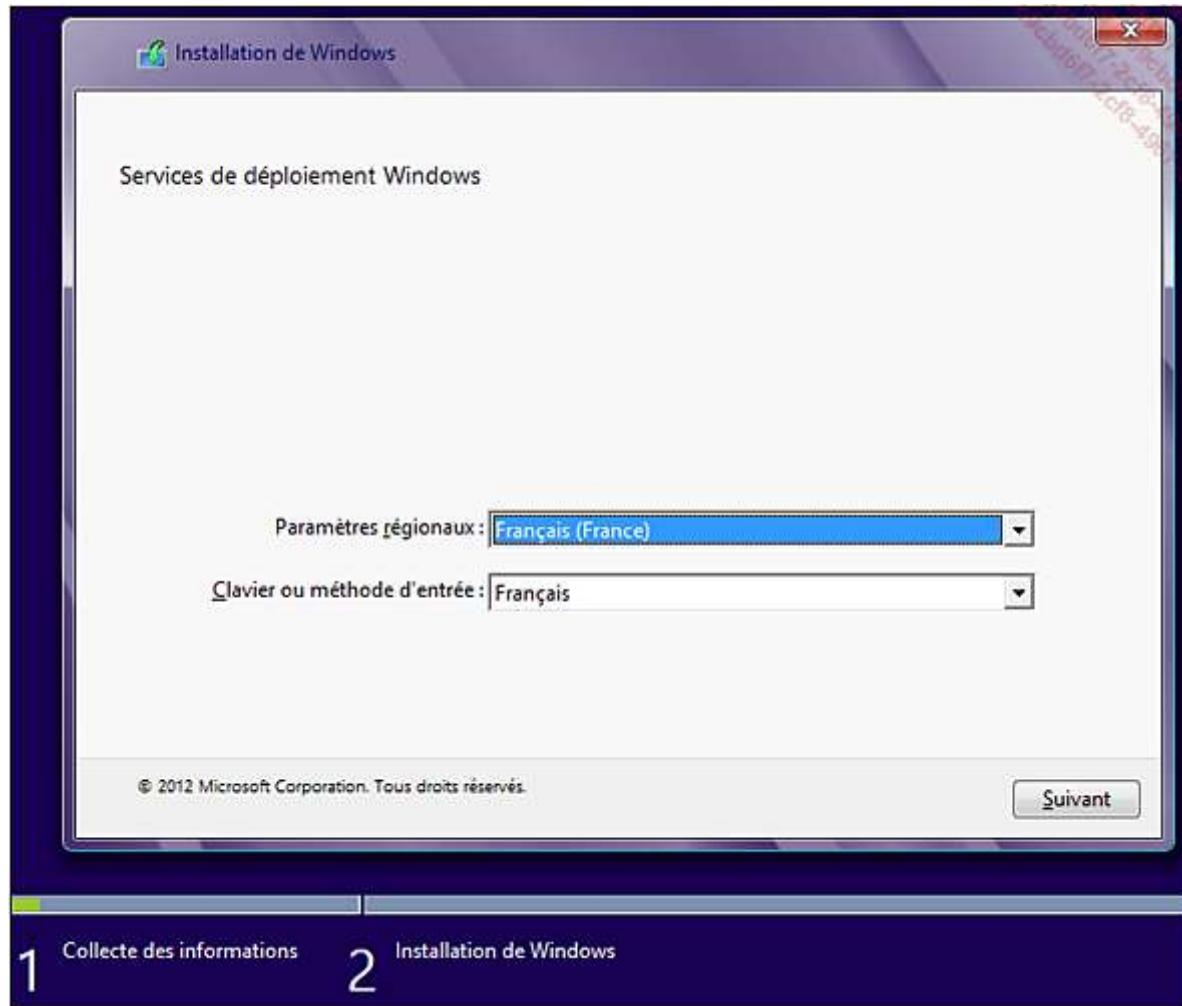
Saisissez **Windows 11** dans le champ **Créer un groupe d'images nommé** puis validez en cliquant sur **Suivant**. L'assistant importe l'image de démarrage et les images d'installation contenues dans le DVD d'installation. Cliquez sur le bouton **Terminer**.

- Il est nécessaire de posséder une image de démarrage par architecture matérielle (ARM, 32 bits/x86 ou 64 bits/x64 avec ou sans la technologie UEFI), car vous ne pourrez pas démarrer un ordinateur 32 bits depuis une image Windows PE 64 bits, même si l'inverse est possible.

Les nœuds **Images d'installation** et **Images de démarrage** de la console Services de déploiement Windows permettent d'ajouter des images d'autres systèmes d'exploitation, tels que Windows Server 2012 R2 ou Windows Server 2019.

- L'ajout d'une image d'installation dans WDS en ligne de commande est aussi possible à l'aide de la commande suivante : `WDSUTIL /Add-Image /ImageFile:"d:\sources\Install.wim" /ImageType:Install`

Pour permettre au poste cible de démarrer en mode PXE depuis sa carte réseau puis d'obtenir une adresse IP (*Internet Protocol*) fournie par le serveur WDS, et ainsi démarrer l'installation de Windows 11, il suffit généralement de presser la touche du clavier [F12] dès le démarrage de l'ordinateur :

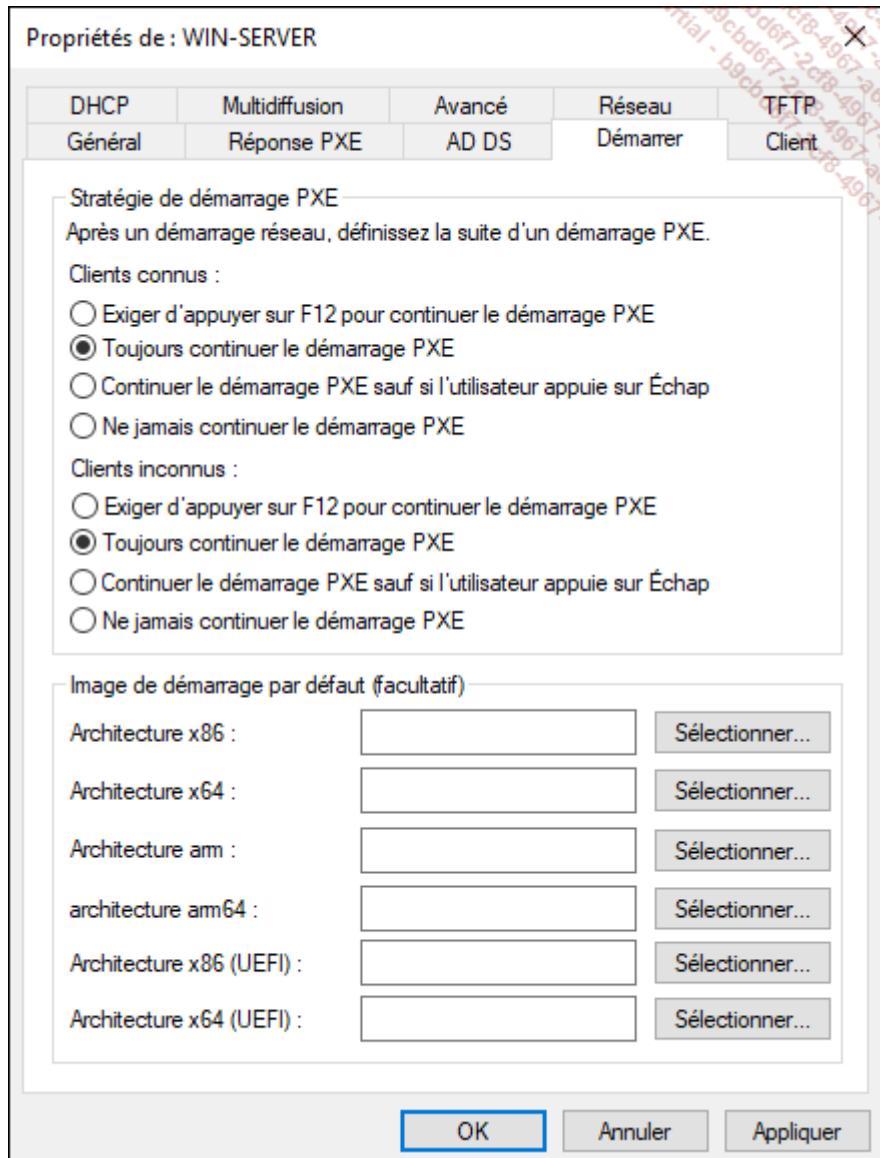


Vous pouvez éviter cette action en configurant la stratégie de démarrage PXE dans les propriétés du serveur WDS :

Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils** puis sur **Services de déploiement Windows**.

Développez le nœud **Serveurs**, puis cliquez avec le bouton droit sur le nom de votre serveur et choisissez **Propriétés**.

Cliquez sur l'onglet **Démarrer** et cochez la case **Toujours continuer le démarrage PXE** pour les clients connus et inconnus.



D'autres produits vous permettent de déployer des images par l'intermédiaire du réseau, comme **Microsoft MECM** (*Microsoft Endpoint Configuration Manager*). Celui-ci offre en outre une supervision centralisée du processus de déploiement, ainsi qu'un outil de séquencement des tâches permettant de définir des actions pour automatiser l'intégralité du processus en le rendant entièrement silencieux.

b. Réveil d'un ordinateur

En prévision du déploiement d'une image, un ordinateur éteint peut être démarré à distance à l'aide d'un protocole standard Ethernet nommé **WOL** (*Wake on LAN*). La plupart des cartes mères récentes implémentent le composant nécessaire à ce démarrage, mais nécessitent parfois l'activation de cette fonction dans le BIOS, comme le montre l'image ci-dessous (paramètres **Power On By PCI Devices** et **Power On By PCIE Devices**) :



Dans certains cas, l'activation de la fonctionnalité WOL sera requise depuis Windows 11, dans les propriétés de la carte réseau.

La carte réseau reçoit un paquet magique (*Magic Packet*) spécialement conçu à travers le protocole UDP (*User Datagram Protocol*) et démarre normalement l'ordinateur sans qu'aucune intervention ne soit nécessaire.

- En configurant le routeur de votre réseau local pour qu'il redirige le paquet magique (ports 7 ou 9) vers l'ordinateur cible, vous pourrez démarrer un client Windows 11 depuis Internet.

c. Multidiffusion

Le serveur WDS permet d'optimiser le déploiement du client Windows 11 grâce à la technologie de multidiffusion. Le transfert des images WIM déconnectera les ordinateurs lents et séparera les transmissions en plusieurs flux en fonction de leur vitesse.

Windows Server 2019 apporte son lot de fonctionnalités dans la gestion de la multidiffusion :

- Support du protocole TFTP et de flux multidiffusion dans un réseau IPv6 (*Internet Protocol Version 6*), cf. chapitre Connectivité réseau, section Protocoles IPv4 et IPv6.
- Amélioration du déploiement d'une image d'installation en supprimant la nécessité de créer une copie locale complète du fichier install.wim pour démarrer l'installation.
- Prise en charge des images d'installation et de démarrage avec UEFI (*Unified Extensible Firmware Interface*), successeur du BIOS pour les ordinateurs avec une architecture Itanium ou 64 bits.
- Transmission des données et des images par multidiffusion sur un serveur autonome en incluant un fournisseur PXE pour le démarrage des clients.

Avant de créer une transmission par multidiffusion, il est nécessaire de créer une stratégie de transfert sur le serveur WDS. Vous avez le choix entre quatre paramètres :

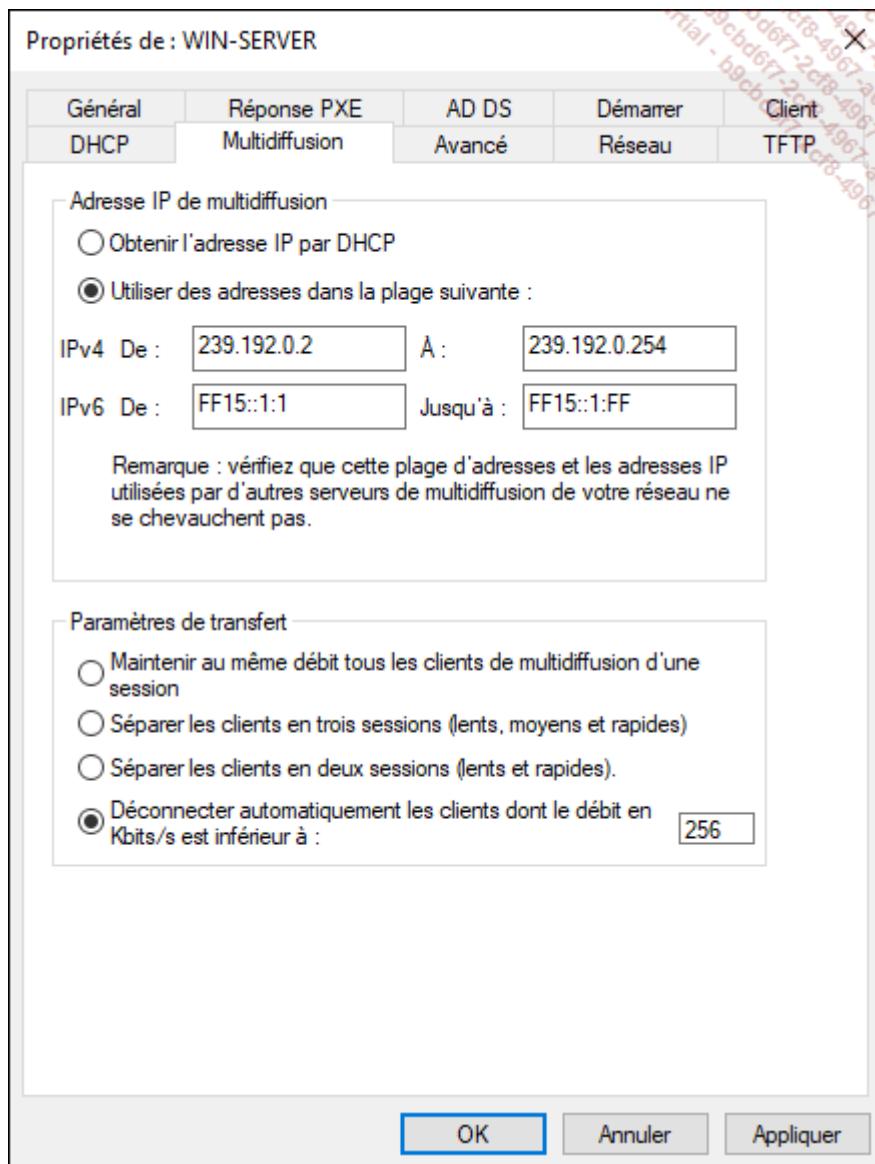
- Maintenir au même débit tous les clients de multidiffusion d'une session : quelle que soit la vitesse du client, le flux unique sera le même pour tous.
- Séparer les clients en trois sessions (lents, moyens et rapides).
- Séparer les clients en deux sessions (lents et rapides).
- Déconnecter automatiquement les clients dont le débit en Kbits/s est inférieur à 256 (valeur par défaut).

La procédure est la suivante :

Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils** puis sur **Services de déploiement Windows**.

Développez le nœud **Serveurs**, puis cliquez avec le bouton droit sur le nom de votre serveur et choisissez **Propriétés**.

Cliquez sur l'onglet **Multidiffusion** et définissez les paramètres de transfert.



- Dans le même onglet, vous pouvez aussi définir une plage d'adresses IP à attribuer aux clients qui se connecteront au serveur WDS, ou bien utiliser une adresse IP fournie par le DHCP faisant autorité dans votre réseau.

La stratégie de transfert définie, un assistant vous aide à la création d'une transmission par multidiffusion d'une image. Elle sera transmise une seule fois, plutôt qu'une par client, ce qui augmenterait la bande passante nécessaire.

Deux méthodes permettent de définir les réponses du serveur WDS à l'initiation d'une méthode de multidiffusion :

- Diffusion automatique : dès qu'un client en fait la demande, il reçoit une image d'installation. Si d'autres systèmes font la demande, après le premier client, ils rejoignent la transmission commencée.
- Diffusion planifiée : à partir d'un nombre de clients défini et/ou d'une date et d'une heure planifiée, l'image est transférée en multidiffusion. Si vous ne spécifiez pas de valeur, vous devrez démarrer le transfert manuellement en cliquant avec le bouton droit sur la transmission puis sur **Démarrer**.

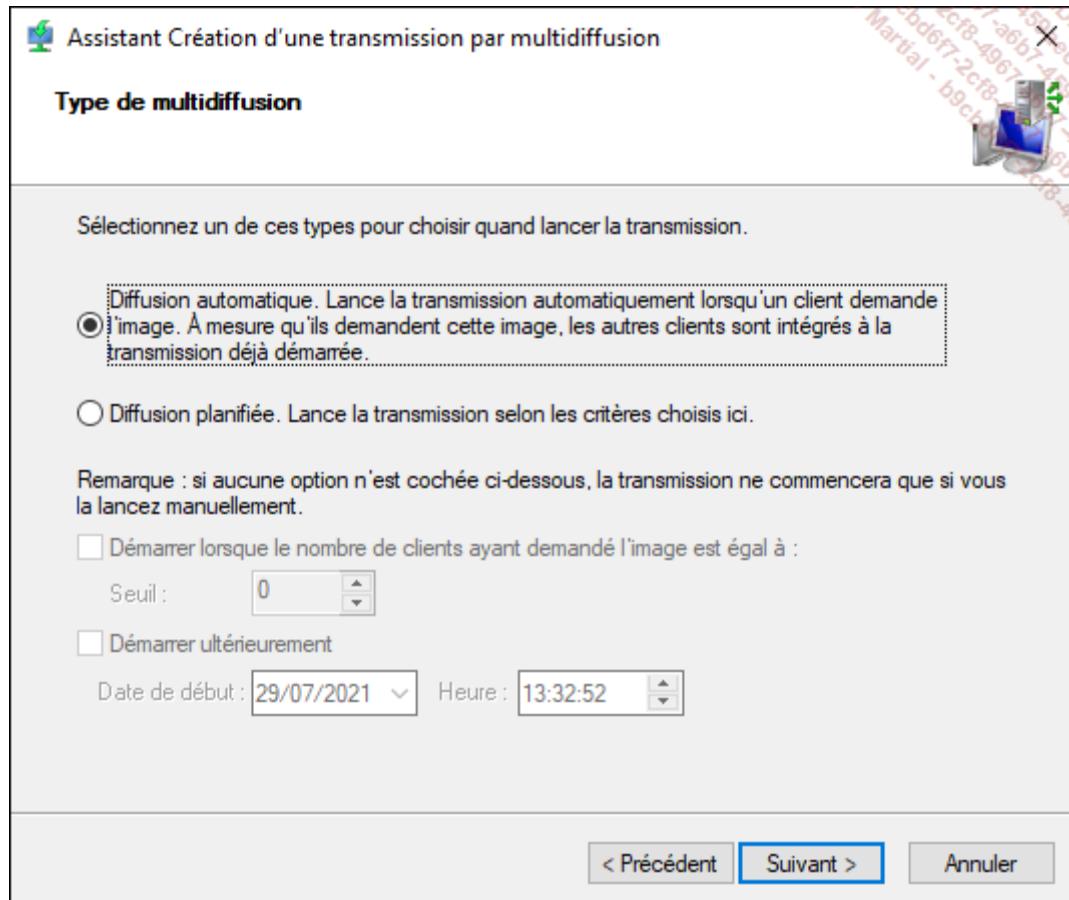
Pour créer une transmission par multidiffusion dans la console **Services de déploiement Windows** :

Effectuez un clic droit sur **Transmission par multidiffusion**, puis cliquez sur **Créer une transmission par multidiffusion**.

Nommez votre multidiffusion puis cliquez sur le bouton **Suivant**.

Selectionnez le groupe d'images contenant le fichier **install.wim** concernées par la transmission par multidiffusion, puis l'image à diffuser et cliquez sur le bouton **Suivant**.

Selectionnez une méthode de diffusion : **Diffusion automatique** ou **Diffusion planifiée**.



Cliquez sur le bouton **Suivant**, puis **Terminer**.

La création d'une transmission par multidiffusion automatique est aussi possible en ligne de commande à l'aide de la commande `wdsutil`, en utilisant des priviléges élevés :

```
wdsutil /New-MulticastTransmission /FriendlyName:"WDS pour poste  
Windows 11" /Image:"NomImageNoeudInstallation" /ImageType:install  
/TransmissionType:AutoCast
```

d. Installation sans surveillance

Le processus d'installation de Windows 11 peut être entièrement automatisé à l'aide d'un fichier au format standard XML (*eXtensible Markup Language*), nommé **autounattend.xml**. Celui-ci stocke les réponses nécessaires aux boîtes de dialogue qui proposent par exemple de créer une partition ou de choisir une langue d'installation.

Ainsi, il suffira à l'utilisateur de démarrer l'ordinateur depuis le DVD Windows 11, et d'insérer une clé USB contenant sur sa racine le fichier `autounattend.xml` pour que l'installation se déroule seule sans aucune intervention de l'utilisateur.

Les services WDS permettent aussi de déployer une image WIM de manière automatisée, en attribuant le fichier de réponses cible à celle-ci et en le transférant par le réseau.

Comme le format du fichier de réponses est au format XML, il est possible de le modifier à l'aide d'un simple éditeur de texte. Le Windows System Image Manager (**Windows SIM**) fourni avec le kit ADK (sous la fonctionnalité **Outils de déploiement**), offre une interface graphique et surtout un vérificateur de syntaxe, proposant ainsi une méthode simple de création d'un fichier de réponses.

Avant de créer le fichier autounattend.xml, il est préférable d'ouvrir l'image (install.wim) sur laquelle nous souhaitons travailler, afin que le fichier de réponses soit configuré avec l'ensemble des fonctionnalités disponibles. Un fichier de catalogue possédant l'extension .clg sera généré, contenant l'état de tous les paramètres et les packages d'une image Windows.

La génération d'un fichier de réponses s'effectue en trois étapes :

1. Crédation de la structure vierge du fichier de réponses après avoir ajouté une image WIM à traiter.
2. Ajout et configuration des paramètres (composants) à automatiser dans le fichier de réponses.
3. Vérification du fichier généré à l'aide de l'outil **Valider le fichier de réponses**.

Première étape : création du fichier de réponses

Il faut un ordinateur avec le kit Windows ADK installé et disposant de l'image install.wim. L'outil doit posséder un accès en lecture/écriture à ce fichier.

Dans cette étape, nous allons créer un fichier de réponses vierge, et un fichier de catalogue associé à l'image de base.

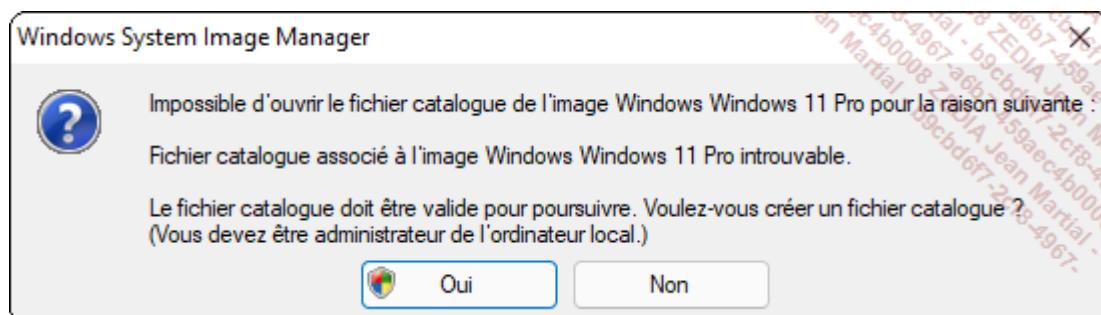
Ouvrez une session sur l'ordinateur Windows 11 pourvu du kit ADK. Cliquez sur le menu **Démarrer** et cherchez **Windows System Image Manager**. Dans le menu **Fichier**, cliquez sur **Sélectionner l'image Windows**.

Sélectionnez le fichier **install.wim** que vous aurez préalablement copié du DVD d'installation Windows 11 vers un répertoire local.

Sélectionnez éventuellement une des images parmi celles proposées dans ce fichier et validez en cliquant sur le bouton **Ouvrir**.

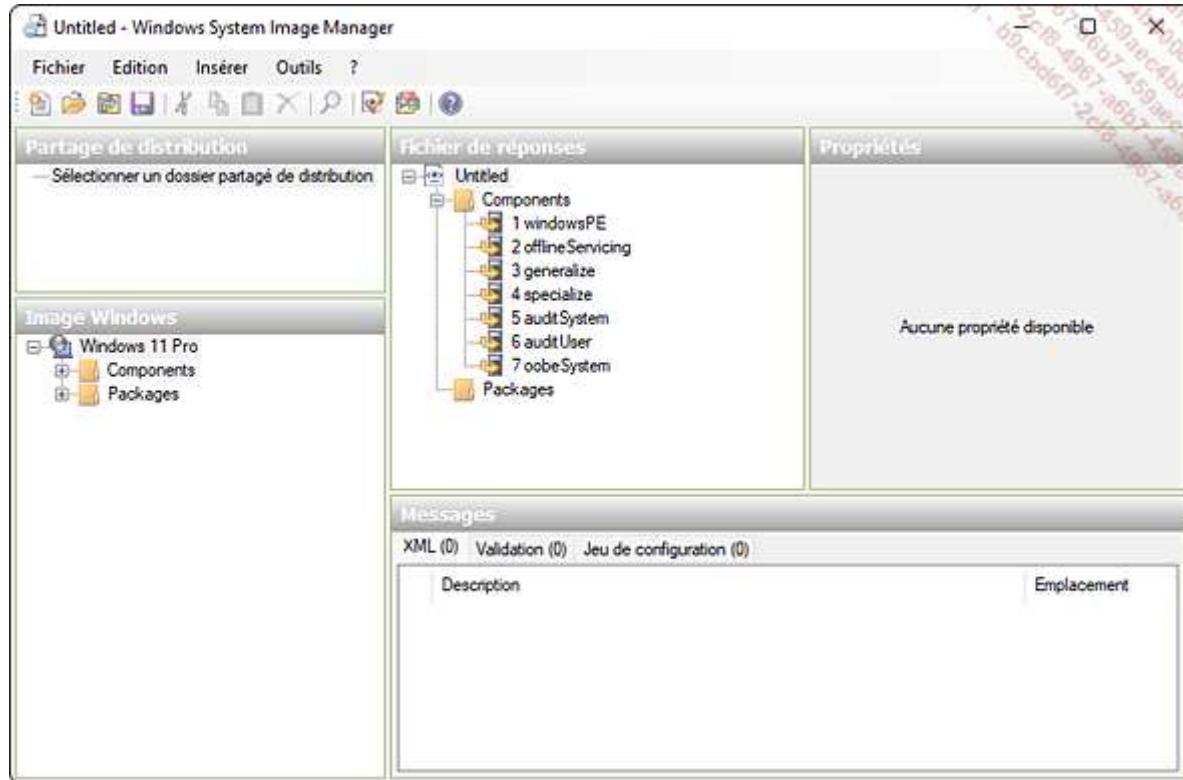
Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

- Un message peut apparaître, mentionnant que le fichier catalogue est manquant : validez sa création en cliquant sur le bouton **Oui**.



Si vous avez une erreur du type « Windows was unable to generate a catalog », tentez de résoudre le problème en installant la version française d'ADK.

Patiencez quelques minutes, puis, dans le menu **Fichier**, cliquez sur **Nouveau fichier de réponses**. Le fichier de réponses contenant les sept étapes de configuration est généré, comme le montre l'image ci-dessous :



Seconde étape : ajout des étapes d'installation à automatiser

Les sept étapes de configuration reflètent les phases d'une installation de Windows 11. Ces paramètres d'installation sans assistance de Windows peuvent être appliqués dans une ou plusieurs étapes de configuration, selon le composant sélectionné :

1. **Windows PE** : cette étape est appliquée lorsque l'installation de Windows est exécutée depuis l'environnement Windows PE.
2. **Offline Servicing** : ce module correspond à l'application des mises à jour, des pilotes de périphériques ou des modules linguistiques.
3. **Generalize** : les informations spécifiques à l'ordinateur, telles que le SID de sécurité, sont supprimées de l'installation Windows pour que l'administrateur puisse capturer l'image (commande sysprep /generalize).
4. **Specialize** : lors du premier démarrage de Windows 11, cette étape configure les paramètres du réseau et internationaux, ainsi que la jonction à un domaine Microsoft.
5. **Audit System** : si l'ordinateur est démarré en mode audit (commande sysprep /audit) des étapes supplémentaires sont disponibles, comme l'installation des pilotes de périphériques tiers.
6. **Audit User** : cette étape de configuration gère les paramètres d'installation suite à l'ouverture d'une session utilisateur en mode audit.
7. **Oobe System** : avant les écrans d'accueil, cette étape sert à créer des comptes d'utilisateurs locaux et à définir des paramètres linguistiques et régionaux.

Au cours de cette étape, nous allons définir les paramètres suivants dans le fichier de réponses :

- Création d'une partition disposant de 64 Go sur le disque dur primaire.
- Acceptation des conditions d'utilisation (licence) et insertion de la clé du produit Windows 11.

Voici la procédure :

Dans le volet **Image Windows** du **Gestionnaire d'images système Windows**, développez le nœud **Composants** pour afficher les paramètres disponibles.

Ajoutez les composants suivants à votre fichier de réponses en cliquant avec le bouton droit sur le composant, puis en sélectionnant l'étape de configuration appropriée et complétez les champs **Paramètres** du cadre **Propriétés** :

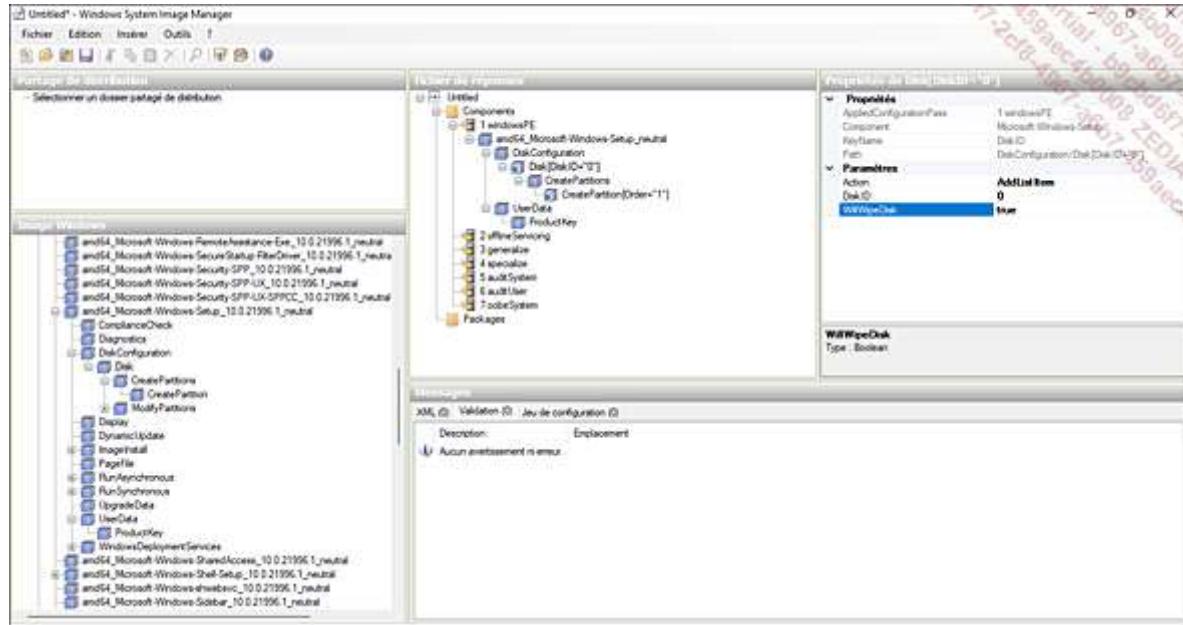
Configuration de la partition d'installation :

amd64_Microsoft-Windows-Setup_10.0.21996.1_neutral DiskConfiguration\Disk\ CreatePartitions\CreatePartition ajouter le paramètre à la passe 1 windowsPE	\ Extend = false Order = 1 Size = 64000 Type = Primary (notez la présence du paramètre EFI)
amd64_Microsoft-Windows-Setup_10.0.21996.1_neutral DiskConfiguration \Disk ajouter le paramètre à la passe 1 windowsPE	DiskID = 0 WillWipeDisk = true

Acceptation de la licence EULA et insertion de la clé produit :

amd64_Microsoft-Windows-Setup_10.0.21996.1_neutral \UserData ajouter le paramètre à la passe 1 windowsPE	AcceptEula = true	L'image ci-dessous montre la
amd64_Microsoft-Windows-Setup_10.0.21996.1_neutral \UserData\ProductKey ajouter le paramètre à la passe 1 windowsPE	Key = Votrecléduproduit	

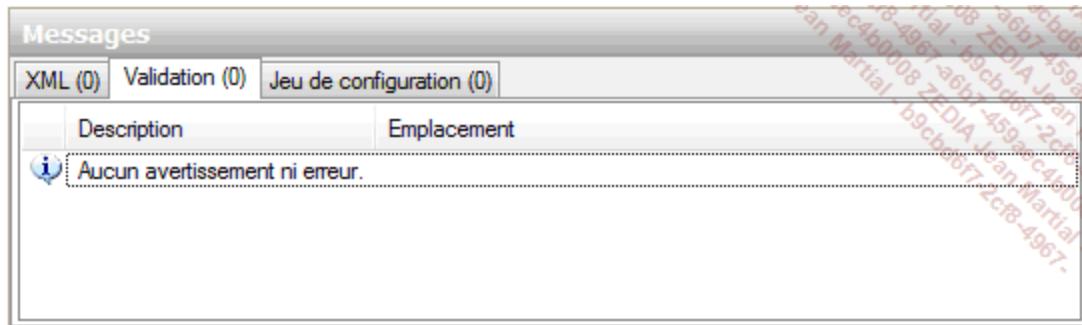
modification du paramètre de création d'une partition :



Pour plus d'informations sur les nombreux paramètres des fichiers de réponses, consultez les informations techniques à l'adresse : <https://docs.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/automate-windows-setup>

La dernière étape consiste à vérifier la cohérence du fichier de réponses, au niveau des paramètres et de sa syntaxe. Dans le menu **Outils**, cliquez sur **Valider le fichier de réponses**.

Vérifiez les remontées d'avertissement ou d'erreur dans le volet **Messages**, onglet **Validation**, comme le montre l'image ci-dessous :



Pour terminer la création du fichier de réponses, il faut l'enregistrer à la racine d'un média amovible USB ou le stocker dans le dossier RemoteInstall situé sur le serveur WDS.

Dans le menu **Fichier** du **Gestionnaire d'images système Windows**, cliquez sur **Enregistrer le fichier de réponses sous** et spécifiez l'emplacement de stockage et le nom du fichier (**autounattend.xml**).

- Un fichier de réponses nommé oobe.xml permet quant à lui de personnaliser l'écran d'accueil de Windows qui apparaît lors du premier démarrage du système.

Pour tester l'installation silencieuse, il est nécessaire de démarrer un ordinateur à l'aide du DVD Windows 11 et de brancher un disque mémoire flash USB dans le groupe principal des ports USB. La racine doit contenir le fichier autounattend.xml. Le programme d'installation recherchera automatiquement ce fichier et le traitera.

Il est bien entendu possible d'assigner à un serveur WDS un fichier de réponses pour le démarrage (boot.wim) et pour l'installation (install.wim) de Windows 11, comme nous le verrons juste après.

Voici le fichier de réponses généré à partir des informations saisies précédemment (mentionnées en gras ci-dessous) :

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="windowsPE">
        <component name="Microsoft-Windows-Setup">
            processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
            language="neutral" versionScope="nonSxS" xmlns:wcm=
                "http://schemas.microsoft.com/WMIConfig/2002/State"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                <DiskConfiguration>
                    <Disk wcm:action="add">
                        <CreatePartitions>
                            <CreatePartition wcm:action="add">
                                <Size>64000</Size>
                                <Type>Primary</Type>
                                <Order>1</Order>
                            </CreatePartition>
                        </CreatePartitions>
                    </DiskConfiguration>
                </Disk>
            </component>
        </settings>
    </unattend>
```

```

<DiskID>0</DiskID>
<WillWipeDisk>true</WillWipeDisk>
</Disk>
</DiskConfiguration>
<UserData>
<ProductKey>
<Key>azertyuiopmlkjhgfdssqwxcb</Key>
</ProductKey>
<AcceptEula>true</AcceptEula>
</UserData>
</component>
</settings>
<cpi:offlineImage cpi:source="wim:c:/temp/install_11en.wim#
Windows 10 Home" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
```

- Notez que dans notre exemple, le paramètre WillWipeDisk avec la valeur true spécifie que le disque principal sera effacé avant la création de la nouvelle partition.

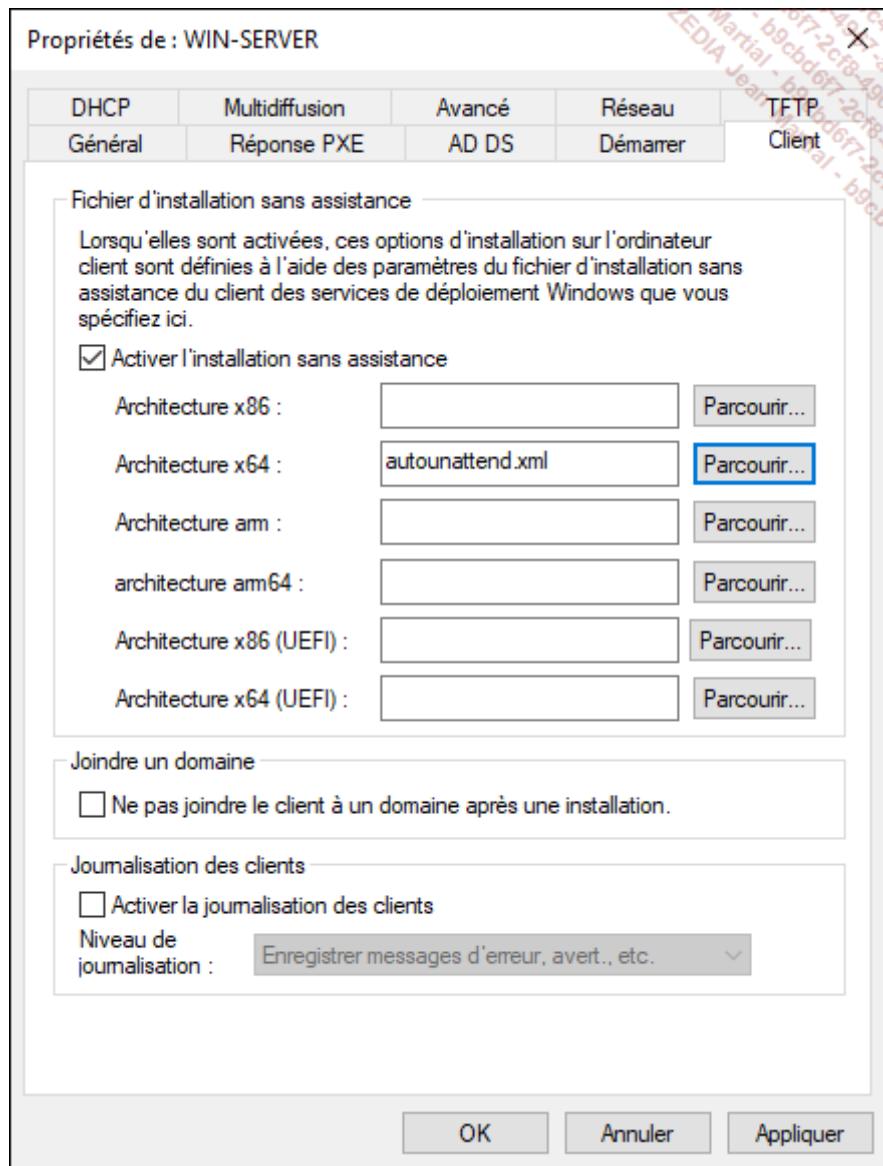
Deux fichiers de réponses sont nécessaires lors de l'installation automatisée de Windows 11 : l'un complétant les étapes de Windows PE (boot.wim), l'autre complétant celles de l'installation de Windows 11 (install.wim).

Ces fichiers doivent être intégrés au serveur WDS et aux images à déployer :

Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Services de déploiement Windows**.

Développez le nœud **Serveurs**, puis cliquez avec le bouton droit sur le nom de votre serveur et choisissez **Propriétés**.

Cliquez sur l'onglet **Client** puis spécifiez un fichier d'installation XML en fonction de l'architecture de déploiement nécessaire au démarrage de Windows PE.



Validez en cliquant sur le bouton **Valider** puis **OK**.

Définissons maintenant un fichier de réponses pour l'image d'installation :

Déployez l'arborescence sous le nom de votre serveur WDS. Cliquez sur le nœud **Windows 11**.

Windows 11 - 14 image(s) d'installation						
Nom de l'image	Architecture	État	Taille décompressée	Date	Version du système	
Windows 11 Pro for Workstations	x64	En li...	14735 Mo	29/0...	10.0.21996	
Windows 11 Pro N for Workstations	x64	En li...	13753 Mo	29/0...	10.0.21996	
Windows 11 Famille	x64	En li...	17285 Mo	29/0...	10.0.22000	
Windows 11 Famille N	x64	En li...	16230 Mo	29/0...	10.0.22000	
Windows 11 Collaboration	x64	En li...	16993 Mo	29/0...	10.0.22000	
Windows 11 Home N	x64	En li...	13478 Mo	29/0...	10.0.21996	
Windows 11 Home Single Language	x64	En li...	14459 Mo	29/0...	10.0.21996	
Windows 11 Education	x64	En li...	14735 Mo	29/0...	10.0.21996	
Windows 11 Education N	x64	En li...	13753 Mo	29/0...	10.0.21996	
Windows 11 Pro	x64	En li...	14735 Mo	29/0...	10.0.21996	
Windows 11 Pro N	x64	En li...	13753 Mo	29/0...	10.0.21996	
Windows 11 Pro Education	x64	En li...	14735 Mo	29/0...	10.0.21996	
Windows 11 Pro Education N	x64	En li...	13753 Mo	29/0...	10.0.21996	
Windows 11 Home	x64	En li...	14459 Mo	29/0...	10.0.21996	

Cliquez avec le bouton droit sur l'image choisie et choisissez **Propriétés**.

Cochez la case **Autoriser l'image à s'installer en mode sans assistance** puis cliquez sur le bouton **Sélectionner un fichier**.

Choisissez le fichier d'installation sans assistance précédemment créé avec l'Assistant Gestion d'installation grâce au bouton **Parcourir** puis validez en cliquant sur le bouton **OK**.

2. Microsoft Deployment Toolkit

MDT (*Microsoft Deployment Toolkit*) est un ensemble d'outils gratuits permettant de déployer des images de postes de travail (Windows 7 et version supérieure), de serveurs (Windows Server 2008 R2 ou version supérieure) et d'applications (suite Office). MDT supporte la séparation de fichiers WIM dans des scénarios d'utilisation de BIOS UEFI.

L'outil peut être téléchargé en version 32 bits et 64 bits à l'adresse internet : <https://www.microsoft.com/en-us/download/details.aspx?id=54259>

Sa gestion s'effectue au travers d'une console MMC (*Microsoft Management Console*).

MDT supporte le déploiement partiellement automatisé et totalement automatisé (Zero Touch).

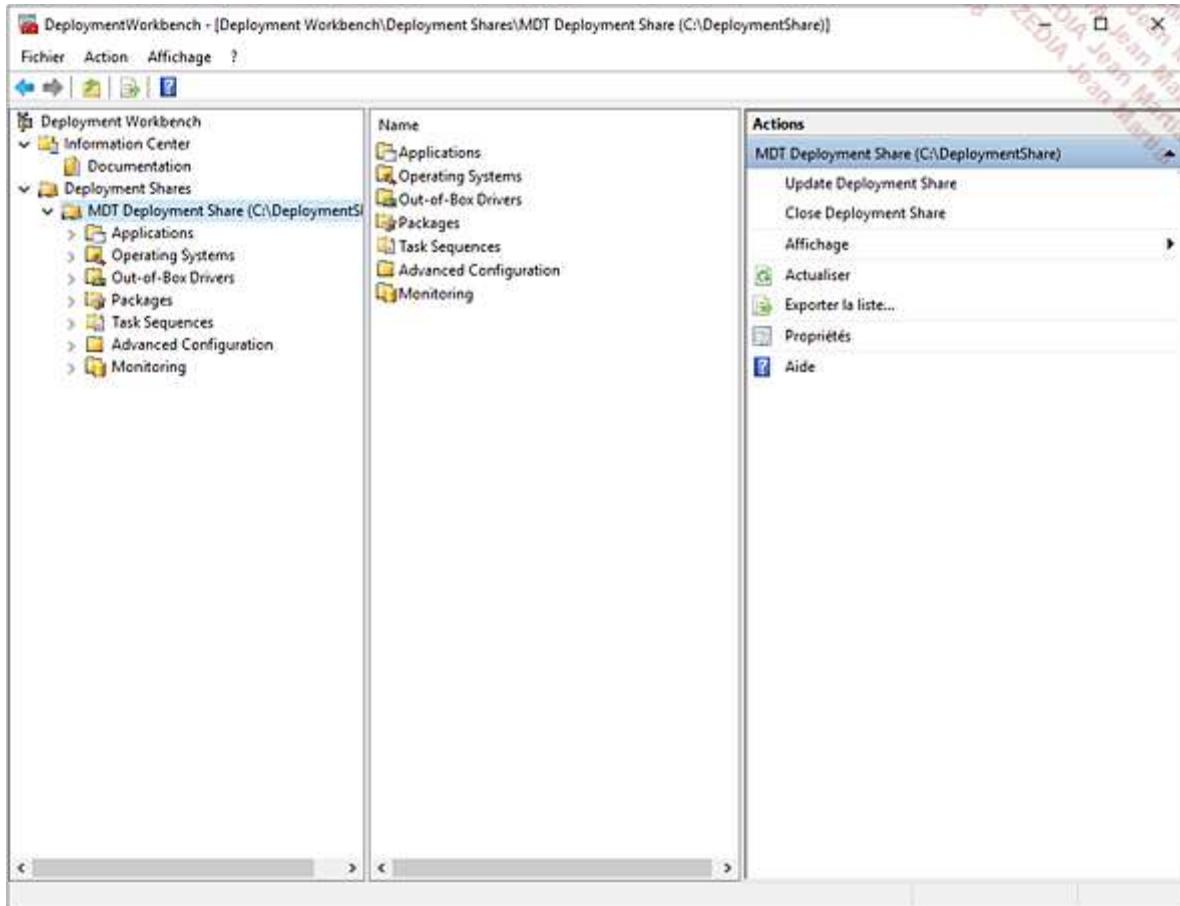
Bien que le produit existe uniquement en anglais, son principal avantage est qu'il peut être installé sur une version cliente de Microsoft Windows, au contraire du service WDS qui, lui, est tributaire d'une version serveur.

De plus, MDT gère les images au format ISO, le déploiement depuis un média amovible (clé USB, DVD...), le démarrage natif VHD, la gestion des architectures UEFI, l'automatisation de tâches grâce aux scripts PowerShell et l'installation d'une image sur une partition GPT.

Son fonctionnement est simple : l'utilisateur importe dans un premier temps les images et applications à déployer dans MDT, puis après avoir été configurées, les tâches et images de démarrage sont stockées sur un partage réseau caché (\$). Sur l'ordinateur de référence, le processus d'installation est exécuté en téléchargeant l'image

correspondante depuis le partage. Celle-ci est alors générée et importée une nouvelle fois dans MDT pour être partagée ensuite sur les ordinateurs cibles.

La première étape consiste à créer le partage qui contiendra les images, applications et pilotes à déployer, en cliquant avec le bouton droit sur **Deployment Shares** puis **New Deployment Share**.



Un autre avantage de MDT est la possibilité de déployer automatiquement des applications tierces non packagées, fournies par exemple sous forme de fichier exécutable (extension .exe), et ceci sur un nombre conséquent de postes de travail. Le produit est aussi capable de gérer les licences associées aux applications déployées.

3. Client Hyper-V

Comme Windows 10 avant lui, Windows 11 offre la possibilité d'utiliser une technologie de virtualisation nommée Hyper-V. Celle-ci consiste à exécuter un ou plusieurs systèmes d'exploitation invités sur le système hôte.

Apparu avec Windows Server 2008, Hyper-V permet par exemple aux développeurs d'utiliser plusieurs systèmes de test sur leur ordinateur physique, ceci sans coût matériel supplémentaire.

Les avantages liés à la virtualisation sont nombreux : la technologie est transparente pour l'utilisateur, les machines invitées peuvent utiliser des systèmes d'exploitation différents de l'hyperviseur, le matériel de ce dernier est pleinement exploité, les applications des machines virtuelles sont isolées complètement de l'hyperviseur et le déploiement d'un nouveau système est très simple.

Hyper-V procure le matériel virtuel et les fonctionnalités qui sont présentés à l'ordinateur virtuel grâce à un système de génération. Deux générations sont prises en charge : la génération 1 et la génération 2. Cette dernière propose un modèle de matériel virtuel simplifié et prend en charge le microprogramme UEFI (*Unified Extensible Firmware Interface*) plutôt que le microprogramme BIOS.

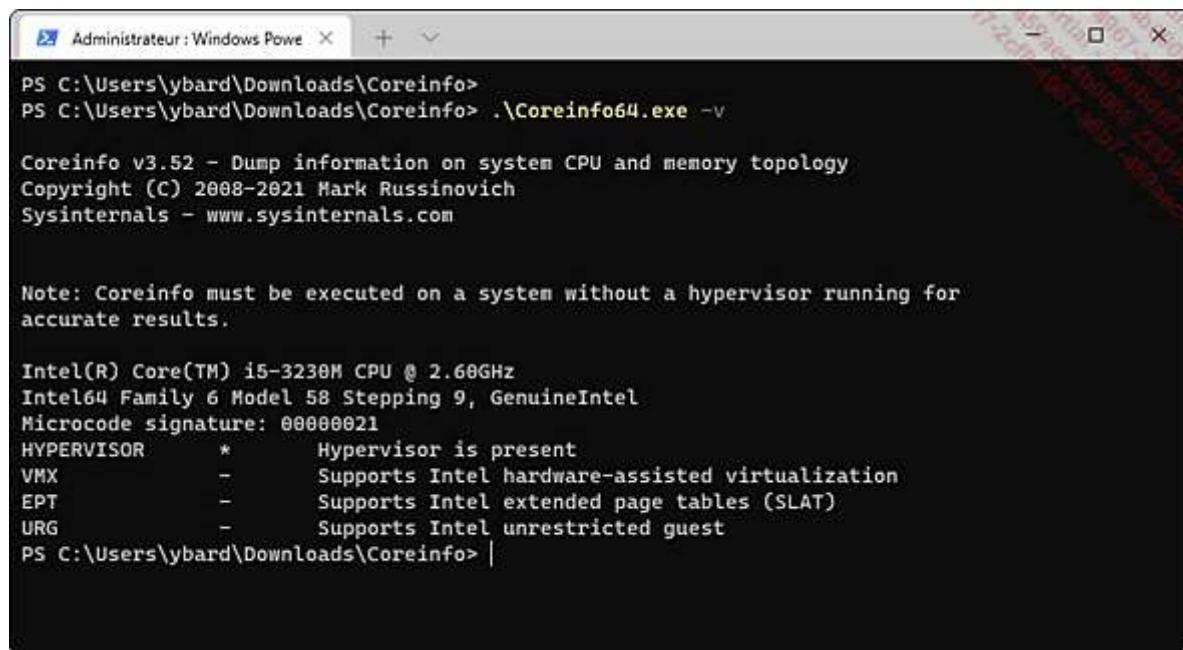
Tous les systèmes d'exploitation actuels supportés par Microsoft peuvent être pris en charge en tant qu'ordinateurs virtuels de génération 2.

La génération 2 propose les fonctionnalités ci-dessous sur une machine virtuelle :

- Démarrage PXE depuis une carte réseau standard.
- Démarrage à partir d'un disque dur ou DVD virtuel SCSI.
- Démarrage sécurisé.

Le client Hyper-V requiert une architecture 64 bits dotée de SLAT (*Second Level Address Translation*), généralement incluse sur les derniers processeurs Intel et AMD (*Advanced Micro Devices*), ainsi que la version 64 bits de Windows 11. Il est disponible avec les versions Windows 11 Professionnel, Windows 11 Education et Windows 11 Entreprise.

L'utilitaire en ligne de commande **coreinfo.exe**, téléchargeable depuis le site Microsoft Docs (<https://docs.microsoft.com/fr-fr/sysinternals/downloads/coreinfo>), permet de vérifier si on possède les prérequis matériels nécessaires. Depuis un Terminal, saisissez la commande suivante :



```
Administrator : Windows PowerShell
PS C:\Users\ybard\Downloads\Coreinfo>
PS C:\Users\ybard\Downloads\Coreinfo> .\Coreinfo64.exe -v

Coreinfo v3.52 - Dump information on system CPU and memory topology
Copyright (C) 2008-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

Note: Coreinfo must be executed on a system without a hypervisor running for
accurate results.

Intel(R) Core(TM) i5-3230M CPU @ 2.68GHz
Intel64 Family 6 Model 58 Stepping 9, GenuineIntel
Microcode signature: 00000021
HYPERVISOR * Hypervisor is present
VMX -
EPT -
URG -
PS C:\Users\ybard\Downloads\Coreinfo> |
```

Un tiret (-) signifie que la fonctionnalité est manquante. Une étoile * valide sa présence.

Au moins 2 Go de RAM supplémentaires sont nécessaires pour la création des ordinateurs virtuels 32 bits et 64 bits.

L'administrateur peut accéder à une machine virtuelle de deux façons :

- Console d'ordinateur virtuel (VMConnect) : visualisation de l'ordinateur virtuel sous forme de console. L'avantage non négligeable de cette méthode d'accès est la possibilité de voir le processus de démarrage de l'ordinateur invité.
- Bureau à distance : lorsque l'administrateur est connecté à l'ordinateur virtuel, il voit le bureau de celui-ci comme s'il était assis devant, en ayant accès à tous les programmes et documents stockés. Le système d'exploitation invité doit être complètement démarré pour pouvoir s'y connecter.

Le client Hyper-V supporte la fonctionnalité de déplacement de stockage dynamique, permettant de déplacer un système invité vers un autre support (disque local, périphérique USB, partage réseau) sans nécessité de l'arrêter.

Les captures instantanées enregistrent l'état complet de l'ordinateur afin de pouvoir le restaurer à un état antérieur, ce qui peut être utile lors d'une maintenance planifiée d'un serveur.

a. Installation d'Hyper-V

Pour installer Hyper-V, trois méthodes sont proposées, à exécuter en tant qu'administrateur du poste de travail Windows 11 :

Première méthode

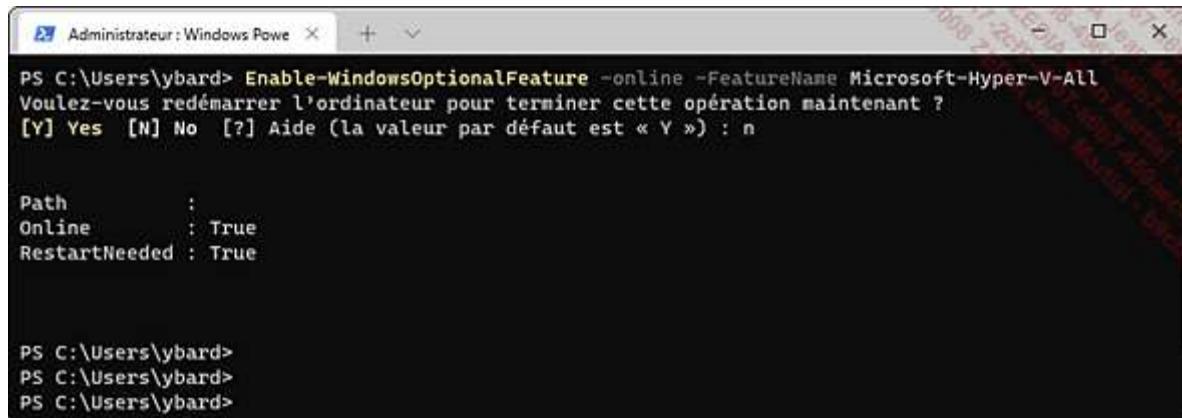
En ligne de commande Windows PowerShell : ce langage de script est à destination des administrateurs système (cf. chapitre Gestion des clients Windows, section Accès à distance) :

Après un clic droit sur le bouton **Démarrer**, cliquez sur **Terminal Windows (administrateur)**.

Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

Dans la fenêtre Windows PowerShell, saisissez la commande suivante : enable-windowsoptionalfeature -online -featurename microsoft-hyper-v-all puis validez par la touche [Entrée].

Voici le résultat :



```
PS C:\Users\ybard> Enable-WindowsOptionalFeature -online -FeatureName Microsoft-Hyper-V-All
Voulez-vous redémarrer l'ordinateur pour terminer cette opération maintenant ?
[Y] Yes [N] No [?] Aide (la valeur par défaut est « Y ») : n

Path      :
Online    : True
RestartNeeded : True

PS C:\Users\ybard>
PS C:\Users\ybard>
PS C:\Users\ybard>
```

Il est nécessaire de redémarrer l'ordinateur pour la prise en compte de l'installation du client Hyper-V.

Deuxième méthode

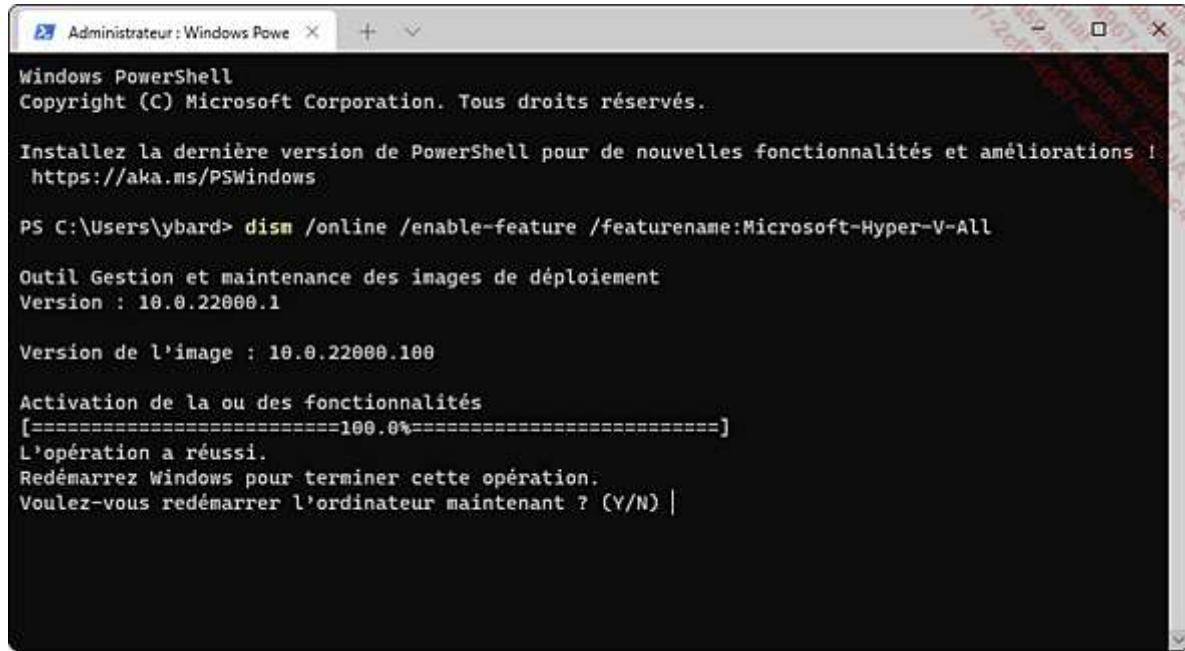
En ligne de commande avec l'utilitaire DISM (cf. Crédit d'une installation de référence dans ce chapitre).

Après un clic droit sur le bouton **Démarrer**, cliquez sur **Terminal Windows (administrateur)**.

Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

Dans la fenêtre Windows PowerShell, saisissez la commande suivante :

Dism /online /enable-feature /featurename:Microsoft-Hyper-V-All



```
Administrator : 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:\Users\ybard> dism /online /enable-feature /featurename:Microsoft-Hyper-V-All

Outil Gestion et maintenance des images de déploiement
Version : 10.0.22000.1

Version de l'image : 10.0.22000.100

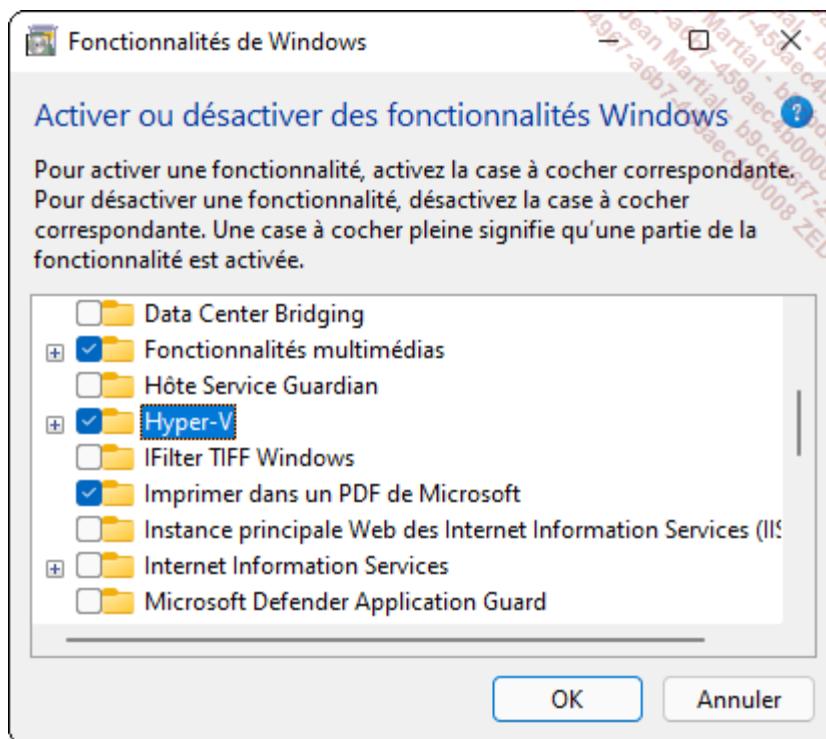
Activation de la ou des fonctionnalités
[=====100.0%=====]
L'opération a réussi.
Redémarrez Windows pour terminer cette opération.
Voulez-vous redémarrer l'ordinateur maintenant ? (Y/N) |
```

À l'invite, redémarrez votre ordinateur.

Troisième méthode

Ajout de la fonctionnalité Hyper-V à l'aide de l'interface graphique :

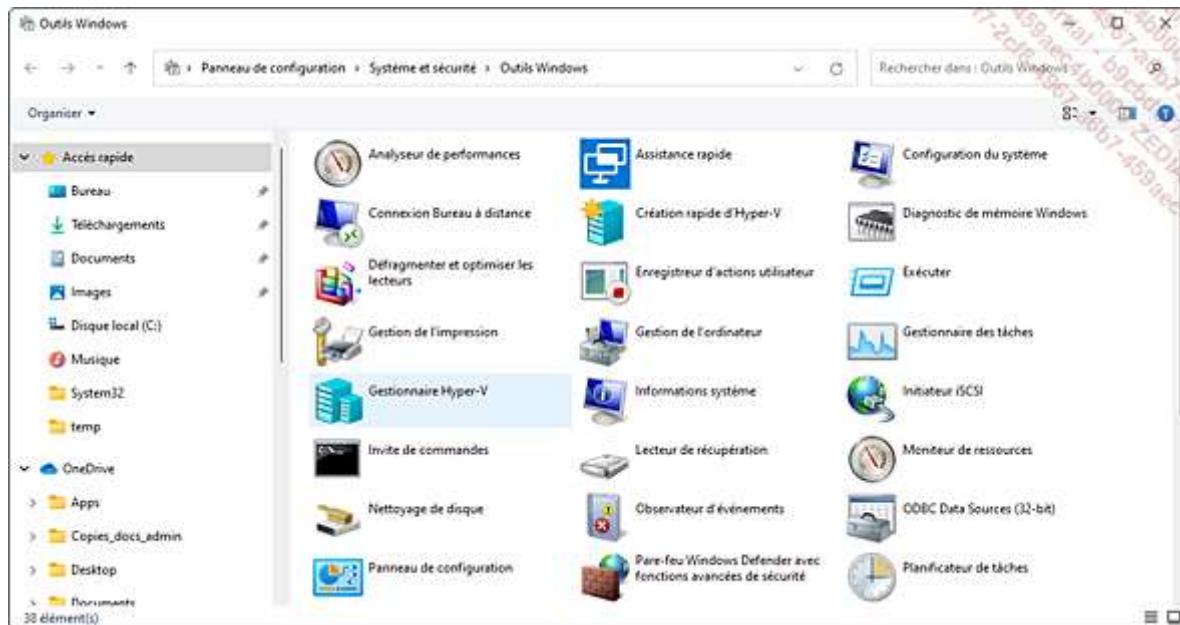
Dans la barre de recherche, saisissez **fonctionnalités** et cliquez sur le menu **Activer ou désactiver des fonctionnalités de Windows**. La fenêtre suivante apparaît :



Cochez la case **Hyper-V** et validez avec le bouton **OK**. La fonctionnalité est installée et la machine redémarre.

Cette fenêtre est également accessible depuis le **Panneau de configuration**, **Programmes** et **fonctionnalités** et **Activer ou désactiver des fonctionnalités Windows**.

Une fois la fonctionnalité Hyper-V installée, les outils d'administration contiennent le **Gestionnaire Hyper-V**. Pour y accéder, saisissez **hyper-V** dans le champ de recherche de la barre des tâches. Il est aussi tout à fait possible d'y accéder par le **Panneau de configuration**, en double cliquant sur **Système et sécurité** et enfin **Outils Windows**.



b. Création d'un ordinateur virtuel

Disposant d'un hyperviseur, commençons par créer un ordinateur virtuel afin d'y installer un système d'exploitation invité. Dans notre exemple, nous allons installer/virtualiser Windows 10 Entreprise pour une architecture 64 bits. Une version d'évaluation de 90 jours est disponible depuis le Centre d'évaluation Microsoft : <https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-10-enterprise>

- Windows 10 Entreprise (x64) nécessite au minimum un processeur de 2 GHz, 1 Go de RAM et un espace disque disponible de 32 Go.

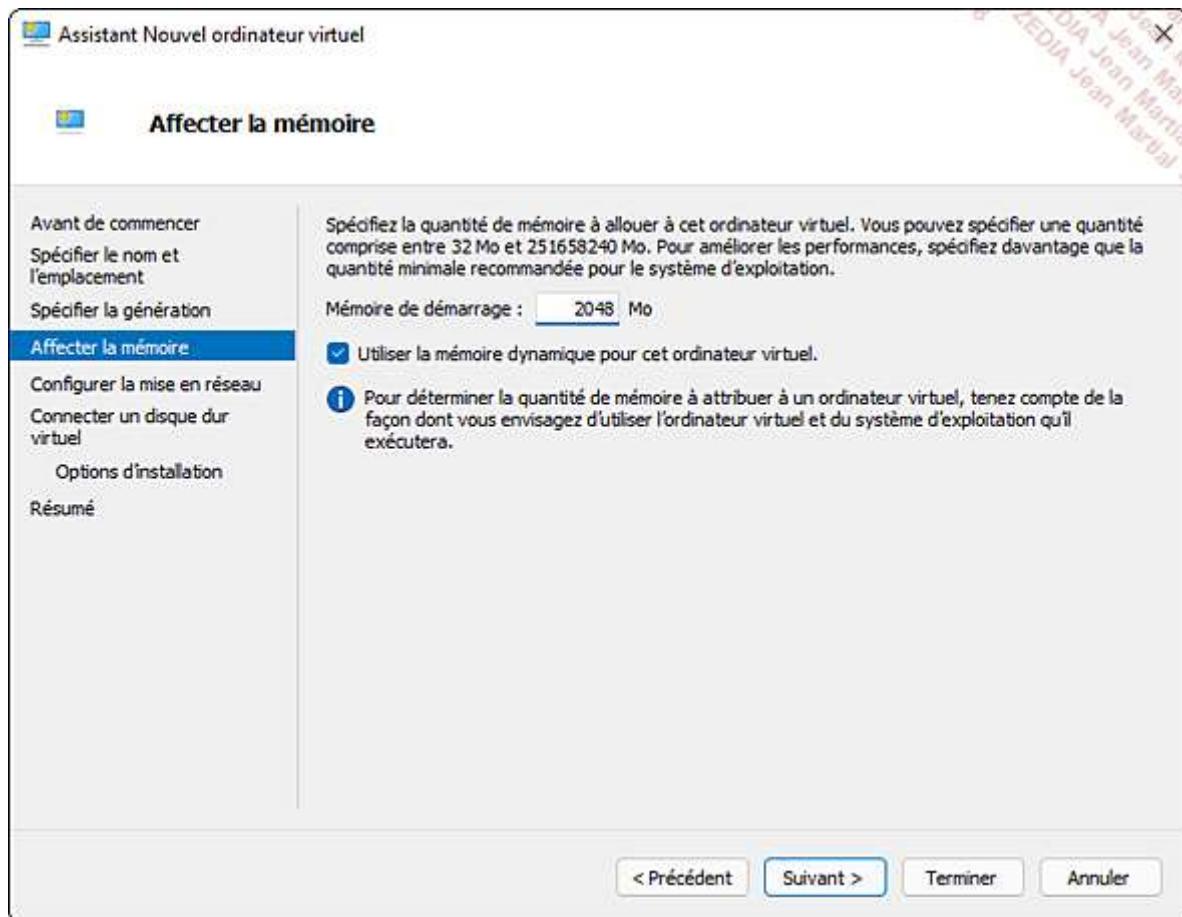
Une fois le fichier ISO contenant l'image de Windows 10 Entreprise téléchargé, cliquez sur **Gestionnaire Hyper-V** depuis les outils d'administration.

Dans la console **Gestionnaire Hyper-V**, sélectionnez le nom de votre ordinateur dans l'arborescence à gauche, et cliquez sur le menu **Action - Nouveau** puis sur **Ordinateur virtuel**.

Dans l'**Assistant Nouvel ordinateur virtuel**, cliquez sur le bouton **Suivant**. Dans le champ **Nom**, nommez l'ordinateur virtuel **Client Windows 10**. Si nécessaire, cochez la case **Stocker l'ordinateur virtuel à un autre emplacement** puis cliquez sur **Parcourir** et sélectionnez un dossier de stockage. Par défaut, l'emplacement de stockage de l'ordinateur invité est **C:\ProgramData\Microsoft\Windows\Hyper-V**. Validez par **Suivant**.

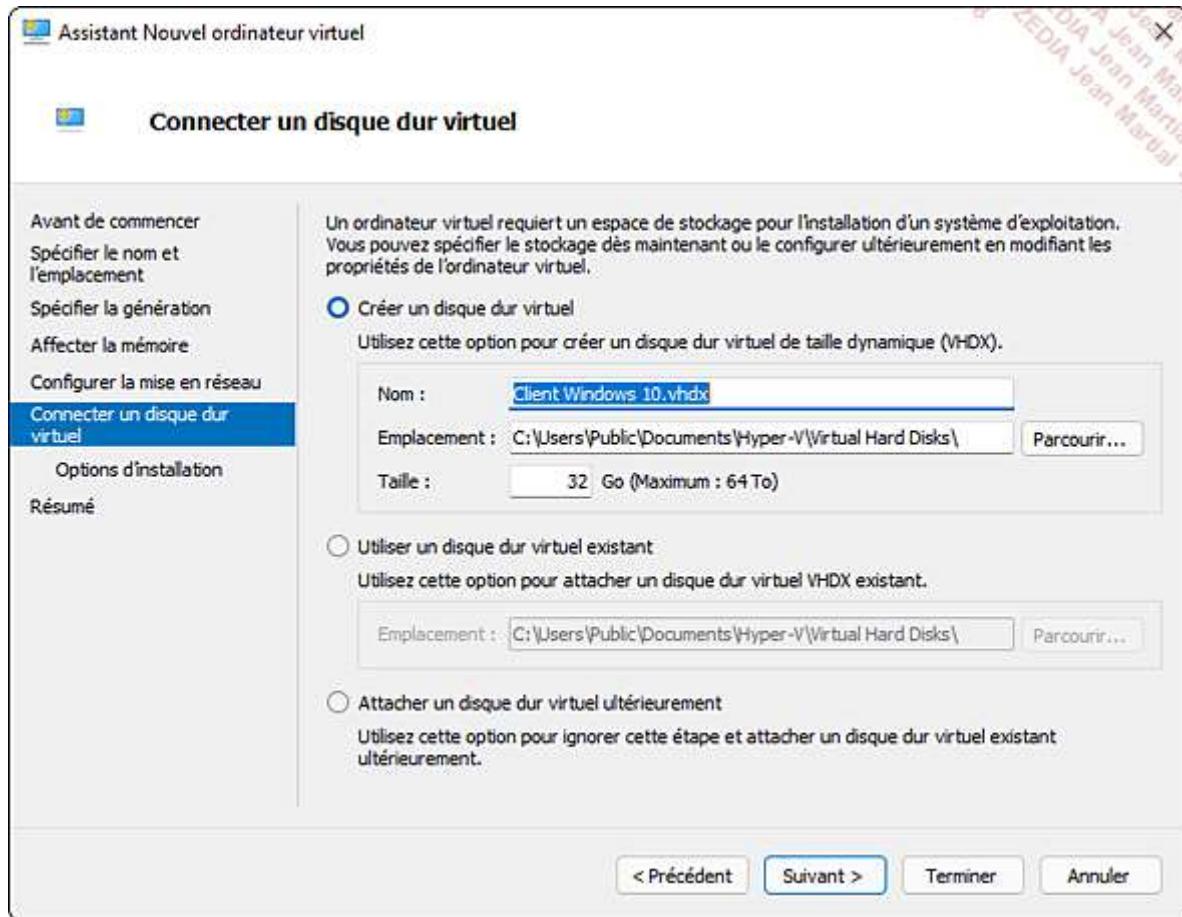
Sélectionnez l'option **Génération 2** afin d'assurer une compatibilité avec Windows 10 (64 bits).

Dans l'étape **Affecter la mémoire**, entrez la quantité de mémoire vive dédiée à l'ordinateur virtuel, soit **2048 Mo** dans notre cas. Vous pouvez allouer de manière dynamique une quantité de RAM, en cochant la case **Utiliser la mémoire dynamique pour cet ordinateur virtuel**.



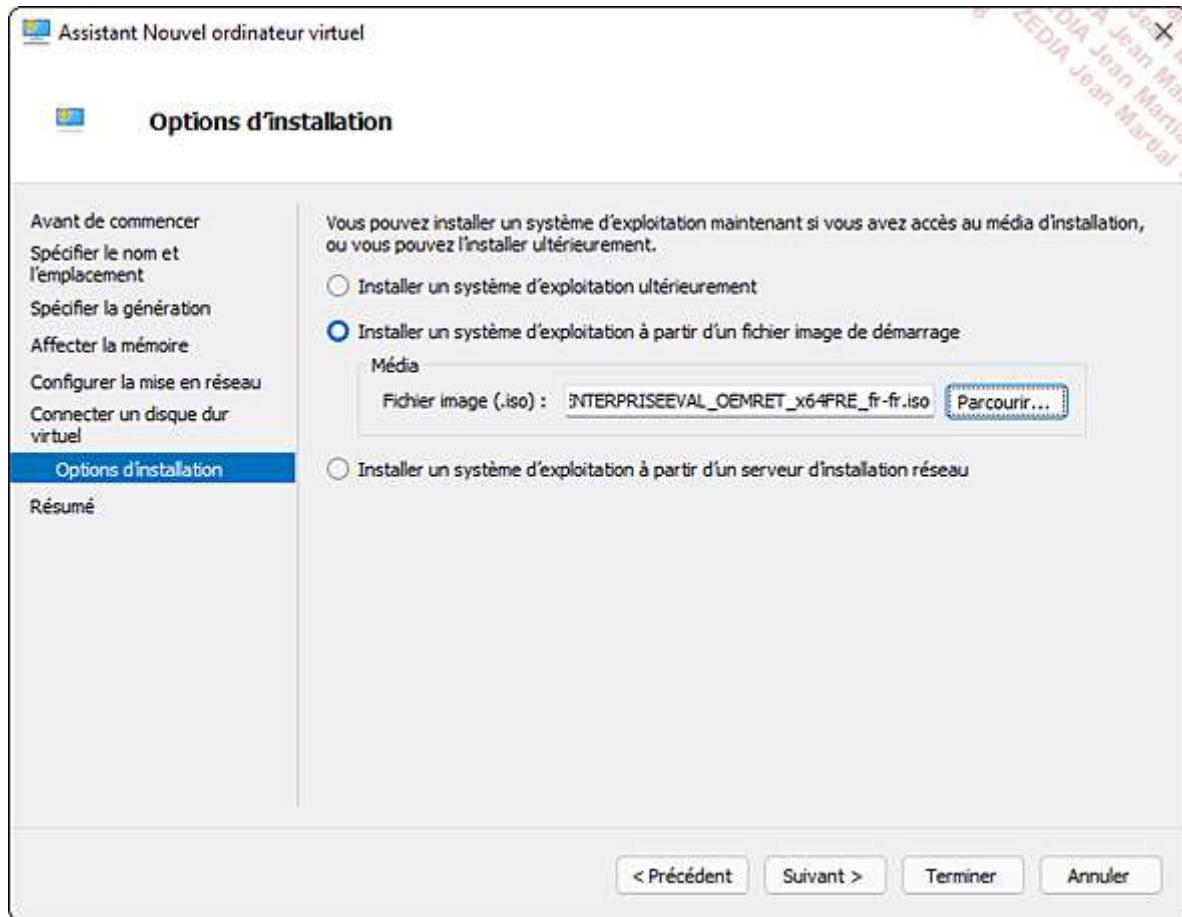
Cliquez sur **Suivant**.

Selectionnez une carte réseau utilisée par l'ordinateur virtuel, par défaut **Default Switch** et validez par **Suivant**. Créez un disque virtuel en spécifiant un nom de fichier au format VHDX (**Client Windows 10.vhdx**), son emplacement de stockage et sa taille de **32 Go** (maximum 64 To). Notez que l'administrateur peut utiliser un disque virtuel existant ou en attacher un ultérieurement.



Cliquez sur **Suivant**.

Dans l'étape **Options d'installation**, sélectionnez l'option **Installer un système d'exploitation à partir d'un fichier image de démarrage** puis cliquez sur **Parcourir**. Sélectionnez le dossier contenant l'image de Windows 10 Entreprise précédemment téléchargée depuis le site Microsoft.

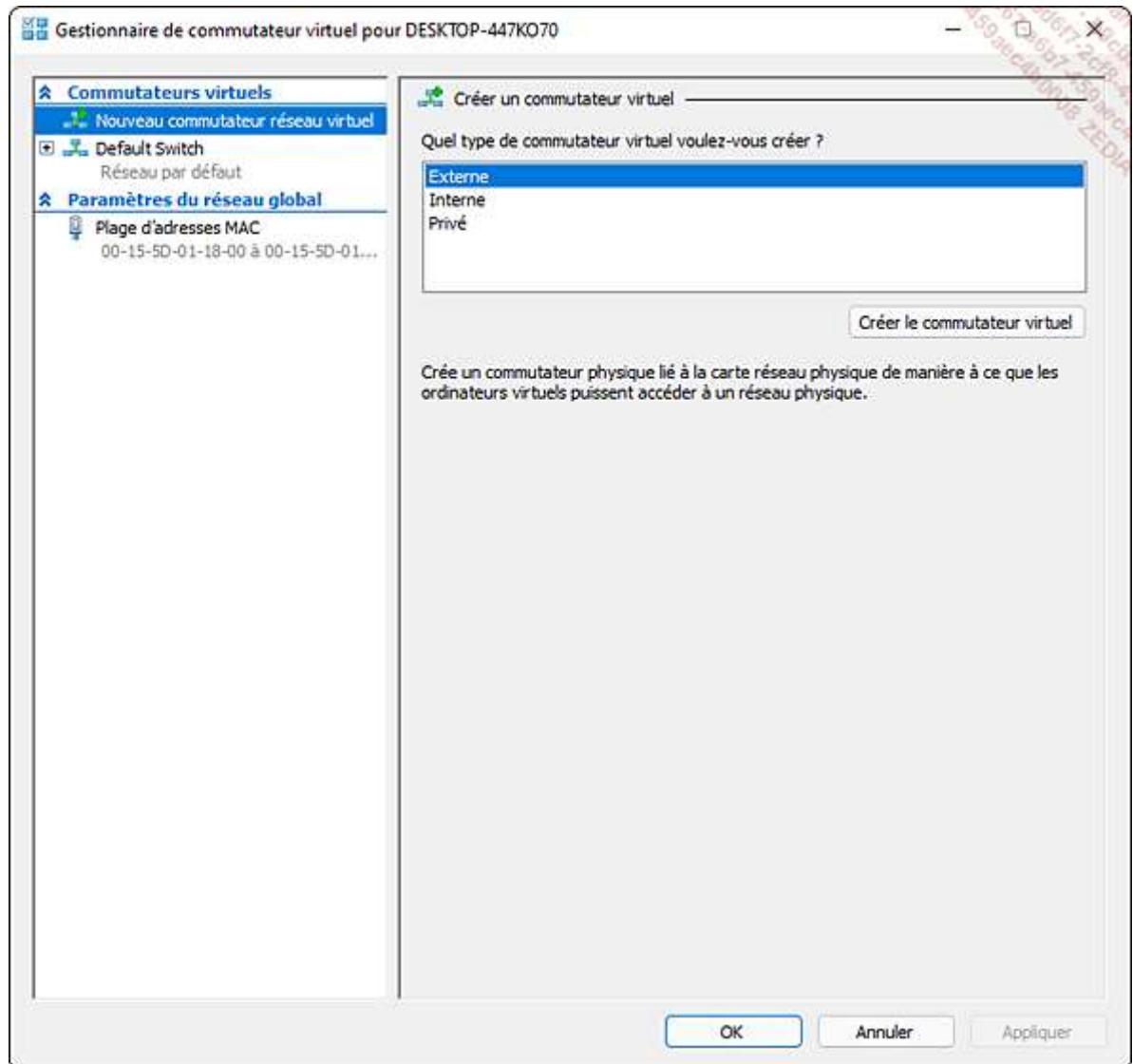


Cliquez sur **Suivant**.

Vérifiez les paramètres sélectionnés dans l'étape **Résumé** et cliquez sur le bouton **Terminer**. Votre système d'exploitation invité contenant les fichiers d'installation de Windows 10 Entreprise est prêt à être démarré.

Hyper-V propose de créer des réseaux virtuels attribués aux machines virtuelles hébergées, en fonction de l'un des trois types suivants :

- **Réseau externe** : permet à un ordinateur virtuel de communiquer avec les clients externes, le système d'exploitation hôte Windows 11, ainsi que les ordinateurs virtuels hébergés sur l'ordinateur. Le réseau virtuel est connecté au réseau physique.
- **Réseau interne** : ce type de réseau autorise les communications entre les ordinateurs virtuels et le système hôte Windows 11, mais pas avec des clients externes. Un réseau virtuel interne est généralement utilisé pour créer un environnement de test. Le réseau virtuel n'est pas connecté au réseau physique.
- **Réseau privé** : seules les communications entre ordinateurs virtuels hébergés sur le poste Windows 11 sont autorisées.



Vous trouverez ces options en cliquant sur **Gestionnaire de commutateur virtuel**, présent dans le panneau droit du **Gestionnaire Hyper-V**.

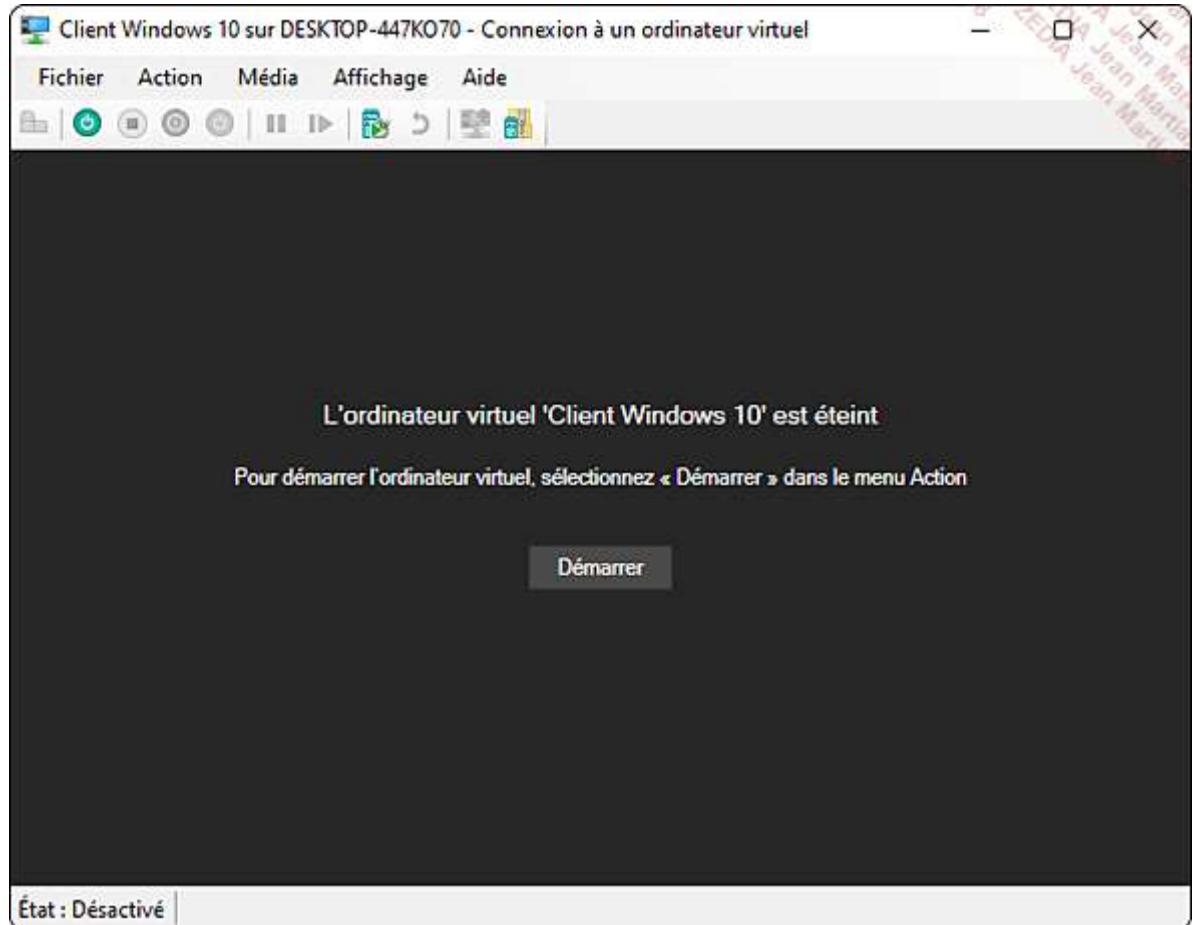
Nous avons ainsi créé un ordinateur virtuel nommé Client Windows 10 possédant un disque dur virtuel nommé Client Windows 10.vhdx d'une taille de 32 Go et une mémoire vive de 2048 Mo. En langage de script PowerShell, il suffirait de taper la commande suivante pour créer le même ordinateur virtuel :

```
new-vm -name "Client Windows 10" -MemoryStartupBytes 2048Mb  
-NewVHDPath "c:\Users\Public\Documents\Hyper-v\Virtual Hard  
Disks\Client Windows 10.vhdx" -newVHDSIZEBytes 32Gb
```

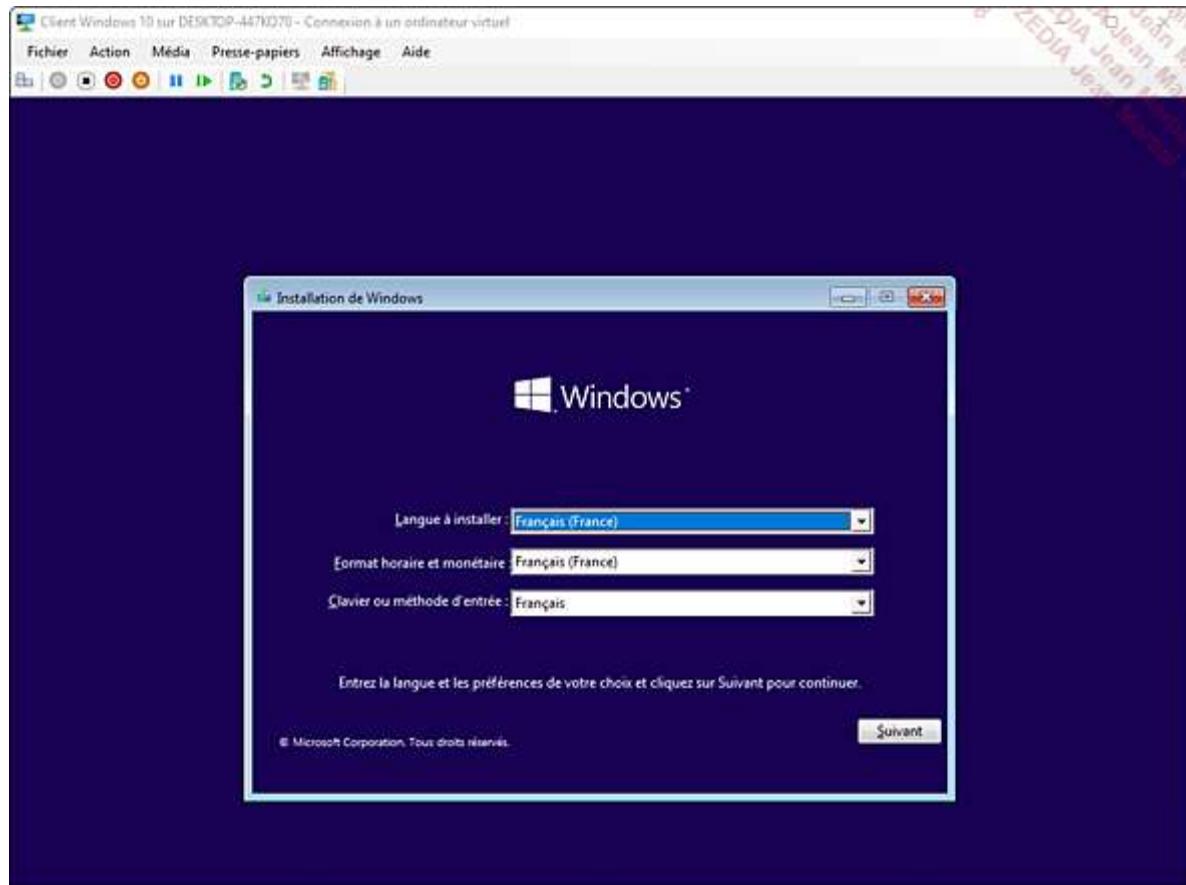
- Chaque ordinateur virtuel nécessite la licence d'exploitation adéquate.

Pour démarrer l'installation de l'ordinateur virtuel Windows 10 Professionnel précédemment créé :

Dans le **Gestionnaire Hyper-V**, sélectionnez votre ordinateur virtuel nommé **Client Windows 10** puis cliquez avec le bouton droit et choisissez **Se connecter**, ou bien double cliquez sur celui-ci.



Cliquez sur le bouton **Démarrer** (ou pressez les touches [Ctrl]+S. L'ordinateur virtuel **Client Windows 10** démarre. À l'invite, cliquez sur l'écran pour démarrer à partir du fichier ISO précédemment téléchargé et ainsi commencer à installer le système d'exploitation invité.



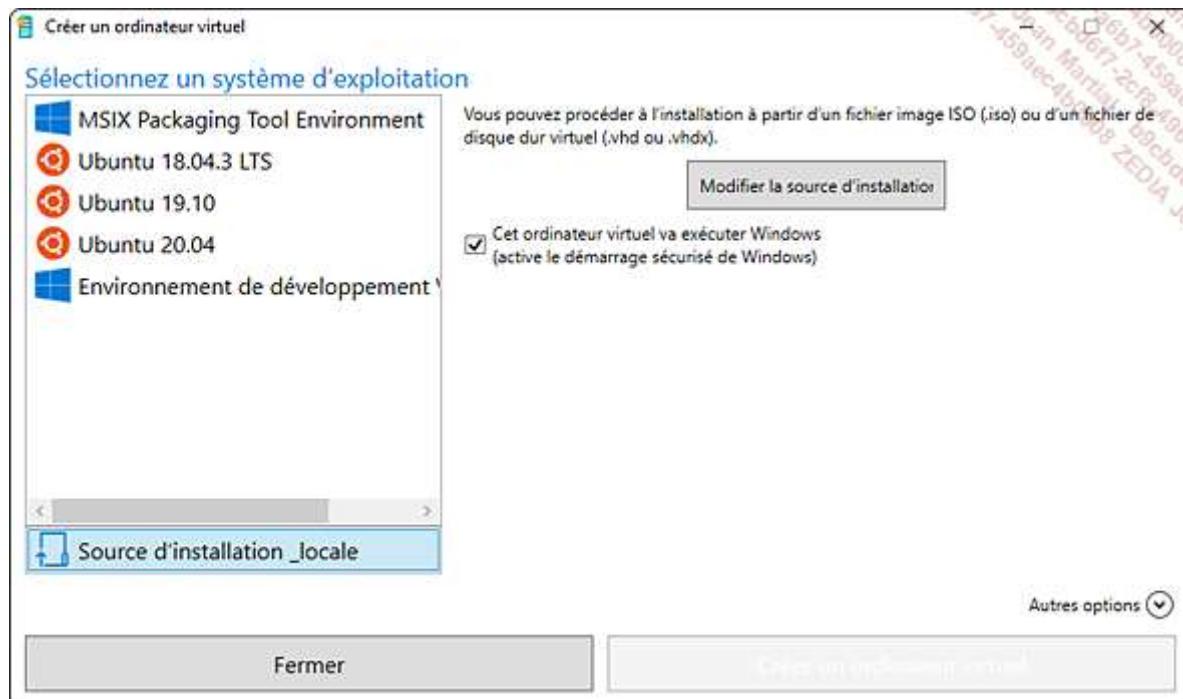
Notez que lorsque l'ordinateur hôte Windows 11 entre en mode veille, les machines invitées sont automatiquement sauvegardées puis mises en veille à leur tour afin de retrouver leur état d'origine lors de la sortie de l'hibernation.

Windows 11 Hyper-V est parfaitement compatible avec l'hyperviseur Hyper-V fourni avec Windows Server 2019 (ou versions antérieures), ce qui signifie que vous pouvez importer des machines virtuelles créées avec Windows 11 vers un serveur Windows Server 2019.

Depuis la version Fall Creators Update de Windows 10 il est possible de créer rapidement une machine virtuelle à l'aide du menu **Création rapide** :

Cliquez sur le menu **Démarrer**, puis sur **Création rapide d'HyperV**. Ce menu est également accessible depuis le **Gestionnaire Hyper-V** dans le volet **Actions** situé à droite de l'interface, en cliquant sur **Création rapide**.

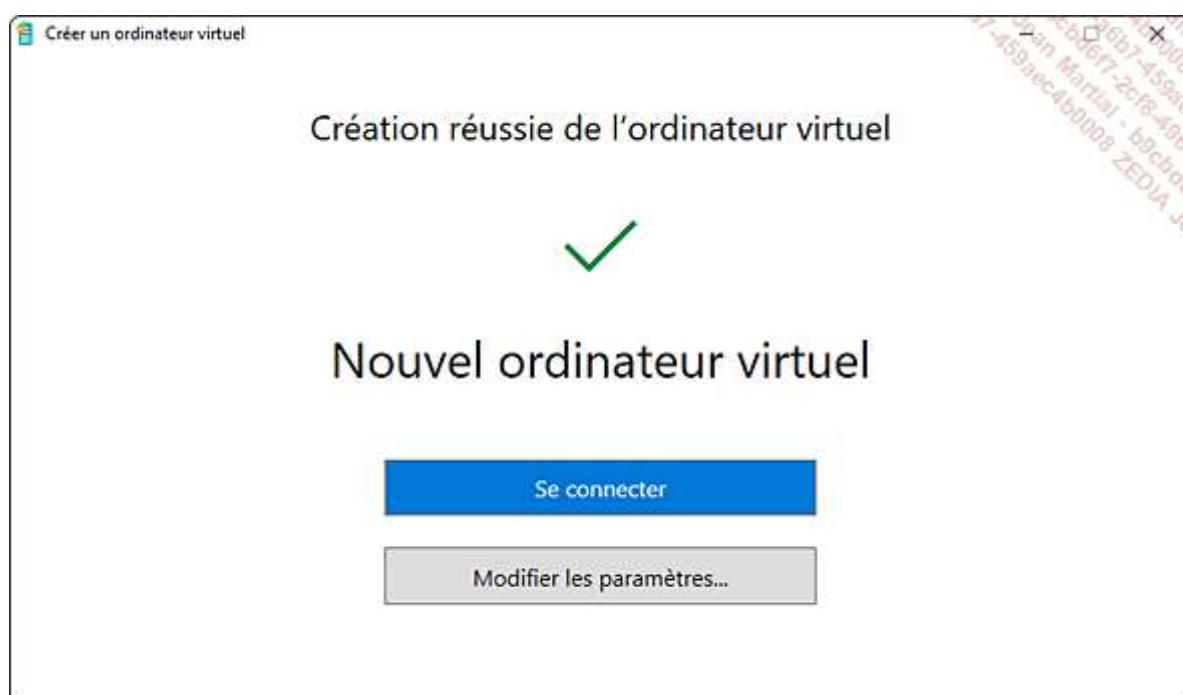
Certains systèmes d'exploitation sont proposés par défaut, dont Ubuntu. Si celui que vous désirez installer n'apparaît pas, cliquez sur **Source d'installation locale**, puis **Modifier la source d'installation** et sélectionnez le fichier ISO.



En bas à droite, le bouton **Autres options** permet de modifier le chaDans le champ **Nom**, ainsi que le réseau.

Cliquez sur le bouton **Créer un ordinateur virtuel**. La machine est créée avec les paramètres par défaut.

- Notez qu'en cas de sélection d'un système d'exploitation proposé, les sources sont téléchargées avant la création de la machine virtuelle.



Une fois l'installation terminée, cliquez sur le bouton **Se connecter** puis sur le bouton **Démarrer**. Tapez sur une touche du clavier. Les étapes d'installation s'affichent...

Résumé du chapitre

- Deux méthodes permettent de déployer un poste de travail Windows 11 dans un environnement d'entreprise : Lite Touch et Zero Touch.
- La méthode Lite Touch implique une intervention minime de l'utilisateur. Un déploiement Zero Touch installe un poste de manière entièrement automatisée.
- Le format de fichier WIM permet à une seule image de disque Windows 11 d'être déployée et appliquée au travers du réseau sur un ensemble de postes de travail.
- L'outil sysprep permet de supprimer toutes les données spécifiques au système Windows 11, comme l'ID unique de sécurité, afin de générer une image qui pourra être appliquée sur d'autres ordinateurs.
- ICD (Concepteur de fonctions d'acquisition d'images et de configuration) est un outil de création de package de mise en service, utilisable pour personnaliser le parc informatique Windows 11 de la société (ordinateurs, appareils mobiles) sans avoir à réinstaller les cibles.
- Le kit ADK offre des outils pour déployer une image sans intervention de l'utilisateur. Le processus d'installation de Windows 11 peut être entièrement automatisé à l'aide d'un fichier au format standard XML.
- De multiples produits Microsoft existent pour déployer des systèmes d'exploitation, certains gratuits comme MDT ou les services de déploiement Windows WDS, d'autres, payants, incluant la gestion de parc informatique comme Microsoft Endpoint Configuration Manager.
- Windows 11 embarque la fonctionnalité Hyper-V afin de virtualiser des systèmes d'exploitation et ainsi d'y accéder depuis son poste de travail.

Interface et applications

Interface Windows 11

Microsoft propose une interface utilisateur innovante, apparue avec le projet Windows 10X et apportant des changements importants, tels que le positionnement de la barre des tâches, la refonte intégrale des icônes et des menus, la disparition des tuiles dynamiques.

Les programmes développés pour Windows 11 sont adaptés à cette nouvelle interface, tels que Microsoft Edge, le nouveau navigateur de Microsoft.

Les changements dans l'interface de l'Explorateur de fichiers seront abordés dans le chapitre Gestion des disques et des pilotes, section Partitionnement et gestion des fichiers.

1. Le bureau et le menu Démarrer

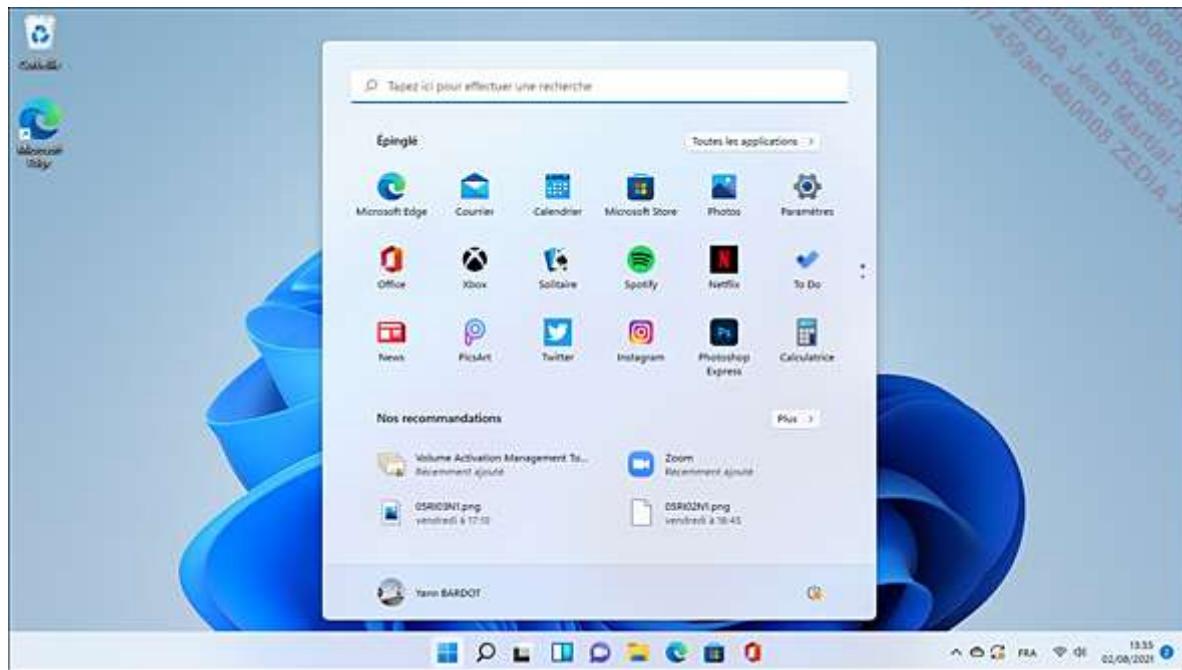
Le bureau s'affiche dès l'ouverture de session : simple, lumineux. Premier gros changement : les icônes applicatives de la barre des tâches sont désormais centrées sur celle-ci. Les icônes de notifications se trouvent toujours sur la droite, mais leur section a été réduite.

Le menu **Démarrer** est toujours présent au centre de la barre des tâches, à gauche des éléments présents par défaut. Il a été profondément remanié, mettant en valeur les fichiers et applications récemment utilisés dans la section **Recommandations**.

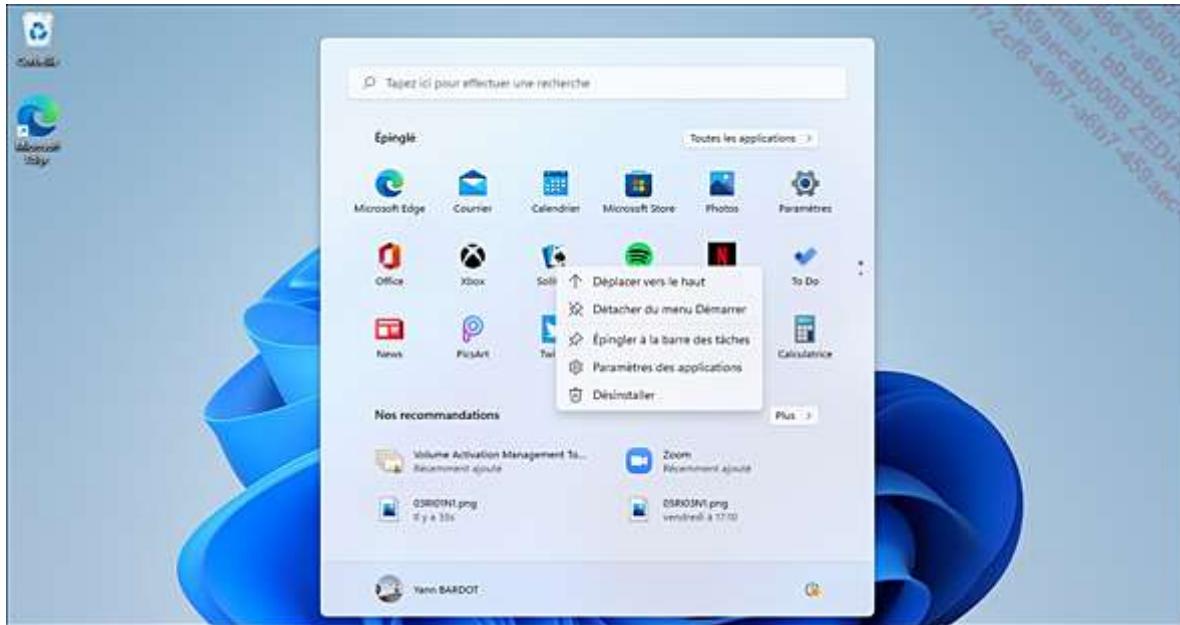
La section appelée **Epinglé** est une zone d'accès rapide à certaines applications ou certains dossiers. Il est possible d'ajouter ou de supprimer ses éléments.

L'accès aux autres applications installées se fait en cliquant sur le bouton **Toutes les applications** situé en haut à droite du menu **Démarrer**.

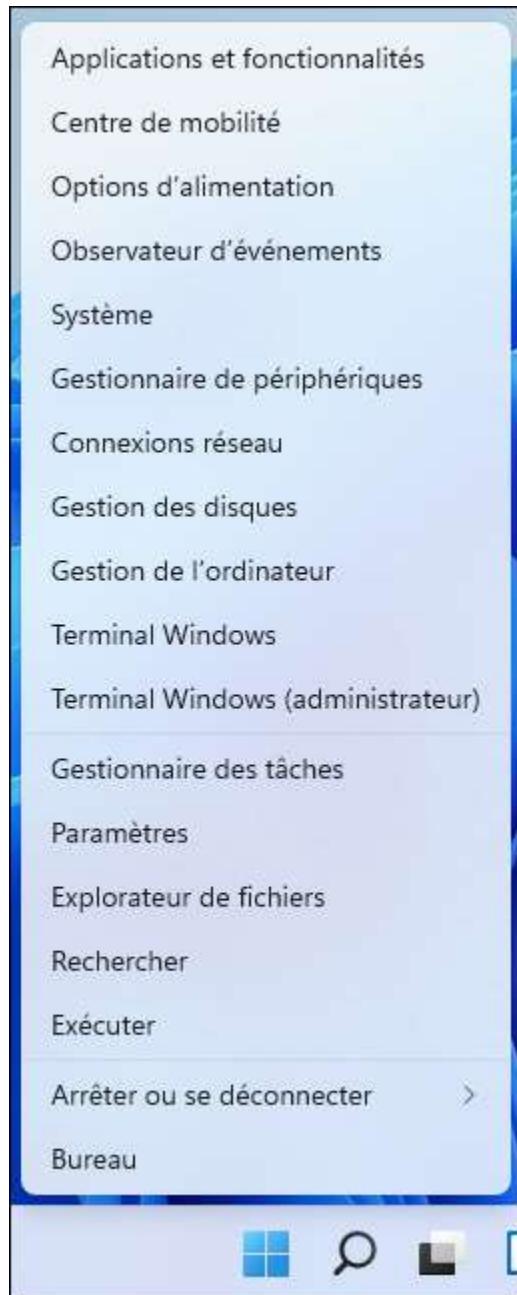
Enfin, la barre de recherche a été incorporée au sommet de ce menu.



En cliquant avec le bouton droit sur une application épingle (Edge dans notre exemple), il est possible de détacher celle-ci de l'écran de démarrage, de la déplacer, de désinstaller l'application, ou bien d'exécuter d'autres actions en fonction de l'application :



En cliquant avec le bouton droit sur le bouton du menu **Démarrer**, les principales fonctionnalités du système (**Applications et fonctionnalités**, **Observateur d'évènements**, **Terminal Windows**, **Gestionnaire des tâches**, etc.) sont accessibles rapidement.

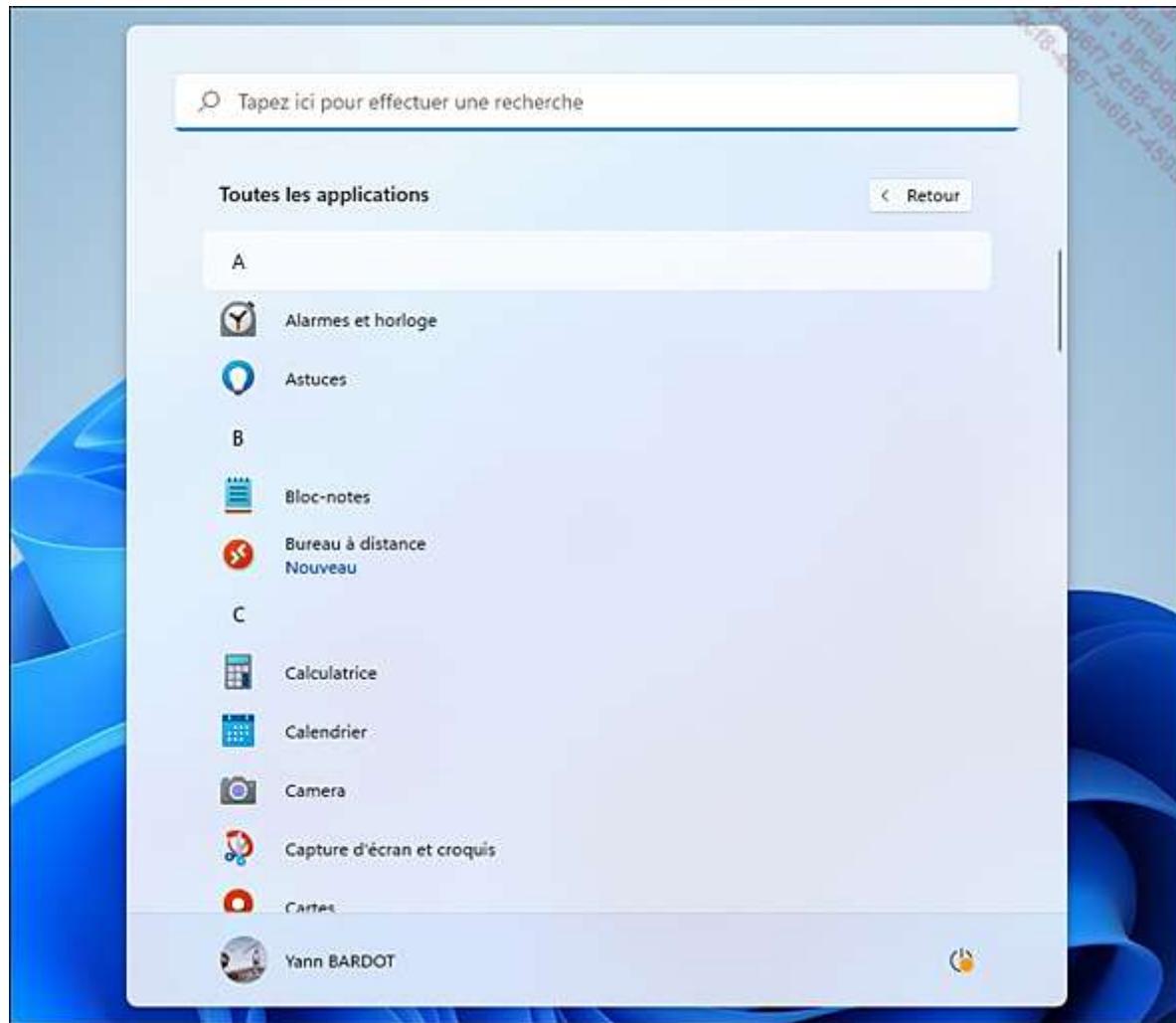


Notez que le raccourci + X effectue la même action.

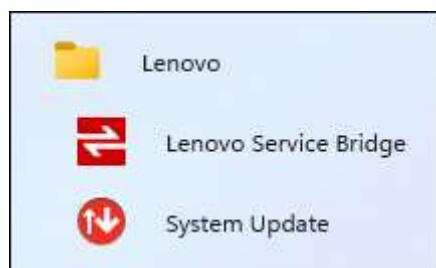
a. Exécution et fermeture d'une application

Dès qu'une nouvelle application est installée, le menu **Démarrer** vous prévient à l'aide d'une étiquette "**Récemment ajoutées**" en dessous de l'application, qui sera elle-même affichée dans la section **Recommandations**. Plus vous utiliserez une application, plus longtemps celle-ci sera affichée dans cette section.

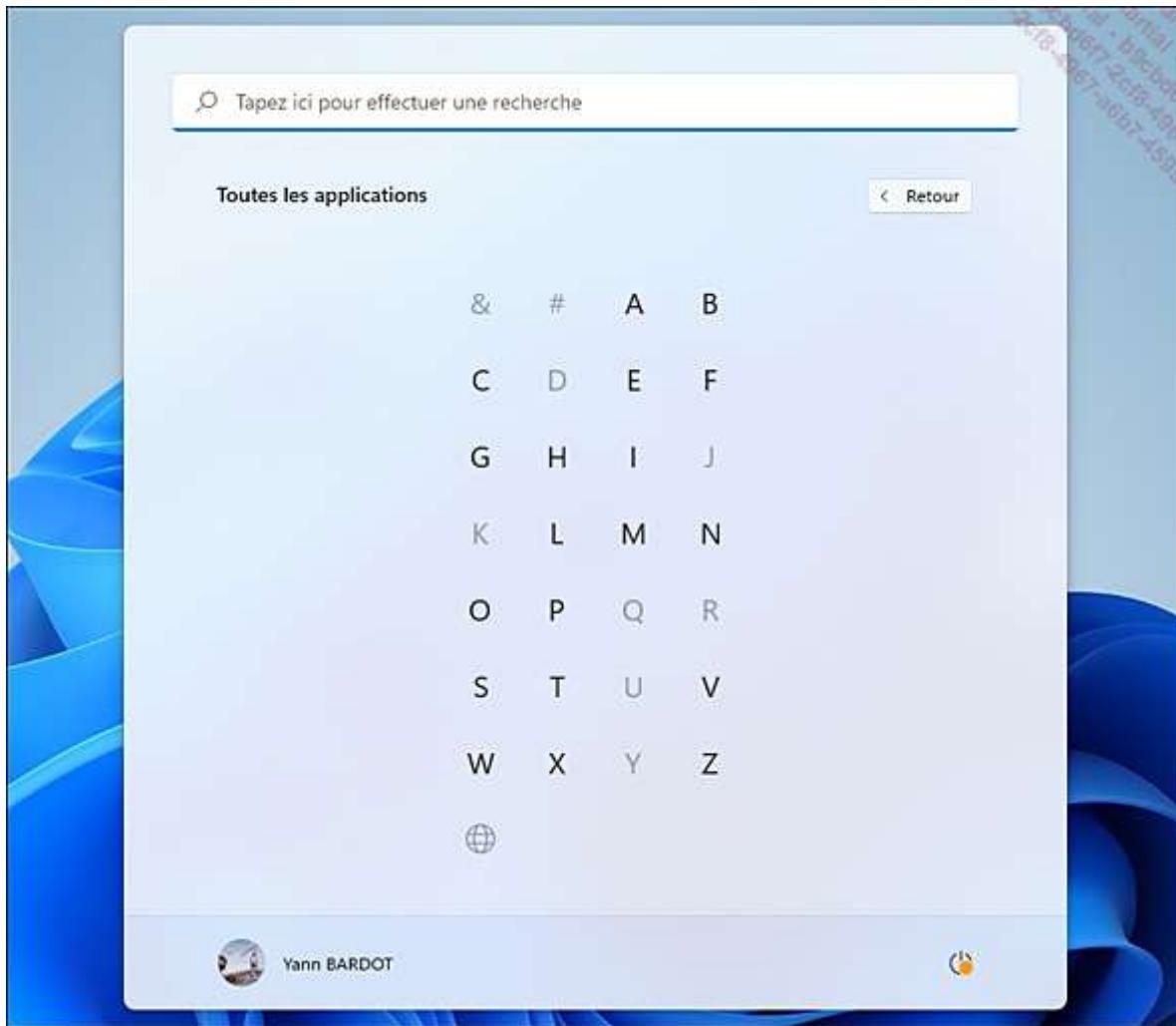
Pour afficher toutes les applications classées par ordre alphabétique, cliquez sur le menu **Démarrer**, puis sur le bouton **toutes les applications** :



Les dossiers contenant les applicatifs sont affichés à l'aide de l'icône jaune représentant un dossier :

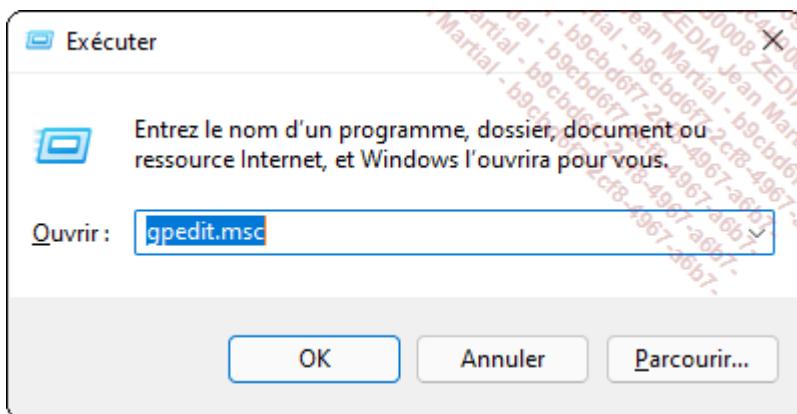


Par défaut, les applications sont affichées en fonction de leur nom. En cliquant sur une lettre de l'alphabet, l'utilisateur peut plus rapidement accéder à ces dernières :



Pour revenir à l'écran principal du menu **Démarrer**, cliquez sur la flèche pointant vers la gauche nommée **Retour**. En pressant la touche du clavier, le menu **Démarrer** se ferme ou s'ouvre en fonction de son état initial.

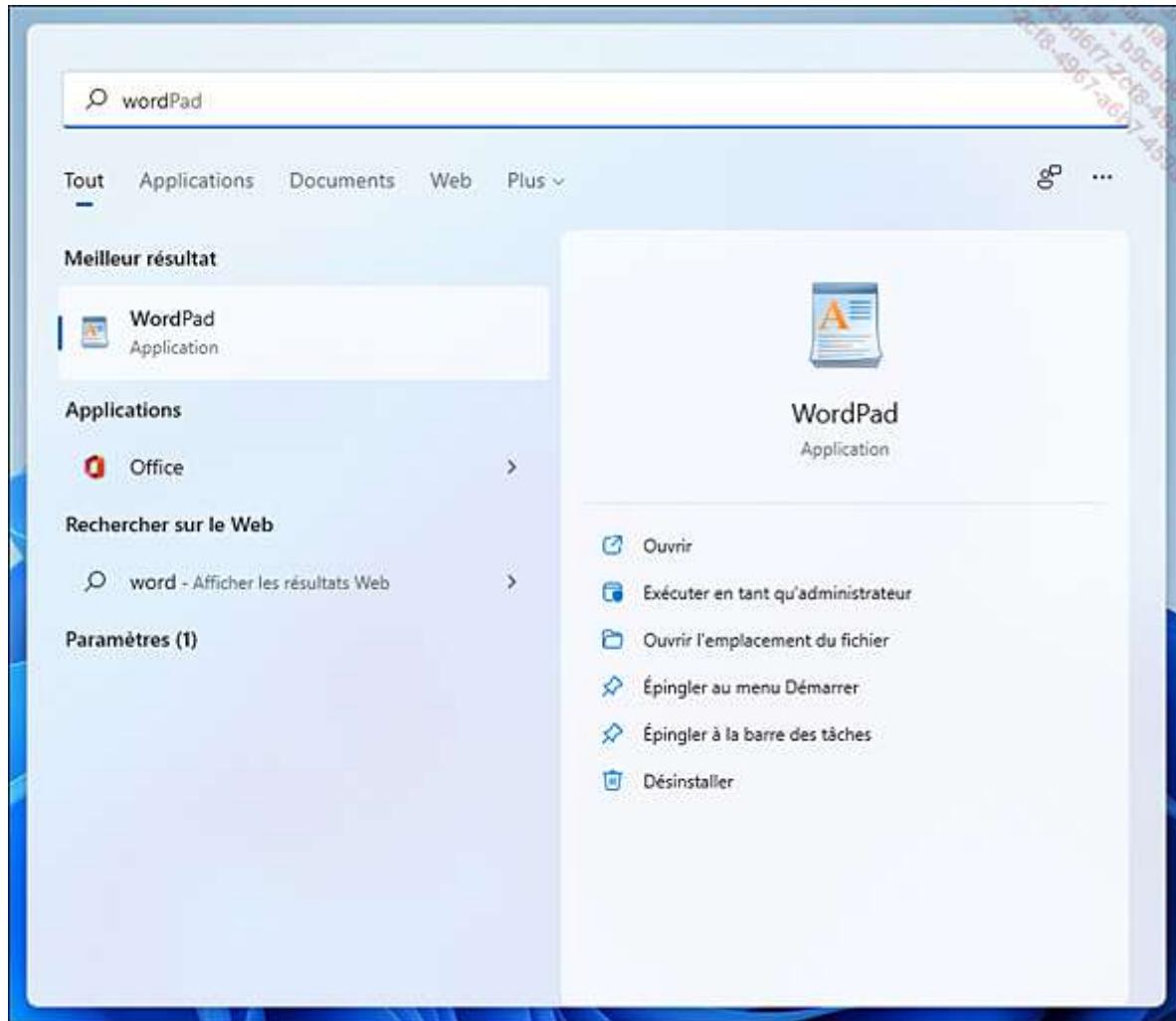
La fenêtre **Exécuter** reste accessible en pressant les touches + R.



Pour exécuter une application Windows 11, pressez simplement votre doigt sur l'icône, ou bien cliquez dessus avec le bouton gauche de la souris.

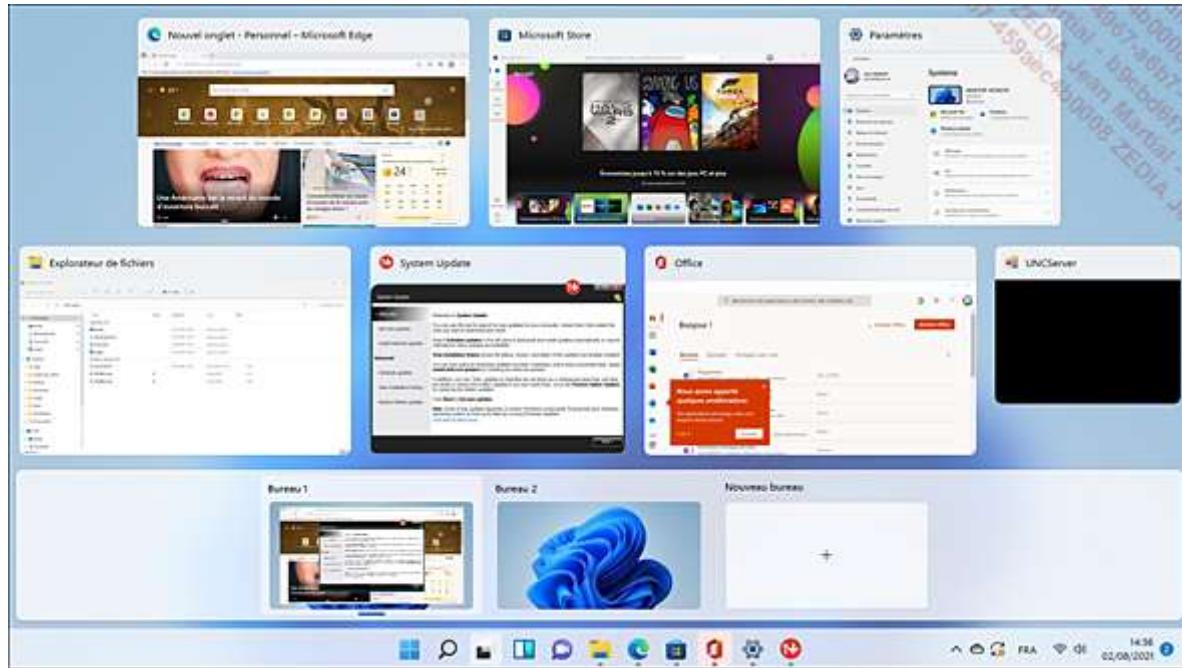
Rechercher une application installée est facile : depuis la zone de recherche du menu **Démarrer**, ou simplement en ouvrant le menu **Démarrer**, saisissez les premières lettres composant son nom pour la rechercher et afficher son menu. Notez que, désormais, le résultat de votre requête contient une liste de sites internet indexés par le

moteur de recherche Bing et accessibles via le navigateur par défaut, mais aussi les fichiers récemment ouverts associés au programme recherché.



Pour fermer l'application, pointez la souris ou votre doigt en haut à droite de l'écran l'affichant, et cliquez sur le bouton **Fermer** (représenté par une croix). La combinaison des touches [Alt] + [F4] du clavier est toujours utilisable.

Visualiser les applications en cours d'exécution s'effectue en pressant simultanément les touches + [Tab] du clavier.



Toutes les applications Windows 11 en cours d'exécution sont affichées, qu'il s'agisse des programmes exécutés depuis le bureau ou ceux provenant du Microsoft Store.

Notez que les bureaux virtuels sont accessibles avec cette même combinaison de touches.

La personnalisation du menu **Démarrer** s'effectue depuis le panneau des **Paramètres**, accessible depuis cette



icône :  puis en cliquant sur **Personnalisation**, puis **Démarrer**. Dans cette section, vous pouvez désactiver l'affichage des applications les plus utilisées ou récemment ajoutées, ou encore modifier l'affichage de l'icône de certaines fonctionnalités ou certains dossiers (Explorateur, Téléchargements, etc.).

The screenshot shows the Windows 11 Settings app with the following interface:

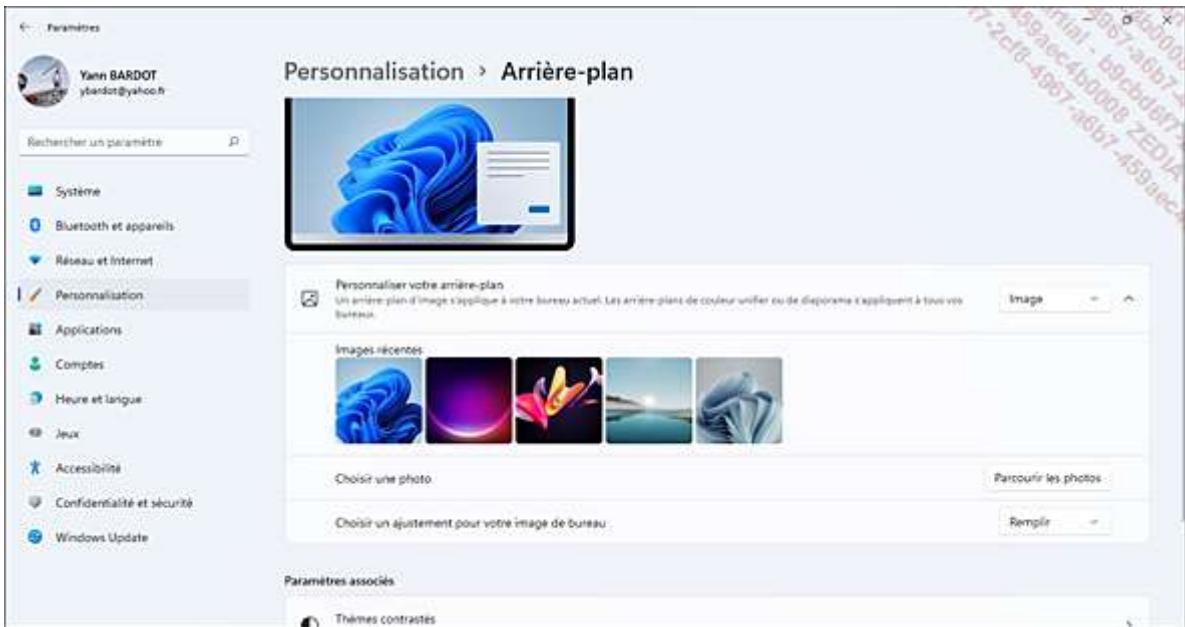
- Header:** Personnalisation > Démarrer
- Left sidebar (Paramètres):**
 - Système
 - Bluetooth et appareils
 - Réseau et Internet
 - Personnalisation** (selected)
 - Applications
 - Comptes
 - Heure et langue
 - Jeux
 - Accessibilité
 - Confidentialité et sécurité
 - Windows Update
- Right pane (Démarrer):**
 - Afficher les applications récemment ajoutées (Activé)
 - Afficher les applications les plus utilisées (Activé)
 - Afficher les articles récemment ouverts dans Accueil, Listes de raccourcis et Explorateur de fichiers (Activé)
 - Dossiers**: Ces dossiers apparaissent dans Démarrer en regard du bouton Marche/Arrêt
- Bottom right:**
 - Obtenir de l'aide
 - Envoyer des commentaires

b. Personnaliser Windows 11

Windows 11 propose de personnaliser l'interface utilisateur, dont le fond d'écran du bureau ou l'écran de verrouillage, ainsi que l'image d'avatar du compte d'utilisateur.

Pour personnaliser l'arrière-plan du bureau, rendez-vous dans le menu **Démarrer**, cliquez sur **Paramètres** et **Personnalisation**. La section **Arrière-plan** permet de :

- sélectionner une image parmi les vôtres ou celles proposées par Microsoft ;
- choisir une couleur unie ;
- mettre en place un diaporama d'images qui changera par défaut toutes les 30 minutes.



Une fois l'arrière-plan défini, si vous souhaitez afficher l'image suivante du diaporama configuré, cliquez avec le bouton droit sur une zone vierge du bureau, puis sur **Afficher l'arrière-plan suivant**.

L'utilisateur peut aussi définir un fond d'écran affiché sur l'écran de verrouillage de la session : toujours dans **Personnalisation**, cliquez sur la section **Écran de verrouillage**.

Par défaut, de magnifiques images sont sélectionnées et affichées par Microsoft (option **Windows à la une**). Si vous souhaitez afficher l'image de votre choix, choisissez l'option **Image** et cliquez sur le bouton **Parcourir les photos**.

L'utilisateur peut aussi ajouter une application dont les informations dynamiques seront affichées sur l'écran de verrouillage, en sélectionnant parmi celles proposées dans la section **État de l'écran de verrouillage**. Une application (Courrier, Météo, Calendrier...) affichera donc un état détaillé (température actuelle, dernier rendez-vous...) dans l'écran de déverrouillage.

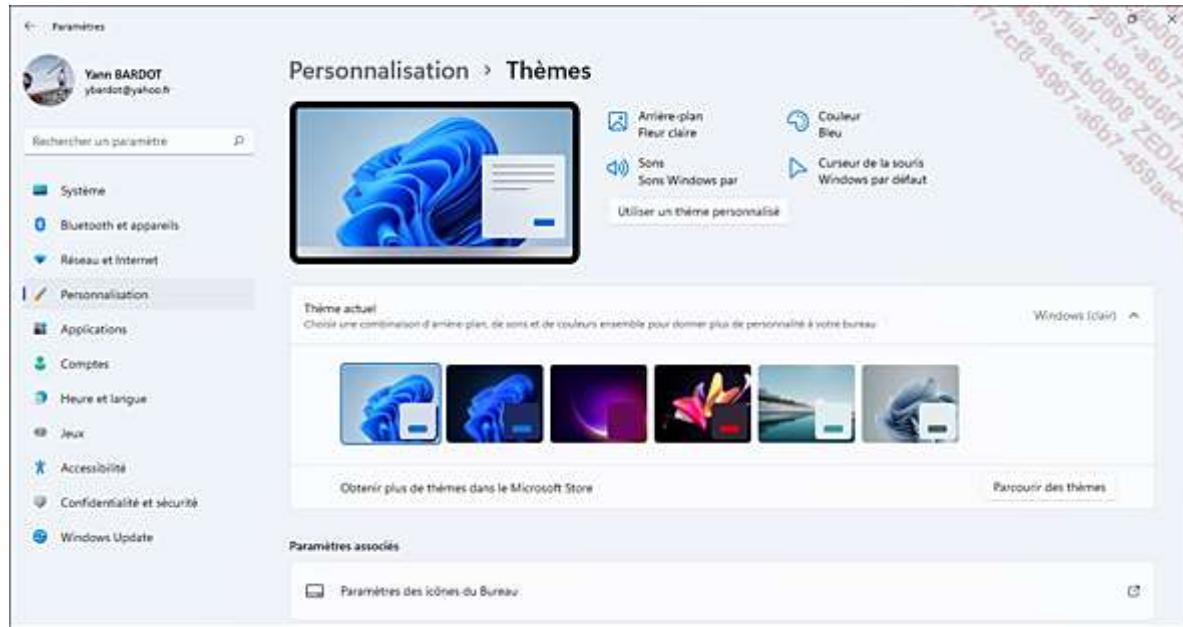


Tout comme l'arrière-plan du bureau, l'utilisateur peut aussi lire un diaporama de ses photos lors de l'affichage de l'écran de verrouillage, en sélectionnant **Diaporama** dans le menu déroulant puis en ajoutant un dossier.

Déverrouiller une session s'effectue en pressant les touches [Entrée] ou [Espace] du clavier, ou en glissant la souris ou le doigt du bas de l'écran vers le haut. L'utilisateur peut verrouiller une session en pressant les touches **Windows + L** ou bien en pressant les touches **[Ctrl] + [Alt] + [Suppr]** et en cliquant/pointant sur **Verrouiller**.

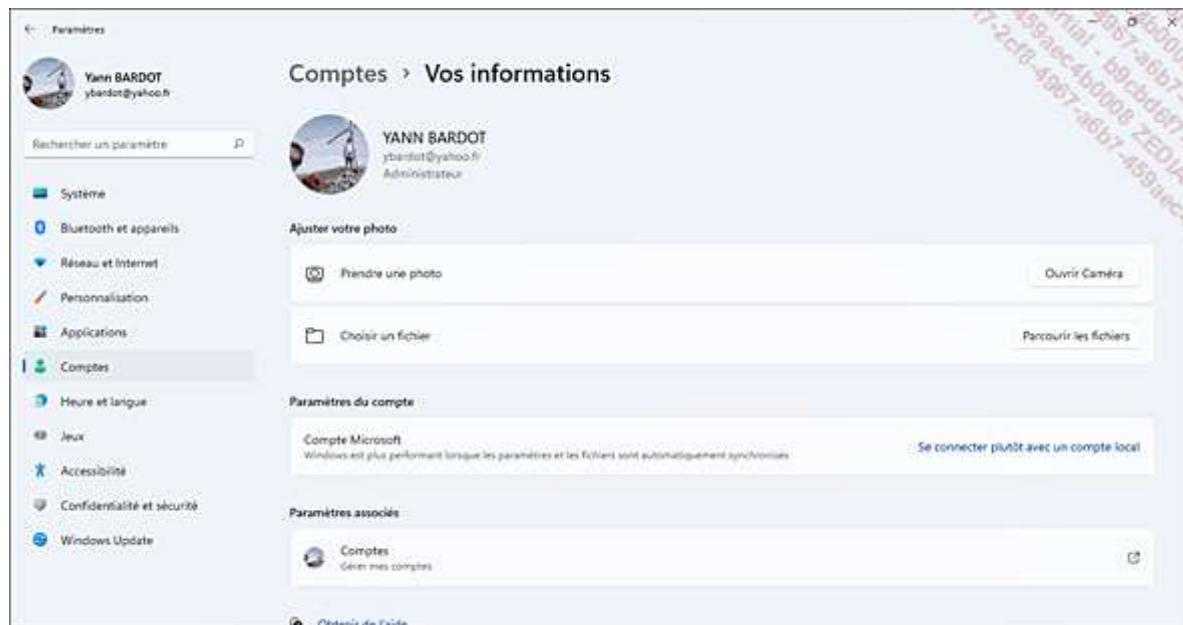
C'est également ici, que l'utilisateur pourra définir les délais d'extinction de l'écran, et de mise en veille.

Enfin, la modification du thème par défaut de Windows 11 est possible depuis la section **Thèmes** de l'interface de personnalisation.



Thèmes clairs, thèmes sombres prédéfinis, création de son propre thème avec personnalisation de l'arrière-plan, de la couleur dominante, des sons et des curseurs de souris : tout est paramétrable.

Pour attribuer une image à un compte d'utilisateur, restez dans les **Paramètres** et rendez-vous cette fois dans le menu **Comptes**.



Il est également possible d'utiliser la caméra de la machine pour prendre une photo ou de choisir un fichier et de sélectionner l'image de son choix.

c. Customisation de l'écran de démarrage

Les éditions Windows 11 Professionnel, Entreprise et Education offrent à l'administrateur d'un domaine Active Directory la possibilité de personnaliser l'écran de démarrage, le menu **Démarrer** et la barre des tâches de ses utilisateurs, afin de déployer la même configuration sur tous les postes de travail de l'entreprise. Cette personnalisation est disponible depuis Windows 10, version 1607.

L'administrateur doit dans un premier temps, configurer (ajouter, enlever...) le menu **Démarrer** et la barre des tâches avec les applications souhaitées, puis exporter la disposition générée dans un fichier au format XML, afin de le déployer par l'intermédiaire d'un objet stratégie de groupe.

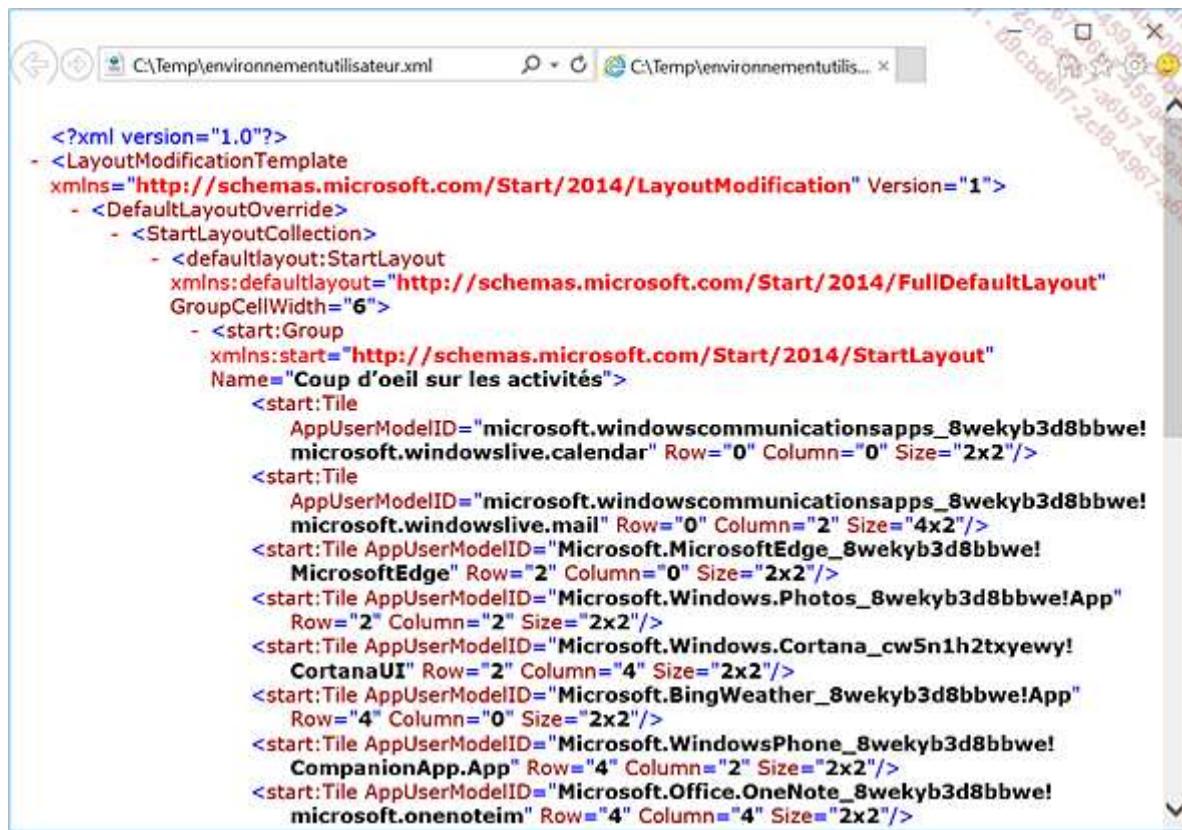
Pour cela, une fois l'environnement personnalisé, exécutez une fenêtre Windows PowerShell :

Depuis la zone de recherche située sur la barre des tâches, saisissez **Windows PowerShell** puis cliquez avec le bouton droit sur le résultat et sur **Exécuter comme administrateur**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

Dans la fenêtre Windows PowerShell, saisissez la commande suivante afin de générer le fichier de configuration au format XML :

- Export-StartLayout -Path c:\temp\environnementutilisateur.xml

Voici un exemple de fichier XML généré lors de l'étape précédente :



```
<?xml version="1.0"?>
- <LayoutModificationTemplate
  xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification" Version="1">
  - <DefaultLayoutOverride>
    - <StartLayoutCollection>
      - <defaultlayout:StartLayout
        xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayout"
        GroupCellWidth="6">
          - <start:Group
            xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout"
            Name="Coup d'œil sur les activités">
              <start:Tile
                ApplicationUserModelID="microsoft.windowscommunicationsapps_8wekyb3d8bbwe!
                microsoft.windowslive.calendar" Row="0" Column="0" Size="2x2"/>
              <start:Tile
                ApplicationUserModelID="microsoft.windowscommunicationsapps_8wekyb3d8bbwe!
                microsoft.windowslive.mail" Row="0" Column="2" Size="4x2"/>
              <start:Tile ApplicationUserModelID="Microsoft.MicrosoftEdge_8wekyb3d8bbwe!
                MicrosoftEdge" Row="2" Column="0" Size="2x2"/>
              <start:Tile ApplicationUserModelID="Microsoft.Windows.Photos_8wekyb3d8bbwe!App"
                Row="2" Column="2" Size="2x2"/>
              <start:Tile ApplicationUserModelID="Microsoft.Windows.Cortana_cw5n1h2txyewy!
                CortanaUI" Row="2" Column="4" Size="2x2"/>
              <start:Tile ApplicationUserModelID="Microsoft.BingWeather_8wekyb3d8bbwe!App"
                Row="4" Column="0" Size="2x2"/>
              <start:Tile ApplicationUserModelID="Microsoft.WindowsPhone_8wekyb3d8bbwe!
                CompanionApp.App" Row="4" Column="2" Size="2x2"/>
              <start:Tile ApplicationUserModelID="Microsoft.Office.OneNote_8wekyb3d8bbwe!
                microsoft.onenoteim" Row="4" Column="4" Size="2x2"/>
```

Pour de plus amples informations sur le fichier LayoutModification.xml, consultez la page : <https://docs.microsoft.com/fr-fr/windows/configuration/start-layout-xml-desktop>

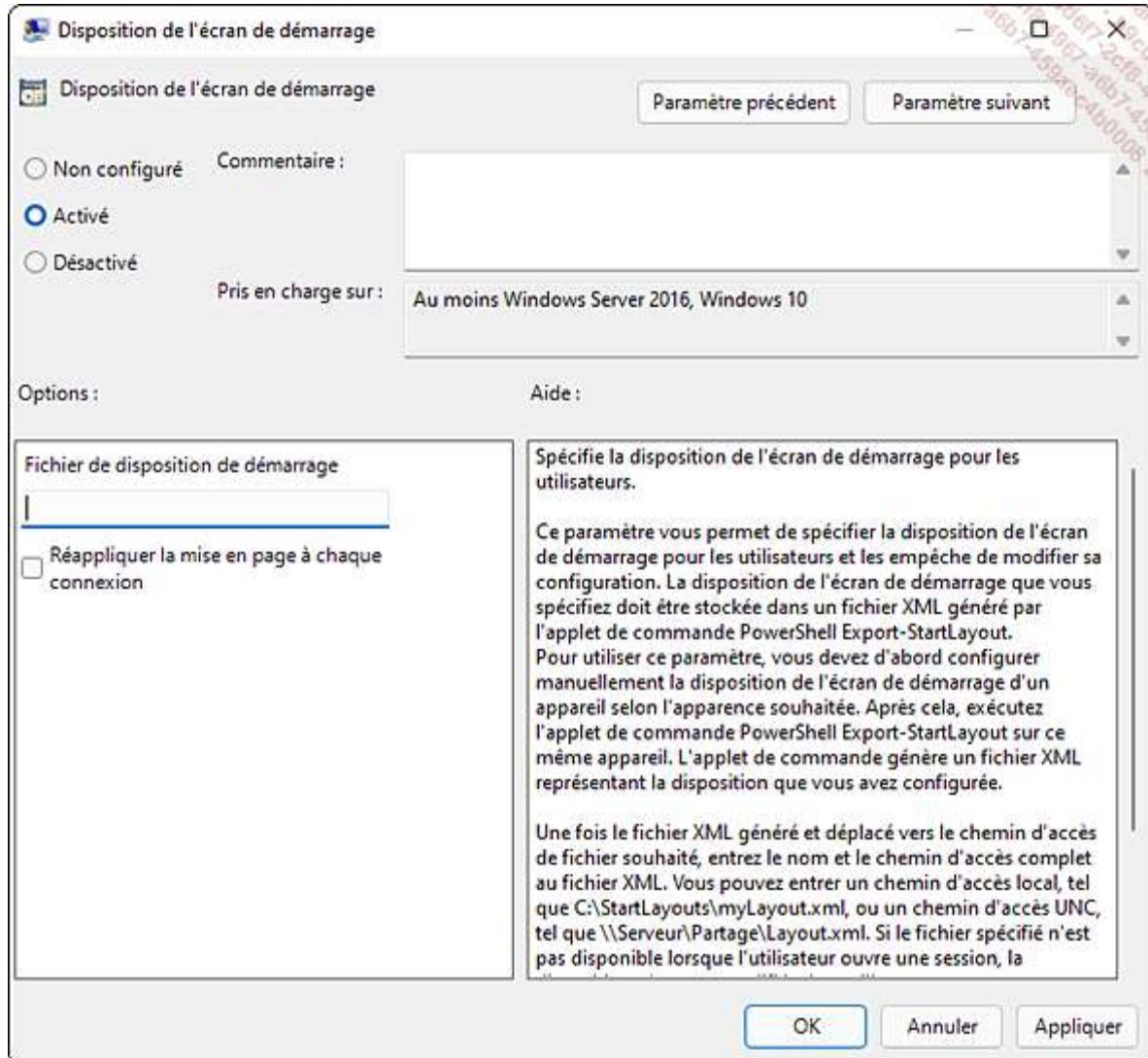
Copiez le fichier sur un partage accessible en lecture aux utilisateurs du domaine Active Directory.

Microsoft propose également un autre format de personnalisation de l'écran de démarrage Windows 11, le format json, compatible avec Microsoft EndPoint Manager. Pour plus d'informations, consultez la page <https://docs.microsoft.com/fr-fr/windows/configuration/customize-start-menu-layout-windows-11>

Depuis la console **Gestion des stratégies de groupe** d'un serveur Windows Server 2012 ou supérieur, sélectionnez un objet de stratégie de groupe existant ou créez-en un nouveau. Modifiez ses paramètres et

développez le noeud **Configuration utilisateur - Stratégies - Modèles d'administration - Menu Démarrer et barre des tâches**, et ouvrez le paramètre **Disposition de l'écran de démarrage**.

Cochez la case **Activé**, puis, dans la zone **Fichier de disposition de démarrage**, entrez le chemin d'accès vers le partage contenant le fichier de configuration XML précédemment généré :



L'administrateur peut forcer la propagation immédiate sur le poste client de l'objet stratégie de groupe configuré à l'aide de la commande suivante exécutée en tant qu'administrateur :

- gpupdate /force

Grâce à cette fonctionnalité en ouvrant une session sur un poste de travail Windows 11 Entreprise du domaine, l'utilisateur ne pourra pas modifier la disposition du menu **Démarrer**.

2. Affichage des applications

L'ergonomie d'une application développée pour tablette tactile devient un élément aussi important que ses fonctionnalités.

Les Apps fournies avec Windows 11 supportent trois affichages : plein écran, milieu d'écran (mais pas taille maximale) et côté à côté. Le mode d'exécution par défaut est milieu d'écran.

Pour changer la résolution actuelle, il suffit de cliquer avec le bouton droit sur le bureau puis de sélectionner **Paramètres d'affichage**.

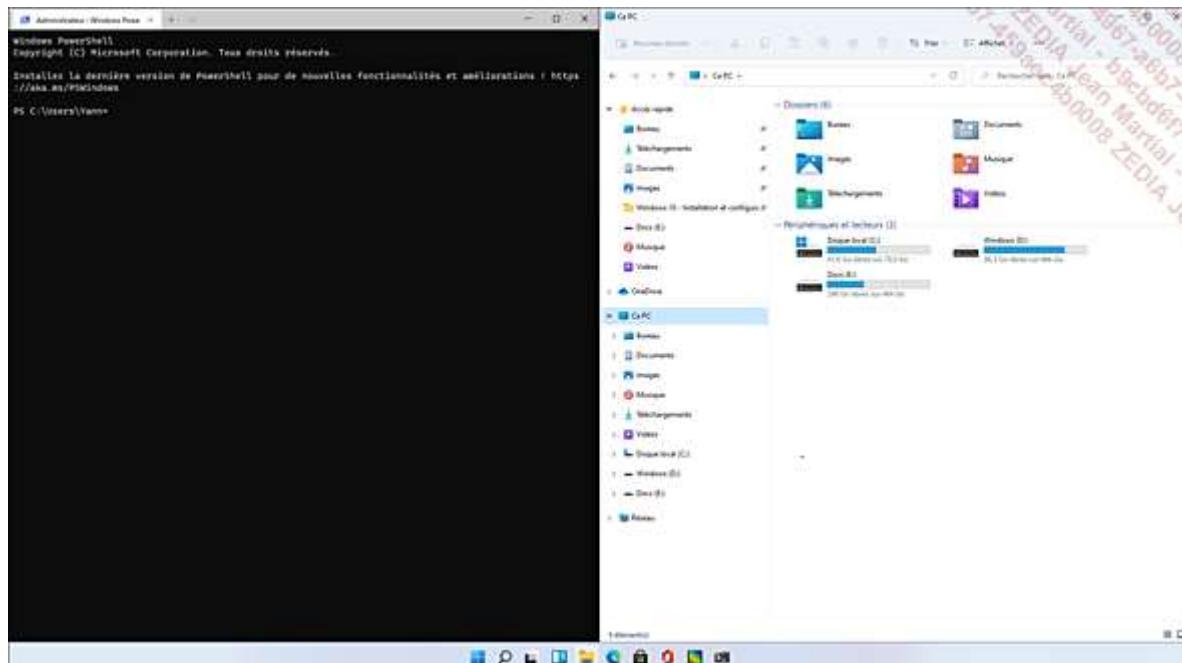
Sélectionnez la résolution optimale (**recommandé**). Après avoir modifié celle-ci, Windows vous demande confirmation quant à son application définitive. En l'absence d'action pendant 15 secondes, les paramètres précédents seront automatiquement restaurés. Cliquez sur **Conserver les modifications**.



La résolution maximale gérée par Windows 11 pour un ordinateur est 8K (7680×4320) sur un écran externe branché, et 4K (3840×2160) pour les tablettes tactiles.

Pour utiliser deux applications côté à côté, il suffit de glisser sans relâcher la fenêtre de l'application vers la gauche ou la droite de l'écran. L'application utilisera la moitié de la surface d'affichage. Un écran de l'autre côté vous proposera de choisir la deuxième application à afficher à côté de la première. Les raccourcis-clavier + [Flèche à droite] et + [Flèche à gauche] permettent d'exécuter la même action.

Dans l'exemple ci-dessous sont affichés côté à côté l'Explorateur de fichiers à droite et une invite de commandes à gauche :

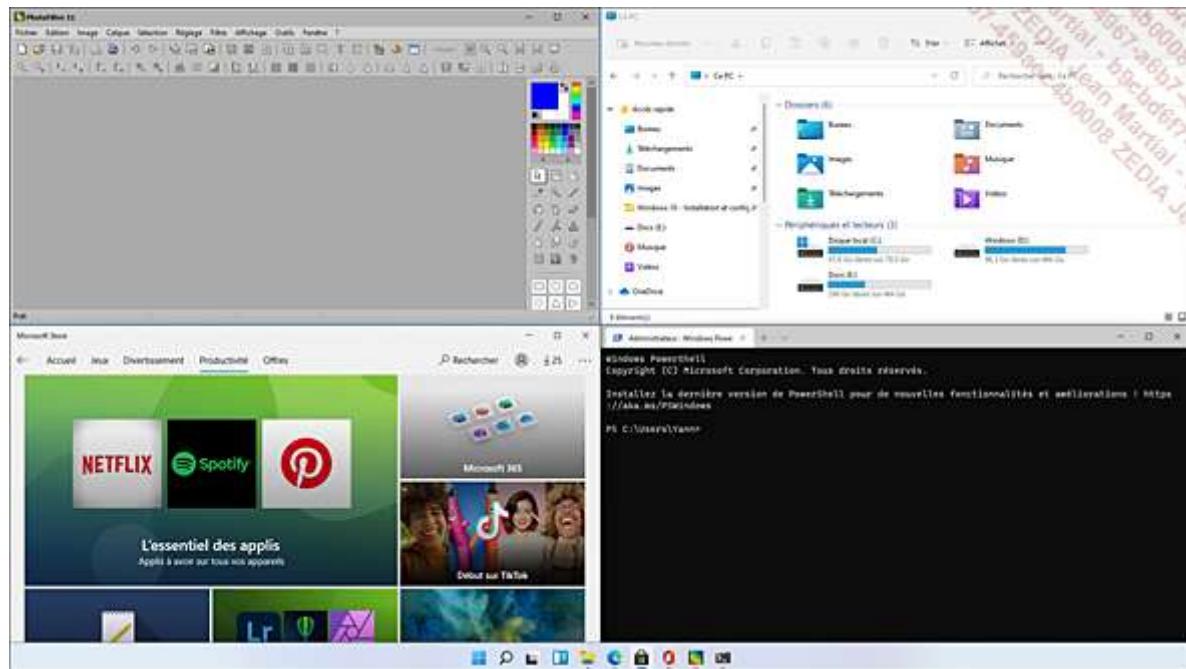


Il est aussi possible d'afficher une application sur un quart de l'écran en appliquant la même procédure que précédemment. Ce mode d'affichage nécessite une résolution minimale de 1024 x 768 pixels.

Pour redimensionner les applications, faites glisser le séparateur vertical ou horizontal représenté par la bordure de fenêtre de celles-ci, ou bien cliquez sur les touches  + haut ou bas.

Si vous exécutez une troisième application, cette dernière s'affichera au-dessus des deux autres.

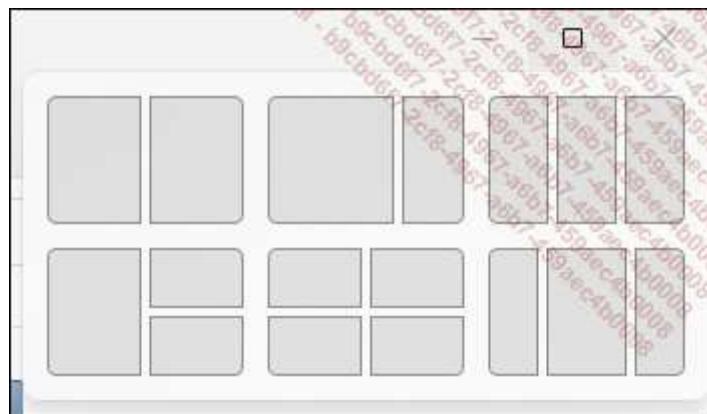
Si vous voulez afficher quatre applications côté à côté, faites glisser successivement les fenêtres vers les angles de l'écran.



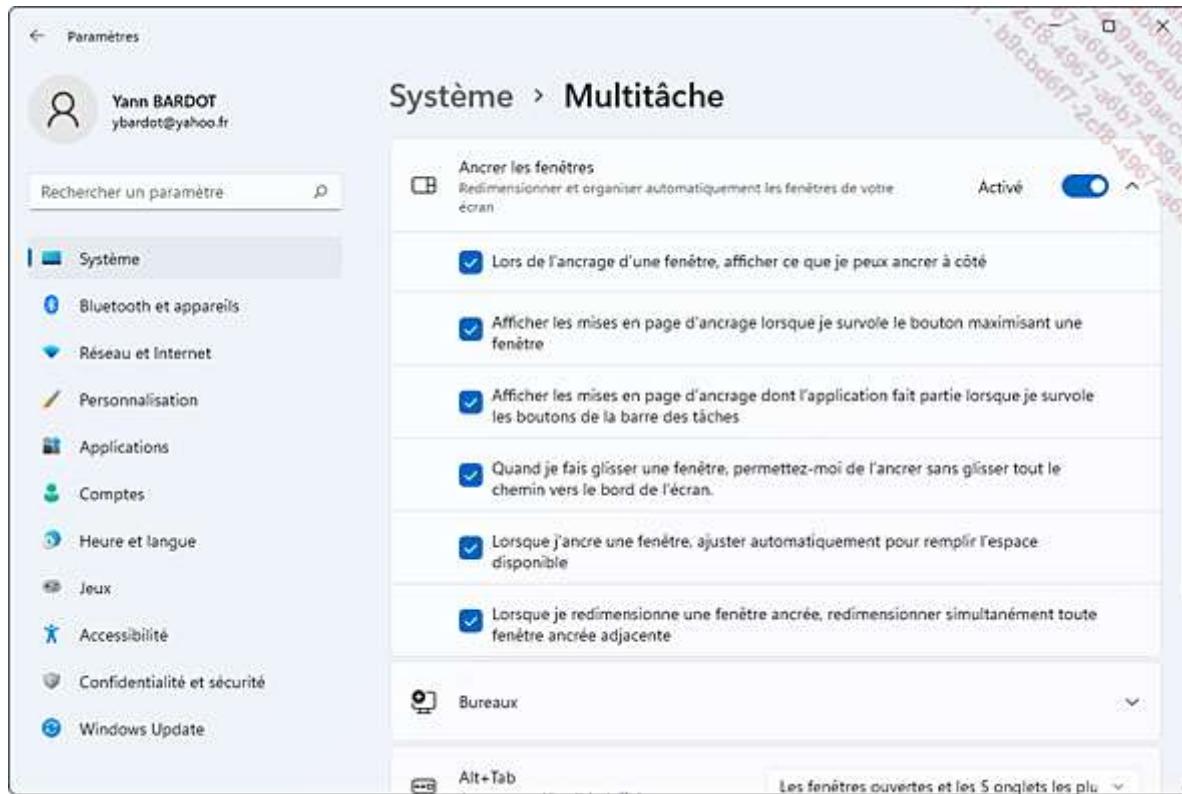
Ainsi, huit applications peuvent être affichées simultanément sur deux écrans, quatre sur chaque écran.

Windows 11 propose une amélioration significative du système d'ancrage des fenêtres avec la fonctionnalité Snap Layouts (Dispositions automatiques), inspirée des Fancy Zones disponibles avec les PowerToys. Cette fonctionnalité propose des dispositions de fenêtres prédéfinies lorsque l'utilisateur survole le bouton d'agrandissement d'une fenêtre. Suivant la résolution ou la taille de votre écran, quatre ou six dispositions seront proposées.

Un clic gauche sur un des modèles permet de disposer automatiquement les fenêtres suivant cet agencement.

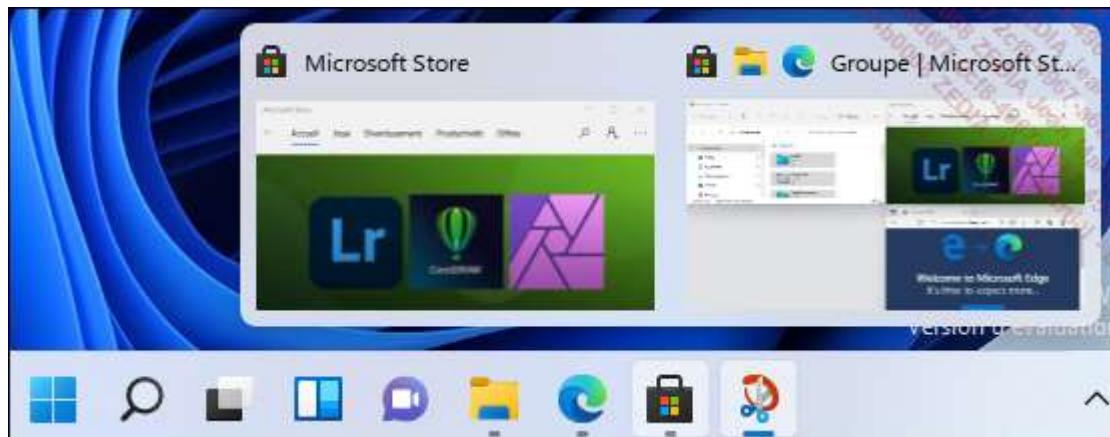


Le comportement de l'ancrage est configurable dans les **Paramètres, Système, Multitâche**.



Lorsque la souris survole, dans la barre des tâches, une application faisant partie d'une disposition automatique, le groupe composé de toutes les applications incluses dans cette disposition apparaît et devient sélectionnable. Il est ainsi plus facile d'afficher en un seul clic un ensemble de fenêtres.

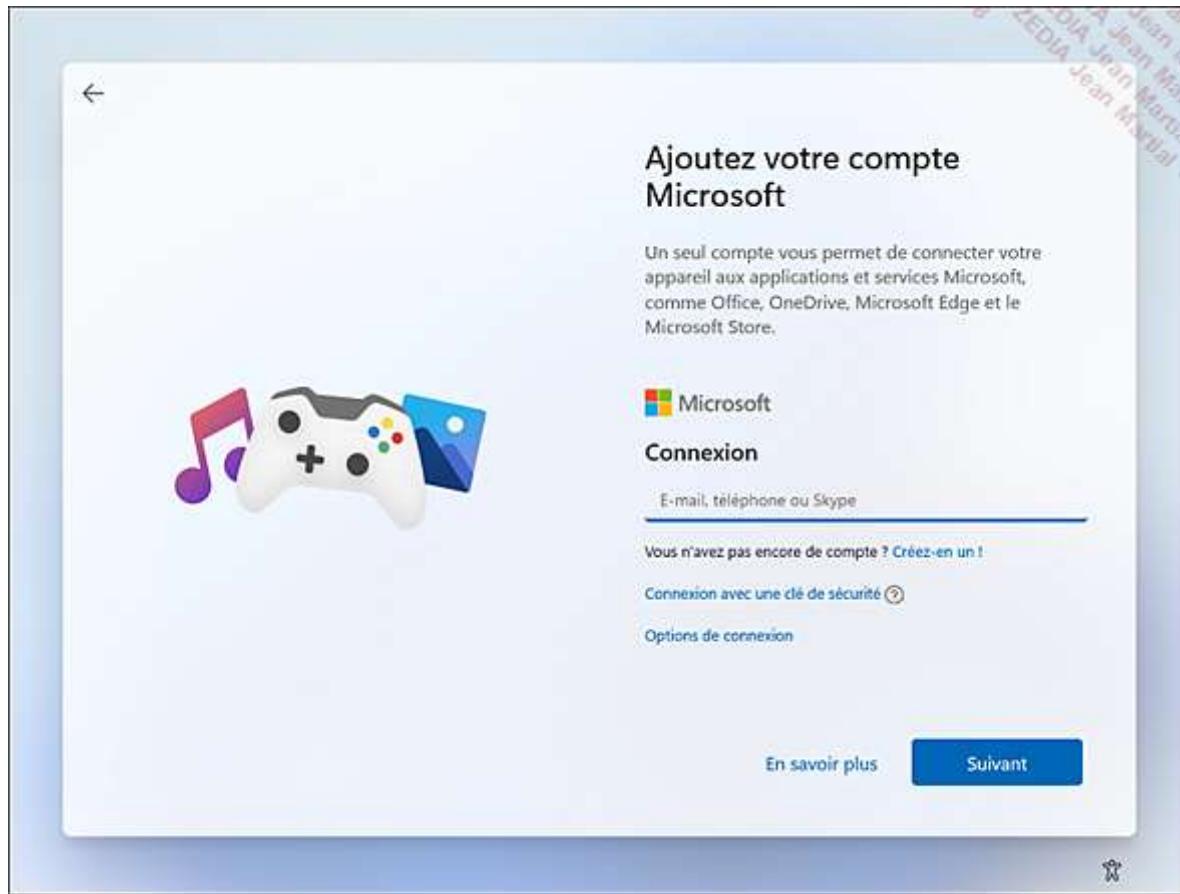
Microsoft a nommé cette fonctionnalité Snap Groups.



3. Barre des tâches

La barre des tâches de Windows 11 est une évolution de celle intégrée à Windows 10. On y retrouve les mêmes fonctionnalités : un menu Démarrer, un champ de recherche, un affichage des tâches et des bureaux virtuels, ainsi que les icônes de raccourcis des applications en cours d'exécution. La partie droite regroupe les notifications et le calendrier. En cliquant sur le coin inférieur droit de l'interface, à droite de l'heure, l'utilisateur peut réduire toutes les fenêtres du bureau afin de n'afficher que ce dernier. Cette action est équivalente au raccourci-clavier + D (D pour Desktop).

La configuration de la barre des tâches est accessible en effectuant un clic avec le bouton droit sur une zone vierge de la barre des tâches, puis **Paramètres de la barre des tâches**.



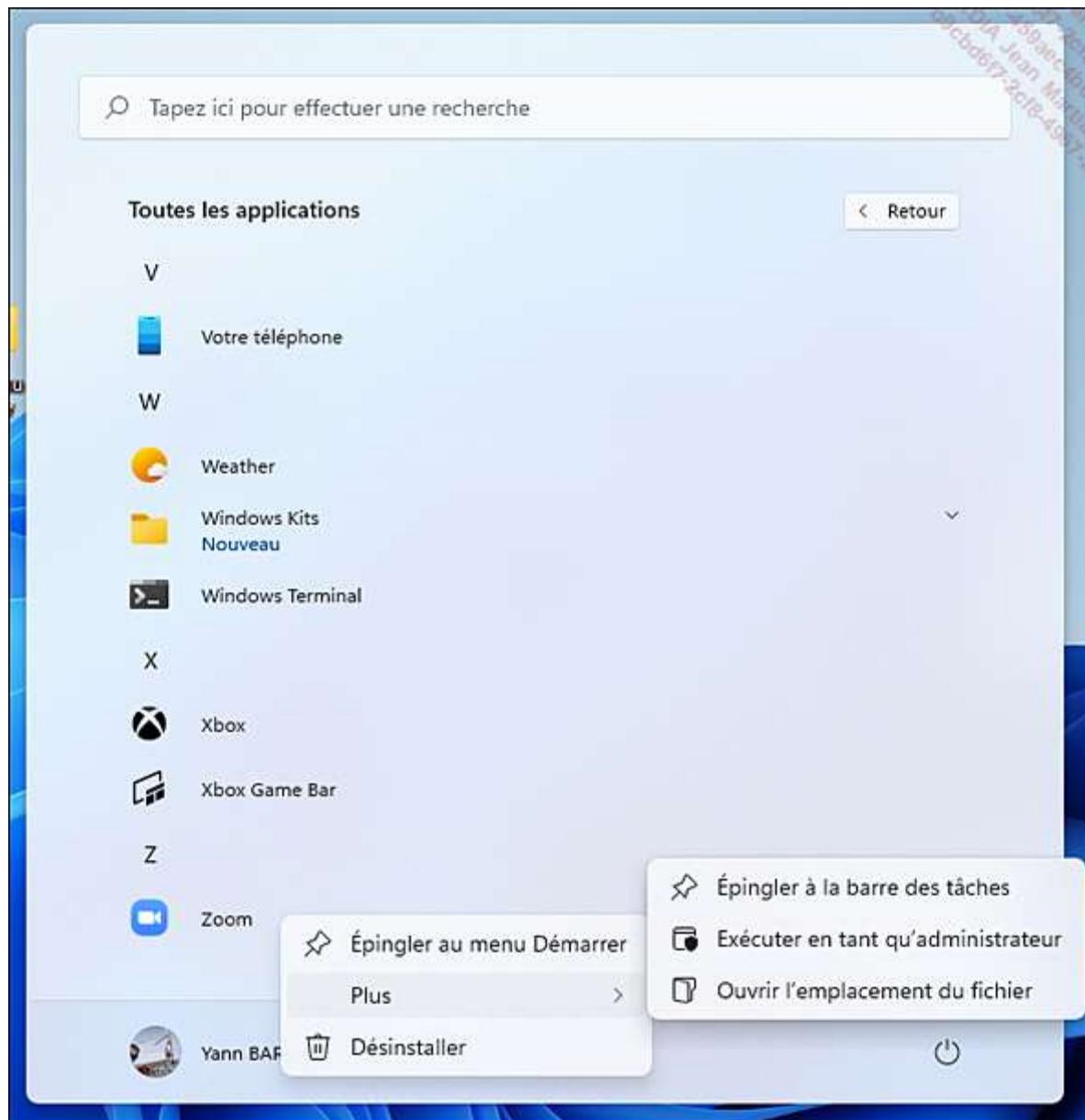
La section **Éléments de la barre des tâches** permet d'afficher ou masquer les boutons des éléments (recherche, tâches, widgets...) qui apparaissent.

La section **Icônes de l'angle de la barre des tâches** autorise ou non l'affichage de certaines icônes spécifiques dans la partie droite (stylet, clavier tactile...).

La section **Dépassement de capacité** permet de définir le comportement et l'affichage des icônes apparaissant dans la partie droite et dans la fenêtre de dépassement. Cela évite de remplir totalement d'icônes la barre des tâches. Les icônes des applications activées apparaîtront directement dans la barre des tâches tandis que les autres seront accessibles en déroulant le menu. Cette section correspond à l'ancien menu **Sélectionner les icônes à afficher dans la barre des tâches**.

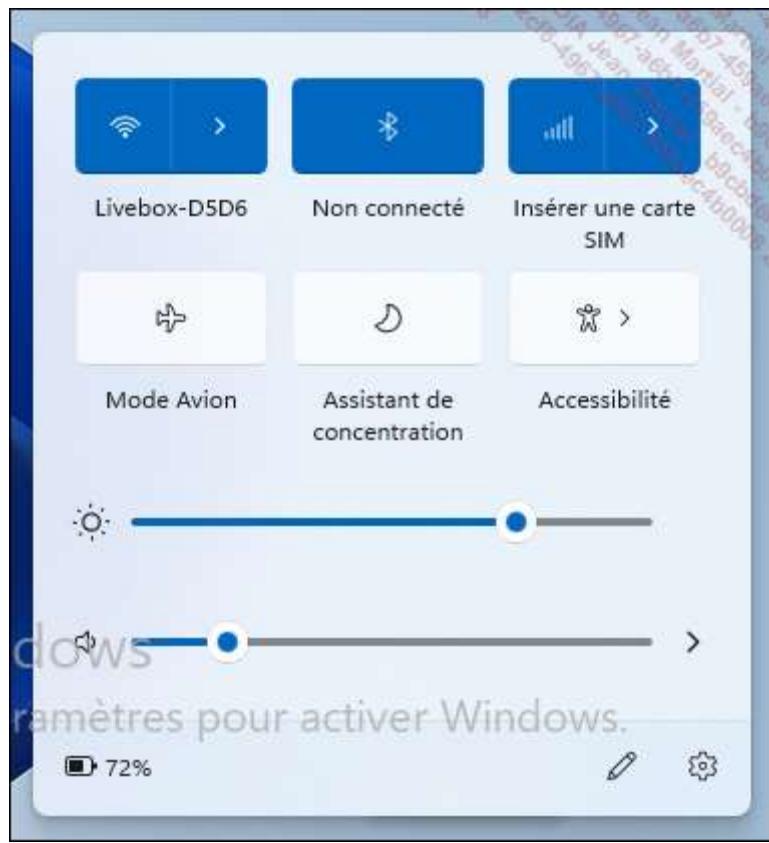
La section **Comportement de la barre des tâches** permet de gérer l'alignement de celle-ci (centré ou gauche), de la masquer, de l'afficher sur plusieurs écrans... Par contre, il n'est plus possible de définir sa position sur le bureau (droite, haut...).

Microsoft simplifie l'accès de l'utilisateur à ses ressources en lui donnant la possibilité d'épingler ses applications préférées sur la barre des tâches. Par exemple, depuis le menu Démarrer, faites un clic droit sur une application (menu contextuel), cliquez sur **Plus**, puis sur **Epingler à la barre des tâches**. Un nouveau bouton apparaîtra à la droite des précédents.

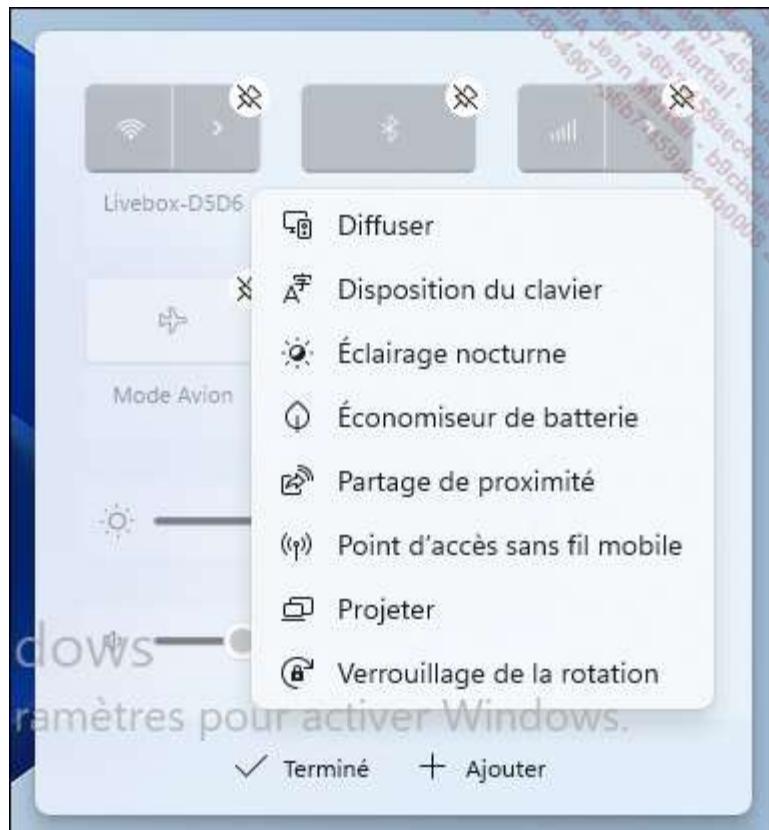


Pour supprimer de la barre des tâches une application ajoutée précédemment, faites un clic droit sur son icône et cliquez sur **Détacher de la barre des tâches**.

Les Paramètres rapides ont été séparés du Centre de notifications. Le panneau des Paramètres rapides a évolué dans sa présentation. Il a été épuré et affiche les informations primordiales (Wi-Fi, Assistant de concentration...) d'un simple clic.



L'utilisateur peut modifier les éléments présents en cliquant sur le stylo et le bouton **Ajouter**. Il peut alors rendre d'autres paramètres faciles d'accès parmi ceux proposés. Il a également la possibilité d'enlever les paramètres qui ne lui sont pas utiles, en cliquant sur l'épingle barrée dans le coin supérieur droit de chaque paramètre rapide.

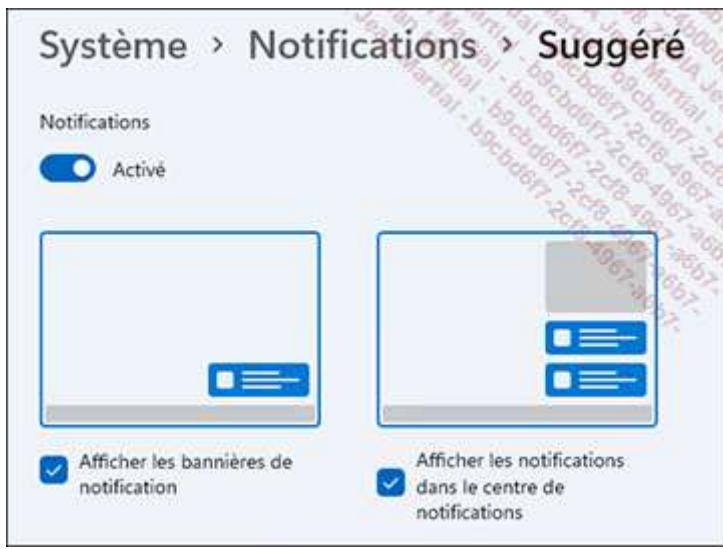


Le Centre de notifications a lui aussi subi un lifting pour rester en accord avec le nouveau thème de Windows 11. Il est désormais affiché avec le calendrier. Un clic avec le bouton gauche sur l'horloge affiche le calendrier et les notifications.



Il est possible de développer le calendrier en cliquant sur l'icône associée. L'Assistant de concentration est accessible très facilement avec le lien présent au-dessus des notifications.

Les paramètres de notifications sont configurables en cliquant sur l'icône "..." (trois points) d'une notification ou en ouvrant les **Paramètres, Système, Notifications**. Pour chaque application, il est possible de paramétrier le mode d'affichage des notifications : sous forme de bannières ou dans le Centre de notifications.



4. Zone de recherche

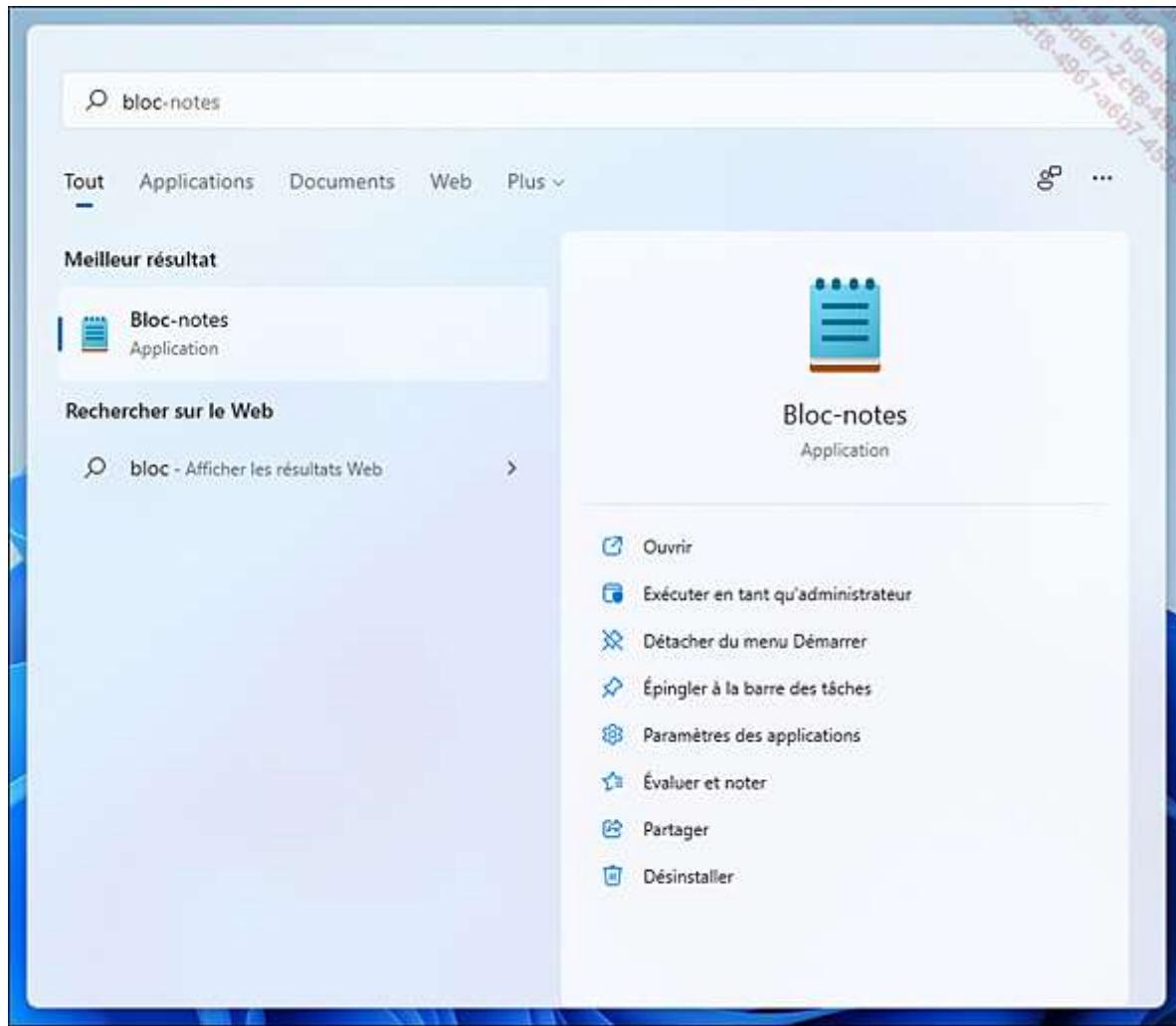
Microsoft fournit avec Windows 11 une barre de recherche située dans la barre des tâches, accessible en cliquant



sur l'icône , ou encore en appuyant sur la touche  du clavier et en saisissant les premières lettres de l'application recherchée.

Elle est multifonction, offrant la possibilité de trouver une application, un fichier ou encore une page web.

Ainsi, pour exécuter l'application Bloc-notes, il suffit de taper bloc dans la zone de recherche. Notez qu'un ensemble de résultats sont proposés à l'utilisateur, tels qu'un dossier local possédant les caractères recherchés, une recherche web avec le moteur de recherche Bing, ou encore des paramètres de l'ordinateur.



5. Assistante vocale Cortana

Cortana est une assistante vocale (nécessitant donc un microphone) aidant l'utilisateur à effectuer des recherches sur son PC ou le Web, à gérer son calendrier, mais pouvant également discuter ou encore raconter des blagues... L'assistante enregistre les propos et habitudes de l'utilisateur afin de lui fournir une expérience personnalisée, en étant connectée à Internet pour un résultat optimal.

Suite au manque de succès rencontré ces dernières années par cette assistante, Microsoft a réorienté l'outil en ciblant les professionnels avec pour but l'amélioration de leur productivité. Ainsi, Cortana n'est plus activée par défaut sur Windows 11 et perd certaines fonctionnalités grand public, comme la gestion des appareils connectés (domotique) ou le lancement de fichiers musicaux.

Désormais, Cortana est une assistante de productivité intégrée dans la suite Microsoft 365. Elle permet de mieux gérer les tâches, l'agenda, de rechercher des personnes et des fichiers, d'interagir avec des courriers électroniques, le tout... en anglais pour le moment. Côté français, l'assistante vocale permet de faire des recherches en utilisant le moteur Bing, de traduire des mots et expressions...

Il est néanmoins possible d'activer et d'utiliser Cortana, même si l'assistante est désactivée par défaut. Pour cela, il faut posséder un compte Microsoft. Pour activer Cortana, suivez la procédure ci-dessous :

Saisissez cortana dans la zone de recherche située dans la barre des tâches, puis cliquez sur **Cortana**.

Cliquez sur **Se connecter** et utilisez votre compte Microsoft pour vous identifier.

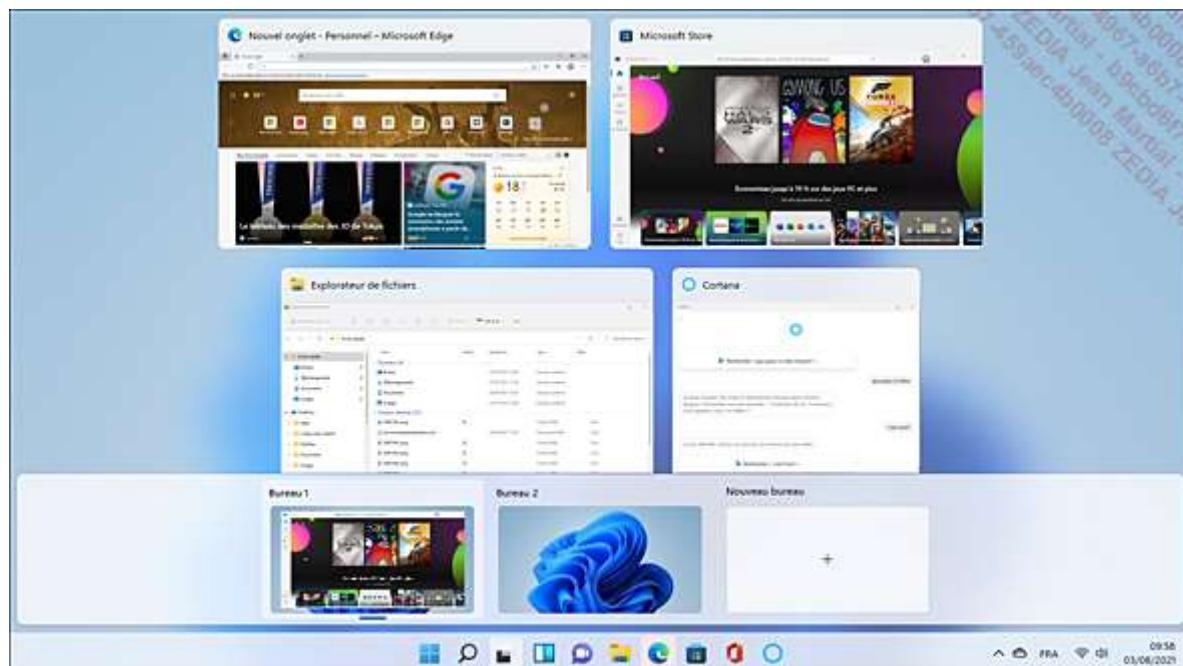
Acceptez que Cortana utilise votre localisation pour affiner le résultat de ses recherches si nécessaire.

Notez que Cortana n'est pas disponible dans tous les pays, et certaines de ses fonctionnalités peuvent ne pas être présentes selon les langues qu'elle gère.

6. Bureau virtuel

Un bureau virtuel permet à tout un chacun de mieux organiser les nombreuses fenêtres en démultipliant son environnement : ainsi, vous pouvez créer un bureau pour les recherches internet, un autre pour les tâches bureautiques (Word, Excel) et un autre pour les jeux. De cette manière, chaque application d'un type différent ne sera plus mélangée avec les autres.

La notion de bureau virtuel est intégrée de manière intuitive à Windows 10 avec l'icône **Affichage des tâches** , présente dans la barre des tâches. En cliquant sur cette icône, le centre de l'écran affiche alors les applications en cours d'utilisation du bureau virtuel courant. Le raccourci-clavier  + [Tab] lance la même action.



Les vignettes des applications s'affichent. Un clic sur l'une d'entre elles permet d'y accéder directement. Notez la présence de deux bureaux virtuels par défaut, dans la partie inférieure de l'écran.

En cliquant sur **Nouveau bureau**, un utilisateur peut créer un nouveau bureau virtuel. Le raccourci-clavier  + [Ctrl] + D effectue la même action.

Naviguer d'un bureau virtuel à un autre s'effectue en cliquant/pointant sur l'icône **Affichage des tâches** ou bien en utilisant les raccourcis-clavier  + [Ctrl] + [Flèche à gauche] ou  + [Ctrl] + [Flèche à droite].

Il est possible de fermer le bureau virtuel en cours de deux manières : avec la combinaison de touches  + [Ctrl] + [F4] ou bien en cliquant/pointant sur l'icône **Affichage des tâches** puis sur le bouton **Fermer**  du bureau virtuel cible.



À noter que les applications qui composent ce bureau virtuel (Bureau 2 dans notre exemple) ne seront pas fermées mais transférées dans le bureau virtuel de départ.

a. Gestion d'un écran connecté

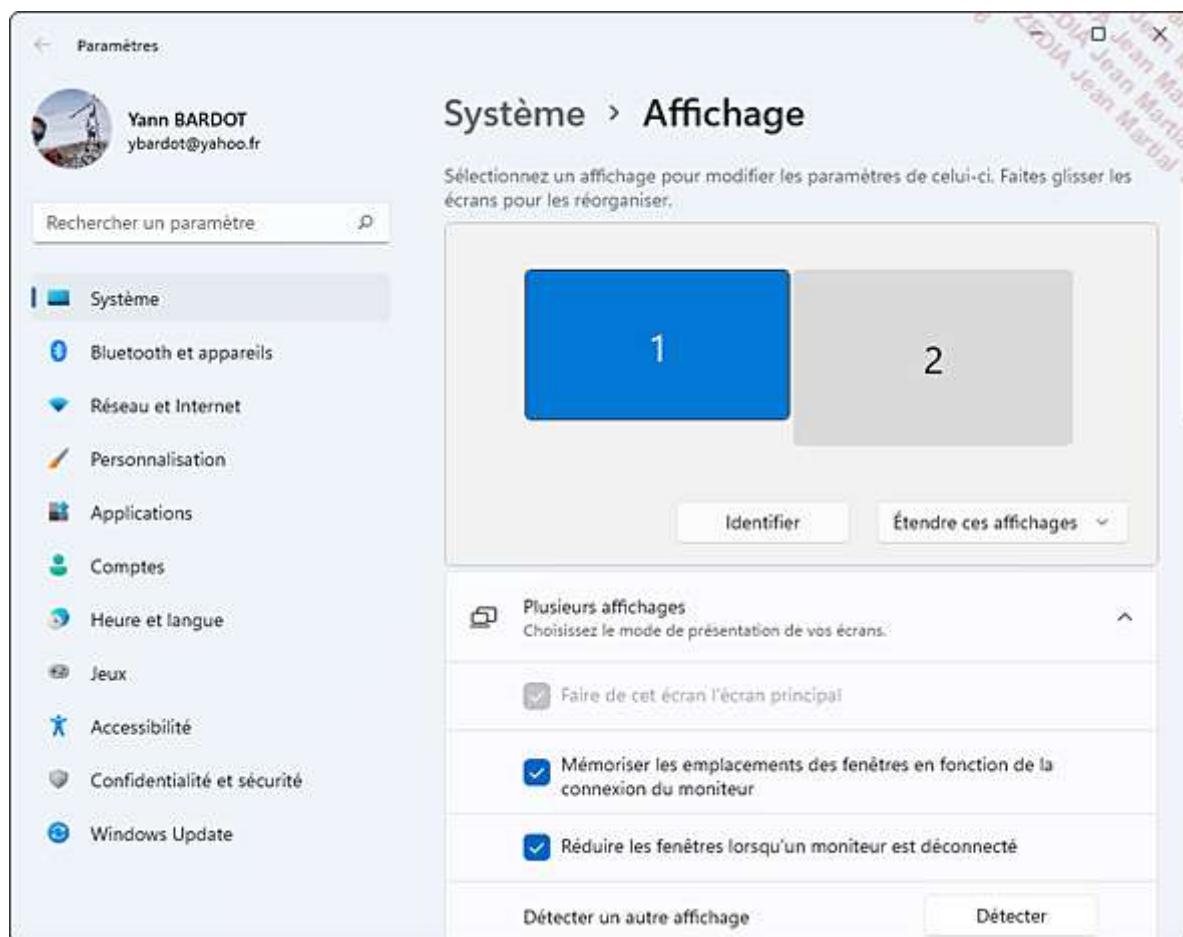
Utiliser un second écran permet de visualiser simultanément plusieurs applications. La connexion d'un projecteur affichera par exemple une présentation face à plusieurs personnes.

Windows 11 gère les ports HDMI (*High-Definition Multimedia Interface*), DVI (*Digital Visual Interface*) et VGA (*Video Graphics Array*), ainsi que les écrans connectés via un réseau.

Si l'utilisateur utilise deux écrans, la barre des tâches peut être étendue sur toute la superficie du bureau et les applications de chaque écran peuvent être positionnées au choix.

Pour modifier les paramètres d'affichage lors du branchement d'un écran supplémentaire, effectuez les opérations suivantes :

Cliquez avec le bouton droit sur le bureau et sélectionnez **Paramètres d'affichage**. Cliquez ensuite sur **Affichage**.



En cliquant sur le bouton **Identifier**, un numéro d'écran s'affiche sur l'écran principal et sur celui raccordé à l'ordinateur Windows 11. L'utilisateur peut aussi déclencher manuellement la détection d'écrans ou encore se connecter à un affichage sans fil compatible. Il est ensuite possible de les déplacer avec la souris pour les positionner sur la gauche, la droite, au-dessus ou en-dessous l'un de l'autre.

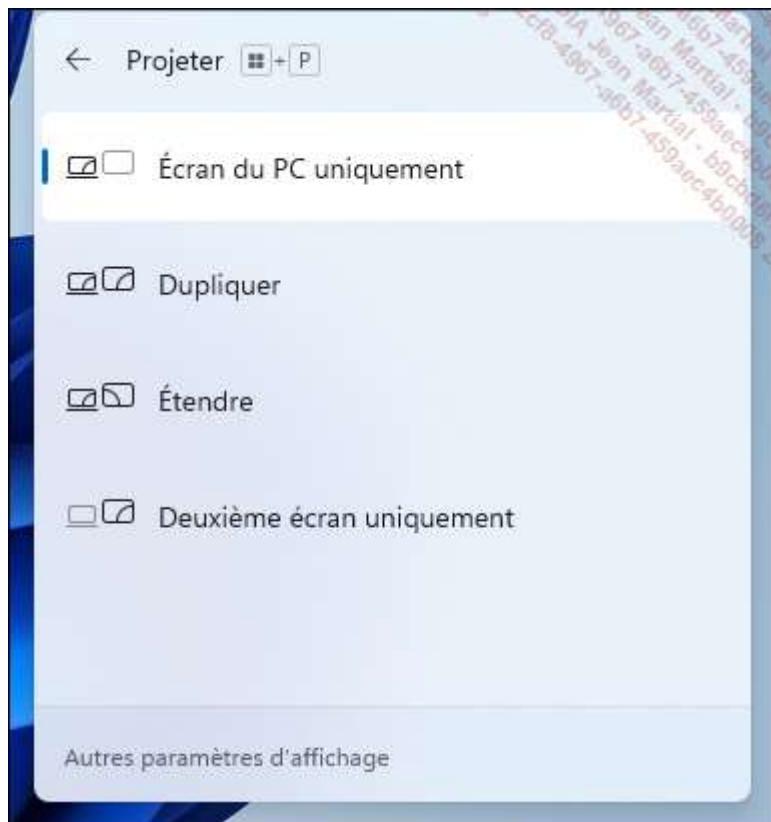
La liste déroulante permet de choisir le mode de présentation, c'est-à-dire ce que l'on veut afficher sur l'écran secondaire : rien du tout, la même chose que sur l'écran 1 ou étendre le bureau sur les deux écrans.

En déroulant le menu **Plusieurs affichages**, l'option **Mémoriser les emplacements des fenêtres en fonction de la connexion du moniteur** apparaît. Elle favorise l'ergonomie et la productivité en permettant de réaffecter

les fenêtres à l'écran sur lequel elles étaient affichées auparavant, suite par exemple à un débranchement/rebranchement d'un écran, typiquement lorsqu'un utilisateur déconnecte son écran fixe de son ordinateur portable pour se déplacer (réunion, rendez-vous...) puis le rebranche en revenant à son bureau.

Le raccourci-clavier  + P permet d'accéder rapidement au mode de présentation. La commande DisplaySwitch.exe, disponible dans le dossier %windir%\System32\, permet de changer les paramètres d'affichage dans une invite de commandes. Par exemple, le paramètre /extend étend le bureau de l'utilisateur au deuxième écran connecté, alors que /clone affiche l'interface Windows 11 de manière identique sur les deux écrans.

À l'utilisation de cette commande ou du raccourci-clavier, un panneau apparaît sur le côté droit de l'interface :



Cet écran de configuration est également accessible depuis les paramètres rapides, situées à gauche de l'heure dans la barre des tâches, puis en cliquant sur **Projeter** si l'icône a été ajoutée.

Lorsqu'un écran sans-fil est connecté au poste de travail via le réseau, une barre située en haut de l'écran permet de gérer la connexion/déconnexion et propose trois modes optimisés : Jeu, Productivité et Vidéo. Ainsi, en mode Jeu, la latence sera minimale pour éviter les ralentissements.

La manière d'afficher la barre des tâches du bureau sur les différents écrans peut être configurée en effectuant un clic avec le bouton droit sur celle-ci, puis en cliquant sur **Paramètres de la barre des tâches**. Par défaut, la barre des tâches est positionnée sur tous les écrans. En cliquant sur le menu déroulant **Comportement de la barre des tâches**, l'utilisateur peut choisir :

- d'afficher sur tous les écrans en cochant **Afficher ma barre des tâches sur tous les affichages** ;
- d'afficher les boutons des applications sur une ou plusieurs barres des tâches, en fonction de l'écran sur lequel l'application est ouverte.

The screenshot shows the Windows Settings application with the following interface details:

- Header:** Personnalisation > Barre des tâches
- Left sidebar:** Rechercher un paramètre, Système, Bluetooth et appareils, Réseau et Internet, Personnalisation (selected), Applications, Comptes, Heure et langue, Jeux, Accessibilité, Confidentialité et sécurité, Windows Update.
- Right pane title:** Comportements de la barre des tâches
- Right pane content:**
 - Alignement de la barre des tâches: Centre (dropdown menu)
 - Masquer automatiquement la barre des tâches
 - Afficher les badges (compteurs de messages non lus) sur les applications de la barre des tâches
 - Afficher ma barre des tâches sur tous les affichages
 - Afficher les recherches récentes lorsque je pointe sur l'icône de recherche
 - En cas d'utilisation de plusieurs affichages, afficher les applications de ma barre des tâches: Toutes les barres des tâches (dropdown menu)
 - Sélectionnez le coin éloigné de la barre des tâches pour afficher le bureau
- Bottom right buttons:** Obtenir de l'aide, Envoyer des commentaires

b. Gestion des langues

Dans les anciennes versions de Microsoft Windows, le changement de la langue de l'interface s'effectuait lors de l'installation des mises à jour facultatives, et ceci uniquement pour des versions spécifiques du système d'exploitation.

La grande majorité des utilisateurs utilisaient la langue sélectionnée lors de la phase d'installation de l'ordinateur.

Désormais, il est très simple d'ajouter ou de supprimer des langues une fois Windows 11 installé. Par exemple, pour installer la langue Français (Suisse), réalisez les opérations suivantes :

Dans la zone de recherche située dans la barre des tâches, saisissez **Ajouter une langue** et sélectionnez **Ajouter une langue à cet appareil**. Le panneau des **Paramètres** s'ouvre. Cliquez sur **Langue et région**.

The screenshot shows the Windows Settings application with the following interface details:

- Header:** Heure et langue > Langue et région
- Left sidebar:** Rechercher un paramètre, Système, Bluetooth et appareils, Réseau et Internet, Personnalisation, Applications, Comptes, Heure et langue (selected), Jeux, Accessibilité, Confidentialité et sécurité, Windows Update.
- Right pane sections:**
 - Langue:**
 - Langue d'affichage de Windows: Français (France)
 - Langues préférées: Français (France), Espagnol (Équateur)
 - Ajouter une langue
 - Region:**
 - Pays ou région: France
 - Format régional: Nos recommandations
 - Paramètres associés:** Saisie

La vue principale affiche les langues activées sur votre système ainsi que les paramètres régionaux et de saisie.

Cliquez sur **Ajouter une langue** et saisissez **Suisse** puis cliquez sur **Français (Suisse)** et validez en cliquant sur les boutons **Suivant** et **Installer**. Notez que la partie voix est aussi téléchargée.

Choisir une langue à installer

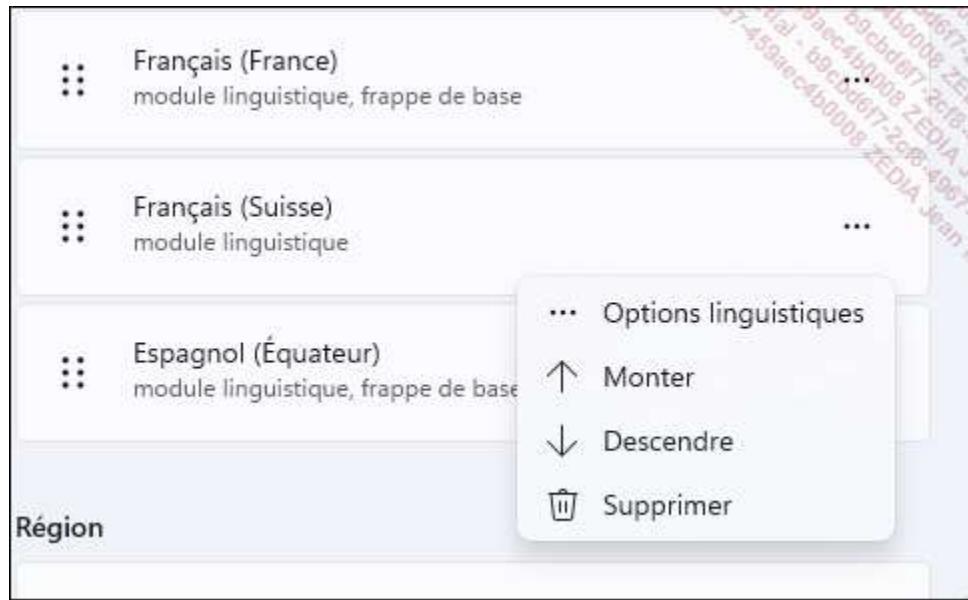
suiss| X

Deutsch (Schweiz)			
Allemand (Suisse)			
Elsässisch			
Alsacien			
English (Switzerland)			
Anglais (Suisse)			
Français (Suisse)			
Français (Suisse)			
Italiano (Svizzera)			
Italien (Suisse)			
Português (Suíça)			
Portugais (Suisse)			
Walser (Schwiz)			

Langue d'affichage Conversion de texte par synthèse vocale
 Reconnaissance vocale Écriture manuscrite

Suivant **Annuler**

La langue est téléchargée sous la forme d'une mise à jour puis installée. Elle est désormais visible dans la vue principale. L'utilisateur peut ensuite cliquer sur "..." (trois points) et sur les flèches haut et bas pour définir la langue par défaut et la priorité donnée aux autres langues.



La bascule entre deux langues se fait rapidement avec les touches +[Espace] ou en cliquant sur l'icône des langues placée à droite dans la barre des tâches.

7. Mouvements tactiles

Comme son prédécesseur, Windows 11 est un système d'exploitation hybride : il convient aussi bien aux ordinateurs pourvus d'un clavier et d'une souris qu'aux tablettes tactiles et ce quelle que soit l'édition. Les principales actions ne nécessitent que deux doigts ; néanmoins, le matériel qui embarquera le nouveau système de Microsoft devra supporter au minimum cinq doigts grâce à une gestion multipoint.

Comme nous allons le voir, le balayage depuis le bord gauche ou droit de l'écran joue un rôle prépondérant dans l'utilisation du système.

Pour vérifier les paramètres tactiles de votre matériel, suivez la procédure ci-dessous :

Cliquez sur le menu **Démarrer** puis sur **Paramètres** et sur **Système**. Pointez sur **Informations système**. Vérifiez le champ **Stylet et fonction tactile**.

← Paramètres

 Yann BARDOT
ybardot@yahoo.fr

Rechercher un paramètre

Système > **Informations système**

WIN11ENT
20HCT01WW

Renommer ce PC

Système

- Bluetooth et appareils
- Réseau et Internet
- Personnalisation
- Applications
- Comptes
- Heure et langue
- Jeux
- Accessibilité
- Confidentialité et sécurité
- Windows Update

Spécifications de l'appareil

Nom de l'appareil	WIN11ENT
Processeur	Intel(R) Core(TM) i5-7300U CPU @ 2.60GHz 2.71 GHz
Mémoire RAM installée	8.00 Go (7.84 Go utilisable)
ID de périphérique	24322746-F4BA-4A44-B388-DC67D79F98F4
ID de produit	00329-00000-00003-AA344
Type du système	Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile	Prise en charge du stylet et de la fonction tactile avec 10 points de contact

Copier

Liens connexes Domaine ou groupe de travail Protection du système

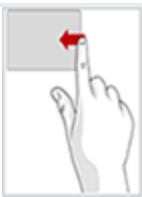
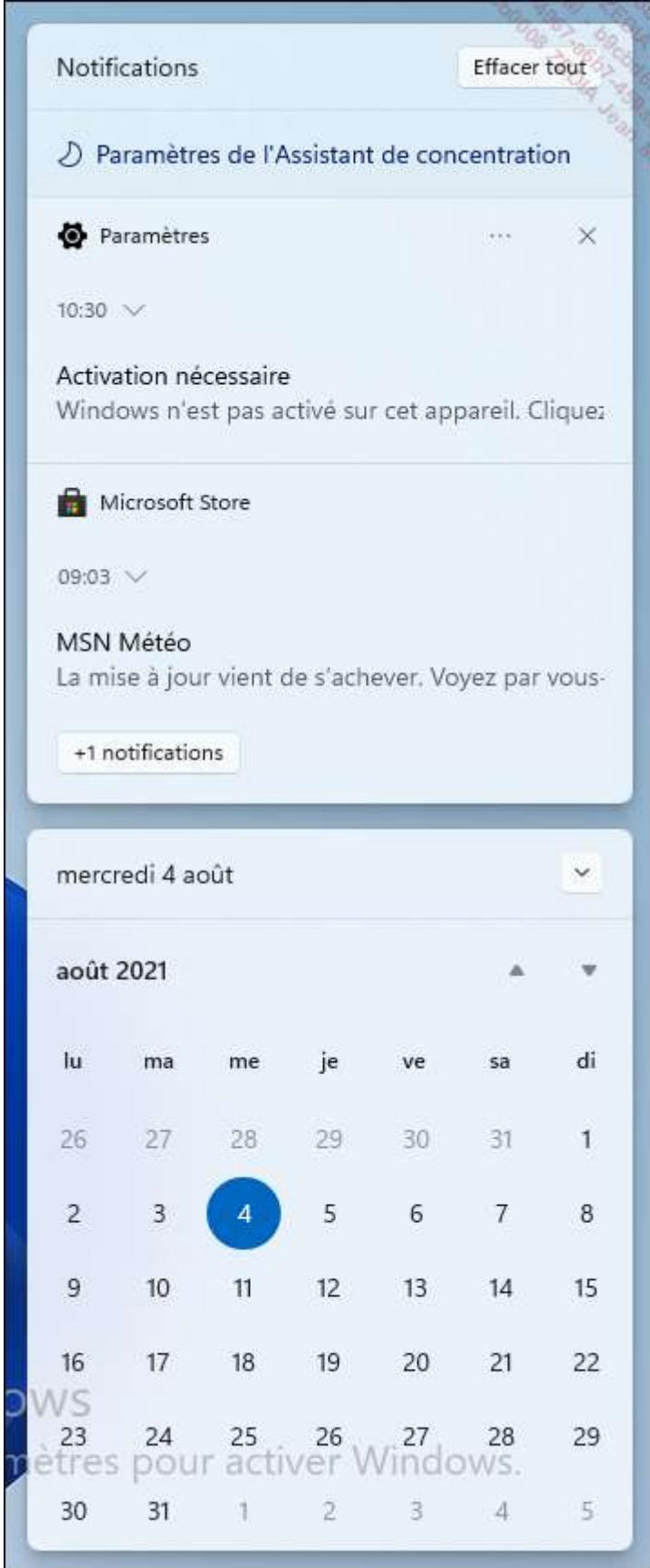
Paramètres avancés du système

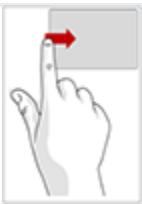
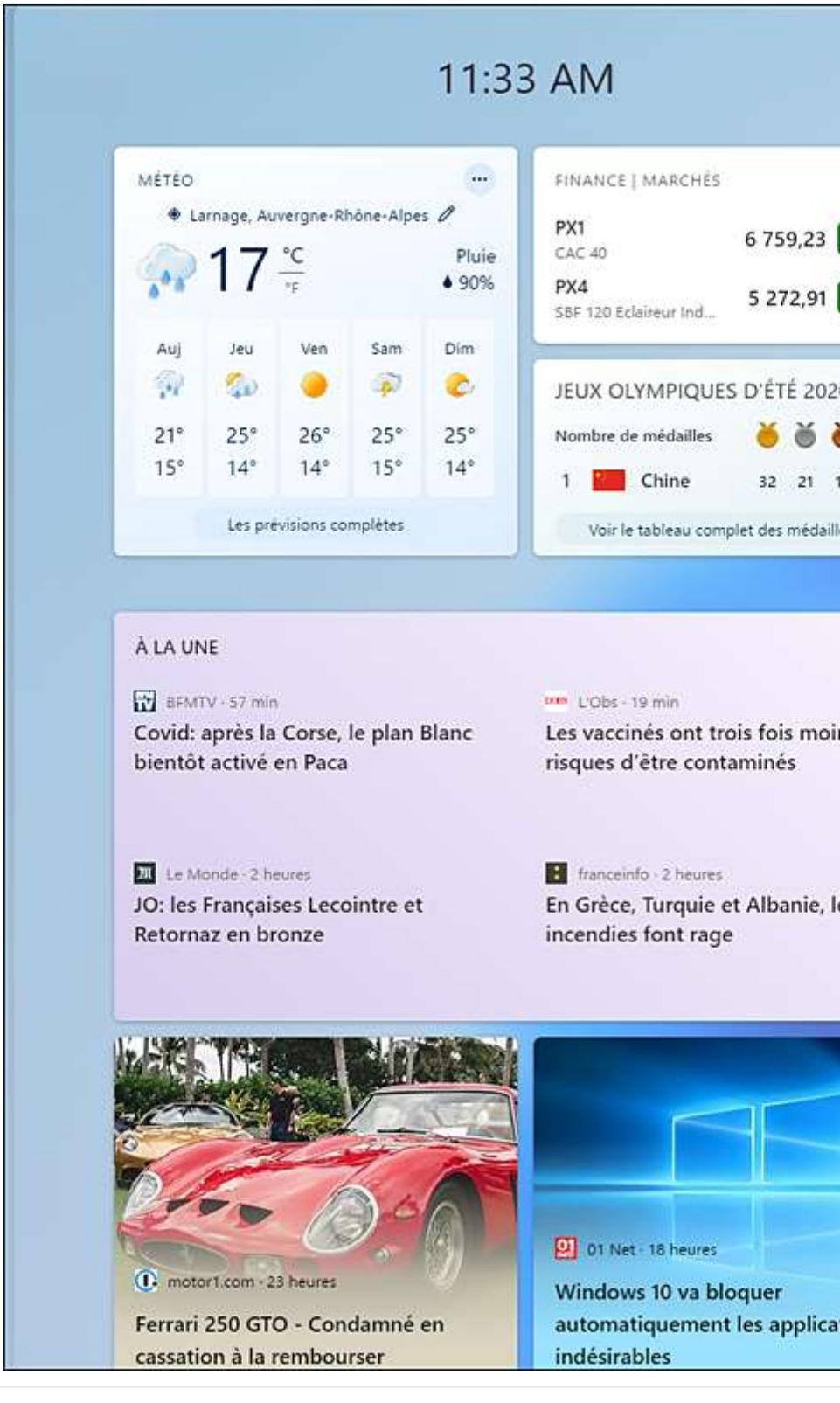
Spécifications de Windows

Édition	Windows 11 Entreprise
Version	21H2

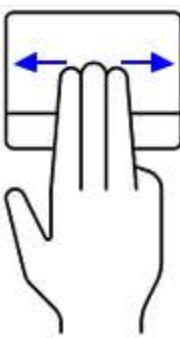
Copier

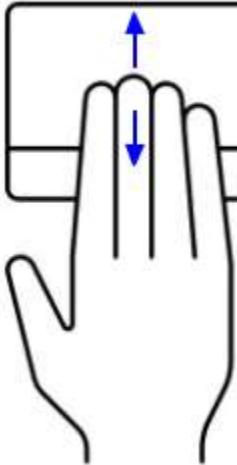
La liste des actions réalisables avec les doigts est affichée dans le tableau ci-dessous :

Manipulation	Résultat	Aperçu																																																	
	En partant du bord droit de l'écran, le balayage affiche les notifications et le calendrier.	 <p>Notifications</p> <p>Effacer tout</p> <p>Paramètres de l'Assistant de concentration</p> <p>Paramètres</p> <p>10:30</p> <p>Activation nécessaire Windows n'est pas activé sur cet appareil. Cliquez</p> <p>Microsoft Store</p> <p>09:03</p> <p>MSN Météo</p> <p>La mise à jour vient de s'achever. Voyez par vous-</p> <p>+1 notifications</p> <p>mercredi 4 août</p> <p>août 2021</p> <table border="1"> <thead> <tr> <th>lu</th><th>ma</th><th>me</th><th>je</th><th>ve</th><th>sa</th><th>di</th></tr> </thead> <tbody> <tr> <td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td>1</td></tr> <tr> <td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr> <tr> <td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr> <tr> <td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td></tr> <tr> <td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td></tr> <tr> <td>30</td><td>31</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr> </tbody> </table>	lu	ma	me	je	ve	sa	di	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5
lu	ma	me	je	ve	sa	di																																													
26	27	28	29	30	31	1																																													
2	3	4	5	6	7	8																																													
9	10	11	12	13	14	15																																													
16	17	18	19	20	21	22																																													
23	24	25	26	27	28	29																																													
30	31	1	2	3	4	5																																													

Manipulation	Résultat	Aperçu
	En partant du bord gauche de l'écran, le balayage affiche le panneau des widgets.	
	L'appui sur un élément déclenche son action principale (exécution)	

Manipulation	Résultat	Aperçu
	d'une application).	
	L'appui prolongé affiche des informations didactiques (menu contextuel).	
	Pincer puis écarter les doigts pour effectuer un zoom avant. Équivalent du maintien de la touche [Ctrl] du clavier, tout en utilisant la molette de défilement de sa souris. Un zoom dans une application telle que Microsoft Edge ou Microsoft Word est donc possible.	
	Pincer puis rapprocher les doigts pour effectuer un zoom arrière. Équivalent du maintien de la touche [Ctrl] du clavier, tout	

Manipulation	Résultat	Aperçu
	en utilisant la molette de défilement de sa souris.	
	Déplacement horizontal ou vertical sur l'écran. Équivalent de l'utilisation du maintien du bouton gauche de la souris puis d'un déplacement.	
	Effectuer un mouvement de rotation avec deux doigts pour faire pivoter l'écran.	
	Glisser un doigt sur l'écran pour faire défiler son contenu.	
	Un appui avec trois doigts et un déplacement vers la droite ou vers la gauche bascule vers l'application	

Manipulation	Résultat	Aperçu
	<p>précédemment utilisée. Équivalent à [Alt] + [Tab].</p> <p>Un appui avec trois ou quatre doigts et un déplacement vers le bas ou le haut permet de réduire toutes les applications actives et de voir le bureau ou de repositionner les applications et masquer le bureau.</p> <p>Équivalent à  + D.</p>	
	<p>Un appui avec quatre doigts et un déplacement vers la droite ou la gauche permet de naviguer entre les bureaux virtuels.</p>	

Il est possible de modifier ce fonctionnement depuis les **Paramètres**, **Bluetooth et appareils**, dans la section **Pavé tactile**. Les gestes du pavé tactile fonctionnent également sur l'écran tactile.

8. Raccourcis-clavier

Bien qu'un écran tactile soit très pratique, connaître les raccourcis-clavier permet de gagner un temps précieux : une combinaison de touches qui, une fois enfoncées, exécutent un logiciel ou une fonctionnalité. Certains ont déjà été abordés dans les premiers chapitres de cet ouvrage et d'autres le seront dans la suite.

Voici le tableau résumant les principaux raccourcis-clavier utiles à l'utilisateur, classés par ordre alphabétique. La touche  est systématiquement utilisée :

Combinaison	Description de l'action réalisée
 [Tab]	Affiche le menu Démarrer .
 [Ctrl][Entrée]	Affiche le bureau virtuel courant et les applications exécutées sur celui-ci.
 [Espace]	Exécute le narrateur.
 [Impr Ecran]	Change la langue et la disposition du clavier en cours.
 [Shift] S	Enregistre une capture complète de l'écran dans un fichier stocké dans le dossier Images.
 [Shift] S	Ouvre l'outil Capture et croquis et propose de sélectionner une zone à capturer.
 [Ctrl] Q	Ouvre l' Assistance rapide .
 ;	Affiche le panneau des émojis.
 A	Affiche le panneau des Paramètres rapides .
 C	Ouvre la liste des contacts Teams pour démarrer rapidement une conversation.
 D	Affiche ou masque le bureau.
 E	Affiche l' Explorateur de fichiers .
 I	Affiche le panneau Paramètres .
 G	Ouvre la barre de jeux.
 H	Lance la saisie vocale.
 K	Ouvre l'interface de recherche des périphériques sans fil.
 L	Verrouille la session en cours.
 M	Réduit toutes les fenêtres affichées sur le bureau.
 N	Affiche le panneau des Notifications .
 P	Affiche les fonctions de gestion d'écran multiples (duplicier, étendre...).
 Q	Affiche la fenêtre Recherche .
 R	Affiche la fenêtre Exécuter sur le bureau.

Combinaison	Description de l'action réalisée
U	Ouvre le menu Accessibilité du panneau des Paramètres .
W	Affiche le panneau des Widgets .
X	Affiche le menu Lien rapide vers les fonctions système.
Z	Affiche les dispositions automatiques de fenêtres disponibles (Snap layouts). Il est ensuite possible de naviguer avec les flèches pour sélectionner son emplacement.
[Ctrl] Q	Ouvre l'Assistance rapide.
[Shift] S	Exécute le logiciel de capture d'écran.
[Flèche en haut]	Agrandit la fenêtre active.
[Flèche en bas]	Réduit la fenêtre active.
[Flèche à gauche] ou [Flèche à droite]	Agrandit la fenêtre active sur le côté gauche ou droit de l'écran.
[Shift] [Flèche à gauche] ou [Flèche à droite]	Déplace la fenêtre active vers le moniteur de gauche ou de droite.
[Shift][Ctrl] B	Sort l'ordinateur du mode veille.

Une liste complète est disponible à cette adresse : <https://support.microsoft.com/fr-fr/windows/raccourcis-clavier-dans-windows-dcc61a57-8ff0-cffe-9796-cb9706c75eec>

9. Mode tactile

Windows 11 a été conçu comme un système d'exploitation à la fois universel et flexible. Quel que soit le périphérique utilisé (PC, PC hybride, tablette tactile), l'environnement de travail de l'utilisateur sera le même.

De nos jours, certains équipements actuels permettent aux utilisateurs de passer d'un ordinateur à une tablette simplement en décrochant le clavier de l'écran ou en repliant le clavier derrière l'écran. Bien conscient de l'ampleur de ces nouvelles façons de travailler, Microsoft avait donc créé une interface adaptée à ces nouveaux usages, via Windows 8 et 10.

Windows 11 continue dans cette lignée, mais en proposant de s'adapter automatiquement à la manière dont nous utilisons l'ordinateur. Le mode Tablette a disparu, mais l'interface utilisateur se modifie automatiquement selon les besoins.

Si vous utilisez une machine hybride et que vous déconnectez le clavier ou repliez celui-ci, l'interface va s'adapter :

- Les boutons et icônes de la barre des tâches vont s'écartier.
- L'explorateur de fichiers va ajouter des cases à cocher devant les éléments de chaque dossier.
- Une icône d'accès au clavier visuel (et au stylet si disponible) va apparaître sur la droite de la barre des tâches.



- Ce clavier va apparaître dès que vous pressez une zone de texte.

Apps

Windows 11 est proposé avec des applications préinstallées, couvrant l'essentiel des besoins de l'utilisateur, comme la gestion du courrier électronique, la lecture de flux RSS (*Rich Site Summary*), l'achat de musiques... Bien entendu, celles et ceux qui utilisent le système peuvent télécharger de nouvelles applications (ou Apps) au travers du magasin en ligne Microsoft Store, accessible depuis l'Ecran de démarrage ou la Barre des tâches. Elles sont développées avec la plateforme Windows Runtime et permettent à l'utilisateur de rester dans le même style graphique Windows 11.

Les utilisateurs de smartphones éteignent rarement leurs téléphones, car ceux-ci entrent dans un mode de très basse consommation pendant qu'ils ne sont pas utilisés, afin de continuer à recevoir des notifications (courriels, SMS...). Auparavant, quand l'ordinateur était en mode veille ou en mode veille prolongée, les applications bureautiques ne pouvaient pas accéder aux ressources du système.

1. Microsoft Store

Les concurrents de Microsoft proposent le téléchargement d'applications gratuites et payantes, communément nommées **Apps** : Apple et son magasin App Store, Google et Play Store. Ainsi, des développeurs et sociétés indépendants vendent un contenu, comme des Apps, de la musique, des films, des jeux ou encore des livres numériques. Grâce au service Cloud Computing, l'utilisateur peut télécharger une application depuis son téléphone portable (smartphone) et y accéder depuis son ordinateur ou sa tablette tactile.

Les Apps livrées avec Windows 11, ainsi que celles téléchargées depuis le magasin Microsoft Store, sont accessibles à l'aide d'un compte Microsoft ou d'un compte utilisateur local.

Couplées à ce type de compte (cf. chapitre Installation du client Windows 11, section Authentification), les applications restent accessibles depuis dix ordinateurs et peuvent être téléchargées depuis le magasin Microsoft Store.

Par exemple, Microsoft optimise l'utilisation du smartphone avec Windows 11 via l'App « Votre téléphone ». Il devient ainsi possible de passer des appels, d'envoyer des SMS depuis son poste de travail ou de prendre une photo depuis son smartphone Android et de la visualiser sur Windows 11.

Une des grandes nouveautés de Windows est l'ouverture de ce magasin en ligne aux applications Android. Cela signifie que l'utilisateur a la possibilité d'installer des applications jusqu'ici réservées aux smartphones et de les exécuter de manière native. Microsoft utilise la technologie Intel Bridge (un post-compilateur d'exécution) associée à un émulateur, *Windows Subsystem for Android* (WSA) pour exécuter des applications directement depuis Windows. Ce post-compilateur est une technologie logicielle, donc indépendant du type de processeur (Intel, AMD). Il permet aux applications de s'exécuter de manière native, donc offre plus de performances qu'un émulateur classique.

Comme mentionné précédemment, lors de la rédaction de cet ouvrage, la prise en charge native des applications Android n'avait pas encore été implémentée dans la version de Windows 11 disponible et était annoncée pour l'année 2022.

L'éditeur s'associe à Amazon pour proposer les applications Android provenant de l'Amazon Appstore. De plus, il autorise l'installation de fichiers APK sans passer par une boutique en ligne. Néanmoins, les applications populaires issues de Google ne sont pour le moment pas disponibles dans ce magasin.

Le magasin de Microsoft propose désormais des applications sous plusieurs formats :

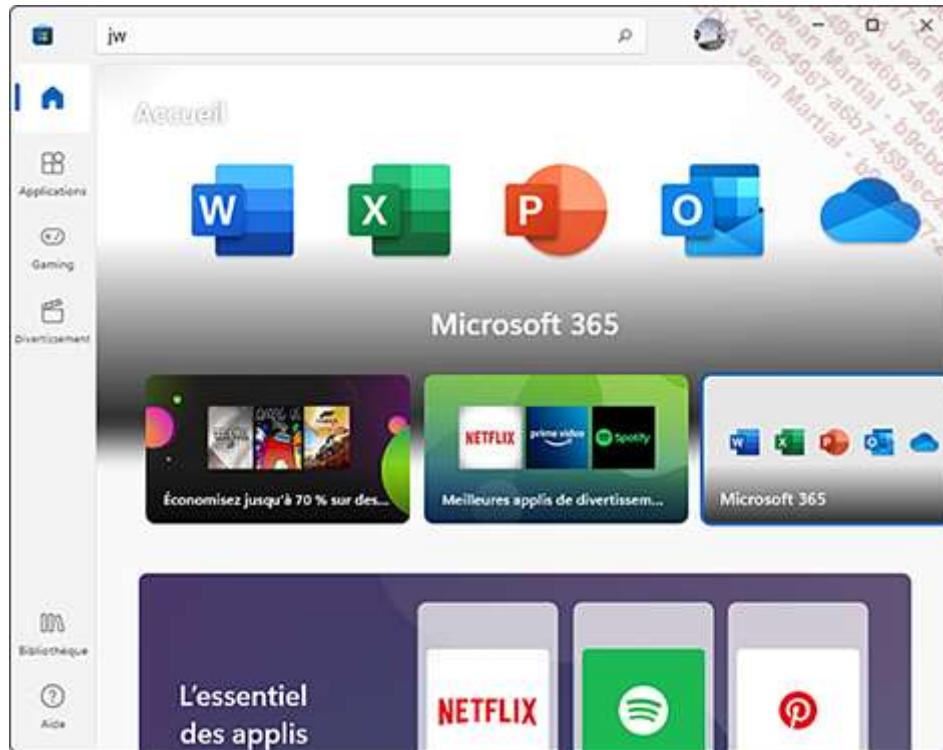
- Win32 (.exe ou .msi). Cela signifie que des applications comme Zoom, Adobe Reader ou VLC peuvent être désormais installées depuis le Store. Néanmoins, celles-ci restent des applications Windows classiques, c'est-à-dire que la mise à jour automatique, fonctionnalité pratique des Apps, ne fonctionne pas avec ce format.
- UWP (*Universal Windows App*).

- PWA (*Progressive Web Apps*).

La compatibilité des Apps Android ne dépend pas du CPU : Intel, AMD, ARM... les applications fonctionneront sur toutes architectures.



Dans la barre des tâches, cliquez sur la vignette **Microsoft Store** ; un grand nombre de catégories sont disponibles : **Applications, Gaming, Divertissement...**



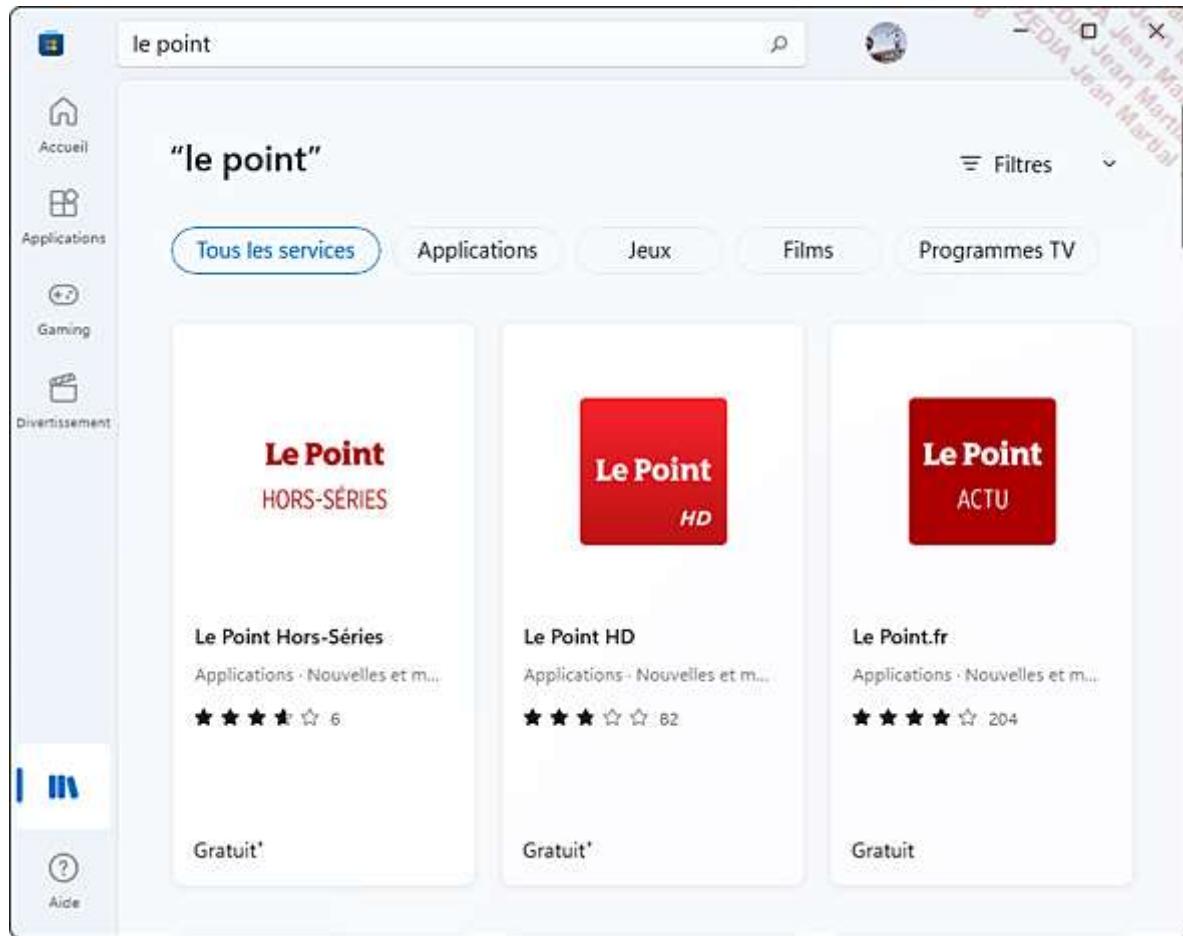
En cliquant sur **Bibliothèque**, la liste de vos applications, jeux, musiques et films acquis et/ou installés apparaît.

La présence du bouton **Lancer** signifie que l'application est installée sur la machine.

Un bouton **Installer** vous permet de télécharger et d'installer une application précédemment acquise sur cette machine ou une autre.

La mise à jour des applications s'effectue en cliquant sur le bouton **Obtenir les mises à jour**.

Vous pouvez également chercher des applications grâce au champ de recherche situé en haut du Microsoft Store puis valider en cliquant sur la loupe. Saisissez le nom de l'App que vous recherchez, dans notre exemple **Le Point.fr** ; le résultat s'affiche en fonction des catégories.



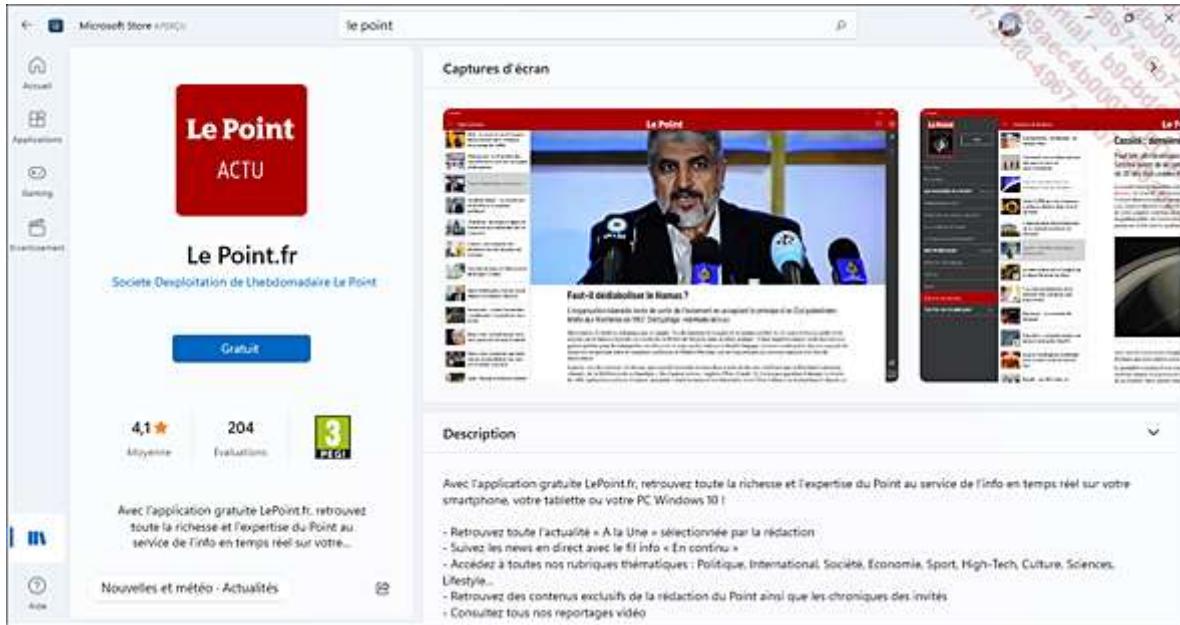
Depuis l'avatar, le menu **Modes de paiement** permet d'ajouter des informations de paiement supplémentaires en vous connectant à votre compte Microsoft.

a. Installation d'une App

Tout comme ses concurrents, Microsoft simplifie au maximum le processus d'installation d'une application. Il suffit de pointer ou de cliquer sur l'App visée pour qu'une vue d'ensemble de celle-ci soit affichée.

Dans la vue d'ensemble, vous trouverez les informations suivantes :

- La description de l'application.
- Les avis des utilisateurs.
- Les fonctionnalités et nouveautés.
- La configuration requise : système d'exploitation, architecture, type de périphérique...
- Des informations supplémentaires comme la catégorie, la taille, la nécessité d'une connexion internet active...
- La classification par âge : couplée avec la fonctionnalité de contrôle parental, l'utilisateur pourra interdire un contenu inapproprié à un enfant.



En cliquant sur le bouton **Gratuit**, la phase de téléchargement et d'installation s'effectue en arrière-plan, l'utilisateur peut ainsi continuer à travailler. Une fois celle-ci installée, l'intitulé du bouton devient **Lancer**.

La vignette de l'application téléchargée, dans notre cas celle du journal Le Point, est désormais visible dans le menu **Démarrer**. Le service utilisé pour installer les applications est **Windows Installer**, qui gère le déploiement automatisé d'applications au format MSI (*Microsoft Software Installer*).

Notez que la commande msiexec permet d'installer des Apps packagées. Par exemple, pour déployer une App nommée skype.msi sans interaction de l'utilisateur, utilisez la commande :

```
msiexec /i skype.msi
```

Le paramètre /qn spécifie que l'interface d'installation n'est pas utilisée.

Un autre paramètre important est /qb, qui affiche une barre de progression de l'installation de l'App.

En cas de réinstallation du poste Windows 11, les applications téléchargées depuis le Microsoft Store sont automatiquement réinstallées si le type de compte utilisateur est Microsoft.

Afin de garantir une sécurité et une stabilité efficaces, Microsoft Store affiche automatiquement sur sa vignette la disponibilité de mises à jour pour les applications installées.

Pour obtenir la liste de toutes les applications Windows installées, utilisez la commande PowerShell suivante :

```
Get-AppxProvisionedPackage -Online | Format-Table DisplayName,  
PackageName
```

Pour connaître la liste des applications système installées, utilisez la commande PowerShell suivante :

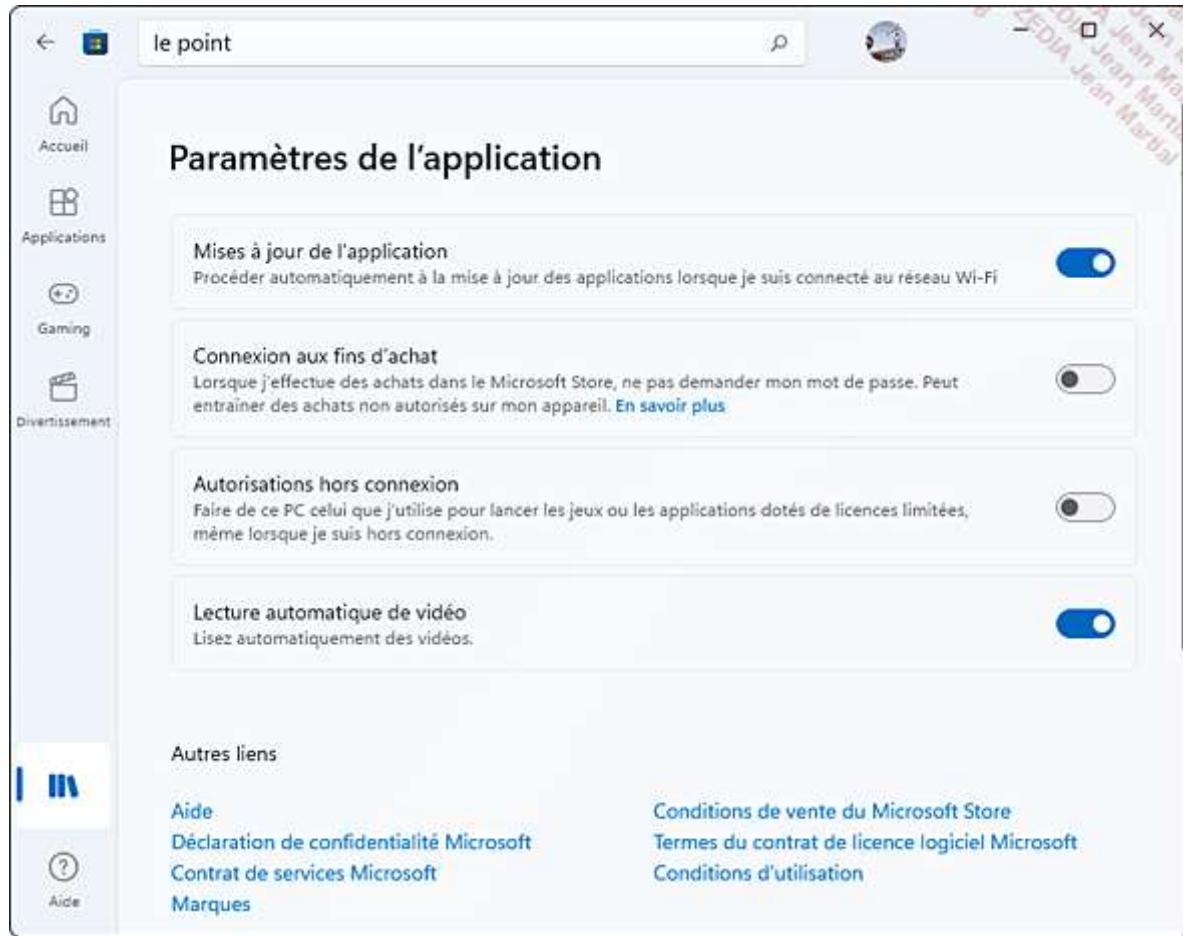
```
Get-AppxPackage -PackageTypeFilter Main | ? { $_.SignatureKind  
-eq "System" } | Sort Name | Format-Table Name, InstallLocation
```

b. Gérer les mises à jour

Une application possède un cycle de vie ; elle évolue par l'ajout de nouvelles fonctionnalités, et elle s'améliore quand un développeur corrige des bugs. Ensuite, elle n'est plus maintenue si elle devient obsolète. Windows 11 propose une gestion simplifiée des mises à jour des logiciels en provenance du magasin Microsoft Store.

Pour vérifier que les applications sont automatiquement mises à jour :

Cliquez sur l'icône du **Microsoft Store** disponible dans la barre des tâches, puis cliquez sur votre avatar, puis sur le sous-menu **Paramètres de l'application**. Vérifiez que la mise à jour des applications est automatique.



Notez qu'une méthode permet de contrôler l'installation et l'exécution d'applications, grâce à la fonctionnalité **AppLocker** (cf. chapitre Configuration de la sécurité Windows, section Contrôle des applications avec AppLocker).

c. Déploiement SideLoading

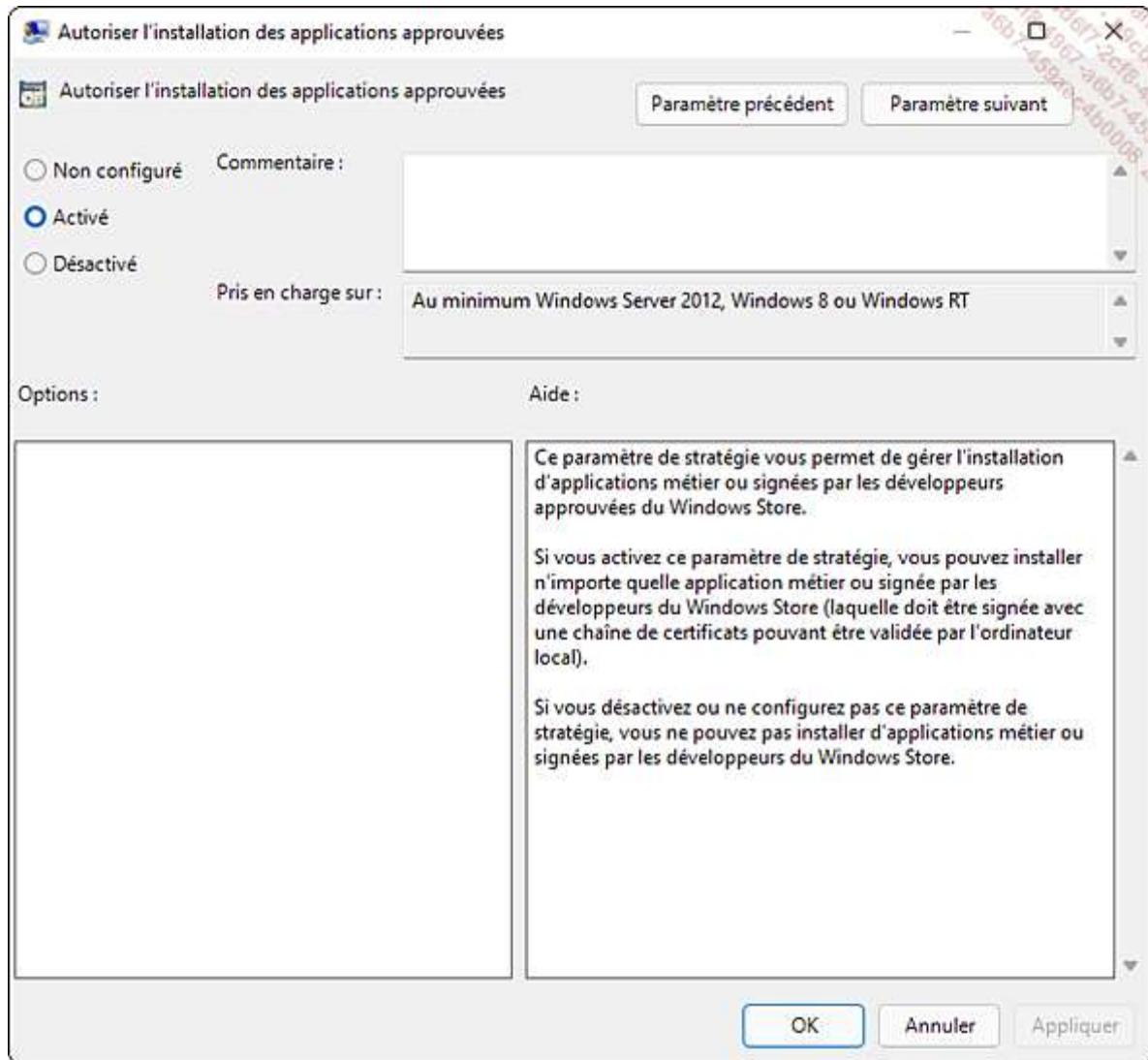
Les applications peuvent être installées depuis le Microsoft Store, mais celles-ci doivent être obligatoirement signées par Microsoft car elles sont testées par l'éditeur. Une entreprise ne peut attendre cette validation, et va donc déployer ses propres applications directement auprès de ses postes de travail, à condition que ceux-ci soient membres d'un domaine. Dans le cas contraire, une clé d'activation dédiée sera nécessaire.

SideLoading est le nom de cette fonctionnalité qui nécessite néanmoins que l'application soit signée par une autorité de certification reconnue par les clients et que la version du système soit Windows 11 Entreprise.

Avant d'installer des applications développées par une société, l'administrateur doit activer la fonctionnalité SideLoading sur les ordinateurs du domaine, grâce à un objet de stratégie de groupe :

Sélectionnez **Modifier la stratégie de groupe**. Dans la fenêtre **Éditeur de stratégie de groupe locale** qui apparaît, développez **Configuration ordinateur - Modèles d'administration - Composants Windows et Déploiement de package Appx**.

Double cliquez sur le paramètre **Autoriser l'installation des applications approuvées**. Sélectionnez l'option **Activé**.



Validez par le bouton **OK**.

Une application propriétaire possède une extension .appx et peut être installée de deux manières : à l'aide du langage PowerShell ou de la commande DISM (cf. chapitre Conception d'une image de déploiement, section Création d'une installation de référence). Utilisez la commande PowerShell afin d'installer l'application pour l'utilisateur courant. Si l'objectif est de déployer l'application pour tous les utilisateurs d'un ordinateur, préférez la commande DISM.

Voici la procédure à suivre pour les deux cas de figure :

PowerShell : cliquez avec le bouton droit sur le menu **Démarrer** puis **Windows PowerShell (admin)**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît. Dans la fenêtre **Windows PowerShell**, saisissez les commandes suivantes :

```
import-module appx
```

puis

```
add-appxpackage C:\test.appx
```

(où test.appx est le nom du fichier d'installation de l'application que vous souhaitez installer).

La suppression d'une application est possible grâce à la commande PowerShell Remove-AppxPackage.

Commande DISM : il est possible d'ajouter des applications dans une image Windows 11. Cliquez avec le bouton droit sur le menu **Démarrer**, puis **Windows PowerShell (admin)**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît. Saisissez la commande suivante :

```
dism /Online /Add-ProvisionedAppxPackage /PackagePath:C:\test.appx /SkipLicense
```

Il est préférable de fermer la session des utilisateurs actifs avant d'exécuter cette commande.

Obtenir la liste des applications propriétaires déjà installées s'effectue avec le paramètre Get-ProvisionedAppxPackages de la commande DISM.

Pour tester une application Windows 11 avant son déploiement, un développeur peut utiliser le kit de développement logiciel Windows, disponible en téléchargement depuis le site suivant : <https://developer.microsoft.com/fr-fr/>

Windows 11 introduit l'offre groupée d'applications (ou package .appxbundle) afin d'optimiser la création de package et la distribution d'une App dans le Microsoft Store.

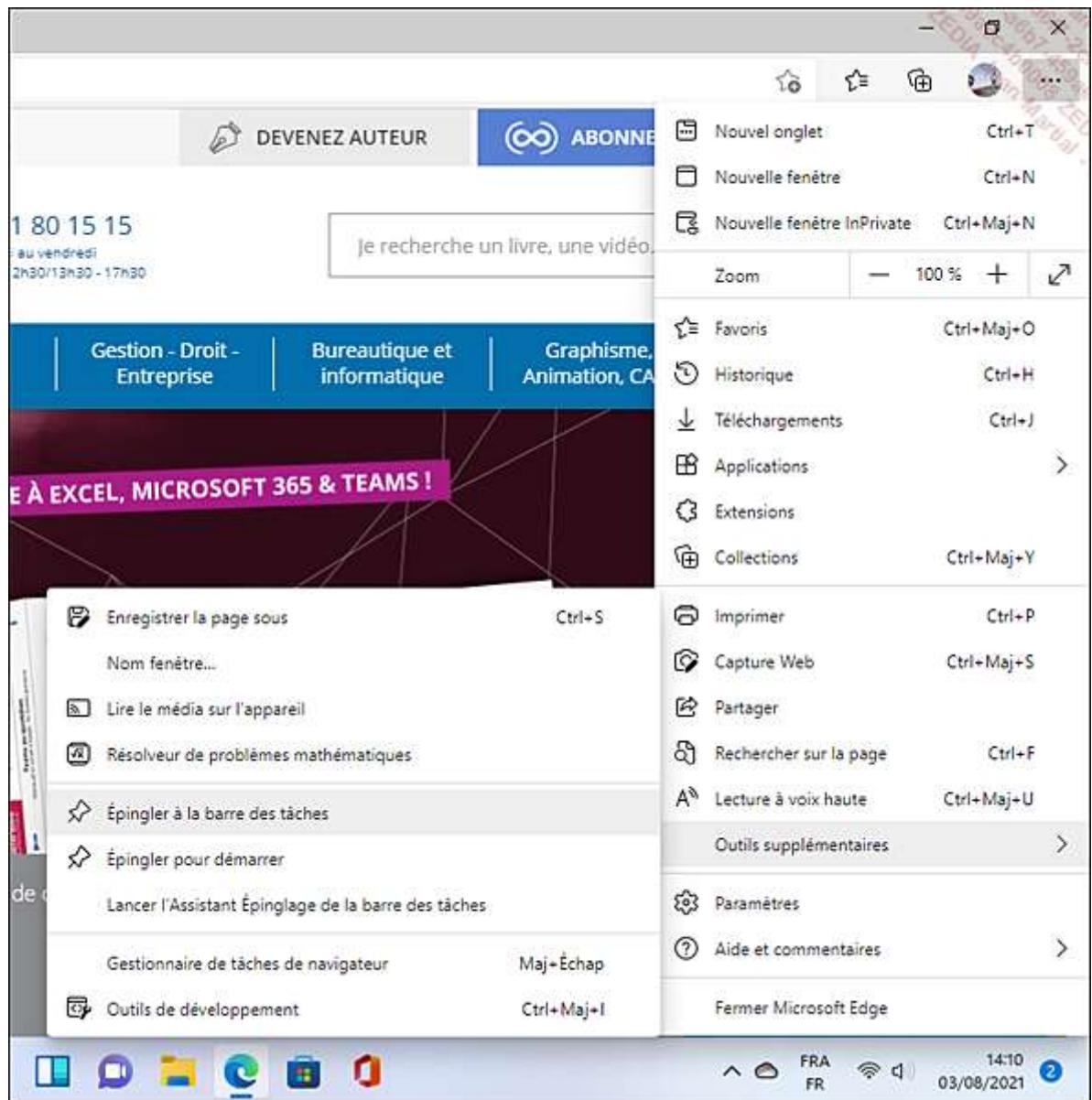
Ainsi, l'expérience d'application est enrichie, et l'espace disque nécessaire à l'installation réduit. De plus, les packs de ressources proposent des suppléments, tels qu'une traduction ou la gestion des écrans haute résolution.

Le contrôle des applications Windows 11 qui peuvent être installées et exécutées s'effectue à l'aide de la fonctionnalité AppLocker.

2. Microsoft Edge

Le navigateur internet devient une application gérée par les administrateurs au même titre que n'importe quel programme, afin de prémunir la société contre les attaques informatiques.

Il est désormais possible d'épingler un site web dans la barre des tâches pour y accéder plus rapidement.



Microsoft Edge dispose du mode Lecture. La fonctionnalité d'entrée manuscrite, qui permettait de prendre des notes directement sur une page web, n'a pour le moment pas été reconduite (depuis la mise à jour d'avril 2020). Néanmoins, il est fort possible que celle-ci soit incluse dans une des prochaines mises à jour.

Microsoft limite l'utilisation des plug-ins de navigation (composants logiciels tiers compilés) sur Microsoft Edge ; ils surutilisent généralement les ressources de l'ordinateur client et augmentent la surface d'attaque.

Internet Explorer 11 est néanmoins intégré à Edge afin de supporter des technologies d'ancienne génération telles qu'ActiveX.

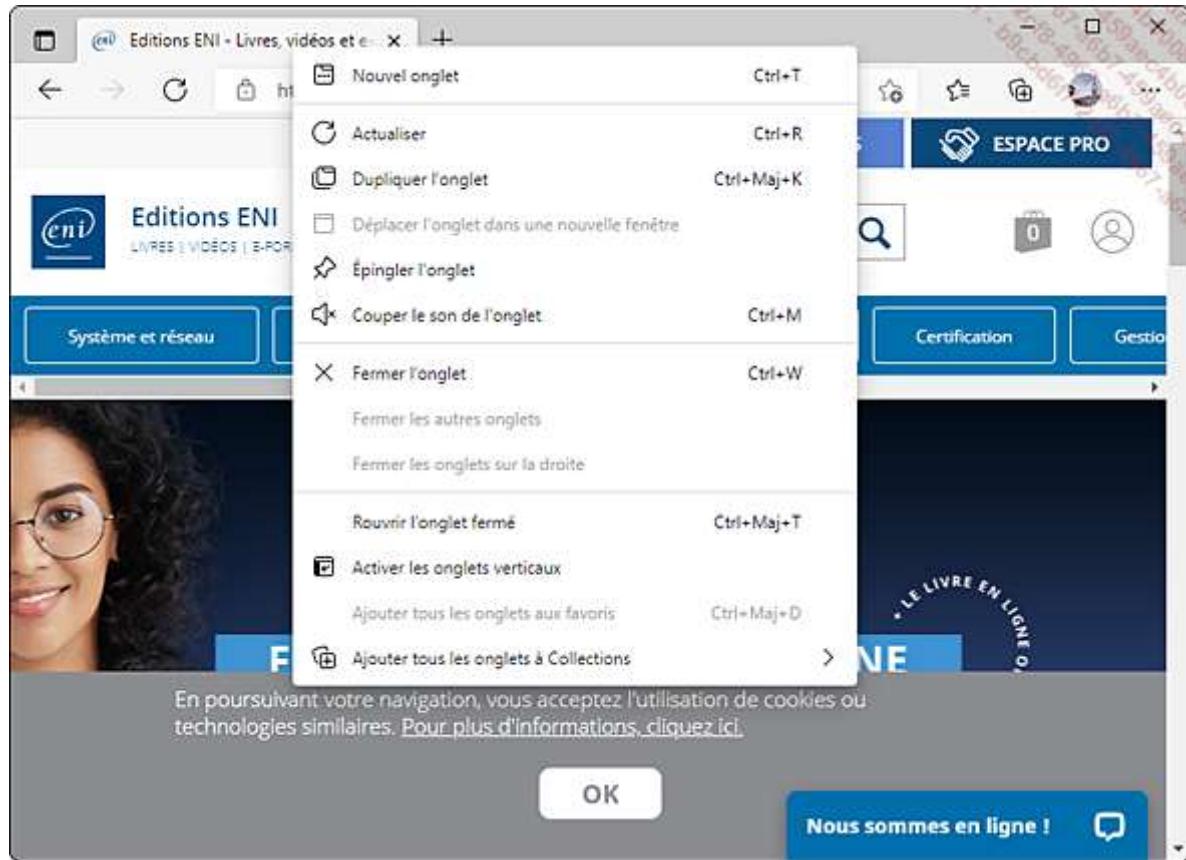


Pour ouvrir le navigateur Microsoft Edge, cliquez sur l'icône dans la barre des tâches.

La barre d'adresse de Microsoft Edge est le point de départ pour effectuer un ensemble d'actions, comme naviguer, créer des recherches ou afficher des suggestions.

Grâce aux onglets, l'utilisateur peut ouvrir plusieurs sites internet dans une seule fenêtre. Pour ouvrir un nouvel onglet, cliquez sur le bouton +. Pour fermer les onglets, fermer tous les onglets sauf celui actif, les dupliquer ou les actualiser, cliquez avec le bouton droit sur l'un d'eux et cliquez sur l'option de votre choix. Notez également

les fonctionnalités permettant de couper le son d'un onglet, de rouvrir un onglet fermé par inadvertance ou de positionner les onglets verticalement.



Les **Paramètres** sont accessibles depuis le bouton en haut à droite. L'utilisateur peut y choisir une nouvelle apparence, épinglez le volet des Favoris, importer ces derniers d'un autre navigateur, configurer le contenu des nouveaux onglets, effacer les éléments de navigation afin de préserver sa vie privée ou encore définir le style du mode de lecture.

Paramètres

Rechercher dans les paramètres

Profils

-  Confidentialité, recherche et services
-  Apparence
-  Démarrer, Accueil et nouveaux onglets
-  Partager, copier et coller
-  Cookies et autorisations de site
-  Navigateur par défaut
-  Téléchargements
-  Contrôle parental
-  Langues
-  Imprimantes
-  Système
-  Rétablir les paramètres
-  Téléphone et autres appareils
-  À propos de Microsoft Edge

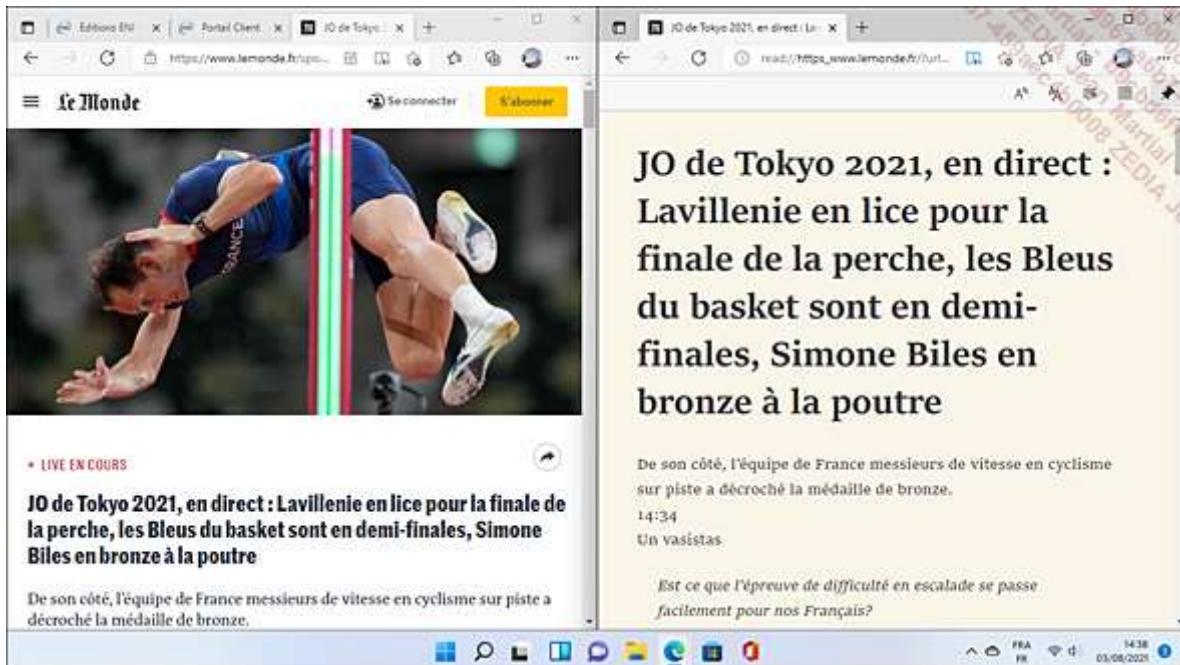
Pour ouvrir plusieurs sites internet en page d'accueil lors de l'exécution de Microsoft Edge sur une tablette tactile ou sur un ordinateur, suivez la procédure ci-dessous :

Depuis le navigateur, cliquez ou pointez sur le bouton  puis sur **Paramètres**.

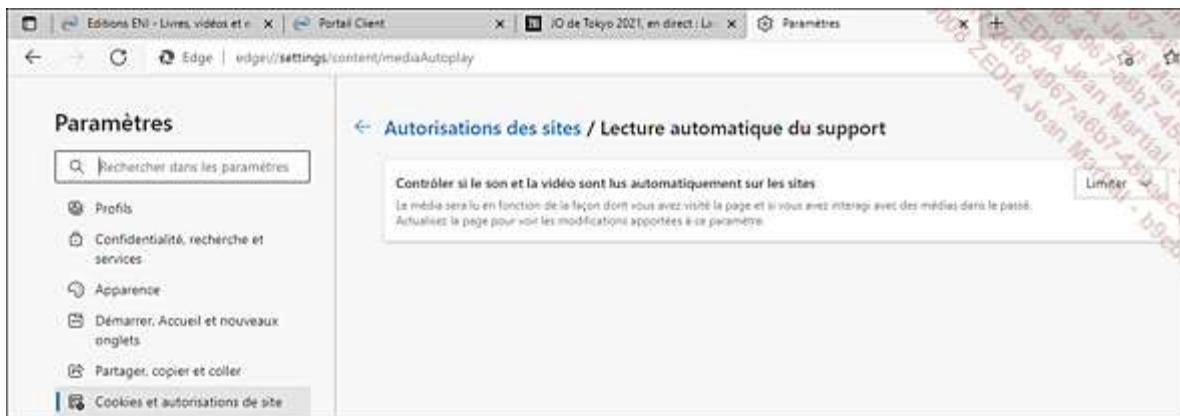
Ouvrez le menu **Démarrer, Accueil et nouveaux onglets** ; dans la section **Au démarrage de Microsoft Edge**, cochez **Ouvrir ces pages** et cliquez sur **Ajouter une nouvelle page** pour insérer une ou plusieurs pages.

Lorsque vous naviguez sur un site proposant des articles, Edge propose le mode Lecteur immersif (touche [F9]). Ainsi, les publicités sont supprimées, et la page est affichée pour procurer un confort de lecture optimal à l'utilisateur. Quand le mode Lecteur immersif est compatible avec le site internet visité, l'icône  est activée dans la barre d'adresse.

Voici le contenu d'un article avant et après l'utilisation de la fonctionnalité :



Une autre option intéressante est la lecture automatique d'un support, accessible depuis le menu **Paramètres et Cookies et autorisations de site**. Dans la section **Autorisations des sites**, cliquez sur **Lecture automatique du support** et sélectionnez l'option adéquate. Ainsi, Edge peut automatiquement lire des vidéos ou limiter la lecture (en sourdine) en fonction des habitudes de l'utilisateur.



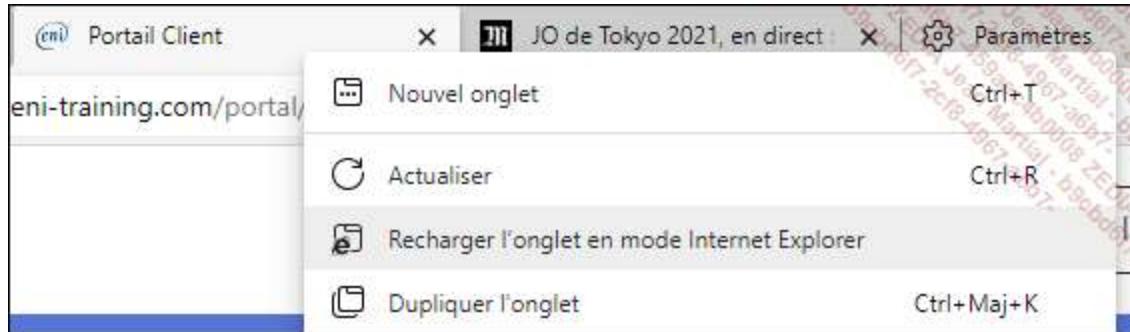
Enfin, en cliquant avec le bouton droit sur l'icône de Microsoft Edge située sur la barre des tâches, la liste des sites les plus visités va apparaître.

a. Affichage de compatibilité

Les sites internet anciens peuvent être affichés de manière dénaturée ; des applications développées pour des versions spécifiques d'Internet Explorer peuvent ne pas fonctionner avec Edge. Dans ce cas, l'administrateur a la possibilité de les ouvrir avec Internet Explorer dans Edge.

Par défaut, tous les sites s'ouvrent avec Edge et son nouveau moteur Chromium. Le paramétrage de ce comportement est accessible depuis le menu des **Paramètres, Navigateur par défaut**. Dans la section **Compatibilité d'Internet Explorer**, seuls les sites compatibles avec Internet Explorer s'ouvriront dans ce dernier et son moteur Trident MSHTML. Il s'agit de l'option recommandée.

Il est possible également de forcer un mode avec l'option **Autoriser le rechargement des sites en mode Internet Explorer**. Cela permettra à l'utilisateur de recharger une page en mode Internet Explorer. Pour rendre plus facile l'utilisation d'IE, associez à ce paramétrage un menu, depuis les **Paramètres, Apparence**. Dans la section **Personnaliser la barre d'outils**, activez la ligne **Afficher le bouton du mode Internet Explorer**. Désormais, sur chaque onglet, vous avez la possibilité de basculer d'un mode à l'autre.



La page internet sera chargée une nouvelle fois mais en mode Internet Explorer 11. Le site sera affiché comme si l'utilisateur y accédait depuis l'ancien navigateur. La majorité des problèmes d'affichage (images, zones de texte pas à leur place) seront ainsi résolus. Lorsqu'un site est chargé en mode IE, le logo bleu Internet Explorer s'affiche sur le côté de la barre de navigation et une pop-up vous en avise.

La liste des sites présentant un problème de compatibilité avec Edge est régulièrement mise à jour par Microsoft. L'administrateur peut diffuser sa propre liste interne à l'entreprise par l'intermédiaire d'un objet de stratégie de groupe.

Pour qu'un site s'ouvre avec Internet Explorer, vous devez mettre en place une stratégie de groupe :

Exécutez gpedit.msc et développez les menus **Configuration ordinateur - Modèles d'administration - Composants Windows - Microsoft Edge**.

Activez la stratégie **Configurer la liste des sites en Mode entreprise** et pointez vers le fichier XML contenant cette liste.

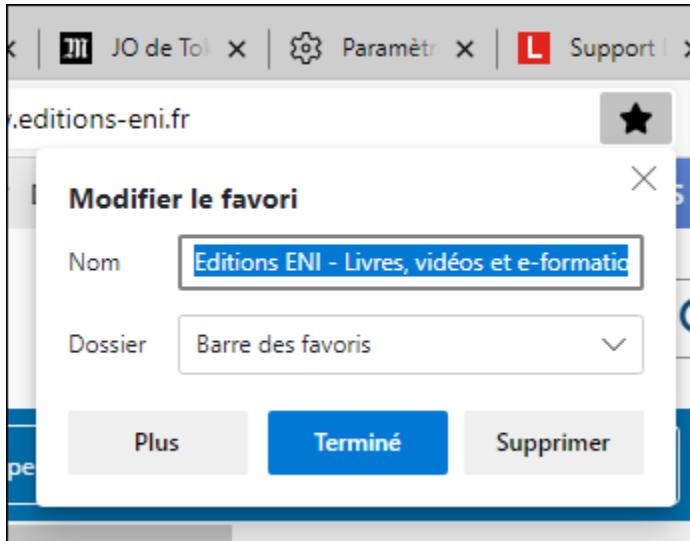
Cette stratégie est prioritaire à **Configuration ordinateur - Modèles d'administration - Composants Windows - Internet Explorer - Utiliser la liste des sites Web en mode Entreprise d'Internet Explorer**.

Enfin, sachez que par défaut, les sites intranet de l'entreprise sont affichés en mode **Affichage de compatibilité** dans Internet Explorer 11 si la stratégie **Configuration ordinateur - Modèles d'administration - Composants Windows - Microsoft Edge - Envoyer tous les sites intranet vers Internet Explorer** est activée.

b. Épingler un site

Les Favoris sont disponibles dans Edge, où ils sont représentés par une étoile . L'utilisateur peut épinglez le site dans les Favoris pour y accéder rapidement :

Saisissez par exemple l'URL suivante dans Microsoft Edge <https://www.editions-eni.fr> et cliquez sur l'icône puis sélectionnez un nom et un dossier, et enfin cliquez sur **Terminer**.

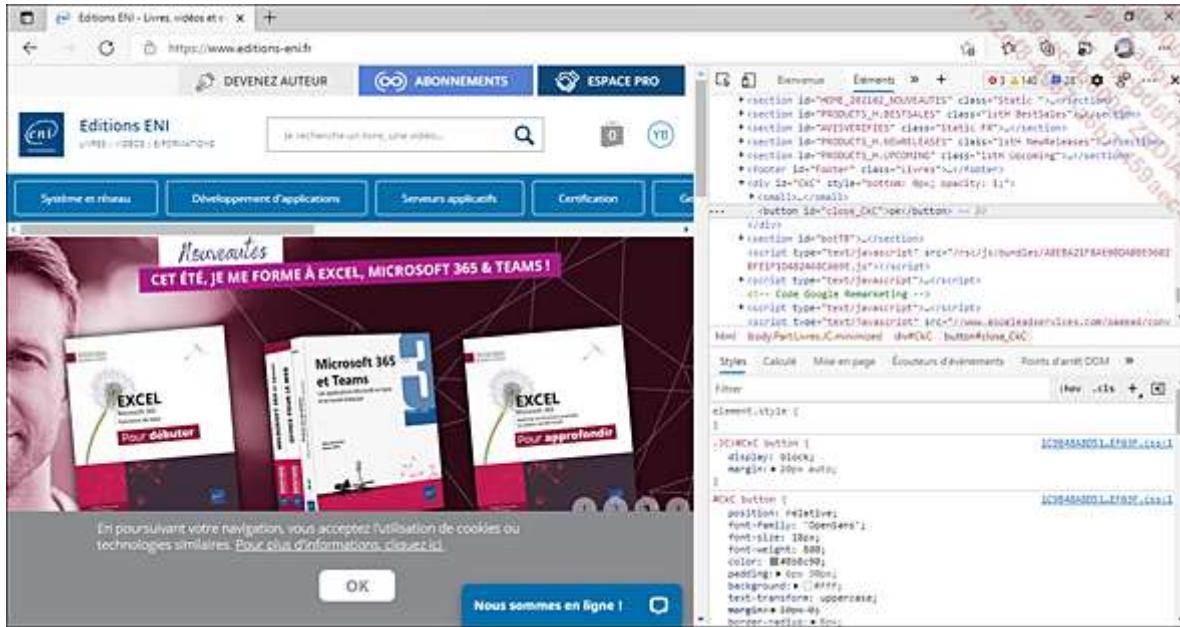


Le site est désormais disponible dans les favoris, accessibles en cliquant sur l'icône **Favoris**, représentée par une étoile avec trois filaments.

c. Outils de développement F12

Avec Microsoft Edge, un développeur peut visualiser le code du site internet visité, afin de détecter et corriger les problèmes qui peuvent survenir : il suffit de presser la touche [F12] du clavier (et de valider l'ouverture de **Devtools**) ou bien depuis le bouton **Outils supplémentaires**, **Outils de développement**.

Un panneau apparaît sur la droite de la page et réduit cette dernière. Il contient le code source de la page et permet d'afficher différentes informations en fonction des onglets sélectionnés (**Eléments**, **Console**, **Sources**, **Réseau**, **Performances**, **Mémoire**, **Application**, **Sécurité** et **Lighthouse**) :



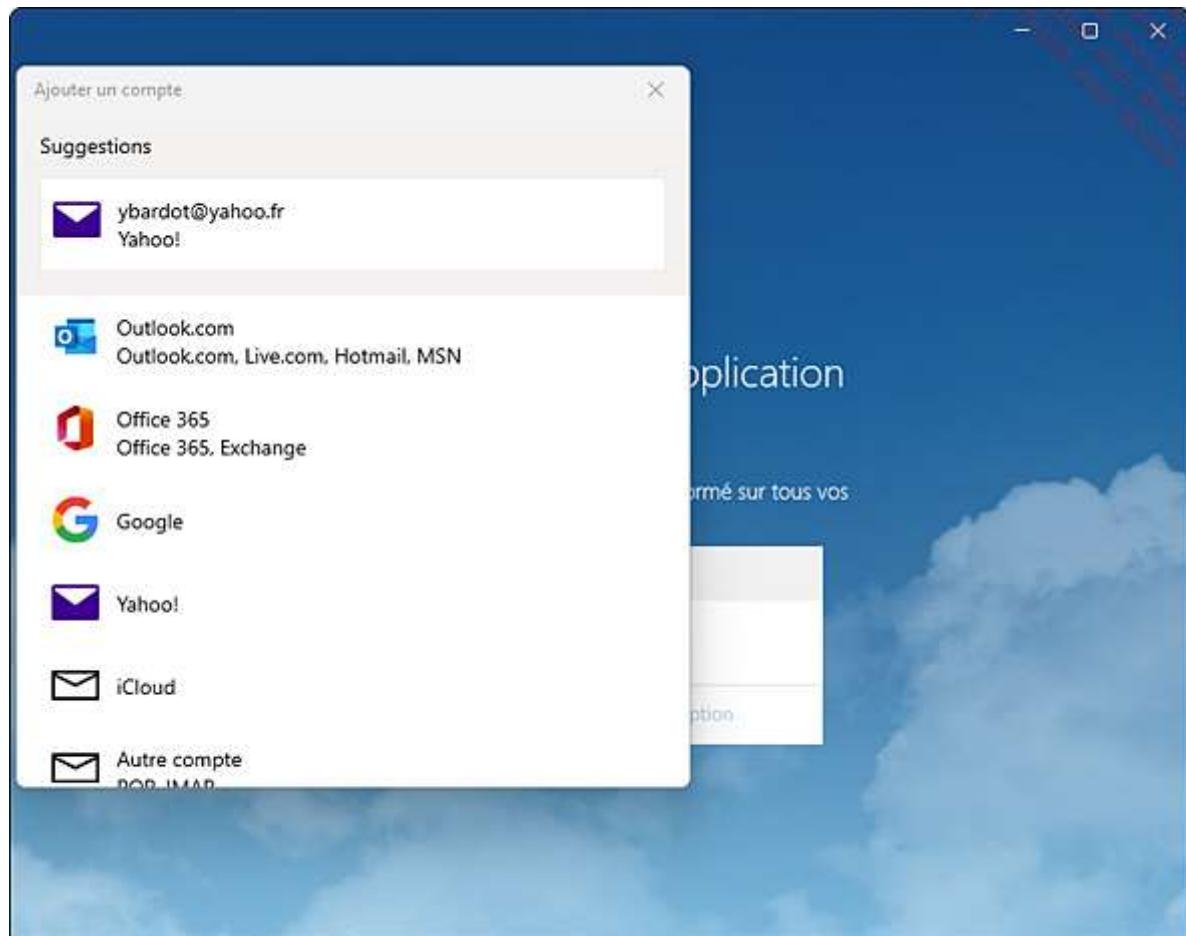
En cliquant sur l'onglet **Eléments**, la personne en charge du développement visualisera le code HTML interprété en le sélectionnant dans une page web.

Les fonctionnalités liées à la sécurité du navigateur Microsoft Edge sont détaillées dans le chapitre Configuration de la sécurité Windows, section Sécurité dans Microsoft Edge.

3. Courrier

De nos jours, un utilisateur possède plusieurs comptes de messagerie, couvrant les domaines professionnel et personnel, et reçoit ainsi un nombre conséquent de courriels, parfois indésirables. Ce moyen de communication devient extrêmement addictif, car nous souhaitons de plus en plus recevoir des notifications sur notre ordinateur, mais aussi sur notre téléphone portable.

Au premier démarrage, l'App propose d'ajouter un compte parmi les fournisseurs ci-dessous.



Sélectionnez votre domaine et suivez les instructions : identifications...

L'interface se divise en trois volets, celui de gauche contenant les comptes et les dossiers, celui du milieu, les courriels reçus et celui de droite, le volet de lecture, affiche un aperçu du contenu de ces derniers :

Boîte de réception - Gmail

Nouveau message

Comptes

Gmail formationyb@gmail.com 14

Dossiers

Boîte de réception 14

Brouillons

Messages envoyés

Plus

Consultez votre courrier Gmail sur votre téléphone.

Rechercher

Boîte de réception tous

Google Workspace Updates > Alerte de sécurité (2) Windows a désormais accès à votre com 16/20

Google Workspace Updates Google Workspace Updates: 3 new pos 10/14

samedi 31 juillet 2021

Google Workspace Updates Google Workspace Updates: 2 new sam. 31/07

vendredi 30 juillet 2021

Google Workspace Updates Google Workspace Updates: 3 new ven. 30/07

jeudi 29 juillet 2021

Google Workspace Updates Google Workspace Update: Enhanc jeu. 29/07

mardi 27 juillet 2021

Répondre Répondre à tous Transférer Archiver

Google Workspace Updates: 3 new posts

Google Workspace Updates <noreply+feedproxy@google.com> 10/14

A : formationyb@gmail.com

Google Workspace Updates: 3 new posts

- Updated emoji experience in Google Chat
- Directly open Office editing from shared links
- Smart Compose now available in comments for Google Slides, Sheets, and Drawings

Updated emoji experience in Google Chat

Posted: 02 Aug 2021 01:45 PM PDT

What's changing

It's now easier to express yourself more authentically in Chat. We're making the following updates to the emoji mobile:

- Emoji set is updated to the latest version (Emoji 13.1), reflecting the latest emoji set and diversity and inclusion.
- Addition of a gender-neutral option for gender-modifiable emojis
- Emojis with tones and gender references are now used on individual accounts.

Certains boutons sont constamment visibles dans l'interface Courrier et assurent les principales fonctions de gestion de la messagerie électronique :

- **Nouveau message** : création d'un courriel en spécifiant les destinataires, la priorité et les pièces jointes éventuelles. La sélection d'un texte affiche des options de mises en forme supplémentaires (gras, italique, police utilisée...).
- **Répondre** : permet de répondre à l'émetteur.
- **Répondre à tous** : permet de répondre à tous les destinataires.
- **Transférer** : transfère le courriel sélectionné.
- **Archiver** : classe un message.

Il est possible d'accéder à des options supplémentaires, comme **Supprimer**, **Déplacer un message**, le **Marquer comme non lu**, en cliquant sur l'icône ou avec le bouton droit sur un message.

Dossiers

Boîte de réception 15

Brouillons

Messages envoyés

Plus

Windows a désormais accès à votre com

Google Workspace Updates

Google W Google W Google W

samedi 31 juillet

Google W Google W Google W

vendredi 30 juillet

Google W Google W Google W

Google Workspace Updates: 3 new posts

Archiver Supprimer Déplacer Définir un indicateur Marquer comme lu(s) Ignorer Déplacer vers le courrier indésirable

L'impression d'un courriel s'effectue en le sélectionnant puis en cliquant sur l'icône  et sur **Imprimer**.

En passant la souris sur le nom d'une personne vous ayant écrit, il est possible d'accéder à des actions rapides, comme envoyer un courriel, appeler, ou bien communiquer grâce à une messagerie instantanée.



Les paramètres des comptes de messagerie sont accessibles depuis l'icône **Paramètres** située en bas à gauche de l'interface. L'utilisateur peut ajouter un compte de messagerie, régler la fréquence de téléchargement du contenu, les dossiers à synchroniser, les notifications, sa signature ou son message d'absence...

Paramètres

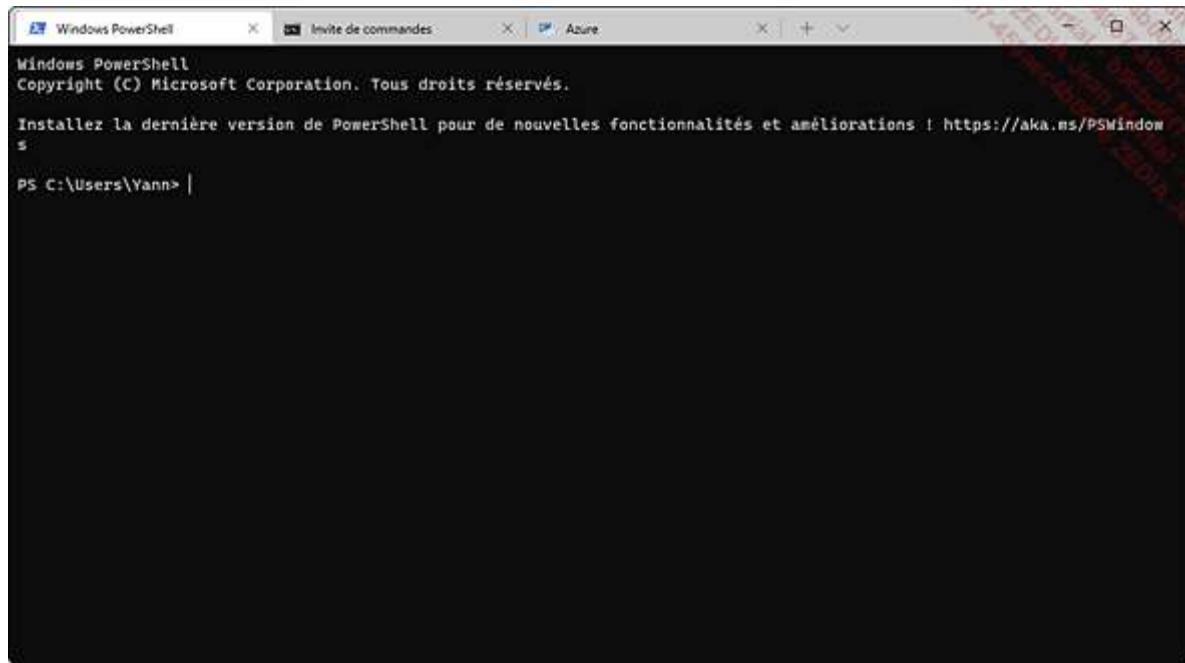
- Gérer les comptes
- Personnalisation
- Réponses automatiques
- Boîte de réception Prioritaire
- Liste des messages
- Volet de lecture
- Signature
- Police par défaut
- Notifications
- Sécurité du courrier
- Nouveautés
- Outlook pour Android et iOS
- Aide
- Centre de gestion de la confidentialité
- Votre avis
- À propos de

Par défaut, l'application Courrier télécharge les nouveaux courriels lors de leur arrivée dans le ou les comptes de messagerie. L'utilisateur peut néanmoins définir la fréquence d'interrogation des nouveaux messages (15 minutes, 30 minutes, toutes les heures ou manuellement), afin de préserver la batterie de son ordinateur, depuis **Paramètres** et **Gérer les comptes**.

Dans le cas où la bande passante de l'utilisateur serait limitée et facturée, l'application Courrier téléchargera les vingt premiers kilo-octets d'un courriel, en excluant les pièces jointes.

4. Terminal Windows

Apparu en 2019, le Terminal Windows a pour objectif d'offrir une interface moderne, conviviale et rapide pour les utilisateurs de la ligne de commande. Il comble enfin les lacunes de l'invite de commandes. Grâce à ses onglets, il permet d'utiliser des environnements différents comme l'invite de commandes, PowerShell, WSL (*Windows Subsystem for Linux*) et Azure Cloud Shell dans la même fenêtre.



Parmi ses autres points forts, citons :

- La prise en charge des caractères Unicode et UTF-8. Le Terminal Windows peut donc afficher des Emojis et des caractères issus de langues autres que celles installées.
- Une amélioration des performances grâce à l'utilisation du GPU pour restituer le texte. Il est donc possible de zoomer dans une fenêtre de Terminal Windows ([Ctrl] + roulette).
- La personnalisation de la fenêtre : création de thèmes, modification des couleurs, prise en charge des images d'arrière-plan, animées ou non...

Le Terminal Windows est accessible depuis le menu **Démarrer** en saisissant terminal et en cliquant sur **Terminal Windows** ou en cliquant avec le bouton droit sur le bouton **Démarrer** puis avec le bouton gauche sur **Terminal Windows** dans le menu qui apparaît. L'ouverture d'un nouvel onglet se fait en cliquant sur l'icône + disponible à droite de l'onglet ouvert ou avec le raccourci-clavier [Ctrl] + [Shift] + T. Pour plus de lisibilité, il est possible de scinder la fenêtre en deux en appuyant sur la touche [Alt] et en cliquant sur le +. Cela permet de comparer plus facilement les informations. Saisissez exit pour fermer un des Shell et revenir à un onglet non fractionné.

```
Répertoire : C:\Users\Yann

Mode          LastWriteTime    Length Name
----          ——————       ——— ——
d-r---        02/08/2021    08:48  Contact
d-r---        24/08/2021    09:59  Desktop
d-r---        25/08/2021    10:14  Document
d-r---        25/08/2021    10:12  Downloads
d-r---        02/08/2021    08:48  Favorites
d-----        03/08/2021    21:43  Intel
d-r---        02/08/2021    08:48  Links
d-r---        02/08/2021    08:48  Music
dar--l        25/08/2021    09:02  OneDrive
d-r---        25/08/2021    10:18  Pictures
d-r---        02/08/2021    08:48  SavedGames
d-r---        03/08/2021    07:57  Searches
d-r---        13/08/2021    17:12  Videos

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

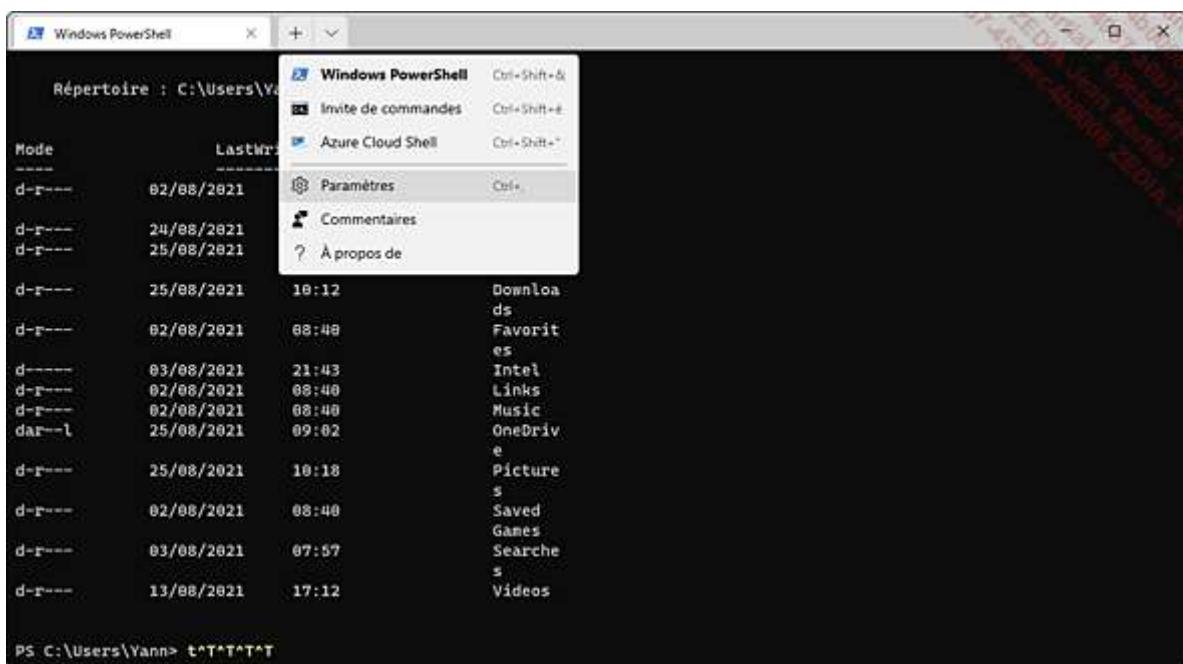
```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

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

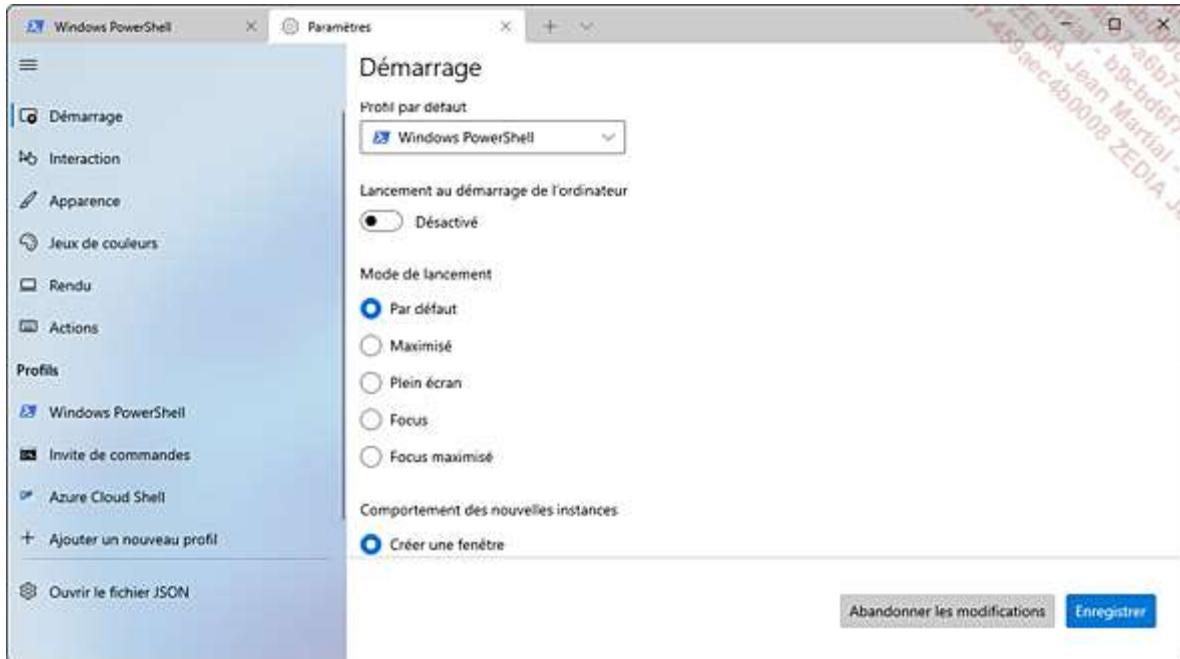
PS C:\Users\Yann>
```

Cliquez sur le + et appuyez simultanément sur la touche [Shift] afin d'ouvrir une nouvelle fenêtre de Terminal.
Le Terminal Windows est également paramétrable graphiquement.

Cliquez sur le bouton représentant un chevron vers le bas puis sur **Paramètres**. Au passage, notez la possibilité d'ouvrir d'autres Shell.



Plusieurs sections sont disponibles.



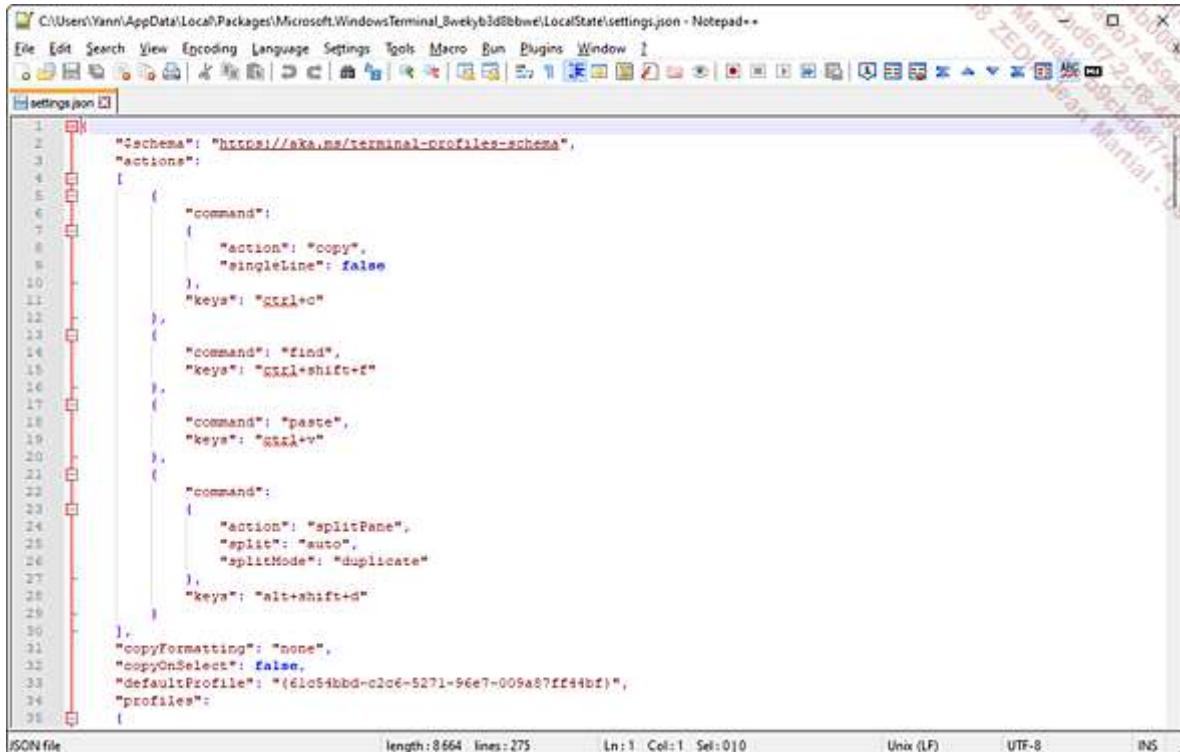
Le profil par défaut ouvre un environnement PowerShell. Chaque ouverture rapide d'un onglet ouvrira donc un nouveau Shell PowerShell. Il est possible de choisir un autre profil et même d'en ajouter (WSL...) depuis la section **Démarrage** des **Paramètres**.

Les sections **Apparences** et **Jeux de couleurs** permettent de personnaliser l'apparence de son terminal.

La section **Actions** indique les raccourcis-clavier disponibles.

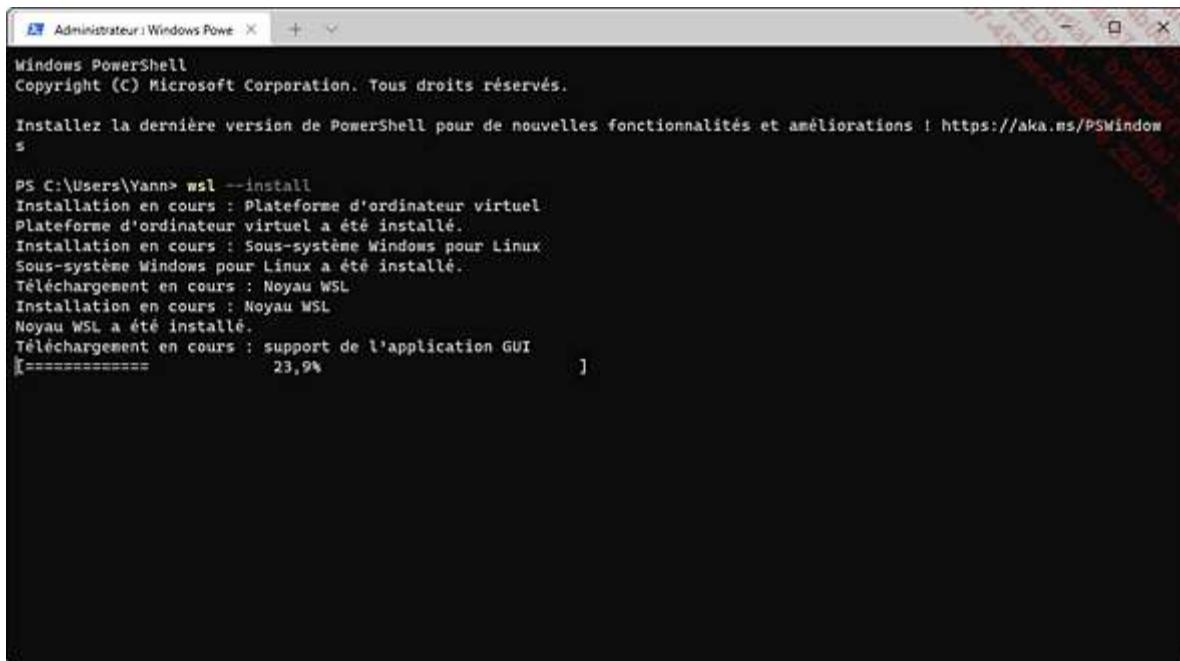
Tous les paramètres sont enregistrés dans un fichier de profil nommé **settings.json**, dans le dossier personnel de l'utilisateur

(**%USERPROFILE%**\AppData\Local\Packages\Microsoft.WindowsTerminal_8wekyb3d8bbwe\LocalState). Il est tout à fait possible d'éditer manuellement ce fichier depuis les **Paramètres**, en cliquant sur **Ouvrir le fichier JSON**. Il faudra disposer d'en éditeur de texte comme le Bloc-notes ou un éditeur tiers comme Notepad++ pour en visualiser et modifier le contenu.



```
1  "schema": "https://aka.ms/terminal-profiles-schema",
2  "actions": [
3    {
4      "command": {
5        "action": "copy",
6        "singleLine": false
7      },
8      "keys": "ctrl+c"
9    },
10   {
11     "command": "find",
12     "keys": "ctrl+shift+f"
13   },
14   {
15     "command": "paste",
16     "keys": "ctrl+v"
17   },
18   {
19     "command": {
20       "action": "splitPane",
21       "split": "auto",
22       "splitMode": "duplicate"
23     },
24     "keys": "alt+shift+d"
25   }
26 ],
27 "copyFormatting": "none",
28 "copyOnSelect": false,
29 "defaultProfile": "(61c54bbd-c2c6-5271-96e7-009a27ff4abf)",
30 "profiles": []
31 ]
```

L'installation d'un nouveau Shell peut se faire depuis un onglet PowerShell, en tant qu'administrateur. Par exemple, pour installer le sous-système Linux Ubuntu, saisissez : wsl --install



```
PS C:\Users\Yann> wsl --install
Installation en cours : Plateforme d'ordinateur virtuel
Plateforme d'ordinateur virtuel a été installé.
Installation en cours : Sous-système Windows pour Linux
Sous-système Windows pour Linux a été installé.
Téléchargement en cours : Noyau WSL
Installation en cours : Noyau WSL
Noyau WSL a été installé.
Téléchargement en cours : support de l'application GUI
[===== 23,9%]
```

De nombreuses autres applications sont livrées gratuitement avec Windows 11, telles que Calendrier ou encore Météo. Le menu **Démarrer** les répertorie toutes, bien évidemment.

Compatibilité des applications

25 De nombreux problèmes peuvent survenir durant l'installation d'une application : celle-ci peut par exemple essayer de copier des fichiers dans un répertoire appartenant à une ancienne version d'un système d'exploitation Microsoft, mais absent de Windows 11. Lors du développement du programme, le concepteur peut avoir fait appel à une fonction désormais inexistante. Le contrôle de compte utilisateur, qui encadre les manipulations sensibles, peut interférer avec le bon fonctionnement du processus d'installation.

26 Comme la version du noyau du système d'exploitation Windows 11 est 10.0.22000, une application recherchant un ancien numéro de version pour s'exécuter (par exemple version 6.2 pour Windows 8) sera dans l'incapacité d'effectuer cette opération.

27 Lorsque le programme est déjà installé, par exemple suite à une mise à niveau de Windows 7 vers Windows 10, puis vers Windows 11, quelques méthodes permettent de corriger les problèmes de compatibilité lors de son exécution :

- Utiliser les technologies de virtualisation : dans certains cas, il sera impossible d'exécuter une application sur Windows 11. Le client Hyper-V peut pallier cette contrainte.
- Configurer le programme : l'administrateur peut modifier les paramètres de l'application, comme les droits définis sur les fichiers et dossiers nécessaires à son fonctionnement.
- Appliquer les mises à jour : les éditeurs de logiciels proposent aux utilisateurs de télécharger les mises à jour assurant ainsi la compatibilité de leurs produits.
- Désactiver le contrôle de compte utilisateur : en diminuant la sécurité apportée par le contrôle de compte utilisateur, un programme peut devenir pleinement fonctionnel. Néanmoins, cette méthode est à éviter vu les problèmes de sécurité qu'elle engendre.
- Exécuter Microsoft Application Compatibility Toolkit : ce logiciel regroupe différents outils pour résoudre les problèmes de compatibilité.

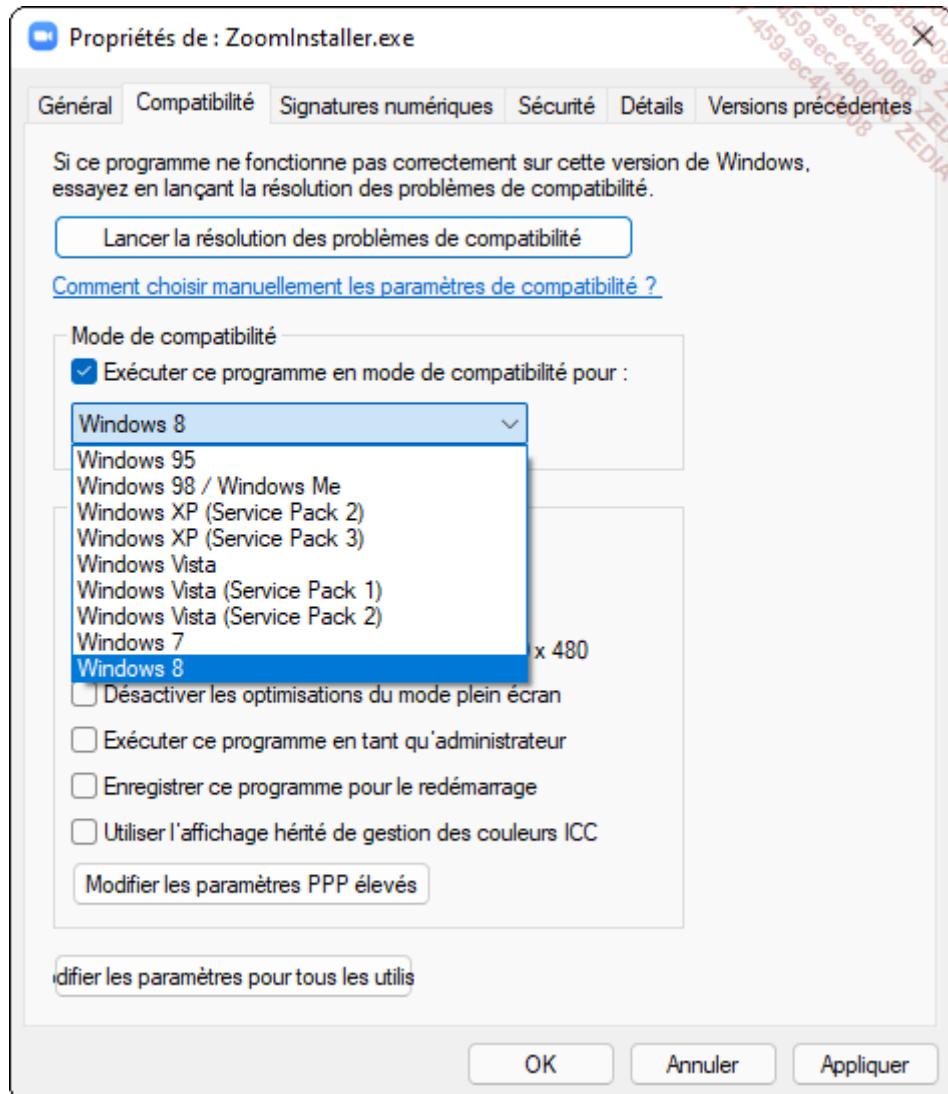
28 Qu'advient-il lorsque l'utilisateur souhaite installer une ancienne application Windows XP ou Windows 95, sur un ordinateur déjà équipé de Windows 11 ? Microsoft propose quelques outils pour pallier les nombreux problèmes de compatibilité, que nous allons détailler ci-après.

Microsoft confirme que les applications compatibles Windows 10 le seront avec Windows 11. Cela semble logique étant donné que ce système d'exploitation en est une évolution majeure.

1. Assistant Compatibilité des programmes

29 Les programmes développés pour Windows XP, Windows Vista et Windows 7 devraient fonctionner avec la nouvelle mouture de Microsoft. Dans le cas contraire, l'utilisateur a la possibilité d'exécuter le fichier d'installation (extension .exe ou .msi) en simulant son système d'exploitation de référence, à l'aide de l'Assistant Compatibilité des programmes. Pour y accéder, il suffit d'effectuer un clic avec le bouton droit sur le fichier exécutable incriminé depuis l'Explorateur de fichiers, puis de choisir **Propriétés** et de sélectionner l'onglet **Compatibilité**.

30 La première étape est de choisir le système d'exploitation à simuler parmi un large choix : Windows 95, 98/Millenium, XP (SP2 ou SP3), Vista (SP1 ou SP2), Windows 7 ou Windows 8.



31 La seconde étape est de définir les paramètres d'exécution : nombre de couleurs, résolution d'écran et l'exécution du programme en tant qu'administrateur.

32 En cliquant sur le bouton **Lancer la résolution des problèmes de compatibilité**, l'administrateur exécute un assistant qui va vérifier les paramètres pouvant bloquer le bon fonctionnement de l'application et proposer des solutions.

33 Bien entendu, l'utilisation de cet outil nécessite de s'assurer que la simulation du système cible ne va pas entraîner des problèmes de sécurité sur Windows 11.

2. Outils de compatibilité des applications

34 ACT (*Application Compatibility Toolkit*) est un ensemble d'outils de gestion des applications permettant de créer un inventaire des logiciels installés et de créer des rapports de compatibilité en vue d'une mise à niveau vers Windows 11. Il est fourni avec le kit d'évaluation et de déploiement Windows ADK.

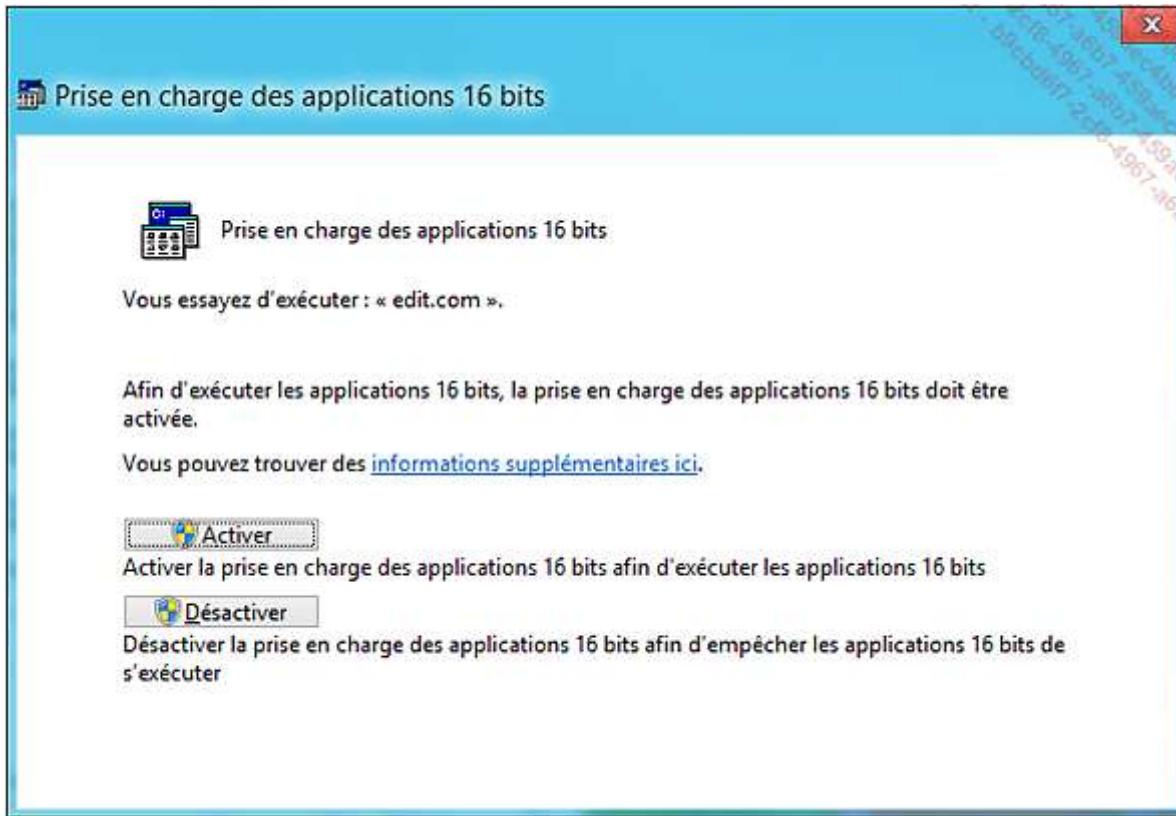
35 La console Microsoft Application Compatibility Manager nécessite une base de données SQL Server, ainsi qu'un dossier partagé pour stocker les journaux liés aux applications.

36 ACT utilise le composant Framework Microsoft .NET.

37 L'outil suit un processus d'atténuation des problèmes de compatibilité applicative en cinq étapes :

- 38 1. 39 Identification des applications installées sur les ordinateurs du parc informatique.

- 40 2. 41 Choix des applications à tester.
- 42 3. 43 Test des programmes sélectionnés précédemment.
- 44 4. 45 Analyse des résultats.
- 46 5. 47 Atténuation des problèmes à l'aide des méthodes de résolution fournies avec ACT.
- 48 L'outil propose aussi de corriger une application à l'aide d'un shim. Un shim est une portion de code injectée qui intercepte l'appel à une API (*Application Programming Interface*) et renvoie les réponses attendues par l'application cible.
- 49 C'est donc un correctif généré par ACT pour rendre compatible une application qui ne l'est pas avec Windows 11. Il modifie au choix les paramètres transmis par une application à une fonction spécifique ou intercepte le retour d'exécution d'une fonction pour rendre l'application compatible.
- 50 L'outil **Compatibility Administrator** génère les shims pour des applications répertoriées ou non. Utilisez le nœud **Compatibility Fixes** pour les visualiser.
- 51 En cliquant sur le bouton **Search**, l'administrateur sélectionne le programme qu'il souhaite analyser.
- 52 Le bouton **Fix** sert à choisir les shims à appliquer à l'application préalablement sélectionnée.
- 53 La base de données du produit contient une liste d'applications connues comme ayant des problèmes de compatibilité avec Windows 11. Utile aux services de développement, un outil comme SUA (*Standard User Analyzer*) teste une application en cours d'exécution avec des priviléges élevés afin que l'administrateur puisse savoir si elle nécessite un haut niveau d'élévation. Ainsi, les logiciels auparavant non compatibles avec la sécurité proposée par le Contrôle de compte utilisateur pourront fonctionner.
3. Prise en charge des applications 16 bits
- 54 Windows 11, en tant que système d'exploitation exclusivement architecturé en 64 bits, ne prend pas en charge les applications 16 bits. La seule solution consiste à installer une version 32 bits de Windows 10 (dans une machine virtuelle par exemple) et de suivre la procédure ci-après. Par défaut, cette fonctionnalité est désactivée. Par exemple, en utilisant une ancienne commande, comme `edit.com`, l'utilisateur est invité à activer la prise en charge des applications 16 bits.
- Saisissez `cmd` dans le champ de recherche situé dans la barre des tâches, puis cliquez sur **Invite de commandes**. Saisissez `edit.com` puis validez par la touche [Entrée]. La fenêtre de prise en charge des applications 16 bits apparaît.



Cliquez ensuite sur le bouton **Activer** pour exécuter la commande **edit**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

Paramètres et panneau de configuration

- Avec Windows 8, Microsoft a introduit une nouvelle façon de configurer son système d'exploitation avec le panneau **Paramètres**. Cette interface, plus en accord visuellement avec le reste du système, évolue et se complète petit à petit au fur et à mesure des mises à jour et des mises à niveau, le but étant de remplacer complètement le panneau de configuration datant des débuts de Windows. Néanmoins, celui-ci reste encore utile pour certains réglages avancés.
- Les paramètres et le panneau de configuration permettent aux utilisateurs de visualiser et de modifier les réglages et paramètres du système d'exploitation Windows 11. Ces interfaces donnent accès à la gestion des périphériques, à l'ajout ou la suppression d'applications, à la sécurité du poste, au paramétrage de la connexion réseau, etc. Des composants peuvent y être ajoutés lors de l'installation de certains logiciels tiers.



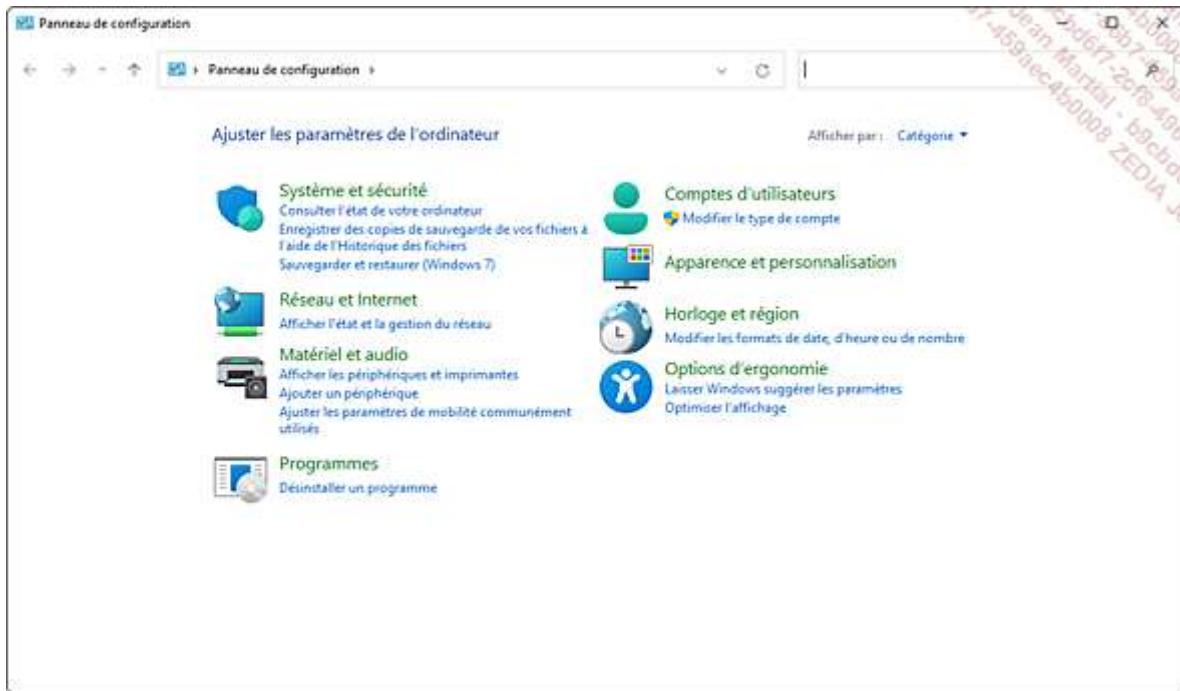
55 Pour accéder aux paramètres, cliquez sur le menu **Démarrer** puis **Paramètres**, ou bien appuyez sur les touches + I.



- Un ensemble de paramétrages est proposé :

- **Système** : l'administrateur est invité à gérer les notifications, les paramètres d'affichage, le stockage, l'activation du produit, les paramètres de récupération ou de démarrage, visualiser les informations système, etc.
- **Bluetooth et appareils** : regroupe les anciennes sections Périphériques et Téléphone. Elle permet l'installation de périphériques (imprimante, téléphone...), la configuration du pavé tactile, de la caméra ou de la souris, l'apprentissage des mouvements tactiles...
- **Réseau et Internet** : contient les connexions Wi-Fi, filaires, cellulaires, VPN ainsi que la configuration d'un proxy ou encore l'assistant Consommation des données qui affiche dans une vue synthétique la consommation des données réseau de l'utilisateur.
- **Personnalisation** : définit l'arrière-plan, les couleurs de l'interface, l'écran de verrouillage, les polices, etc.
- **Applications** : permet de désinstaller les applications, définit les logiciels par défaut en fonction de l'extension du fichier source, autorise la gestion des applications lancées au démarrage de la machine...
- **Comptes** : permet la création ou la gestion d'un compte d'utilisateur et le paramétrage des options de connexion (cf. chapitre Installation du client Windows 11, section Authentification).
- **Heure et langue** : ajuste les paramètres de langue, de fuseaux horaires, de date et d'heure.
- **Jeux** : contrôle comment le système affiche les jeux sur l'ordinateur Windows 11. C'est ici qu'il est possible de définir quelle carte graphique sera utilisée pour quelle application ou jeu.
- **Accessibilité** : permet de configurer les programmes et paramètres d'accessibilité disponibles dans Windows 11, au niveau de l'affichage et de la voix. La gestion du contrôle visuel se fait dans cette section.
- **Confidentialité et sécurité** : autorise la gestion des paramètres de sécurité de la machine, spécifie le comportement des applications vis-à-vis des données privées de l'utilisateur, comme l'accès à sa localisation géographique, définit les autorisations.
- **Windows Update** : gère le téléchargement et l'application des mises à jour du système.

- Le panneau de configuration est accessible en saisissant les premières lettres dans le menu **Démarrer**.



- Son contenu a tendance à diminuer au fur et à mesure que s'étoffent les paramètres. Les icônes ont cependant été modernisées pour être en accord avec le thème graphique de Windows 11.
- L'affichage s'effectue par défaut en catégories, mais il est possible de visualiser l'ensemble des paramètres en sélectionnant **Grandes icônes** ou **Petites icônes** dans la liste **Afficher par :**.
- Huit catégories composent le panneau de configuration :
 - Système et sécurité** : gère toutes les fonctionnalités liées à la sécurité, telles que la sauvegarde, la restauration, l'antivirus, le pare-feu...
 - Réseau et Internet** : permet de configurer l'adresse IP, les profils réseau, les options internet ou un groupe résidentiel.
 - Matériel et audio** : propose une interface de gestion des périphériques, comme une imprimante, un scanner, mais aussi les options d'alimentation ou de sons.
 - Programmes** : permet à l'utilisateur d'ajouter/supprimer/modifier un programme ou de définir un programme par défaut pour une extension.
 - Comptes d'utilisateurs** : définit les paramètres de compte local, et met à disposition le gestionnaire d'identification.
 - Apparence et personnalisation** : permet de définir le thème, le fond d'écran, la résolution du moniteur, la barre des tâches ou l'affichage des dossiers et polices.
 - Horloge et région** : gère le fuseau horaire, les langues de l'interface.
 - Options d'ergonomie** : gère les méthodes d'accessibilité à destination des personnes présentant un handicap.
- Bien souvent, l'accès à la configuration renvoie vers le panneau **Paramètres**. Il est donc fortement conseillé d'utiliser ce dernier.

Les paramètres du panneau de configuration sont stockés sous forme de fichiers au format .cpl, accessibles en exécutant le fichier correspondant. Par exemple, l'écran de réglage de la date et de l'heure est configurable depuis

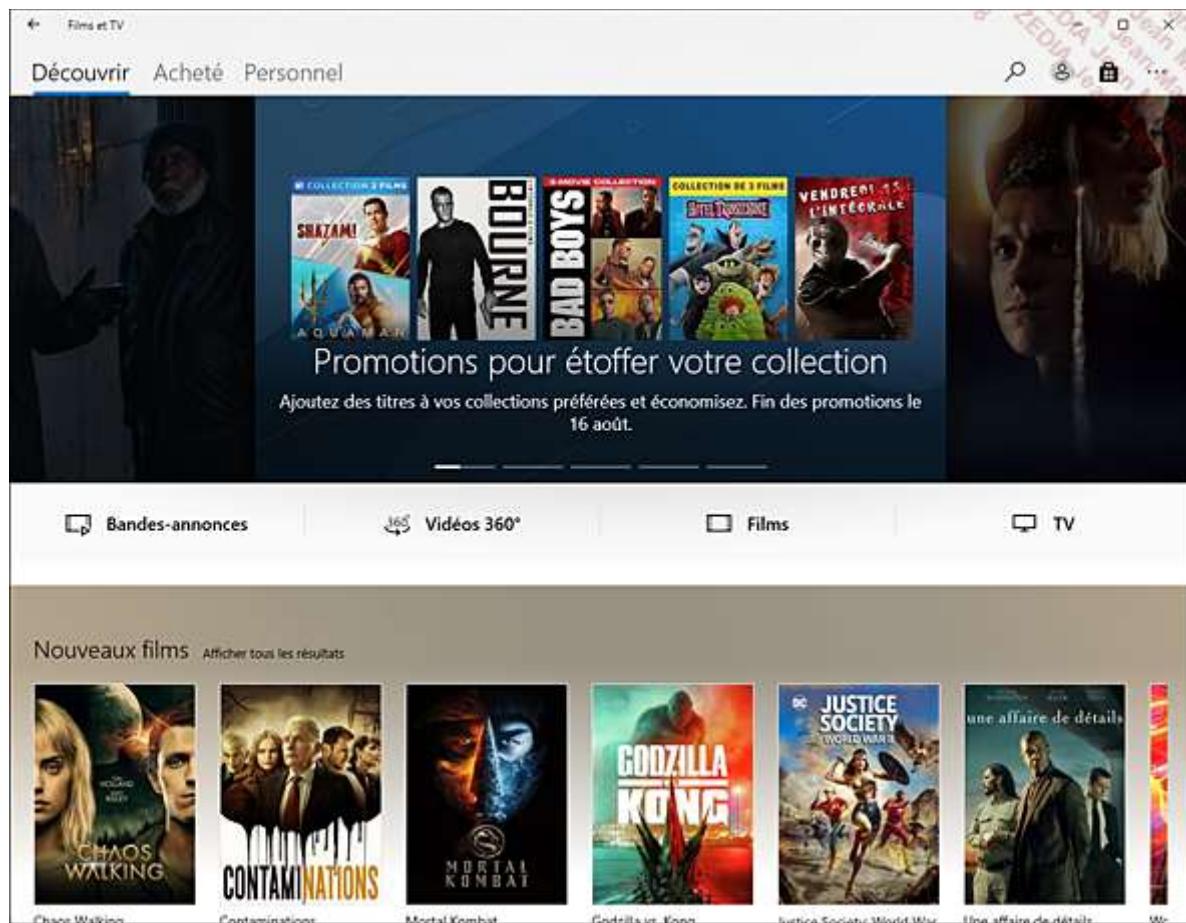
le fichier timedate.cpl contenu dans le dossier windows\system32. Pour y accéder, pressez les touches  + R et saisissez timedate.cpl puis validez par la touche [Entrée] ou le bouton **OK**. L'écran **Date et heure** apparaît.

Gestion du contenu multimédia

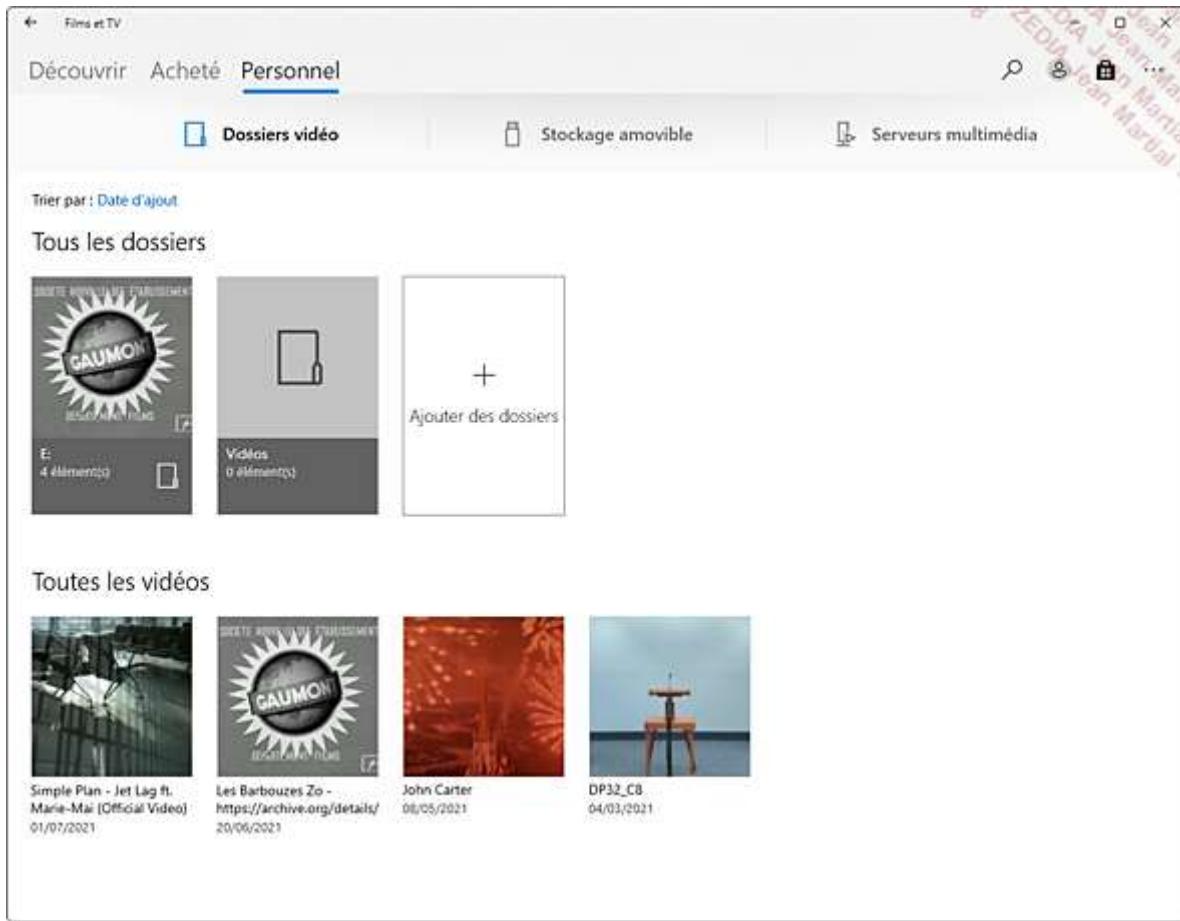
56 Visionner des films et en créer, écouter une musique, jouer en ligne, sont autant de fonctionnalités multimédias utilisées quotidiennement par les utilisateurs. Windows 11 a été conçu avec l'objectif d'optimiser la batterie tout en offrant une lecture réactive des scénarios multimédias, en réduisant la latence réseau.

1. Lecteur Film et TV

57 Le lecteur historique Windows Media est toujours disponible sur Windows 11, mais il est plus intéressant d'utiliser le nouveau gestionnaire de contenu multimédia **Films et TV**.



58 Connecté à Internet, il permet la visualisation de bandes-annonces disponibles sur le Web, l'achats de films en VOD ou la visualisation de vidéos stockées dans les dossiers de l'ordinateur ou sur un serveur multimédia comme les box des fournisseurs d'accès à Internet.



59 Il est possible de partager la projection en connectant un périphérique (écran TV par exemple), au moyen d'un câble HDMI ou avec la technologie de connexion sans fil Miracast.

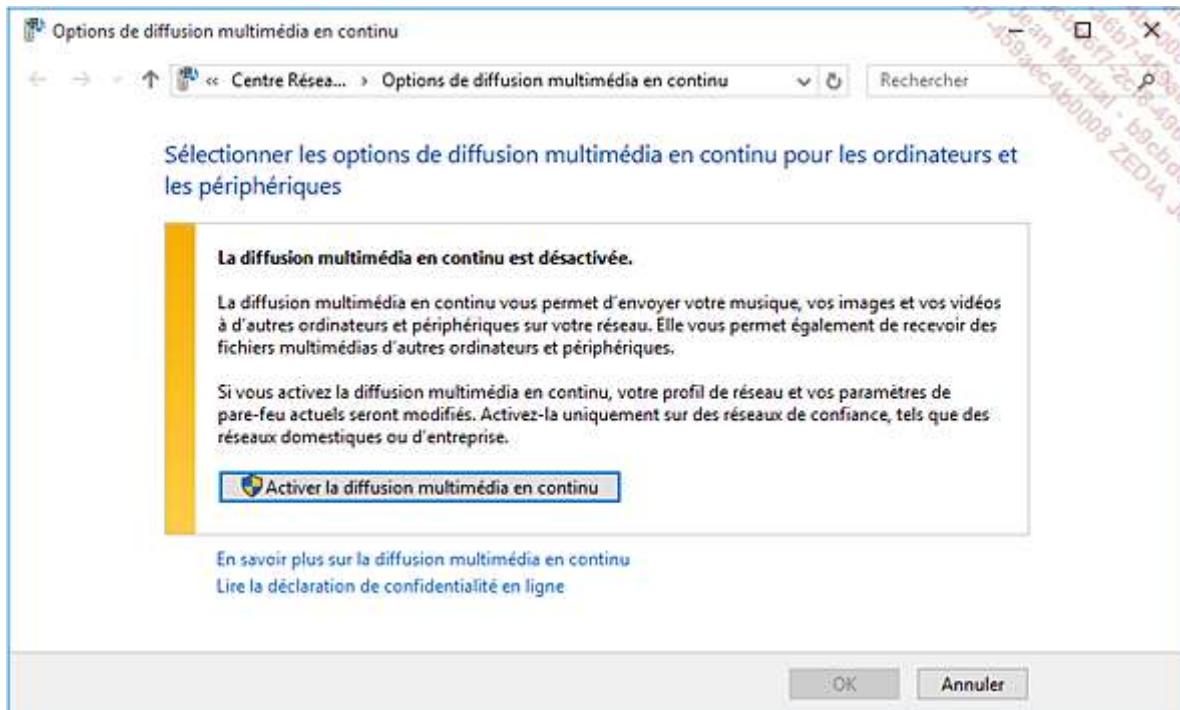
2. Lire sur

60 Devant l'avènement des réseaux sans fil et la place prépondérante qu'ils occupent dans nos foyers, de plus en plus de périphériques sont interconnectés, tels que la télévision, la chaîne hi-fi ou une console de jeux vidéo. Outre la possibilité de partage d'affichage, Windows 11 peut diffuser en continu vers ces périphériques de la musique, des vidéos ou des images. Cette fonctionnalité, connue sous le nom de **Lire sur**, peut être utilisée sur le lecteur Windows Media ou en effectuant un clic avec le bouton droit sur toutes ressources multimédias, puis **Lire sur**.

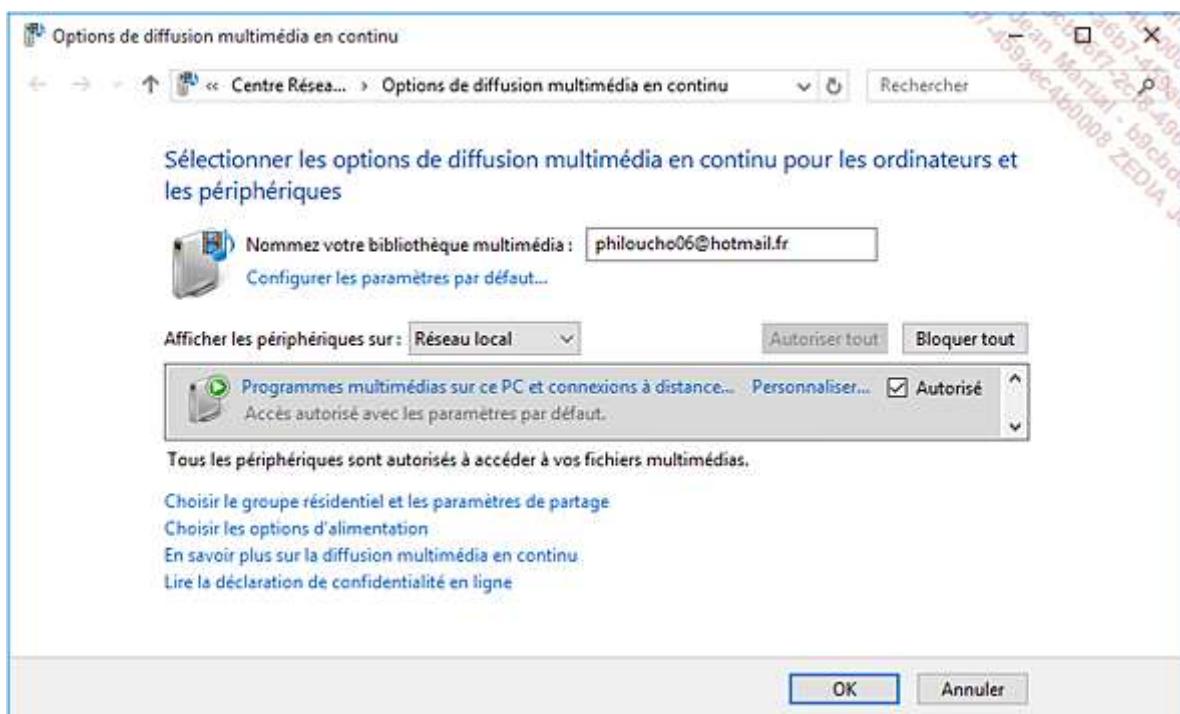
61 Avant de pouvoir utiliser cette fonctionnalité, il est nécessaire d'activer la diffusion multimédia en continu sur le poste Windows 11, grâce au Lecteur Windows Media :

Depuis le Lecteur Windows Media, cliquez sur **Diffuser en continu** puis sur **Activer la diffusion multimédia en continu** dans la fenêtre **Lecteur Windows Media**.

Cliquez sur le bouton **Activer la diffusion multimédia en continu**.



Nommez votre bibliothèque multimédia et sélectionnez le réseau qui affichera les périphériques.



Validez en cliquant sur le bouton **OK**.

62 Recherchez maintenant sur le poste de travail Windows 11 un fichier multimédia que vous souhaitez diffuser sur un périphérique de votre réseau :

Cliquez avec le bouton droit sur la ressource puis sélectionnez **Lire sur** et cliquez sur le périphérique de votre réseau devant recevoir le fichier. Dans la boîte de dialogue **Lire sur**, vous pouvez lire, mettre en pause ou annuler la diffusion du contenu multimédia.

63 L'utilisateur peut aussi utiliser la fonctionnalité **Lire sur** depuis le Lecteur Windows Media :

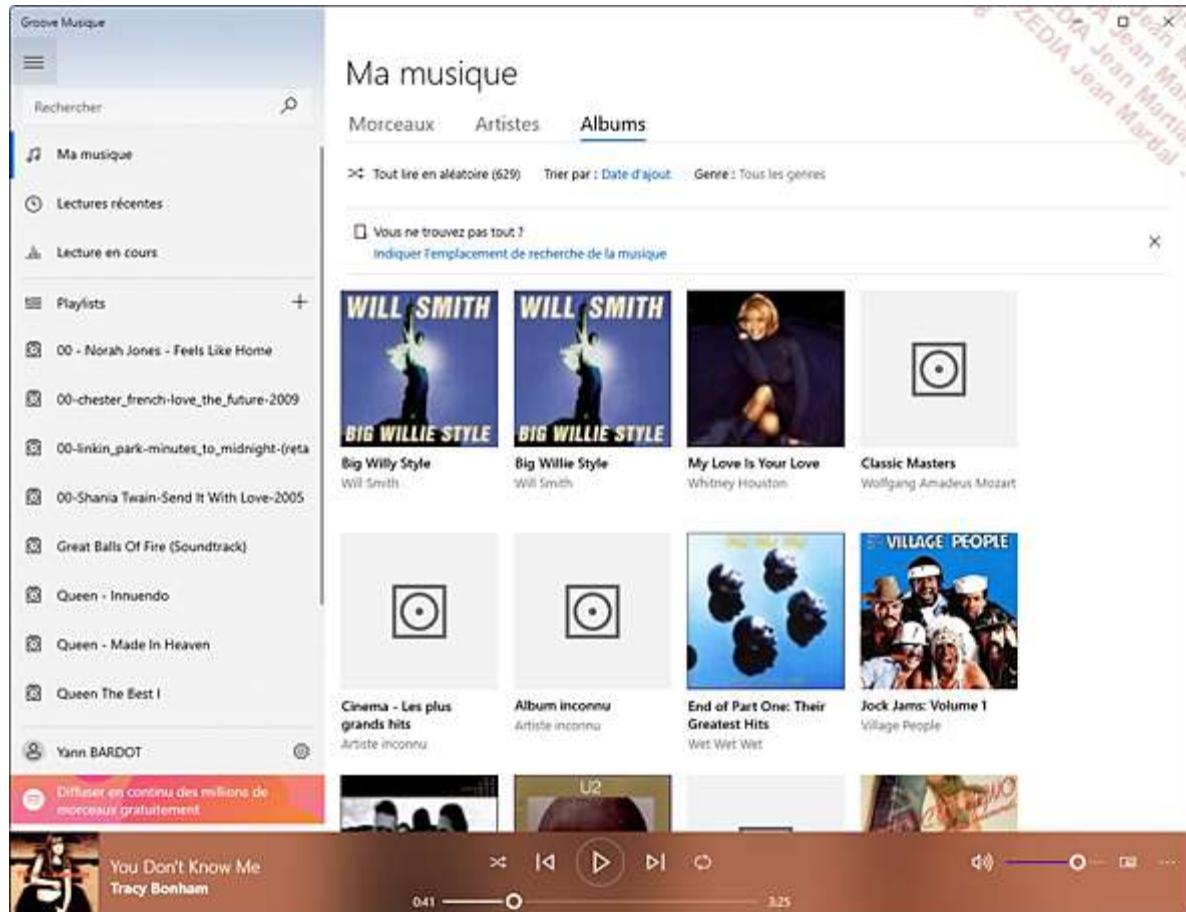
Sélectionnez l'onglet **Lecture** et glissez/déposez le fichier multimédia à lire.

Cliquez sur le bouton **Lire sur**  situé en haut à droite du volet **Liste**, puis sélectionnez le périphérique réseau qui lira le fichier.

La fonctionnalité **Lire sur** est disponible sur les quatre éditions de Windows 11.

3. Groove Musique

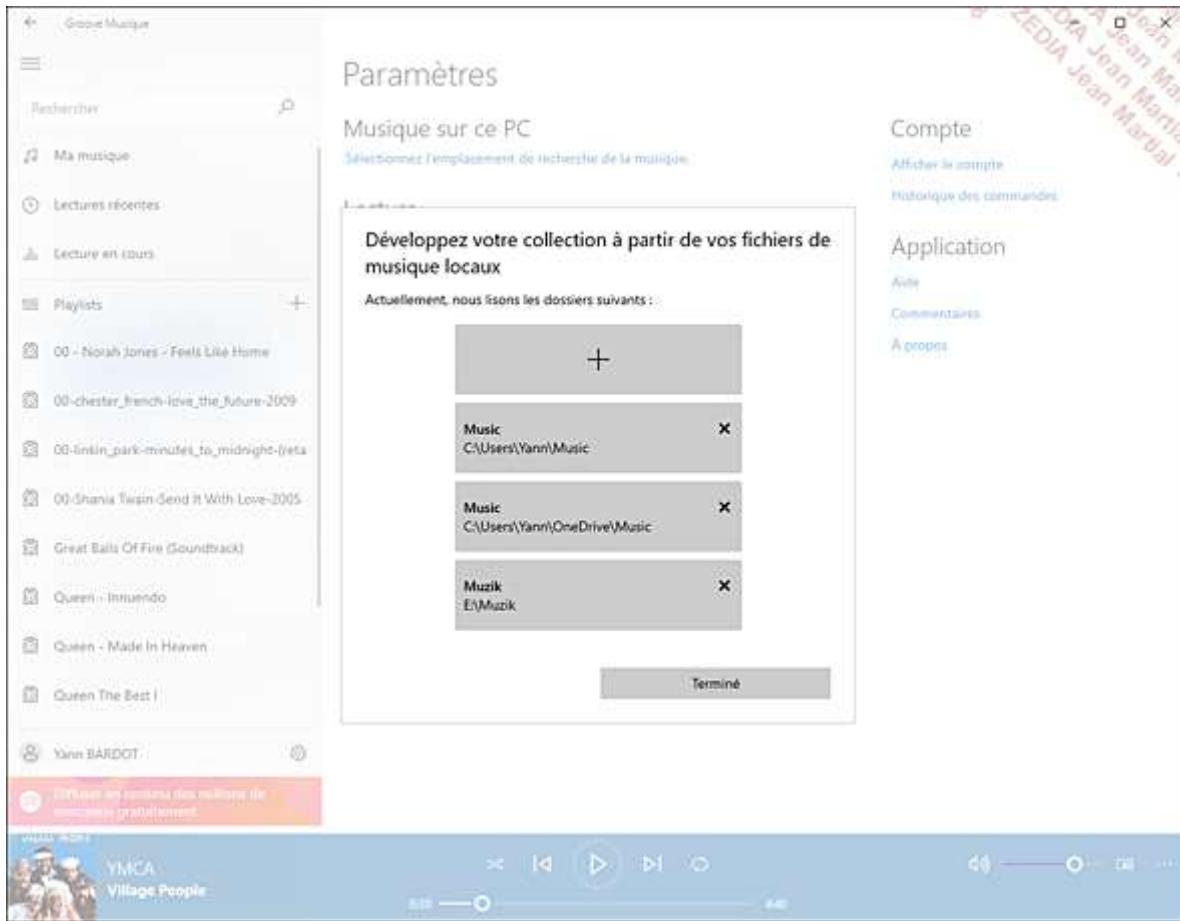
64 Windows 11 dispose également d'un gestionnaire de fichiers audio. Il permet de retrouver tous les fichiers musicaux éparsillés sur la machine, de classer des musiques par artistes ou albums, de créer des listes de lecture (*Playlists*).



65 Pour permettre à Groove de gérer d'autres dossiers, suivez ces étapes :

Ouvrez les paramètres de Groove (la roue dentée en bas à gauche, à côté de votre compte), et cliquez sur **Sélectionnez l'emplacement de recherche de la musique**.

Cliquez sur le bouton **+**, sélectionnez un dossier et cliquez sur le bouton **Ajouter ce dossier à Musique**, puis cliquez sur le bouton **Terminé**.



66 Depuis 2017, Groove ne permet plus l'achat ni la diffusion de musique depuis Internet.

Résumé du chapitre

- Windows 11 offre une nouvelle interface utilisateur, privilégiant les fonctionnalités tactiles. Le menu Démarrer perdure mais sa position et sa forme changent. Il permet toujours d'accéder à toutes les fonctionnalités de Windows.
- L'interface offre de nouvelles fonctionnalités : clarté et simplicité, diaporama affiché sur l'écran de verrouillage et le fond d'écran du bureau, recherche améliorée depuis la barre des tâches...
- L'utilisation sans clavier, en mode 100 % tactile est facilitée avec une ergonomie automatiquement adaptée (boutons, clavier virtuel...).
- La nouvelle fonctionnalité automatique de disposition d'ancre favorise la productivité. Jusqu'à huit applications exécutées peuvent être disposées sur deux écrans.
- Grâce à la fonctionnalité de personnalisation, en ouvrant une session sur un poste de travail Windows 11 Entreprise d'un domaine, l'utilisateur ne pourra pas modifier la disposition du menu Démarrer générée par l'administrateur de l'entreprise.
- Microsoft Store est un magasin qui regroupe dans différentes catégories des applications à télécharger. De nombreuses applications sont livrées avec Windows 11, comme Courrier, Photos... La mise à jour des applications est automatisée. Ce magasin permet désormais d'installer des applications Win32 et Android.

- Pour naviguer sur Internet, Microsoft encourage fortement d'utiliser son nouveau navigateur nommé Edge, et supprime Internet Explorer, même si ce dernier reste disponible dans Edge pour des raisons de compatibilité avec des sites d'entreprises.
- Les programmes développés pour les systèmes antérieurs devraient fonctionner avec la nouvelle mouture de Microsoft. Dans le cas contraire, l'utilisateur a la possibilité d'utiliser l'Assistant Compatibilité des programmes, les outils ACT ou encore la technologie de virtualisation Client Hyper-V.
- Le logiciel de gestion du contenu vidéo est désormais Films et TV, tandis que Groove Musique se destine aux fichiers musicaux.

Gestion des disques et des pilotes

Partitionnement et gestion des fichiers

Toute nouvelle installation de Windows 11 implique que l'administrateur se soit posé les bonnes questions : mon matériel est-il adapté ? Mes logiciels sont-ils compatibles ? De quel espace disque ai-je besoin pour stocker les données utilisateur et les programmes ?

Partitionner un disque dur signifie le diviser en sections distinctes, afin par exemple de séparer le stockage des données du système d'exploitation de celles des utilisateurs ou des journaux d'événements...

En général, un ordinateur équipé du système d'exploitation Windows 11 est livré avec un seul disque physique, configuré comme un volume unique. Nous allons voir qu'il est possible de réduire ou d'augmenter la taille d'une partition, ou encore d'améliorer la disponibilité en utilisant des technologies éprouvées.

Des logiciels livrés avec Windows 11 permettent d'optimiser les performances du système de fichiers, comme le défragmenteur de disque ou les quotas.

Dans le cas où les différentes opérations effectuées sur le disque dur n'améliorent pas ses performances de manière significative, il peut être intéressant d'acquérir un disque SSD (*Solid-State Drive*), plus rapide et robuste car constitué de mémoire à semi-conducteurs à l'état solide. L'usage d'un tel périphérique diminue la consommation électrique. Néanmoins, le coût au Mo de cette technologie reste encore relativement élevé.

1. Partitions GPT

L'installation de Windows 11 est uniquement possible sur un disque dur utilisant une table de partitionnement au format **GPT** (*GUID Partition Table*). Uniquement disponible sur un ordinateur UEFI, la table de partition GPT résout les restrictions de sa prédécesseure, MBR. Contrairement à celle-ci qui gère des références LBA (*Logical Block Address*) codées sur 32 bits, une partition GPT étend l'adressage à 64 bits lui permettant la prise en charge de 128 partitions principales et offre une redondance pour une taille de volume maximale de 18 Eo (exaoctets). De plus, une partition système ESP (*Extensible Firmware Interface System Partition*) est stockée sur chaque disque démarable, ainsi qu'une partition MSR (*Microsoft Reserved Partition*). La technologie GPT est disponible depuis Windows Vista et Windows Server 2008, et sur toutes les versions ultérieures.

Étant donné que Windows 11 nécessite un démarrage sécurisé (*Secure Boot*) et que celui-ci n'est disponible que sur un système UEFI, les disques au format MBR ne sont pas supportés par ce système d'exploitation. Si l'architecture de la machine supporte les deux formats de microprogrammes BIOS et UEFI, il sera nécessaire de choisir ce dernier et donc la structure GPT pour installer Windows 11.

Lors de l'installation de Windows 11 sur un disque GPT de démarrage, ce dernier crée trois partitions :

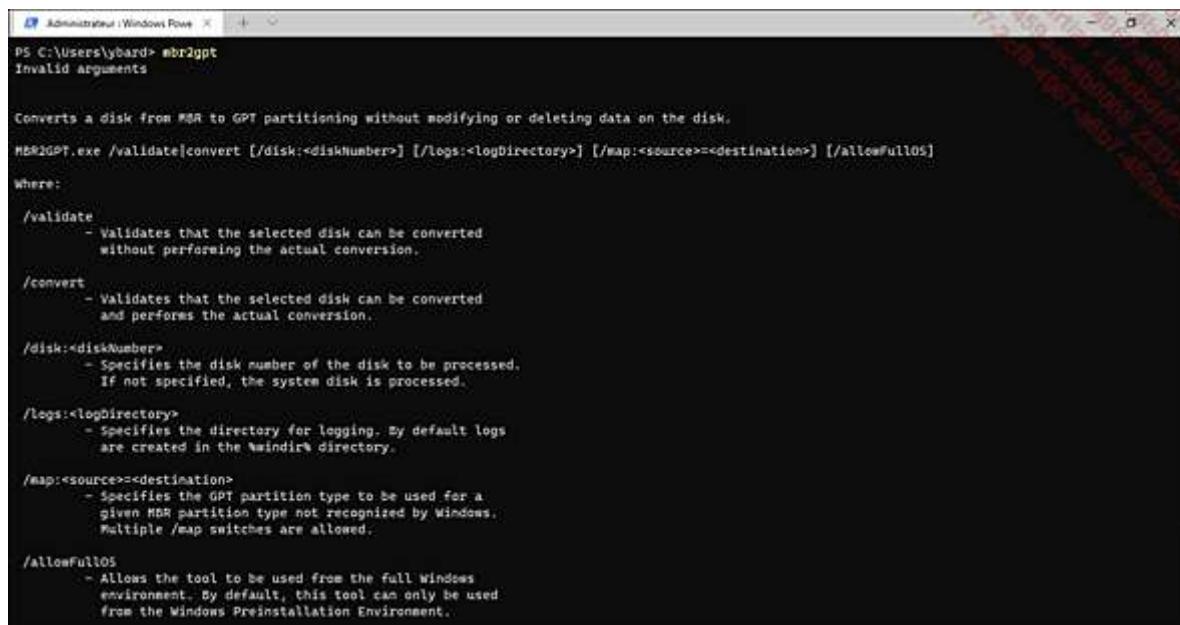
- ESP (*EFI System Partition*) : d'une taille variable, cette partition contient le gestionnaire de démarrage nécessaire à l'exécution de Windows 11.
- Celle qui héberge le système d'exploitation.
- MSR : partition cachée ne possédant aucune lettre de lecteur, celle-ci est réservée au fonctionnement de Windows 11. Elle ne doit pas être chiffrée. Elle est parfois appelée partition de récupération.

Depuis la version Creators Update de Windows 10, il est possible de convertir simplement une partition MBR vers une partition GPT à l'aide de l'outil en ligne de commande mbr2gpt.exe, sans modifier ou supprimer les données du disque. Cette commande est également disponible avec Windows 11.

Depuis une invite de commandes, tapez la commande :

mbr2gpt.exe

Le paramètre /validate permet de valider la faisabilité de conversion d'un disque spécifique et /convert convertit le disque ciblé.



```
Administrator: Windows PowerShell
PS C:\Users\lybardi> mbr2gpt
Invalid arguments

Converts a disk from MBR to GPT partitioning without modifying or deleting data on the disk.

MBR2GPT.exe [/validate][convert [/disk:<diskNumber>] [/logs:<logDirectory>] [/map:<source>=<destination>] [/allowFullOS]
where:
/validate
    - Validates that the selected disk can be converted
        without performing the actual conversion.

/convert
    - Validates that the selected disk can be converted
        and performs the actual conversion.

/disk:<diskNumber>
    - Specifies the disk number of the disk to be processed.
        If not specified, the system disk is processed.

/logs:<logDirectory>
    - Specifies the directory for logging. My default logs
        are created in the %windir%\Logs directory.

/map:<source>=<destination>
    - Specifies the GPT partition type to be used for a
        given MBR partition type not recognized by Windows.
        Multiple /map switches are allowed.

/allowFullOS
    - Allows the tool to be used from the full Windows
        environment. By default, this tool can only be used
        from the Windows Preinstallation Environment.
```

Trois autres outils permettent de gérer les partitions utilisées par Windows 11 : **DiskPart**, la console de **Gestion des disques** et **Windows PowerShell**.

a. Utilitaire DiskPart

L'exécution de DiskPart nécessite que l'utilisateur soit membre du groupe Opérateurs de sauvegarde ou Administrateurs. L'outil peut être intégré à un fichier de réponses pour automatiser le partitionnement du disque dur de l'utilisateur lors de l'installation de Windows 11.

DiskPart déclenche uniquement des actions sur l'ordinateur local, ce qui limite sa portée.

La plupart des commandes DiskPart fonctionnent sur un disque spécifique, une partition ou un volume, ce qui signifie que c'est à l'utilisateur de définir la portée de ses modifications.

Voici par exemple la procédure permettant de réduire un disque de 50 Mo en ligne de commande. Chaque commande doit être validée par la touche [Entrée] :

Cliquez avec le bouton droit sur le menu **Démarrer** puis sur **Terminal Windows (administrateur)**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît. Dans la fenêtre **Administrateur : Windows PowerShell**, saisissez : diskpart

Listez les disques en tapant : list disk

Sélectionnez ensuite un disque à réduire en tapant la commande : select disk NUMERODUDISQUE

Listez les volumes disponibles en tapant la commande : list volume

Puis, sélectionnez le volume à réduire : select volume NUMERODUVOLUME

Diminuez la partition de 50 Mo en tapant : shrink desired=50

Quittez l'invite avec : exit

L'image suivante montre le résultat de ces commandes :

```
Copyright (C) Microsoft Corporation.
Sur l'ordinateur : DESKTOP-447K070

DISKPART> list disk

Nº disque Statut Taille Libre Dyn GPT
----- ----- -----
Disque 0 En ligne 465 G octets 3872 K octets *

DISKPART> select disk 0

Le disque 0 est maintenant le disque sélectionné.

DISKPART> list volume

Nº volume Ltr Nom Fs Type Taille Statut Info
----- ----- -----
Volume 0 C NTFS Partition 240 G Sain Démarrag
Volume 1 D DATA NTFS Partition 224 G Sain
Volume 2 FAT32 Partition 100 M Sain Système
Volume 3 NTFS Partition 584 M Sain Masqué

DISKPART> select volume 1

Le volume 1 est le volume sélectionné.

DISKPART> shrink desired=50

DiskPart a réduit la taille du volume de : 50 M octets

DISKPART> |
```

D'autres options sont disponibles, comme la possibilité d'attacher (attach) un fichier de disque virtuel, de fusionner un disque enfant avec son parent (merge) ou encore de définir un disque hors connexion (offline).

Pour étendre une partition, utilisez l'option extend. Par exemple : extend size=50 Disk=3

Vous pouvez convertir un disque MBR en disque GPT grâce à la commande diskpart convert GPT.

Néanmoins, avant d'effectuer cette opération, il est conseillé de sauvegarder les données présentes et de s'assurer que le disque est actif. Si votre ordinateur contient plusieurs systèmes d'exploitation installés sur un disque MBR, la conversion en disque GPT supprimera la possibilité de les démarrer.

La conversion d'une partition GPT en une partition MBR n'est possible que si le disque ne contient aucun volume ou partition.

DiskPart prend aussi en charge l'exécution d'un script à l'aide du commutateur /s.

Exemple : diskpart /s monscript.txt.

b. Console Gestion des disques

Le composant logiciel enfichable **Gestion des disques** permet d'effectuer toutes les actions courantes sur les disques Windows 11 de manière graphique : l'initialisation, la conversion et la création des volumes ou du style de partition et, bien entendu, le formatage du système de fichiers.

La majorité des tâches associées aux disques peuvent être effectuées sans nécessiter le redémarrage de l'ordinateur.

Partitionner un disque peut engendrer dans certains cas la perte de données, il est donc fortement recommandé de sauvegarder celles-ci avant toute modification majeure de vos partitions.

Pour exécuter la console **Gestion des disques**, cliquez avec le bouton droit sur le menu **Démarrer** et sélectionnez **Gestion du disque**.

Une autre solution est de presser les touches  + R depuis l'écran d'accueil puis de saisir diskmgmt.msc dans la fenêtre de recherche.

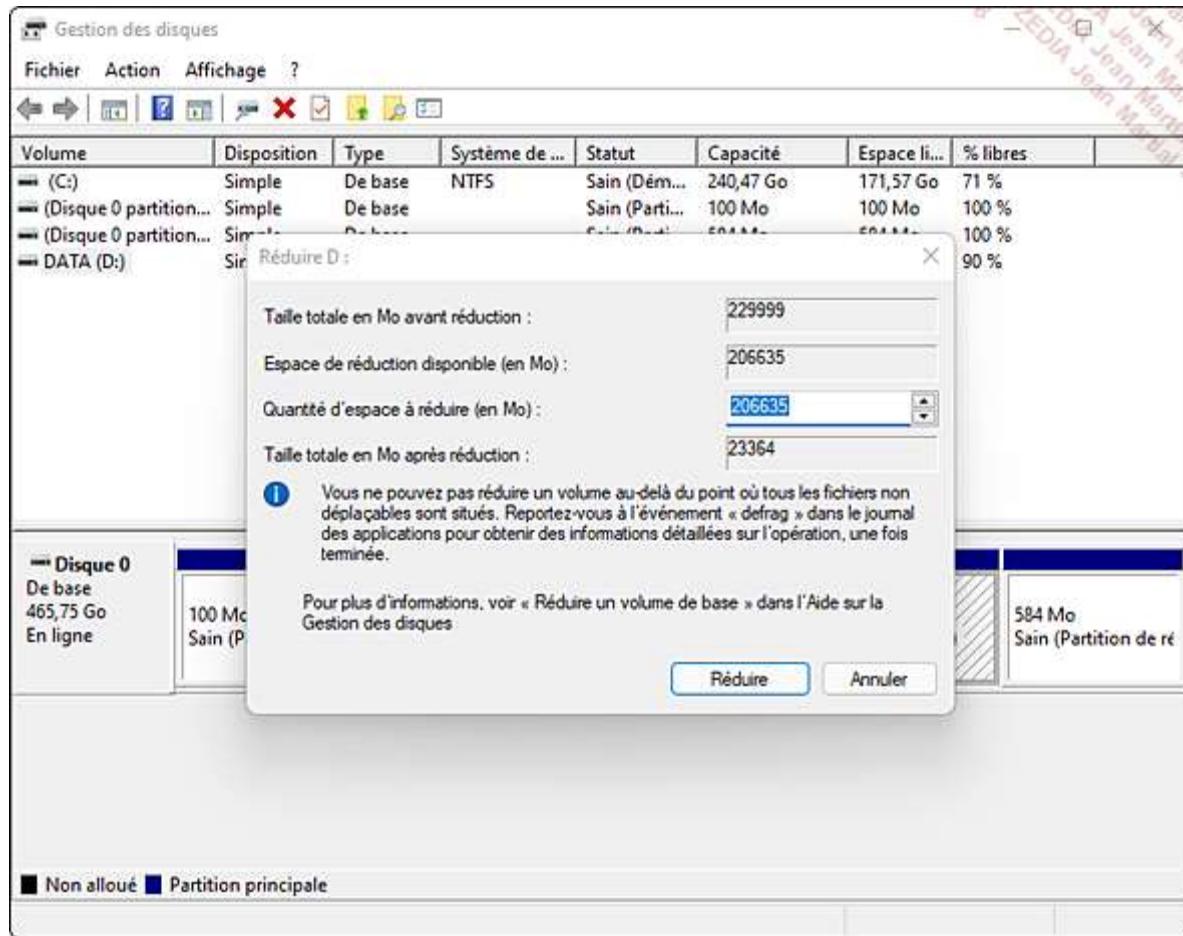
Notez la conversion automatique d'un disque MBR en GPT lorsque l'utilisateur ajoute plus de quatre partitions à un disque de base.

La console permet aussi de démarrer un disque dur virtuel Windows (extension VHD ou VHDX) sur le matériel désigné sans aucun autre système d'exploitation parent (cf. chapitre Installation du client Windows 11, section Disque virtuel avec démarrage natif).

Étendre ou réduire un volume nécessite de respecter quelques règles en amont : défragmentez le disque et vérifiez qu'aucun fichier d'échange n'y est stocké, et idéalement, sauvegardez vos données.

Pour réduire un volume, il suffit d'effectuer la procédure suivante :

Cliquez avec le bouton droit sur la partition que vous souhaitez réduire, puis choisissez l'option **Réduire le volume**.



Dans la boîte de dialogue, entrez la quantité d'espace à réduire et validez par le bouton **Réduire**.

La console **Gestion des disques** peut administrer les partitions d'un ordinateur distant, à condition que celui-ci soit membre d'un domaine Active Directory.

c. Commandes Windows PowerShell

Le langage de script PowerShell, successeur de l'interface en ligne de commande et du logiciel Windows Scripting Host, permet d'effectuer nativement des opérations complexes sur le disque dur de l'ordinateur. Elle remplace également l'historique Invite de commandes. D'ailleurs, avec Windows 11, c'est sous la dénomination Terminal que se cache PowerShell.

Pour exécuter l'invite Windows PowerShell, faites un clic droit sur le bouton **Démarrer** et sélectionnez **Windows Terminal (administrateur)**. Validez le message de contrôle de compte utilisateur.

Pour obtenir la liste de toutes les commandes liées aux opérations sur les disques, saisissez : `get-command -module storage | more`

Appuyez sur la touche [Entrée] pour afficher le résultat ligne par ligne ou sur la touche [Espace] pour afficher le résultat page par page. [Q] permet de quitter l'affichage.

Notez que PowerShell supporte l'autocomplétion : il suffit de taper les premières lettres d'une commande et d'appuyer sur la touche [Tab] pour qu'il vous propose de la compléter. Appuyez de nouveau sur [Tab] jusqu'à trouver la commande que vous recherchez.

Pour visualiser l'historique des commandes tapées, saisissez :

`history`

La commande qui efface toutes les données présentes sur les partitions d'un disque dur est :

clear-disk

Pour afficher la liste de tous les disques durs d'un ordinateur, saisissez :

get-disk

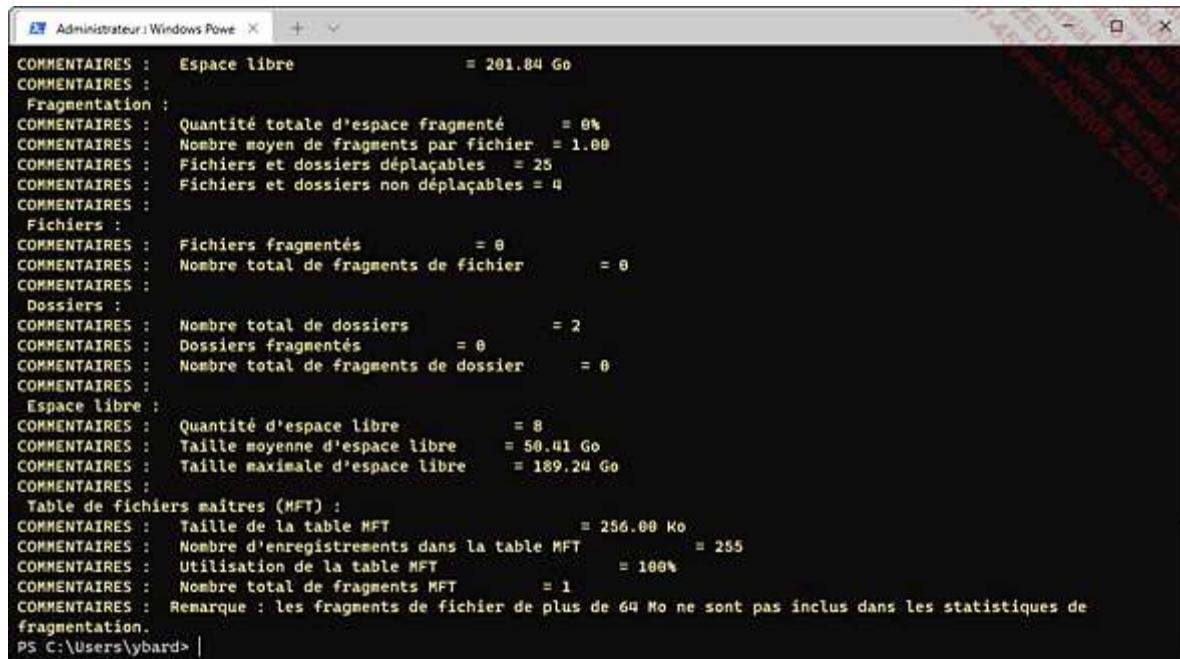
Pour formater une partition E: en utilisant le système de fichiers NTFS et en la nommant "Donnees" tapez :

format-volume -DriveLetter E -NewFileSystemLabel Donnees

-FileSystem NTFS

Pour défragmenter la partition D: saisissez :

Optimize-Volume -DriveLetter D -Defrag -Verbose



```
Administrateur : Windows PowerShell
COMMENTAIRES : Espace libre = 201.84 Go
COMMENTAIRES :
Fragmentation :
COMMENTAIRES : Quantité totale d'espace fragmenté = 0%
COMMENTAIRES : Nombre moyen de fragments par fichier = 1.00
COMMENTAIRES : Fichiers et dossiers déplaçables = 25
COMMENTAIRES : Fichiers et dossiers non déplaçables = 4
COMMENTAIRES :
Fichiers :
COMMENTAIRES : Fichiers fragmentés = 0
COMMENTAIRES : Nombre total de fragments de fichier = 0
COMMENTAIRES :
Dossiers :
COMMENTAIRES : Nombre total de dossiers = 2
COMMENTAIRES : Dossiers fragmentés = 0
COMMENTAIRES : Nombre total de fragments de dossier = 0
COMMENTAIRES :
Espace libre :
COMMENTAIRES : Quantité d'espace libre = 8
COMMENTAIRES : Taille moyenne d'espace libre = 50.41 Go
COMMENTAIRES : Taille maximale d'espace libre = 189.24 Go
COMMENTAIRES :
Table de fichiers maîtres (MFT) :
COMMENTAIRES : Taille de la table MFT = 256.00 Ko
COMMENTAIRES : Nombre d'enregistrements dans la table MFT = 255
COMMENTAIRES : Utilisation de la table MFT = 100%
COMMENTAIRES : Nombre total de fragments MFT = 1
COMMENTAIRES : Remarque : les fragments de fichier de plus de 64 Mo ne sont pas inclus dans les statistiques de fragmentation.
PS C:\Users\ybard> |
```

Pour optimiser un disque SSD possédant la lettre de lecteur X :

Optimize-Volume -DriveLetter X -ReTrim -Verbose

d. Commandes courantes d'opérations sur les disques

Windows 11 propose un ensemble de commandes pour effectuer des opérations sur les disques de l'ordinateur.

Le système ne peut être installé que sur une partition NTFS. Néanmoins, si l'utilisateur possède un disque formaté en volume FAT (*File Allocation Table*), la commande convert.exe permettra de la convertir en volume NTFS, sans perte de données. En revanche, l'inverse n'est pas possible. L'utilitaire fonctionne aussi avec les périphériques de stockage amovibles USB.

Pour convertir un volume C: en FAT32 vers le format NTFS, en démontant le volume si nécessaire, saisissez dans une fenêtre de Terminal :

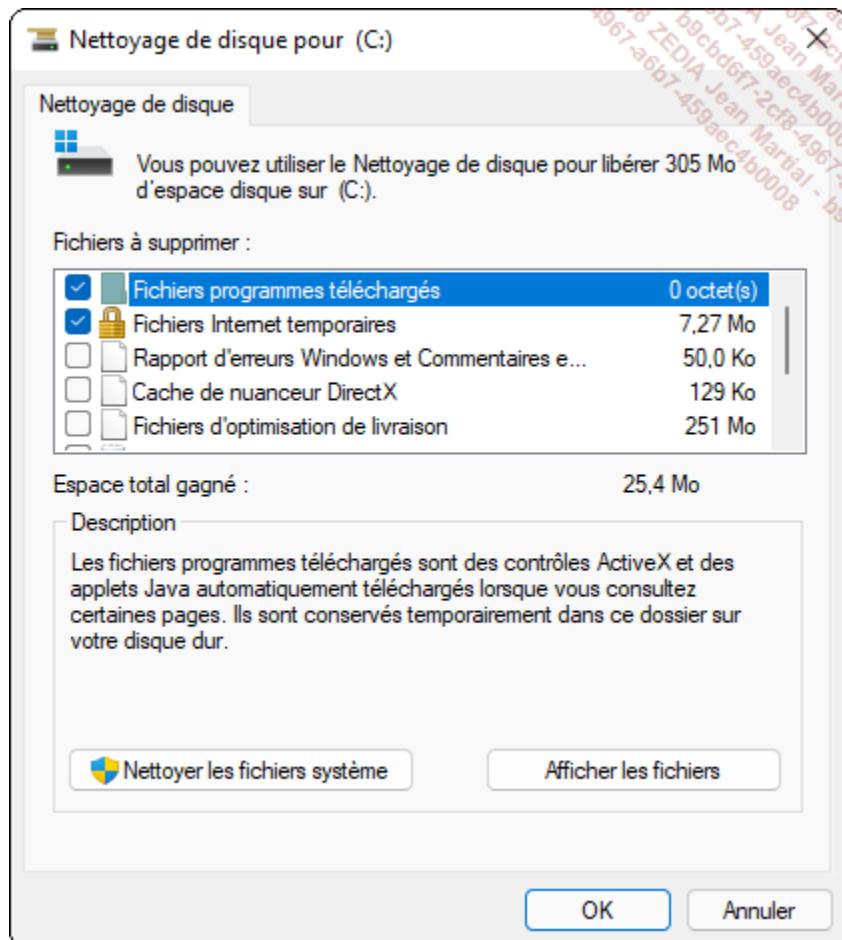
convert c: /FS:NTFS /X

La commande format.exe permet de formater un disque en spécifiant le système de fichiers parmi FAT, FAT32, EXFAT, NTFS ou UDF (*Universal Disk Format*). Pour formater le volume D: en système de fichiers NTFS rapidement, et en s'assurant qu'il sera au préalable démonté, saisissez la commande suivante en tant qu'administrateur dans une invite de commandes :

format D: /FS:NTFS /Q /X

L'outil de nettoyage de disque cleanmgr.exe supprime les fichiers inutiles (corbeille, fichiers temporaires, rapports d'erreurs, clichés instantanés, programmes inutilisés, fichiers non critiques Windows Defender, etc.) de l'ordinateur après l'avoir analysé. Il fonctionne depuis une interface graphique.

Pour l'exécuter, pressez les touches **Windows + R** puis saisissez cleanmgr.exe et validez en pressant la touche [Entrée]. Sélectionnez le lecteur sur lequel vous souhaitez libérer de l'espace disque et cliquez sur le bouton **OK**.



Windows 11 propose la commande chkdsk.exe. Celle-ci permet de vérifier un disque, de corriger les problèmes rencontrés et d'afficher un rapport général. Par exemple, lors d'une coupure de courant imprévue, les métadonnées du système de fichiers peuvent être endommagées.

Le système détecte une erreur dans les métadonnées NTFS, puis tente de la corriger sans positionner le disque en mode hors connexion. Si l'erreur est sérieuse, l'utilisateur est prévenu des actions à entreprendre pour corriger le problème.

En mode hors connexion, le temps nécessaire à l'exécution de chkdsk est désormais proportionnel au nombre d'endommagements et non plus au nombre de fichiers présents. À l'aide du paramètre /spotfix (dédié aux partitions NTFS), les corrections sur les volumes nécessitent quelques secondes, contre plusieurs heures auparavant.

La commande chkdsk doit être exécutée en tant qu'administrateur dans un Terminal de commandes.

L'état des lecteurs est affiché dans le **Centre de notifications**.

Chkdsk ne fonctionnant que localement, l'applet de commande PowerShell Repair-volume permet de gérer l'intégrité des disques sur des ordinateurs distants.

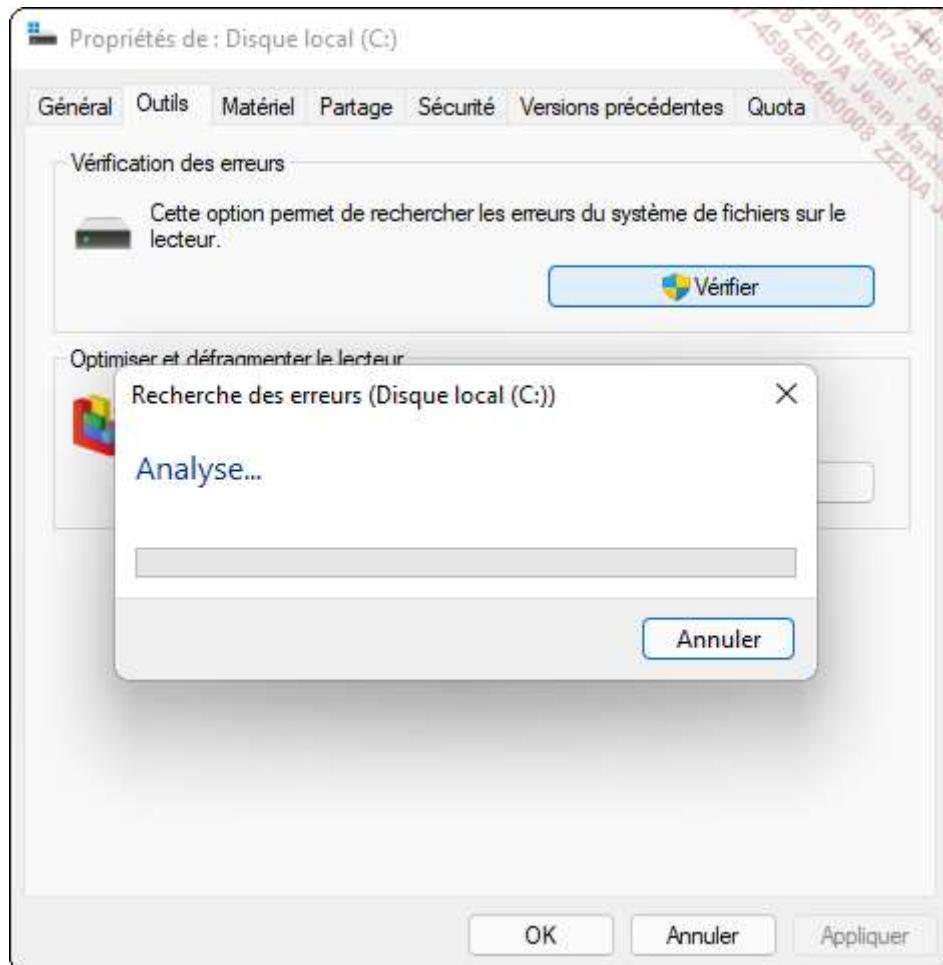
Si l'utilisateur ne souhaite pas redémarrer son système pour que Chkdsk corrige les erreurs, il peut utiliser l'onglet **Outils** des propriétés du volume NTFS :

Cliquez sur l'**Explorateur de fichiers** situé dans la barre des tâches puis développez **Ce PC**.

Cliquez avec le bouton droit sur la lettre de lecteur de votre disque dur défectueux, puis choisissez **Propriétés**.

Sélectionnez l'onglet **Outils** et cliquez sur le bouton **Vérifier**.

L'analyse du disque est exécutée et les éventuelles erreurs sont corrigées.



Si le disque impacté contient le système Windows, l'utilisateur devra probablement redémarrer son ordinateur pour résoudre les problèmes détectés.

2. Espaces de stockage

Grâce à Windows 11, l'utilisateur peut accéder à des technologies de redondance afin de se protéger contre un disque défaillant ou d'ajouter de l'espace disque supplémentaire en cas de capacité insuffisante grâce à la fonctionnalité **Espaces de stockage**.

Cette fonctionnalité procure aux disques NTFS une fiabilité plus importante et surtout des fonctionnalités de récupération.

Windows 11 permet donc de répartir les données sur plusieurs disques afin de garantir la tolérance aux pannes ou d'améliorer les performances en lecture et en écriture via un système RAID logiciel, qui s'avère moins performant qu'un RAID matériel s'appuyant sur un contrôleur dédié, mais toutefois utile pour renforcer la sécurité des données, tout en augmentant leur disponibilité.

Six niveaux de RAID existent, chacun utilisant un algorithme propre. Nous allons en détailler quelques-uns avant de décrire plus précisément la fonctionnalité **Espaces de stockage** :

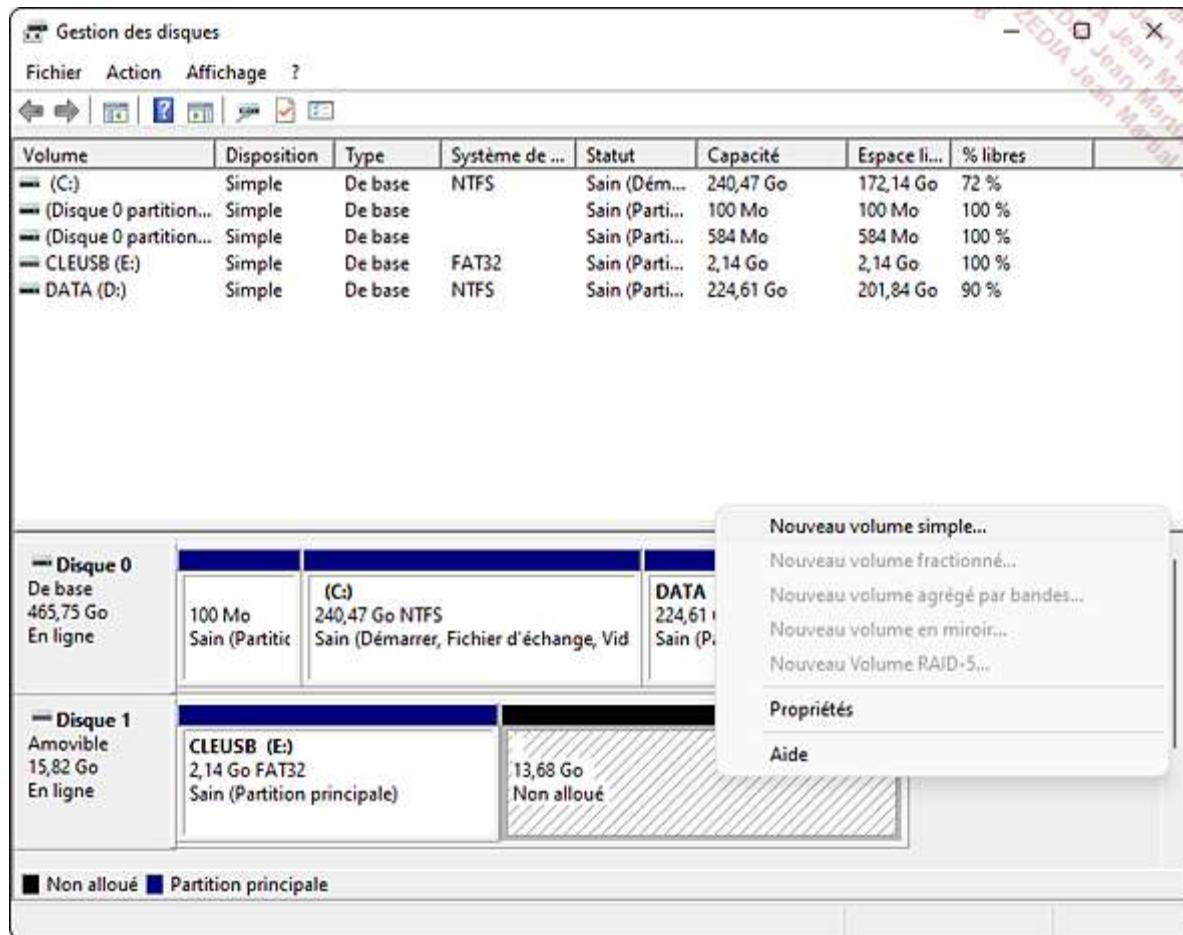
- **Volume simple** : ce type de volume permet de stocker des données dans une partie d'un disque physique mais peut être étendu sur le même disque. Aucune tolérance de panne n'est proposée, toute

défaillance du disque physique entraînera la perte des volumes simples rattachés. Les performances des entrées/sorties sont équivalentes à celles du disque physique hôte.

Avec Windows 11, il est possible de créer plus de 26 volumes simples, mais seules 26 lettres de lecteur (l'alphabet) sont disponibles pour accéder à ces volumes. Dans ce cas, vous pourrez monter les partitions sans lettre de lecteur dans des dossiers.

Pour créer un volume simple :

Ouvrez la console **Gestion des disques** (console MMC diskmgmt.msc). Sélectionnez un espace libre, cliquez dessus avec le bouton droit et sélectionnez **Nouveau volume simple**.



Définissez ensuite la taille en **Mo** du volume, sa **lettre de lecteur** ou son **dossier NTFS vide**.

- **Volume fractionné** : permet de joindre l'espace disque disponible sur au moins deux disques physiques (et au plus 32) dans un seul volume. Malgré l'absence de tolérance de panne, un volume fractionné peut être réduit ou étendu. Lors de sa création, il faut définir la quantité d'espace à allouer à partir de chaque disque physique. De même lors de sa réduction, il n'est pas possible de réduire un espace du volume fractionné sur un disque, mais l'intégralité des espaces qui le composent. Depuis la console Gestion des disques, sélectionnez l'action **Nouveau volume fractionné**.
- **Volume agrégé par bandes (RAID0)** : équivalent au volume fractionné sur le nombre de disques minimum (deux) et maximum (32) à utiliser, le volume agrégé par bandes nécessite quant à lui un espace identique sur chaque disque. Vous ne pouvez pas étendre ou réduire un volume RAID0 mais les performances d'entrées/sorties sont meilleures qu'un volume simple ou fractionné. Enfin, aucune tolérance de panne n'est fournie, la perte d'un disque entraînant la perte de l'intégralité du volume agrégé par bandes. RAID0 est souvent utilisé pour isoler le fichier d'échange. Depuis la console Gestion des disques, sélectionnez l'action **Nouveau volume agrégé par bandes**.

- **Volume en miroir (RAID1)** : deux disques physiques sont nécessaires, chacun contenant exactement les mêmes données que l'autre, d'où l'utilisation du mot "miroir" pour décrire cette redondance. RAID1 permet d'effectuer une tolérance de panne : la capacité utilisée pour créer ce type de volume est de 50 % de l'espace disque total disponible. Ainsi, si deux disques de 100 Go étaient utilisés pour créer un volume en miroir, seuls 100 Go seraient utilisables par l'utilisateur. Le coût de l'octet est donc relativement important. En cas de disque défaillant, Windows 11 est capable de continuer à fonctionner normalement, en attendant le remplacement du disque défectueux et la reconstruction du RAID1. Depuis la console Gestion des disques, sélectionnez l'action **Nouveau volume en miroir**.
- **Volume agrégé par bandes avec parité (RAID5)** : il faut au minimum trois disques physiques pour créer un volume RAID5, et jusqu'à 32 disques. Ce système fournit une tolérance de panne mais reste moins performant que RAID1 dont la reprise est plus rapide en cas de défaillance. Un volume RAID5 utilise la parité, information indiquant sur quel disque a été stocké tel ou tel fragment des données. Ainsi, si un fragment d'une donnée devait manquer, la comparaison entre les informations de parité et les autres fragments de la donnée permettrait de reconstituer le fragment perdu. Le RAID5 gère la défaillance d'un disque dur, et l'espace disque disponible est calculable à l'aide de la formule suivante :

Espace disponible = (espace disque total de l'un des disques) x (nombre de disques du RAID5 - 1)

Si l'utilisateur possède trois disques ayant chacun une capacité de 10 Go, l'espace disque disponible sera donc de 20 Go.

Les volumes RAID5 ne peuvent être étendus.

La fonctionnalité Espaces de stockage utilise ces technologies de redondance en réunissant les disques internes et externes de l'utilisateur dans une réserve (ou pool) de stockage unique, représentée par un disque virtuel.

Celui-ci est utilisé comme n'importe quel disque physique, il peut être partitionné, formaté, supprimé, chiffré avec BitLocker... Cette réserve de stockage n'est pas figée, mais évolutive en fonction du besoin de redondance ou d'espace disque.

Windows 11 ne peut pas démarrer à partir d'un espace de stockage.

Espaces de stockage gère les disques SSD, SATA (*Serial Advanced Technology Attachment*), USB et SAS (*Serial Attached SCSI*). Si le disque physique prend en charge le protocole SCSI Enclosure Services, un témoin lumineux rouge sera affiché en cas de défaillance de celui-ci, sinon, les messages d'avertissement seront affichés dans le Centre de notifications. L'administrateur devra alors changer le disque et recréer le pool depuis l'interface Espaces de stockage ou grâce aux commandes Windows PowerShell.

La réserve de stockage peut être composée de disques physiques de capacités et de connexions différentes.

Un stockage amovible du type clé USB, même formaté en NTFS et ayant une grande capacité d'espace disque, n'est pas supporté par Espaces de stockage.

L'allocation des ressources est dynamique. Par exemple, l'utilisateur crée un espace fixe virtuel de 20 To. Il ajoute ensuite deux disques physiques de 3 To dans la réserve de stockage. L'espace de stockage est toujours constitué de 20 To, mais réellement (physiquement) de 6 To. Et les 14 To manquants ? Le système effectuera une requête depuis le Centre de notifications pour ajouter de la capacité uniquement si celle des deux disques physiques était atteinte.

Si nécessaire, la taille maximale de l'espace (20 To dans notre exemple) peut être accrue.

Lorsqu'un disque physique est ajouté à la réserve de stockage, ses données sont effacées et inaccessibles, même depuis la corbeille.

En résumé, l'espace de stockage contient la quantité d'espace disque disponible théorique, la réserve de stockage gère au moins un (ou plusieurs) disque physique réel en fonction des besoins de l'utilisateur.

Pour créer un espace de stockage, branchez d'abord physiquement le deuxième disque que vous utiliserez avec cette fonctionnalité, puis :

Ouvrez les **Paramètres** depuis le champ de recherche de la barre des tâches. Cliquez sur **Système**, puis **Stockage, Paramètres de stockage avancés** et enfin **Espaces de stockage**.

Cliquez sur **Créer un pool de stockage et de l'espace de stockage**.

Création du pool de stockage : nommez le nouveau pool, puis sélectionnez le ou les disques cibles en cochant la ou les cases correspondantes. Une fois terminé, cliquez sur le bouton **Créer**.

Création de l'espace de stockage : nommez le nouvel espace de stockage, choisissez la **Taille** (la taille proposée par défaut est celle du nouveau disque) puis le type de **Résilience** parmi les cinq proposés :

- **Simple (sans résilience)** : requiert un seul disque. Aucune tolérance de panne n'est assurée. C'est le choix que vous allez faire pour cet exemple.
- **Miroir double** : copie les données sur un disque, assurant une redondance. Équivalent au RAID 1.
- **Miroir triple** : requiert trois disques. Si deux disques étaient défectueux simultanément, les données seraient encore accessibles.
- **Parité** : les données sont stockées sur au moins trois disques avec un système de parité. Un disque défaillant maintiendra la redondance. Ce type de résilience est équivalent au RAID 5.
- **Double parité** : l'espace disque est constitué d'au moins cinq disques. Ce type de résilience peut surmonter deux défaillances de disques comme une topologie RAID 6.

La fonctionnalité **Espaces de stockage** gère le nombre de défaillances de disques qui peuvent être tolérées avant que les données ne soient inaccessibles : c'est le **quorum**. L'accès aux données reste opérationnel si le nombre de disques sains dépasse celui du nombre de disques défaillants. Néanmoins, si l'espace est défini en miroir triple et peut utiliser tous les disques du pool, l'administrateur accédera toujours aux données même si deux disques tombaient en panne.

Nouvel espace de stockage

Pour utiliser un pool de stockage, vous devez d'abord créer un espace de stockage. Vous pouvez en créer un maintenant ou le faire ultérieurement à partir de la page des paramètres d'espace de stockage.

Nom

Espace de stockage

Taille et résilience

Un espace de stockage peut être plus grand que la capacité du pool de stockage. Vous pourrez ajouter des disques au pool ultérieurement pour augmenter la capacité du pool.

79 Go ▾

La résilience est un moyen de protection contre les pannes de disques. Les types de résilience disponibles sont :

- Simple (sans résilience)
- Miroir double
- Miroir triple
- Parité
- Double parité

Capacité maximale du pool : 100 Go

Capacité du pool (Pool de stockage) : 79,4 Go (79,2 Go libre)

Créer

Puis cliquez sur le bouton **Créer**.

Création du volume : saisissez un nom d'**Etiquette**, assignez une **Lettre de lecteur** et un **Système de fichiers**, puis cliquez sur le bouton **Formater**. Attention : toutes les données présentes sur celui-ci seront supprimées. Cliquez sur le bouton **Créer**.

Le volume est maintenant prêt et formaté. Dans la fenêtre **Espaces de stockage**, l'utilisateur peut visualiser son pool de stockage, le renommer, le supprimer en le sélectionnant et en cliquant sur **propriétés**. Il peut également en afficher les fichiers en cliquant sur **Découvrir** ou ajouter des disques supplémentaires.

The screenshot shows the Windows Storage Settings window. On the left, a sidebar lists system parameters: Système, Bluetooth et appareils, Réseau et Internet, Personnalisation, Applications, Comptes, Heure et langue, Jeux, Accessibilité, Confidentialité et sécurité, and Windows Update. The main area is titled "Pools" and shows a storage pool named "Pool de stockage" with 79.4 Go total capacity, 1.25 Go used, and 78.2 Go free. Below it is the "Espaces de stockage" section, which contains an "Espace de stockage (E)" volume with 79.0 Go capacity, simple resiliency, and 1.00 Go reserved. The "Disques physiques" section shows a "Msft Virtual Disk" with 80.0 Go capacity, identified as "Disque 1", with unknown support type and OK status. A "Créer un nouveau pool de stockage" button is at the top of the Pools section.

Le nouvel espace de stockage est vu comme un seul disque dans la console **Gestion des disques**, quel que soit le nombre de disques physiques au sein de ce volume.

Pour créer un pool de sauvegarde à l'aide du langage PowerShell, saisissez les commandes suivantes :

Récupérez le nom de l'espace de stockage, il vous servira plus tard (dans l'exemple « Windows Storage on DESKTOP ») :

```
Get-StorageSubsystem
```

Définissez une variable \$a contenant les disques physiques éligibles à la création du groupe de disques :

```
$a = (get-physicaldisk -CanPool $True)
```

Créez le groupe de disques nommé Stockage à partir de l'espace de stockage nommé comme « * Storage * » :

```
New-StoragePool -FriendlyName "Stockage"  
-StorageSubSystemFriendlyName "* Storage *"  
-PhysicalDisks $a
```

Créez le nouveau volume que vous nommerez Disque 2 en utilisant l'espace maximum disponible avec un type de résilience simple :

```
New-VirtualDisk -FriendlyName "Disque 2" -StoragePoolFriendlyName
```

"Stockage" -ResiliencySettingName Simple -UseMaximumSize

Initialisez le nouveau disque au format GPT :

Initialize-Disk -FriendlyName "Disque 2" -PartitionStyle GPT

Créez une partition qui s'étendra sur tout le disque n° 2 et assignez la lettre E au lecteur :

New-Partition -DiskNumber 2 -UseMaximumSize -DriveLetter E

Formatez la partition nouvellement créée en NTFS et nommez la partition Disque 2 :

Format-Volume -DriveLetter E -FileSystem NTFS

-NewFileSystemLabel "Disque 2"

The screenshot shows a Windows PowerShell window with the following command history:

```
PS C:\Users\ybard> New-StoragePool -FriendlyName "Stockage" -StorageSubSystemFriendlyName "* Storage *" -PhysicalDisks $a
FriendlyName OperationalStatus HealthStatus IsPrimordial IsReadOnly      Size
Stockage     OK             Healthy    False       False      ...7 GB

PS C:\Users\ybard> Get-StorageSubsystem
FriendlyName          HealthStatus OperationalStatus
Windows Storage on DESKTOP-GE5PG33  Healthy        OK

PS C:\Users\ybard> $a = (Get-PhysicalDisk -CanPool $true)
PS C:\Users\ybard> New-StoragePool -FriendlyName "Stockage" -StorageSubSystemFriendlyName "* Storage *" -PhysicalDisks $a
FriendlyName OperationalStatus HealthStatus IsPrimordial IsReadOnly      Size
Stockage     OK             Healthy    False       False      ...7 GB

PS C:\Users\ybard> New-VirtualDisk -FriendlyName "Disque 2" -StoragePoolFriendlyName "Stockage" -ResiliencySettingName Simple -UseMaximumSize
FriendlyName ResiliencySettingName FaultDomainRedundancy OperationalStatus HealthStatus      Size FootprintOnPool StorageEfficiency
Disque 2      Simple           0            OK             Healthy     158 GB      158 GB 100,00 %

PS C:\Users\ybard> Initialize-Disk -FriendlyName "Disque 2" -PartitionStyle GPT
PS C:\Users\ybard> New-Partition -DiskNumber 2 -UseMaximumSize -DriveLetter E

DiskPath : \\?\storage#disk#{369656f2-6ce2-4d78-be53-d6123a10f215}#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
PartitionNumber DriveLetter Offset                               Size Type
2                  E          16777216                   157.98 GB Basic

PS C:\Users\ybard> Format-Volume -DriveLetter E -FileSystem NTFS -NewFileSystemLabel "Disque 2"
DriveLetter FriendlyName FileSystemType DriveType HealthStatus OperationalStatus SizeRemaining      Size
E          Disque 2      NTFS        Fixed   Healthy    OK           157.89 GB 157.98 GB

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

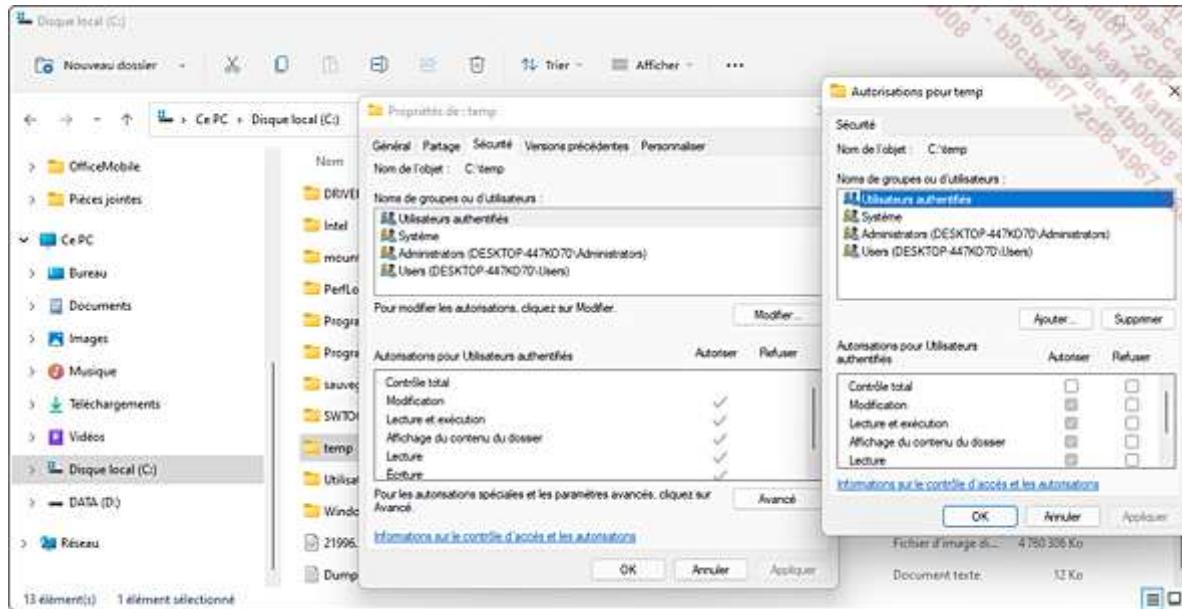
3. Autorisations NTFS

Tout administrateur doit savoir configurer des autorisations NTFS sur des dossiers ou fichiers et les rendre accessibles grâce aux partages. Une autorisation définit le droit d'effectuer une opération sur une ressource.

La définition précise des droits permet d'éviter la fuite de données et les écueils de sécurité. Par défaut, le propriétaire d'une ressource est seul habilité à définir des autorisations d'accès, à un utilisateur ou à un groupe. Un administrateur peut en outre prendre possession d'un fichier à l'aide de la commande takeown.exe.

Les autorisations NTFS protègent les données contre des accès non souhaités effectués localement et depuis le réseau, en conjonction avec celles du partage. L'administrateur peut définir des autorisations standards (lecture, modification...) ou spéciales (appropriation, lecture d'attributs...) plus précises.

Ces autorisations peuvent être définies en cliquant avec le bouton droit sur un dossier ou fichier, puis en sélectionnant **Propriétés**. Cliquez ensuite sur l'onglet **Sécurité** puis sur le bouton **Modifier** pour attribuer les autorisations adéquates.



La commande `icacls.exe` modifie et sauvegarde en ligne de commandes les autorisations NTFS. Pour sauvegarder les listes de contrôle d'accès du dossier Windows et de ses sous-dossiers dans le fichier `ACLWINDOWS.txt`, utilisez la commande :

```
icacls c:\windows\* /save ACLWINDOWS.txt /t
```

Un dossier (parent) peut contenir un ou plusieurs sous-dossiers (enfants). Une autorisation définie explicitement sur le dossier parent sera propagée sur ses sous-dossiers. Ainsi, en cas de modification sur le plus haut niveau hiérarchique, celle-ci sera déployée sur les niveaux inférieurs.

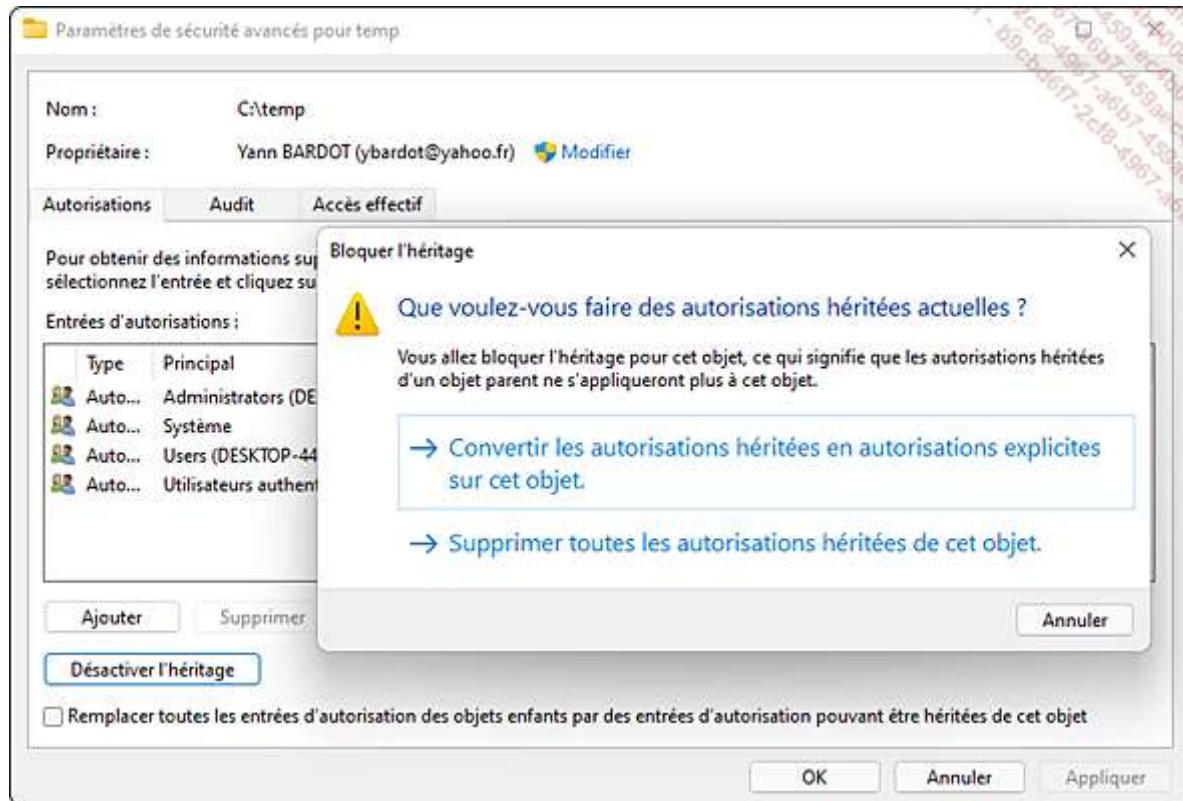
Une autorisation définie explicitement est toujours prioritaire sur une autorisation héritée. Néanmoins, si l'accès à un objet est refusé par héritage et que vous définissez explicitement l'autorisation Autoriser, cette dernière sera retenue.

L'héritage sur un dossier enfant peut être bloqué, élevant ce dossier au rang de parent. Lors de ce processus, l'utilisateur doit choisir entre copier les autorisations existantes ou recommencer sur une base vierge.

Pour bloquer l'héritage sur un dossier stocké sur une partition NTFS :

En tant qu'administrateur, depuis l'**Explorateur de fichiers**, cliquez avec le bouton droit sur un dossier, puis choisissez **Propriétés**. Cliquez sur l'onglet **Sécurité** puis sur le bouton **Avancé**.

Cliquez sur le bouton **Désactiver l'héritage**. Choisissez de convertir les autorisations héritées en autorisations explicites ou de supprimer toutes les autorisations héritées.



Lorsqu'un utilisateur copie un dossier dans une autre partition ou sur la même partition NTFS, celui-ci hérite des autorisations définies sur la partition de destination.

Lorsqu'un utilisateur déplace un dossier dans une autre partition NTFS, celui-ci hérite des autorisations définies sur le dossier de destination. S'il déplace un dossier dans la même partition, il héritera toujours des autorisations du dossier de destination, mais gardera celles qui lui ont été explicitement attribuées.

En cas de copie ou de déplacement sur une partition autre que NTFS, telle que FAT, le dossier perd toutes ses autorisations.

La commande robocopy.exe permet de maintenir les autorisations sur les dossiers ou fichiers lors d'actions de copie ou de déplacement.

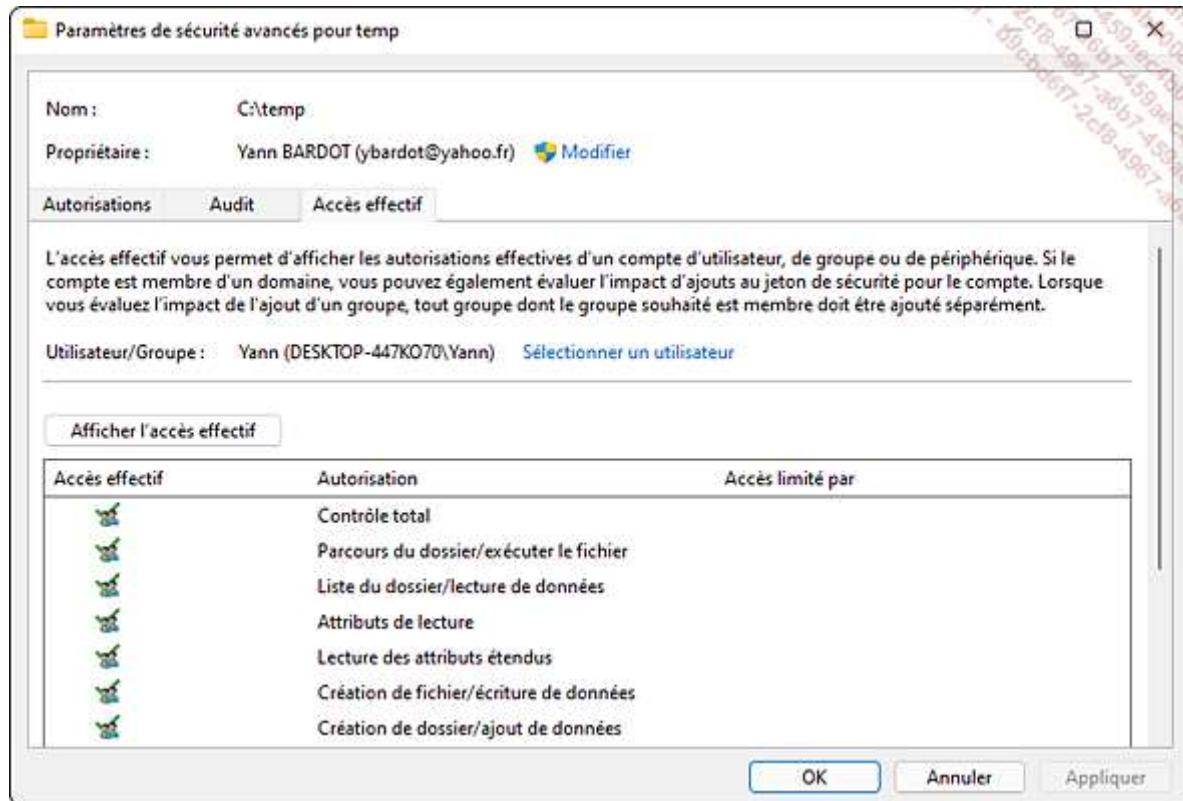
Les autorisations effectives sont la combinaison des autorisations détenues par l'utilisateur et par tous ses groupes d'appartenance.

Pour les visualiser, Microsoft met à disposition l'onglet **Accès effectif**, disponible dans les propriétés d'un dossier :

Cliquez sur l'onglet **Sécurité** puis sur le bouton **Avancé** et sélectionnez l'onglet **Accès effectif**.

Cliquez sur **Sélectionner un utilisateur** puis entrez le nom de l'utilisateur, du groupe ou du périphérique (bouton **Types d'objets**) dont vous souhaitez connaître les autorisations effectives. Validez par le bouton **OK**.

Cliquez ensuite sur le bouton **Afficher l'accès effectif**.



4. Partage de fichiers

Une autorisation de partage définie sur un dossier permet quant à elle de le rendre accessible, ainsi que son contenu (fichiers ou sous-dossiers) au travers du réseau. À noter qu'il est impossible de partager un fichier. Seuls les membres des groupes Administrateurs, Utilisateurs avec pouvoir et Opérateurs de serveur peuvent partager des dossiers.

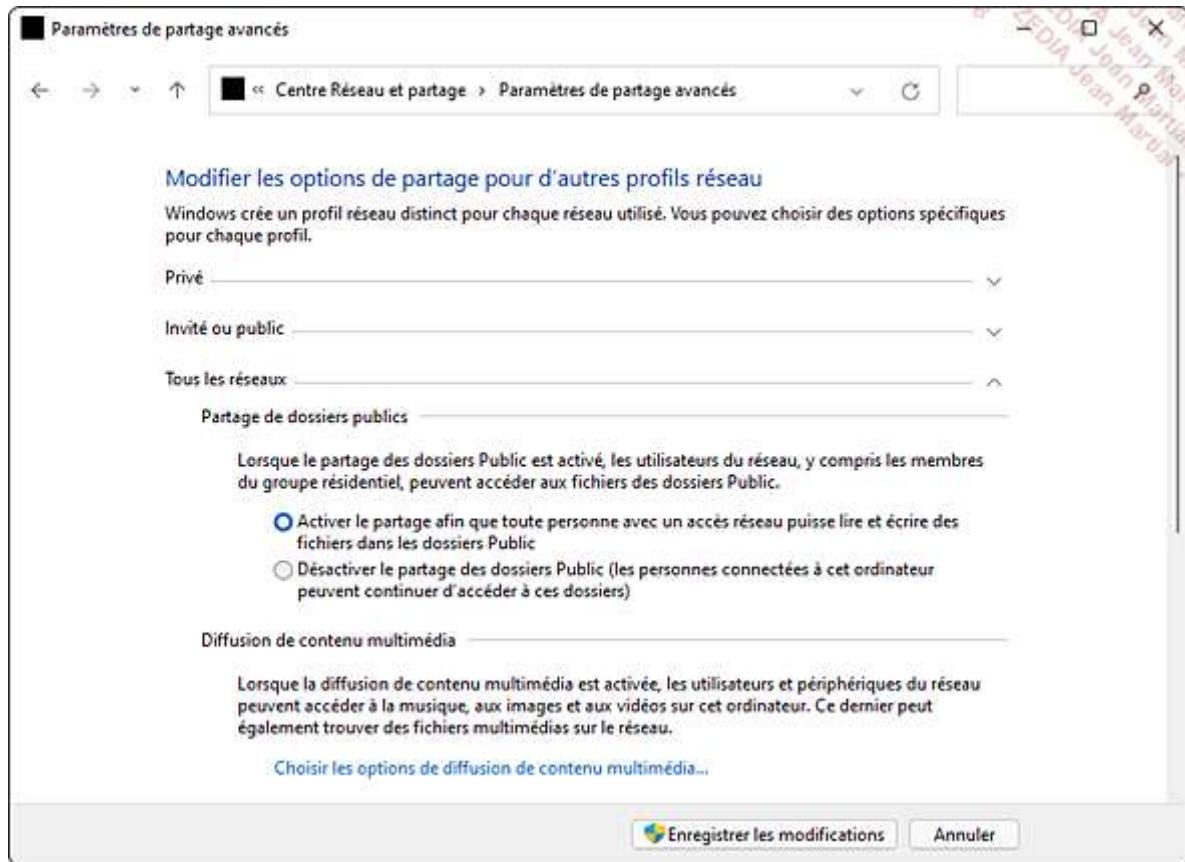
Windows 11 permet de partager simplement des ressources avec des ordinateurs du même réseau, grâce au dossier **Public**, accessible par toute personne ayant un compte sur l'ordinateur cible.

Les paramètres avancés de partage sont définis dans le **Centre Réseau et partage**. Pour activer ce type de partage, non disponible dans les paramètres :

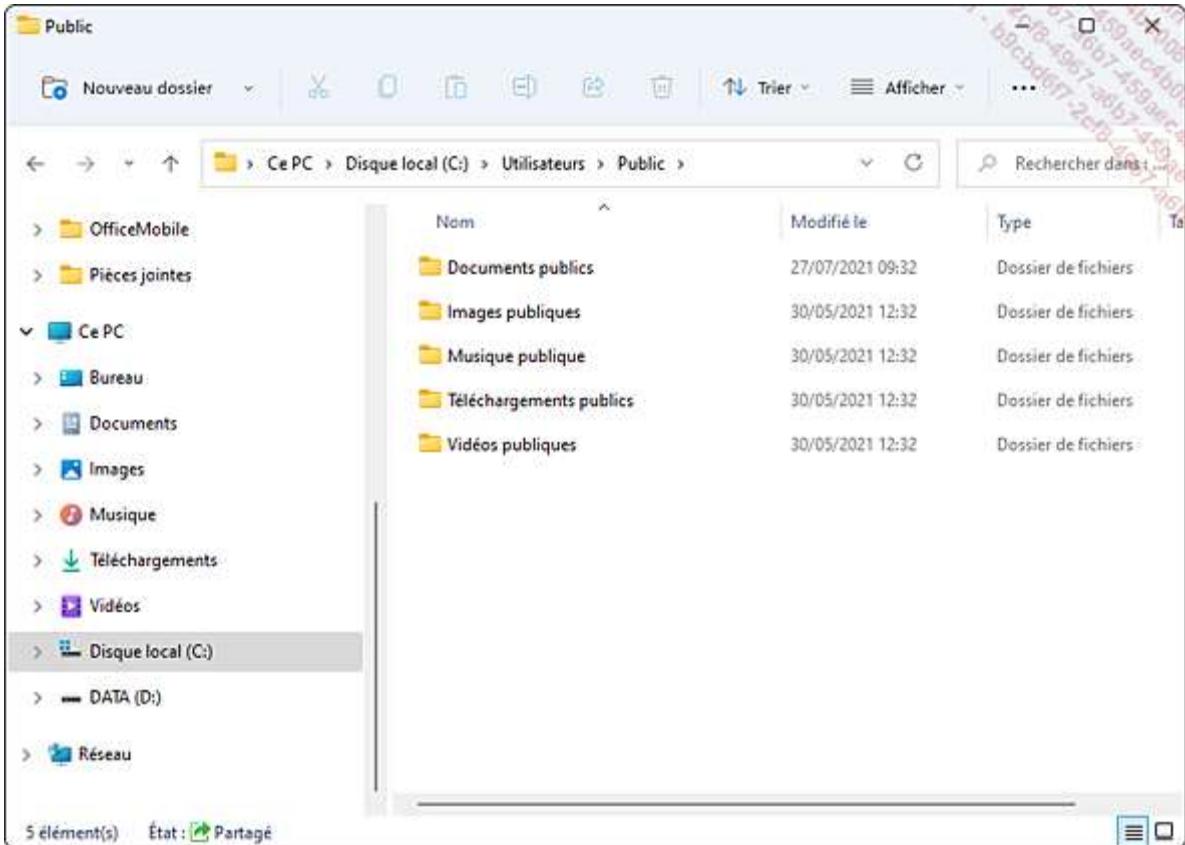
Ouvrez le **Panneau de configuration** et sélectionnez l'affichage par icônes. Cliquez sur **Centre Réseau et partage**.

Sur la gauche, cliquez sur **Modifier les paramètres de partage avancés** et développez **Tous les réseaux**.

Cochez la case **Activer le partage afin que toute personne avec un accès réseau puisse lire et écrire des fichiers dans les dossiers Public** et, tout en bas, la case **Activer le partage protégé par mot de passe**. Cette dernière option définit que seules les personnes possédant un compte utilisateur sur l'ordinateur Windows 11 pourront accéder aux dossiers publics.

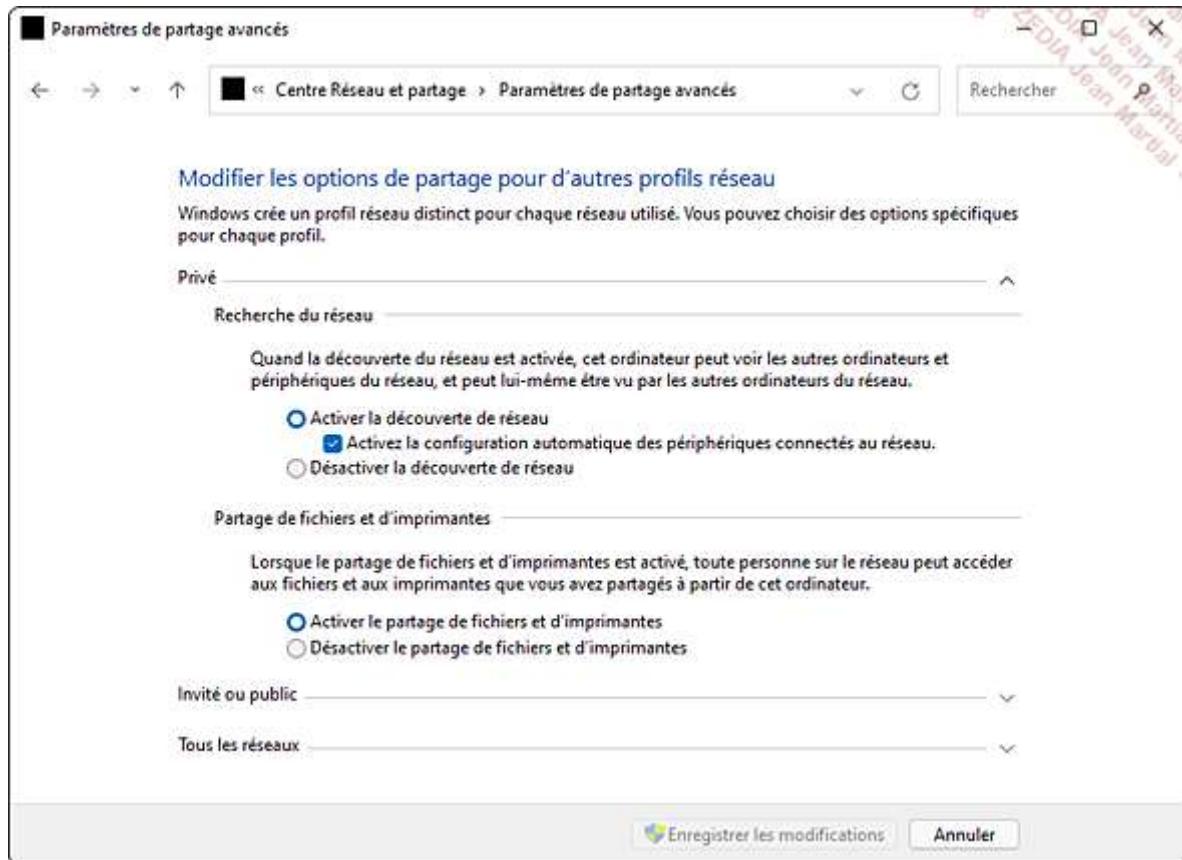


La hiérarchie mise en place pour le dossier Public permet de partager le contenu en fonction de son type : **Documents publics, Images publiques, Musique publique, Téléchargements publics et Vidéos publiques**. Pour y accéder, exécutez l'**Explorateur de fichiers** et développez le dossier **C:\Users\Public**, puis copiez les données à partager dans le type de dossier public prévu à cet effet.



Les paramètres avancés de partage définis dans le **Centre Réseau et partage** permettent, en fonction de chaque profil (Privé, Public ou Tous les réseaux), d'appliquer des règles de sécurité. Par exemple, lorsqu'elle est activée, la découverte du réseau offre la possibilité à Windows 11 d'être détecté par les ordinateurs du réseau.

Dans le **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de partage avancés** et configurez les options en fonction du profil **Privé** pour autoriser la découverte du réseau.



Windows 11 propose le menu rapide **Accorder l'accès à**, pour partager une ressource avec des droits simples ou cesser de la partager. Pour ce faire :

Depuis l'**Explorateur de fichiers**, cliquez avec le bouton droit sur le dossier que vous souhaitez partager, puis cliquez sur **Afficher plus d'options** et choisissez **Accorder l'accès à** et **Des personnes spécifiques**.

Saisissez un nom d'utilisateur ou nom de groupe local (ou de domaine) puis cliquez sur les boutons **Ajouter** et **Partager**. Le dossier est maintenant partagé.

The screenshot shows a Windows-style dialog box for sharing a folder. At the top left is a back arrow and the text "Accès réseau". The main title is "Choisir les utilisateurs pouvant accéder à votre dossier partagé". Below it is a sub-instruction: "Tapez un nom et cliquez sur Ajouter, ou cliquez sur la flèche pour rechercher un utilisateur." A search bar contains the text "yanou". To its right is an "Ajouter" button. The main area has two columns: "Nom" and "Niveau d'autorisation". It lists two users: "Philou" with "Lecture" permission and "Yann BARDOT (ybardot@yahoo.fr)" with "Propriétaire" permission. At the bottom left is a link "Je rencontre des difficultés pour partager.". At the bottom right are "Partager" and "Annuler" buttons.

Notez que vous pouvez envoyer par courrier électronique le lien du partage ou bien le copier à destination d'un programme.

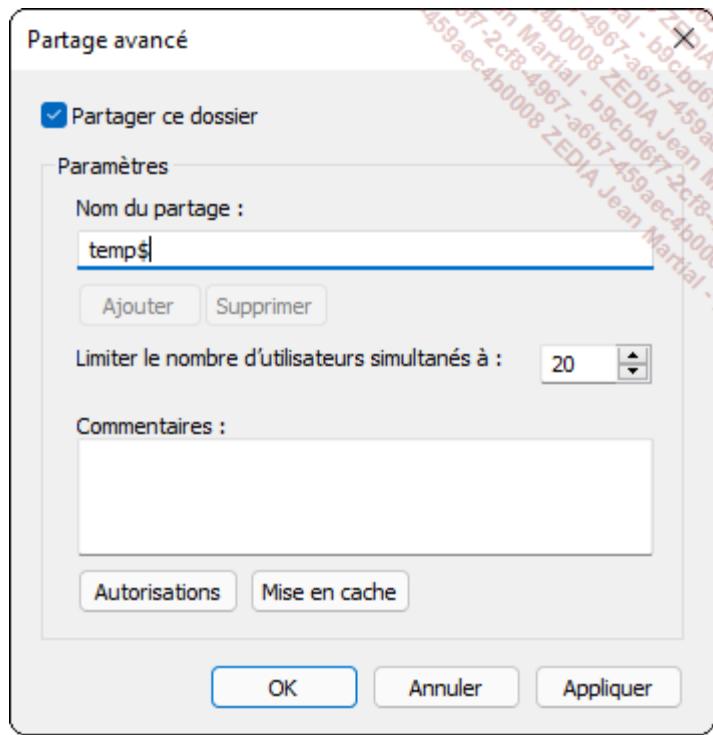
Vous pouvez aussi supprimer l'accès au dossier en procédant de manière similaire.

Le paramétrage du partage est également accessible depuis l'onglet **Partage** du menu contextuel **Propriétés**.

Cette méthode simple répond à des besoins de partage basiques. Il est néanmoins possible de définir des autorisations plus précises :

Cliquez sur le bouton **Partage avancé** depuis l'onglet **Partage** des propriétés d'un dossier.

Cochez la case **Partager ce dossier**, puis définissez le ou les noms du partage (en cliquant sur le bouton **Ajouter**, s'il est déjà partagé). Éventuellement, vous pouvez cacher un partage au reste du réseau en ajoutant un \$ au nom de partage. L'utilisateur devra alors connaître son chemin complet pour y accéder : \\NOMSERVEUR\\NOMPARTAGE\$.



Définissez le nombre maximum d'utilisateurs pouvant accéder au partage simultanément (20 par défaut) et cliquez sur le bouton **Autorisations** pour créer les accès.

Ajoutez des utilisateurs ou des groupes et, pour chacun, définissez les autorisations souhaitées parmi : **Contrôle total**, **Modifier** ou **Lecture (Autoriser ou Refuser)**. Validez par le bouton **OK**.

Le bouton **Mise en cache** permet de définir l'accès par le client au contenu du dossier en mode hors connexion (sans connexion réseau).

Outre l'interface graphique, il est possible de partager un dossier à l'aide de commandes :

- Avec net share.
- Grâce à la commande New-SmbShare du langage PowerShell.

Exemple : New-SmbShare -Name Partage1 -Path c:\temp

La commande PowerShell Remove-SmbShare supprime un partage existant.

Grant-SmbShareAccess définit les permissions de partage.

Un dossier peut se voir attribuer une lettre de lecteur (mappage) pour un accès plus rapide, à l'aide de la commande net use. Exemple de mappage du lecteur Y: sur le dossier partagé "Partage" stocké sur l'ordinateur nommé mytraining : net use Y: \\mytraining\partage

Par défaut, le groupe Tout le monde possède l'autorisation de lecture sur une ressource partagée. Idéalement, l'administrateur doit le supprimer et le remplacer par Utilisateurs authentifiés, afin d'améliorer la sécurité lors de l'accès aux ressources du poste Windows 11.

Le composant logiciel enfichable **Dossiers partagés** affiche les sessions en cours, les fichiers ouverts et donne la possibilité de créer des dossiers partagés au travers d'un assistant. Pour l'ouvrir, procédez comme suit :

Pressez les touches + R et saisissez mmc puis validez via la touche [Entrée]. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît. Cliquez sur le menu **Fichier** puis sur **Ajouter/Supprimer un composant logiciel enfichable**.

Dans la liste de gauche **Composants logiciels enfichables disponibles**, sélectionnez **Dossiers partagés**, puis cliquez sur le bouton **Ajouter**.

Il est possible de passer directement par la console **Gestion de l'ordinateur** depuis le menu contextuel du bouton **Démarrer**.

Dans la fenêtre **Dossiers partagés**, sélectionnez la case **L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)**, puis cliquez sur **Terminer**. Validez par **OK**.

Développez **Dossiers partagés (local)**, puis cliquez sur **Partages** :

The screenshot shows the Windows File Explorer interface with the title bar "Console1 - [Racine de la console]\Dossiers partagés (local)\Partages". The left sidebar shows "Racine de la console" expanded, with "Dossiers partagés (local)" selected, and "Partages" highlighted. The main pane displays a table of shared folders:

Nom du partage	Chemin du dossier	Type	Nb. de connexions client	Description
ADMIN\$	C:\WINDOWS	Windows	0	Administration à distance
C\$	C\$\	Windows	0	Partage par défaut
DS\$	D\$\	Windows	0	Partage par défaut
IPC\$		Windows	0	IPC distant
temp\$	C:\temp	Windows	0	
Users	C:\Users	Windows	0	

The right pane shows an "Actions" menu with "Partages" selected.

La liste des partages s'affiche, avec le nombre de connexions client.

Pour créer un nouveau partage depuis cette console :

Cliquez avec le bouton droit sur **Partages**, puis cliquez sur **Nouveau partage**.

Sélectionnez le dossier à partager et cliquez deux fois sur **Suivant**.

Définissez les autorisations selon vos besoins. Vous pouvez les personnaliser par utilisateur et par groupe.

Cliquez sur **Suivant** et **Terminer**.

Un dossier partagé sur une partition NTFS combine les autorisations NTFS et de partage afin d'être protégé : les permissions les plus restrictives s'appliquent. Par exemple, si un utilisateur PP possède l'autorisation NTFS **Modifier** et l'autorisation de partage **Lecture** sur le dossier Training, son accès effectif est **Lecture**.

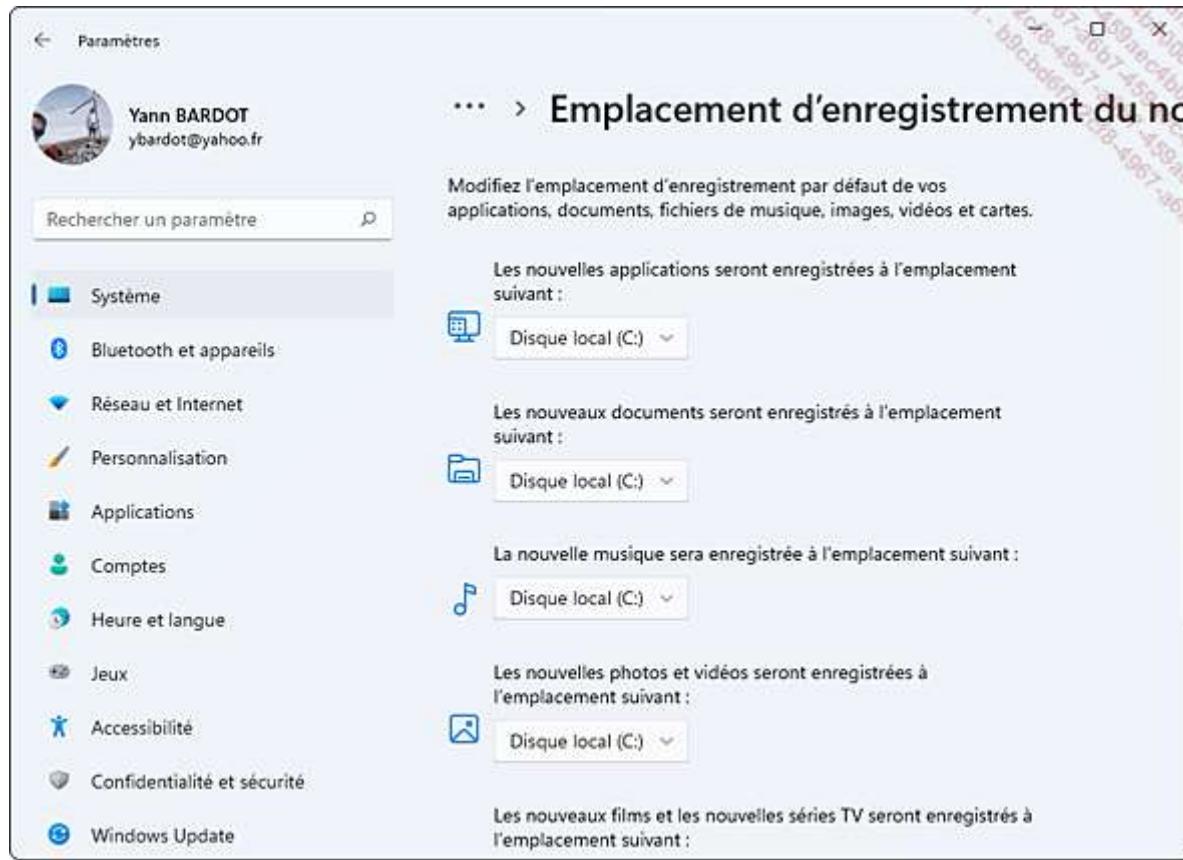
Les permissions NTFS s'appliquent lors d'une ouverture de session locale sur Windows 11, mais aussi depuis un accès distant à un partage.

5. Emplacements d'enregistrement

Windows 11 offre une nouvelle fonctionnalité à ses utilisateurs : la redirection des emplacements d'enregistrement pour les documents, images, vidéos, musiques et applications. Ainsi, lorsque le disque C: devient saturé, il est possible d'enregistrer les données suivantes dans une autre partition.

Cela s'effectue simplement en cliquant sur **Paramètres** du menu **Démarrer** puis en sélectionnant **Système** et **Stockage**.

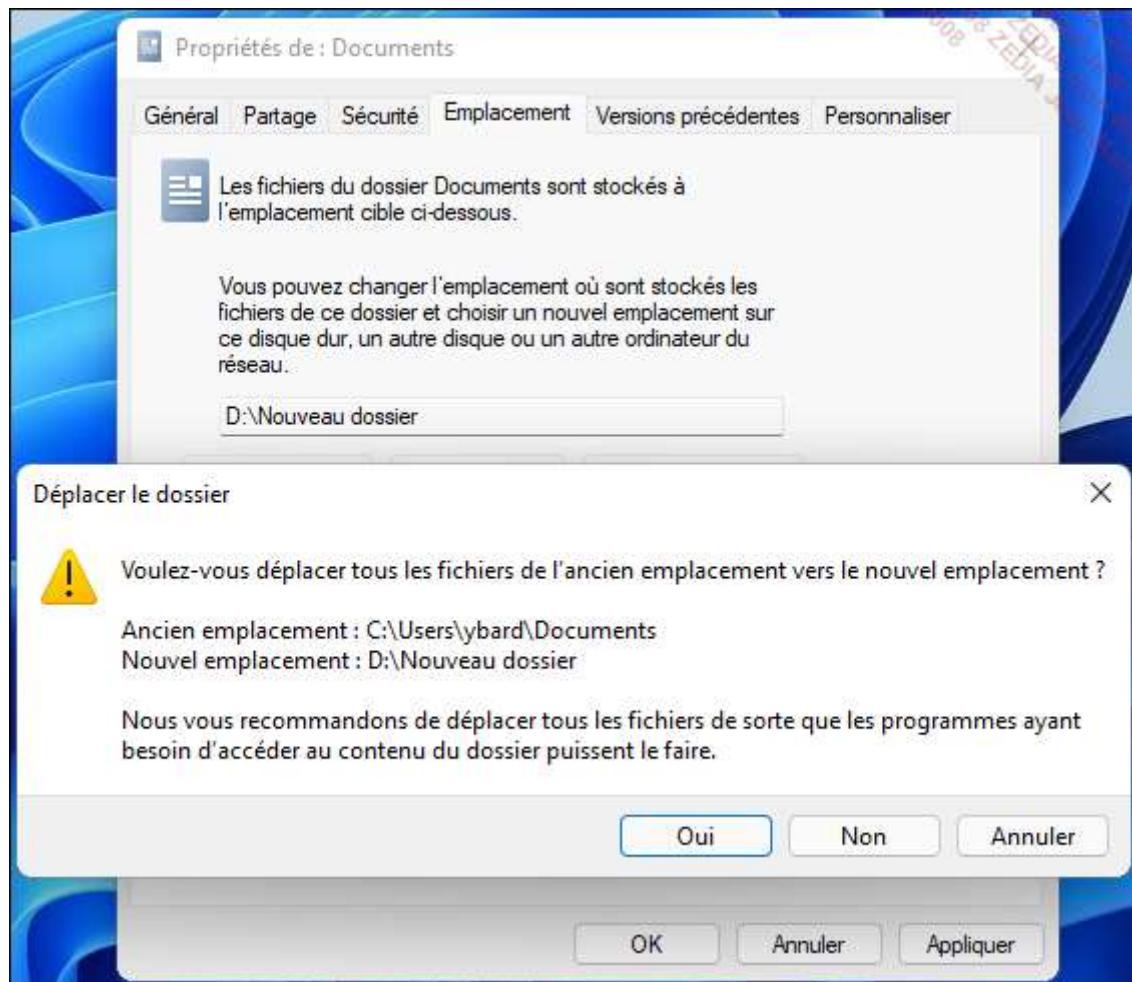
Développez **Paramètres de stockage avancés** et cliquez sur **Emplacement d'enregistrement du nouveau contenu**. Choisissez en fonction du type de données (documents, images, etc.) le dossier cible d'enregistrement :



Dans notre exemple, nous pouvons choisir la partition C:

Cette méthode ne déplace malheureusement pas les anciens dossiers stockés dans Documents, Images, etc. avant l'application de cette procédure, seulement les prochaines données créées.

Pour pallier ce problème, il suffit d'effectuer un clic droit sur un de ces dossiers dans l'**Explorateur de fichiers**, puis sélectionnez **Propriétés** et l'onglet **Emplacements**. Spécifiez un nouveau dossier cible grâce au bouton **Déplacer** puis cliquez sur le bouton **Appliquer**. Un message vous proposant de déplacer les données situées dans l'ancien emplacement vers le nouveau apparaît. Cliquez sur le bouton **Oui** pour confirmer le déplacement.



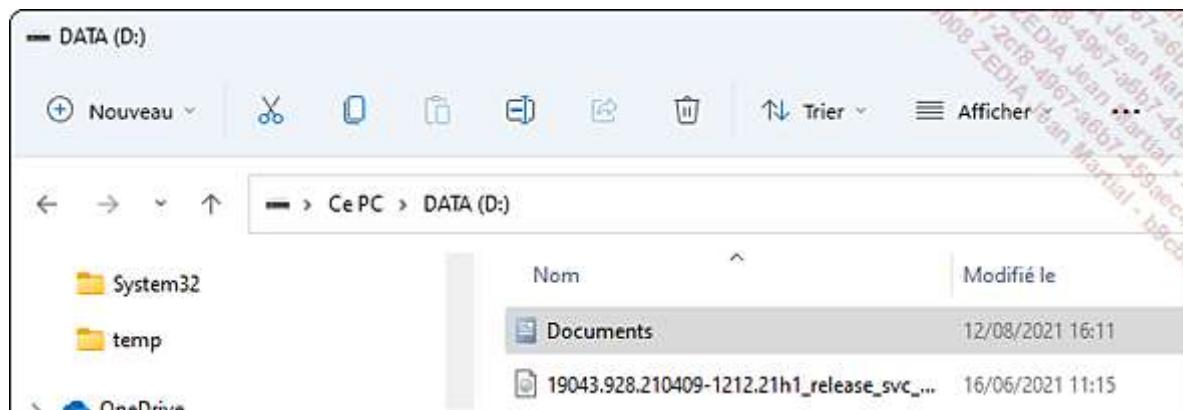
Notez que s'il advenait que le support de destination ne soit plus disponible, le système basculerait automatiquement sur le disque C:.

6. Explorateur de fichiers

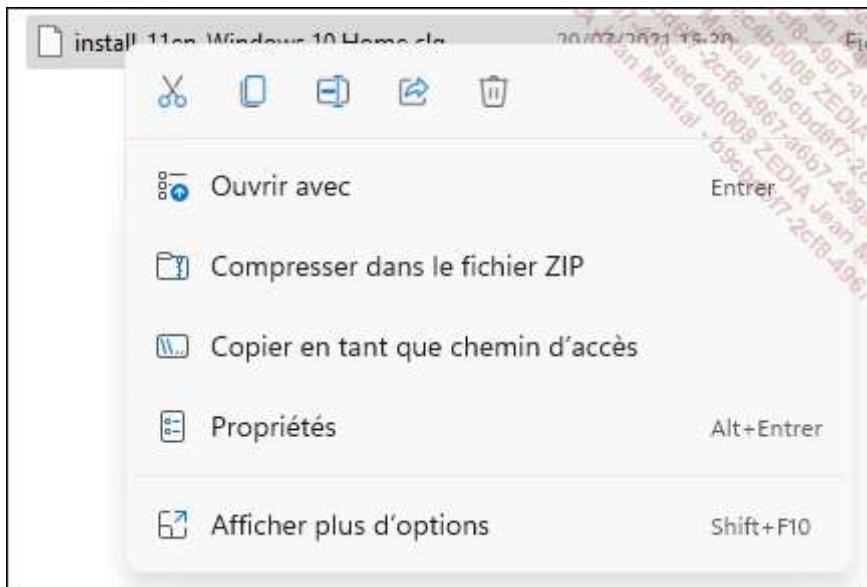
Un des outils les plus utilisés sur les postes de travail Windows est sans conteste l'Explorateur de fichiers (accessible depuis la barre des tâches ou en pressant les touches + E), qui gère les opérations courantes sur les fichiers : copie, déplacement, suppression, affichage des propriétés... mais aussi, l'affichage de photos ou l'exécution de logiciels par exemple.

Avec Windows 11, il a subi un important relooking pour en faire un outil épuré, moderne et fonctionnel :

Les menus du ruban ont été remplacés par des icônes.



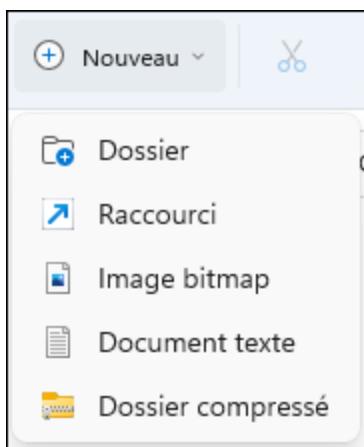
Le menu contextuel (clic droit) a été simplifié et utilise ces mêmes icônes, donnant un accès rapide aux fonctions les plus utilisées.



D'autres options sont disponibles en cliquant sur **Afficher plus d'options**.

Les icônes des boutons ont été modernisées, les boutons et menus espacés, facilitant la navigation tactile.

Le bouton **Nouveau**, outre créer un nouveau dossier, permet de créer un raccourci, un nouveau fichier (bitmap ou texte par défaut) ou encore un dossier compressé.



Les trois boutons suivants, **Couper**, **Copier** et **Coller**, permettent toujours de déplacer des fichiers et dossiers. Les raccourcis-clavier [Ctrl] + X, [Ctrl] + C et [Ctrl] + V permettent d'exécuter les mêmes actions.

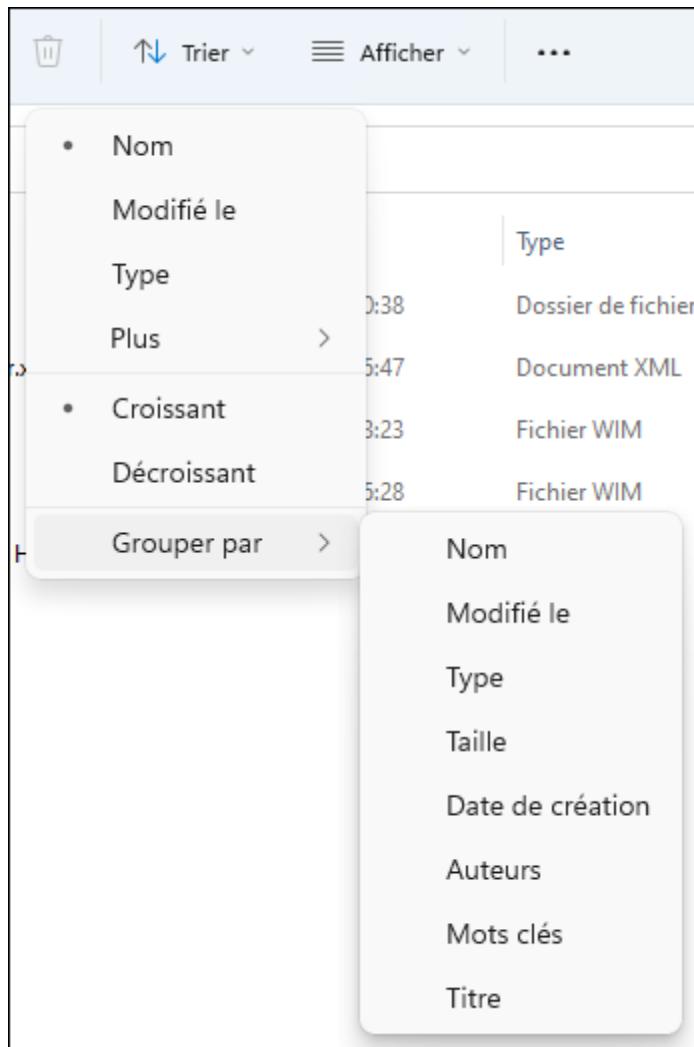


Les trois boutons suivants permettent respectivement de renommer un fichier ou un dossier ([F2]), de partager un fichier au moyen d'une application et de supprimer un fichier ou un dossier ([Suppr]).



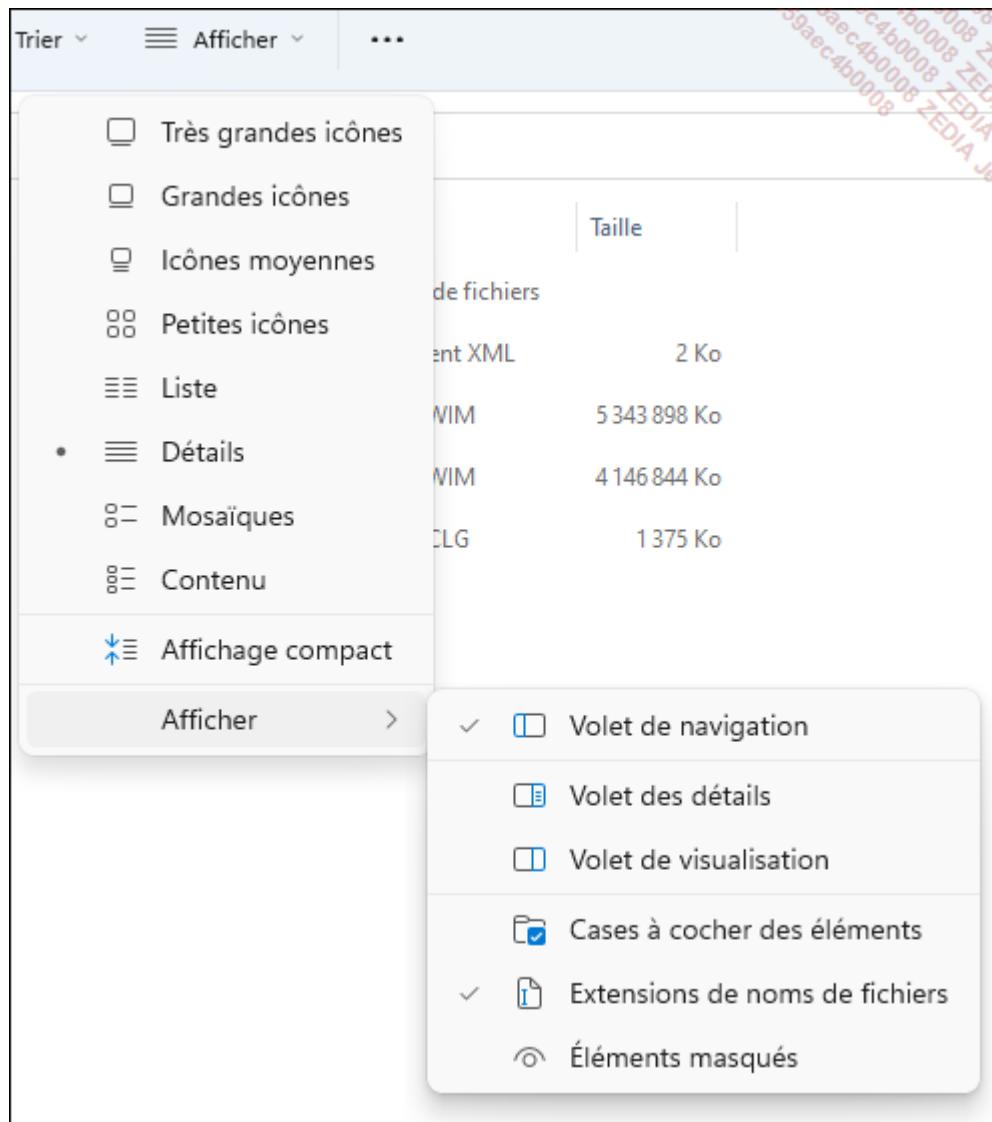
La suppression n'est pas définitive, le fichier ou le dossier est simplement envoyé dans la Corbeille, accessible sur le Bureau. Il n'y a pas de confirmation demandée. La suppression permanente est possible en appuyant sur la touche [Shift] lors de la suppression. Il n'y a alors aucune restauration possible.

La liste déroulante **Trier** modifie l'affichage en fonction des critères de tri sélectionnés par l'utilisateur : nom, date, croissant... Le menu **Grouper par** permet de regrouper des fichiers selon certains critères.

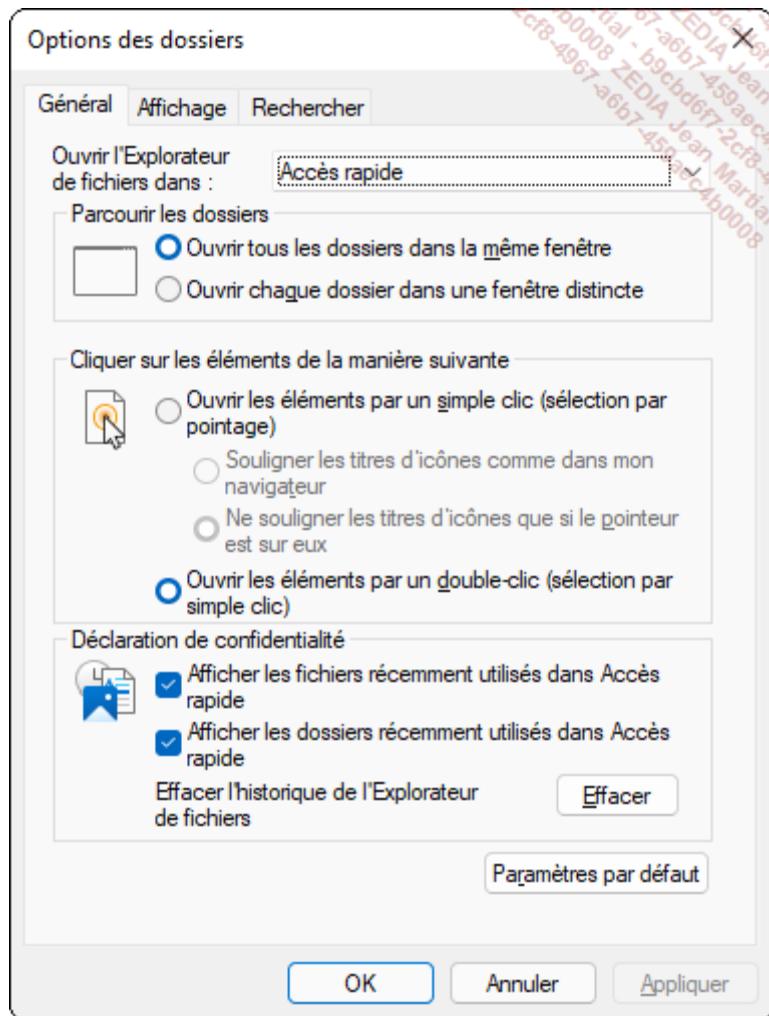


La liste déroulante **Afficher** permet de choisir le type d'affichage souhaité : par icônes, en liste, etc. L'option **Contenu** permet d'obtenir des informations supplémentaires sur le fichier. Dans le cas d'une vidéo, la durée et la résolution seront affichées.

Il est possible de resserrer les éléments avec l'option **Affichage compact**. Le sous-menu **Afficher** offre des options comme : ajouter un volet à l'Explorateur de fichiers, afficher des cases à cocher devant les éléments, montrer les extensions ou les fichiers masqués.



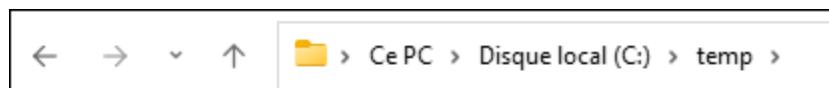
Enfin, le menu **En savoir plus** (More options) offre quelques actions supplémentaires, comme **Annuler**, **Epingler à Accès rapide**, sélectionner, accéder aux propriétés ou ouvrir les **Options** de l'Explorateur de fichiers. Parmi les options proposées, notez la possibilité de modifier la manière d'ouvrir les éléments (par simple ou double clic) et celle d'**Effacer l'historique de l'Explorateur de fichiers**.



De nouveaux boutons peuvent apparaître de manière interactive. Par exemple, l'ouverture d'un dossier compressé, fait apparaître le bouton **Extraire tout**.

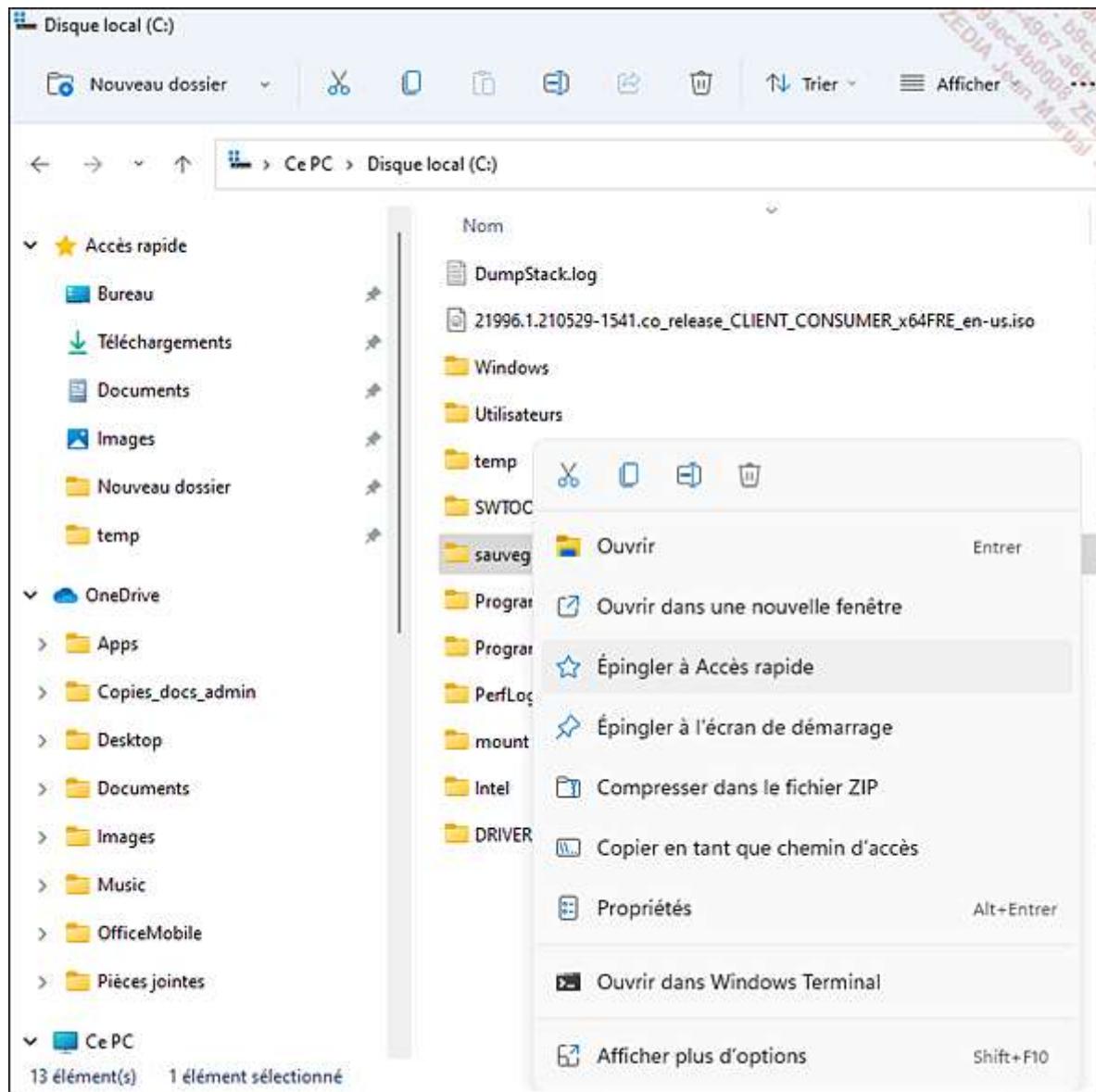
Dans la barre d'adresse, les flèches permettent de naviguer :

- vers les dossiers précédemment visités ;
- vers le dossier parent (flèche vers le haut), pour remonter d'un niveau dans l'arborescence des fichiers.

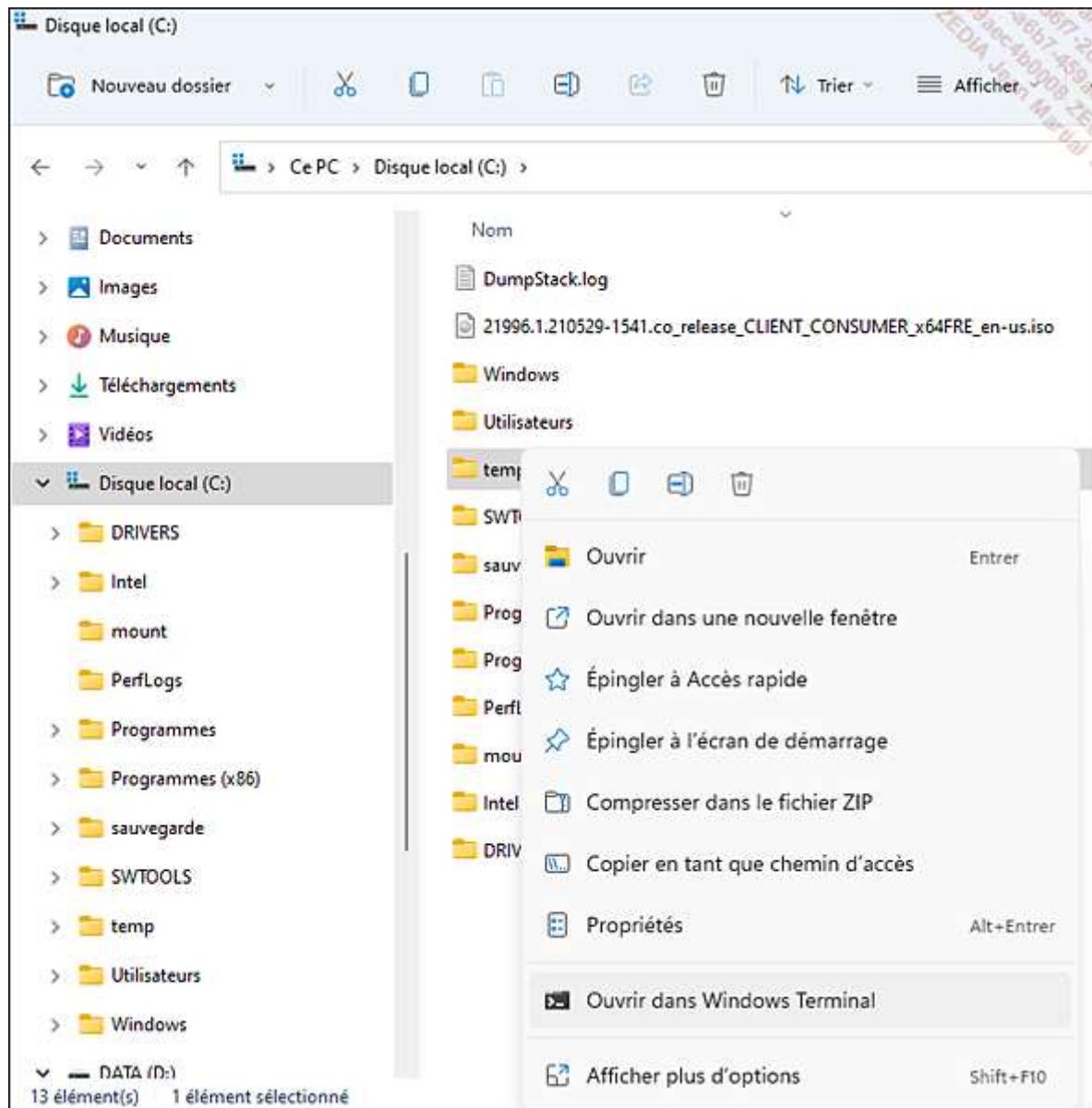


La combinaison des touches du clavier [Alt] et [Flèche à gauche, droite ou haut] effectuent les mêmes opérations qu'en pressant les boutons susmentionnés.

Le menu **Accès rapide**, qui contient les dossiers accédés fréquemment par l'utilisateur, est toujours présent. Ajouter un dossier à ce menu est simple : le sous-menu précédemment mentionné le permet. Autre manière de procéder : il suffit d'effectuer un clic avec le bouton droit sur l'élément (menu contextuel) puis de sélectionner **Épingler à Accès rapide**.

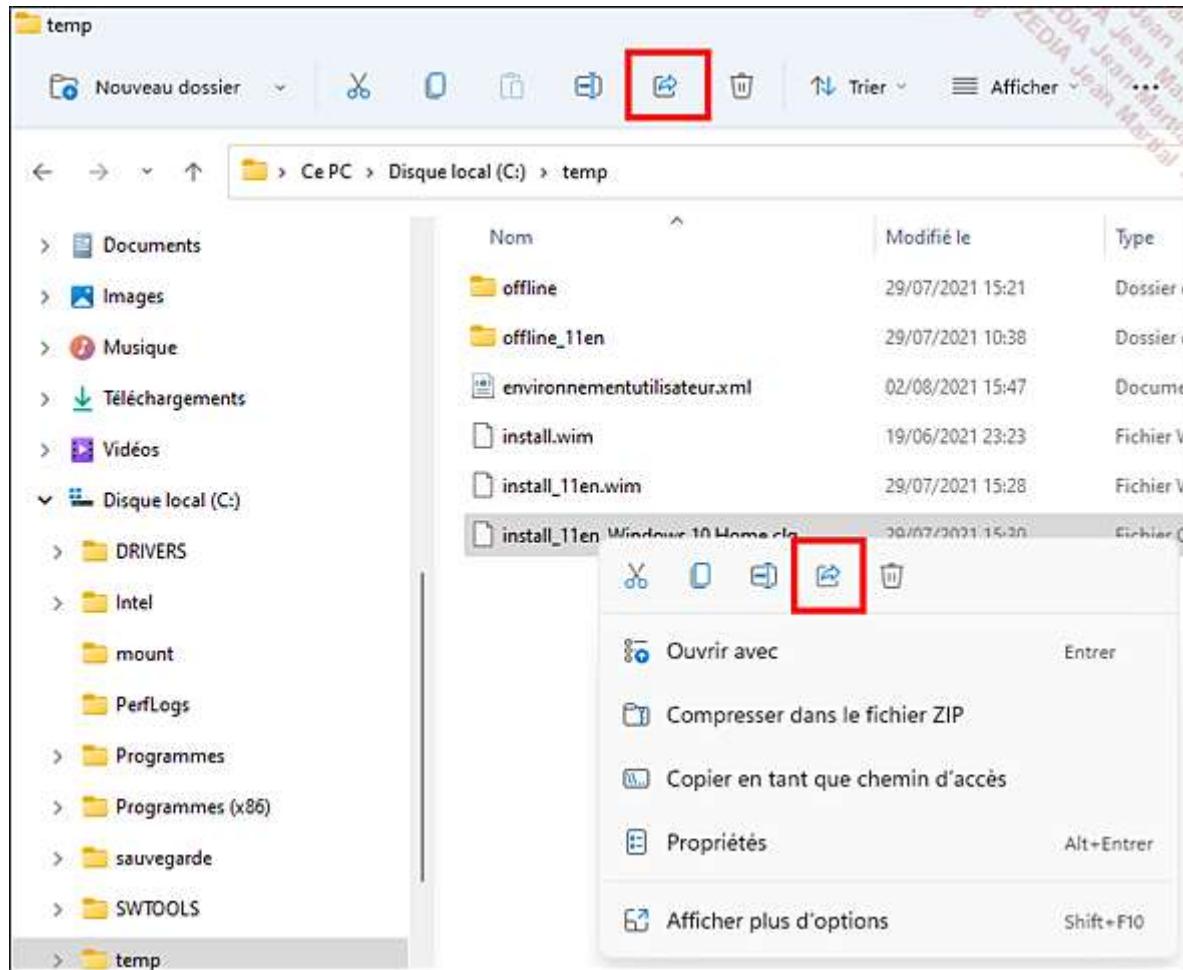


Depuis Windows 10 (la version 1809), l'administrateur a la possibilité d'exécuter directement un interpréteur de commandes Linux ou PowerShell dans un dossier cible en cliquant avec le bouton droit sur un dossier puis en sélectionnant **Ouvrir dans Windows Terminal**.



Notez que cette option est cachée si vous cliquez sur un dossier dans le volet de navigation (colonne de gauche) de l'Explorateur ou sur une zone vide. Elle se trouve dans **Afficher plus d'options**.

L'utilisateur peut aussi partager un fichier auprès d'une application en sélectionnant le fichier puis en cliquant sur l'icône **Partage** du menu contextuel ou de l'Explorateur de fichiers. Cette icône est apparue avec Windows 11.



Le panneau **Partager** apparaît au milieu de l'écran et vous indique les applications éligibles à ce partage.

Dans l'exemple ci-dessous, nous avons partagé un fichier avec l'application **Courrier**. Cela aura pour effet de proposer l'envoi d'un courriel avec le fichier mentionné en pièce jointe.

 Partager 1 élément

Partage de proximité Désactivé ▾

Partage désactivé

Envoyer un e-mail à un contact Rechercher...

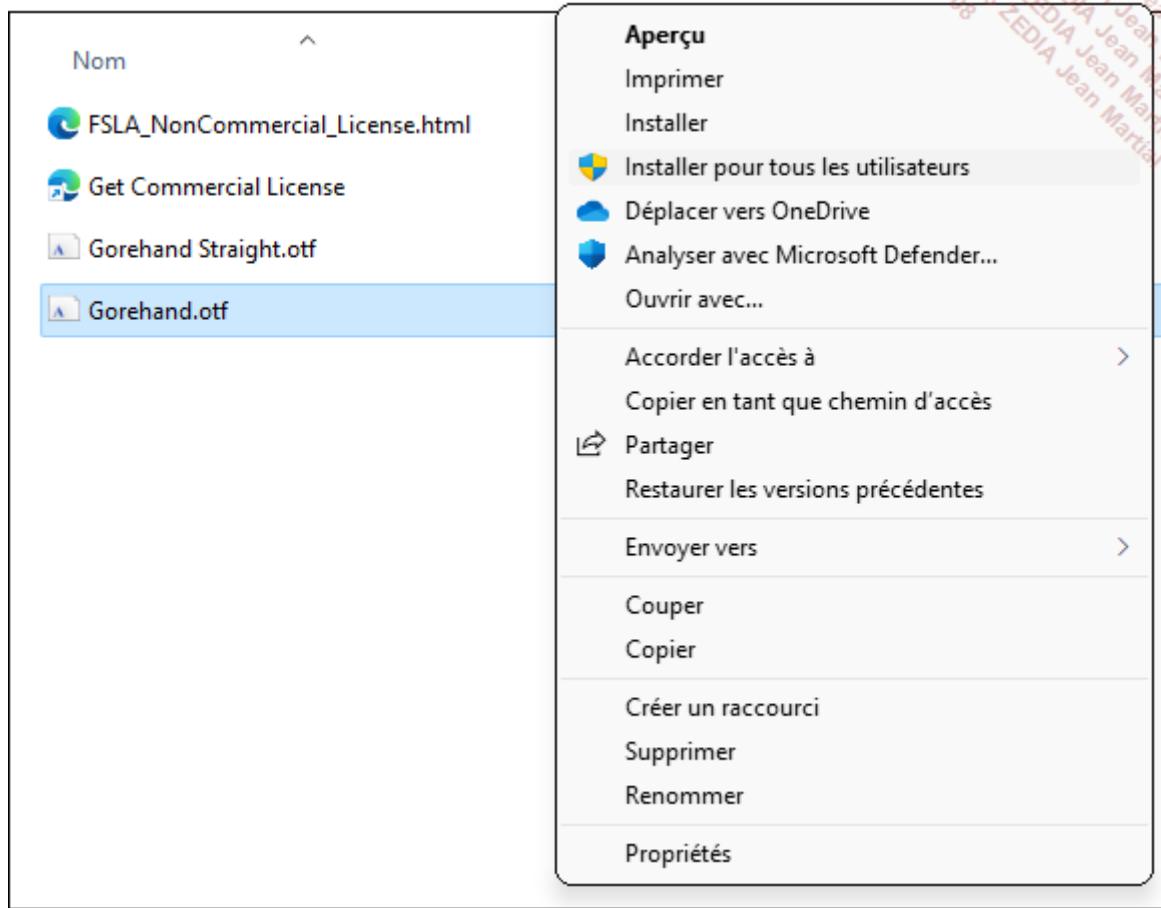
 Me

Partager avec une application Rechercher plus...

 Courier

Partage à proximité désactivé |  Paramètres de partage de proximité

Lorsque vous effectuez un clic droit sur un fichier de police dans l'Explorateur de fichiers, vous pouvez sélectionner **Afficher plus d'options**, **Installer** pour l'installer uniquement pour votre compte d'utilisateur ou **Installer pour tous les utilisateurs** pour tous les utilisateurs du système. Cette dernière action nécessite des droits élevés.



Les anciens systèmes d'exploitation Microsoft affichaient une fenêtre par tâche de copie. Depuis Windows 10, toutes les opérations sont désormais regroupées dans une seule interface : chaque copie peut être suspendue puis reprise.

2 Actions en cours d'exécution

Copie d'un élément de DATA (D:) vers Téléchargements
8% terminé

Vitesse : 10,4 Mo/s

Nom : Windows10_x64_x86.iso
Temps restant : Environ 3 minutes et 30 secondes
Éléments restants : 1 (6,74 Go)

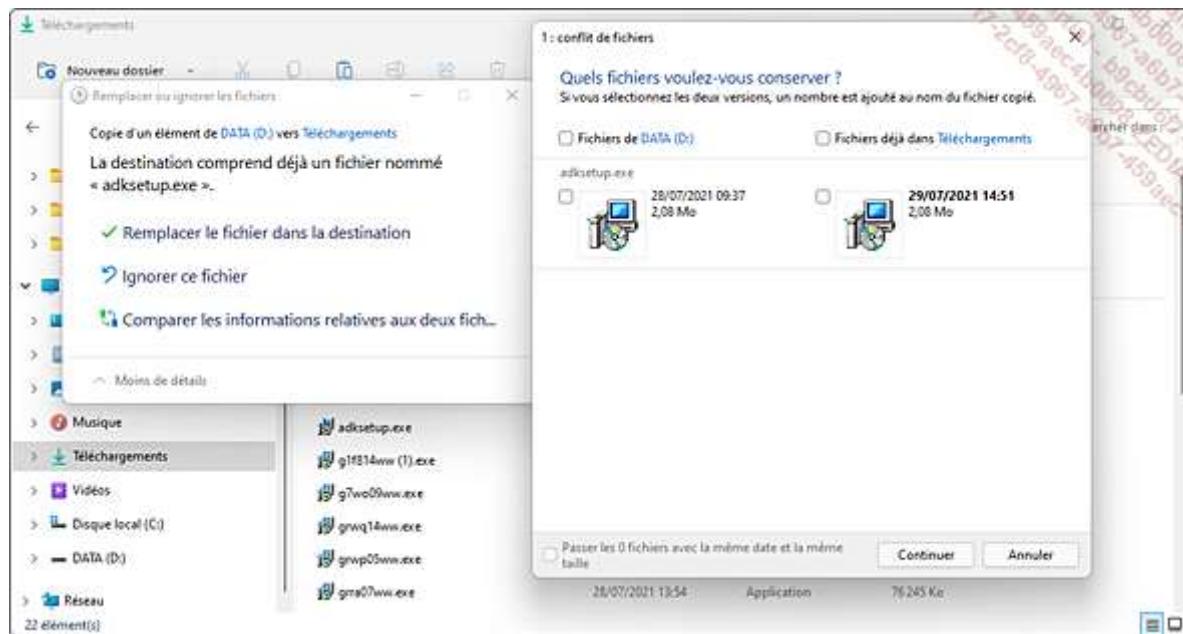
Copie d'un élément de DATA (D:) vers Disque local (C):
8% terminé

Vitesse : 31,1 Mo/s

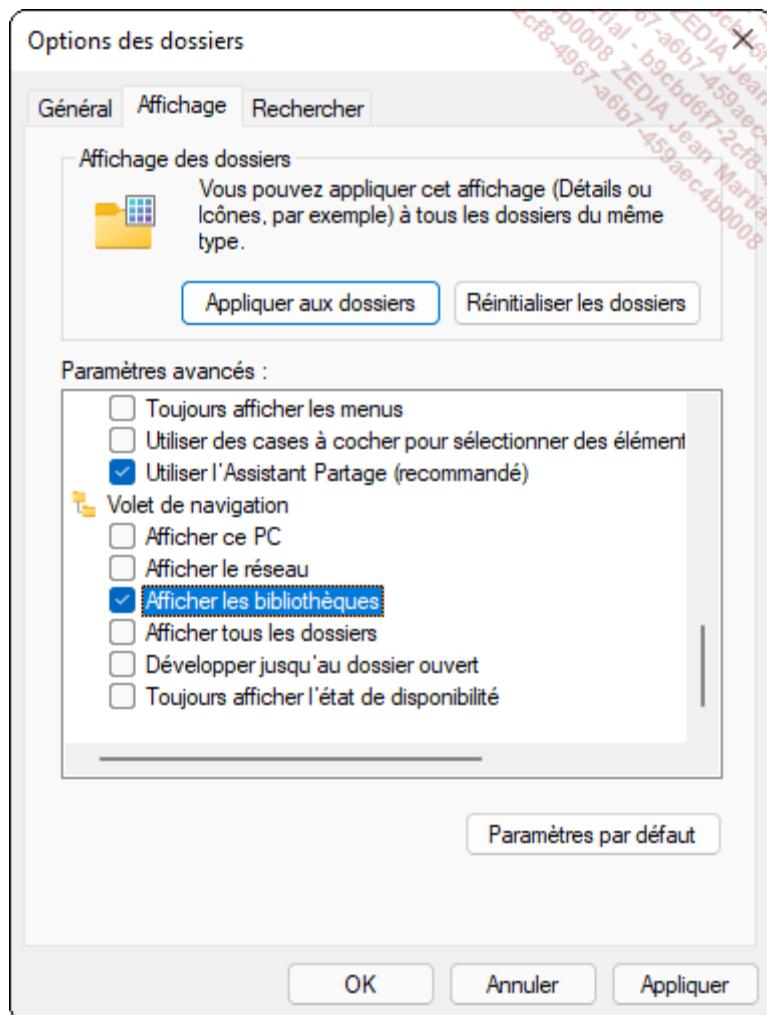
Nom : Windows10_x64_x86.iso
Temps restant : Environ 30 secondes
Éléments restants : 1 (6,78 Go)

[Moins de détails](#)

Lorsque l'emplacement de destination contient déjà un fichier portant le même nom que celui en cours de copie, l'utilisateur peut comparer le fichier source et celui de destination pour choisir lequel garder en cliquant sur **Comparer les informations relatives aux deux fichiers** dans la boîte de dialogue **Remplacer ou ignorer les fichiers** :



Les bibliothèques, présentes dans les anciennes versions de Windows, ne sont plus affichées par défaut. Pour y remédier, il suffit de cliquer sur le bouton **En savoir plus**, puis **Options**. Affichez l'onglet **Affichage** et dans **Paramètres avancés** descendez jusqu'à **Volet de navigation** et cochez **Afficher les bibliothèques**.



7. OneDrive

OneDrive est le service de cloud computing proposé par Microsoft aux utilisateurs possédant un compte Microsoft (anciennement Windows Live). Implémentée avec Windows 11 (depuis Windows 10) et totalement intégrée à l'Explorateur de fichiers, la fonctionnalité permet de stocker ses données personnelles gratuitement dans un espace de 5 Go, et nécessite de payer un abonnement annuel pour augmenter cette capacité. Ainsi, plusieurs périphériques, tels qu'un téléphone (supérieur ou égale à iOS 12.0, supérieur ou égale à Android 6.0) ou un ordinateur pourvu d'une version supérieure à Windows Vista SP2 ou macOS 10.12, peuvent accéder aux mêmes fichiers stockés sur Internet.

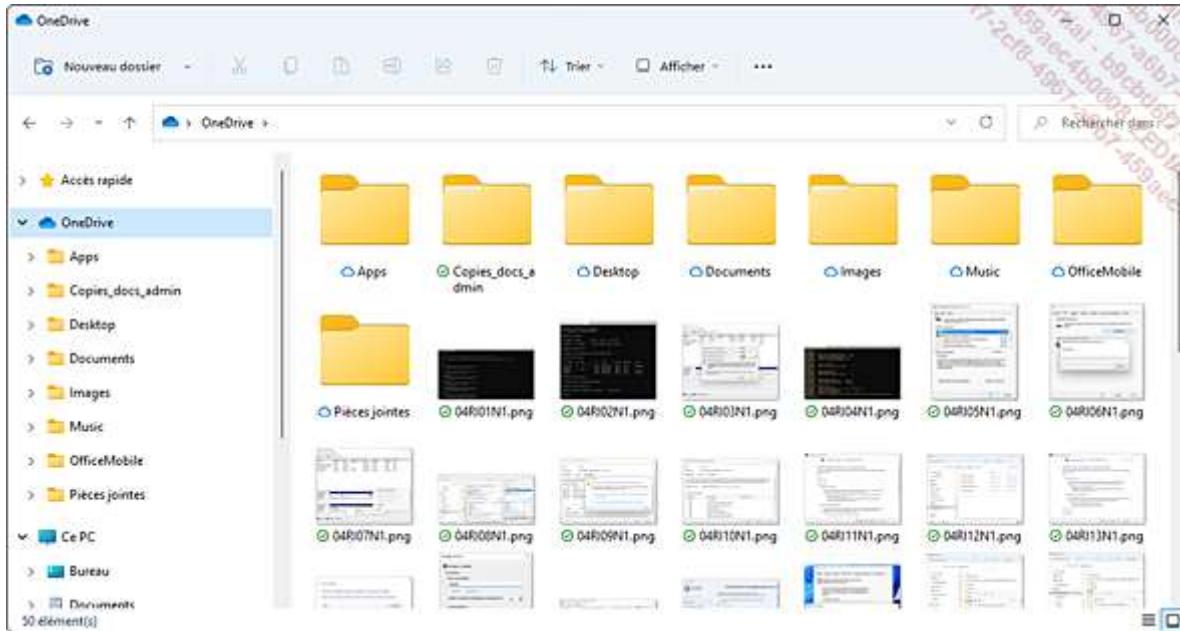
OneDrive est désormais un composant principal de Windows 11, ainsi que d'autres logiciels, comme Microsoft Office ou le moteur de recherche Bing.

Après avoir tapé onedrive dans le champ de recherche situé sur la barre des tâches, l'utilisateur est invité à entrer ses informations de connexion (compte Microsoft) et à sélectionner les dossiers à synchroniser sur le poste de travail Windows 11.

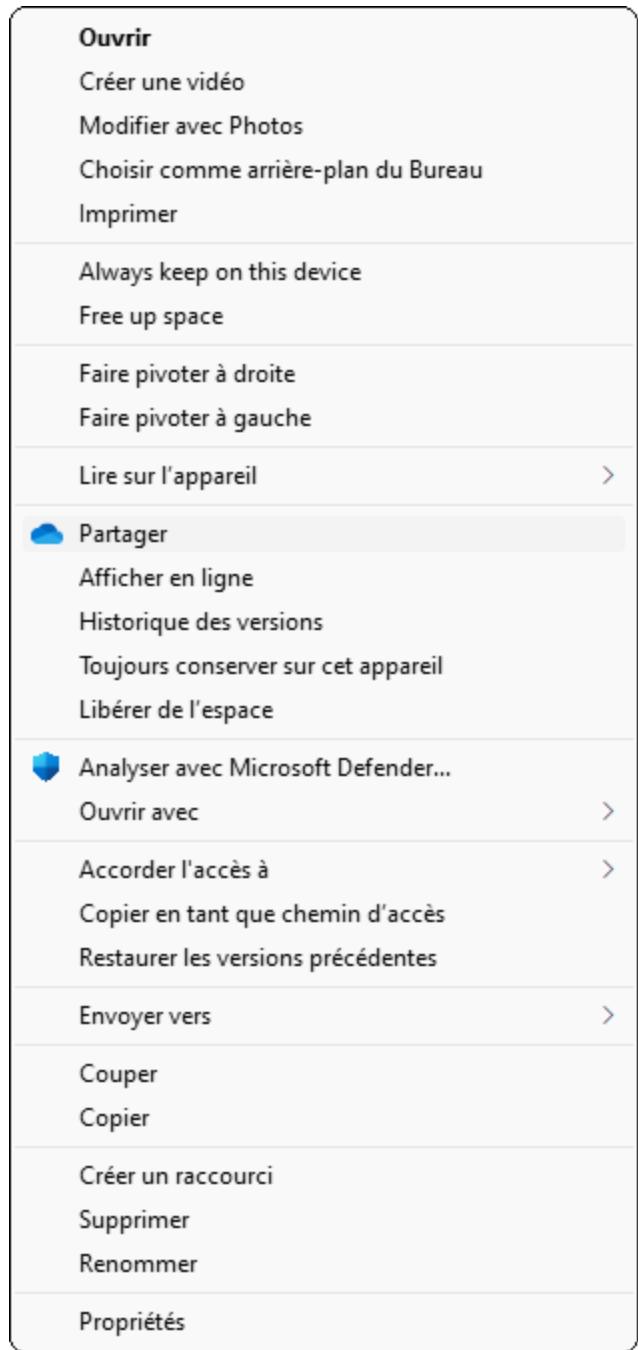
Le service peut être utilisé de trois manières :

- Depuis un navigateur internet en se connectant au site <https://onedrive.live.com/> et en s'authentifiant à l'aide d'un compte Microsoft.

- Depuis l'application OneDrive, disponible avec un compte Microsoft Passeport, mais aussi en téléchargement pour des systèmes d'exploitation concurrents de Microsoft, tels que macOS et Android.
- Depuis l'Explorateur de fichiers et le nœud **OneDrive**, les documents sont affichés comme s'ils étaient stockés uniquement sur l'ordinateur et non dans le cloud.



Un simple clic avec le bouton droit sur ceux-ci et l'utilisateur peut les partager avec d'autres utilisateurs grâce à l'option **Afficher plus d'options, Partager** (celui avec l'icône d'un nuage bleu).



Par défaut, quelques dossiers sont créés (Documents, Images, Music...) pour y stocker des fichiers en ligne. En cliquant avec le bouton droit sur ces fichiers ou dossiers, le menu contextuel standard apparaît, afin de pouvoir supprimer la sélection, la renommer...

Les dossiers OneDrive sont automatiquement synchronisés. Un simple glissé-déposé d'un dossier ou fichier dans l'arborescence OneDrive permet de synchroniser celui-ci dans le cloud de Microsoft.

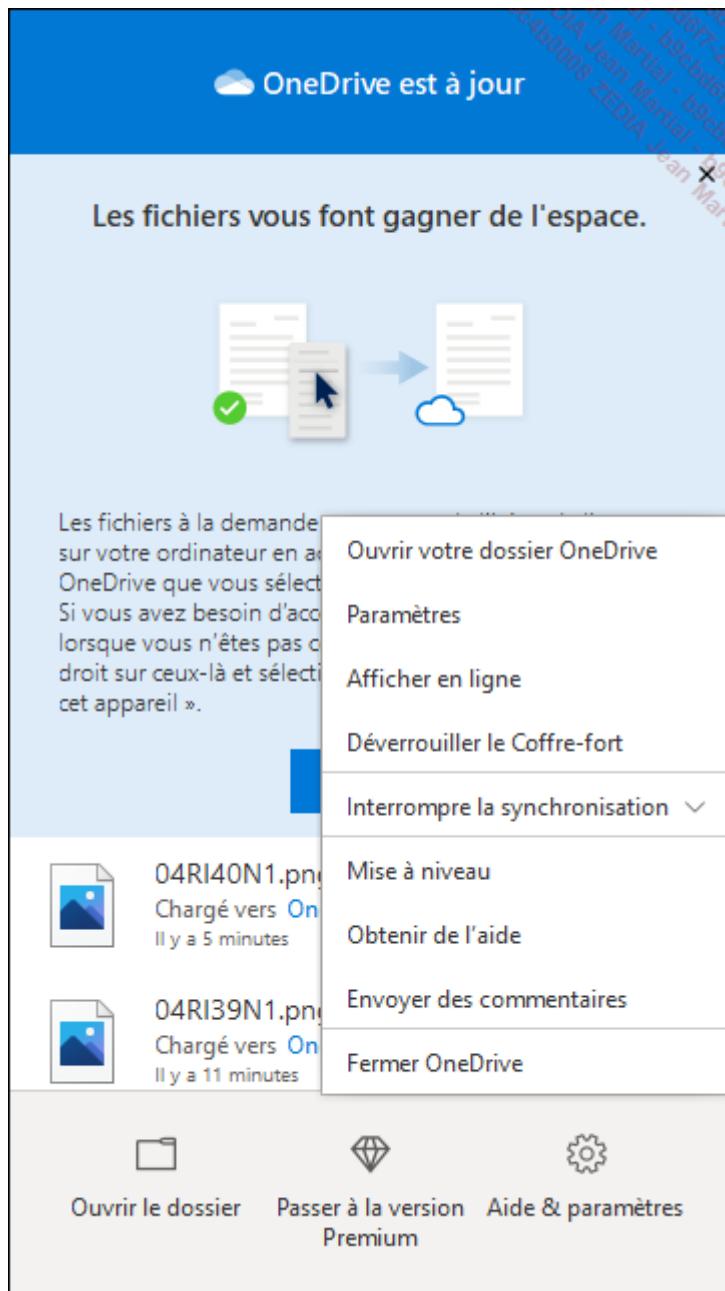
Un dossier ou fichier OneDrive peut passer par trois états :

- Ressource synchronisée avec sa version en ligne dans le cloud OneDrive.
- Ressource en cours de synchronisation.
- Ressource non synchronisée.

Enfin, la version intégrée à Windows 11 affiche dans la barre des tâches une icône OneDrive représentée par un nuage blanc/gris. Elle permet à l'utilisateur de visualiser l'état de la synchronisation en cours ainsi que les problèmes de connectivité éventuels.



Un clic droit sur cette icône permet d'accéder directement au dossier local (**Ouvrir votre dossier OneDrive**) ou en ligne (**Afficher en ligne**), ainsi qu'aux paramètres du logiciel : démarrage automatique, état de l'espace de stockage, dossiers sauvegardés, limitation de la vitesse de chargement ou de téléchargement...

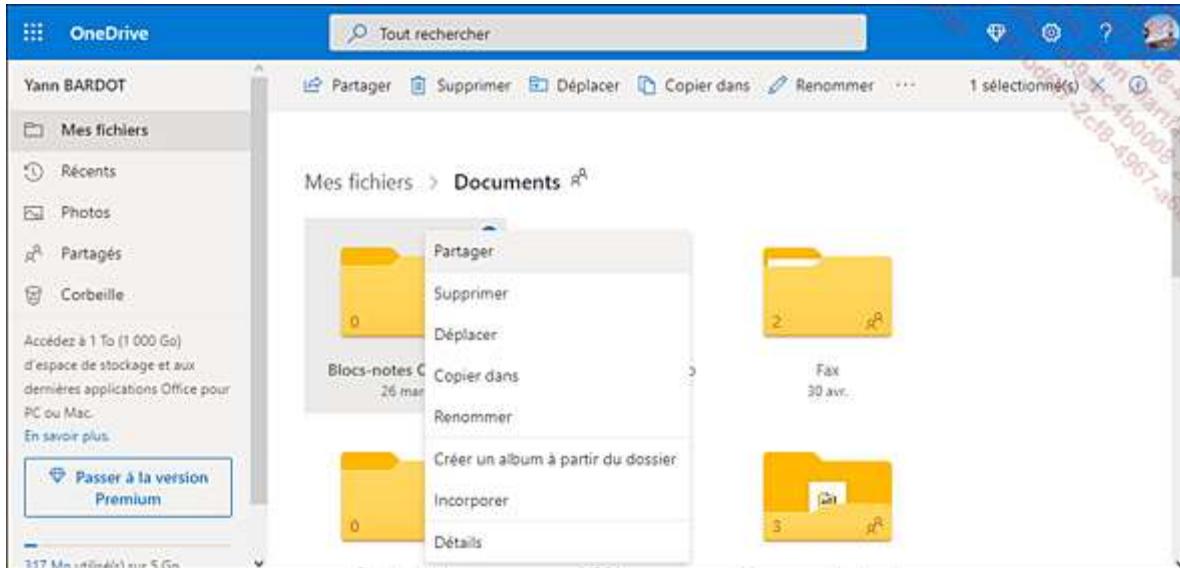


Depuis un navigateur internet, en vous authentifiant sur le site : <https://onedrive.live.com/>

Vous pouvez accéder à vos données de manière sécurisée, et les rendre disponibles à d'autres personnes simplement.

En cliquant avec le bouton droit sur un dossier, puis sur **Partager**, il est possible de le partager en l'envoyant par courrier électronique ou en partageant un lien. Les données sont accessibles en consultation ou en modification, auprès de n'importe qui ou pour des personnes désignées.

Toutes les opérations de base sur un fichier sont possibles : **Partager**, **Télécharger**, **Supprimer**, **Copier dans**, **Incorporer**... Il suffit d'effectuer un clic avec le bouton droit sur la ressource cible.



Notez la présence d'un système d'historique et de restauration qui permet de retrouver la version précédente d'un fichier après l'avoir modifié. Il est accessible en cliquant avec le bouton droit sur un fichier et en sélectionnant **Historique des versions**.

Le site permet en outre de créer des documents **Microsoft Office (Word, Excel, PowerPoint et OneNote)** depuis le navigateur, sans posséder la suite bureautique, en cliquant sur l'icône associée depuis le menu **+Nouveau**. Lorsqu'un fichier est supprimé, il est envoyé à la corbeille de OneDrive, située en bas à gauche de l'interface.

8. Amélioration des performances

Sécurité, fiabilité et prise en charge de disques de grande capacité sont autant d'éléments à prendre en compte lors du choix du système de fichiers.

L'utilisation du système de fichiers NTFS est recommandée pour gérer efficacement les données stockées sur le disque dur de l'ordinateur, grâce aux fonctionnalités d'espaces de stockage, de quota et de compression des données. En outre, NTFS peut appliquer des permissions précises sur les fichiers et dossiers.

a. Compression

Compresser un fichier ou un dossier permet de libérer de l'espace disque pour stocker de nouvelles données. Un disque saturé peut rendre le système Windows 11 lent et instable s'il devient impossible d'utiliser le fichier de pagination.

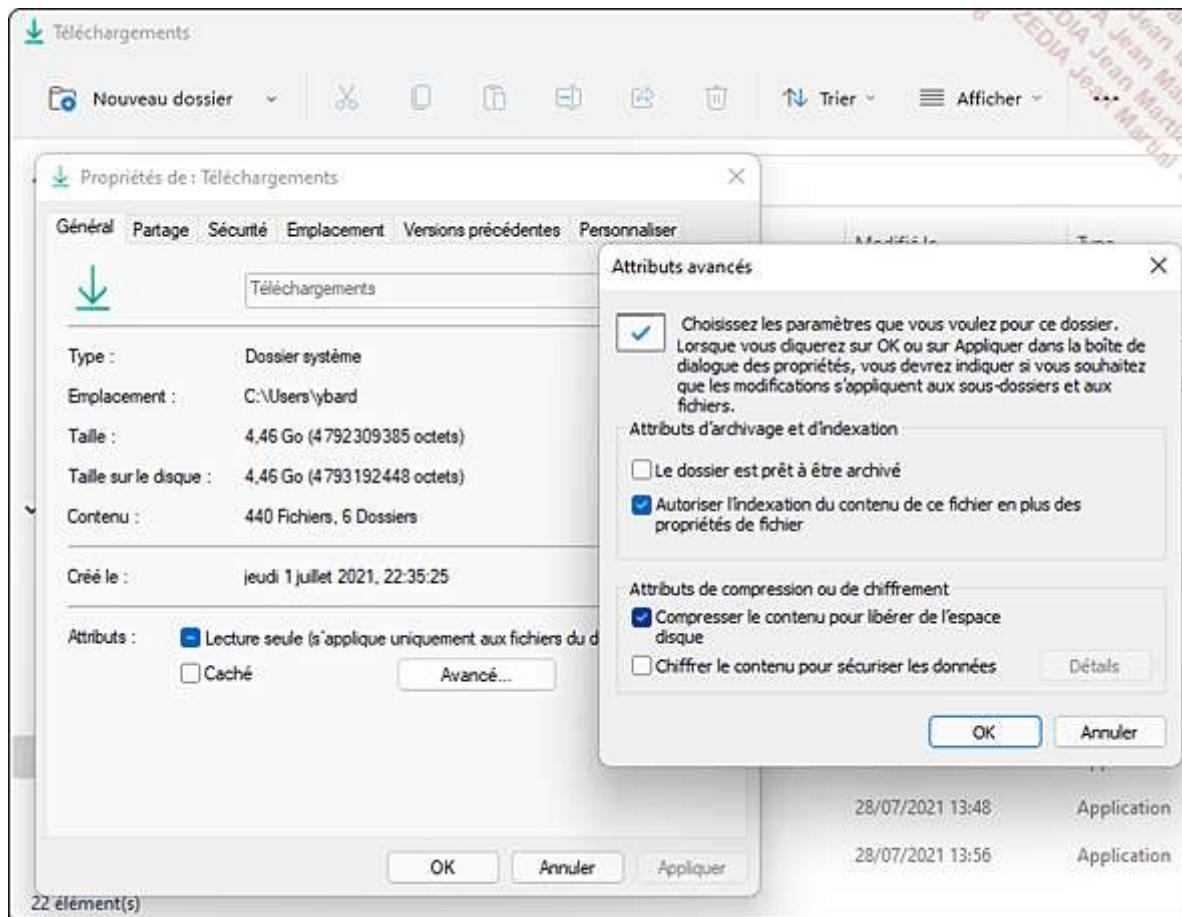
La fonctionnalité de compression est un processus invisible pour l'utilisateur, disponible sur les partitions NTFS uniquement. Lorsque vous copiez ou déplacez un fichier ou un dossier compressé, sachez que le système calcule la taille nécessaire sur la destination comme si les données étaient décompressées. Il en est de même pour les quotas : la taille allouée aux utilisateurs est calculée en fonction de l'espace utilisé par ses données décompressées.

Un dossier compressé est affiché en bleu. Un fichier ne peut être chiffré et compressé en même temps. Dans les deux cas, lors de l'ouverture, sa décompression ou son déchiffrement sont invisibles pour l'utilisateur.

Pour compresser un fichier :

Depuis l'Explorateur de fichiers, cliquez avec le bouton droit sur le fichier, puis choisissez **Propriétés**.

Cliquez sur le bouton **Avancé** de l'onglet **Général** puis cochez la case **Compresser le contenu pour libérer de l'espace disque**. Notez que cocher la case **Chiffrer le contenu pour sécuriser les données** décoche celle liée à la compression, et inversement.



L'utilisateur peut aussi créer un fichier zippé (extension .zip) contenant des dossiers et fichiers compressés. Aucun code couleur ne définit cette méthode de compression.

Par exemple, pour compresser un fichier, cliquez dessus avec le bouton droit, puis cliquez sur **Compresser dans le fichier ZIP**. Un dossier compressé portant le même nom que le fichier original est créé, avec l'extension .zip.

Autre possibilité de compression, celle d'utiliser la commande compact.exe. Sans argument, elle affiche l'état de compression du dossier en cours, et de tous les fichiers qu'il stocke.

b. Quota de disque

Un autre moyen d'optimiser les performances des disques d'un ordinateur est de limiter la quantité d'espace disque disponible pour les utilisateurs de celui-ci.

L'activation des quotas est possible sur les serveurs de fichiers, les volumes locaux NTFS mais aussi sur les périphériques de stockage amovibles.

Un quota peut superviser l'espace disque que consomme un utilisateur en alertant l'administrateur, sans forcément en limiter l'écriture.

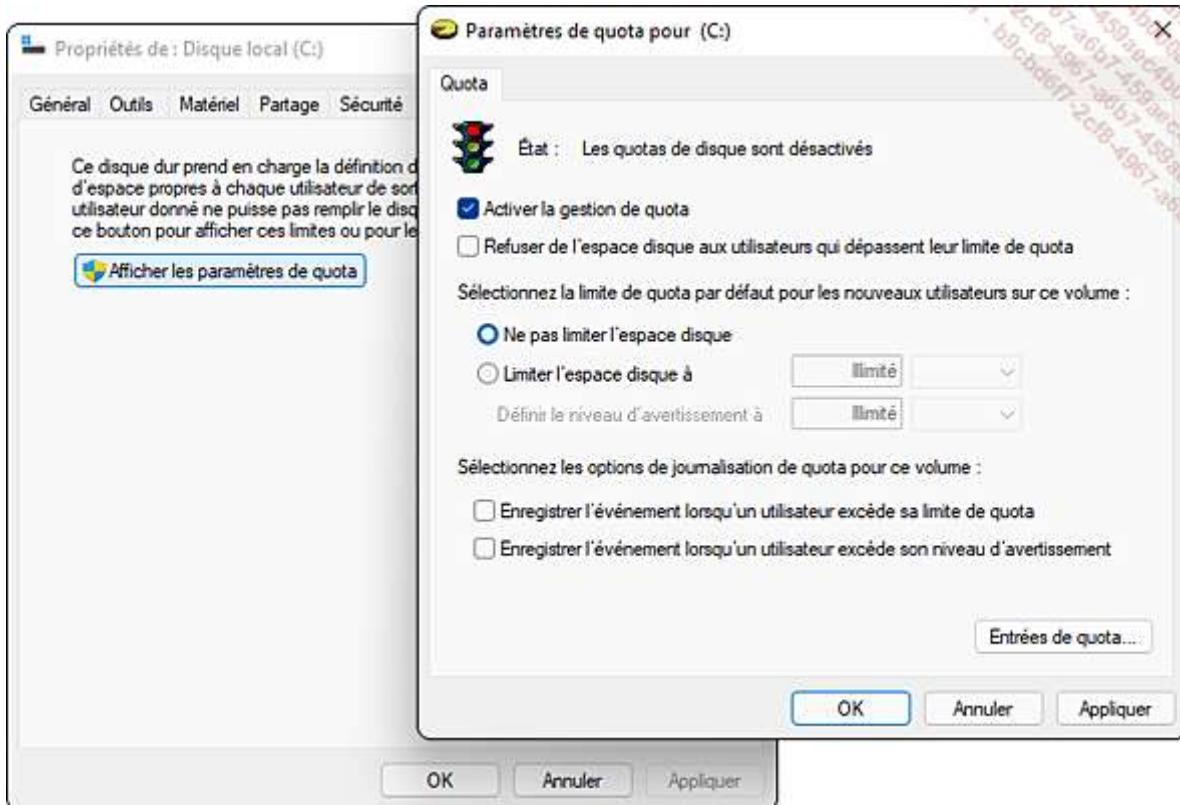
Les quotas sont configurables, au travers d'un objet stratégie de groupe, pour uniformiser la gestion de l'espace disque dans un environnement d'entreprise.

Une fois un quota créé sur un volume, vous pouvez exporter ses paramètres pour les importer sur d'autres volumes.

Pour activer un quota sur une partition NTFS :

Cliquez sur l'Explorateur de fichiers situé dans la barre des tâches puis développez **Ce PC** et **C:**. Cliquez avec le bouton droit sur la lettre de lecteur de votre disque dur, puis choisissez **Propriétés**.

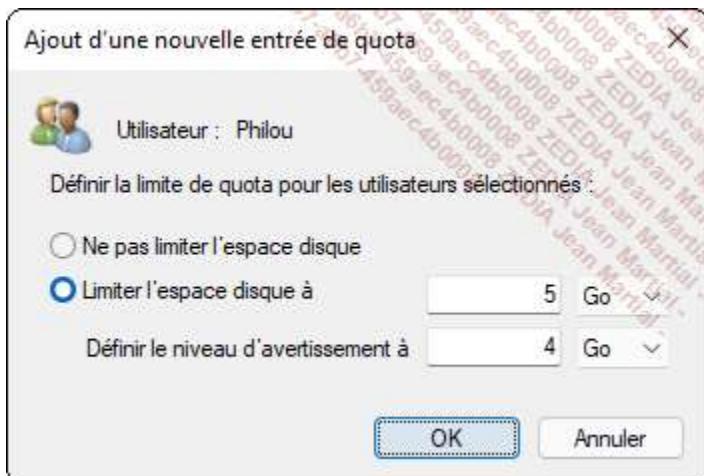
Sélectionnez l'onglet **Quota**, et cliquez sur le bouton **Afficher les paramètres de quota**. En premier lieu, cochez la case **Activer la gestion de quota**.



Vous pouvez créer une règle globale sur le volume en sélectionnant la case **Limiter l'espace disque à** et en spécifiant une valeur de référence ainsi qu'un niveau d'avertissement.

L'enregistrement de dépassement d'un quota dans les journaux d'événements s'effectue en cochant la case **Enregistrer l'événement lorsqu'un utilisateur excède sa limite de quota**.

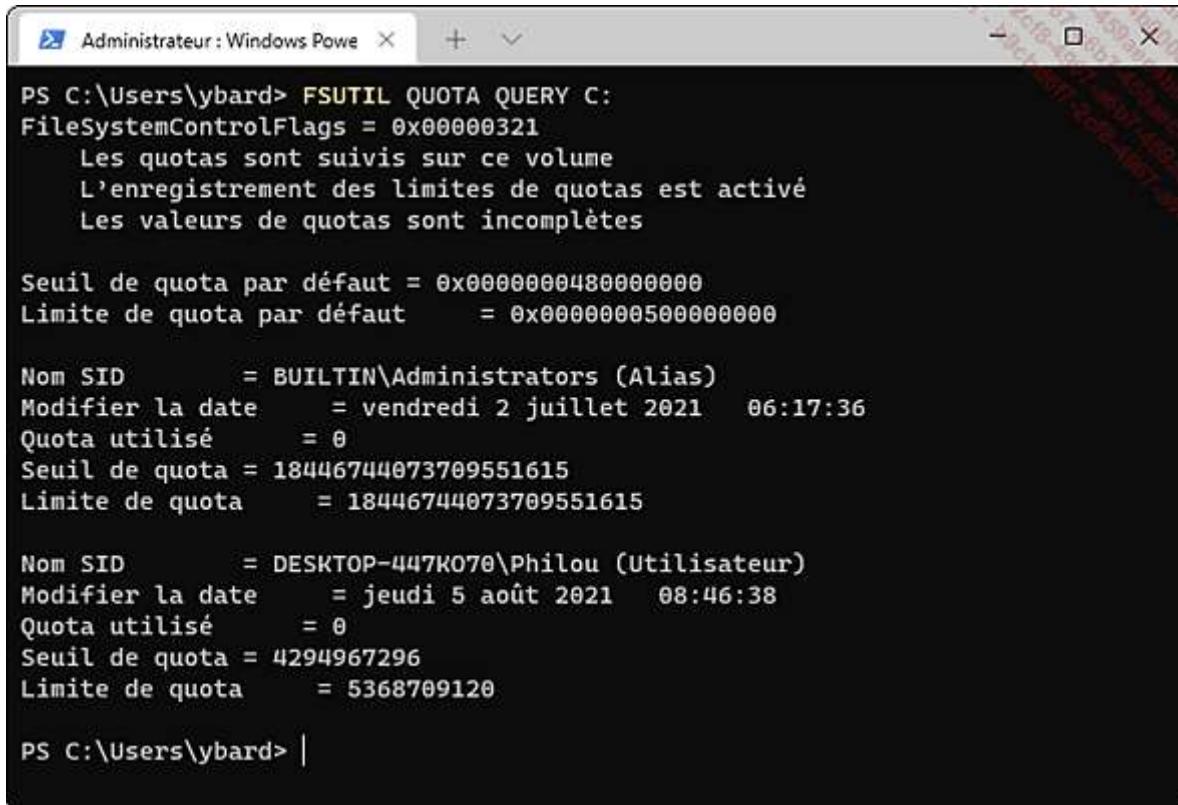
Définissez ensuite des quotas spécifiques par utilisateur en cliquant sur le bouton **Entrées de quota**. Cliquez sur **Nouvelle entrée de quota**, saisissez le nom d'un utilisateur, validez avec le bouton **OK** et entrez la limite d'espace disque pour cet utilisateur.



Le menu **Quota** permet également d'importer ou d'exporter des règles de quota.

Une entrée de quota ne se configure que pour des utilisateurs, pas pour des groupes.

Toutes ces opérations sont également possibles à l'aide de la commande fsutil quota, exécutée en tant qu'administrateur de l'ordinateur.



```
PS C:\Users\ybard> FSUTIL QUOTA QUERY C:
FileSystemControlFlags = 0x00000321
Les quotas sont suivis sur ce volume
L'enregistrement des limites de quotas est activé
Les valeurs de quotas sont incomplètes

Seuil de quota par défaut = 0x0000000480000000
Limite de quota par défaut      = 0x0000000500000000

Nom SID      = BUILTIN\Administrators (Alias)
Modifier la date      = vendredi 2 juillet 2021  06:17:36
Quota utilisé      = 0
Seuil de quota = 18446744073709551615
Limite de quota      = 18446744073709551615

Nom SID      = DESKTOP-447K070\Philou (Utilisateur)
Modifier la date      = jeudi 5 août 2021  08:46:38
Quota utilisé      = 0
Seuil de quota = 4294967296
Limite de quota      = 5368709120

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

c. Défragmentation du disque

Lors d'une nouvelle installation de Windows 11, le système classe les blocs de fichiers de façon contiguë dans l'espace disque disponible, optimisant ainsi les performances d'accès.

Un disque fragmenté contient des fichiers épars dans des espaces non contigus, car les utilisateurs et processus exécutés par le système manipulent régulièrement les fichiers (modification, suppression et création).

Défragmenter un disque permet aux têtes de lecture/écriture du disque dur de réorganiser efficacement ces données et donc d'y accéder plus rapidement.

La défragmentation n'est bien évidemment utile que pour les disques durs mécaniques. Les SSD (*Solid State Drive*), du fait de leur fonctionnement, n'ont pas besoin d'être défragmentés. Au contraire, cette opération réalisée régulièrement pourrait même réduire leur durée de vie.

Windows 11 exécute de manière hebdomadaire la défragmentation du disque au travers du planificateur de tâches. Il faudra donc désactiver cette planification si l'ordinateur dispose d'un SSD.

La défragmentation manuelle s'effectue comme suit :

Cliquez avec le bouton droit sur le volume à défragmenter dans le nœud **Ce PC** de l'Explorateur de fichiers puis choisissez l'option **Propriétés**.

Sélectionnez l'onglet **Outils**, et cliquez sur le bouton **Optimiser**.

The screenshot shows the Windows Disk Defragmenter interface. At the top, a message states: "Vous pouvez optimiser vos lecteurs pour permettre à l'ordinateur de fonctionner plus efficacement ou bien analyser ces lecteurs pour rechercher s'ils doivent être optimisés. Seuls les lecteurs connectés et installés sur votre ordinateur sont affichés." Below this is a section titled "État" (Status) containing a table:

Lecteur	Type de média	Dernière analyse o...	État actuel
■ (C:)	Lecteur de disque dur	04/08/2021 16:12	OK (0 % fragmentés)
■ DATA (D:)	Lecteur de disque dur	04/08/2021 16:01	OK (0 % fragmentés)

Below the table are two buttons: "Analyser" (Analyze) and "Optimiser" (Optimize). To the left of these buttons is a checkbox labeled "Vue Avancé" (Advanced View). Further down, under "Optimisation planifiée" (Planned Optimization), it says "Activé" (Enabled) and "Les lecteurs sont en cours d'analyse à une fréquence planifiée et optimisée selon les besoins." (The drives are being analyzed at a planned frequency and optimized according to needs.) There is also a button "Modifier les paramètres" (Change parameters). At the bottom right of the window is a "Fermer" (Close) button.

Si nécessaire, cliquez sur **Analyser** puis sur **Optimiser** pour exécuter la défragmentation.

Vous pourrez aussi modifier/désactiver la date de défragmentation planifiée, grâce au bouton **Modifier les paramètres**. Si Windows est installé sur un SSD, c'est donc ici qu'il vous faudra intervenir. Après l'impossibilité de défragmenter un disque trois fois consécutives, Windows 11 affiche un message à l'utilisateur.

Plus le pourcentage de fragmentation est élevé, plus la défragmentation prend son sens. Un périphérique USB peut être défragmenté, mais bien entendu, la vitesse d'exécution du processus dépendra du débit de l'interface USB.

En tant qu'administrateur de l'ordinateur, vous pouvez exécuter une défragmentation à l'aide de la commande defrag.

Par exemple, la commande defrag /c /m effectue une défragmentation de tous les volumes en arrière-plan. Néanmoins, cette commande ne permet pas de défragmenter un disque à distance.

Pilotes de périphériques

Un pilote (ou driver en anglais) est un programme permettant à des applicatifs d'interagir avec des composants matériels, comme un clavier, une souris ou encore une imprimante ; ce sont des périphériques qui ajoutent des fonctionnalités à l'ordinateur.

Il existe deux types de périphériques : ceux d'entrée qui servent à fournir des données à l'ordinateur (clavier, scanner...), et ceux de sortie, permettant d'exporter l'information (écran, haut-parleur...).

Le pilote est souvent fourni par le constructeur du matériel. S'il était absent, le matériel serait difficilement utilisable ou du moins limité en termes d'exploitation des fonctionnalités. Toutefois, Windows 11 intègre en standard des pilotes correspondant aux matériels informatiques les plus usités, même s'il reste possible de télécharger les pilotes manquants par l'intermédiaire du site internet du constructeur, ou simplement en exécutant le programme Windows Update sur son ordinateur.

Un serveur **WSUS** (*Windows Server Update Services*) peut également déployer les pilotes signés par Microsoft sur les postes de travail de l'entreprise.

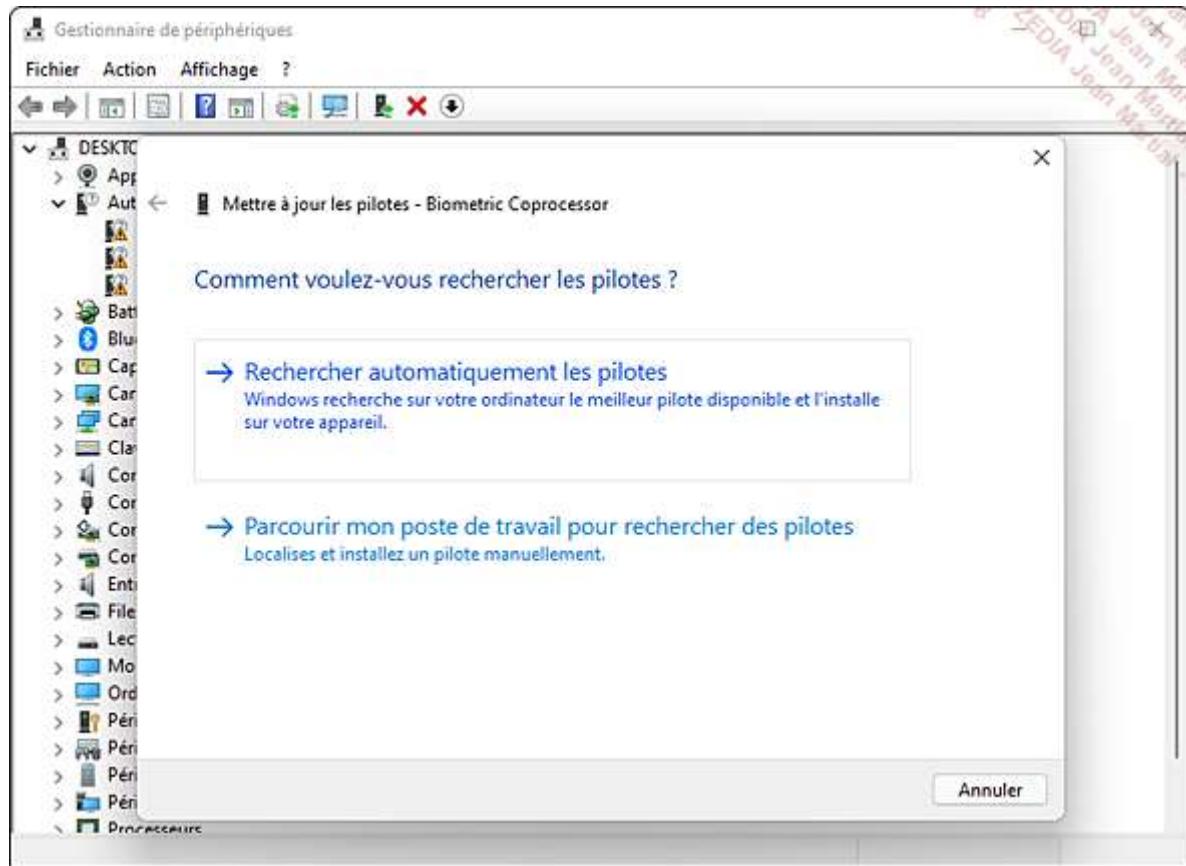
L'utilisation d'un pilote développé spécifiquement pour un périphérique assure à l'utilisateur l'exploitation maximale des fonctionnalités du matériel acheté. Ainsi, le nombre d'appels au support technique de l'entreprise est diminué et la satisfaction du client final plus importante.

Un pilote est dépendant de l'architecture sur lequel il est installé : un pilote 32 bits développé pour un périphérique ne peut être installé sur la version 64 bits de Windows 11. Si un pilote était manquant ou défectueux, le système générera un rapport d'erreurs contenant des informations aidant à la résolution du problème rencontré.

Un pilote à jour corrige généralement des failles de sécurité et des bugs. Le programme Windows Update propose aux clients de télécharger les derniers pilotes fournis par les fabricants. Il est aussi possible de les mettre à jour manuellement pour un périphérique précis :

Cliquez avec le bouton droit sur le menu **Démarrer** puis sélectionnez **Gestionnaire de périphériques**.

Cliquez sur le périphérique cible avec le bouton droit puis choisissez **Mettre à jour le pilote**. Choisissez la méthode de recherche du pilote : sur Internet ou sur votre poste de travail, indiquez ensuite l'emplacement de stockage du pilote.



Notez que seul un compte administrateur peut supprimer des pilotes du système ou en réinstaller une ancienne version.

Les pilotes fournis avec Windows 11 sont signés par Microsoft, assurant une compatibilité parfaite avec le système d'exploitation. Ils sont stockés dans un référentiel, nommé le magasin central.

1. Pilotes signés et non signés

Un pilote signé est un pilote validé numériquement par son concepteur (signature numérique), ce qui signifie qu'il n'a pas été modifié par une personne malveillante, et qu'il provient donc d'une source de confiance.

Windows Update ou un serveur WSUS permettent de télécharger sur les postes les pilotes signés de constructeurs connus.

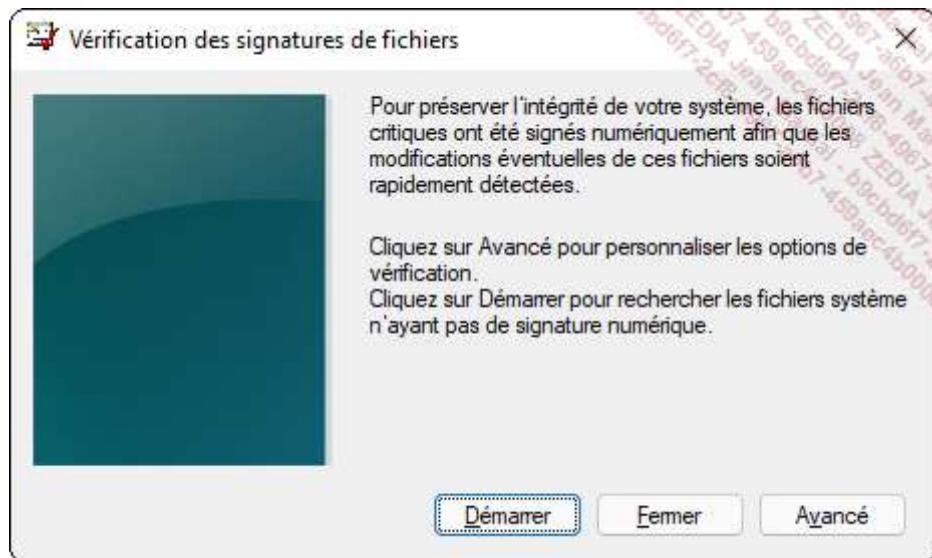
Privilégier ces derniers contribue à renforcer la sécurité, diminuant ainsi les coûts liés à l'utilisation d'un support technique. Les fichiers de signature portent l'extension .cat et sont stockés dans le même dossier que les pilotes qu'ils signent.

Pour visualiser les pilotes non signés sur un ordinateur, Windows 11 propose la commande sigverif.

Voici la procédure :

Dans le champ **Rechercher** de la barre des tâches, saisissez sigverif et sélectionnez **sigverif**.

Dans la fenêtre **Vérification des signatures de fichiers**, cliquez sur le bouton **Démarrer**.



À la fin de l'analyse, la liste des pilotes signés et non signés sera visible en cliquant sur le bouton **Avancé**, puis **Afficher le journal**.

SIGVERIF.TXT - Bloc-notes

Fichier Modifier Format Affichage Aide

Vérification de signature Microsoft

Fichier journal généré sur 05/08/2021 à 11:14

Plate-forme : Windows (x64), Version : 10.0, build : 22000, CSDVersion :

Résultats : nombre total de fichiers : 709, signé(s) : 709, non signé(s) : 0, non analysés(s) : 0

Fichier	Modifié	Version	État	Catalogue	Signé par
...

Ln 1, Col 1 100% Windows (CRLF) UTF-16 LE

This screenshot shows a Microsoft Notepad window displaying the contents of the SIGVERIF.TXT log file. The window title is "SIGVERIF.TXT - Bloc-notes". The content starts with the title "Vérification de signature Microsoft" and a timestamp. It then provides system information and analysis results. Below this, there is a table with six columns: "Fichier", "Modifié", "Version", "État", "Catalogue", and "Signé par". The table has a single row with ellipsis values. At the bottom of the window, there are status indicators for line number (Ln 1, Col 1), zoom level (100%), and encoding (Windows (CRLF), UTF-16 LE).

Pour obtenir la liste des pilotes de périphériques signés et non signés, utilisez la commande :

driverquery /si | more

L'avantage de cette commande est qu'elle permet d'interroger des systèmes distants, au contraire de sigverif.

```
PS C:\Users\ybard> driverquery /si |more

DeviceName           InfName     IsSigned Manufacturer
=====
WAN Miniport (Network Monitor) netrasa.inf   TRUE    Microsoft
WAN Miniport (IPv6)       netrasa.inf   TRUE    Microsoft
WAN Miniport (IP)        netrasa.inf   TRUE    Microsoft
WAN Miniport (PPPOE)     netrasa.inf   TRUE    Microsoft
WAN Miniport (PPTP)      netrasa.inf   TRUE    Microsoft
WAN Miniport (L2TP)      netrasa.inf   TRUE    Microsoft
WAN Miniport (IKEV2)     netavpna.inf  TRUE    Microsoft
WAN Miniport (SSTP)      netsstpa.inf  TRUE    Microsoft
Generic software device c_swdevice.in  TRUE    Microsoft
Hyper-V Virtual Switch Extension wvms_mp_windo TRUE    Microsoft
Local Print Queue       printqueue.in  TRUE    Microsoft
Xvdd SCSI Miniport      oem32.inf    TRUE    Xbox
Generic software device c_swdevice.in  TRUE    Microsoft Corporation
Generic software device c_swdevice.in  TRUE    SoftAtHome
```

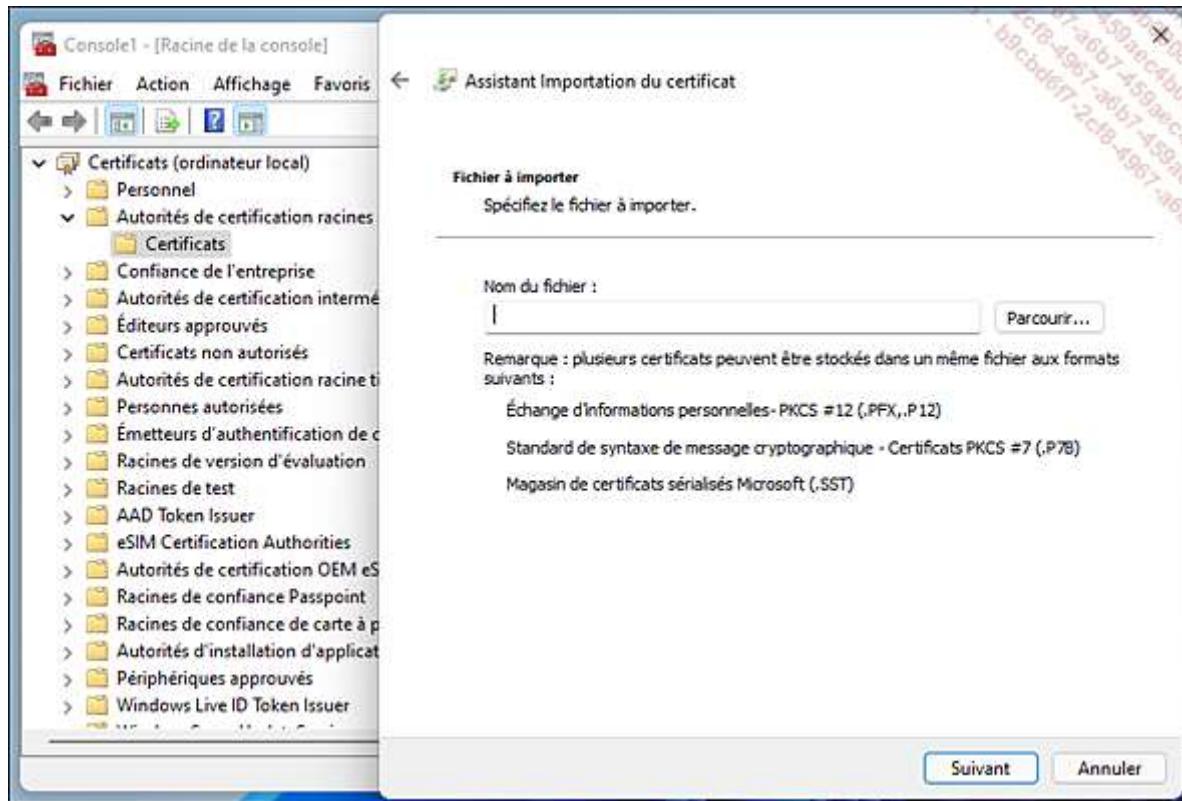
Windows 11 maintient un magasin des certificats de confiance. L'administrateur peut ajouter des certificats provenant d'éditeurs de confiance afin de s'assurer de l'installation des périphériques. Les pilotes signés numériquement par une autorité de certification contiennent un fichier catalogue. Ce fichier contient le hachage des fichiers présents dans le fichier .inf du pilote à installer.

La console MMC **Certificats** permet d'ajouter les certificats externes pour des pilotes tiers dans les magasins **Autorités de certification racines de confiance** et **Éditeurs approuvés**. Pour ce faire :

Pressez les touches + R, saisissez mmc dans le champ **Ouvrir** puis validez par la touche [Entrée]. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît. Cliquez sur le menu **Fichier** puis sur **Ajouter/Supprimer un composant logiciel enfichable**.

Dans la liste de gauche **Composants logiciels enfichables disponibles**, sélectionnez **Certificats**, puis cliquez sur le bouton **Ajouter**. Dans la fenêtre **Composant logiciel enfichable Certificats**, sélectionnez la case **Un compte d'ordinateur**, puis cliquez sur **Suivant** et **Terminer**. Validez par **OK**.

Développez dans la zone de gauche **Certificats (ordinateur local)**, puis le nœud **Autorités de certification racines de confiance**. Effectuez un clic avec le bouton droit sur **Certificats** puis choisissez **Toutes les tâches** et **Importer**. Sélectionnez ensuite le certificat fourni avec le pilote à installer. Renouvez l'opération depuis le nœud **Éditeurs approuvés**.



Notez que l'ajout de certificats sur un ensemble d'ordinateurs peut être effectué à l'aide d'un objet de stratégie de groupe.

2. Magasin central de pilotes

Le magasin central de pilotes est le référentiel des pilotes approuvés pour l'installation sur un ordinateur. Il est stocké dans le dossier %systemroot%\System32\DriverStore.

L'utilité du magasin de pilotes est d'inclure des packages propres au matériel sur chaque poste de l'entreprise, afin d'éviter les interventions manuelles d'installation.

La suppression d'un package de pilotes de périphériques du magasin ne désinstalle pas un périphérique actif qui l'utilisera. Les copies des fichiers pilotes installées ne sont donc pas supprimées mais la copie stockée dans le magasin de pilotes l'est en revanche. Si un nouveau périphérique utilisant le pilote supprimé était branché, Windows 11 chercherait une nouvelle fois le package de pilotes en utilisant les emplacements par défaut.

a. Utilitaire Pnputil

Pour supprimer un pilote du magasin de pilotes en tant qu'administrateur :

Pressez les touches + R et saisissez cmd dans la fenêtre **Exécuter**. Saisissez la commande :

```
pnputil -e
```

Dans la liste des pilotes affichée, notez le nom publié du fichier (OEM et son numéro) avec l'extension .inf.

Pour supprimer un pilote même s'il est en cours d'utilisation, saisissez la commande :

```
pnputil.exe -f -d oemnomfichier.inf
```

Le paramètre -a permet d'ajouter un pilote au magasin de pilotes.

b. Commande DISM

Il est possible d'ajouter ou de supprimer des pilotes du magasin de pilotes dans une image WIM montée hors connexion : pour effectuer cette action, nous utiliserons la commande DISM (cf. chapitre Conception d'une image de déploiement, section Crédit d'une installation de référence).

Avant d'effectuer la procédure, il est nécessaire de copier le fichier image install.wim (répertoire Sources du DVD d'installation) dans un dossier de travail, dans notre exemple c:\temp. De plus, l'image doit être montée dans un sous-dossier vide, que nous nommerons Offline dans le répertoire de travail c:\temp.

Les actions suivantes ajouteront des pilotes au magasin de pilotes :

Depuis une invite de commandes exécutée en tant qu'administrateur, l'option get-wiminfo permet de lister les versions et ainsi récupérer l'index utilisé :

```
dism /get-wiminfo /wimfile:c:\temp\install.wim
```

Nous utiliserons le numéro d'index correspondant à Windows 11 Professionnel.

Montez l'image dans le dossier c:\temp\offline :

```
Dism /Mount-Wim /WimFile:C:\temp\install.wim  
/index:6 /MountDir:C:\temp\offline
```

Ajoutez maintenant un pilote stocké dans le répertoire c:\windows\inf au magasin de pilotes :

```
Dism /Image:c:\temp\offline /Add-Driver  
/Driver:C:\windows\inf\cdrom.inf
```

Notez que si le pilote n'est pas signé, vous pourrez forcer son ajout à l'aide de l'option /ForceUnsigned.

Vous pouvez ajouter à une image tous les fichiers portant l'extension .inf stockés dans un dossier, en utilisant l'option /recurse.

Une fois que l'image WIM a été personnalisée, il est nécessaire d'enregistrer les modifications en démontant l'image :

```
dism /unmount-wim /mountdir:c:\temp\offline /commit
```

La suppression d'un pilote spécifique dans l'image montée nécessite l'utilisation du paramètre /Remove-Driver :

Pour supprimer un pilote précis de l'image montée hors connexion :

```
Dism /Image:C:\temp\offline /Remove-Driver  
/Driver:oemfichierpilote.inf
```

3. Gestionnaire de périphériques

La console **Gestionnaire de périphériques** aide l'utilisateur à installer et à mettre à jour les pilotes de périphériques matériels locaux, tout en proposant des outils de résolution des problèmes.

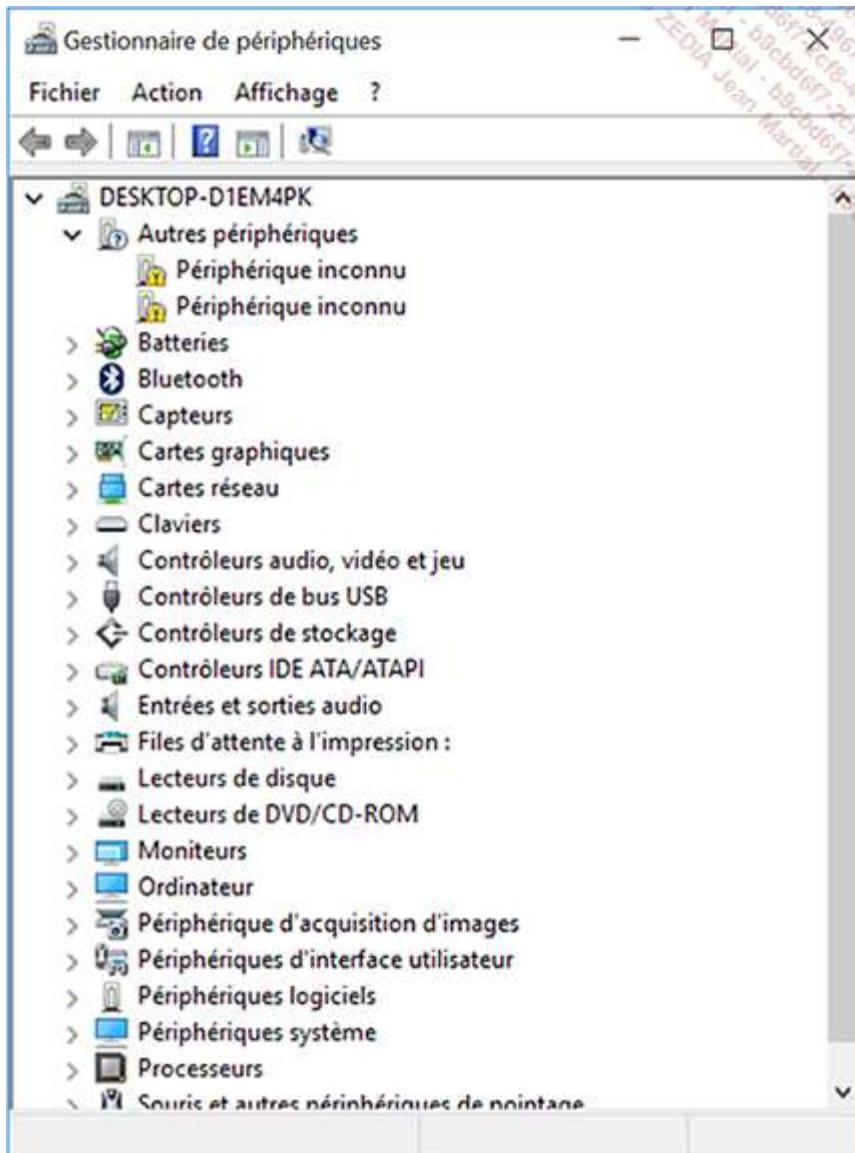
L'état d'un périphérique est affiché dans cette console :

- Un point d'interrogation noir derrière un triangle jaune signifie que le système n'a pas trouvé le pilote pour son utilisation.
- Un point d'interrogation derrière une flèche noire pointée vers le bas indique que le périphérique est désactivé.

Par l'intermédiaire du Gestionnaire de périphériques, il est possible d'installer des périphériques non "Plug-and-Play", comme par exemple une imprimante fonctionnant sur le port parallèle. Depuis le menu **Action** de la console Gestionnaire de périphériques, cliquez sur **Ajouter un matériel d'ancienne génération**.

En outre, les opérations sur les pilotes sont centralisées : désinstallation, mise à jour ou restauration.

Pour accéder à la console, depuis le bureau, effectuez un clic avec le bouton droit sur le menu **Démarrer**, puis sélectionnez **Gestionnaire de périphériques** :



Enfin, en sélectionnant le menu **Affichage** puis l'option **Afficher les périphériques cachés**, la console affichera les périphériques non "Plug-and-Play" (périphériques avec des versions antérieures de pilotes de périphériques Windows).

Le Gestionnaire de périphériques peut se connecter à distance à un ordinateur afin de visualiser sa configuration matérielle, mais ne peut pas la modifier.

Une autre méthode de gestion des périphériques s'effectue par le biais des paramètres :

Cliquez sur le menu **Démarrer** puis choisissez **Paramètres** et **Bluetooth et appareils**.

Paramètres

Yann BARDET
ybardot@yahoo.fr

Rechercher un paramètre

- Système
- Bluetooth et appareils**
- Réseau et Internet
- Personnalisation
- Applications
- Comptes
- Heure et langue
- Jeux
- Accessibilité
- Confidentialité et sécurité
- Windows Update

Bluetooth et appareils

Ajouter l'appareil

Afficher d'autres périphériques

Bluetooth
Le Bluetooth est désactivé

Appareils
Souris, clavier, stylet, audio, écrans et stations d'accueil, autres appareils [Ajouter un appareil](#)

Imprimantes et scanners
Préférences et résolution des problèmes

Cliquez sur **Ajouter l'appareil** et sélectionnez le type d'appareil parmi **Bluetooth**, **Ecran ou station d'accueil sans fil**, ou **Tout le reste**.

59pbh
42693c4b0000
0008 ZEDIA Jean Mar
X

Ajouter un appareil

Choisissez le type d'appareil que vous voulez ajouter.

- Bluetooth
Souris, claviers, stylos, périphériques audio, contrôleurs, etc.

- Écran ou station d'accueil sans fil
Moniteurs sans fil, téléviseurs ou PC qui utilisent Miracast ou des docks sans fil

- Tout le reste
Manettes Xbox avec adaptateur sans fil Xbox, DLNA, et autres appareils

Annuler

Cependant, pour ajouter une imprimante ou un scanner, ne choisissez pas ce menu. Cliquez sur **Imprimantes et scanners**, puis le menu de gauche **Ajouter un appareil**.

Résumé du chapitre

- Windows 11 offre différents outils permettant de gérer les disques de l'ordinateur avec les données qu'ils contiennent, et facilitant l'utilisation de périphériques.
- Windows 11 peut uniquement être installé sur un disque GPT.
- La console Gestion des disques permet d'effectuer les actions courantes sur les disques : initialisation des disques, conversion et création des volumes ou du style de partition. Diskpart et le langage PowerShell sont des compléments en ligne de commande.
- La commande Chkdsk est améliorée : en mode hors connexion, le temps nécessaire au dépannage d'un disque dur est désormais proportionnel au nombre d'endommagements et non plus au nombre de fichiers présents.
- La fonctionnalité Espaces de stockage réunit les disques internes et externes de l'utilisateur dans une réserve (ou pool) de stockage unique, scindée en un ou plusieurs disques virtuels, permettant d'offrir une protection contre un disque défaillant ou d'ajouter de l'espace disque supplémentaire en cas de capacité insuffisante.
- Les autorisations NTFS protègent les données contre les accès non autorisés effectués localement et depuis le réseau, en conjonction de celles du partage.
- OneDrive est le service de cloud computing proposé par Microsoft qui permet de stocker ses données personnelles gratuitement dans un espace de 5 Go. Cette application constitue désormais une fonctionnalité complètement intégrée à Windows 11.
- Des outils offrent des fonctions d'optimisation des performances d'un disque : quota, compression ou défragmentation.
- Concernant les pilotes de périphériques, Windows 11 propose la commande sigverif afin de visualiser les pilotes non signés sur un ordinateur.
- Le magasin central de pilotes est le référentiel des pilotes approuvés pour l'installation sur un ordinateur.

Gestion des clients Windows

Accès à distance

La gestion à distance des clients Windows 11 est une tâche majeure pour tout administrateur d'entreprise, car elle contribue à la disponibilité du système d'information.

Le poste de travail est au cœur du fonctionnement de l'entreprise, le service de support aux utilisateurs doit donc être efficace et réactif. L'évolution du parc est prise en compte par les directions informatiques qui doivent maîtriser les coûts des environnements de travail utilisateur.

Le cycle de vie d'un système d'exploitation pourrait être résumé ainsi : planification, déploiement, utilisation, maintenance et transition.

Windows 11 propose un vaste panel de fonctionnalités pour réaliser ces tâches, au travers par exemple de la virtualisation des postes, du dépannage à distance ou d'outils de centralisation comme la console de gestion **MMC** (*Microsoft Management Console*).

1. Microsoft Management Console

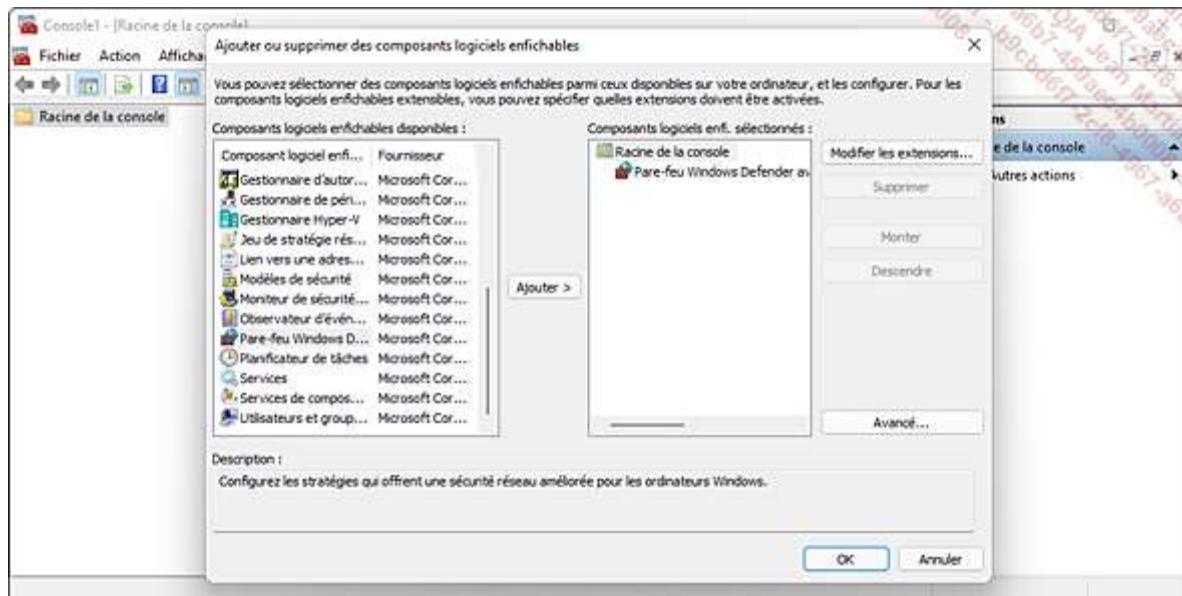
La console MMC fournit des outils d'administration afin de gérer des composants réseau (DHCP, DNS), des ordinateurs (comptes, sessions) ou des services (NAP, BITS), localement et à distance.

La console est accessible en exécutant la commande mmc.exe depuis une fenêtre Windows PowerShell. Chaque composant à administrer doit être ajouté manuellement à la console, leur appellation est **composant logiciel enfichable**.

Pour ajouter ou supprimer un composant logiciel enfichable, voici la procédure :

Pressez les touches  + R, et saisissez mmc dans la fenêtre **Exécuter**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

Cliquez sur le menu **Fichier**, puis **Ajouter/Supprimer un composant logiciel enfichable**. Sélectionnez-le ou les (mais à la suite) composants logiciels enfichables disponibles et cliquez sur le bouton **Ajouter**. Par exemple, pour configurer le pare-feu d'un ordinateur distant, sélectionnez **Pare-feu Windows avec fonctionnalités avancées**. Si une boîte de dialogue apparaît (voir image ci-après) vous invitant à sélectionner quel ordinateur local ou distant le composant devra gérer, sélectionnez l'option adéquate et validez par le bouton **Terminer**.

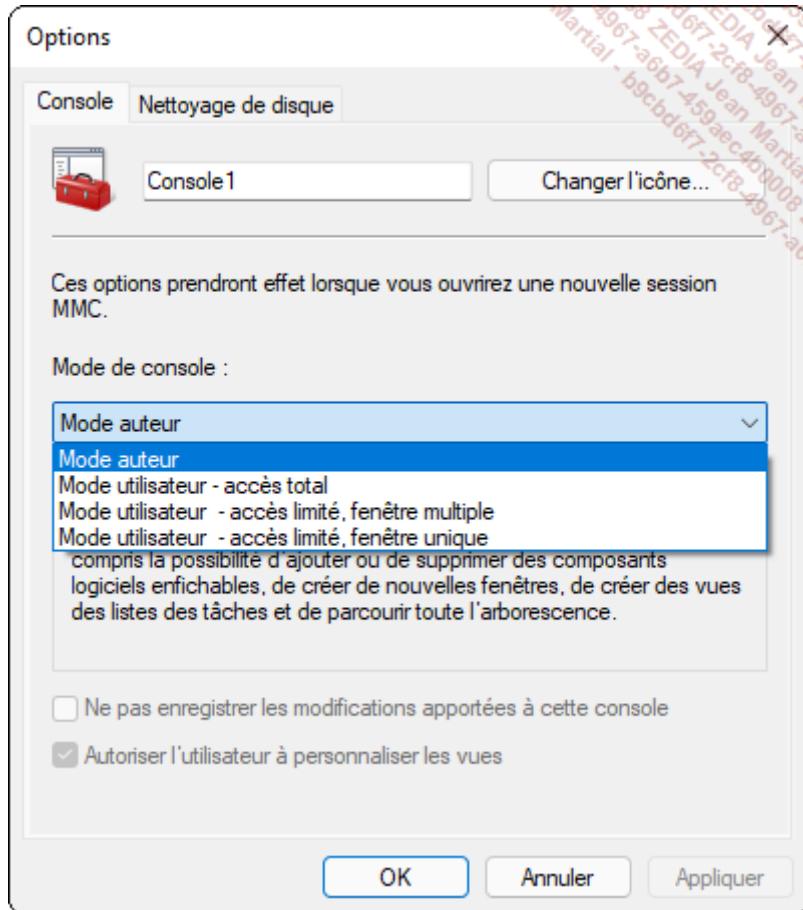


67 Tous les composants logiciels enfichables ne permettent pas d'administrer des ordinateurs à distance, comme **Modèles de sécurité**.

Pour supprimer un composant logiciel enfichable, sélectionnez-le dans **Composants logiciels enfichables sélectionnés**, puis cliquez sur le bouton **Supprimer**.

Vous pouvez, après avoir constitué la liste des composants logiciels enfichables, sauvegarder dans un dossier partagé (ou un périphérique amovible) la console dans un fichier portant l'extension .msc, et ainsi la réutiliser pour administrer d'autres clients Windows 11 ou serveurs de votre réseau d'entreprise.

Dans le menu **Fichier - Options**, l'administrateur peut restreindre l'accès aux composants logiciels enfichables en sélectionnant un **Mode de console** :



Quatre modes sont à votre disposition :

- **Mode auteur** : accès à toutes les fonctionnalités de la console, y compris l'ajout ou la suppression de composants logiciels enfichables.
- **Mode utilisateur - accès total** : visualisation complète de l'arborescence sans possibilité d'ajouter ou supprimer des composants.
- **Mode utilisateur - accès limité, fenêtre multiple** : les zones de l'arborescence non visibles dans l'interface de composants logiciels enfichables ne seront pas accessibles.
- **Mode utilisateur - accès limité, fenêtre unique** : la console est exécutée dans une seule fenêtre, l'utilisateur ne peut accéder aux zones non visibles de celle-ci.

Comme les consoles enregistrées dans le profil de l'utilisateur utilisent de l'espace disque, l'onglet **Nettoyage de disque** permet de supprimer les fichiers contenant les modifications d'affichage d'un fichier console.

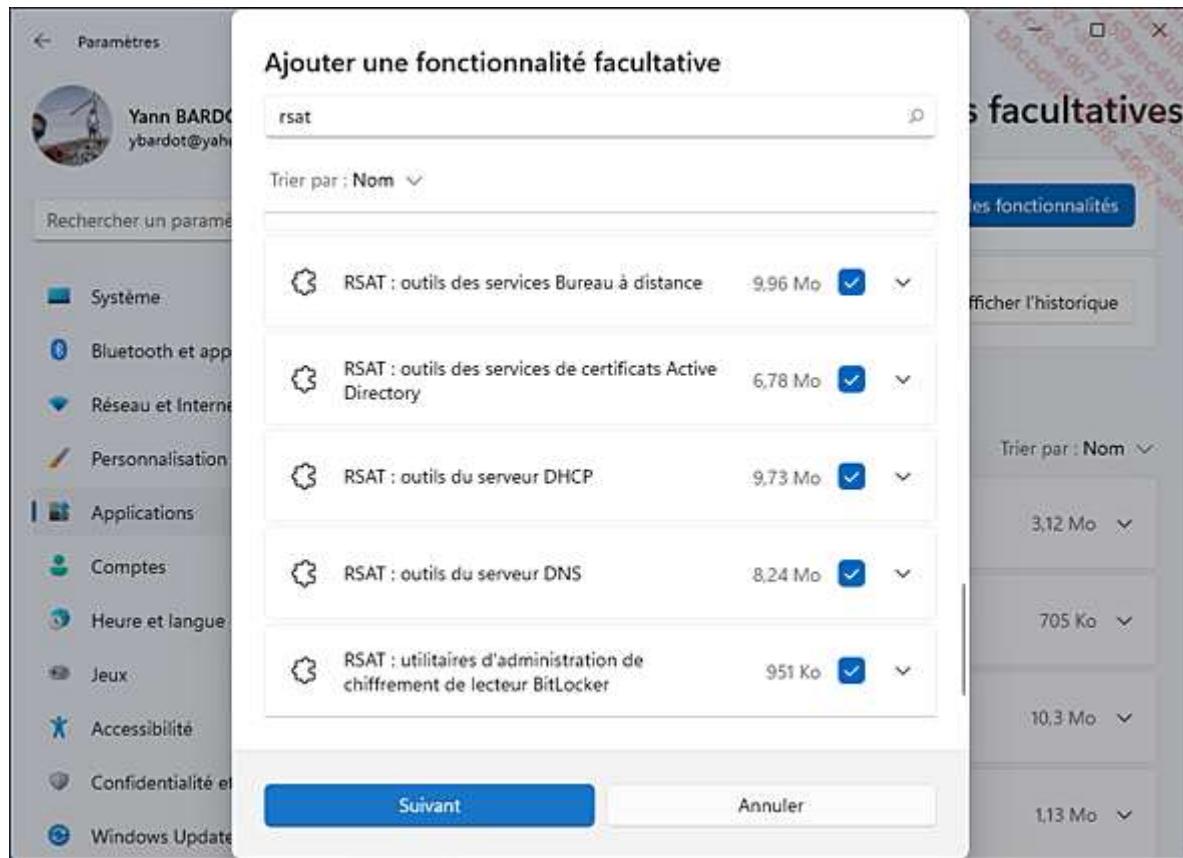
Un administrateur doit pouvoir accéder à toutes les fonctionnalités et tous les rôles des serveurs de son entreprise, tels que Windows Server 2019 par exemple, et ce où qu'il soit, le but étant de dépanner ou de configurer les services critiques, tels que Active Directory et DNS. Nous avons étudié précédemment que la console MMC permettait d'ajouter des composants à administrer, mais l'outil est limité : il ne permet d'ajouter que les composants logiciels enfichables pouvant être administrés sur le poste Windows 11 local, non ceux d'un serveur distant.

Pour pallier cette lacune, Microsoft propose aux administrateurs de télécharger gratuitement les composants logiciels enfichables correspondant aux rôles et fonctionnalités d'un serveur Windows, à l'adresse suivante : <https://www.microsoft.com/fr-FR/download/details.aspx?id=45520>

De plus, depuis Windows 10 version 1809 (octobre 2018), les outils RSAT sont disponibles en tant que fonctionnalités optionnelles. Voici comment les installer sur un poste Windows 11 :

Ouvrez **Paramètres**, **Applications** et cliquez sur **Fonctionnalités facultatives**.

Dans la section **Ajouter une fonctionnalité facultative**, cliquez sur le bouton **Afficher les fonctionnalités**. Saisissez les premières lettres de la fonctionnalité que vous recherchez (dans l'exemple rsat), sélectionnez la ou les fonctionnalités à ajouter puis cliquez sur le bouton **Suivant** :



Cliquez sur **Installer**.

En matière de sécurité, il est préférable d'éviter d'ouvrir une session à distance sur un serveur pour l'administrer, mais plutôt de privilégier l'utilisation d'une méthode sécurisée, au travers des outils RSAT.

En effet, les communications sont sécurisées par défaut : seuls les ports et les exceptions de services requis pour la gestion à distance sont définis dans le pare-feu avec les fonctionnalités avancées de sécurité.

Vous pouvez administrer la version Core (minimale) de Windows Server 2019 depuis les outils RSAT. Après avoir installé ces outils en tant qu'administrateur du poste Windows 11, tous les outils d'administration sont activés, contrairement aux anciennes versions RSAT.

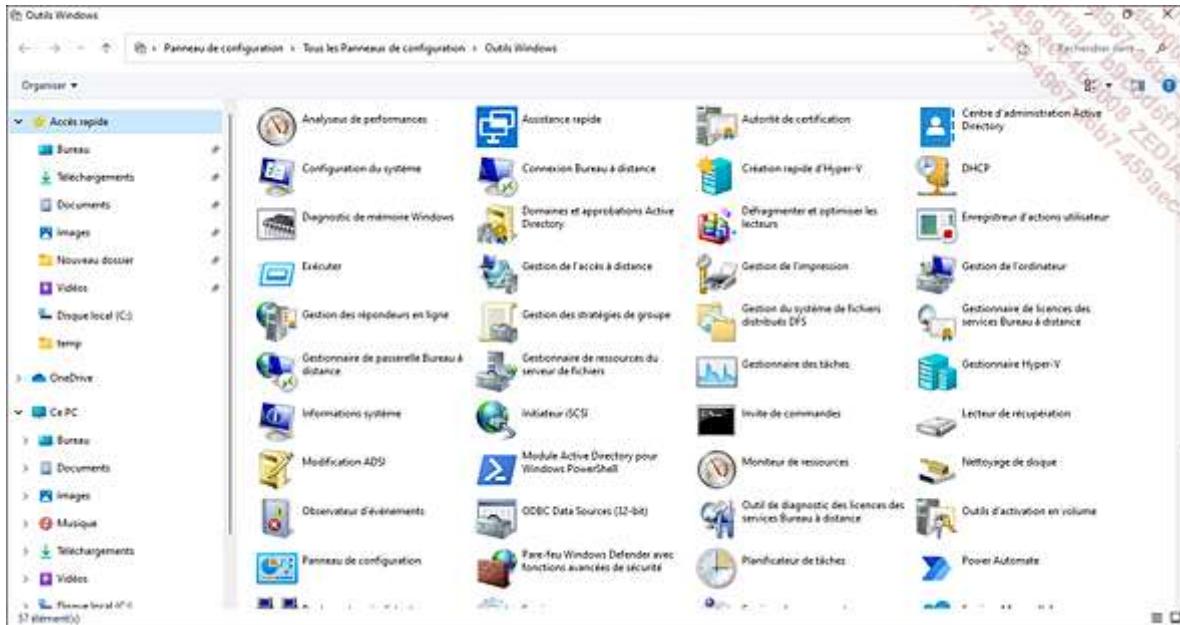
Pour désinstaller un composant RSAT, procédez de même :

Ouvrez **Paramètres**, **Applications** et cliquez sur **Fonctionnalités facultatives**.

Dans la section **Fonctionnalités installées**, saisissez le nom de la fonctionnalité à désinstaller dans le champ de recherche.

Déroulez la fonctionnalité et cliquez sur le bouton **Désinstaller**.

L'accès aux outils d'administration de serveur distant s'effectue via différents biais, notamment en choisissant **Toutes les applications** dans le menu **Démarrer** puis en cliquant sur **Outils Windows**. Le panneau de configuration s'ouvre alors :



68 Les outils RSAT ne peuvent administrer que des ressources distantes.

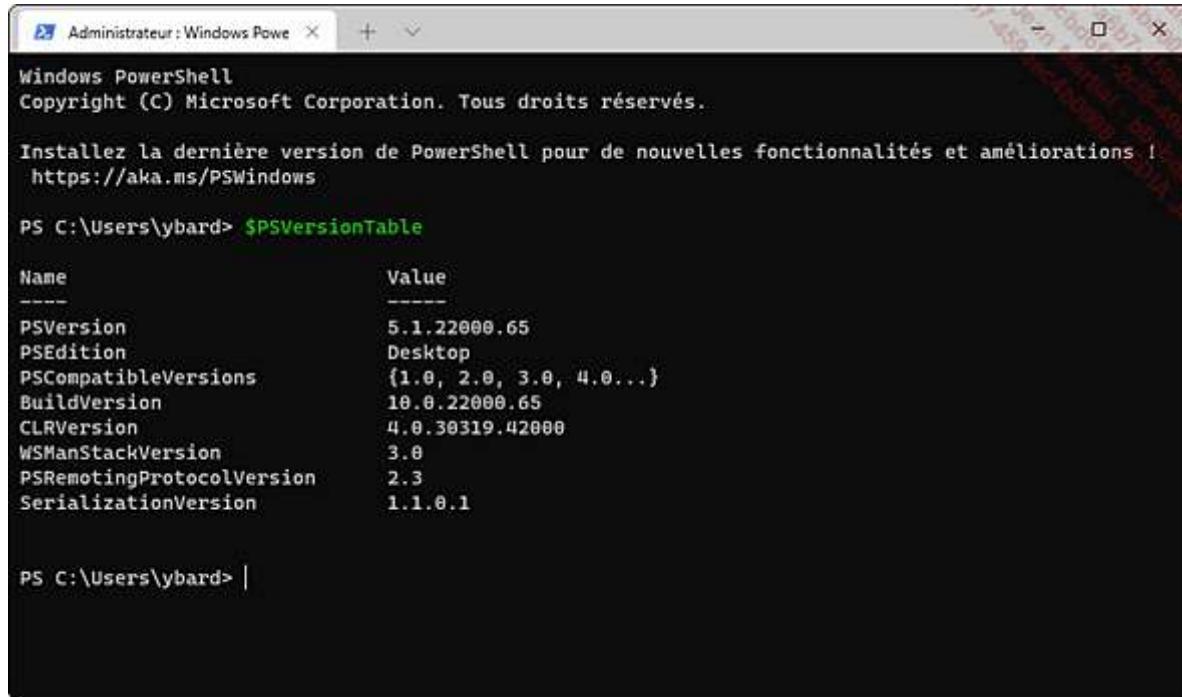
Quand des outils d'administration RSAT installent les consoles de gestion des rôles et des fonctionnalités, ils installent également les commandes PowerShell permettant de les administrer. La commande Get-Command -Module NOMMODULE (par exemple RemoteAccess pour Remote Desktop Services) permet de lister ces nouvelles commandes.

Désormais, l'administration des rôles et des fonctionnalités, tels que DHCP, les services Active Directory ou encore l'équilibrage de la charge, est grandement facilitée depuis un ordinateur équipé de Windows 11 Entreprise ou Windows 11 Professionnel.

3. Windows PowerShell

PowerShell version 5.1 combine un langage de script et un interpréteur de ligne de commande permettant de gérer et automatiser les actions d'administration sur les systèmes Microsoft. Le langage est inclus dans Windows 11 et est exécutable sur des ordinateurs distants en arrière-plan. Les applets de commande permettent de gérer efficacement le registre, les processus, les journaux, etc.

Pour connaître la version de Windows PowerShell installée sur votre ordinateur, saisissez simplement \$PSversionTable dans une fenêtre Windows PowerShell ( + X, puis **Terminal Windows**).



```
Administrator : 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:\Users\ybard> $PSVersionTable

Name                           Value
----                           ---
PSVersion                      5.1.22000.65
PSEdition                      Desktop
PSCompatibleVersions              {1.0, 2.0, 3.0, 4.0...}
BuildVersion                     10.0.22000.65
CLRVersion                       4.0.30319.42000
WSManStackVersion                 3.0
PSRemotingProtocolVersion        2.3
SerializationVersion               1.1.0.1

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

L'édition installée par défaut avec Windows 11 se nomme Desktop. Une édition Core est développée en parallèle et la remplacera à terme. À l'heure où cet ouvrage est rédigé, la version 7.1.3 de PowerShell Core est disponible, c'est elle qui est mentionnée dans le message d'ouverture du Terminal (« Installez la dernière version de PowerShell... »). Pour des raisons de simplicité, nous utiliserons la version fournie par défaut avec le système d'exploitation, la version Desktop 5.1.

Windows PowerShell, qui nécessite .NET Framework 5.0, propose également un environnement graphique (*PowerShell Integrated Scripting Environment* ou ISE) incluant un débogueur. Il permet l'exécution de scripts planifiés, l'exécution sélective de code et la modification multiligne.

Concrètement, l'administrateur peut ainsi gérer grâce à des commandes un domaine Active Directory, incluant la sauvegarde, les services d'accès distants, mais aussi des ordinateurs membres d'un groupe de travail (base de registre, système de fichiers, etc.) et des fonctionnalités telles qu'Hyper-V ou BitLocker.

La version de Windows PowerShell livrée avec Windows 11 supporte toujours les améliorations apportées avec Windows 10 :

- **Gestion des raccourcis-clavier** : les fonctions copier ([Ctrl] + C), coller ([Ctrl] + V) ou tout sélectionner ([Ctrl] + A) sont supportées.
- **Gestion des liens symboliques** : la création ou suppression des raccourcis symboliques est possible via la commande New-Item.
- **Journal dédié dans l'Observateur d'événements** : le journal **Windows PowerShell** est disponible depuis le nœud **Journaux des applications et des services**.
- **Commande PSEdit** : il est désormais possible d'éditer des fichiers à distance via une session PowerShell.
- **OneGet** : permet d'importer des packages tiers pour mieux gérer les applicatifs et le système d'exploitation.
- **PowerShellGet** : import via Internet de nouveaux modules PowerShell.
- **Gestion des archives** : gestion des archives comme ZIP via les commandes compress-archive ou expand-archive.

Avec Windows 11, Microsoft supporte la fonctionnalité, nommée *Windows PowerShell Desired State Configuration* (DSC). L'administrateur peut désormais gérer le déploiement et la configuration de plusieurs environnements de manière automatisée :

- Activation ou désactivation de rôles ou services.
- Gestion des paramètres de la base de registre.
- Gestion des fichiers et répertoires.
- Démarrage, arrêt de services ou processus.
- Déploiement de logiciels.
- Gestion des groupes et des utilisateurs.

DSC procure donc de nouvelles commandes et ressources Windows PowerShell.

Les applets de commande Windows PowerShell ont une syntaxe précise : un verbe puis un nom, séparés par un tiret (-).

Le langage permet d'imbriquer des applets entre eux pour réaliser une série d'actions, en les séparant par un *pipe* ("|"). Des conditions peuvent aussi être créées.

L'administrateur utilise souvent les verbes *Get* (obtenir), *Set* (fixer) ou *Format* lors de l'exécution de commandes.

Windows PowerShell gère la définition de variables, qu'il suffit de déclarer en les précédant du caractère "\$" et d'instancier le signe avec "=".

Exemple avec la commande :

```
$d=get-process | where-object {$_.WorkingSet -gt 5000000}
```

Elle enregistre dans la variable "d" les processus locaux dont la plage de travail est supérieure à 5 Mo. Pour afficher la valeur de la variable, donc le résultat, il suffit ensuite de taper :

```
echo $d
```

ou simplement :

```
$d
```

The screenshot shows a Windows PowerShell window titled "Administrateur : Windows Powe". The command entered was:

```
PS C:\Users\ybard> $d=Get-Process | Where-Object {$_.WorkingSet -gt 5000000}
PS C:\Users\ybard> echo $d
```

The output displays a table of processes filtered by a working set greater than 5000000 bytes. The columns are: Handles, NPM(K), PM(K), WS(K), CPU(s), Id, SI, and ProcessName. The table includes entries for AggregatorHost, ApplicationFrameHost, BtwRSupportService, conhost, Cortana, csrss, ctfmon, dasHost, dllhost, and several instances of dwm, explorer, FileCoAuth, fontdrvhost, GameBarFTServer, and gamingservices.

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
88	6	1864	5848	0,06	5572	0	AggregatorHost
574	33	23196	50344	13,66	376	1	ApplicationFrameHost
158	11	1828	8980	0,09	4840	0	BtwRSupportService
177	12	6176	16508	0,13	4788	1	conhost
687	50	30312	72608	10,84	1564	1	Cortana
588	26	1996	5648	3,16	716	0	csrss
582	24	2552	6312	12,45	804	1	csrss
574	20	21716	43656	21,70	6624	1	ctfmon
512	24	8596	24776	2,59	4200	0	dasHost
126	9	1472	8484	0,03	8660	0	dasHost
135	9	1600	9240	0,22	4556	1	dllhost
295	26	7828	18176	2,47	4668	1	dllhost
184	11	2304	15020	0,41	10984	1	dllhost
1412	93	114596	145456	1 282,52	1352	1	dwm
6583	814	235640	357812	427,34	7428	1	explorer
433	19	6480	29416	3,61	8608	1	FileCoAuth
33	10	4228	10744	1,86	936	1	fontdrvhost
257	13	2824	14516	0,17	11380	1	GameBarFTServer
529	23	7272	30832	5,02	5236	0	gamingservices

Pour accéder au fichier d'aide d'un applet, utilisez la commande :

get-help

suivie du nom de l'applet.

Pour connaître la liste des applets, utilisez la commande :

get-command

L'interpréteur de ligne de commande Windows PowerShell est accessible dans Windows 11 depuis le bureau :

Cliquez avec le bouton droit sur **Démarrer** puis choisissez **Terminal Windows (administrateur)**. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

L'invite de commandes Windows PowerShell exécute par défaut les commandes mais pas les scripts (extension .ps1) : c'est le mode **Restricted**. Pour connaître le mode courant, saisissez la commande :

get-executionpolicy

Trois autres modes d'exécution des scripts sont proposés :

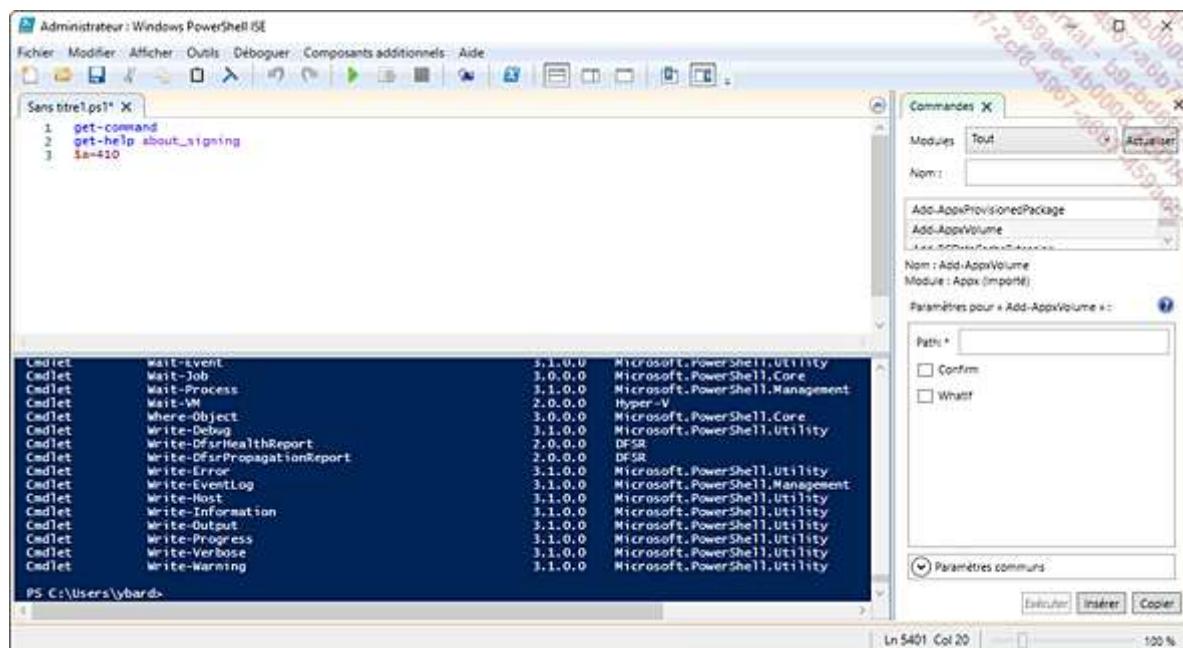
- **AllSigned** : les scripts signés par un fournisseur approuvé sont exécutés.
- **RemoteSigned** : exécution possible d'un script créé par l'administrateur mais pas d'un script non signé en provenance d'Internet.
- **Bypass** : tous les scripts signés et non signés seront exécutés, quelle que soit leur provenance.

Pour définir le mode d'exécution des scripts à **RemoteSigned**, saisissez la commande suivante dans une invite de commandes Windows PowerShell exécutée avec des priviléges administrateur :

set-executionpolicy remotesigned

Windows PowerShell propose une interface graphique nommée Windows PowerShell ISE disponible en tapant la commande powershell_ise.exe depuis une fenêtre PowerShell ou une invite de commandes.

Il y est ainsi possible d'exécuter un script ligne par ligne, de définir des points d'arrêt et de visualiser le résultat directement dans une fenêtre. Le script généré peut être enregistré avec l'extension .ps1. L'interface ISE comprend trois volets au sein d'un onglet représentant le script courant : le volet de commandes situé en haut, le volet de sortie en bas et le volet d'exécution des modules additionnels sur la droite. L'administrateur est aidé dans la saisie des commandes par une méthode de complétion.



Concernant l'exécution de scripts sur des machines distantes, Windows PowerShell nécessite le protocole WinRM (*Windows Remote Management*) et .NET Framework 5.0, tous deux installés sur l'ordinateur source et les ordinateurs de destination.

Windows 11 n'active pas par défaut l'exécution de scripts distants, contrairement à Windows Server 2019.

Pour l'activer, depuis une fenêtre Windows PowerShell exécutée en tant qu'administrateur, suivez la procédure :

Démarrez le service WinRM en tapant : start-service WinRM

Activez l'exécution de scripts à distance : enable-psremoting -force

Notez que la commande winrs permet d'exécuter une commande sur un poste distant, en affichant le résultat sur l'ordinateur local.

69 Pour que l'activation de l'exécution des scripts soit opérationnelle, il ne faut pas qu'une carte réseau de l'ordinateur soit définie dans le profil Public.

Trois modes de communication sont proposés :

- **Communication directe** : permet d'exécuter un script sur un ordinateur précis.
- **Communication à distribution ramifiée** : établit une communication vers plusieurs ordinateurs puis exécute des commandes dont le résultat sera affiché sur l'ordinateur source.
- **Communication "plusieurs à un"** : plusieurs administrateurs créent des connexions avec des priviléges différents vers un ordinateur unique.

Lors de la création d'une connexion, celle-ci peut être temporaire ou permanente.

Une connexion temporaire est fermée lorsque l'exécution de la commande sur l'ordinateur distant se termine.
L'administrateur utilisera l'applet de commande : invoke-command

en spécifiant le ou les noms DNS ou NetBIOS des ordinateurs distants.

Une connexion permanente s'initie au moyen de l'applet : new-pssession

et s'exploite à l'aide de la commande : enter-pssession

La déconnexion d'une session active s'effectue grâce à : disconnect-pssession

La liste des sessions persistantes s'affiche avec la commande : get-pssession

70 Vous pouvez utiliser le paramètre UseSSL pour chiffrer les communications lors de l'utilisation des applets de commande invoke-command, new-pssession et enter-pssession.

La commande est exécutée sur l'ordinateur distant, son résultat est affiché sur l'ordinateur local.

Dans un domaine Active Directory, les scripts Windows PowerShell peuvent aussi effectuer un grand nombre d'opérations sur les objets de stratégie de groupe, comme les lier à des UO (Unité d'Organisation), les modifier ou les supprimer, définir des autorisations, etc., en important le module groupolicy comme suit :

import-module groupolicy

Pour connaître la liste des commandes Windows PowerShell liées aux stratégies de groupe, utilisez la commande :

get-help groupolicy

Les commandes courantes d'administration dans une invite de commandes "cmd" fonctionnent mais ont également leur équivalent en langage PowerShell, par exemple :

Invite de commandes	PowerShell
Ipconfig	Get-NetIPConfiguration

Invite de commandes	PowerShell	Visualiser
Net Start	Start-Service	
Shutdown	Restart-Computer	

l'historique des trente dernières commandes tapées est simple, il suffit d'utiliser la commande :

history

ou de presser la touche [F7] du clavier.

```

Administrator : Windows PowerShell
PS C:\Windows\system32> history

Id CommandLine
-- -----
1 Get-ExecutionPolicy
2 start-service WinRM
3 enable-psremoting -force
4 Get-ExecutionPolicy
5 enable-psremoting -force
6 Get-ExecutionPolicy
7 start-service WinRM
8 set-executionpolicy remotesigned

PS C:\Windows\system32>

```

Invoquer une commande avec un ID spécifique s'effectue via la commande : invoke-history ID

4. Dépannage à distance

Un administrateur a souvent besoin de se déplacer physiquement face à un serveur, afin de le configurer et d'en assurer la disponibilité. Le Bureau à distance permet de s'affranchir de cette distance en permettant une connexion par le réseau. Mais un utilisateur peut aussi demander de l'aide, en lançant un appel d'**Assistance à distance** ou d'**Assistance rapide** : dans un cas, c'est l'administrateur qui se connecte de son propre chef à une ressource (Bureau à distance), dans l'autre cas, il y est invité (Assistance à distance).

a. Bureau à distance

Le Bureau à distance connecte deux ordinateurs, un client et un serveur, sur un réseau ou depuis Internet au travers, par exemple, d'une connexion VPN. Lorsque l'administrateur est connecté, il visualise le bureau de l'ordinateur distant comme s'il était assis devant, en ayant accès à tous les programmes et documents stockés, ainsi qu'aux périphériques connectés.

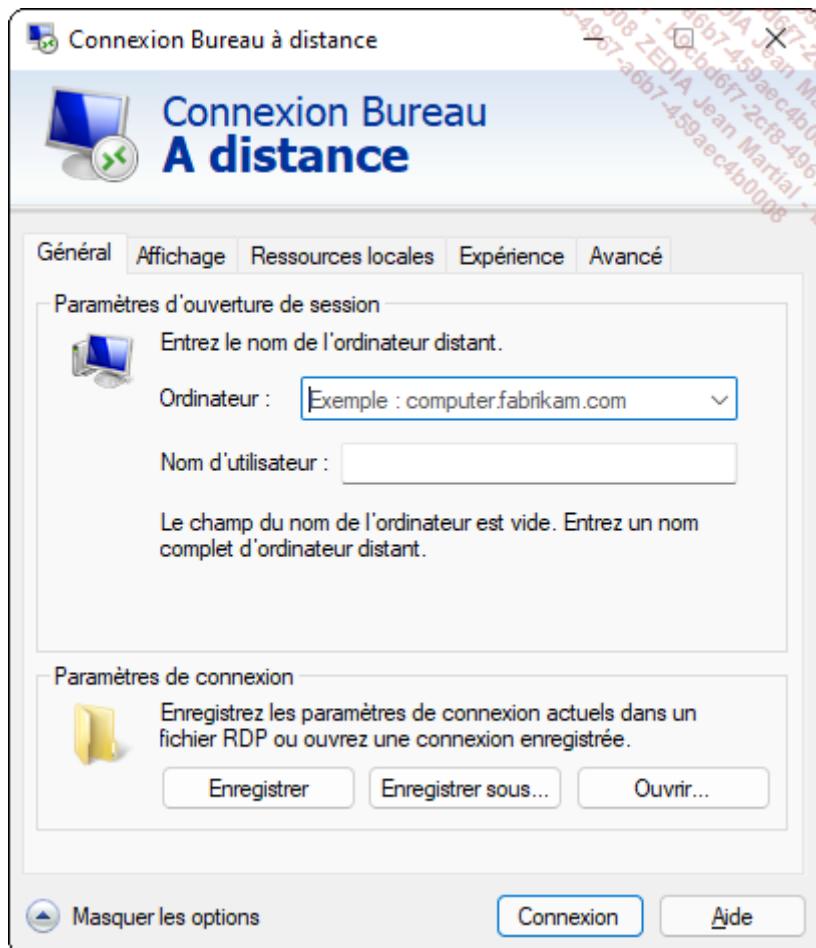
La fonctionnalité Bureau à distance est basée sur une architecture client/serveur :

- Le serveur : permettre une connexion à un ordinateur au travers de la méthode de Bureau à distance implique l'ouverture du port TCP 3389 entrant et donc la possibilité offerte à un attaquant de se connecter à distance sur un poste du réseau de l'entreprise. Il convient donc d'être prudent lors de l'activation de cette fonctionnalité et de bien mesurer ses conséquences en matière de sécurité.
- Le client : c'est un logiciel fourni avec les quatre éditions de Windows 11, qui permet de se connecter à un serveur ou à un autre poste de travail Microsoft Windows, depuis un réseau (filaire, sans fil, 3G...).

Pour exécuter le client Bureau à distance :

Depuis le champ de recherche situé dans la barre des tâches, saisissez **Connexion bureau à distance**.

Une autre méthode à exécuter depuis le bureau de l'utilisateur : pointez la souris en bas à gauche de l'écran, effectuez un clic avec le bouton droit sur le menu **Démarrer** puis **Exécuter**. Saisissez mstsc puis validez par la touche [Entrée].



71 Notez que le client Bureau à distance permet aussi de se connecter à la technologie Microsoft RDS (*Remote Desktop Services*).

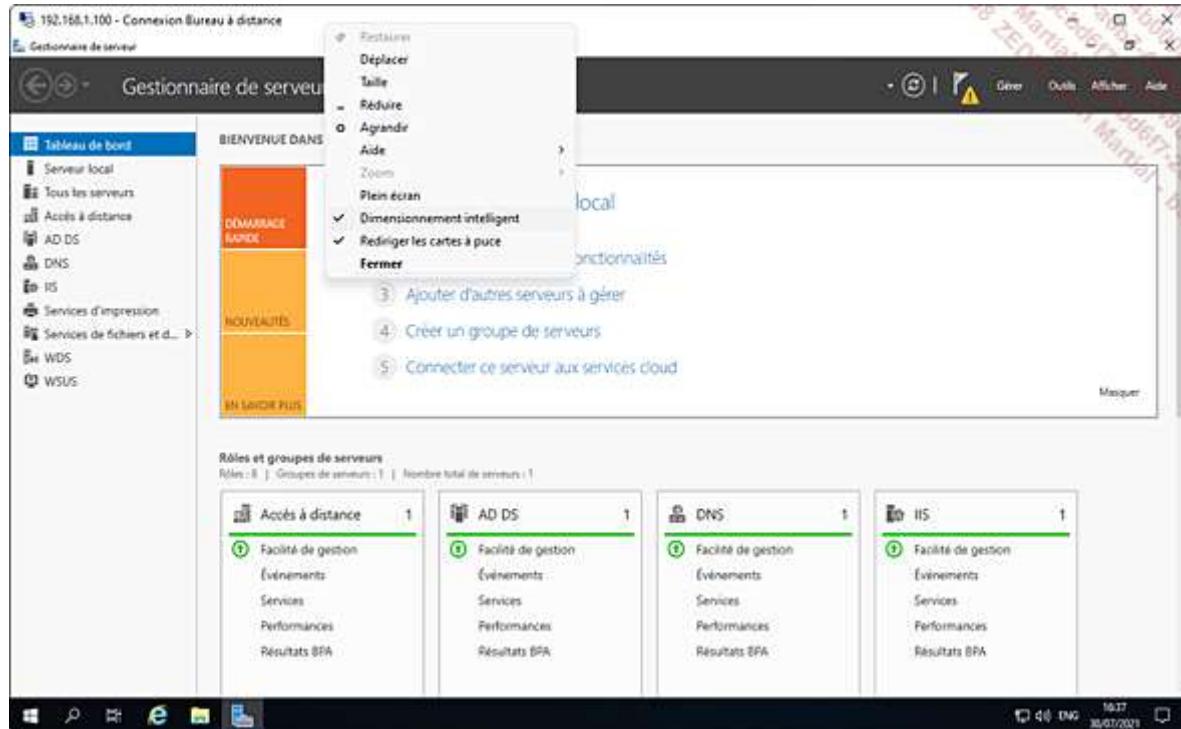
Il est ainsi possible d'afficher le bureau distant de l'ordinateur sur lequel nous sommes connectés, de manière sécurisée au travers du protocole RDP. Les options ci-dessous sont accessibles grâce aux différents onglets du logiciel client, en cliquant sur la flèche pointant vers le bas **Afficher les options** :

- L'onglet **Général** gère les informations d'identification d'ouverture de session (**Nom d'utilisateur** et mot de passe), ainsi que le nom DNS ou l'adresse IP de l'**Ordinateur** distant. L'utilisateur peut enregistrer la configuration des **Paramètres de connexion** dans un fichier portant l'extension .rdp.
- L'onglet **Affichage** permet de définir la résolution du Bureau à distance, ainsi que la qualité des couleurs.
- L'onglet **Ressources locales** offre à l'administrateur la possibilité de configurer la redirection des ressources du poste Windows 11 vers le serveur (son, imprimantes, clavier, caméra, disques locaux...).

72 Avec cette nouvelle version du client Bureau à distance, il est maintenant possible de rediriger un périphérique USB, tel qu'une mémoire flash. Dans l'onglet **Ressources locales**, cliquez sur le bouton **Autres**, développez le nœud **Lecteurs** et si le périphérique USB n'est pas branché, cochez la case **Lecteurs que je branche plus tard**.

- L'onglet **Expérience** permet de définir la bande passante utilisée lors de la connexion Bureau à distance, afin d'optimiser l'affichage des fonctionnalités telles que le lissage des polices, le style visuel...
- L'onglet **Avancé** définit le comportement du client en cas d'échec lors de l'authentification au serveur ou encore les paramètres de connexion via la passerelle Bureau à distance.

Une fois la connexion à l'ordinateur distant initiée, l'utilisateur peut redimensionner automatiquement la fenêtre **Connexion Bureau à distance** en cliquant avec le bouton droit sur le bandeau, puis en sélectionnant **Dimensionnement intelligent**, comme le montre l'image ci-dessous lors de la connexion à une machine virtuelle Windows Server 2019 hébergée dans Microsoft Azure :



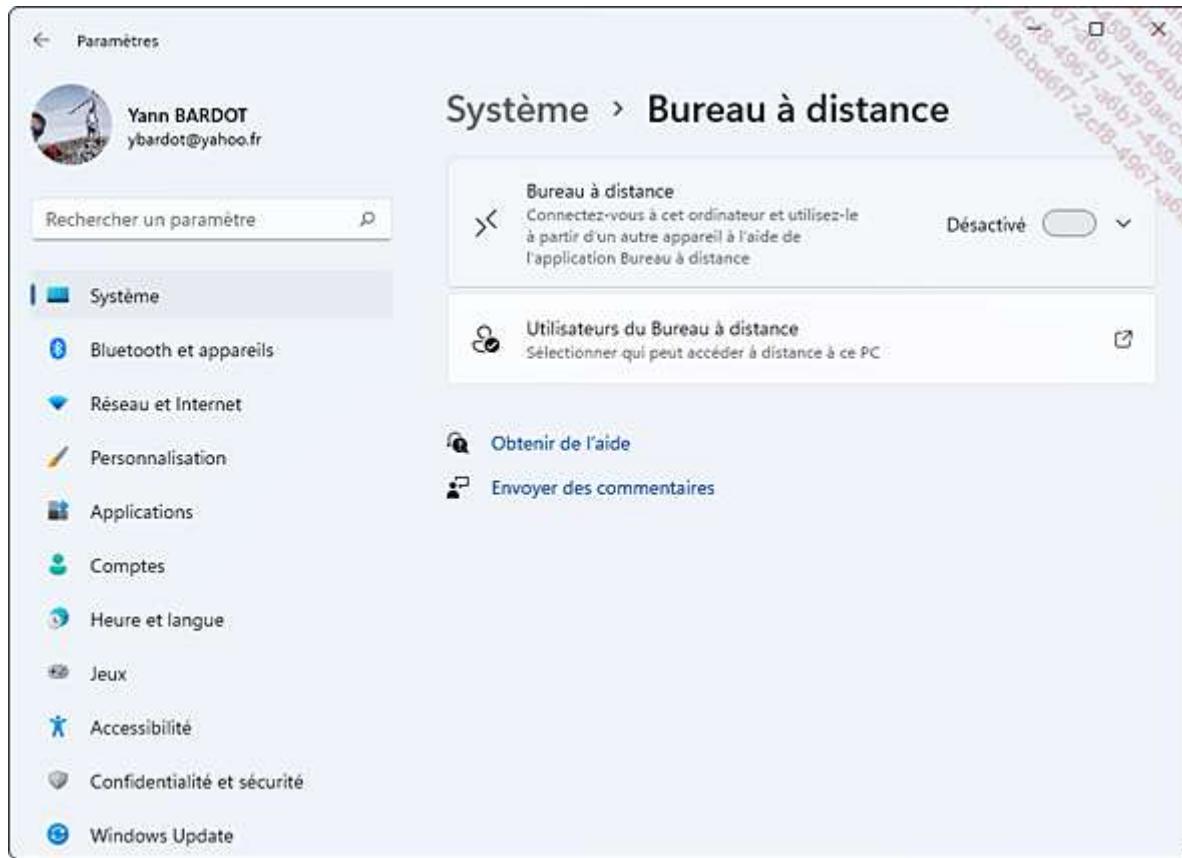
Le Bureau à distance verrouille le système cible, empêchant ainsi temporairement une ouverture de session interactive.

Enfin, le client prend en charge le fractionnement sur plusieurs écrans positionnés horizontalement, dans le but de former un bureau unique de plus grande taille, à l'aide de la commande :

```
mstsc /span
```

Pour activer le Bureau à distance côté serveur, dans notre cas un poste de travail Windows 11, suivez la procédure ci-dessous :

En tant qu'administrateur local, effectuez un clic avec le bouton droit sur le menu **Démarrer** puis cliquez sur **Système**. Cliquez sur **Bureau à distance**, puis sur la ligne **Bureau à distance**, activez la fonction.



Validez le message d'activation en cliquant sur **Confirmer**.

Déroulez le menu **Bureau à distance**. Vérifiez que la case **Exiger que les utilisateurs utilisent l'authentification au niveau du réseau pour se connecter (recommandé)** est bien cochée. Cette authentification au niveau réseau porte aussi le nom de NLA. Le port TCP 3389 sera automatiquement ouvert en flux entrant dans le pare-feu Windows 11, pour les profils Privé et Public de la carte réseau. Pour changer le port d'écoute par défaut et ainsi améliorer la sécurité du serveur, ouvrez la base de registre et modifiez la valeur de la clé PortNumber accessible depuis le nœud : **HKEY_LOCAL_MACHINE - System - CurrentControlSet - Control - TerminalServer - WinStations - RDP-Tcp**

Il est également possible d'activer l'authentification au niveau réseau via une stratégie de groupe. Ouvrez l'éditeur de stratégies et modifiez celle nommée **Requérir l'authentification utilisateur pour les connexions à distance à l'aide de l'authentification au niveau du réseau** en déroulant l'arborescence **Configuration ordinateur - Modèles d'administration - Composants Windows - Services Bureau à distance - Hôte de la session Bureau à distance - Sécurité**.

Cliquez sur **Utilisateurs du Bureau à distance** pour ajouter les comptes des utilisateurs pouvant accéder à distance au serveur RDP de cette machine. Le groupe Administrateurs dispose automatiquement d'un accès.

Notez que seules les éditions Professionnel et Entreprise de Windows 11 supportent l'activation du Bureau à distance en mode serveur.

b. Se connecter au PC distant joint à Azure Active Directory

Azure Active Directory (ou Azure AD) est le service hébergé sur le cloud Microsoft Azure qui gère les identités et les accès via un modèle PaaS (*Platform as a Service*). Azure AD permet à des employés de se connecter et d'accéder aux ressources telles que Microsoft Office 365 ou des applications situées sur un réseau on-premise.

Depuis Windows NT, Microsoft propose la prise en charge des connexions à distance des ordinateurs joints à un domaine Active Directory. Depuis Windows 10 version Creators update, l'administrateur peut se connecter à un ordinateur joint à Azure Active Directory, via le protocole RDP.

73 La connexion à un ordinateur joint à Azure AD n'est possible que si la nouvelle fonctionnalité Remote Credential Guard (cf. chapitre Configuration de la sécurité Windows, section Windows Defender Credential Guard) est désactivée sur le poste distant.

L'activation du Bureau à distance en mode serveur s'effectue de la même façon qu'un poste sur le réseau local. Si l'administrateur ayant procédé à la jonction de l'ordinateur à Azure AD est le seul qui doit se connecter à distance, aucune configuration supplémentaire n'est nécessaire. Sinon, il suffit de spécifier les comptes susceptibles de pouvoir se connecter en les joignant au groupe **Utilisateurs authentifiés** local.

Aucun compte individuel Azure AD ne peut être utilisé pour les connexions à distance.

Trois méthodes d'authentification à distance sont disponibles via cette fonctionnalité :

1. Mot de passe
2. Carte à puce
3. Windows Hello Entreprise (si le domaine Active Directory est géré par System Center Configuration Manager)

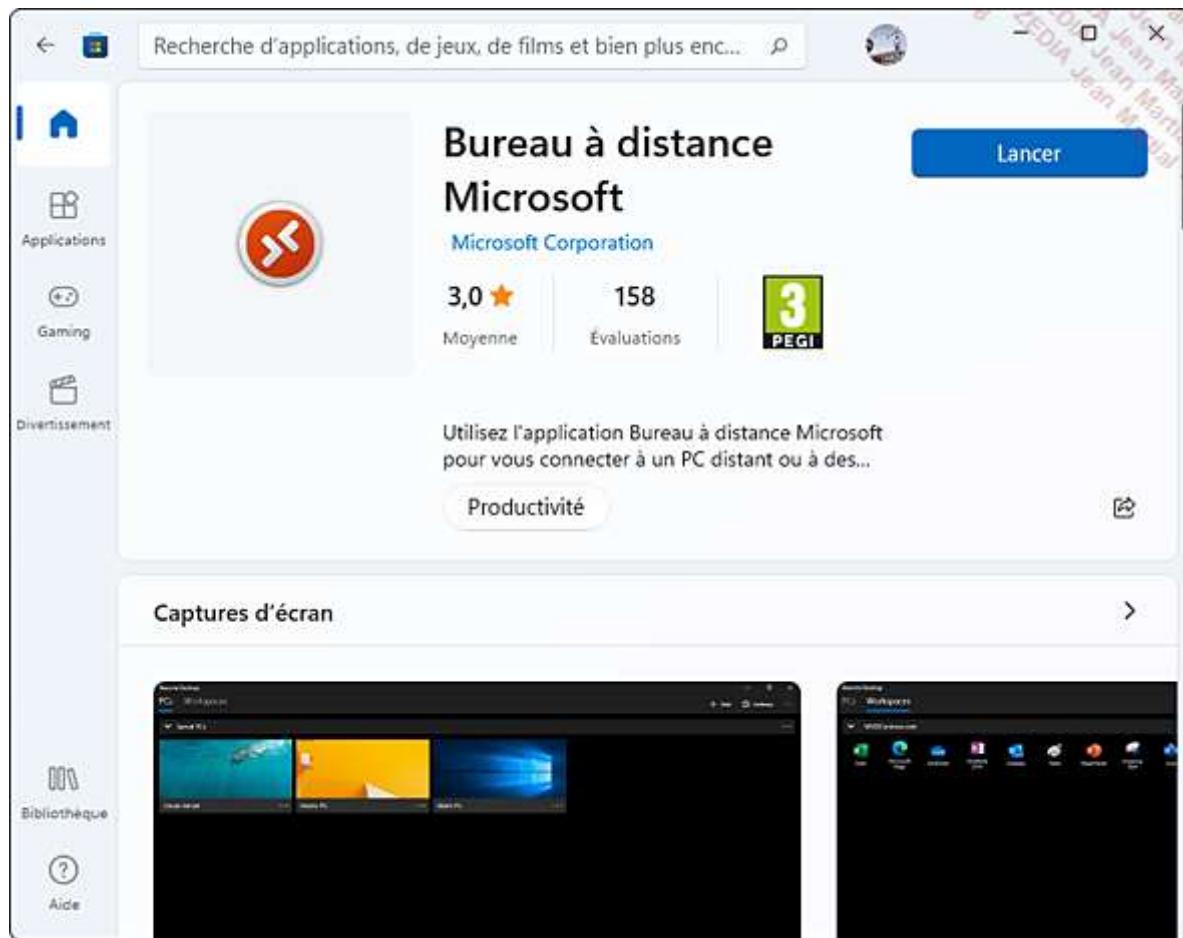
c. Application Bureau à distance du Microsoft Store

Microsoft propose en téléchargement depuis le Microsoft Store l'application gratuite Bureau à distance Microsoft. Le principal avantage est la possibilité de regrouper dans un emplacement centralisé les connexions actives. De plus, la mise à jour se fera de manière automatique et vous permettra de disposer des dernières fonctionnalités.

Grâce au partage d'écran, l'administrateur peut à tout moment surveiller un ordinateur distant tout en continuant ses tâches courantes. Orientée tablette tactile, l'application gère le zoom par écartement des doigts ou le clavier visuel. De nouvelles fonctionnalités sont supportées, offrant une utilisation plus fluide d'une session à distance : RemoteFX Multi-Touch Remoting (gestion des 10 doigts des mains), RemoteFX Multimedia and Sound et RemoteFX EasyPrint (impression simplifiée sur l'hôte distant). Les performances ont été améliorées pour les plateformes 64 bits. Les modes clair et sombre sont pris en charge...

Pour télécharger et installer l'application Bureau à distance :

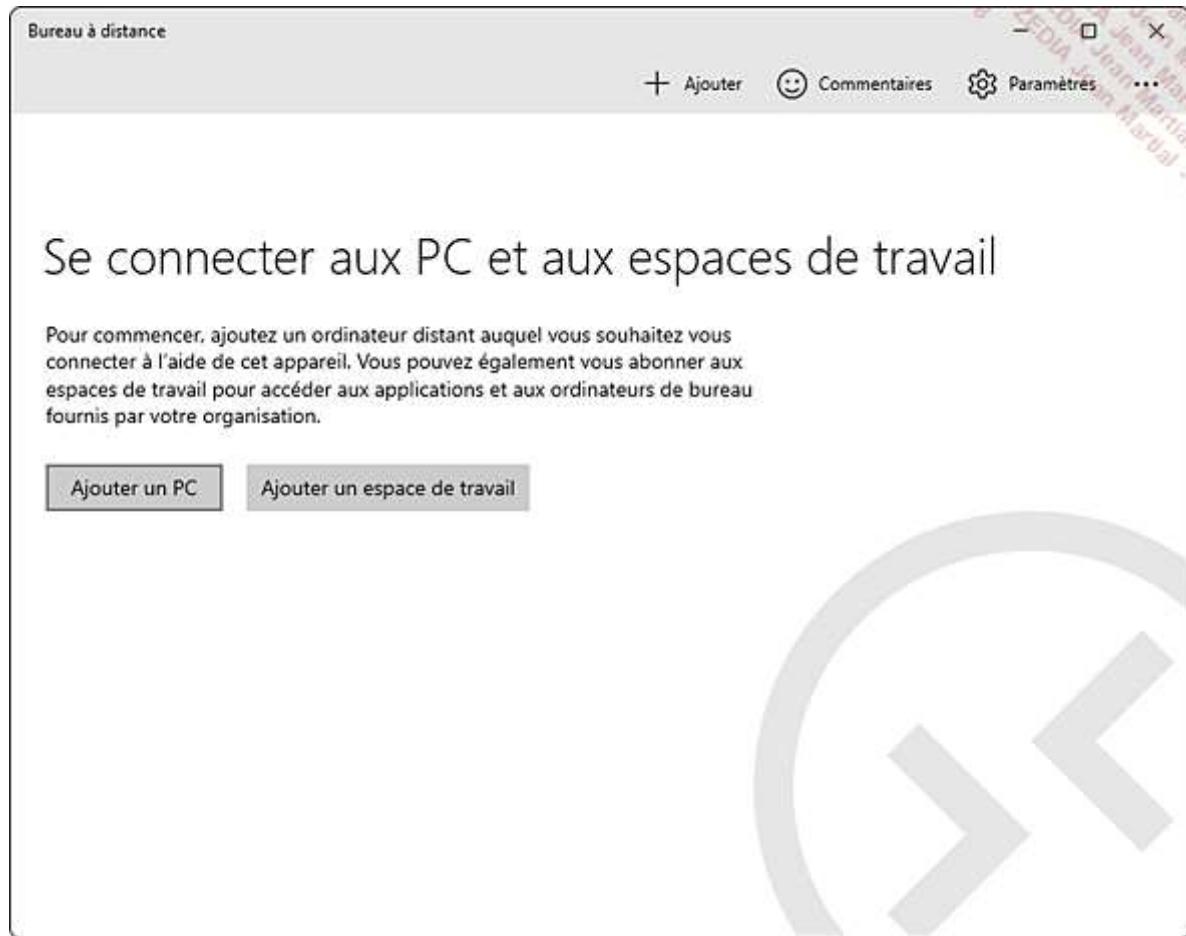
Depuis l'icône du **Microsoft Store** située dans la barre des tâches, saisissez **bureau à distance** dans la zone de recherche prévue à cet effet (en haut) puis validez en pointant sur la loupe. Sélectionnez l'application **Bureau à distance Microsoft** dans les résultats de la recherche puis cliquez sur le bouton **Télécharger**.



Une fois l'application installée, l'icône **Bureau à distance** est disponible depuis le menu **Démarrer**.

Lors de l'exécution de l'application, l'administrateur a plusieurs choix :

- Ajouter une machine à laquelle se connecter.
- Se connecter à l'espace de travail de son entreprise, c'est-à-dire un environnement de travail contenant les applications et ordinateurs fournis par celle-ci.

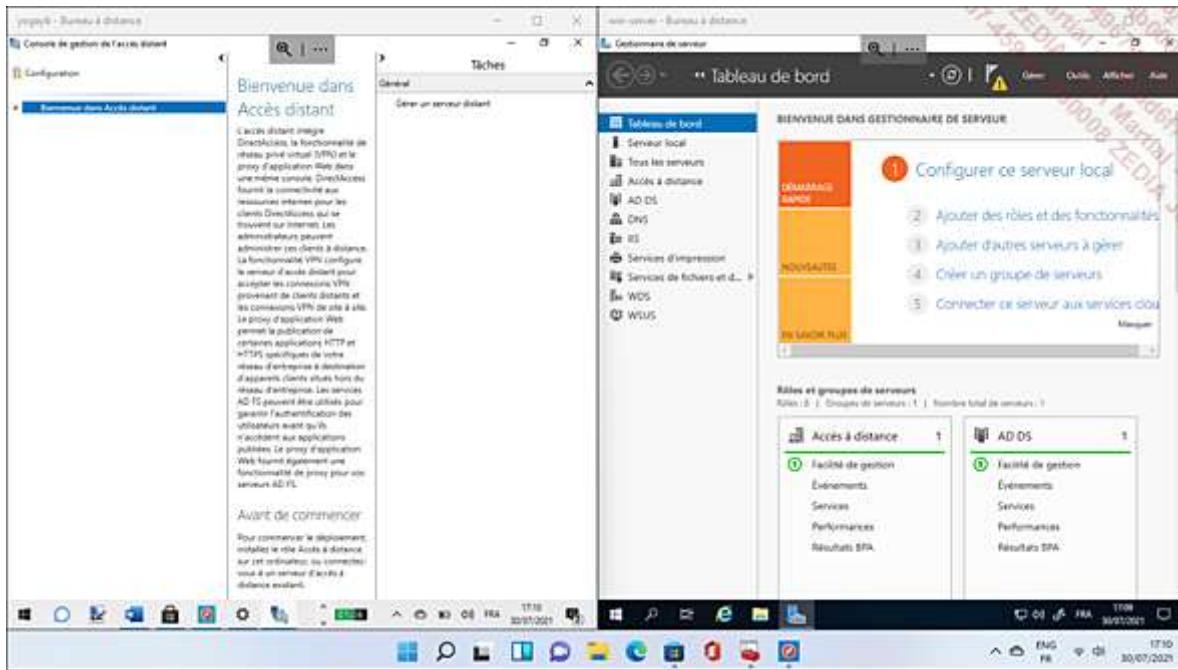


Choisissez la première option en cliquant sur le bouton **Ajouter un PC**. Saisissez le nom de la machine distante ou son adresse IP. Il est également possible de configurer un nom d'utilisateur si vous le souhaitez. Cliquez sur le bouton **Enregistrer**.

Cliquez ensuite sur l'icône représentant la connexion. Un nom d'utilisateur et un mot de passe sont obligatoirement requis. Le nom de domaine est facultatif et peut être défini en respectant la méthode suivante : **NOMDOMAINE\Nom d'utilisateur**. Si l'ordinateur distant fait partie d'un groupe de travail, il faut indiquer **NOM-ORDI\nom d'utilisateur**. L'application tente ensuite d'authentifier l'ordinateur distant.

Si l'authentification de l'ordinateur distant ne fonctionne pas (certificat non approuvé), un message d'avertissement apparaît. Cochez la case **Ne plus redemander pour ce certificat** puis cliquez sur le bouton **Connecter quand même**. La connexion est établie, l'administrateur a désormais un accès complet aux ressources (dossiers, fichiers, imprimantes...) du poste connecté.

Il est possible de positionner l'application Bureau à distance dans une moitié ou un quart de l'écran. Dans notre exemple, l'application Bureau à distance, affichant un poste de travail distant Windows 10, est positionnée à gauche de l'écran, et une autre application Bureau à distance est connectée à un serveur 2019 :



d. RemoteFX

Apparu avec Windows 7 et Windows Server 2008 R2 Service Pack 1, RemoteFX s'appuie sur le protocole RDP (*Remote Desktop Protocol*) pour offrir une expérience utilisateur améliorée dans le cas d'une connexion distante : prise en compte de l'affichage de vidéos, redirection des périphériques (imprimante, caméra) ou écoute de musique.

Grâce à la virtualisation d'un poste de travail, appelé VDI (*Virtual Desktop Infrastructure*) hébergé sur un serveur Hyper-V ou via le service RDS, les ressources matérielles d'accélération graphique de celui-ci seront partagées entre les utilisateurs.

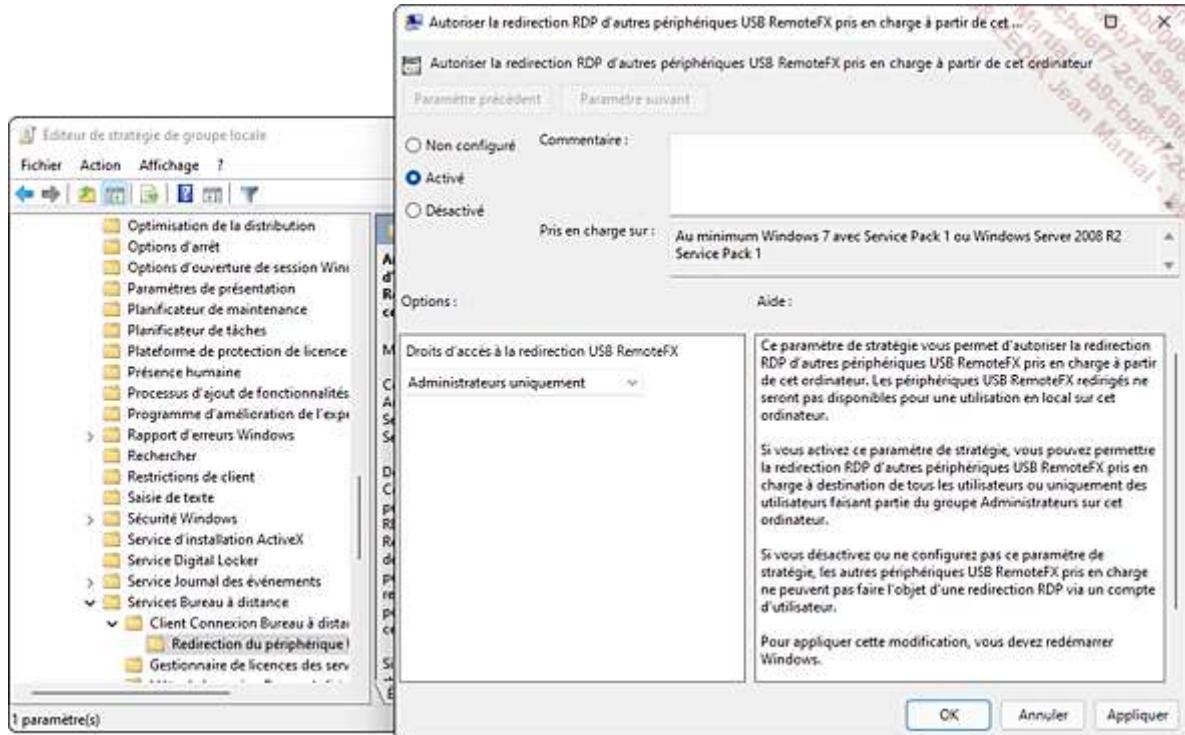
Disponible avec Windows 11 Entreprise, cette technologie peut aussi utiliser le matériel du client pour fournir le contenu multimédia, plutôt que les ressources du serveur distant, réduisant ainsi l'utilisation de la bande passante.

RemoteFX USB Redirection permet à un périphérique USB (scanner, imprimante multifonction...), branché sur un serveur, d'être redirigé sur le poste Windows 11, sans avoir besoin d'installer le pilote adéquat. Pour configurer la prise en charge de cette technologie, il est nécessaire d'utiliser l'Éditeur de stratégie de groupe locale :

Pressez les touches + R du clavier puis saisissez gpedit.msc et validez via le bouton **OK**.

Dans la fenêtre **Éditeur de stratégie de groupe locale**, développez le nœud **Configuration ordinateur - Modèles d'administration - Composants Windows - Services Bureau à distance - Client Connexion Bureau à distance - Redirection du périphérique USB RemoteFX**.

Double cliquez sur le paramètre **Autoriser la redirection RDP d'autres périphériques USB RemoteFX pris en charge à partir de cet ordinateur**. Sélectionnez l'option **Activé**.



Validez par le bouton **OK**.

74 Des vulnérabilités ayant été identifiées dans la fonctionnalité vGPU de RemoteFX, elle a été dépréciée et désactivée des systèmes d'exploitation depuis la version 1809 de Windows 10 et de Windows Server 2019. À la place, il est conseillé d'utiliser la virtualisation DDA (*Discrete Device Assignment*) sur les serveurs. Les autres fonctionnalités n'ont pas été affectées.

e. Assistance rapide

La fonctionnalité d'Assistance rapide (remplaçante de l'Assistance à distance et disponible uniquement depuis Windows 10) offre à l'utilisateur le choix de demander de l'aide à un administrateur, sans déconnexion de sa session courante, tout en voyant ce qu'effectue le technicien, au contraire du Bureau à distance. Il est également possible de converser par écrit avec l'utilisateur distant.

Cliquez sur **Démarrer** et saisissez assistance rapide, ou bien appuyez sur les touches [Ctrl] + + Q.

L'assistant apparaît et vous propose deux options :

- **Obtenir de l'aide.** C'est l'option à choisir si vous souhaitez partager votre écran avec un autre utilisateur pour qu'il vous assiste. Un code à six chiffres vous sera fourni par l'utilisateur chargé de vous aider.

Assistance rapide

L'Assistance rapide Microsoft permet à deux utilisateurs de partager un ordinateur via une connexion à distance ; cela permet à l'intervenant de résoudre les problèmes sur l'ordinateur du premier utilisateur.



Obtenir de l'aide

Autorisez une personne de confiance à prendre le contrôle de votre ordinateur pour vous aider. Saisissez le code de sécurité à 6 chiffres qui vous a été communiqué.

Code provenant de l'assistant

Partager l'écran



Offrir de l'aide

Aider un autre utilisateur via une connexion à distance.

Aider un autre utilisateur

Saisissez le code fourni et cliquez sur le bouton **Partager l'écran**. Il peut vous le transmettre de manière orale ou par courrier électronique.

Cliquez sur **Autoriser** pour que la personne puisse prendre le contrôle total de votre machine... et regardez-la agir !

- **Offrir de l'aide.** Vous allez prendre le contrôle d'une machine distante.

Cliquez sur le bouton **Aider un autre utilisateur**, connectez-vous avec votre compte Microsoft ou Azure Active Directory. Un code de sécurité valable 10 min vous est fourni.

Assistance rapide

Connecté en tant que :



Yann

ybardot@yahoo.fr

[Se connecter avec un autre compte](#)

Partager le code de sécurité

La personne que vous aidez a besoin d'un code de sécurité pour vous autoriser à vous connecter à son appareil.

Code de sécurité : 445014

Le code expire dans **08:33**

Comment voulez-vous transmettre ces informations ?

[Copier dans le Presse-papiers](#)

[Envoyer un courrier électronique](#)

[Fournir des instructions](#)

Transmettez-le à la personne que vous souhaitez aider, soit par téléphone, soit en cliquant sur le lien **Envoyer un courrier électronique**. La personne va le saisir dans l'assistant pour vous autoriser à vous connecter et partager sa machine.

Sélectionnez **Prenez le contrôle total** et cliquez sur le bouton **Continuer**.

Assistance rapide

Choisissez une option de partage.



Prenez le contrôle total

Prenez le plein contrôle de l'ordinateur distant.

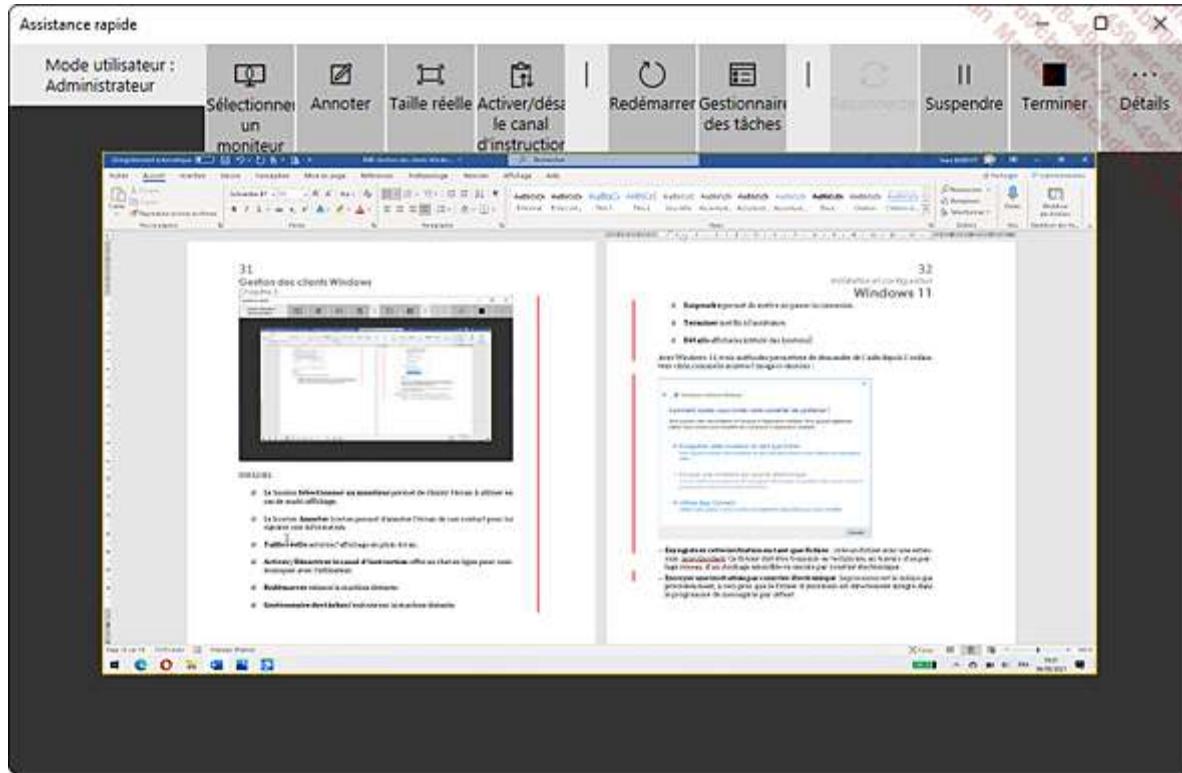


Afficher l'écran

Afficher l'écran distant sans avoir un contrôle total.

Continuer

L'interface de l'assistant rapide se présente ainsi :



- **Sélectionner un moniteur** permet de choisir l'écran à utiliser en cas de multi-affichage.
- **Annoter** permet de dessiner sur l'écran de son contact pour lui signaler une information.
- **Taille réelle** autorise l'affichage en plein écran.
- **Activer/Désactiver le canal d'instruction** offre un chat en ligne pour communiquer avec l'utilisateur.
- **Redémarrer** relance la machine distante.
- **Gestionnaire des tâches** exécute le Gestionnaire des tâches sur la machine distante.
- **Suspendre** permet de mettre en pause la connexion.
- **Terminer** met fin à l'assistance.
- **Détails** affiche les intitulés des boutons.

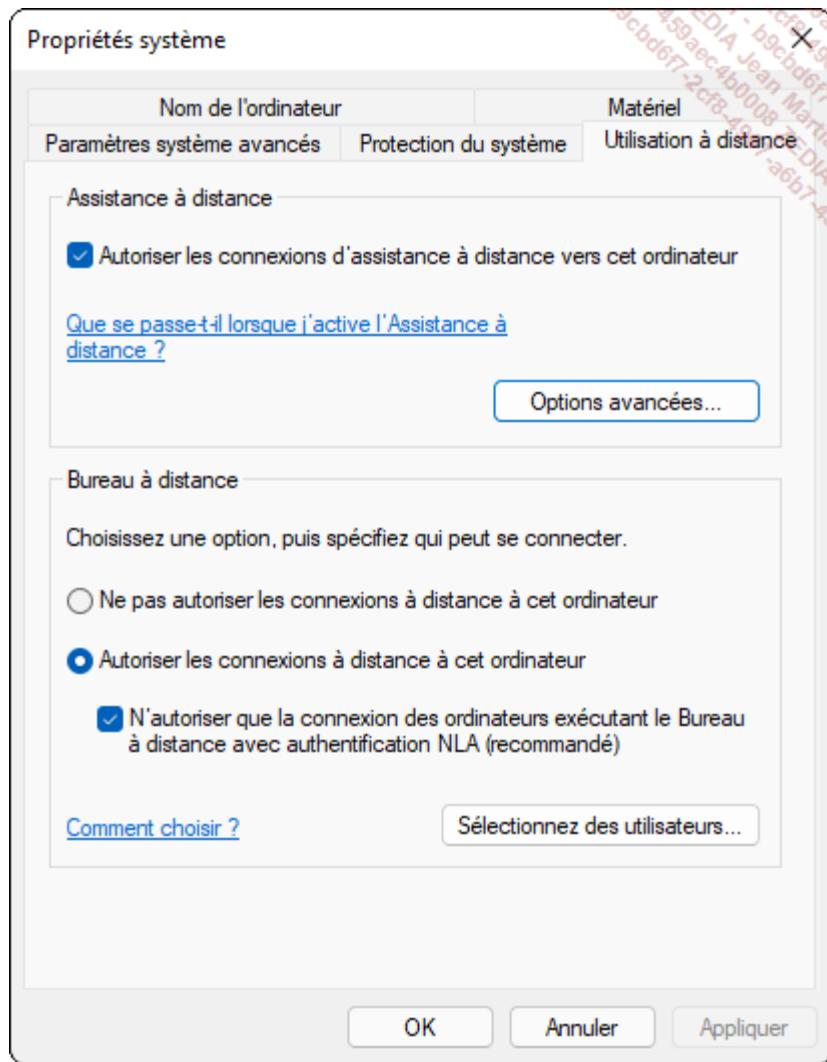
75 L'assistance rapide utilise le port 443 (<https://>) et le protocole RDP (*Remote Desktop Protocol*). Elle se connecte au service d'assistance à distance <https://remoteassistance.support.services.microsoft.com>. Tout le trafic est chiffré à l'aide de TLS 1,2.

L'Assistance rapide est activée par défaut sur Windows 11. Pour désactiver la fonctionnalité :

Ouvrez le panneau des **Paramètres, Système, Informations systèmes**.

Cliquez sur le lien **Paramètres avancés du système** puis sur l'onglet **Utilisation à distance**.

Décochez la case **Autoriser les connexions d'assistance à distance vers cet ordinateur**. Notez qu'en cliquant sur le bouton **Options avancées**, l'utilisateur peut définir la durée maximale de la validité des invitations, ainsi que la version minimale du système d'exploitation pouvant se connecter à son ordinateur.



Assistance à distance est toujours accessible sur Windows 11. Pour l'utiliser, cliquez sur le menu **Démarrer** et saisissez **msra**, puis sélectionnez **msra**.

Cliquez ensuite sur **Inviter une personne de confiance à vous aider**. Plusieurs options sont proposées :

Comment voulez-vous inviter votre conseiller de confiance ?

Vous pouvez créer une invitation et l'envoyer à l'application auxiliaire. Vous pouvez également utiliser Easy Connect pour simplifier les connexions à l'application auxiliaire.

→ Enregistrer cette invitation en tant que fichier

Vous pouvez envoyer cette invitation en tant que pièce jointe si vous utilisez une messagerie Web.

→ Envoyer une invitation par courrier électronique

Si vous utilisez un programme de messagerie électronique compatible, cette option lancera le programme et attachera le fichier d'invitation.

→ Utiliser Easy Connect

Utilisez cette option si Easy Connect est également disponible pour votre conseiller.

Annuler

- **Enregistrer cette invitation en tant que fichier** : crée un fichier avec une extension .msrcIncident. Ce fichier doit être transmis au technicien, au travers d'un partage réseau, d'un stockage amovible ou encore par courrier électronique.
- **Envoyer une invitation par courrier électronique** : le processus est le même que précédemment, à ceci près que le fichier d'invitation est directement intégré dans le programme de messagerie par défaut.
- **Utiliser Easy Connect** : cette fonctionnalité permet à l'utilisateur de demander de l'aide en rendant disponible son poste de travail depuis Internet, sans envoyer de fichier d'invitation. L'initiation de la demande peut s'effectuer au travers de la liste des contacts de l'utilisateur en difficulté.

76 Easy Connect utilise le protocole PNRP (Peer Name Resolution Protocol) pour envoyer une invitation d'Assistance à distance par le biais d'Internet. Votre routeur doit donc le prendre en charge.

Si possible, sélectionnez **Utiliser Easy Connect** puis suivez les instructions à l'écran. Sinon, utilisez les deux autres options pour générer un fichier d'invitation et l'envoyer à la personne chargée de vous assister.

L'Assistance à distance peut être configurée précisément grâce à la ligne de commande msra.exe :

- /novice : l'Assistance à distance est exécutée pour demander de l'aide.
- /openfile : ouvre un fichier d'invitation spécifique.
- /offereeasyhelp : utilise la fonctionnalité EasyConnect en exécutant l'Assistance à distance.
- /expert : l'administrateur propose de l'aide, grâce à un fichier d'invitation ou Easy Connect.

5. Liaison distante sécurisée

L'accès distant d'un poste Windows 11 désigne le fait d'atteindre des données stockées sur des ordinateurs connectés à un réseau, comme Internet ou un extranet.

Un utilisateur nomade, comme un commercial, a besoin d'accéder aux ressources de l'entreprise (dossiers, courriers électroniques...) en dehors du réseau de celle-ci.

Windows 11 propose des fonctionnalités utiles pour rendre le système d'information disponible et sécurisé auprès des utilisateurs itinérants. Par exemple avec DirectAccess, l'administrateur pourra facilement accéder aux serveurs critiques de l'entreprise, tout en étant physiquement en dehors de celle-ci.

a. Client VPN

Windows 11 propose aux utilisateurs itinérants d'installer des plug-ins VPN (*Virtual Private Network*) compatibles avec les principales solutions du marché : Check Point, F5, Juniper Networks et SonicWall. De plus, il y a deux manières de créer une connexion VPN : l'une par l'intermédiaire du **Centre Réseau et partage**, l'autre par le biais de l'interface **Paramètres, Réseau et Internet**. Nous allons détailler cette dernière :

Depuis la zone de recherche située sur la barre des tâches, saisissez **VPN** puis cliquez sur **Paramètres VPN**. Cliquez ensuite sur **Ajouter un VPN**.

Dans le champ **Fournisseur VPN**, sélectionnez **Windows (intégré)**. Nommez la connexion dans le champ **Nom de la connexion**. Saisissez ensuite l'adresse du serveur distant, un type d'authentification, un nom d'utilisateur et un mot de passe. Assurez-vous que la case **Mémoriser mes informations d'identification** est cochée. Validez en cliquant sur le bouton **Enregistrer**.

Ajouter une connexion VPN

Fournisseur VPN

Windows (intégré)

Nom de la connexion

VPN-ENI

Nom ou adresse du serveur

139.54.217.1

Type de réseau privé virtuel

Automatique

Type d'informations de connexion

Nom d'utilisateur et mot de passe

Nom d'utilisateur (facultatif)

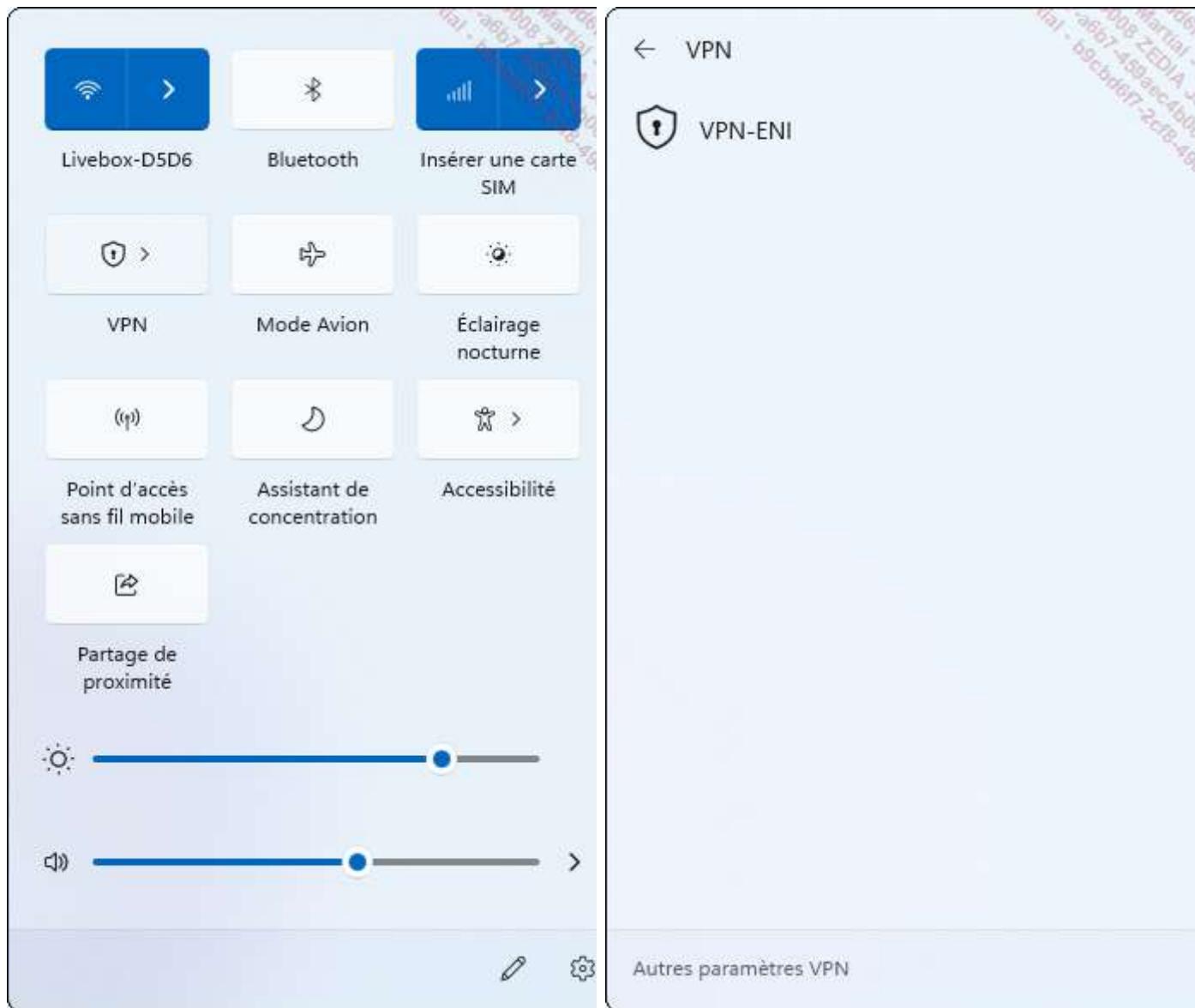
Mot de passe (facultatif)

Mémoriser mes informations de connexion

Enregistrer

Annuler

La connexion à un réseau privé virtuel est désormais effective en cliquant sur l'icône réseau de la barre des tâches, puis en cliquant sur le bouton **VPN** :



Notez que Windows 11 supporte l'authentification à l'aide d'une carte à puce, d'un OTP (*One Time Password*) ou d'un certificat.

Pour exécuter la connexion VPN précédemment créée, sélectionnez-la et cliquez sur le bouton **Se connecter**.

Si vous souhaitez uniquement utiliser le client VPN pour vous connecter à un serveur d'accès distant Microsoft, suivez la procédure ci-dessous :

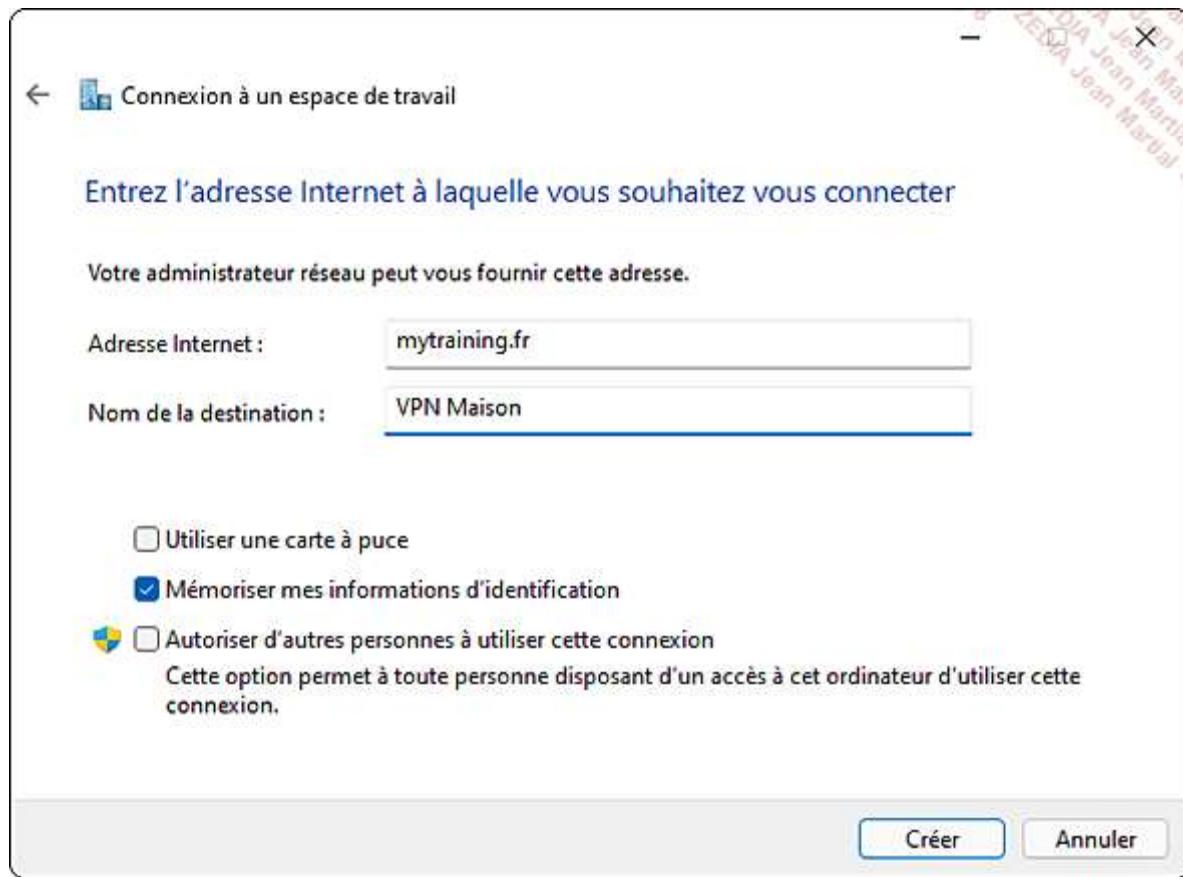
Ouvrez le panneau des **Paramètres**, cliquez sur **Réseau et Internet**, puis **Accès à distance**.

Cliquez sur le lien **Configurer une nouvelle connexion**, puis, dans la fenêtre qui s'ouvre, sélectionnez **Connexion à votre espace de travail** et cliquez sur le bouton **Suivant**.

Cochez **Non, créer une nouvelle connexion** et validez avec le bouton **Suivant**.

Cliquez sur **Utiliser ma connexion Internet (VPN)**.

Entrez l'adresse Internet du serveur VPN (dans notre exemple, mytraining.fr) et nommez la connexion **VPN Maison** par exemple. Assurez-vous que la case **Mémoriser mes informations d'identification** est cochée. Cliquez sur le bouton **Créer**.



Votre connexion VPN avec le client Microsoft est créée.

b. VPN lié à une application

Le BYOD (*Bring Your Own Device*) est une pratique consistant à permettre aux utilisateurs de se servir de leurs périphériques informatiques personnels (smartphone, ordinateur, etc.) dans un contexte professionnel. Cette tendance, de plus en plus répandue au sein des entreprises, amène des questions sociales, comme le fait qu'un salarié puisse désormais travailler de n'importe où, mais aussi tout le temps. De plus, les données de l'entreprise se retrouvent désormais stockées sur des ordinateurs personnels dont elle n'a pas la gestion. La sécurité devient donc un problème majeur dans ce type de pratique.

La fonctionnalité de déclenchement automatique du VPN permet de créer une connexion VPN de manière automatisée lorsqu'une application Windows 11 est exécutée ou bien lorsque le poste de travail utilise un suffixe DNS défini.

Cette fonctionnalité ne fonctionne pas sur un client membre d'un domaine mais peut être mis en place avec le client VPN Windows 11.

Le type de VPN supporté est obligatoirement *split tunneling*, afin de ne pas interrompre la connectivité des autres applications lorsque la connexion VPN est établie.

Par exemple, pour créer une connexion VPN automatique avec le VPN créé précédemment lorsque l'application Teams est exécutée, procédez comme suit :

Cliquez avec le bouton droit sur le menu **Démarrer**, puis cliquez sur **Terminal Windows (administrateur)**.

Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

Définissez le type de VPN *split tunneling* en saisissant la commande : Set-VpnConnection -name VPN-ENI -SplitTunneling \$true

Recherchez maintenant l'identifiant de l'application Teams. Saisissez la commande : Get-AppxPackage *team*

et validez en pressant la touche [Entrée]. Notez la valeur du champ PackageFamilyName : MicrosoftTeams_8wekyb3d8bbwe.

Paramétrez l'exécution de la connexion VPN ENI au lancement de l'application Teams en saisissant la commande ci-dessous : Add-VPNConnectionTriggerApplication -name VPNConnect -ApplicationID MicrosoftTeams_8wekyb3d8bbwe -PassThru

puis validez par la touche [Entrée].

Désormais, lorsque l'App Teams sera exécutée, une connexion VPN sera automatiquement initiée.

Notez que lorsque l'App Teams sera fermée, la connexion VPN le sera également.

D'autres déclencheurs sont paramétrables. Vous trouverez plus d'information sur cette page : <https://docs.microsoft.com/fr-fr/windows/security/identity-protection/vpn/vpn-auto-trigger-profile>

c. Reconnexion automatique VPN

Windows 11 offre aux utilisateurs itinérants la possibilité de rétablir automatiquement la connexion VPN au réseau de l'entreprise en cas de coupure internet temporaire, et ce, sans aucune intervention de l'utilisateur.

Un tunnel VPN fournit à un utilisateur distant une connexion au réseau local de l'entreprise tout en préservant la sécurité des données qui transitent.

Internet est généralement utilisé comme support de transmission en utilisant un protocole de tunneling, chargé d'encapsuler les données. Une connexion VPN relie donc deux réseaux physiques par une liaison privée.

Il existe deux types de connexion VPN :

- **Accès distant VPN** (ou point à site VPN) : permet à un utilisateur d'initier une connexion VPN depuis son poste de travail Windows 11 vers le réseau de l'entreprise, généralement au travers du réseau internet.
- **Site à site VPN** : deux routeurs relient deux sites distants au travers d'un lien WAN sécurisé par une connexion permanente VPN, par exemple le siège d'une entreprise situé à Paris et sa succursale basée à Sophia-Antipolis. Ainsi, les utilisateurs de Paris peuvent accéder aux ressources de Sophia (dossiers partagés, imprimantes...) et vice versa.

Windows 11 supporte cinq protocoles de tunneling :

- PPTP (*Point-to-Point Tunneling Protocol*).
- L2TP/IPsec (*Layer 2 Tunneling Protocol with Internet Protocol Security*) avec certificat.
- L2TP/IPsec (*Layer 2 Tunneling Protocol with Internet Protocol Security*) avec clé.
- SSTP (*Secure Socket Tunneling Protocol*).
- IKEv2 (*Internet Key Exchange*).

La fonctionnalité **Reconnexion automatique VPN** est particulièrement pratique pour les utilisateurs nomades. Ainsi, un utilisateur distant ayant une connexion internet active pourra se reconnecter automatiquement aux ressources de son entreprise en cas de déconnexion.

Cette fonctionnalité utilise le mode de tunnel IPsec avec IKEv2 et l'extension MOBIKE (mobilité et multirésidence d'IKEv2).

L'infrastructure côté serveur gérant l'installation de la reconnexion automatique VPN est moins contraignante que celle de DirectAccess. Pour cela, il est nécessaire de disposer des éléments suivants :

- Une infrastructure à clé publique (PKI) délivrant un certificat pour l'ordinateur client.

- Un serveur VPN (Windows Server 2008 ou supérieur) possédant deux cartes réseau, l'une connectée au réseau Internet, l'autre au réseau local de l'entreprise. Les ports UDP 500 pour IKE et 4500 pour IPsec doivent être autorisés en flux entrant sur le pare-feu.
- Un poste de travail Windows 11 ayant la connectivité nécessaire pour accéder au réseau distant.

77 Les systèmes d'exploitation Windows Server 2008 R2, 2012, 2016 et 2019 et Windows 7/8.1/10 prennent aussi en charge la reconnexion automatique VPN.

Pour que le client Windows 11 puisse se connecter au serveur VPN, il est nécessaire d'importer le certificat racine émis pour ce serveur.

Voici la procédure, automatisable au travers d'un objet stratégie de groupe :

Pressez les touches  + R et saisissez mmc puis validez par la touche [Entrée]. Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît. Cliquez sur le menu **Fichier** puis **Ajouter/Supprimer un composant logiciel enfichable**.

Dans la liste de gauche **Composants logiciels enfichables disponibles**, sélectionnez **Certificats**, puis cliquez sur le bouton **Ajouter**. Dans la fenêtre **Composant logiciel enfichable Certificats**, sélectionnez la case **Un compte d'ordinateur**, puis cliquez sur **Suivant** et **Terminer**. Validez par **OK**.

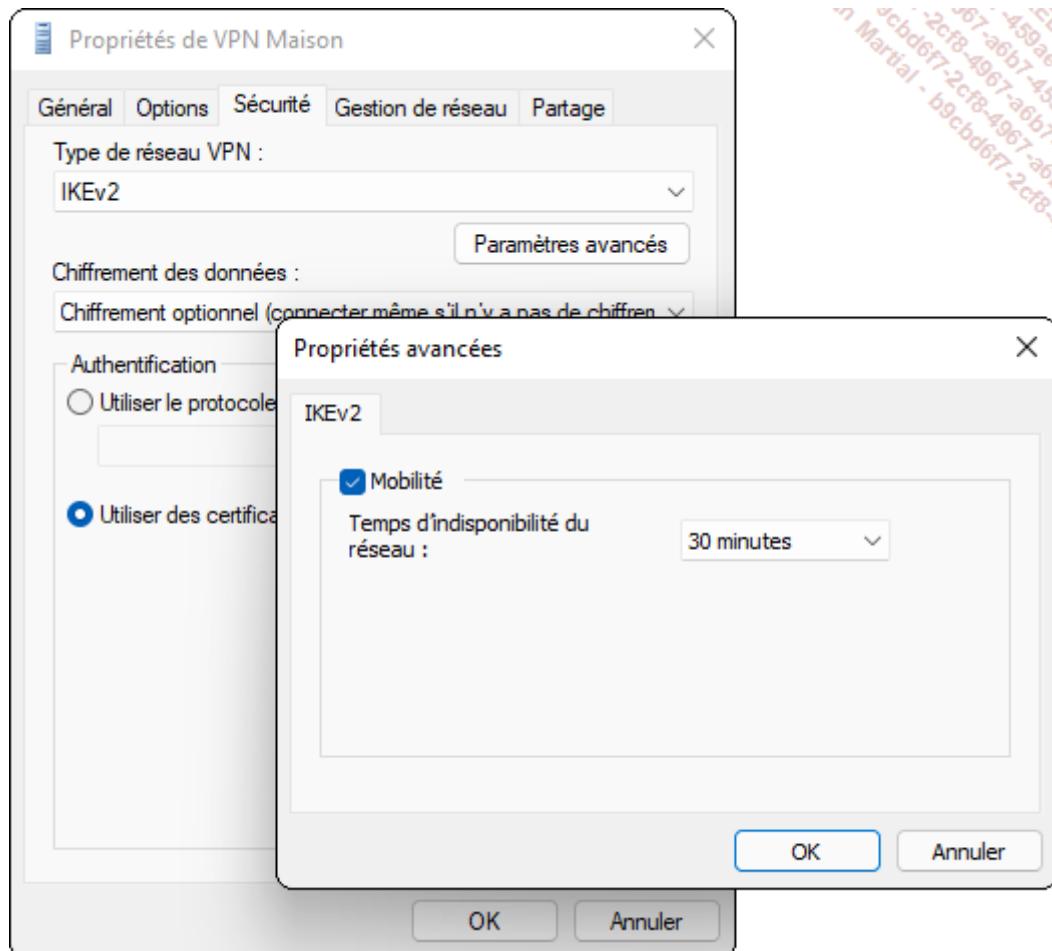
Développez dans la zone de gauche **Certificats (ordinateur local)**, le nœud **Autorités de certification racines de confiance**. Effectuez un clic avec le bouton droit sur **Certificats** puis choisissez **Toutes les tâches** et **Importer**. Cliquez sur le bouton **Suivant** puis sélectionnez le certificat racine émis grâce au bouton **Parcourir**.

Une fois le certificat importé, vous pouvez créer une connexion VPN comme expliqué précédemment.

Pour configurer les paramètres de sécurité permettant la reconnexion VPN, depuis le panneau des **Paramètres, Réseau et Internet, Paramètres réseau avancés**, cliquez sur **Options d'adaptateur réseau supplémentaires**.

Cliquez avec le bouton droit sur la connexion VPN à configurer, puis sur **Propriétés**.

Cliquez sur l'onglet **Sécurité** et sélectionnez **IKEv2** dans le champ **Type de réseau VPN**. En cliquant sur le bouton **Paramètres avancés**, vous pourrez configurer le temps d'indisponibilité du réseau avant déconnexion définitive du client Windows 11. Validez par le bouton **OK**.



La reconnexion VPN est désormais effective du côté du client.

78 Si l'ordinateur portable exécutant Windows 11 entrait en mode veille prolongée, l'utilisateur devrait manuellement entrer ses informations d'authentification à la sortie de veille : la connexion serait en effet perdue.

d. DirectAccess

Windows Server 2008 R2 a introduit la fonctionnalité DirectAccess similaire à la reconnexion automatique VPN, car elle propose de connecter automatiquement l'utilisateur itinérant au réseau de l'entreprise mais cette fois... sans connexion VPN.

Ainsi, les administrateurs peuvent déployer à distance les objets de stratégie de groupe, les mises à jour de sécurité et les logiciels sur les ordinateurs Windows 11 ; la connexion bidirectionnelle est transparente dès lors qu'un accès internet est disponible, même si aucun utilisateur n'a ouvert de session sur l'ordinateur.

La sécurité est assurée par une authentification de l'utilisateur et de l'ordinateur membre du domaine, un chiffrement des données échangées entre les parties et un contrôle des accès aux ressources de l'entreprise (facultatif).

DirectAccess s'intègre désormais avec le service RRAS (*Routing and Remote Access Server*) dans un unique rôle nommé Remote Access (accès à distance), disponible depuis Windows Server 2012 R2.

Le déploiement de DirectAccess ne nécessite plus de PKI (*Public Key Infrastructure*) complexe à implémenter et apporte des fonctionnalités côté serveur :

- Support du protocole d'échange de routes nommé BGP (*Border Gateway Protocol*).
- Prise en charge des fonctions de reverse proxy pour les applications web hébergées dans le réseau interne.

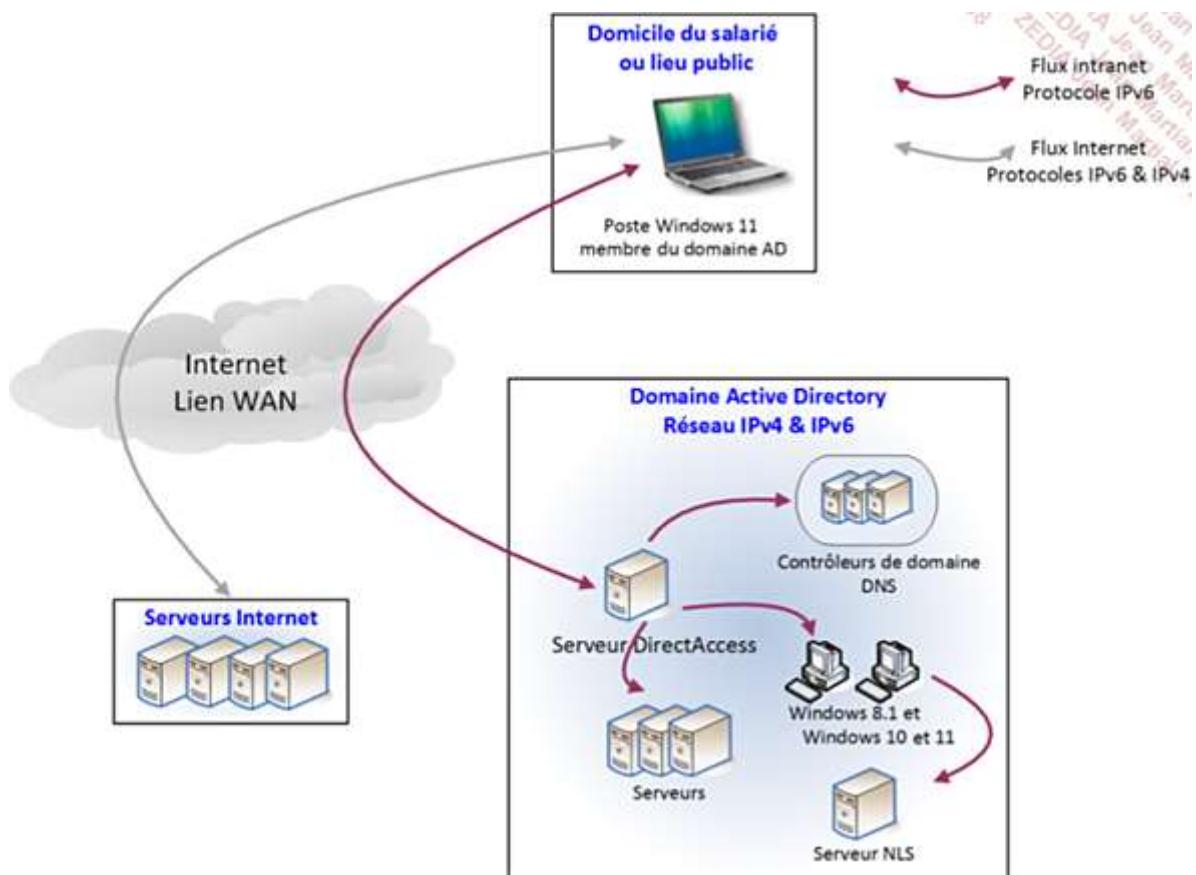
- Gestion de passerelle VPN site à site.
- Distribution des tâches entre les différents serveurs d'un groupe grâce à la répartition de charge. Huit nœuds sont supportés, mais en cas de défaillance de l'un d'eux, les connexions actives ne seront pas transférées aux autres nœuds.
- Gestion de l'authentification par OTP (*One-Time Password*) en utilisant par exemple un module TPM (*Trusted Platform Module*) intégré à un client.
- Support de PowerShell et des versions Core de Windows Server.
- Prise en charge de plusieurs domaines.
- Mise à disposition d'un assistant pour la configuration simplifiée de DirectAccess.

Au niveau du client, Windows 11 permet à des applications préconfigurées de se connecter automatiquement au réseau de l'entreprise en ouvrant une connexion VPN quand celles-ci sont démarrées.

Côté serveur, DirectAccess nécessite un domaine AD DS (*Active Directory Domain Services*), ainsi qu'un serveur Windows disposant de deux cartes réseau physiques, l'une connectée à Internet, l'autre au réseau local d'entreprise. Désormais, il n'est plus nécessaire de posséder deux adresses publiques IPv4 consécutives pour faire fonctionner DirectAccess, car le serveur peut être positionné derrière un routeur supportant la fonction NAT (*Network Address Translation*).

Un poste compatible DirectAccess possède une version client (Windows 7 Intégrale et Entreprise, Windows 8 et 8.1 Entreprise, Windows 10 et 11 Entreprise et Education) ou une version serveur (Windows Server 2008 R2 ou supérieur) d'un système d'exploitation Microsoft, et doit être membre du même domaine d'appartenance que le serveur DirectAccess.

Voici un schéma présentant la solution ainsi que les différents flux :



La fonctionnalité s'appuie sur le protocole IPv6 pour faire transiter les données. Néanmoins, un client DirectAccess peut accéder à des ressources du réseau interne possédant une adresse IPv4 grâce aux protocoles

NAT64 et DNS64, mais la connexion s'effectuera de manière unidirectionnelle, du client DirectAccess vers la ressource visée.

Le service s'intègre avec NAP (*Network Access Protection*) afin de s'assurer que le client DirectAccess qui souhaite se connecter au réseau de l'entreprise a passé avec succès les tests d'intégrité prédéfinis.

Les paramètres et les certificats à appliquer sur les clients Windows 11 sont déployés à l'aide d'un objet stratégie de groupe, généré depuis l'assistant d'installation de DirectAccess.

Un serveur web IIS (*Internet Information Services*) nommé NLS (*Network Location Server*) est placé dans le réseau local de l'entreprise pour n'être accessible qu'aux clients Windows 11 connectés à l'intranet. Ainsi, si le poste de travail n'y accède pas à l'aide du protocole HTTPS, alors il est considéré comme étant connecté à un réseau distant, tel qu'Internet.

Windows 11 maintient les nouveautés apparues avec Windows 10 vis-à-vis de la technologie DirectAccess :

- Gestion de la redondance géographique : les serveurs DirectAccess permettant au client de tester l'accès au réseau de l'entreprise peuvent être positionnés dans des zones géographiques distinctes.
- Affichage du statut d'une connexion DirectAccess dans la zone de notification.
- Intégration de commandes DirectAccess dans PowerShell afin de tester et configurer la solution.

À l'aide de la console DirectAccess, installée avec le rôle Accès à distance, il est possible de définir l'une des deux méthodes de connexion du client Windows 11 :

- Serveur sélectionné : la session sécurisée est établie entre le client et le serveur DirectAccess mais IPsec n'est pas utilisé pour les communications sur le réseau local de l'entreprise.
- Réseau d'entreprise : un chiffrement de bout en bout est requis pour accéder aux ressources internes, ainsi qu'une connectivité IPv6 et l'accès à des serveurs d'applications Windows Server.

Pour établir une connexion au serveur DirectAccess, le client Windows 11 effectue au préalable une série d'étapes :

1. Détection d'une connexion à un réseau. S'il est connecté à l'Intranet, DirectAccess est désactivé. S'il est connecté à Internet, DirectAccess est activé.
2. Connexion au serveur DirectAccess avec authentification des deux parties à l'aide de certificats d'ordinateur.
3. Authentification auprès d'un contrôleur de domaine dont l'adresse IP a été obtenue auprès du serveur DNS référentiel.
4. Accès aux ressources de l'entreprise auquel l'utilisateur s'est vu accorder l'accès. Le serveur DirectAccess transfère le trafic vers l'application.

Tout ce processus est transparent pour l'utilisateur.

Le langage PowerShell permet d'administrer un client Windows 11 DirectAccess, à l'aide de commandes telles que :

- Reset-DAClientExperienceConfiguration : restaure les paramètres de configuration DirectAccess à leurs valeurs par défaut.
- New-DAEntryPointTableItem : crée un point d'entrée pour un nouveau site.
- Get-DAClientExperienceConfiguration : affiche la configuration du client DirectAccess.

e. VPN SSTP

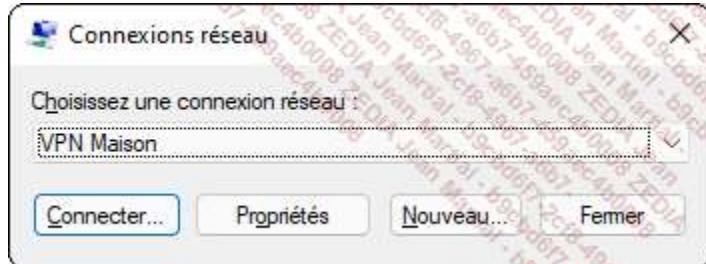
SSTP (*Secure Socket Tunneling Protocol*) est un type de tunnel VPN disponible depuis Windows Server 2008. Il permet l'encapsulation de paquets PPP (*Point-to-Point Protocol*) via le protocole HTTPS. Cette technologie permet par exemple d'utiliser des méthodes d'authentification robustes telles qu'EAPTLS (cartes à puce).

Comme la grande majorité des pare-feu d'entreprise laissent passer le protocole HTTPS (port 443) en flux sortant, l'établissement de la connexion est donc facilité.

Le protocole SSTP est compatible avec les ordinateurs clients exécutant au minimum Windows Vista SP1, et avec les versions serveurs Windows Server 2008 et ultérieures. Ces derniers doivent obligatoirement approuver l'autorité ayant émis le certificat du serveur SSTP.

Pour créer un tunnel SSTP depuis un client Windows 11, il faut d'abord importer le certificat du serveur VPN SSTP (cf. procédure d'import dans la section Reconexion automatique VPN), puis créer la connexion VPN :

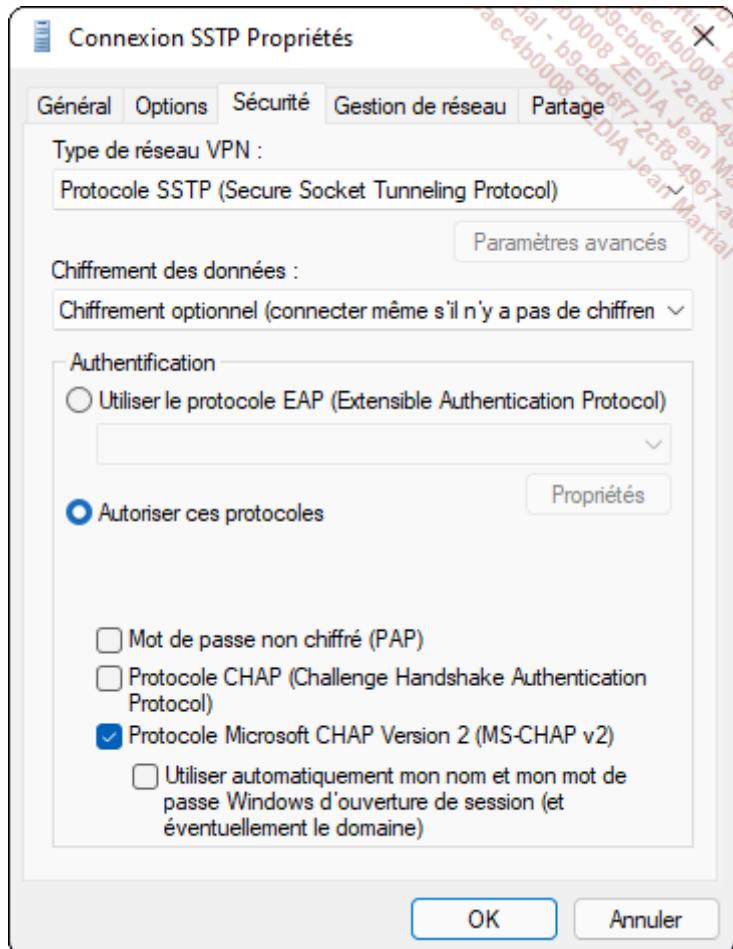
Pressez les touches  et R et saisissez rasphone dans la fenêtre **Exécuter** puis validez par [Entrée]. Si vous n'avez pas créé de connexion distante, cliquez sur le bouton **OK** pour créer une liste d'entrée dans le répertoire des **Connexions réseau**.



Cliquez ensuite sur le bouton **Nouveau**.

Cliquez sur **Réseau du lieu de travail** dans la fenêtre **Set up a new connection**. Entrez l'adresse internet du serveur VPN et nommez la connexion **SSTP** puis cliquez sur le bouton **Créer**.

Cliquez ensuite sur le bouton **Propriétés** de la fenêtre **Connexion réseau**, puis sur l'onglet **Sécurité**. Sélectionnez **Protocole SSTP (Secure Socket Tunneling Protocol)** dans le champ **Type de réseau VPN**. Configurez ensuite la méthode d'authentification : **EAP** (*Extensible Authentication Protocol*), **PAP** (*Password Authentication Protocol*, peu sécurisé), **CHAP** (*Challenge Handshake Authentication Protocol*) ou **MS-CHAP V2**.



Mode PC partagé

- Microsoft propose une fonctionnalité nommée Mode PC partagé. Son principe est simple : le poste de travail est configuré pour ne nécessiter aucune maintenance afin d'être autonome, et il ne peut y avoir qu'un seul utilisateur à la fois qui l'utilise, même lorsque le poste est verrouillé.
- L'ordinateur doit être joint à un domaine Active Directory ou Azure Active Directory pour bénéficier de cette fonctionnalité. De plus, le mode invité permet de ne pas demander un identifiant pour ouvrir une session, et crée dans ce cas un compte local à chaque connexion. Ces comptes temporaires, qu'ils soient locaux ou appartenant à un domaine, sont supprimés lors de la déconnexion de la personne qui utilise l'ordinateur, ou lorsqu'aucun compte ne s'est connecté pendant un temps spécifique.
- Enfin, en couplant cette fonctionnalité avec le mode Kiosque Accès affecté (cf. chapitre Installation du client Windows 11, section Authentification), il est possible de mettre à disposition une borne fournissant l'accès à une seule application précise, sans besoin d'un compte utilisateur membre d'un domaine Active Directory.
- Lorsque l'ordinateur est mis en veille après une période d'inactivité, le système en profite pour télécharger les mises à jour depuis Windows Update, les installer et redémarrer automatiquement. Cette configuration s'effectue via un objet stratégie de groupe : **Configuration ordinateur - Modèles d'administration - Composants Windows - Windows Update - Gérer l'expérience utilisateur final**.

79 Double cliquez sur le paramètre **Configuration du service Mises à jour automatiques** et définissez la valeur sur 4 dans le menu déroulant puis cochez la case **Installer durant la maintenance automatique**.



- L'activation de la fonctionnalité Mode PC partagé n'est pas intuitive. Il est nécessaire d'utiliser le Concepteur de configuration et d'acquisition d'images Windows (ICD) détaillé au chapitre Conception d'une image de déploiement, section Crédit d'une installation de référence, et de créer un package d'approvisionnement en définissant le paramètre Shared PC, comme le montre l'image ci-dessous :

- À noter que le package d'approvisionnement peut être appliqué en mode non destructif sur un poste de travail en cours de fonctionnement, ou bien défini pour les prochaines installations de Windows 11 (via l'insertion d'une clé USB contenant le package, durant la phase de première configuration).
- La liste des nombreux paramètres liés à cette fonctionnalité est disponible depuis le lien internet : <https://docs.microsoft.com/fr-fr/windows/configuration/set-up-shared-or-guest-pc>
- Il est également possible de configurer le mode PC partagé à l'aide de MEM (Microsoft Endpoint Manager) et Intune.

Imprimantes

80 Le développement de l'informatique et les économies escomptées par le « zéro papier » n'ont pas supprimé l'impression de documents comme support d'information.

81 Un administrateur doit pouvoir gérer efficacement plusieurs imprimantes et serveurs d'impression dans le réseau dont il a la charge, afin de se consacrer à des tâches moins chronophages.

82 Selon Microsoft, Windows 11 intègre plusieurs centaines de pilotes d'imprimantes dans le système, les anciens pilotes de périphériques d'impression sont quant à eux disponibles sur le site <https://www.microsoft.com/fr-fr/windows/> ou sur celui du constructeur du matériel.

83 Le support d'XPS (*XML Paper Specifications*), langage de description de document, est implémenté en standard, sous réserve que le périphérique d'impression gère les langages PDL (*Page Description Language*) et XPS. Dans la grande majorité des cas, Windows 11 fournit le pilote d'impression nécessaire au bon fonctionnement de l'imprimante. Sinon, il peut être requis d'utiliser le disque fourni par le fabricant, ou bien de télécharger les pilotes sur son site internet.

84 Windows 11 détecte automatiquement les imprimantes USB mais pas celles utilisant des ports série ou parallèle. Quand l'utilisateur branche une imprimante à son ordinateur, celui-ci lui attribue un port et recherche le pilote adéquat. Un ordinateur ayant une imprimante avec un pilote 64 bits raccordée ne pourra pas traiter l'impression de documents si les clients distants veulent utiliser une version 32 bits du pilote. Dans ce cas, il faudra que l'administrateur installe manuellement le pilote 32 bits depuis les **Propriétés de l'imprimante** et l'onglet **Avancé**.

85 L'ajout d'une imprimante s'effectue depuis le panneau des **Paramètres, Bluetooth et appareils, Imprimantes et scanners**, en suivant la procédure ci-dessous :

Depuis le champ de recherche situé dans la barre des tâches, saisissez **imprimantes** et sélectionnez **Imprimantes et scanners**. Cliquez sur le bouton **Ajouter un appareil**. L'assistant d'installation recherche des imprimantes plug-and-play branchées localement ou sur le réseau.

Dans la zone **Je ne retrouve pas l'imprimante recherchée dans la liste**, cliquez sur le lien **Ajouter manuellement**.

Paramètres

Yann BARDET
ybardot@yahoo.fr

Rechercher un paramètre

Ajouter une imprimante ou un scanner Actualiser

Système

Bluetooth et appareils

Réseau et Internet

Personnalisation

Applications

Comptes

Heure et langue

Jeux

Accessibilité

Confidentialité et sécurité

Windows Update

Je ne trouve pas l'imprimante recherchée dans la liste Ajouter manuellement

Fax

Microsoft Print to PDF

Microsoft XPS Document Writer

Préférences de l'imprimante

Laisser Windows gérer mon imprimante par défaut Activé

Télécharger des pilotes et logiciels d'appareil via des connexions limitées Désactivé

L'utilisateur est invité à définir manuellement les paramètres de l'imprimante.

← Ajouter une imprimante

Rechercher une imprimante par d'autres options

M'aider à trouver mon imprimante un peu plus ancienne

Sélectionner une imprimante partagée par nom

Parcourir...

Exemple : \\ordinateur\imprimante ou
http://ordinateur/printers/imprimante/.printer

Ajouter une imprimante à l'aide d'une adresse IP ou d'un nom d'hôte

Ajouter une imprimante Bluetooth, sans fil ou réseau détectable

Ajouter une imprimante locale ou réseau avec des paramètres manuels

Suivant Annuler

86 Ainsi, l'imprimante peut être recherchée par son nom de partage (\\\Serveur\ NomImprimante), son adresse IP, sa connectivité (Bluetooth, sans fil...) ou par son type de connexion (série, parallèle). La case **M'aider à trouver mon imprimante un peu plus ancienne** exécute un assistant.

87 Une fois la méthode d'ajout définie, Windows 11 recherche un pilote approprié dans le magasin de pilotes (commande pnputil.exe), puis, si celui-ci est introuvable, propose à l'utilisateur d'insérer le média fourni par le fabricant ou d'effectuer une recherche sur le site Windows Update.

88 La gestion des imprimantes installées s'effectue au même endroit (**Paramètres, Bluetooth et appareils, Imprimantes et scanners**) en cliquant sur une imprimante installée. L'utilisateur peut alors effectuer les actions suivantes :

- **Ouvrir la file d'attente d'impression** pour gérer les documents en cours d'impression : suspendre, annuler... Il est également possible de définir comme imprimante par défaut le périphérique.
- **Imprimer une page de test** pour vérifier que l'impression fonctionne correctement.
- Gérer les **Propriétés de l'imprimante** : partage, sécurité (détaillées ultérieurement).
- Gérer les **Préférences d'impression** spécifiques au pilote : profils par défaut, recto-verso, effets, orientation, entretien des buses...
- Accéder aux **Propriétés du matériel**.



89 En cliquant sur les **Propriétés de l'imprimante**, l'onglet **Partage** des propriétés de l'imprimante gère la mise à disposition de celle-ci aux autres utilisateurs du réseau, ainsi que l'ajout de pilotes supplémentaires pour les ordinateurs fonctionnant sur un ancien système d'exploitation Microsoft.

90 L'onglet **Sécurité** permet de définir précisément les comptes autorisés à accéder à l'imprimante, grâce aux autorisations **Imprimer un document** (gestion de ses propres impressions uniquement), **Gérer cette**

imprimante, Gestion des documents (modification de l'ordre d'impression dans la file d'attente) et **Autorisations spéciales (lecture, modification des autorisations et appropriation)**.

- Par défaut, le groupe Tout le monde possède l'autorisation d'imprimer sur une imprimante sélectionnée.
- 91 Windows 11, comme Windows 10, propose une option, activée par défaut, permettant de **Laisser Windows gérer mon imprimante par défaut**. Windows définit comme imprimante par défaut celle que vous avez utilisée récemment sur le site où vous vous trouvez.

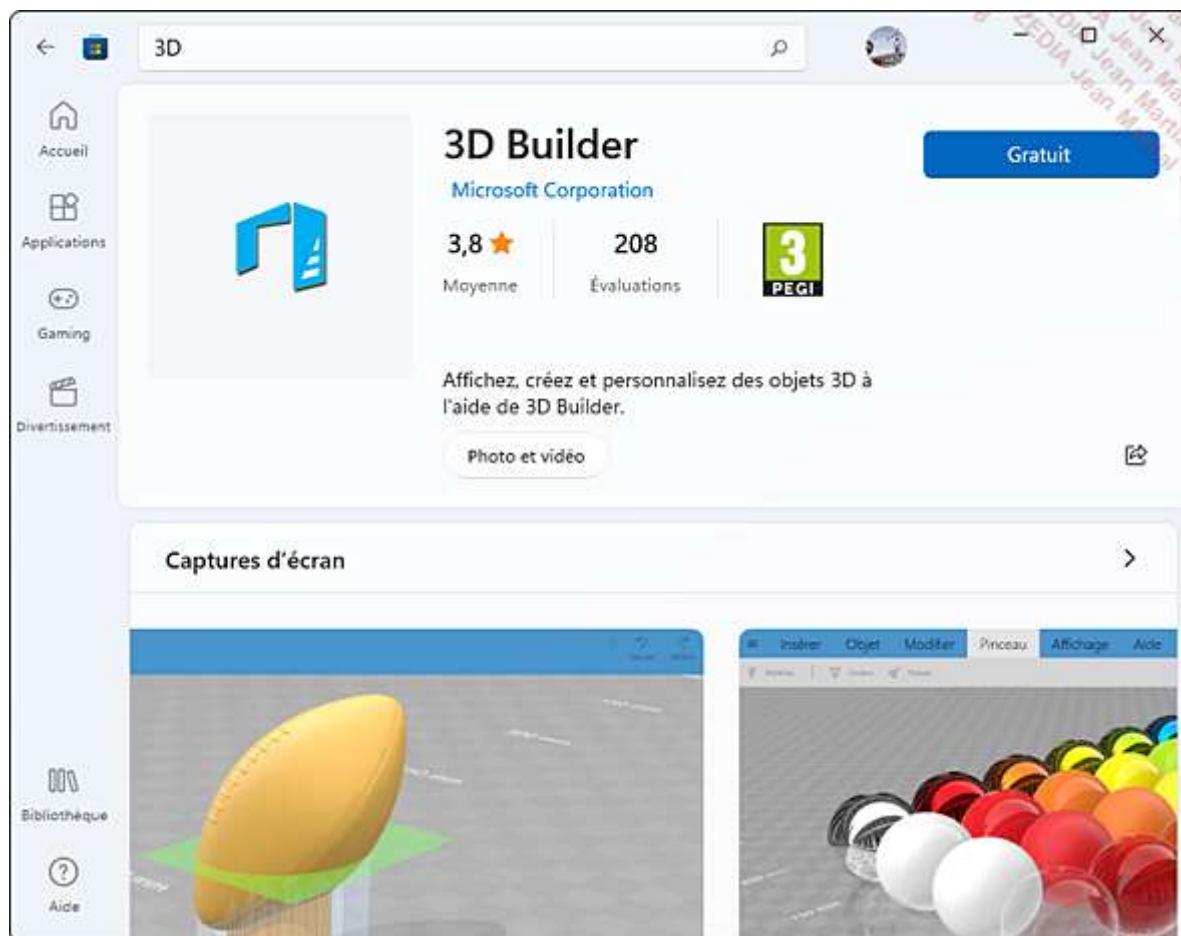
1. Imprimante 3D

92 L'impression 3D (tridimensionnelle) permet de créer un objet réel conçu depuis un logiciel CAO (conception assistée par ordinateur). Le fichier 3D obtenu est transféré vers une imprimante 3D qui dépose de la matière couche par couche pour obtenir la pièce précédemment dessinée. Ainsi un particulier ou une entreprise peut désormais créer ses propres objets personnalisés.

93 Windows 11 reconnaît automatiquement les principales imprimantes 3D du marché grâce à un partenariat créé avec des fabricants tels que 3D Systems ou Makerbot. Les pilotes étant inclus, Microsoft propose en téléchargement gratuit depuis le Microsoft Store l'App 3D Builder, afin que l'utilisateur puisse visualiser, concevoir et imprimer ses propres objets 3D. L'application est livrée avec une bibliothèque d'exemple d'objets.

94 De plus, Windows 11 supporte les formats STL (*STereoLithography*), OBJ ou 3MF nécessaires à l'impression d'objets 3D et lit également les formats PLY (polygones) et VRML (*Virtual Reality Modeling Language*).

95 Une simple recherche dans le Microsoft Store sur le mot-clé « 3D Builder » permet d'installer l'App :



96 Les principaux fabricants d'imprimantes 3D proposent aussi leurs propres Apps dans le magasin Microsoft Store. Bien entendu, les développeurs peuvent aussi utiliser les API (*Application Programming Interface*) natives livrées avec Windows 11 pour fournir des fonctionnalités d'impression 3D à leurs Apps.

2. Wi-Fi Direct Printing

97 La fonctionnalité Wi-Fi Direct Printing est une technologie permettant d'imprimer directement depuis un périphérique (smartphone, tablette tactile ou ordinateur) vers une imprimante, et ce sans point d'accès intermédiaire ou routeur sans fil.

98 L'ajout d'un pilote d'imprimante ou d'un logiciel dédié n'est pas requis, et toutes les fonctions de l'imprimante sont disponibles par l'intermédiaire de ce procédé.

99 De plus en plus de fabricants d'imprimantes supportent la connexion directe sans fil en sécurisant l'accès avec un mot de passe WPA/WPA2 (*Wi-Fi Protected Access*).

100 Wi-Fi Direct Printing nécessite une carte Wi-Fi qui prend en charge le Wi-Fi Direct, ainsi qu'une imprimante réseau supportant également cette technologie.

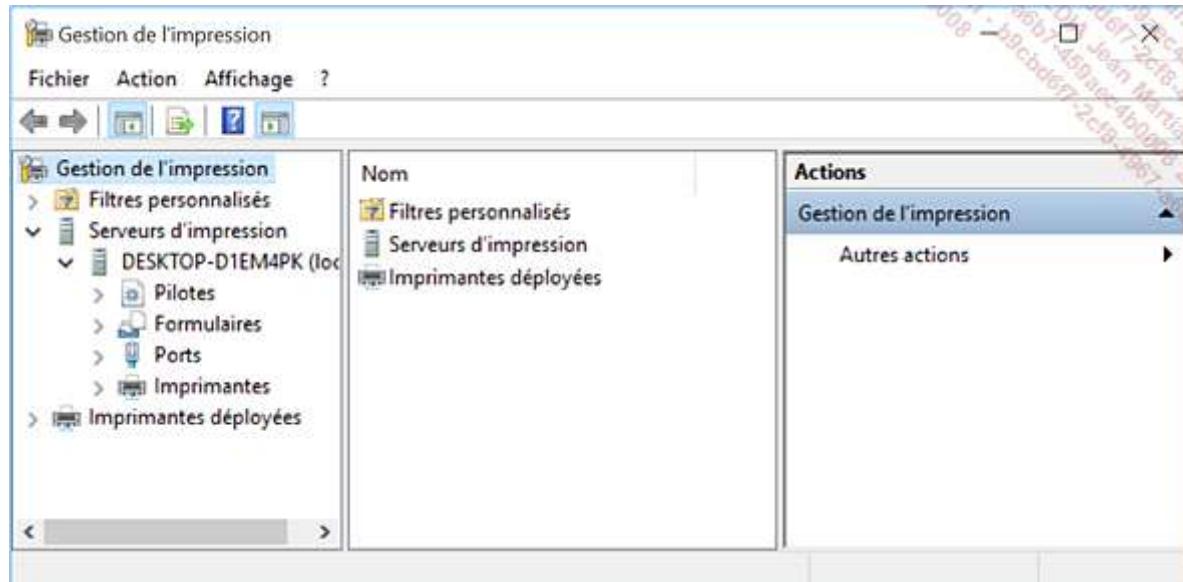
101 Pour imprimer un document sur une telle imprimante, il suffit de sélectionner le réseau sans fil portant le nom de l'imprimante depuis la barre des tâches de la vignette Bureau et de s'y connecter à l'aide du code PIN requis.

3. Console Gestion de l'impression

102 Windows 11 simplifie le déploiement des imprimantes sur les clients membres d'un domaine Active Directory. Grâce au composant logiciel enfichable Gestion de l'impression, l'administrateur peut configurer le déploiement des imprimantes du réseau de l'entreprise. En outre, cette console permet de gérer de manière centralisée les files d'attente d'impression et de recevoir des notifications par courrier électronique lorsqu'un problème apparaît.

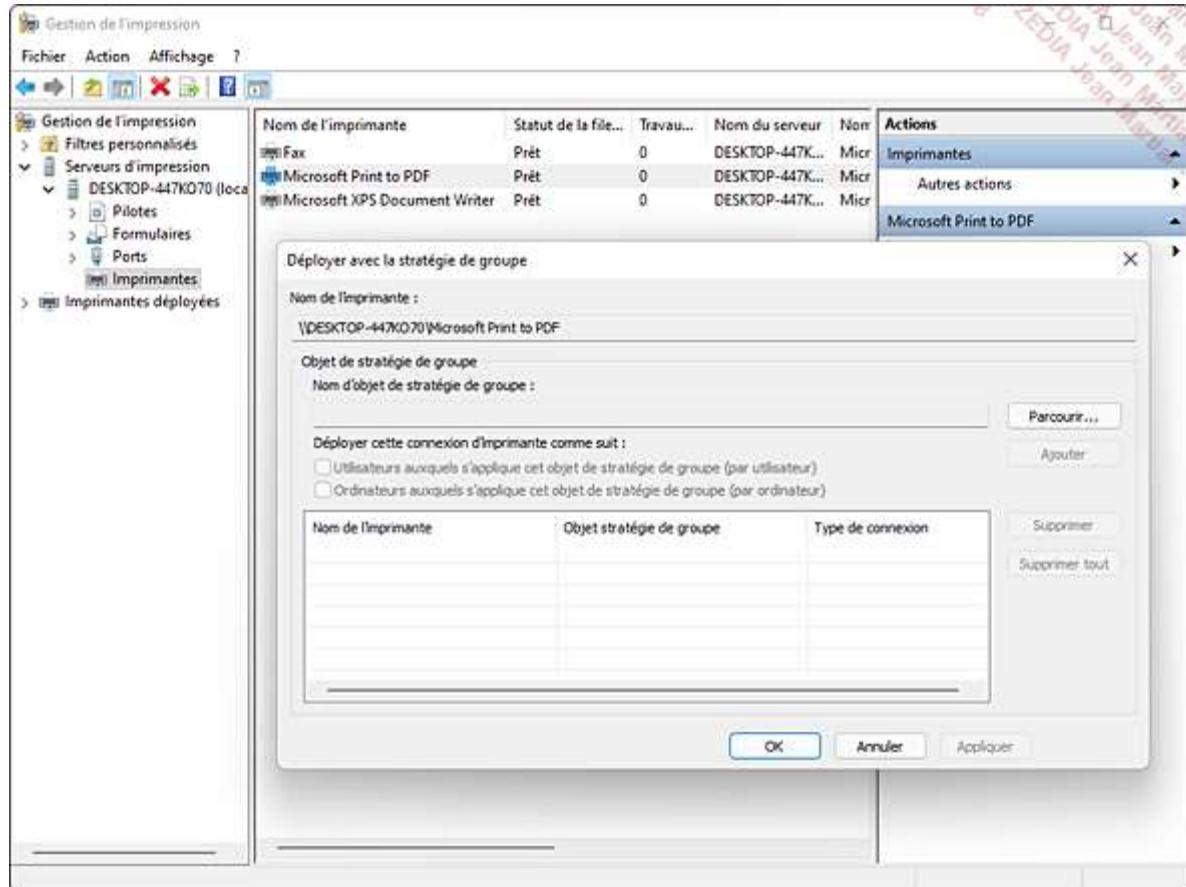
103 Pour accéder à cette console, suivez la procédure ci-dessous, en vous assurant au préalable que le poste Windows 11 est membre d'un domaine Active Directory :

Dans le champ de recherche situé dans la barre des tâches, saisissez **outils** et sélectionnez **Outils Windows**. Dans la fenêtre **Outils Windows**, double cliquez sur **Gestion de l'impression**. Vous pouvez également saisir printmanagement.msc.



104 Pour déployer une imprimante sur les postes clients :

Développez le nœud **Serveurs d'impression - NomDeVotreOrdinateur - Imprimantes**. Cliquez avec le bouton droit sur le nom de l'imprimante à déployer puis choisissez **Déployer avec la stratégie de groupe**.



Dans la fenêtre **Déployer avec la stratégie de groupe**, cliquez sur le bouton **Parcourir** et sélectionnez la stratégie de groupe à utiliser pour le déploiement de l'imprimante puis validez par le bouton **OK**.

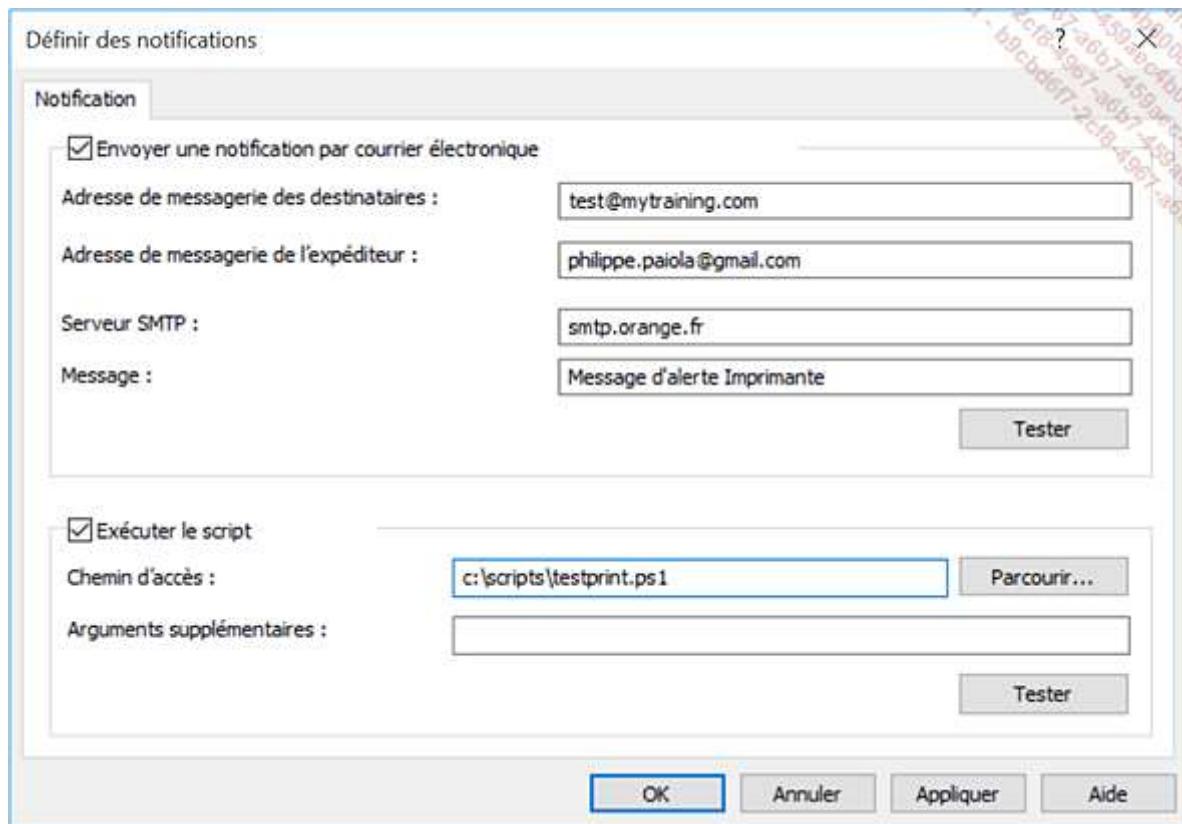
Il convient maintenant de choisir le type de déploiement, soit par **Utilisateurs**, soit par **Ordinateurs**, ou bien les deux, en cochant les cases correspondantes. N'oubliez pas de valider le déploiement en cliquant sur le bouton **Ajouter**, puis sur le bouton **OK**.

105 Pour créer une notification (courriel ou exécution d'un script) liée aux travaux d'impression :

Cliquez avec le bouton droit sur le nœud **NomDeVotreOrdinateur** puis **Définir des notifications**.

Cochez la case **Envoyer une notification par courrier électronique** et entrez l'**Adresse de messagerie des destinataires**, de l'**expéditeur**, le **Serveur SMTP** et le **Message** à transmettre.

106 La case **Exécuter le script** vous permet de définir le **Chemin d'accès** et les **Arguments supplémentaires** d'un script créé à cet effet.



107 En sélectionnant le nœud **Imprimantes déployées**, l'administrateur pourra visualiser l'ensemble des imprimantes déployées à l'aide d'un objet de stratégie de groupe depuis l'ordinateur Windows 11.

108 L'affichage des travaux d'impression en cours s'effectue en cliquant avec le bouton droit sur le nœud **Imprimantes**, puis sur **Affichage étendu**.

109 Dans le délai d'actualisation de 90 minutes de l'objet de stratégie de groupe, les imprimantes seront déployées automatiquement sur les postes visés. Notez que les ordinateurs clients qui exécutent Windows 2000, Windows XP ou Windows Server 2003 devront exécuter le fichier **PushPrinterConnections.exe** grâce à un script de démarrage (pour un déploiement par ordinateur) ou d'ouverture de session (pour un déploiement par utilisateur).

110 Il est également possible de rajouter cette imprimante dans une GPO. La configuration précédente ne sera alors pas nécessaire.

4. Impression directe pour les filiales

111 L'impression directe pour les filiales réduit l'utilisation de la bande passante lorsqu'un utilisateur souhaite imprimer un document sur un périphérique d'impression placé dans une succursale et géré par un serveur Windows Server 2012 (ou supérieur) situé dans un bureau principal. Les données d'impression ne transitent plus du serveur d'impression central vers l'imprimante placée dans la succursale. Elles sont directement transmises du poste Windows 11 vers l'imprimante puis mises en cache dans la filiale, ainsi, lors d'une coupure du lien WAN (*Wide Area Network*) entre la succursale et le serveur d'impression, l'imprimante sera toujours disponible.

112 En résumé, le client Windows 11 n'envoie jamais le document à imprimer au serveur d'impression.

113 La fonctionnalité d'impression directe pour les filiales nécessite une imprimante réseau, un serveur Windows Server 2012 (ou supérieur), et des clients Windows 8, 8.1, 10 ou 11 Entreprise ou Education. Les fonctionnalités de quota, d'audit ou de pool d'impression seront inaccessibles durant l'utilisation de l'impression directe pour les filiales.

114 Les versions précédentes du système d'exploitation client (Windows XP, Windows Vista...) ne pourront pas utiliser la fonctionnalité et imprimeront donc directement sur le serveur placé dans le bureau principal.

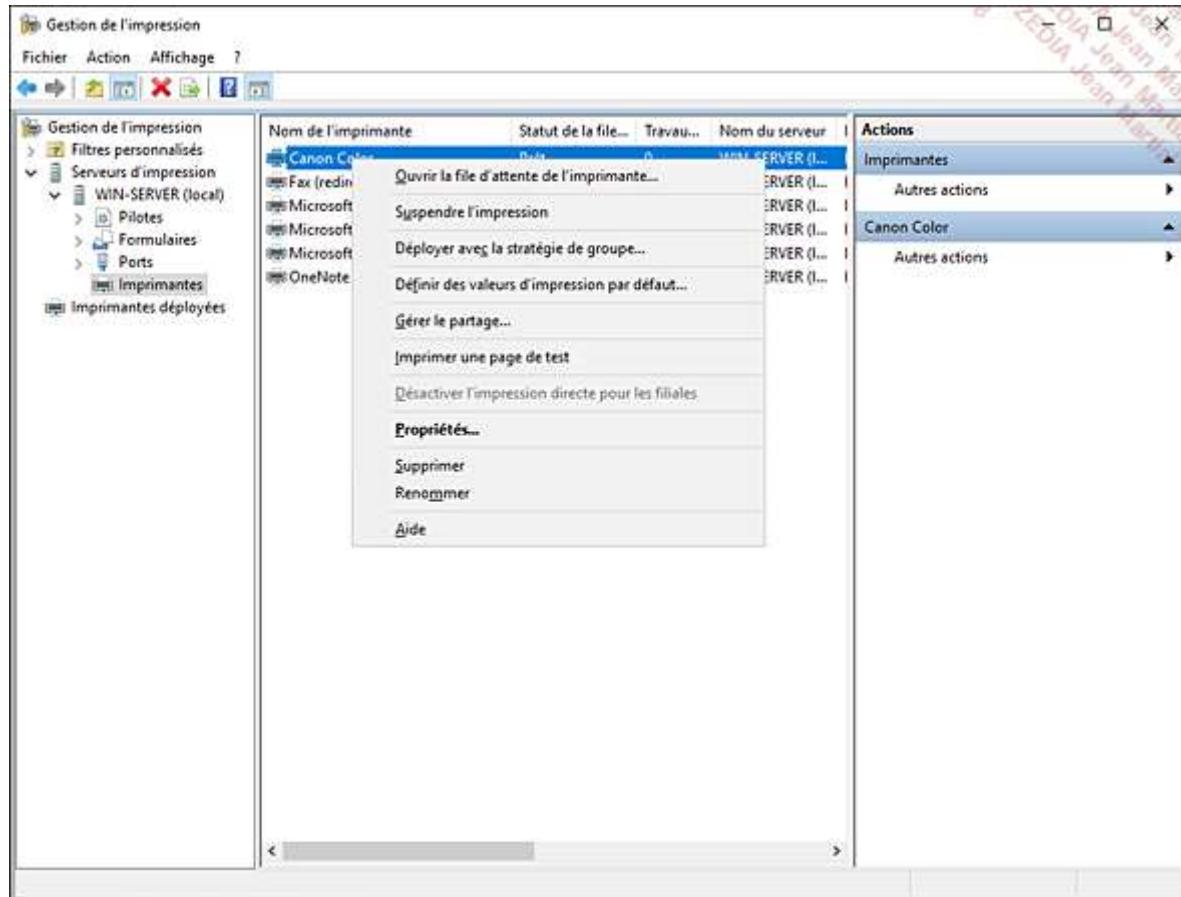
115 Pour configurer cette fonctionnalité, utilisez la console Gestion de l'impression fournie par exemple avec Windows Server, ou bien la commande PowerShell Set-Printer :

Ouvrez une session en tant qu'administrateur sur un serveur Windows Server 2012, puis saisissez la commande Windows PowerShell suivante :

116 Set-Printer -name NomImprimante -ComputerName NomOrdinateur

117 -RenderingMode BranchOffice

118 L'activation du paramètre est visible dans le menu contextuel de l'imprimante.

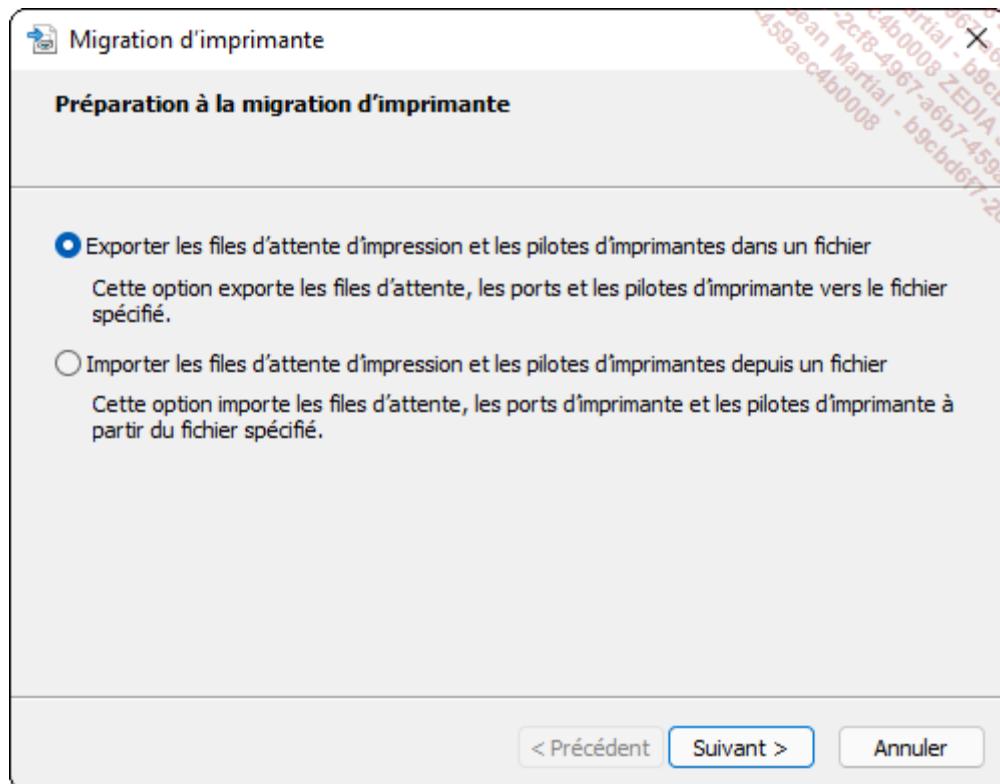


5. Migration d'une imprimante

119 Windows 11 fournit l'assistant **Migration d'imprimante** pour importer (ou exporter) les files d'attente, les ports et les pilotes d'imprimante vers un autre système d'exploitation Microsoft plus récent.

120 L'assistant Migration d'imprimante est accessible depuis le fichier Printbrmui.exe stocké dans le dossier c:\windows\system32. Exécutez ce fichier depuis un Terminal pour exporter les paramètres d'une imprimante :

Depuis l'assistant Migration d'imprimante, cochez la case **Exporter les files d'attente d'impression et les pilotes d'imprimantes dans un fichier**. Validez par **Suivant**.



Sélectionnez la case **Ce serveur d'impression** puis cliquez sur le bouton **Suivant**, vérifiez la liste des éléments à exporter puis cliquez sur **Suivant**. Entrez un dossier de destination pour le fichier portant l'extension **printerExport**. Validez en cliquant sur les boutons **Suivant** et **Terminer**.

- L'assistant Migration d'imprimante est aussi accessible depuis la console Gestion de l'impression, en cliquant avec le bouton droit sur le noeud **Nom du serveur d'impression**, puis en choisissant **Exporter les imprimantes vers un fichier** ou **Importer les imprimantes depuis un fichier**.

6. Impression prenant en charge l'emplacement

121 Windows 11 permet de définir automatiquement l'imprimante par défaut lorsqu'il détecte que l'utilisateur a changé de réseau (filaire ou sans fil).

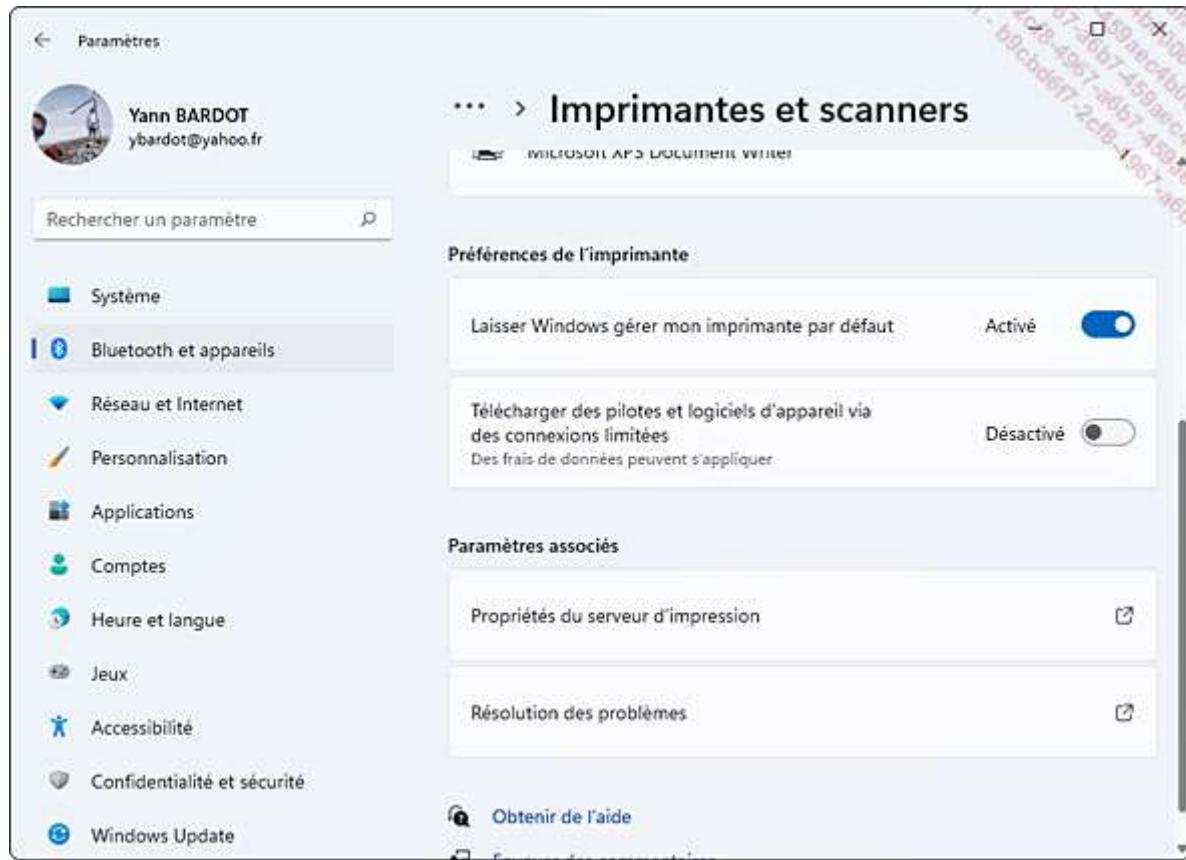
122 Cette fonctionnalité est disponible avec les éditions Professionnel, Entreprise et Education du système et sur des ordinateurs portables uniquement (test de présence d'une batterie).

123 Pour l'utiliser, il suffit de définir une imprimante par défaut, elle sera automatiquement affectée au réseau courant, et ainsi de suite avec les autres imprimantes.

124 Pour gérer les paramètres de l'impression prenant en charge l'emplacement, suivez la procédure ci-dessous :

Cliquez avec le bouton gauche sur le menu **Démarrer** puis sélectionnez **Paramètres**. Double cliquez sur **Bluetooth et appareils**, puis **Imprimantes et scanners**.

Dans la section **Préférences de l'imprimante**, activez le bouton **Laisser Windows gérer mon imprimante par défaut**.



125 Cette fonctionnalité est intéressante car les utilisateurs ne possédant aucune connaissance technique particulière ne contacteront plus le support technique pour configurer leur imprimante lorsqu'ils changeront de réseau, donc de lieu.

Gestion du contenu avec BranchCache

126 La mise à disposition du système d'information d'une entreprise à ses utilisateurs est un processus nécessitant la prise en compte de contraintes de sécurité et de disponibilité. La gestion de contenu a pour objectif la couverture du cycle de vie de l'information : la collecte, l'optimisation, la mise à disposition et l'archivage des données.

127 Bien souvent, la bande passante est fortement sollicitée lors de la mise à disposition des fichiers partagés. Windows 11 propose de mettre en cache certaines informations afin de l'économiser.

1. Présentation de BranchCache

128 Vos liens intersites sont surchargés ? BranchCache est une technologie de mise en cache disponible depuis Windows 7 et Windows Server 2008 R2 (64 bits). Windows 11 (éditions Professionnel, Entreprise ou Education) maintient cette fonctionnalité.

129 Particulièrement utile dans les réseaux séparés par des liens WAN (succursales), BranchCache permet à un client Windows 11 de mettre en cache les données auxquelles il a accédé (pages Internet ou dossiers partagés) auprès d'une succursale, pour les rendre disponibles plus rapidement aux ordinateurs de son propre réseau.

130 Les avantages sont multiples : optimisation de la bande passante et mise à disposition plus rapide des données en cache.

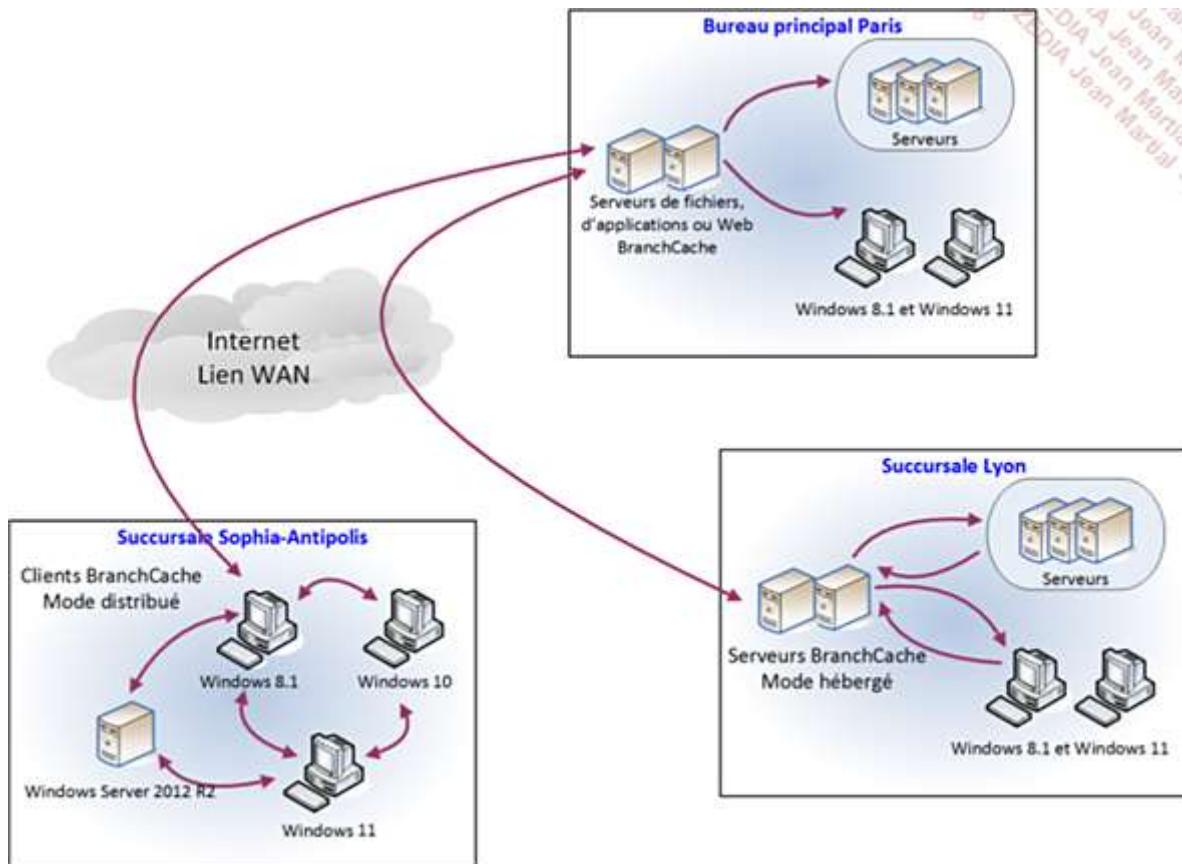
131 Le cache peut être hébergé sur un serveur Windows Server 2008 R2 ou supérieur, situé dans la succursale, ou bien distribué sur les ordinateurs Windows 11 des utilisateurs du réseau. Une succursale peut contenir des serveurs BranchCache configurés en mode hébergé, tandis qu'un autre site peut contenir des clients en mode distribué. Le bureau principal gère quant à lui le serveur BranchCache de contenu, répliqué dans les succursales suivant l'un des deux modes cités précédemment.

132 Un serveur BranchCache peut héberger un contenu accessible depuis les protocoles suivants :

- HTTP et HTTPS (rôle serveur web IIS) permettant l'accès à des sites intranet.
- SMB (*Server Message Block*) pour le partage des dossiers.
- BITS (*Background Intelligent Transfer Service*) pour l'accès à des applications hébergées sur des serveurs.

133 Pour activer BranchCache en mode hébergé sur un serveur Windows, il est nécessaire d'ajouter la fonctionnalité qui porte le même nom pour la gestion des protocoles HTTP/HTTPS et BITS, et le rôle Services de fichier pour la gestion du protocole SMB.

134 Voici un schéma d'implémentation de BranchCache :



135 Le mode distribué est financièrement économique car il ne nécessite pas de serveur.

Les ressources disponibles depuis Internet, telles que des mises à jour de sécurité ou un site visité ne seront pas mises en cache. Seules les données stockées sur les serveurs du réseau local de la société le seront.

2. Mode de cache distribué

136 Le mode de cache distribué est basé sur une architecture pair à pair : le contenu est mis en cache automatiquement sur les clients Windows 11 une fois qu'il a été téléchargé depuis un serveur Windows Server situé dans un autre site.

137 Côté sécurité, les protocoles réseau HTTP(S), SMB et BITS sont supportés et la gestion des accès au cache de la ressource s'effectue en fonction des droits de l'utilisateur. En outre, les transferts entre les clients en mode de cache distribué utilisent un schéma de chiffrement basé sur AES 128. Notez que les éditions Professionnel de Windows prennent en charge uniquement BITS.

138 La procédure d'accès à une ressource BranchCache en mode distribué est simple :

139 1. 140 Le client Windows 11 accède à une ressource située sur un serveur de fichiers Windows Server. Celui-ci, après avoir vérifié ses accès, lui renvoie un ensemble d'identificateurs contenant ce qu'il veut télécharger.

141 2. 142 Le client vérifie ensuite dans son propre réseau local si un autre client possède déjà les données recherchées, à l'aide d'un protocole de multidiffusion en UDP. Dans la négative, il recontacte le serveur pour lui demander la ressource, et la stocke dans son cache local.

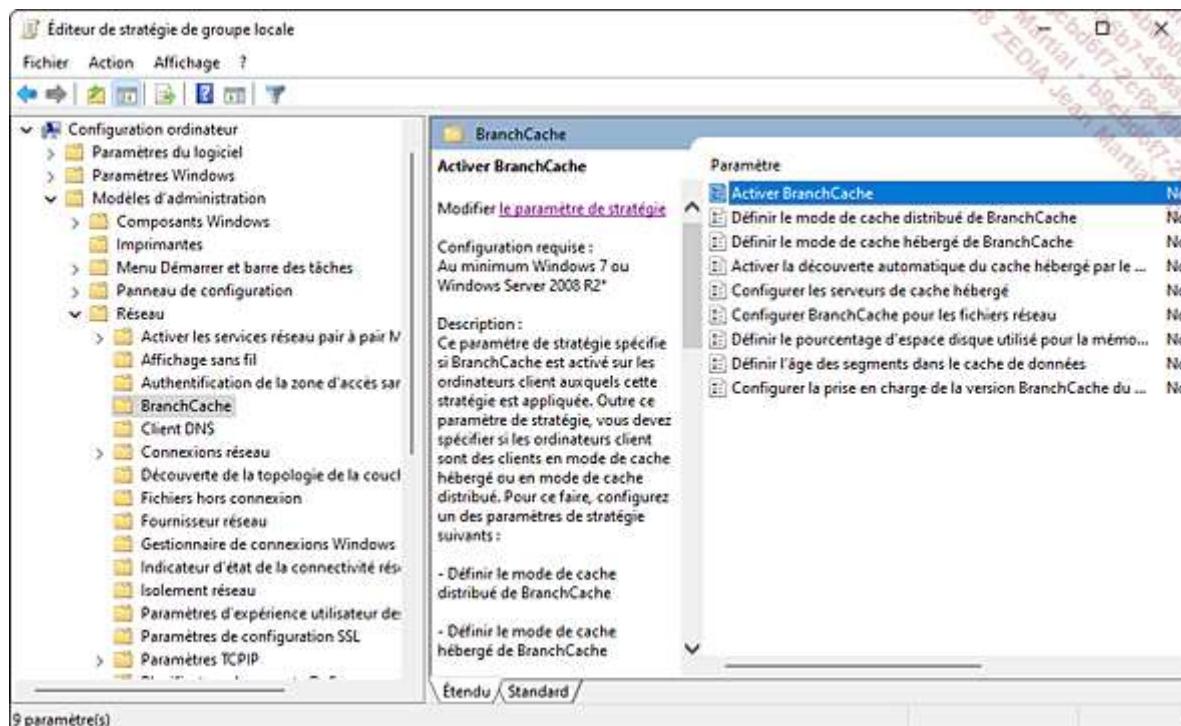
143 3. 144 Si un autre ordinateur souhaite accéder à une ressource déjà stockée sur un client de son réseau, il contactera le serveur de fichiers puis trouvera ce client.

145 Notez que le service BranchCache n'est pas activé par défaut sur Windows 11 mais il est bien entendu possible d'automatiser son lancement grâce à un objet stratégie de groupe.

146 Il est nécessaire de respecter trois étapes pour configurer BranchCache sur un client Windows 11 :

- 147 1. 148 Activer la fonctionnalité.
- 149 2. 150 Choisir le mode de cache (distribué ou hébergé).
- 151 3. 152 Créer des règles dans le pare-feu pour les protocoles BranchCache.
- 153 Procédez dans l'ordre, car le choix du mode de cache n'activera pas BranchCache.
- 154 L'activation de BranchCache sur un poste Windows 11 s'effectue au travers d'une stratégie de groupe locale grâce à la procédure ci-dessous :

Depuis le bureau, pressez les touches  et R et saisissez gpedit.msc dans la fenêtre **Exécuter** puis validez par la touche [Entrée]. Depuis l'arborescence de la console Éditeur de stratégie de groupe locale, développez les nœuds **Configuration ordinateur - Modèles d'administration - Réseau**, puis cliquez sur **BranchCache**.



Double cliquez sur **Activer BranchCache** et cliquez sur la case **Activé** puis validez par le bouton **OK**.

- 155 Pour activer le mode de cache distribué :

Double cliquez sur le paramètre **Définir le mode de cache distribué de BranchCache**, sélectionnez l'option **Activé** puis cliquez sur **OK**.

- 156 Il est aussi possible d'activer BranchCache en mode de cache distribué à l'aide de la commande netsh.exe exécutée en tant qu'administrateur local :

- Netsh branchcache set service mode=distributed

```
PS C:\Users\ybard> netsh branchcache set service mode=distributed
Définition du type de démarrage du service sur Manuel... Réussite
Définition du mode de service... Réussite

PS C:\Users\ybard>
PS C:\Users\ybard>
PS C:\Users\ybard>
PS C:\Users\ybard>
```

157 L'utilisation de cette commande configure automatiquement le pare-feu pour autoriser les flux nécessaires au fonctionnement de BranchCache.

Windows PowerShell propose également des commandes afin de configurer BranchCache. Pour les visualiser, tapez : Get-Command -Module BranchCache

Pour vérifier les paramètres de la machine, saisissez : Get-BCStatus

158 Pour résoudre les problèmes liés à l'utilisation de BranchCache, un journal des opérations est disponible depuis l'**Observateur d'événements** :

Dans la zone de recherche située sur la barre des tâches, saisissez observateur et sélectionnez **Observateur d'événements**. Développez **Journaux des applications et des services - Microsoft - Windows - BranchCache - Opérationnel**.

Notez qu'un client peut utiliser le mode de cache soit hébergé, soit distribué, mais pas les deux à la fois.

159 Bien implémenté, BranchCache est donc transparent pour l'utilisateur et optimise efficacement la bande passante.

Gestion des périphériques BYOD

160 Windows 11 apporte plusieurs solutions pour gérer les périphériques personnels des salariés de l'entreprise. La sécurité des accès aux ressources est un des problèmes majeurs de cette nouvelle tendance. La prolifération d'appareils tels que les tablettes tactiles Android ou les smartphones Apple engendre des problématiques de gestion.

161 L'utilisateur a besoin d'accéder à l'intranet, à sa messagerie électronique, aux données partagées ou encore aux bases de données de l'entreprise.

162 Le principal obstacle à la mise en place BYOD porte sur l'hétérogénéité des systèmes d'exploitation mobiles. Windows 11, grâce au support de l'Open MDM (*Mobile Device Management*), assure la gestion d'appareils mobiles.

163 Ainsi, les administrateurs peuvent contrôler et inventorier le parc BYOD, en dépannant à distance les terminaux et en forçant le déploiement de logiciels de sécurité.

164 Windows 11 supporte le protocole OMA Device Management pour la gestion des appareils mobiles, ainsi, les produits tiers tels que Mobile Iron ou Air Watch pourront gérer les périphériques Windows 11.

165 Microsoft, de son côté, propose Intune aux administrateurs, afin de leur permettre de gérer des appareils ainsi que des applications mobiles tout en offrant des fonctionnalités de gestion d'ordinateurs dans le cloud.

1. Accès professionnel

166 Auparavant, un ordinateur était membre d'un domaine ou non. Si ce n'était pas le cas, il était difficile pour une personne étrangère à l'entreprise d'accéder aux ressources de celles-ci. Accès professionnel est une fonctionnalité qui abolit cette frontière en proposant à l'utilisateur qui apporte son propre matériel d'accéder aux ressources du domaine, tout en ayant son appareil partiellement géré par un administrateur.

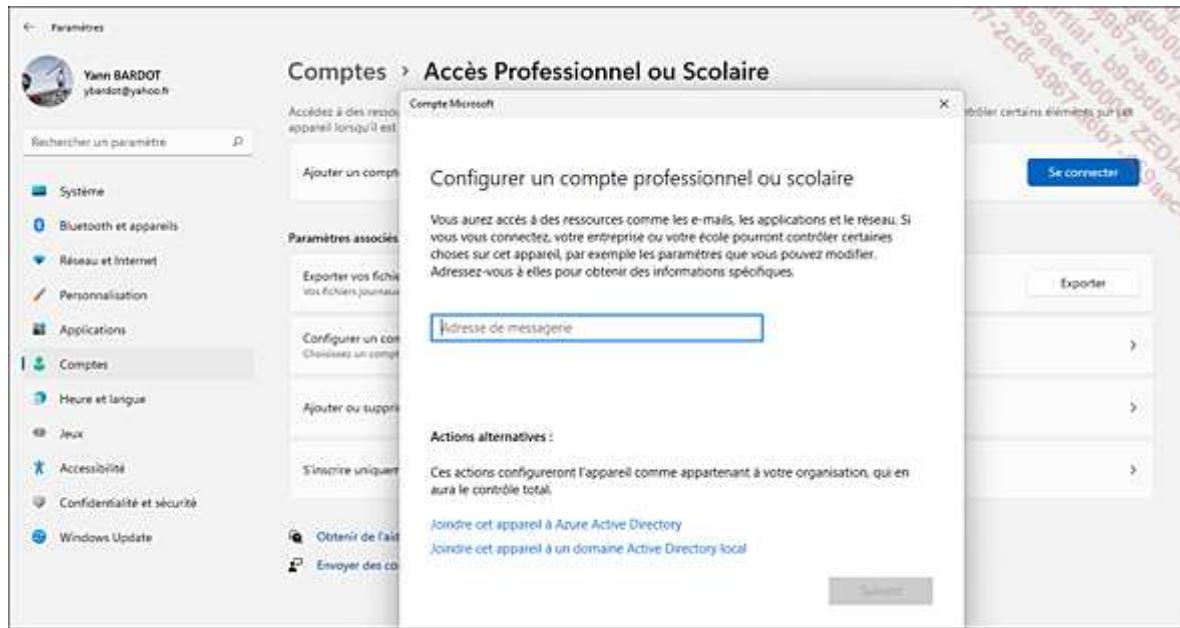
167 L'enregistrement de son matériel ne peut être forcé et est donc obligatoirement à l'initiative de son propriétaire.

168 Grâce à une infrastructure gérée par un serveur Windows Server pourvu du rôle ADFS (*Active Directory Federation Services*), un poste Windows 11 peut être partiellement joint à un domaine Active Directory. Il est bien entendu nécessaire que l'utilisateur possède un identifiant de domaine.

169 Voici la procédure :

Cliquez sur le menu **Démarrer** puis sur **Paramètres**. Sélectionnez ensuite **Comptes**. Cliquez sur **Accès Professionnel ou Scolaire** puis cliquez sur le bouton **Se Connecter**.

Entrez l'adresse e-mail (professionnelle ou scolaire) préinscrit par l'administrateur de l'entreprise et cliquez sur **Suivant**.



170 Après quelques instants, un message apparaît indiquant que votre société ou votre école procède à l'inscription de votre appareil.

Lorsque l'écran **Vous voilà prêt !** s'affiche, cliquez sur **Fermer**. Votre ordinateur est désormais joint au service Intune.

2. Dossiers de travail

171 La fonctionnalité Dossiers de travail (ou *Work Folders*) permet à un utilisateur disposant de son matériel personnel de synchroniser ses fichiers entre plusieurs PC ou appareils, qu'ils soient joints à un domaine Microsoft ou non. Windows 11 Professionnel, Entreprise et Education supportent cette fonctionnalité.

172 Contrairement à l'App OneDrive dont les données sont stockées dans le cloud, celles gérées par Dossiers de travail le sont sur un serveur Windows Server 2012 R2 ou supérieur. L'entreprise garde ainsi la maîtrise de l'emplacement et de la confidentialité des documents.

173 En cas d'absence de connectivité à l'intranet de l'entreprise ou au réseau Internet, l'utilisateur travaillera sur des données stockées localement. Dès la connexion rétablie, elles seront automatiquement synchronisées. Grâce au système de fichiers NTFS, l'administrateur peut attribuer des quotas afin d'empêcher que l'espace disque sur les serveurs soit rapidement surchargé. La bande passante est ainsi préservée. Les utilisateurs peuvent chiffrer leurs documents et profiter des fonctions de haute disponibilité fournies par Windows Server afin d'accéder à tout moment à leurs données.

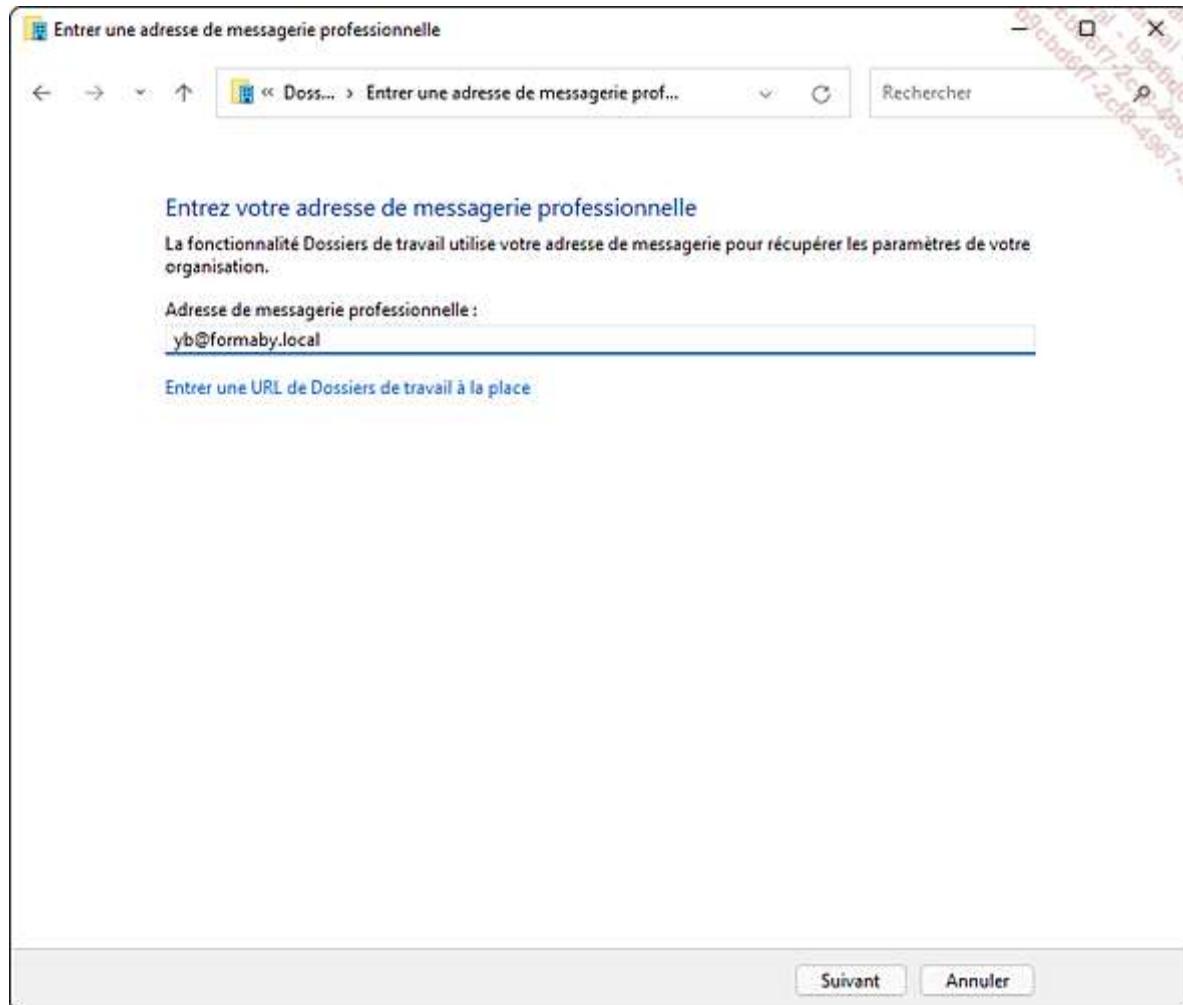
174 Côté serveur, la fonctionnalité nécessite l'installation des rôles AD DS (*Active Directory Domain Services*), DNS, Services de fichiers et de stockage et le sous-rôle Dossiers de travail.

175 Côté client Windows 11, les données synchronisées de l'utilisateur sont stockées par défaut dans le dossier %USERPROFILE%\Dossiers de travail. Un espace disque libre suffisant pour héberger les documents est à prévoir, ainsi que 6 Go supplémentaires minimum si le répertoire Dossiers de travail est stocké sur la partition système (par défaut). Un périphérique USB formaté avec le système de fichiers NTFS peut aussi être utilisé.

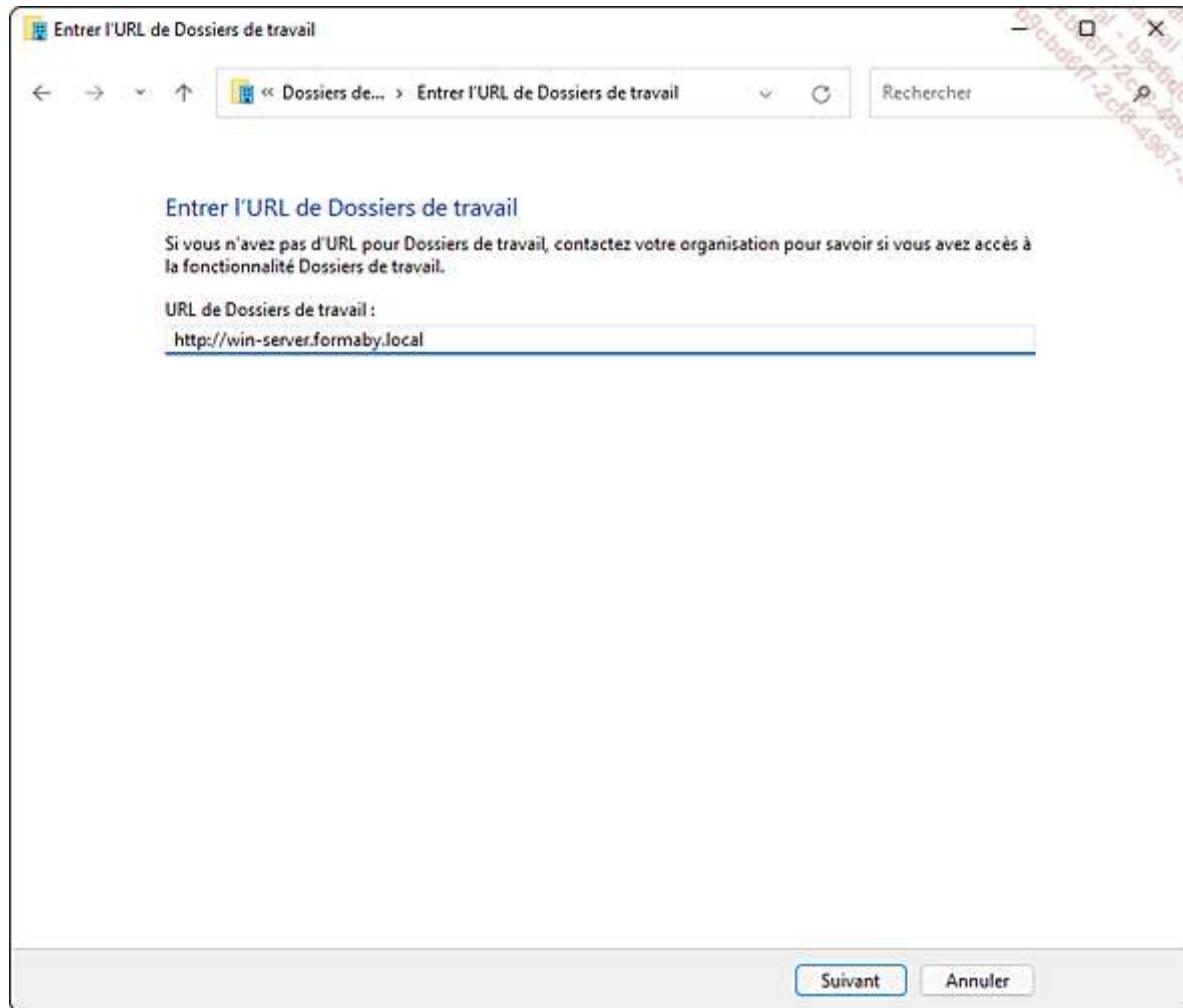
176 Enfin, sachez que, par défaut, la taille maximum d'un fichier individuel ne peut excéder 10 Go.

177 Pour configurer la fonctionnalité Dossiers de travail sur Windows 11, suivez la procédure ci-dessous :

Saisissez panneau de configuration depuis le champ de recherche de la barre des tâches. Cliquez avec le bouton gauche sur le résultat. Double cliquez sur **Dossiers de travail** puis sur **Configurer Dossiers de travail**. Saisissez votre adresse de messagerie professionnelle puis votre identifiant et mot de passe Active Directory.



Définissez le chemin d'accès vers votre dossier Dossiers de travail puis cliquez sur le bouton **Suivant**. Il vous sera fourni par l'administrateur du domaine. Si votre machine n'est pas inscrite au domaine, il vous faudra néanmoins un compte utilisateur du domaine.



178 L'accès HTTPS nécessite la présence d'un certificat. Néanmoins, il est possible d'autoriser l'accès HTTP en ajoutant la clé de registre suivante :

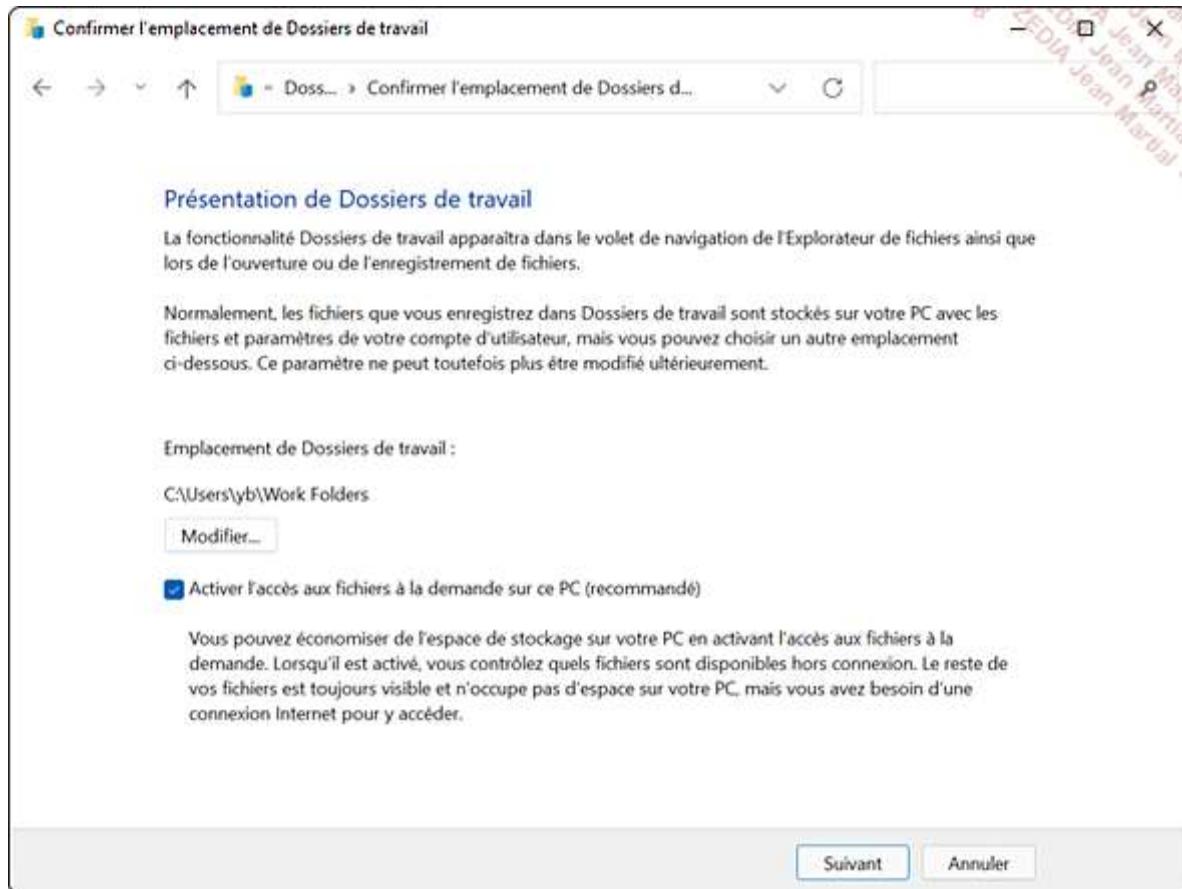
Ouvrez l'éditeur de registre depuis un Terminal en tant qu'administrateur (regedit).

Développez l'arborescence **HKLM - Software - Microsoft - Windows - CurrentVersion** et créez une clé de registre **WorkFolders**.

Créez une clé **DWORD** nommée **AllowUnsecureConnection**.

Éditez-la avec la valeur 1. Fermez le registre et redémarrez la machine.

Le panneau suivant permet de configurer le dossier local de stockage des fichiers synchronisés et de définir les fichiers à rendre disponibles. Si besoin modifiez les paramètres et cliquez sur le bouton **Suivant**.



En cochant l'option **J'accepte ces stratégies sur mon ordinateur**, l'administrateur de l'entreprise peut forcer l'authentification par mot de passe lors d'une ouverture de session, chiffrer les données stockées dans le dossier **Dossiers de travail** ou encore les effacer à distance lors du vol de votre ordinateur. Cliquez sur les boutons **Configurer Dossiers de travail** puis **Fermer** pour terminer la configuration.

179 Depuis le Panneau de configuration, en cliquant sur l'icône **Dossiers de travail**, l'utilisateur peut visualiser la date de la dernière synchronisation, synchroniser les fichiers sur des connexions limitées, communiquer avec le support technique au sein de l'organisation ou encore visualiser l'espace disque disponible sur le serveur :

The screenshot shows the 'Dossiers de travail' (Work Folders) configuration page. On the left, there's a sidebar with links like 'Page d'accueil du panneau de configuration', 'Arrêter d'utiliser Dossiers de travail', 'Gérer les informations d'identification', and 'Synchroniser maintenant'. The main area has a title 'Gérer Dossiers de travail' with a sub-instruction: 'Utilisez Dossiers de travail pour rendre vos fichiers de travail disponibles sur tous les appareils que vous utilisez, même hors connexion.' Below this, it displays '111 Go disponible(s) sur le serveur'. A large green box contains configuration settings: 'Dernière synchronisation : 16/08/2021 15:45', 'Accès à un fichier à la demande : Activé', 'Synchroniser sur des connexions limitées : Non', 'Synchroniser même quand je suis en itinérance : Non', 'Demander de l'aide à votre organisation : Non', 'Envoyer un message électronique au support technique : Non', and 'Configurer des Dossiers de travail sur d'autres appareils : Découvrir la procédure'. At the bottom, a green box says 'Aucune erreur de fichier'.

180 Le menu situé à gauche de l'interface permet d'arrêter la synchronisation *Work Folders*, de gérer les informations d'identification en cas de changement de mot de passe de l'utilisateur, et enfin de pouvoir effectuer une synchronisation manuelle des données.

181 L'accès au dossier synchronisé s'effectue depuis l'Explorateur de fichiers, en dessous de l'accès rapide : une section **Dossiers de travail** est apparue. Les dossiers de travail peuvent également apparaître comme un lecteur réseau supplémentaire.

The screenshot shows the Windows File Explorer interface. The left sidebar lists 'Accès rapide', 'Dossiers de travail' (which is selected and highlighted in blue), 'Nouveau dossier', 'OneDrive', 'Ce PC', 'Bureau', 'Documents', 'Images', 'Musique', 'Téléchargements', 'Vidéos', and 'Disque local (C:)'. The main pane shows a table of files in the 'Dossiers de travail' folder:

Nom	Statut	Modifié le	Type	Taille
Nouveau dossier	Cloud	16/08/2021 15:48	Dossier de fichiers	
test.txt	Cloud	10/07/2021 17:57	Document texte	3 Ko

At the bottom, it says '2 élément(s) Statut de la synchronisation : Dernière synchronisation : 17/08/2021 15:24'.

182 Combiné à la fonctionnalité Accès professionnel, *Work Folders* offre une gestion affinée des utilisateurs hors domaine et des périphériques qu'ils utilisent.

Résumé du chapitre

- Windows 11 propose des outils permettant d'en faciliter la gestion, tels que l'accès au poste à distance, le contrôle d'intégrité, le déploiement et le partage d'imprimantes ou encore la gestion de contenu.
- Windows 11 propose en effet d'utiliser des consoles MMC et des outils RSAT pour gérer l'accès à distance à des fonctionnalités et les rôles de serveurs.
- La fonctionnalité de Bureau à distance permet également d'accéder à un ordinateur distant comme si l'utilisateur était physiquement face à lui, tandis que l'Assistance à distance offre à l'utilisateur le choix de demander de l'aide à un administrateur, sans perdre sa session courante.
- Microsoft propose en téléchargement depuis le Microsoft Store l'application gratuite Bureau à distance dont le principal avantage est de regrouper dans un emplacement centralisé les connexions actives.
- RemoteFX s'appuie sur le protocole RDP pour offrir une expérience utilisateur améliorée dans le cas d'une connexion distante : prise en compte de l'affichage de vidéos, redirection des périphériques (imprimante, caméra) ou écoute de musique.
- Windows PowerShell combine un langage de script et un interpréteur de ligne de commande permettant de gérer et automatiser les actions d'administration sur les systèmes Microsoft. Avec Windows 11, Microsoft développe une fonctionnalité dans Windows PowerShell, nommée DSC : l'administrateur peut désormais gérer le déploiement et la configuration de plusieurs environnements de manière automatisée.
- Les utilisateurs itinérants peuvent rétablir automatiquement la connexion VPN au réseau de l'entreprise en cas de coupure temporaire internet, et ce sans aucune interaction de l'utilisateur.
- La fonctionnalité DirectAccess est similaire à la reconnexion automatique VPN, car elle propose de connecter automatiquement l'utilisateur itinérant au réseau de l'entreprise, sans intervention de celui-ci mais cette fois... sans connexion VPN.
- Enfin, SSTP, qui est un type de tunnel VPN disponible depuis Windows Server 2008, permet l'encapsulation de paquets PPP dans le protocole HTTPS.
- Windows 11 simplifie grandement le déploiement des imprimantes sur les clients membres d'un domaine Active Directory grâce à la console Gestion de l'impression. La fonctionnalité Impression directe pour les filiales réduit l'utilisation de la bande passante lorsqu'un utilisateur souhaite imprimer un document sur un périphérique d'impression placé dans une succursale et géré par un serveur situé dans un bureau principal : les données d'impression sont directement transmises du poste Windows 11 vers l'imprimante puis mises en cache dans la filiale.
- Windows 11 permet de définir automatiquement l'imprimante par défaut lorsqu'il détecte que l'utilisateur a changé de réseau filaire ou sans fil : c'est l'impression prenant en charge l'emplacement.
- La gestion des imprimantes 3D est fournie avec toutes les éditions de Windows 11, ainsi qu'une App de CAO nommée 3D Builder, téléchargeable depuis le magasin Microsoft.
- Windows 11 propose la fonctionnalité Wi-Fi Direct Printing permettant d'imprimer directement depuis un périphérique vers une imprimante, et ce sans point d'accès intermédiaire ou routeur sans fil.

- BranchCache permet à un client Windows 11 de mettre en cache les données auxquelles il a accédé (pages internet ou dossiers partagés) auprès d'une succursale, pour les rendre disponibles plus rapidement aux ordinateurs de son propre réseau.
- Afin de répondre aux problématiques du BYOD, Microsoft propose deux fonctionnalités : Accès professionnel et Dossiers de travail.
- Accès professionnel est une fonctionnalité qui propose à l'utilisateur d'apporter son propre matériel au sein de l'entreprise, afin d'accéder aux ressources du domaine, tout en ayant son appareil partiellement géré par un administrateur.
- La fonctionnalité Dossiers de travail (*Work Folders*) permet à un utilisateur disposant de son matériel personnel de synchroniser ses fichiers entre plusieurs PC ou appareils, qu'ils soient joints à un domaine Microsoft ou non.

Configuration de la sécurité Windows

Protection des postes de travail Windows 11

Avec l'avènement des interconnexions entre les réseaux privés et publics, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires.

Il devient donc primordial de connaître les ressources critiques et de protéger les postes de travail fixes et itinérants des collaborateurs de l'entreprise.

Lorsque l'administrateur souhaite mettre en place une architecture sécurisée, il doit tout d'abord connaître les forces en présence en évaluant ses propres compétences, rédiger une documentation détaillée du système d'information (SI) et maîtriser la prise en charge organisationnelle. La seconde étape consiste à oublier les stéréotypes pour se mettre à la place de l'attaquant, en essayant de connaître ses motivations : un employé mécontent, de l'espionnage pour obtenir des gains financiers, une réponse à un défi...

L'administrateur sécurité doit défendre tous les points de son SI en étant vigilant en permanence, alors que le pirate informatique peut choisir le point le plus faible en attaquant quand il le souhaite. Les différents réseaux doivent être contrôlés et sécurisés : le réseau local, le réseau distant et les partenaires professionnels du type extranet, afin de se prémunir d'une surveillance du réseau, d'une usurpation d'identité ou d'une modification des données...

Le système Windows 11 possède les mêmes bases de sécurité que Windows 10, qui lui-même les tenait de Windows 7, comme le contrôle d'accès utilisateur ou le Centre de notifications, mais apporte des améliorations sur les fonctionnalités AppLocker et BitLocker.

Certaines fonctionnalités de Windows 10 ont été conservées : Credential Guard et Device Guard.

En outre, la fonctionnalité WIP (*Windows Information Protection*) a remplacé EDP (*Enterprise Data Protection*).

Grâce à celle-ci, l'administrateur peut créer une stratégie de protection selon quatre niveaux :

0 - Désactivée. La fonctionnalité WIP n'est pas active et ne protège pas les données de l'entreprise.

1 - Audit : WIP enregistre le partage inapproprié de données, sans rien interdire. Il s'agit d'un mode silencieux.

2 - Remplacer : l'utilisateur est informé d'un partage inapproprié mais il peut choisir de remplacer la stratégie mise en place.

3 - Bloquer : si un partage inapproprié est détecté, l'utilisateur se verra refuser son action.

À tout moment, un employé peut changer le statut d'un document WIP en document personnel. Toutefois, cette action sera auditée et journalisée afin que l'administrateur la valide.

L'authentification par empreinte digitale, par iris ou via le visage de l'utilisateur est désormais intégrée (cf. chapitre Installation du client Windows 11, section Authentification) au système d'exploitation, et permet donc de s'affranchir des pilotes ou applicatifs fournis par les fabricants. De plus, l'achat d'Apps dans le magasin Microsoft Store est géré, ainsi qu'une ouverture de session par ce biais dans un domaine Active Directory.

1. Contrôle de compte d'utilisateur

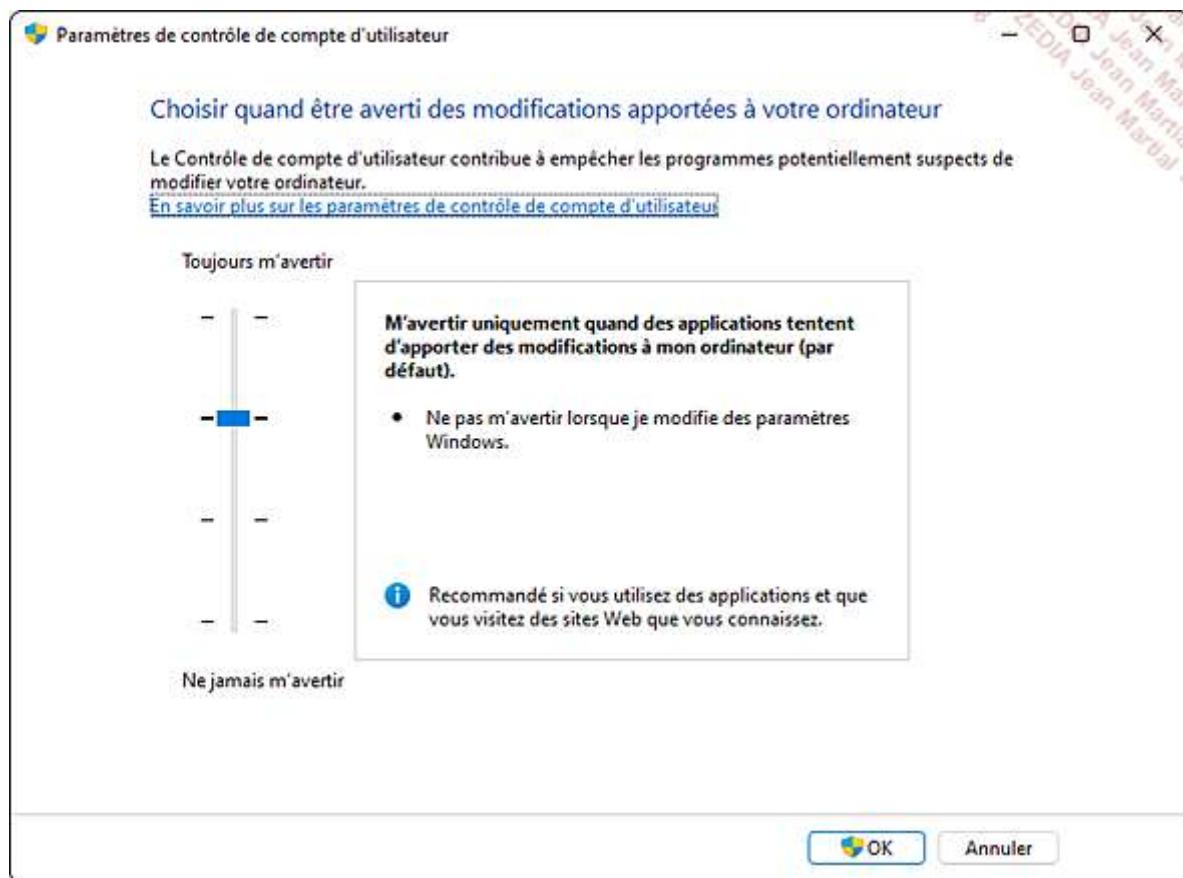
L'**UAC** (*User Account Control*) est une fonctionnalité de sécurité ayant pour but d'encadrer les manipulations sensibles en proposant à un utilisateur standard d'élever son statut, jusqu'à être administrateur durant la réalisation d'une tâche spécifique. Disponible depuis Windows Vista, l'UAC était décrié pour le ralentissement qu'il induisait dans l'accomplissement des tâches courantes. Avec Windows 7 et Windows 8.1, de nombreuses invites d'élévation ont été supprimées et les paramètres de configuration ont été étendus à quatre niveaux modulables.

Lorsqu'un bouclier jaune et bleu  apparaît à côté d'un paramètre, cela signifie que le système Windows 11 requiert que l'utilisateur courant ait les priviléges administrateur pour y accéder, donc qu'il élève temporairement son niveau d'accès. Néanmoins, un utilisateur peut entreprendre un grand nombre d'actions sans avoir besoin d'élever ses priviléges, telles que l'installation des mises à jour de sécurité, la configuration des paramètres réseau, la personnalisation de l'ordinateur (fond d'écran, thème, etc.) ou encore la restauration de fichiers sauvegardés. Parfois, il pourra visualiser des paramètres, comme les règles créées sur le pare-feu, mais leur modification nécessitera une élévation de priviléges.

Pour configurer l'UAC, il est nécessaire de s'authentifier à l'aide d'un compte administrateur local sur le système Windows 11 :

Saisissez panneau de configuration dans la zone de recherche située dans la barre des tâches, puis cliquez sur **Panneau de configuration** et sur **Comptes d'utilisateur**.

Sélectionnez **Modifier les paramètres de contrôle de compte d'utilisateur**.

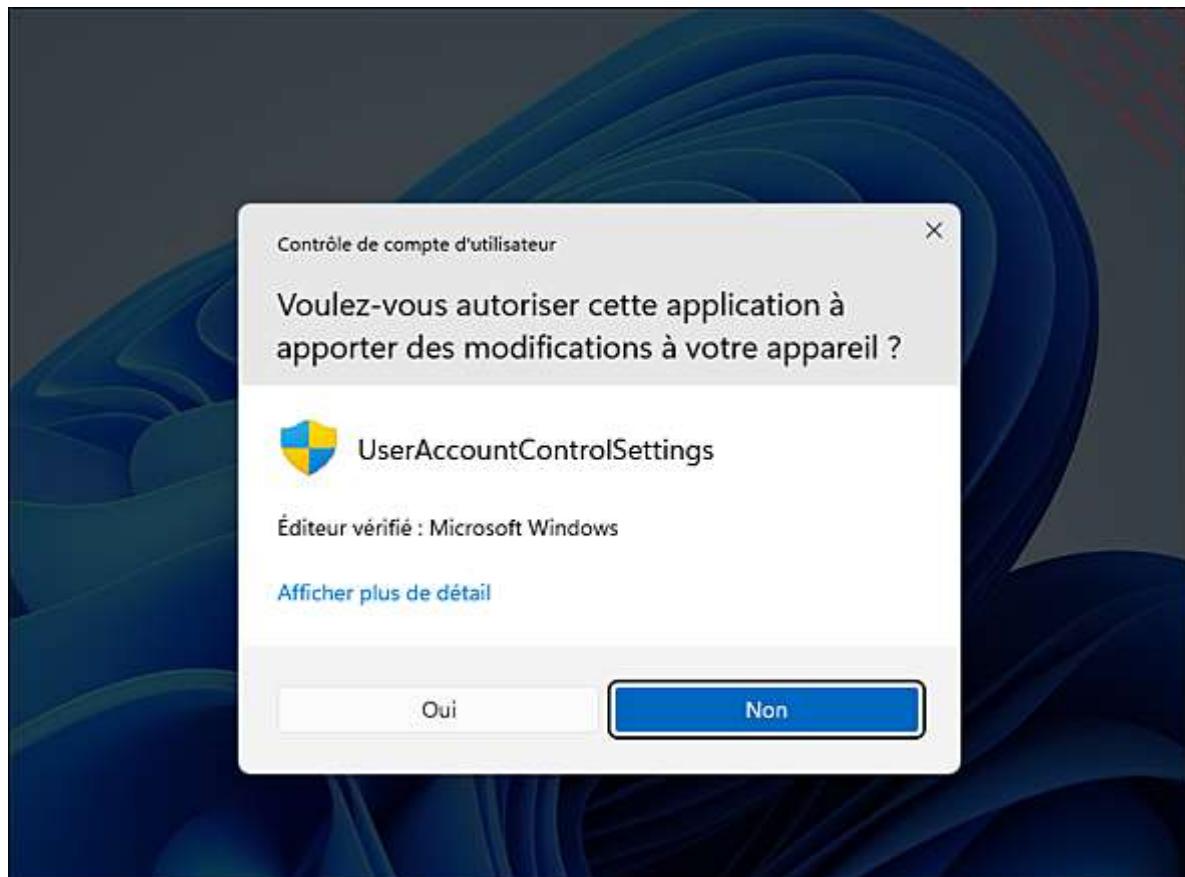


Vous pouvez configurer l'UAC en déplaçant le curseur suivant quatre niveaux :

- **Toujours m'avertir** : niveau d'avertissement le plus sensible, l'utilisateur recevra un message si des programmes ou lui-même tentent de modifier des paramètres Windows sensibles.
- **M'avertir uniquement quand des programmes tentent d'apporter des modifications à mon ordinateur (par défaut)** : niveau par défaut, qui n'affiche pas de message lorsque c'est l'utilisateur qui modifie des paramètres.
- **M'avertir uniquement quand des applications tentent d'apporter des modifications à mon ordinateur (ne pas estomper mon Bureau)** : même paramètre que le précédent, à l'exception que la boîte de dialogue d'avertissement n'estompera pas le bureau. L'utilisateur pourra ainsi plus facilement ignorer les messages.

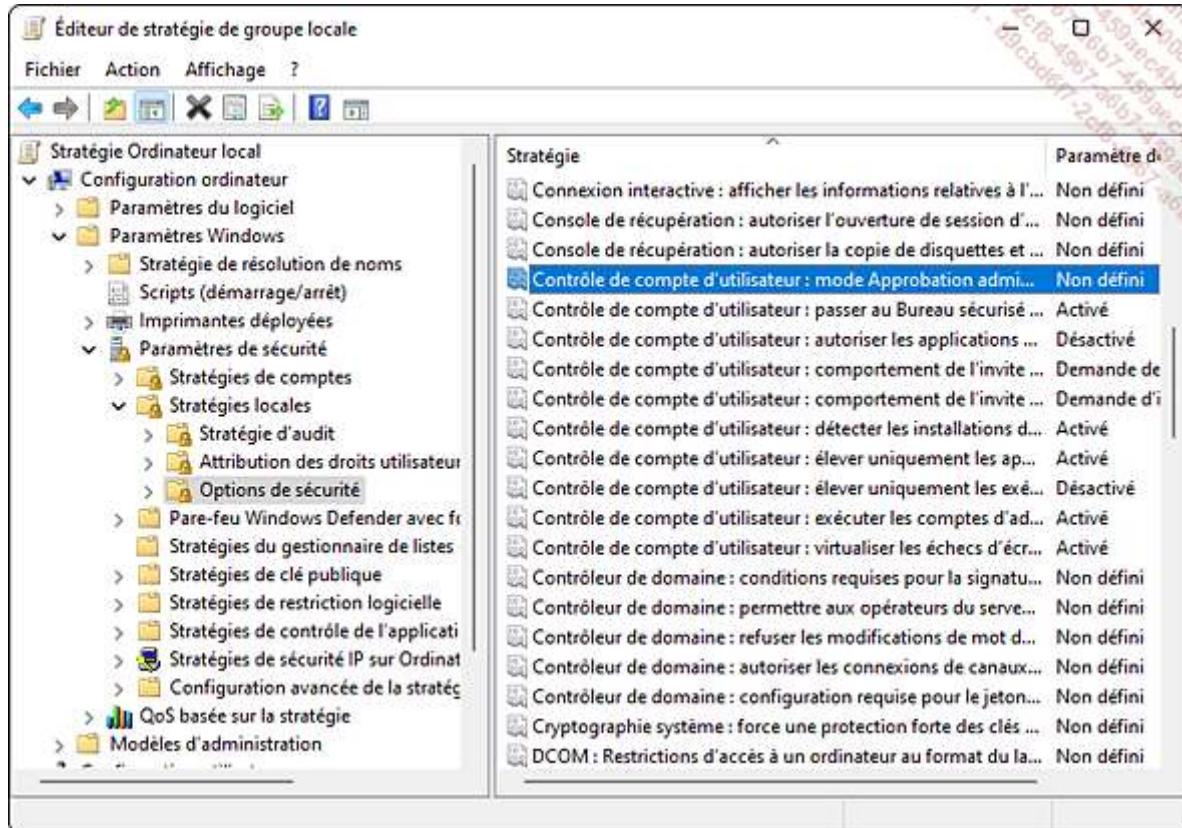
- **Ne jamais m'avertir** : niveau le plus bas et le moins sécurisé, aucun avertissement ne sera affiché si une application procérait à des modifications. Si l'utilisateur courant utilise un compte non administrateur, tout changement nécessitant des priviléges administrateur sera interdit.

En cliquant sur le bouton **OK** dans la fenêtre de validation **Contrôle de compte d'utilisateur**, l'utilisateur demande une élévation de priviléges pour devenir administrateur local du poste Windows 11 :



Dans un domaine Active Directory, l'administrateur peut configurer le comportement de l'UAC sur les postes clients à l'aide d'un objet stratégie de groupe. Il est ainsi possible de configurer le comportement du système lors de l'installation d'application, avec des paramètres GPO comme **Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation**, ou la stratégie **Contrôle de compte d'utilisateur : éléver uniquement les exécutables signés et validés**.

Dans un domaine, en pratique, il suffit d'éditer l'objet stratégie de groupe **Stratégie de domaine par défaut**, puis de développer le nœud **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies locales et Options de sécurité**. Repérez les paramètres commençant par **Contrôle de compte d'utilisateur**.



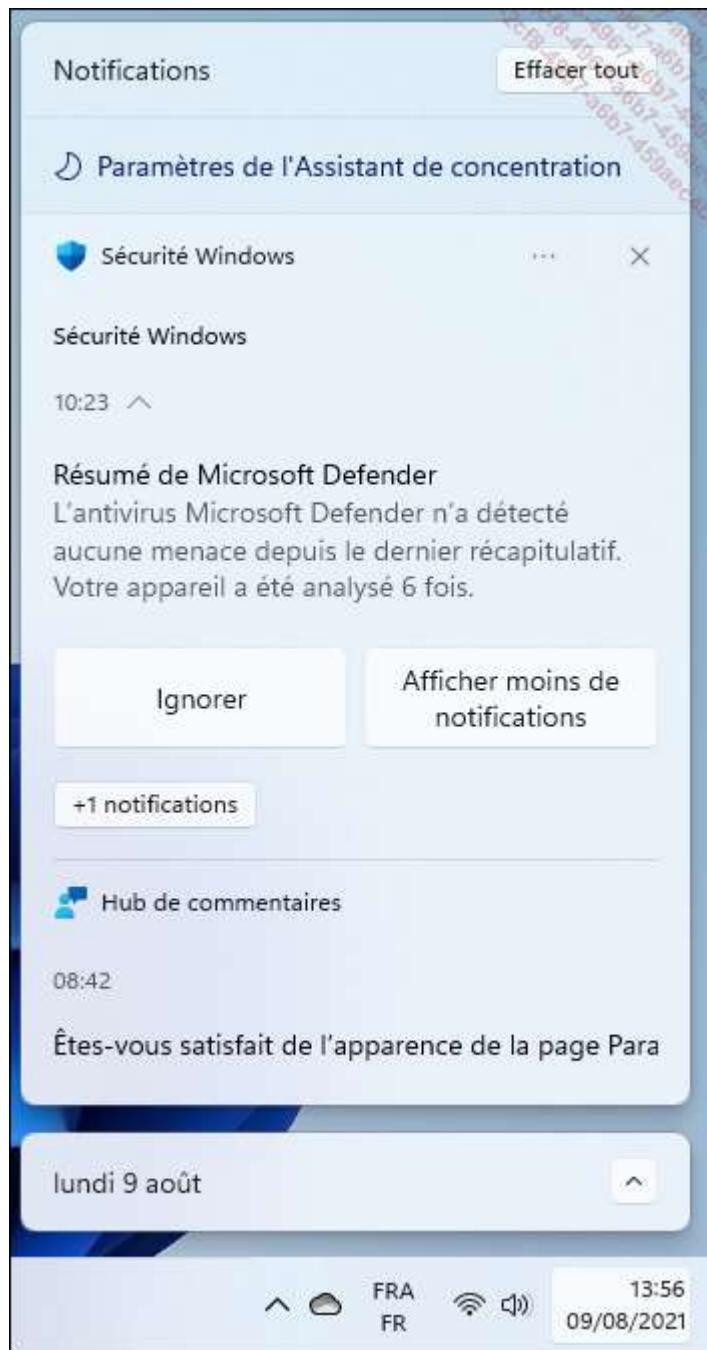
- Ces paramètres peuvent être configurés localement sur le système Windows 11, grâce à l'Éditeur de stratégie de groupe locale (gpedit.msc), comme le montre l'image ci-dessus.

L'UAC contribue donc à empêcher les programmes malveillants de types virus et chevaux de Troie de s'installer sur le poste Windows 11, en restreignant l'usage de priviléges élevés, et en contrôlant les fichiers d'installation (ActiveX, Windows Installer...), la base de registre et bien d'autres paramètres critiques du système.

2. Centre de notifications

Le Centre de notifications affiche dans une vue centrale des alertes récentes concernant la sécurité du client Windows 11, ainsi que la modification de paramètres importants (réseau, localisation, VPN, etc.) liés au système. Avec Windows 11, cette console a été séparée des paramètres rapides.

Les paramètres de sécurité sont surveillés, tels que l'état du pare-feu, l'application des mises à jour de sécurité, les définitions de virus ou bien encore la maintenance de l'ordinateur. Les messages d'avertissement sont affichés dans la zone de notification située en bas à droite de l'écran du bureau, dans la barre des tâches, au-dessus de l'heure comme le montre l'image ci-dessous :



Le Centre de notifications est personnalisable en effectuant un clic avec le bouton droit sur l'heure, puis sur **Paramètres des notifications**. Il est en effet possible d'activer ou désactiver les notifications application par application :

The screenshot shows the Windows 11 Settings app with the following interface details:

- Header:** Système > Notifications
- Left sidebar:** A navigation tree with "Système" selected, followed by "Bluetooth et appareils", "Réseau et Internet", "Personnalisation", "Applications", "Comptes", "Heure et langue", "Jeux", "Accessibilité", "Confidentialité et sécurité", and "Windows Update".
- Search bar:** "Rechercher un paramètre" at the top left.
- Main content area:**
 - Notifications section:** Shows a toggle switch labeled "Activé" for "Notifications" (Obtenir les notifications des applications et des autres expéditeurs).
 - Assistant de concentration section:** Shows a link to "Assistant de concentration" with a description "Contrôlez les temps dans lesquels vous recevez ou non des notifications".
 - Notifications provenant d'applications et d'autres expéditeurs:** A list of notifications from various sources, each with a toggle switch:
 - VPN (Bannières, Sons)
 - Capture d'écran et croquis (Bannières, Sons)
 - Hub de commentaires (Bannières, Sons)
 - Microsoft Store (Bannières, Sons)

Si des catégories de messages devaient ne plus être affichées, il suffirait à l'administrateur de cliquer sur **Sécurité et maintenance** depuis le panneau de configuration et de sélectionner les messages de maintenance ou de sécurité gérés par Windows 11 :

The screenshot shows the Windows Security & Maintenance panel. On the left, there's a sidebar with links like 'Page d'accueil du panneau de configuration', 'Modifier les paramètres du centre Sécurité et maintenance', 'Modifier les paramètres du contrôle de compte d'utilisateur', and 'Afficher les messages archivés'. The main area has sections for 'Examiner les messages récents et résoudre les problèmes' (with a note: 'Aucun problème n'a été détecté par le centre Sécurité et maintenance.'), 'Sécurité' (with 'Pare-feu du réseau' and 'Afficher dans Sécurité Windows'), 'Protection antivirus' (with 'Afficher dans Sécurité Windows'), 'Paramètres de sécurité Internet' (status: 'OK', note: 'Tous les paramètres de sécurité Internet sont réglés à leurs niveaux recommandés.'), 'Contrôle de compte d'utilisateur' (status: 'Activé', note: 'Le contrôle de compte d'utilisateur vous avertit quand des applications tentent d'apporter des modifications à l'ordinateur.', with a 'Modifier les paramètres' link), and 'Comment savoir quels paramètres de sécurité conviennent à mon ordinateur?'. Below this is a 'Maintenance' section with 'Signaler des problèmes' (status: 'Activé', with a 'Afficher l'historique de fiabilité' link), 'Maintenance automatique' (status: 'Aucune action requise', note: 'Date de dernière exécution : 13/08/2021 10:50', 'Windows planifie automatiquement les activités de maintenance qui doivent s'exécuter sur'), and a 'Voir aussi' sidebar with 'Historique des fichiers' and 'Résolution des problèmes de compatibilité des programmes Windows'.

3. Chiffrement des fichiers

La cryptographie est une science permettant de convertir des informations compréhensibles en informations codées, ceci afin de masquer le contenu pour les protéger. Le chiffrement est le procédé utilisé pour rendre incompréhensible une information tant que la clé de déchiffrement n'est pas connue.

Il existe deux principaux types de chiffrement :

- **Symétrique** : clé unique permettant de chiffrer et déchiffrer un message.
- **Asymétrique** : deux clés sont utilisées, la clé privée, gardée secrète, déchiffre l'information, tandis que la clé publique, fournie par exemple à un correspondant, sert au chiffrement de l'information par celui-ci.

Windows 11 utilise ces deux types de chiffrement pour protéger les données personnelles de l'utilisateur.

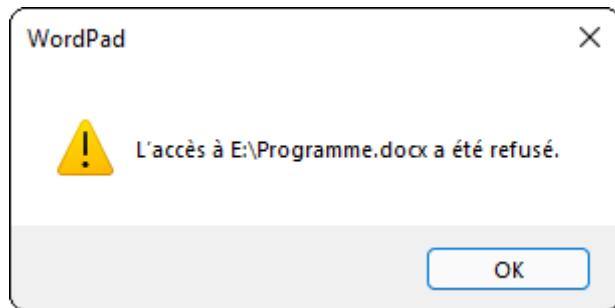
a. Système EFS

EFS (*Encrypting File System*) chiffre les fichiers sélectionnés de manière transparente sur une partition NTFS. Disponible depuis Windows 2000, ce système permet de partager un fichier chiffré en ajoutant les certificats EFS des utilisateurs ayant besoin d'y accéder.

Basé sur un chiffrement à clé publique, EFS peut chiffrer un dossier et tous les fichiers qu'il contient sans demander de mot de passe à l'utilisateur : la clé de déchiffrement est basée sur son compte et le mot de passe associé. En cas de copie ou déplacement d'un fichier chiffré vers une partition FAT, celui-ci perdra son attribut de chiffrement.

EFS utilise une clé symétrique qui est elle-même chiffrée à l'aide de la clé publique de l'utilisateur. Un certificat, basé sur les clés publique et privée de celui-ci (chiffrement asymétrique) est stocké dans son profil.

Si un utilisateur ne possède pas la clé de déchiffrement lors de l'ouverture d'un fichier chiffré, un message "Accès refusé" apparaîtra.



La paire de clés publique et privée, d'une validité de 100 ans, est protégée par le mot de passe de l'utilisateur. Elle peut être générée par une autorité de certification, ou par le poste Windows 11.

Une attaque par force brute sur le mot de passe du compte pourrait compromettre l'accès aux fichiers chiffrés. Donc, plus le mot de passe d'ouverture de session est complexe, meilleure sera la protection des fichiers chiffrés.

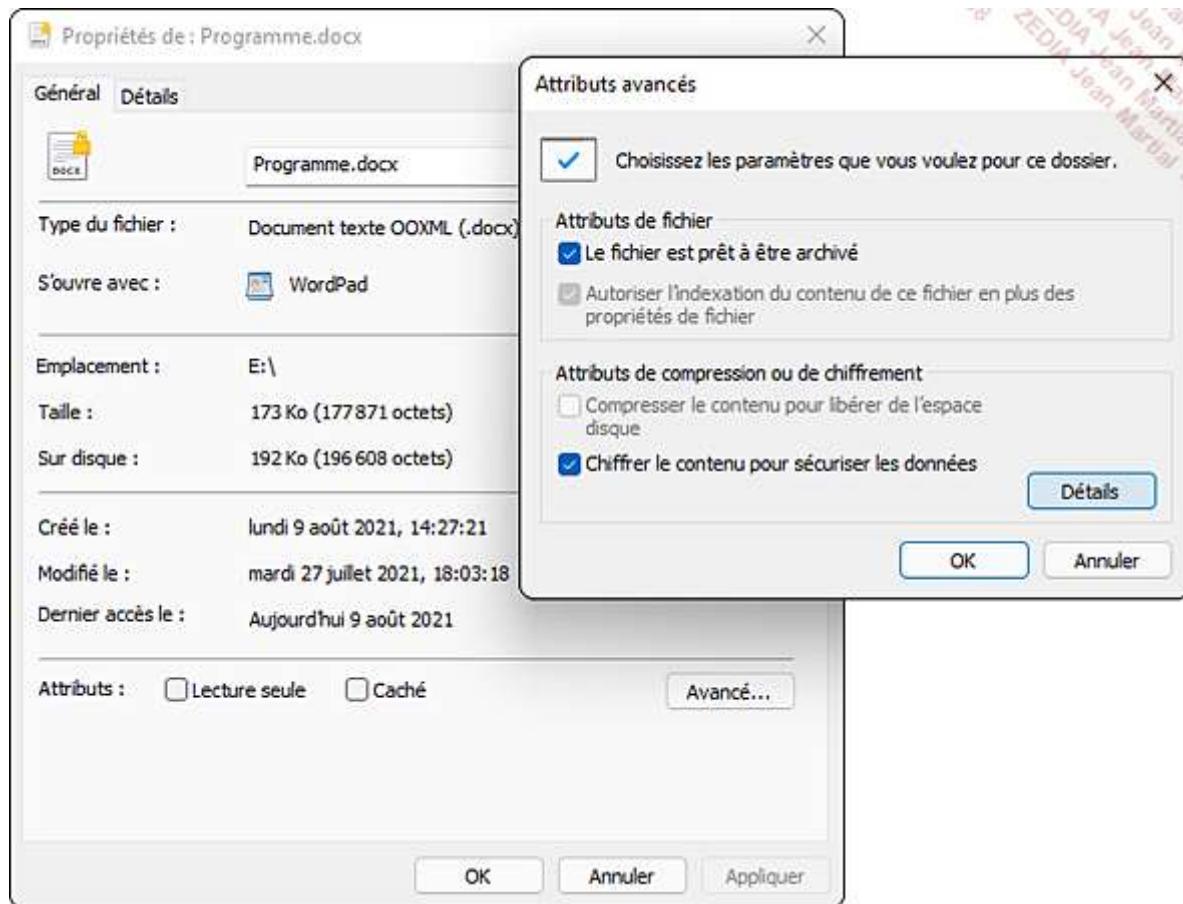
- Lors de l'accès à un fichier chiffré stocké sur un partage, celui-ci est déchiffré durant le transfert des données. Les clés de chiffrement sont disponibles sur le serveur de fichiers.

Par défaut, la fonctionnalité EFS utilise l'algorithme de chiffrement AES (*Advanced Encryption Standard*) 256 bits.

Windows 11 prend en charge le stockage des clés privées sur des cartes à puce, le chiffrement du fichier de pagination et des fichiers hors connexion ainsi que l'assistant de gestion des certificats pour EFS.

Pour chiffrer un fichier stocké sur une partition NTFS :

Cliquez avec le bouton droit sur le fichier que vous souhaitez chiffrer, puis choisissez **Propriétés**. Sur l'onglet **Général**, cliquez sur le bouton **Avancé** et cochez la case **Chiffrer le contenu pour sécuriser les données**.



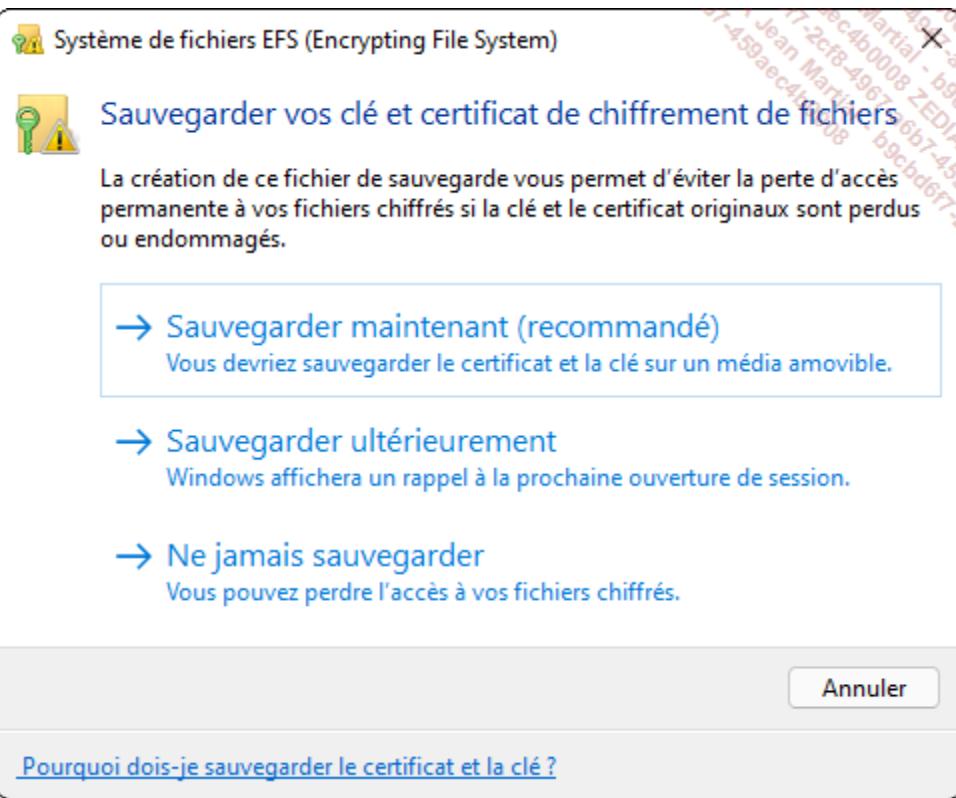
- Notez que vous ne pouvez pas chiffrer et compresser un fichier en même temps, même si le type de case à cocher semble montrer le contraire.

Une fenêtre d'avertissement apparaît : vous avez la possibilité de chiffrer le dossier ou uniquement le fichier. Sélectionnez en fonction de vos besoins et validez.

Une fois le fichier chiffré, le bouton **Détails** ne sera plus grisé, l'utilisateur pourra ainsi ajouter les certificats d'utilisateurs (et non de groupes) locaux ou membres d'un domaine, pour lesquels il souhaite autoriser l'accès au document. L'icône du fichier chiffré affiche désormais un cadenas.

La première fois qu'un fichier est chiffré, Windows 11 propose de sauvegarder la clé et le certificat de chiffrement et affiche une notification en bas à droite.

En cliquant sur le message, la fenêtre de l'assistant **Système de fichiers EFS** (*Encrypting File System*) est exécutée. L'utilisateur peut, au choix, **Sauvegarder maintenant** au format PKCS#12 (*Public Key Cryptographic Standards*) (.pfx), **Sauvegarder ultérieurement** ou **Ne jamais sauvegarder** la clé et le certificat.



- Il est conseillé de stocker sur un média amovible ou un partage réseau sécurisé la clé et le certificat, car, en cas de perte de ceux-ci, les données chiffrées ne pourront plus être déchiffrées.

L'administrateur peut aussi exporter ses certificats critiques depuis le composant logiciel enfichable **Certificats** (magasin **Personnel**).

L'assistant Système de fichiers EFS nommé rekeywiz permet de gérer les certificats de chiffrement de fichiers pour les utilisateurs d'un poste de travail Windows 11 : création d'un nouveau certificat, sauvegarde de celui-ci pour éviter la perte d'accès définitive aux fichiers chiffrés ou encore configuration d'EFS avec une carte à puce.

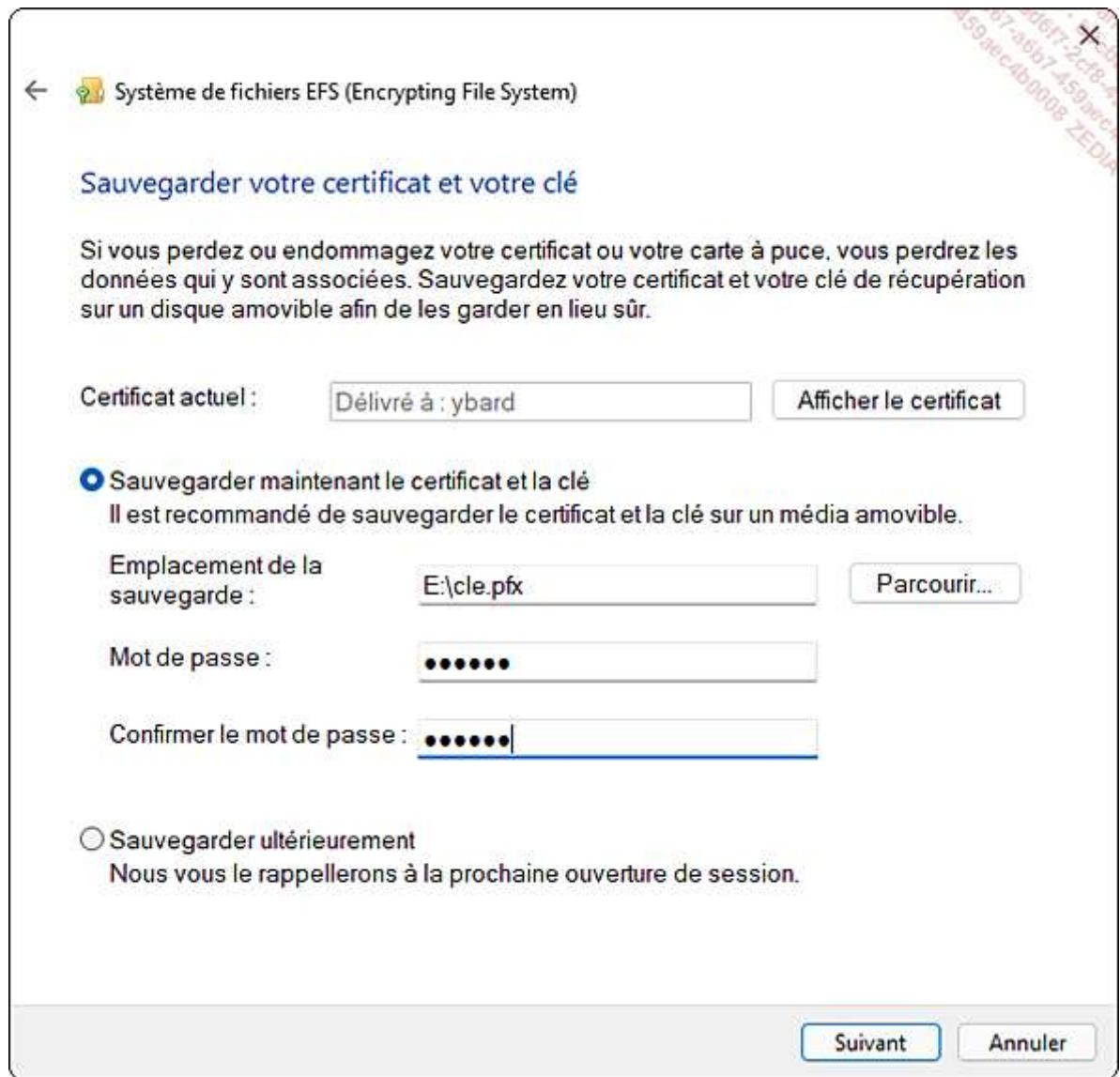
Pour exécuter l'assistant :

Pressez les touches + R. Saisissez rekeywiz dans la fenêtre **Exécuter** puis validez par la touche [Entrée].

Dans la fenêtre **Système de fichiers EFS (Encrypting File System)**, cliquez sur le bouton **Suivant**.

Cochez la case correspondant à votre besoin : **Utiliser ce certificat** ou **Créer un certificat** puis cliquez sur le bouton **Suivant**. Dans notre exemple, nous allons utiliser un certificat existant.

Choisissez de **Sauvegarder maintenant le certificat et la clé** dans un fichier ayant l'extension .pfx (PKCS#12) et définissez puis confirmez un **Mot de passe**.



Passez à la prochaine étape en cliquant sur le bouton **Suivant**.

Vous pouvez appliquer la nouvelle clé générée en mettant à jour les fichiers chiffrés. Validez en cliquant sur le bouton **Suivant**. Terminez l'assistant en cliquant sur le bouton **Fermer**.

La commande cipher affiche et modifie le chiffrement des fichiers stockés sur une partition NTFS. Le paramètre /rekey met à jour tous les fichiers chiffrés pour qu'ils utilisent la clé EFS configurée.

b. Agent de récupération

Lorsqu'un utilisateur chiffre un fichier, la clé de déchiffrement dépend de son compte Windows et du SID (*Security Identifier*) unique associé. Le SID permet au système Windows 11 d'identifier les objets effectuant des actions. En cas de départ d'un salarié, si vous supprimez son compte utilisateur, son SID sera lui aussi supprimé. Vous ne pourrez donc plus ouvrir les fichiers chiffrés par cet utilisateur, même si vous recréez un compte du même nom, car son SID sera obligatoirement différent ! Pour pallier cette problématique, Microsoft propose de créer un agent de récupération, qui est en définitive un compte d'utilisateur pouvant déchiffrer n'importe quel fichier chiffré.

Pour créer un agent de récupération local :

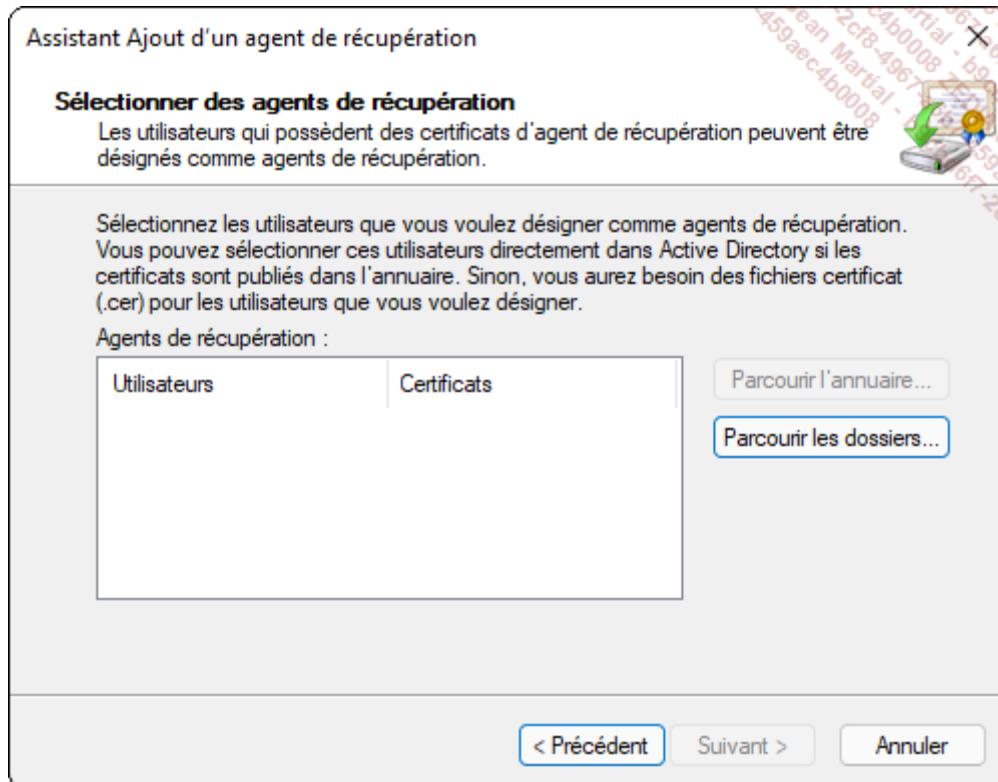
Pressez les touches + R. Saisissez gpedit.msc dans la fenêtre **Exécuter** puis validez par la touche [Entrée].

Dans la fenêtre **Éditeur de stratégie de groupe locale**, développez les nœuds **Configuration de l'ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies de clé publique**.

Cliquez avec le bouton droit sur **Système de fichiers EFS (Encrypting File System)** et sélectionnez **Ajouter un agent de récupération de données**.

Dans l'**Assistant Ajout d'un agent de récupération**, cliquez sur **Suivant**.

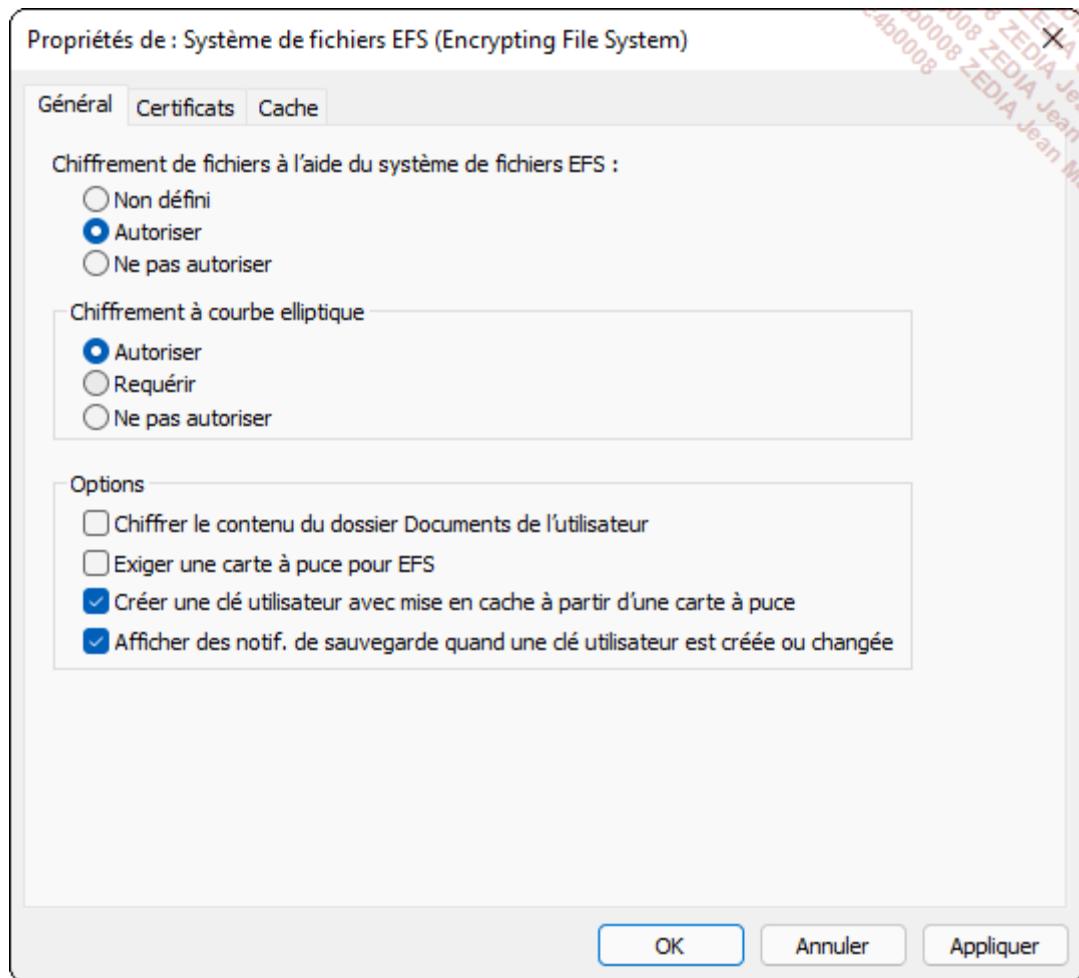
Sélectionnez ensuite le certificat (.cer), ou l'utilisateur membre d'un domaine, à qui vous souhaitez affecter le rôle d'agent de récupération, puis cliquez sur **Suivant**. Suivez les étapes de l'assistant.



La configuration générale d'EFS s'effectue également par l'intermédiaire des propriétés du nœud **Système de fichiers EFS (Encrypting File System)** :

Cliquez avec le bouton droit sur le nœud **Système de fichiers EFS (Encrypting File System)** puis choisissez **Propriétés**.

Dans l'onglet **Général**, autorisez le chiffrement à l'aide d'EFS et définissez les options appropriées (**Chiffrer le contenu du dossier Documents de l'utilisateur**, **Exiger une carte à puce pour EFS**, etc.).



L'onglet **Certificats** propose de choisir le modèle de certificat, ainsi que le comportement d'EFS lorsqu'une autorité de certification n'est pas disponible, à savoir la génération de certificats autosignés.

Le dernier onglet, **Cache**, définit les cas dans lesquels l'effacement du cache de clé de chiffrement doit avoir lieu.

Même si la technologie EFS procure une sécurité importante, la protection physique d'un ordinateur reste primordiale.

4. Windows Information Protection

De plus en plus de salariés possèdent un smartphone prêté par leur employeur, et dans le même temps, utilisent leur ordinateur aussi bien chez eux en télétravail, qu'au sein de l'entreprise. En parallèle, un employé peut parfois transférer des dossiers importants sur sa messagerie privée afin de travailler dessus le temps d'un week-end. La fuite des données, intentionnelles ou non, est une préoccupation de tous les instants d'une société.

Pour ces raisons, Microsoft a introduit la fonctionnalité WIP (*Windows Information Protection*). Elle permet de protéger les applicatifs et données sensibles de l'entreprise contre ces fuites, et ceci sans modification de l'environnement de l'utilisateur.

Malheureusement, le déploiement et la gestion de ce service au quotidien nécessite l'achat d'un autre produit, Microsoft Intune ou bien Microsoft Endpoint Configuration Manager.

La fonctionnalité WIP peut être utilisée dans les cas d'usage ci-après :

- Copie depuis un partage réseau de l'entreprise de fichiers : WIP va les chiffrer sur le poste de travail du collaborateur.
- Approbation d'applicatifs pouvant accéder aux données de l'entreprise.

- Chiffrement des fichiers identifiés comme provenant de l'entreprise lors d'une copie de ceux-ci sur un périphérique USB non chiffré.
- Suppression à distance des données et applicatifs propres à l'entreprise lors du départ d'un salarié.

Sécurisation des données hors connexion

183 Contre le vol de disques durs ou de médias amovibles comme les clés USB, la vigilance est primordiale.
 184 Pour pallier cette problématique, Microsoft propose la technologie de chiffrement de lecteur BitLocker, apparue avec le système Windows Vista.

1. BitLocker

185 Inclus dans les versions Entreprise, Education et Professionnel de Windows 11, BitLocker protège toutes les données stockées sur les partitions, en mode hors connexion. En effet, lors du processus de démarrage, le disque dur est déchiffré par BitLocker, qui n'empêche donc pas l'accès non autorisé à des données lorsque Windows 11 fonctionne. Privilégiez dans ce cas EFS pour chiffrer vos documents.

186 BitLocker est aussi utile en cas de mise hors service définitive d'un disque dur. En le chiffrant complètement, la solution devient vite rentable par rapport au coût d'une entreprise spécialisée dans la destruction physique des disques.

187 Une autre fonctionnalité intéressante apportée par BitLocker est le contrôle d'intégrité, qui authentifie au travers d'une puce **TPM** (*Trusted Platform Module*) le matériel de l'ordinateur et les fichiers critiques (NTFS boot sector, boot manager...) de Windows 11. Ainsi, en cas de vol d'un disque dur chiffré par cette méthode, les données qu'il contient ne seront pas accessibles via un autre ordinateur. Un virus ne pourra pas non plus s'implanter durant la phase de démarrage du système d'exploitation.

188 Voici un tableau comparatif des technologies BitLocker et EFS :

	BitLocker	EFS
Chiffrement complet des partitions	X	
Authentification forte (mot de passe et mémoire flash USB)	X	
Méthode de récupération (mot de passe ou Agent)	X	X
Chiffrement complet d'un périphérique amovible	X	
Vérification de l'intégrité du système et du matériel	X	
Protection des données une fois l'ordinateur démarré		X
Chiffrement de fichiers	X	X
Utilisation d'un certificat utilisateur		X
Assure le DLP (<i>Data Loss Prevention</i>)	X	X
Prise en charge des partitions non NTFS pour les périphériques amovibles	X	

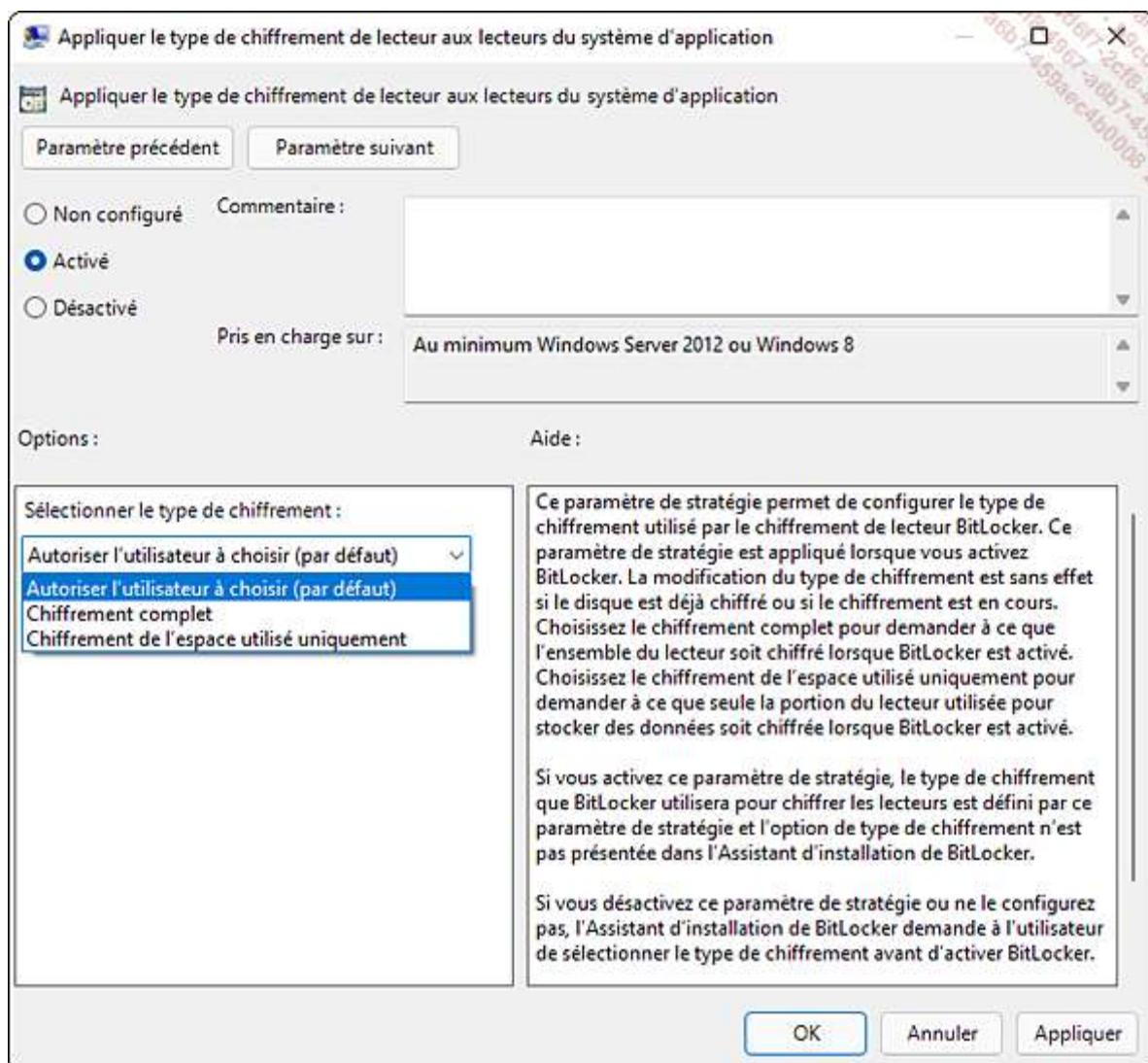
189 Lors du choix d'une méthode de chiffrement de lecteur hors connexion, la diminution des performances est à prendre en compte. Activer BitLocker sur un disque dur réduit les performances d'accès à celui-ci de 3 à 5 %, selon Microsoft.

190 BitLocker nécessite les prérequis suivants :

- Un BIOS prenant en charge des périphériques USB au démarrage ou la présence d'une puce TPM sur la carte mère. Notez que cette dernière fait partie des prérequis pour Windows 11.
- Une partition système (automatiquement créée si absente), d'une taille approximative de 100 Mo, non chiffrée, sans lettre de lecteur et définie comme active.
- De manière facultative, une partition contenant des données peut être formatée en FAT16, FAT32, exFAT et bien entendu NTFS mais doit posséder au moins 64 Mo d'espace disque libre.

191 Windows 11 apporte les fonctionnalités suivantes avec BitLocker :

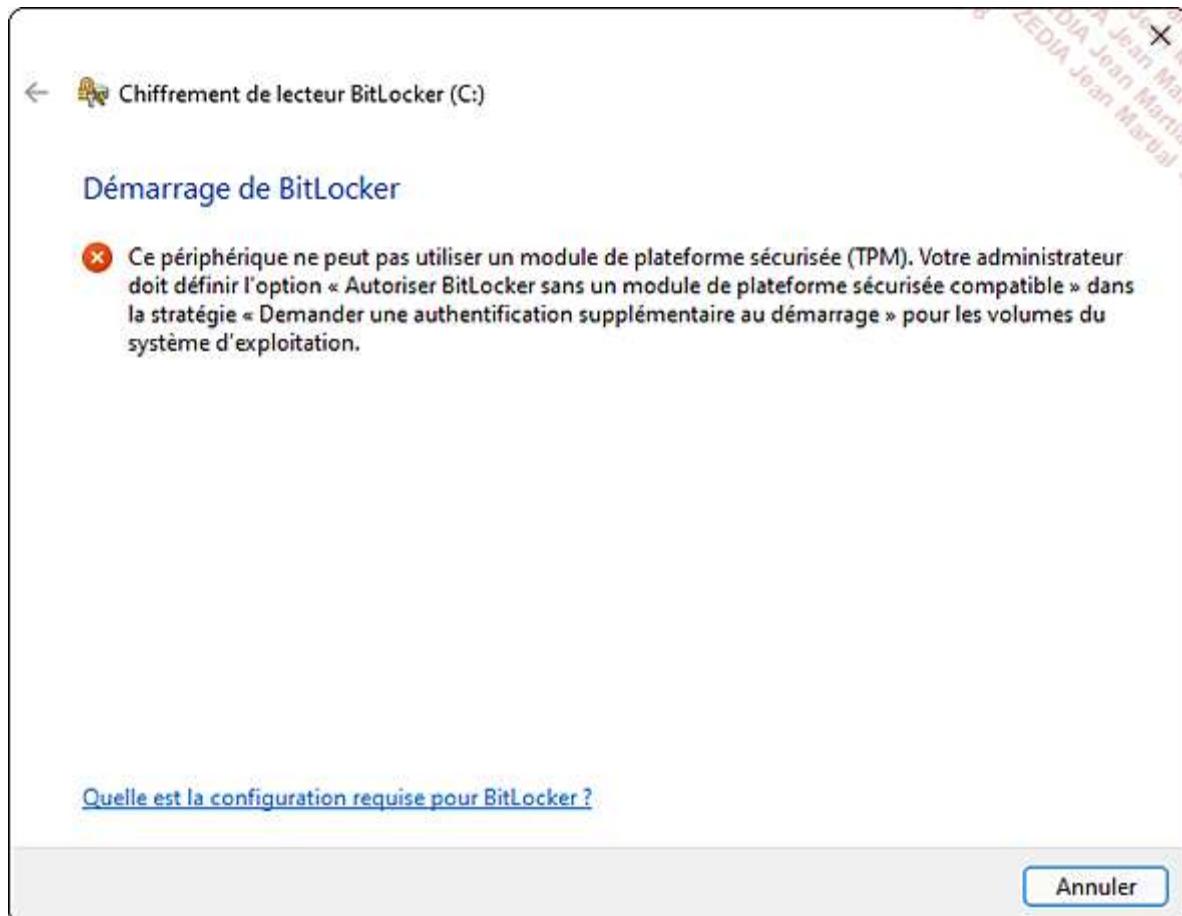
- Un chiffrement de l'espace disque seulement utilisé, accélérant ainsi le temps de chiffrement du lecteur. Cette fonctionnalité peut être imposée depuis la stratégie de groupe locale via les nœuds **Configuration ordinateur - Modèles d'administration - Composants Windows - Chiffrement de lecteur BitLocker - Lecteurs du système d'exploitation (Lecteurs de données fixes ou Lecteurs de données amovibles)** et le paramètre **Appliquer le type de chiffrement de lecteur aux lecteurs du système d'exploitation**.



- Des nouveaux paramètres dans les stratégies de groupe, comme la possibilité de spécifier le dossier par défaut stockant les clés de récupération ou d'imposer des critères de complexité des mots de passe pour les lecteurs. La sauvegarde dans un domaine Active Directory des informations du propriétaire de la puce TPM est désormais possible.

- Un chiffrement de la partition durant la phase d'installation, grâce à Windows PE. Avant le chiffrement définitif, le lecteur est affiché à côté d'un point d'exclamation jaune, avec le message "En attente d'activation". Par défaut, BitLocker chiffre avec une puissance de chiffrement AES de 128 bits.
- Une gestion du mode de veille connectée afin de pouvoir chiffrer les périphériques sur des ordinateurs ayant une architecture x86 ou x64 avec une puce TPM.
- Un support du FVE (*Full Volume Encryption*), chiffrant les disques au niveau matériel. Le paramètre **Configurer l'utilisation du chiffrement au niveau matériel pour les lecteurs du système d'exploitation** active cette fonctionnalité, depuis les nœuds **Configuration ordinateur - Modèles d'administration - Composants Windows - Chiffrement de lecteur BitLocker - Lecteurs du système d'exploitation** (ou **Lecteurs de données fixes**) de la stratégie de groupe locale.
- Un changement du code PIN ou du mot de passe possible pour un utilisateur ayant des priviléges standards. Après cinq tentatives infructueuses de saisie du mot de passe courant pour pouvoir le changer, le système doit être redémarré pour que le compte soit remis à zéro. Un administrateur peut bien entendu changer le code PIN ou le mot de passe. Il est possible de désactiver cette fonctionnalité depuis le paramètre **Ne pas autoriser les utilisateurs standard à modifier le code confidentiel ou le mot de passe** depuis les nœuds **Configuration ordinateur - Modèles d'administration - Composants Windows - Chiffrement de lecteur BitLocker - Lecteurs du système d'exploitation**.

192 Par défaut, chiffrer la partition contenant le système d'exploitation Windows 11 nécessite un ordinateur possédant une puce TPM. En son absence, un message d'erreur apparaît :



193 Pour vérifier qu'un ordinateur possède une puce TPM, se référer à la documentation du constructeur ou bien cliquer sur **Administration du TPM** dans la fenêtre **Chiffrement de lecteur BitLocker**, accessible depuis le **Panneau de configuration**. Si le module de plateforme sécurisé est introuvable, deux options sont possibles :

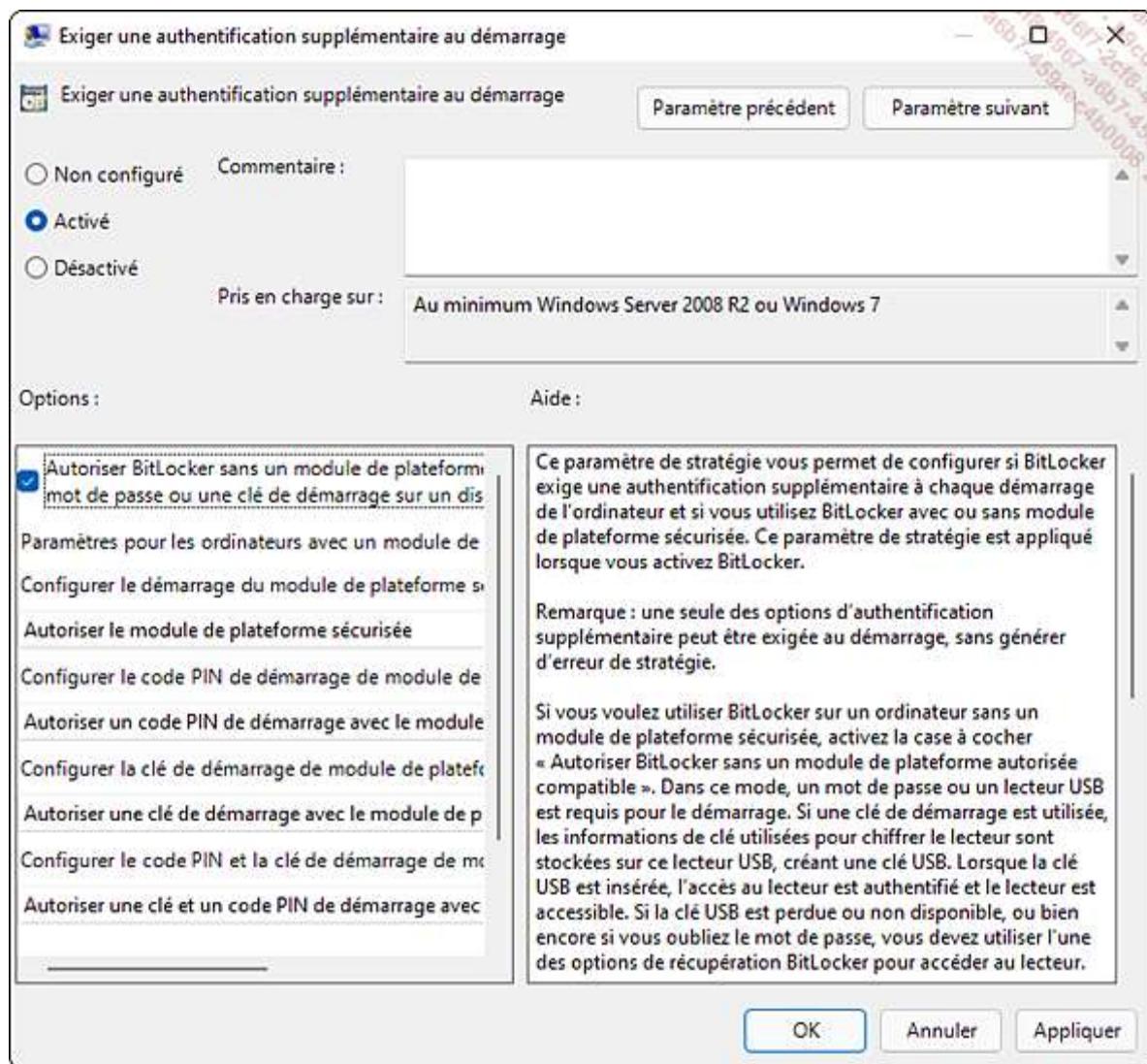
- Le module est présent, mais simplement désactivé dans l'UEFI de la machine (rubrique *Security chip* généralement). Si le module est activé, mais pas en cours de fonctionnement, Windows 11 le détecte, reconfigure la fonctionnalité et propose de redémarrer la machine.
- La machine ne dispose pas de module TPM (peu probable).

194 Sur la version précédente de Windows, s'il n'y avait pas de puce TPM, il existait une méthode de contournement afin de désactiver l'exigence liée à la présence de ce composant. Cette action s'effectuait dans la stratégie de groupe locale :

Utilisez la combinaison de touches  + R puis saisissez gpedit.msc et validez par [Entrée].

Dans l'écran **Éditeur de stratégie de groupe locale**, développez les nœuds **Configuration ordinateur - Modèles d'administration - Composants Windows - Chiffrement de lecteur BitLocker et Lecteurs du système d'exploitation**.

Double cliquez sur le paramètre **Exiger une authentification supplémentaire au démarrage**. Cochez l'option **Activé** et vérifiez dans les options que la case **Autoriser BitLocker sans un module de plateforme sécurisée compatible (requiert un mot de passe ou une clé de démarrage sur un disque mémoire flash USB)** est bien cochée.



195 Avec cette option activée, et sans puce TPM, le système exigera l'insertion d'une clé USB spécifique ou bien la saisie d'un mot de passe conforme pour démarrer.

196 Une configuration homogène de BitLocker sur des ordinateurs Windows 11 peut être effectuée dans un domaine Active Directory à l'aide d'un objet stratégie de groupe.

197 Notez que Windows Server 2008 ou supérieur supportent nativement cette technologie, et peuvent l'installer à l'aide de la commande PowerShell suivante : Install-WindowsFeature BitLocker -IncludeAllSubFeature.

198 Lorsque la partition du système d'exploitation est protégée par BitLocker, l'utilisateur ne peut le démarrer qu'à l'aide d'une clé de déchiffrement, selon trois méthodes :

- Module TPM version 1.2 ou ultérieur : disponible notamment sur les ordinateurs portables, cette puce est un composant matériel installé sur la carte mère. Elle assure un contrôle d'intégrité en plus du chiffrement des lecteurs. Vous pouvez combiner d'autres facteurs d'authentification en ajoutant la fourniture d'un code confidentiel et/ou l'insertion d'un périphérique USB contenant la clé de démarrage. Dans le cas où la puce TPM deviendrait inaccessible, ou qu'un utilisateur essaierait de démarrer l'ordinateur depuis un CD ou un DVD, Windows 11 basculerait en mode de récupération et nécessiterait un mot de passe de récupération.
- Périphérique amovible USB, telle une clé USB : le BIOS de l'ordinateur doit prendre en charge des périphériques USB au démarrage. La clé USB contient la clé de démarrage et doit être obligatoirement branchée lorsque l'ordinateur est mis sous tension. Cette méthode ne fournit pas de vérification d'intégrité des composants matériels lors du prédémarrage de l'ordinateur, mais assure un chiffrement des volumes.
- Mot de passe complexe saisi lors de la première étape de l'assistant.

199 À ce stade, il ne reste plus qu'à activer le chiffrement de lecteur BitLocker sur la partition du système Windows 11 nommée C:, en utilisant les privilèges administrateur :

Saisissez bitlocker dans la zone de recherche du menu **Démarrer**, et sélectionnez **Gérer BitLocker**.

Dans l'écran **Chiffrement de lecteur BitLocker**, cliquez sur **Activer BitLocker** en regard du lecteur à chiffrer, dans notre exemple **C:**.

The screenshot shows the Windows Control Panel under 'Chiffrement de lecteur BitLocker'. It displays the status of BitLocker for three types of drives:

- Lecteur du système d'exploitation:** Drive C: BitLocker désactivé (BitLocker disabled), represented by a blue and white icon.
- Lecteurs de données fixes:** Drive DATA (D): BitLocker désactivé (BitLocker disabled), represented by a blue and white icon.
- Lecteurs de données amovibles - BitLocker To Go:** Drive CLEUSB (E): BitLocker désactivé (BitLocker disabled), represented by a blue and white icon.

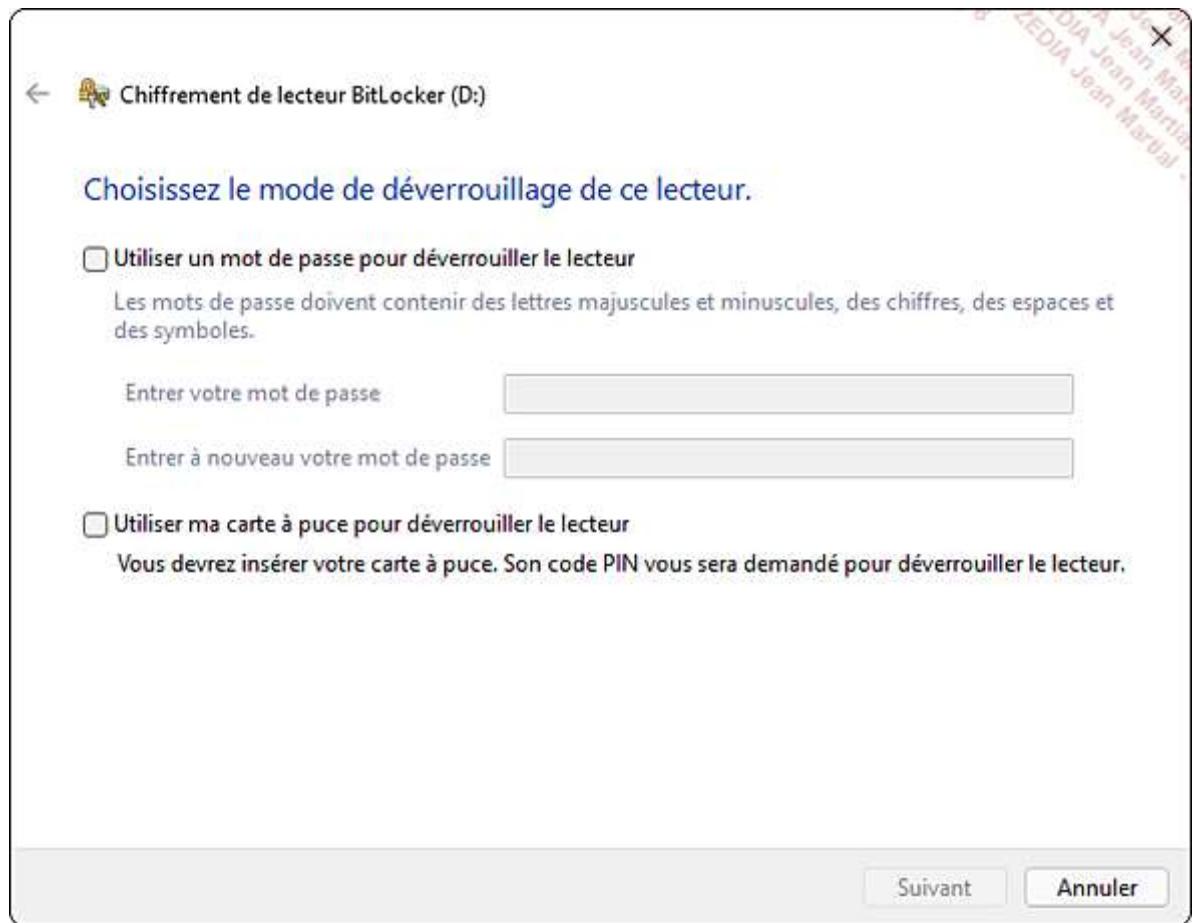
A sidebar on the left lists 'Voir aussi' (See also) links: 'Administration du TPM' and 'Gestion des disques', along with a 'Déclaration de confidentialité' (Confidentiality declaration).

Notez le chiffrement possible des lecteurs de données amovibles USB avec **BitLocker To Go**.

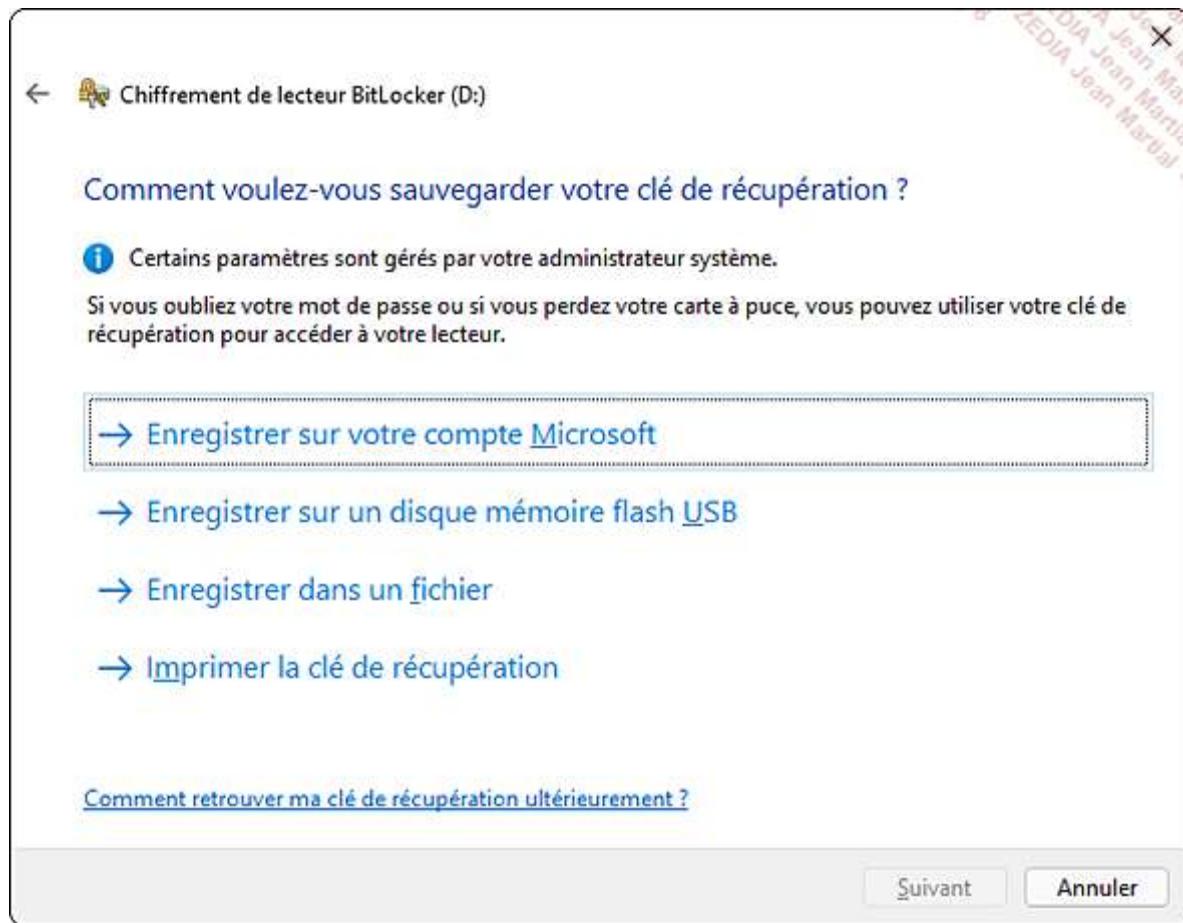
200 Vous pouvez aussi chiffrer un disque dur depuis l'**Explorateur de fichiers**, en sélectionnant la lettre de lecteur à l'aide du bouton droit, puis en choisissant l'option **Activer BitLocker**, ou bien dans une invite de commandes grâce au fichier exécutable manage-bde.exe. L'avantage du script est la possibilité de configurer BitLocker sur des ordinateurs distants.

L'assistant de chiffrement analyse la configuration nécessaire pour activer BitLocker sur le lecteur C:. S'il ne détecte pas de partition système, il proposera de redémarrer la machine et d'en créer une. Ce cas ne devrait pas se produire, Windows 11 ayant créé cette partition lors de l'installation.

Si l'activation de BitLocker est définie sur une partition autre que celle du système d'exploitation, un assistant vérifie la configuration et propose deux méthodes de déchiffrement : par mot de passe complexe (majuscules, minuscules, chiffres et symboles) ou par carte à puce.



- 201 L'utilisateur est ensuite invité à choisir une méthode de sauvegarde de la clé de récupération :
- Dans son compte Microsoft (cf. chapitre Installation du client Windows 11, section Authentification), qui sera accessible depuis d'autres ordinateurs.
 - Dans un lecteur flash USB. Le fichier possédera automatiquement l'attribut Lecture seule. Cette option ne sera pas proposée en cas de chiffrement de la partition contenant le système d'exploitation.
 - Dans un fichier stocké sur un partage réseau ou sur un disque de l'ordinateur local. Cette méthode est peu recommandée en raison des risques de suppression liés par exemple à une attaque virale.
 - Sur une feuille de papier, qu'il faudra garder précieusement dans un endroit sécurisé (coffre-fort ou armoire fermée à clé).



La clé de récupération est composée de 48 chiffres divisés en huit groupes et est propre à chaque lecteur chiffré. Elle est utilisée dans plusieurs cas : perte du mot de passe principal ou de la mémoire flash USB, changement de la configuration matérielle.

202 Dans un environnement Active Directory, les postes de travail chiffrés joints au domaine peuvent stocker la clé de récupération dans l'annuaire. Dans ce cas, l'administrateur du domaine devra obtenir de l'utilisateur bloqué soit le label de la lettre du lecteur chiffré, soit le Password ID (32 caractères) disponible dans les propriétés système de l'ordinateur Windows 11 incriminé. Ceci afin de fournir la clé de récupération.

L'administrateur peut aussi créer un Agent de récupération des données, habilité à déchiffrer n'importe quel lecteur de l'ordinateur visé.

BitLocker propose enfin de ne chiffrer que l'espace disque utilisé (méthode rapide), ou l'intégralité du lecteur (méthode plus lente). À noter cependant que si la première option est sélectionnée, toute nouvelle donnée copiée sur le disque sera automatiquement chiffrée. Cliquez sur le bouton **Suivant**.

Choisissez le **Nouveau mode de chiffrement** (disponible depuis la version 1511 de Windows 10). Attention, si le lecteur à protéger est amovible, choisissez le **Mode Compatible** pour assurer la lecture depuis un système d'exploitation plus ancien. Cliquez sur **Suivant**.

Dans l'avant-dernière étape, l'assistant peut vous proposer de vérifier que votre lecteur pourra lire correctement les clés de récupération et de chiffrement. Cela implique le redémarrage de la machine.

Cliquez sur **Démarrer le chiffrement** pour exécuter le chiffrement de la partition.

203 Comme vu précédemment, la commande manage-bde.exe est proposée pour réaliser des opérations supplémentaires sur la fonctionnalité BitLocker.

204 Par exemple, la commande manage-bde -on D: chiffrera le volume D: sans méthode d'authentification.

205 Pour chiffrer le disque contenant le système d'exploitation Windows 11 C: sans module TPM mais en stockant la clé de récupération sur un périphérique amovible E:, tapez les commandes suivantes :

206 manage-bde -protectors -add C: -startupkey E:

207 manage-bde -on C:

208 Le paramètre -status affiche le chiffrement d'un volume.

209 Le commutateur -w offre la possibilité de supprimer des données fragmentées qui existent dans l'espace disque libre d'un volume chiffré.

210 Repair-bde permet d'accéder à des données stockées sur un volume chiffré, même si celui-ci est endommagé. Notez que la commande ne peut pas réparer un disque qui a été corrompu durant la phase de chiffrement ou de déchiffrement.

211 Des commandes PowerShell sont disponibles pour administrer BitLocker, comme Enable-BitLocker pour chiffrer un volume précis, ou Get-BitLockerVolume pour obtenir des informations sur un disque chiffré. Vous pourrez en trouver d'autres avec la commande Get-Command *bitlock*.

2. BitLocker To Go

212 BitLocker To Go est une fonctionnalité apparue avec Windows 7 proposant un chiffrement complet des dispositifs de stockage portables, comme les clés USB et les disques durs externes.

213 En cliquant avec le bouton droit sur la lettre du média amovible et en sélectionnant **Activer BitLocker**, l'utilisateur est invité à entrer un mot de passe de déverrouillage, ou à insérer une carte à puce avec un code PIN (*Personal Identification Number*) puis à sauvegarder la clé de récupération selon trois méthodes :

- Utiliser son compte Microsoft.
- Stocker dans un fichier (attribut Lecture seule automatiquement appliqué).
- Imprimer sur une page stockée en lieu sûr.

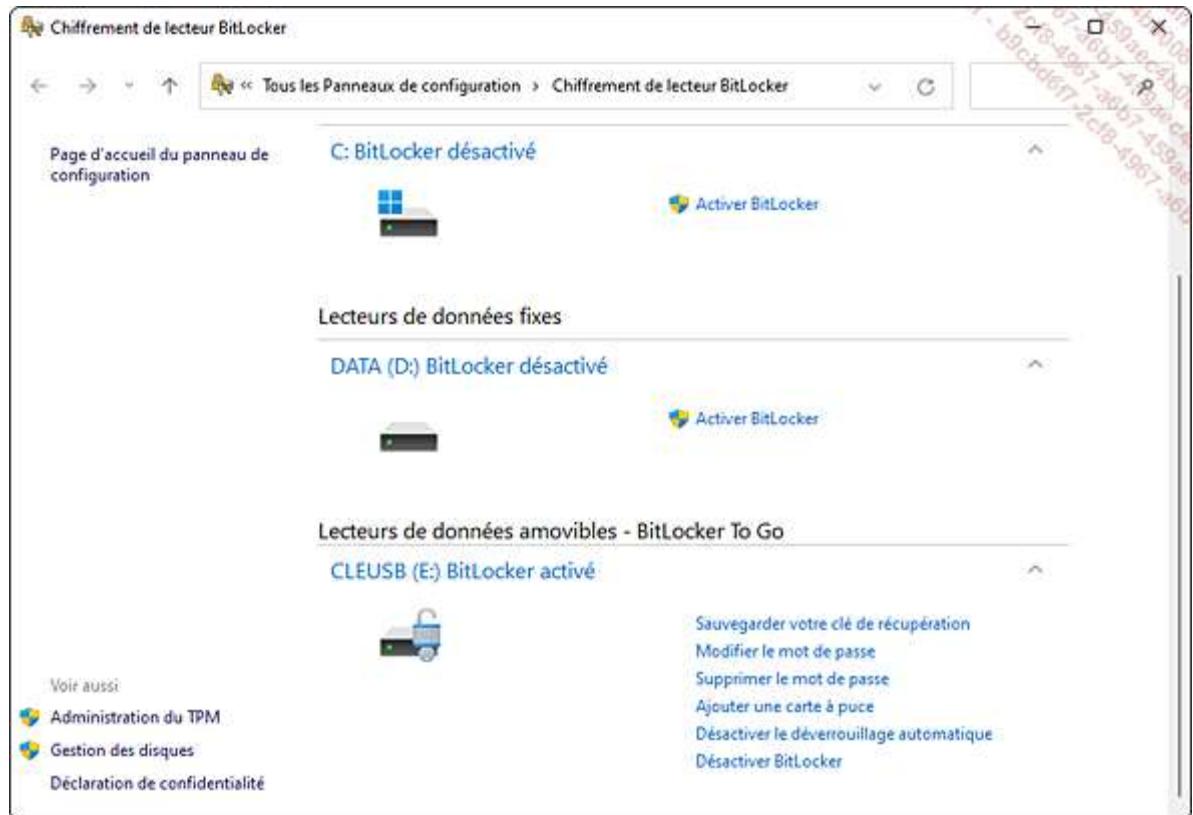
214 BitLocker To Go propose désormais de ne chiffrer que l'espace disque utilisé (méthode rapide), ou l'intégralité du lecteur (méthode plus lente).

215 Une fois la clé USB chiffrée, il est possible de définir des options supplémentaires, comme son déverrouillage automatique sur l'ordinateur cible ou la modification/suppression du mot de passe :

Saisissez bitlocker dans la zone de recherche située dans la barre des tâches, et sélectionnez **Gérer BitLocker**.

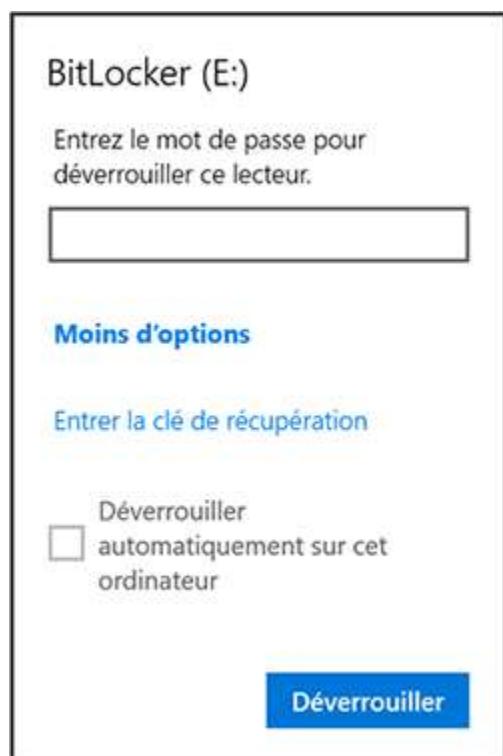
Dans l'écran **Chiffrement de lecteur BitLocker**, cliquez sur l'option choisie en face du périphérique amovible chiffré :

- **Sauvegarder votre clé de récupération** pour créer une nouvelle sauvegarde de la clé de récupération.
- **Modifier ou Supprimer le mot de passe actuel**.
- **Ajouter une carte à puce** pour utiliser une méthode de déverrouillage par carte à puce.
- **Activer le déverrouillage automatique** pour déverrouiller automatiquement le lecteur de données amovible lors de son branchement sur l'ordinateur actuel, sans exiger une méthode d'authentification.
- **Désactiver BitLocker** pour supprimer le chiffrement d'un lecteur, sans effacer les données qu'il contient.



216 Lorsque la clé USB chiffrée sera insérée dans un autre ordinateur équipé d'un système d'exploitation Microsoft Windows, l'utilisateur devra entrer le mot de passe de déchiffrement. Il aura aussi la possibilité de configurer BitLocker To Go pour qu'il se déverrouille automatiquement à l'insertion de cette clé sur cet ordinateur.

217 De la même manière, en insérant le lecteur amovible chiffré dans un poste de travail Windows 10 ou 11, l'utilisateur peut saisir la clé de récupération en cliquant sur **Plus d'options** et Entrer la clé de récupération.

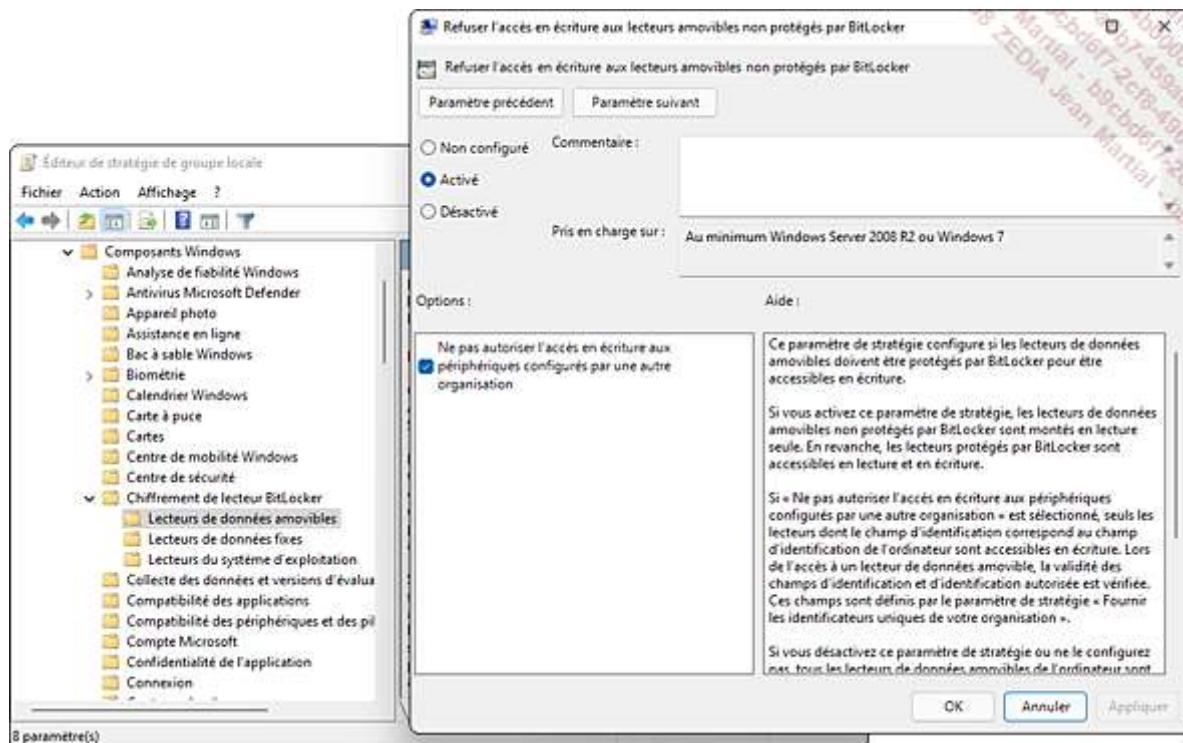


218 Devant le nombre croissant de pertes et de vols de mémoire flash USB, le responsable informatique d'une entreprise doit pouvoir s'assurer que le personnel ne pourra pas copier des données sur ce type de support sans qu'il soit au préalable protégé. Une option intéressante est l'interdiction d'accéder en écriture à un lecteur amovible non protégé par BitLocker To Go. Cette action s'effectue à l'aide d'un objet stratégie de groupe, locale ou de domaine :

Depuis l'écran d'accueil, pressez les touches **F** + R puis saisissez gpedit.msc dans la fenêtre **Exécuter** et validez par la touche [Entrée].

Depuis l'arborescence de la console **Éditeur de stratégie de groupe locale**, développez les nœuds **Configuration ordinateur - Modèles d'administration - Composants Windows - Chiffrement de lecteur BitLocker et Lecteurs de données amovibles**.

Double cliquez sur le paramètre **Refuser l'accès en écriture aux lecteurs amovibles non protégés par BitLocker** et cochez l'option **Activé**. Notez que l'administrateur peut **Ne pas autoriser l'accès en écriture aux périphériques configurés par une autre organisation** en cochant la case correspondante. Il faudra dans ce cas fournir la liste des périphériques autorisés dans le paramètre **Fournir les identificateurs uniques de votre organisation** dans le nœud supérieur.



219 Désormais, lorsqu'un périphérique flash USB sera connecté à l'ordinateur, un message apparaîtra invitant l'utilisateur à chiffrer le lecteur pour pouvoir écrire des données dessus :



Chiffrement de lecteur BitLocker (G:)



Avant de pouvoir enregistrer des fichiers sur ce lecteur, vous devez le chiffrer à l'aide de BitLocker.

→ Chiffrer ce lecteur à l'aide du chiffrement de lecteur BitLocker

Le lecteur sera en lecture seule jusqu'à ce que le chiffrement soit terminé.

→ Ne pas chiffrer ce lecteur

Vous pourrez ouvrir les fichiers qui se trouvent déjà sur le lecteur, mais vous ne pourrez pas enregistrer d'autres fichiers dessus.

Qu'est-ce que le Chiffrement de lecteur BitLocker ?

220 Si le poste de travail Windows 11 est membre d'un domaine, il peut être intéressant de sauvegarder les informations de récupération BitLocker (mot de passe de récupération et données d'identificateur unique) afin de prévenir toute perte des données en l'absence d'informations de la clé. Le paramètre **Enregistrer les informations de récupération BitLocker dans les services de domaine Active Directory** doit être activé depuis les nœuds **Configuration ordinateur - Stratégies - Modèles d'administration - Composants Windows - Chiffrement de lecteur BitLocker**.

Gestion des mises à jour de sécurité

221 La sécurité d'un système d'exploitation passe également par la correction de bugs dans celui-ci et l'ajout de fonctionnalités. Microsoft publie régulièrement des mises jour pour son système d'exploitation phare. Avec Windows 11, l'entreprise a annoncé une amélioration de la taille de celles-ci, avec un volume en baisse de 40 %.

222 Les mises à jour sont maintenant regroupées selon leur objectif :

- Mises à jour des fonctionnalités (précédemment appelées « mises à niveau ») : elles contiennent des révisions de sécurité et de qualité, mais aussi des ajouts et des modifications de fonctionnalités importantes. Auparavant publiées deux fois par an, Microsoft renoue avec une mise à jour de fonctionnalités annuelle avec Windows 11. D'ailleurs Windows 11 est une mise à jour de fonctionnalités de Windows 10.
- Mises à jour qualité (appelée également *Tuesday patch*) : elles regroupent les mises à jour de sécurité, critiques et de pilotes. Elles sont généralement publiées le deuxième mardi de chaque mois (même si elles peuvent être publiées à tout moment si une faille hautement critique est décelée et exploitée). Ainsi, les administrateurs peuvent se préparer à l'application des correctifs, en début de semaine, et ainsi anticiper et corriger les problèmes éventuels.
- Mises à jour de pilotes : comme leur nom l'indique, ces mises à jour améliorent les pilotes et sont spécifiques à vos machines.
- Mises à jour de produits Microsoft : elles concernent généralement Office.

223 Maintenir Windows 11 à jour permet de s'assurer de la stabilité et de la protection du système. Le service Windows Update gère le téléchargement et l'installation des mises à jour des produits Microsoft, lorsque l'utilisateur est connecté au réseau internet. En cas de déconnexion durant un téléchargement, une reprise est effectuée dès lors que la connexion est rétablie.

224 Lorsque l'utilisateur est connecté à un réseau sans fil dont les données utilisées sont facturées, tel que 3G ou 4G, Windows 11 diffère le téléchargement des mises à jour de sécurité en arrière-plan jusqu'à la connexion à un réseau sans fil Wi-Fi, moins coûteux.

225 Néanmoins, si une mise à jour de sécurité classée critique devenait disponible en téléchargement, le service Windows Update la téléchargerait, quel que soit le type de réseau. En initiant manuellement une recherche et un téléchargement de mises à jour, l'utilisateur peut outrepasser ces deux règles.

226 Windows Update utilise désormais l'apprentissage automatique (*machine learning*) pour prédire le moment le plus opportun pour redémarrer le poste de travail. En dehors des heures d'activité configurées, l'ordinateur sera redémarré au moment le plus approprié en fonction de la charge d'utilisation de celui-ci.

227 Il est recommandé d'utiliser les paramètres par défaut lors de la configuration du service de gestion des mises à jour : chaque jour à 2 heures, Windows 11 exécute une maintenance automatique si l'ordinateur n'est pas utilisé. Dans le cas contraire, ou si à cette heure-là le poste de travail est éteint, la maintenance s'exécutera la fois suivante. Si la carte réseau intégrée gère la fonctionnalité WOL (*Wake On LAN*), l'ordinateur éteint peut être allumé à distance pour installer les mises à jour.

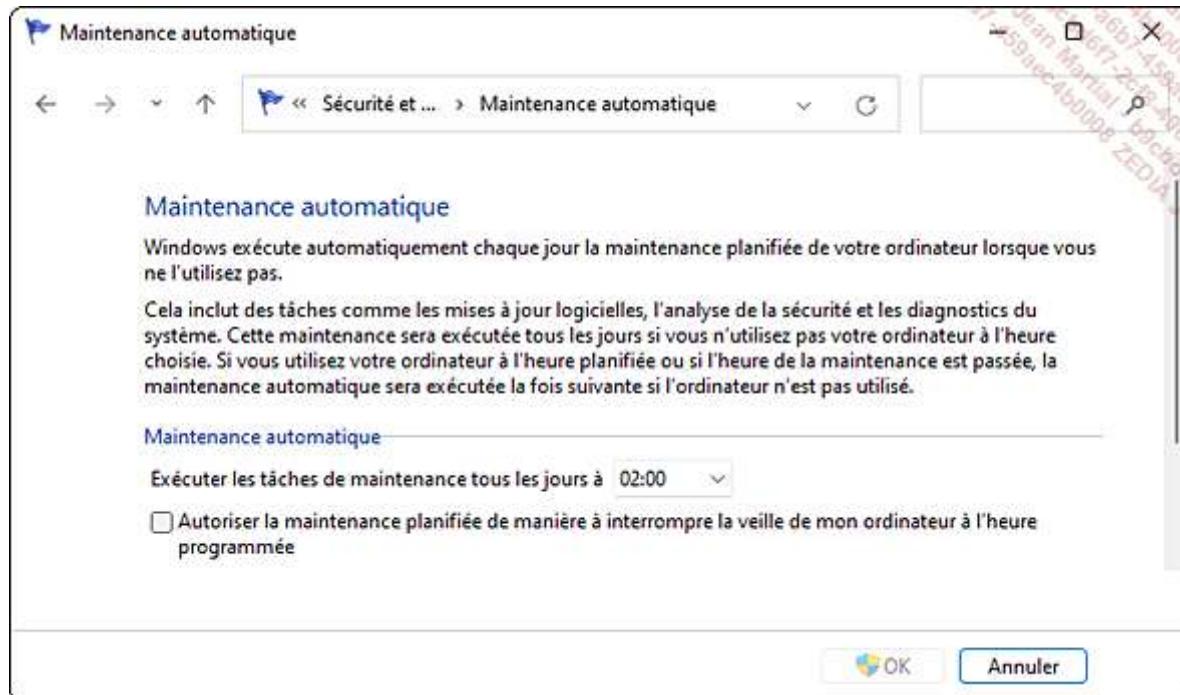
228 La plupart des cartes mères récentes implémentent le composant nécessaire à ce démarrage, mais nécessitent parfois l'activation de cette fonction dans le BIOS.

1. Configuration des paramètres de maintenance et de mise à jour

229 Pour configurer les paramètres de la maintenance automatique, suivez la procédure ci-dessous :

Depuis le champ de recherche du menu **Démarrer**, saisissez maintenance et sélectionnez **Sécurité et maintenance**.

Déroulez la section **Maintenance**, cliquez sur **Modifier les paramètres de maintenance** et configurez l'heure de déclenchement de la maintenance ainsi que la fonctionnalité Wake On LAN.



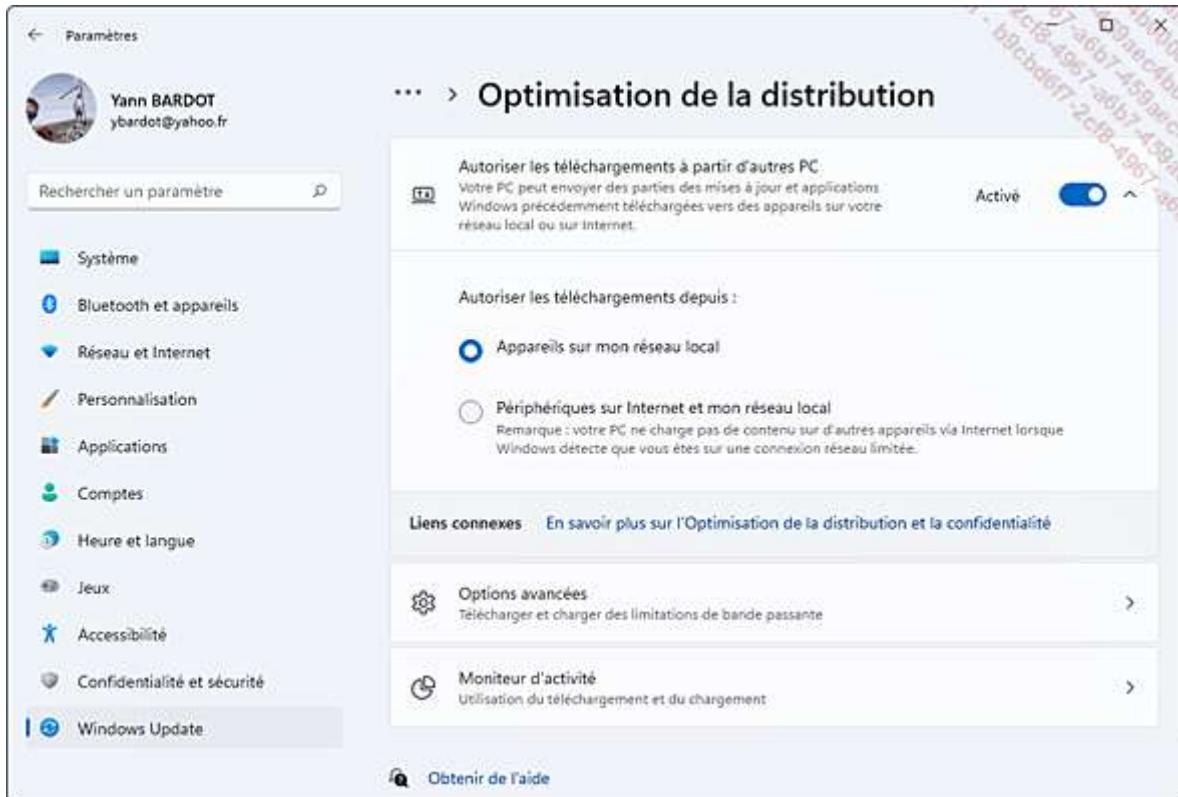
230 Quand une application Microsoft est en cours d'utilisation et qu'une mise à jour de sécurité la concernant est appliquée, Windows 11 sauvegarde les données de celle-ci, la met à jour, puis la redémarre.

231 Configurer les paramètres de Windows Update s'effectue comme suit :

Cliquez sur le menu **Démarrer**, puis **Paramètres** et **Windows Update**. En cliquant sur le bouton **Rechercher des mises à jour** vous pouvez déclencher manuellement celle-ci.

En cliquant sur **Options avancées**, vous pouvez paramétrer différentes options : **Obtenir des mises à jour pour les autres produits Microsoft**, être notifié des redémarrages, autoriser le téléchargement par des connexions limitées...

232 Une nouvelle fonctionnalité (également présente sur Windows 10) permet de télécharger les mises à jour sur les autres PC du même réseau, plutôt que d'utiliser la bande passante internet de l'entreprise pour se connecter au service de mise à jour de Microsoft. Pour y accéder, cliquez sur **Options avancées** puis **Optimisation de la distribution**.



233 Des **Mises à jour facultatives** sont disponibles dans les **Options avancées**. Elles concernent des améliorations de fonctionnalités ou de pilotes de périphériques.

234 Windows Update autorise également l'interruption des mises à jour pour une semaine avec le bouton **Suspendre pour 1 semaine** dans la section **Windows Update**.

235 En cliquant sur **Historique de mise à jour**, la liste des mises à jour est affichée, ces dernières étant classées par catégories.



236 Cette option est particulièrement utile lorsque vous voulez désinstaller des mises à jour ou la dernière version d'évaluation, suite à un problème rencontré (**Désinstaller des mises à jour**).

237 L'entreprise peut aussi utiliser un serveur WSUS (*Windows Server Update Services*), placé dans le réseau local, pour gérer les correctifs de sécurité. Celui-ci télécharge les mises à jour depuis Microsoft Update et se charge de les déployer sur les clients Windows de l'entreprise. Il en résulte une économie substantielle d'utilisation de la bande passante internet car le serveur WSUS utilise le réseau local, souvent architecturé avec une liaison 100 Mbit/s ou 1 Gbit/s. Le rôle WSUS nécessite une version serveur de Microsoft Windows, comme Windows Server 2019.

238 Grâce à un objet stratégie de groupe, l'administrateur du domaine peut définir des paramètres standards de gestion des correctifs, et les appliquer à l'intégralité du parc informatique dont il a la responsabilité. L'arborescence de ces stratégies a beaucoup changé depuis Windows 10. Elle se trouve dans **Configuration de l'ordinateur - Stratégies - Modèles d'administration - Composants Windows - Windows Update**.

239 **Gérer les mises à jour proposées de Windows Server Update Service** autorise les paramétrages suivants :

- Adresse du serveur WSUS auprès duquel le client doit s'enregistrer.
- Appartenance au groupe d'ordinateurs WSUS, c'est le ciblage côté client.
- Fréquence de recherche des mises à jour : par défaut, configurée toutes les 22 heures.

240 Sous **Gérer l'expérience utilisateur final**, vous pouvez configurer les éléments suivants :

- L'accès aux fonctionnalités de Windows Update par l'utilisateur.
- L'affichage ou non des notifications de mises à jour.
- Le téléchargement automatique.
- Le comportement du redémarrage automatique, ainsi que son retardement éventuel.

241 **Gérer les mises à jour proposées de Windows Update**, permet :

- Le report de la mise à niveau : pour les versions Professionnel et Entreprise de Windows 11, l'utilisateur peut différer les mises à niveau jusqu'à la prochaine période de mise à niveau (de 14 à 365 jours).

242 Sous **Stratégies héritées**, vous pouvez gérer :

- La sortie de veille prolongée des ordinateurs si l'installation de mises à jour est planifiée.

2. Windows Update pour entreprises

243 Une version professionnelle de Windows Update est disponible pour les entreprises sous forme de service cloud, Windows Update for Business (WUfB). Ainsi, l'administrateur peut maintenant définir les machines à mettre à jour en priorité, ou les périodes de l'année propices à l'application des mises à jour de sécurité. Un système de peer-to-peer permet à un poste de travail situé dans le LAN (*Local Area Network*) d'être un relai auprès des autres ordinateurs des mises à jour qu'il a reçues.

244 Les mises à jour et les fonctionnalités sont déployées sans devoir attendre le "patch Tuesday".

245 Au niveau de la gestion de la bande passante des entreprises utilisant des interconnexions WAN (*Wide Area Network*), Windows Update pour Entreprises fédère les envois grâce à Microsoft System Center Configuration Manager ou WSUS.

246 Il est aussi possible de limiter les mises à jour aux correctifs de sécurité, sans appliquer les évolutions fonctionnelles.

247 Windows Update pour Entreprises gère aussi bien l'évolution des postes Windows 10 et 11, éditions Professionnel, Entreprise et Education, que des versions serveurs 2016 et 2019.

248 Une fonctionnalité intéressante est la possibilité donnée aux administrateurs de fournir aux salariés de l'entreprise les Apps de celle-ci en téléchargement depuis un conteneur privé du Microsoft Store. Ces applications peuvent être gratuites ou payantes et téléchargeables uniquement sur des postes de travail Windows 11 en volume. L'administrateur peut affecter une App à une personne ou à un groupe, ou bien mettre celle-ci à disposition dans une page privée.

249 Les prérequis côté ordinateur client sont : un navigateur internet compatible tel que les dernières versions de Microsoft Edge, Chrome ou Firefox, et bien entendu le système d'exploitation Windows 10 (version 1511 ou supérieur) ou 11.

250 Côté infrastructure, un abonnement Azure dont la fonctionnalité Azure Active Directory est activée est requis. Il doit héberger une copie synchronisée des comptes des utilisateurs. Si l'entreprise est détentrice d'un abonnement Office 365, alors ce prérequis est aussi respecté.

251 L'administrateur peut mettre à disposition les licences nécessaires au bon fonctionnement de l'entreprise de 2 manières : en ligne et hors connexion. Une licence hors connexion met en cache l'App et sa licence pour les déployer au sein du réseau. Un cas concret d'utilisation de ce mode est le déploiement d'un applicatif métier.

252 L'administrateur peut mettre à disposition une App via un lien dans un courrier électronique ou par la fourniture du magasin privé ouvert dans le Microsoft Store. Dans les deux cas, l'utilisateur doit être connecté avec un compte Azure AD sur son poste Windows 11.

253 Pour pouvoir utiliser la boutique Microsoft pour les entreprises, l'administrateur général de l'organisation doit procéder à une inscription en ligne sur le site <https://www.microsoft.com/business-store>

254 L'administrateur général est invité à saisir son e-mail professionnel pour s'authentifier et à suivre les étapes de création du magasin privé. Une fois celui-ci provisionné, l'administrateur devra affecter des rôles aux utilisateurs afin qu'ils puissent installer les Apps d'éditeurs tiers ou métiers.

255 Depuis Windows 10 (version Creators Update), les ordinateurs peuvent maintenant différer l'installation des mises à jour de fonctionnalités (Build) jusqu'à 365 jours contre 180 jours auparavant.

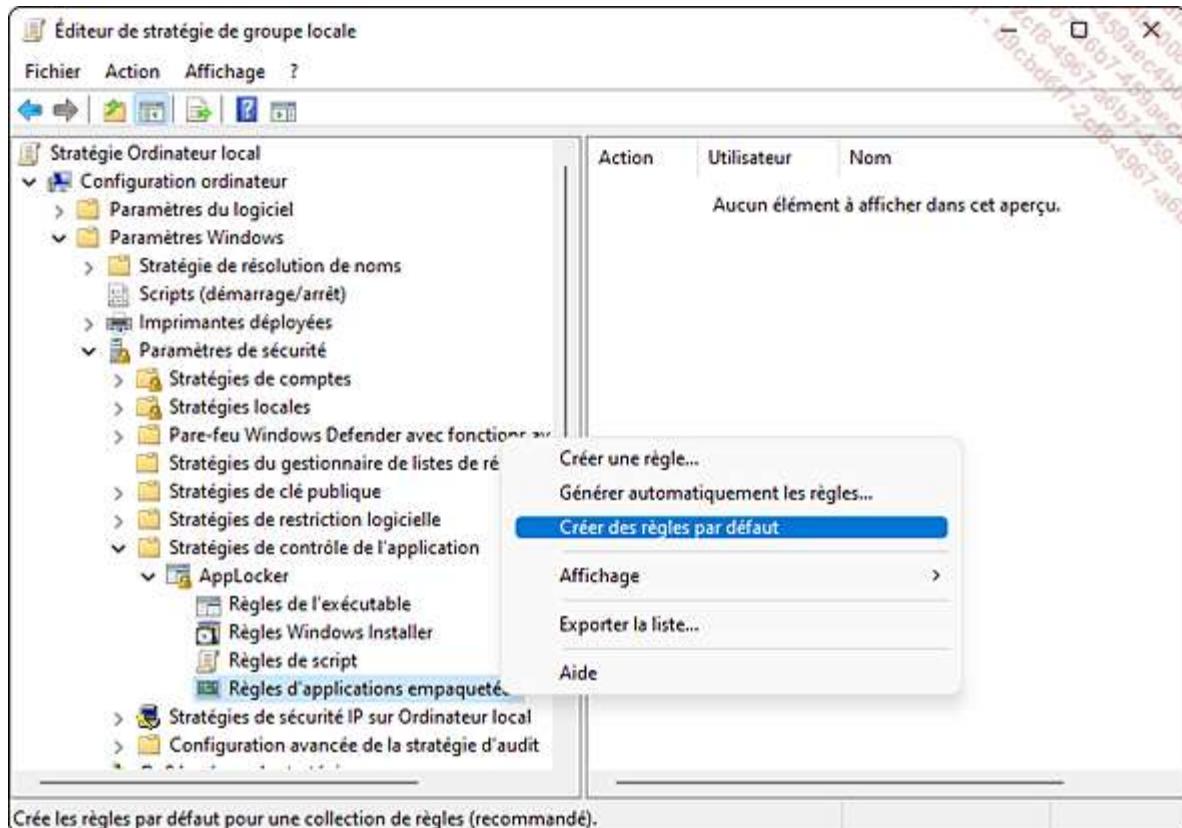
Contrôle des applications avec AppLocker

- Le contrôle des applications installées et sous licence sur les postes d'une entreprise est un enjeu majeur pour tout administrateur système. Face à ce défi, Microsoft propose la fonctionnalité **AppLocker**, qui restreint l'exécution et l'installation des logiciels définies depuis un serveur Windows sur des clients Windows 8.1 (Entreprise), Windows 10 et 11. Il en résulte une réduction de la charge d'administration et un contrôle accru des types de fichiers exécutables, évitant ainsi la propagation des logiciels malveillants, comme les chevaux de Troie.
- AppLocker combine l'inventaire et la standardisation des applications, la protection contre les logiciels non autorisés et la conformité des licences.
- AppLocker remplace la fonctionnalité des stratégies de restriction logicielle des versions précédentes de Windows. Par exemple, lors de la mise à jour vers Windows 10, puis 11 d'un ordinateur Windows 7 possédant une stratégie de restriction logicielle appliquée, une nouvelle règle AppLocker devra être créée pour supporter le blocage d'un logiciel.
- Les règles de restriction sont disponibles pour l'exécution de logiciels, de scripts et pour l'installation de programmes.
- Les extensions suivantes peuvent être soumises à restriction avec un serveur Windows Server 2012 (ou supérieur) et des clients Windows 11 (Professionnel ou Entreprise) ayant la fonctionnalité AppLocker activée :
 - Fichiers exécutables : .exe, .com...
 - Scripts : .ps1, .bat, .cmd, .vbs, .js...
 - Fichiers d'installation : .msi, .msp, .mst...
 - Applications empaquetées : .appx...
 - Fichiers DLL (*Dynamic Link Library*) : .dll, .ocx...
- AppLocker propose des règles basées sur l'éditeur et donc sur la signature numérique de ses applications : par exemple, une entreprise crée une règle autorisant toute version de l'application Skype ultérieure à la version 2.0 à s'exécuter si elle est signée par son éditeur, Microsoft. Si le produit venait à recevoir une mise à jour, la création d'une nouvelle règle ne serait ainsi pas nécessaire.
- AppLocker intègre désormais la gestion des applications et installations empaquetées, que sont les Apps de style Windows 11 disponibles depuis le magasin Microsoft Store. Ce type d'application ne nécessite pas des priviléges élevés pour s'installer et partage les mêmes attributs : nom de l'éditeur et du package, ainsi que sa version. La création d'une règle AppLocker unique s'applique de facto à tous les fichiers contenus dans le package.
- Proposée avec un client Windows 11 membre d'un domaine Active Directory, AppLocker est accessible aussi localement, depuis la console **Éditeur de stratégie de groupe locale** :

Utilisez la combinaison de touches  + R du clavier puis saisissez gpedit.msc, puis validez par la touche [Entrée].

Développez le nœud **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies de contrôle de l'application** et cliquez sur **AppLocker**.

- Avant de créer manuellement des règles ou d'en générer automatiquement, il est important de créer le jeu de règles AppLocker par défaut.
- La création des règles par défaut s'effectue en cliquant avec le bouton droit sur le type de règles, puis en choisissant l'action **Créer des règles par défaut**.

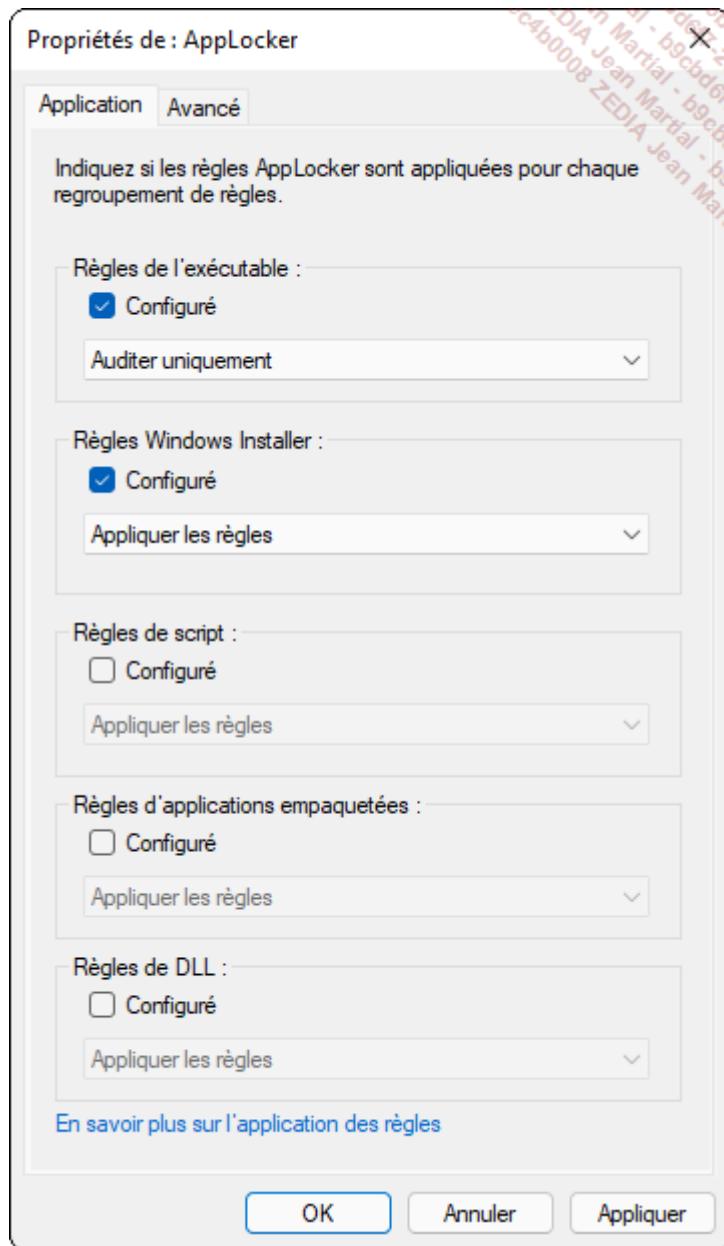


Crée les règles par défaut pour une collection de règles (recommandé).

- Les règles par défaut permettent les opérations suivantes :
 - **Règles de l'exécutable** : tous les utilisateurs peuvent exécuter les programmes contenus dans le dossier Programmes et dans le dossier Windows ; les administrateurs peuvent exécuter tous les fichiers où qu'ils se trouvent.
 - **Règles Windows Installer** : tous les fichiers signés numériquement peuvent être installés ainsi que ceux se trouvant dans le dossier %systemdrive%\Windows\Installer. Les administrateurs peuvent installer tous les programmes, qu'ils soient signés ou non.
 - **Règles de script** : tous les scripts stockés dans les dossiers Programmes et Windows peuvent être exécutés. Les administrateurs peuvent exécuter tous les scripts.
 - **Règles d'applications empaquetées** : tous les utilisateurs peuvent installer des applications empaquetées et signées numériquement.
 - **Règles DLL** : par défaut, la création de ce type de règles n'est pas activée : cochez la case **Activer le regroupement de règles DLL** dans l'onglet **Avancé** des **Propriétés** du nœud **AppLocker**. Tous les utilisateurs peuvent exécuter les DLL Microsoft Windows et toutes les DLL se trouvant dans le dossier Program Files. Les administrateurs peuvent exécuter toutes les DLL.

Notez que les utilisateurs non-administrateurs ne pourront plus exécuter les programmes installés dans leur profil (C:\Utilisateurs).

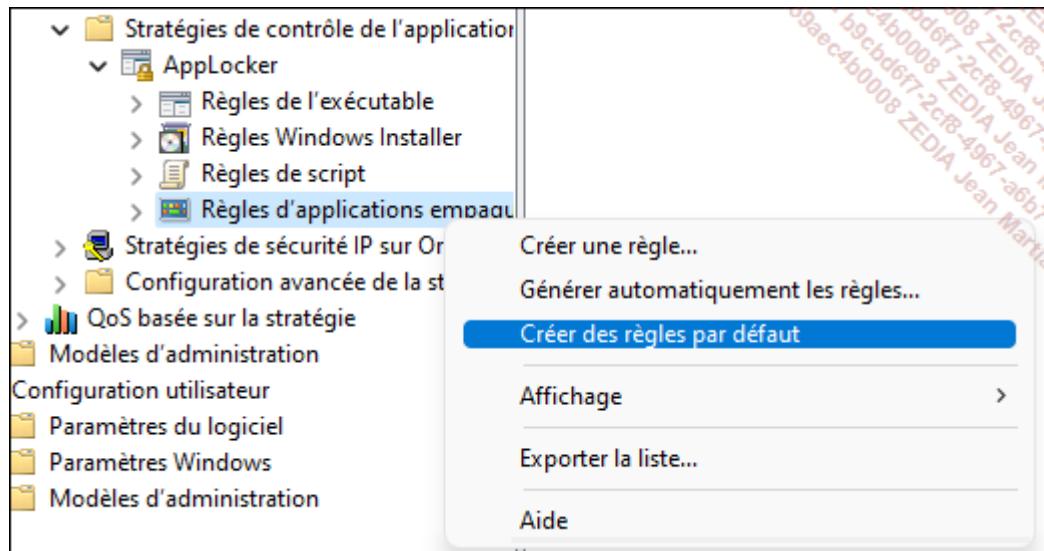
- En effectuant un clic avec le bouton droit sur le nœud **AppLocker**, puis en choisissant **Propriétés**, il est possible, pour chaque catégorie, d'auditer uniquement les règles, c'est-à-dire sans les appliquer mais en ajoutant une entrée au journal d'événements AppLocker. Ainsi, l'administrateur peut évaluer la stratégie de restriction logicielle qu'il souhaite mettre en place.



- Pour chaque catégorie, configuez **Appliquer les règles**.
- L'onglet **Avancé** permet d'activer les règles DLL et donc de pouvoir créer des contraintes sur les fichiers dont les extensions sont .dll et .ocx.
- Une fois les règles par défaut créées et appliquées, il est possible de créer des règles d'application, à l'aide de l'assistant **Générer automatiquement les règles**, et ce pour les fichiers signés et non signés. La définition d'une règle peut s'accompagner de la création d'une exception.
- Lorsqu'une règle est créée manuellement, il est nécessaire de spécifier si elle doit être autorisée ou refusée.
- Pour créer une règle empêchant l'exécution de l'app **Le Point.fr** du Microsoft Store sur un ordinateur Windows 10, procédez de la manière suivante :

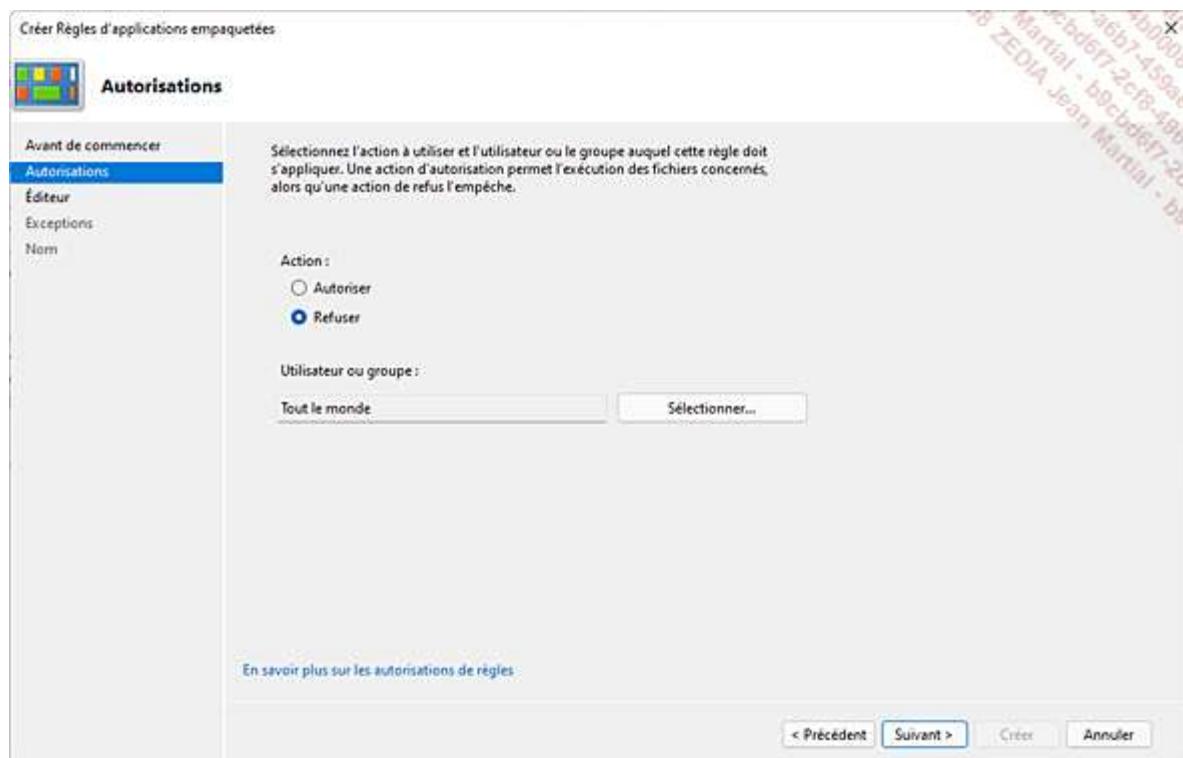
Utilisez la combinaison de touches + R du clavier puis saisissez gpedit.msc, puis validez par la touche [Entrée]. Développez le nœud **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies de contrôle de l'application** et développez l'entrée **AppLocker**.

Cliquez avec le bouton droit sur **Règles d'applications empaquetées** puis, si vous ne l'avez pas fait précédemment, cliquez sur **Créer des règles par défaut**.

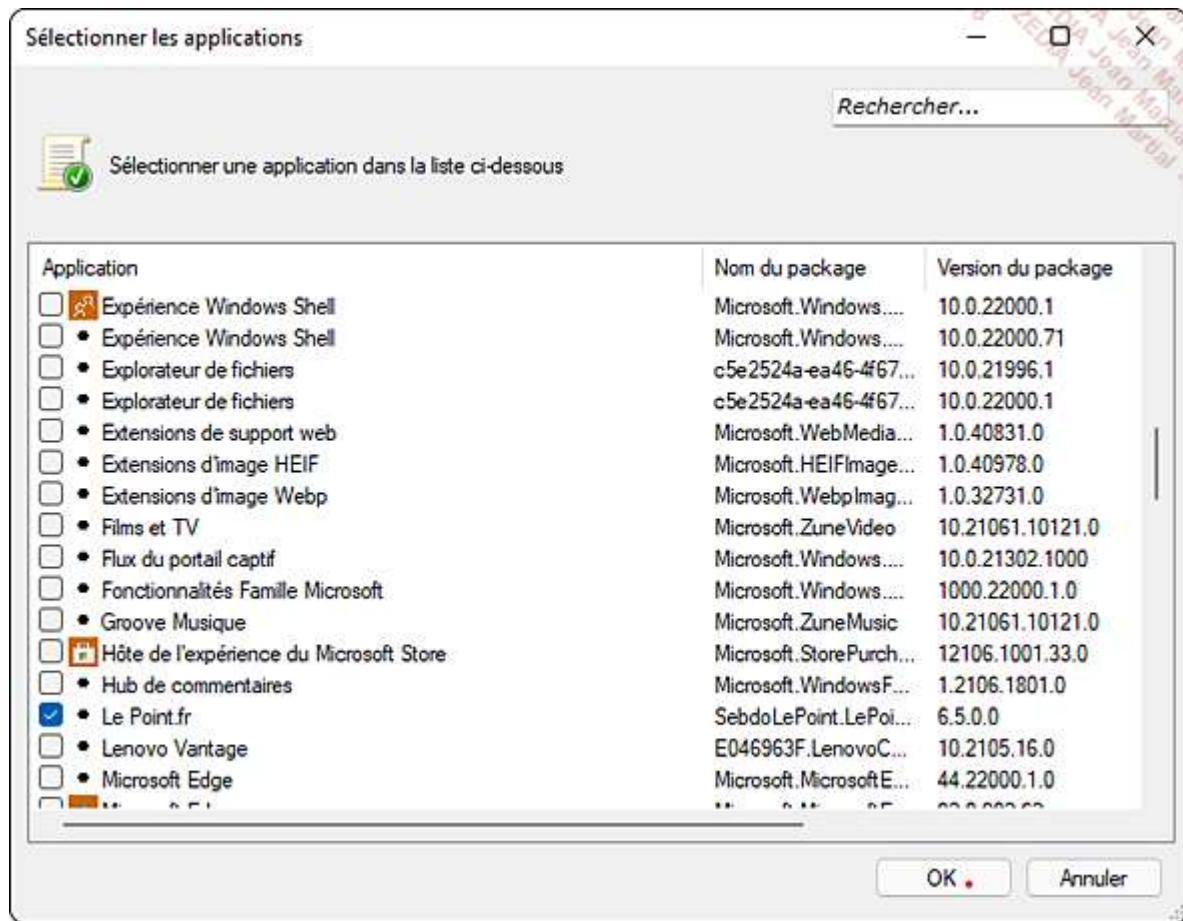


Cliquez une nouvelle fois avec le bouton droit sur **Règles d'applications empaquetées** puis sur **Créer une règle** et sur **Suivant**.

Selectionnez la case **Refuser** et laissez le groupe par défaut (**Tout le monde**). Cliquez sur **Suivant**.



Cochez la case **Utiliser une application empaquetée installée comme référence**, puis cliquez sur le bouton **Sélectionner**. La liste des applications apparaît. Vous pouvez la trier par ordre alphabétique en cliquant sur le titre de colonne **Application**. Recherchez et cochez la case **Le Point.fr**, correspondant à l'App.



Validez en cliquant sur les boutons **OK** et **Créer**.

Évitez de créer des règles sur les dossiers des profils des utilisateurs, la sécurité s'en trouverait amoindrie. En effet, un virus pourrait plus facilement se propager dans le profil courant.

- Pour appliquer les règles sur le client Windows 11, le service AppLocker **Identité de l'application**, désactivé par défaut, doit être démarré manuellement :

Depuis l'écran d'accueil, pressez les touches + R puis saisissez services.msc dans la fenêtre **Exécuter** et validez par la touche [Entrée].

Cliquez avec le bouton droit sur le service **Identité de l'application**, puis sur **Démarrer**.

Assurez-vous aussi que la case **Configuré** est cochée dans le champ **Règles d'applications empaquetées** des propriétés **AppLocker** et qu'**Appliquer les règles** est sélectionné dans le menu déroulant correspondant.

Si vous utilisez une édition Professionnelle de Windows 11, vous remarquerez que la configuration de la stratégie est possible, mais qu'AppLocker ne bloque pas l'application.

Device Guard

- Device Guard représente un ensemble de fonctionnalités liées à la sécurité matérielle et logicielle qui, lorsqu'elles sont définies simultanément, oblige l'utilisateur à n'utiliser que des applications préapprouvées par l'administrateur.
- La fonctionnalité utilise une sécurité basée sur la virtualisation de Windows 11 Entreprise pour isoler le service d'intégrité du code du noyau.
- Le poste de travail du salarié ne peut ainsi être utilisé que pour exécuter du code signé par des signataires approuvés par l'entreprise.
- Device Guard nécessite un microprogramme UEFI 2.3.1 ou supérieur, supportant le démarrage sécurisé, afin d'empêcher le chargement en mémoire d'applications malveillantes au cours du processus de démarrage du système d'exploitation. De plus, un conteneur protégé par Hyper-V isolant les processus critiques de Windows 11 Entreprise est requis.

256 Celui-ci doit être activé depuis les **Paramètres, Applications, Fonctionnalités facultatives, Plus de fonctionnalités Windows**.

257 Sélectionnez **Hyperviseur Hyper V**.



Depuis Windows 10 version 1607, l'activation des fonctionnalités n'est pas nécessaire. La stratégie de groupe installera les fonctionnalités.

- L'approbation par Device Guard de vos applications est créée lorsque ces dernières sont signées à l'aide d'une signature issue du Microsoft Store, de votre PKI ou d'une autorité de certification de confiance.
- La gestion d'ordinateurs protégés par Device Guard est assurée via les stratégies de groupe, Windows PowerShell, Intune ou encore Microsoft Endpoint Configuration Manager.

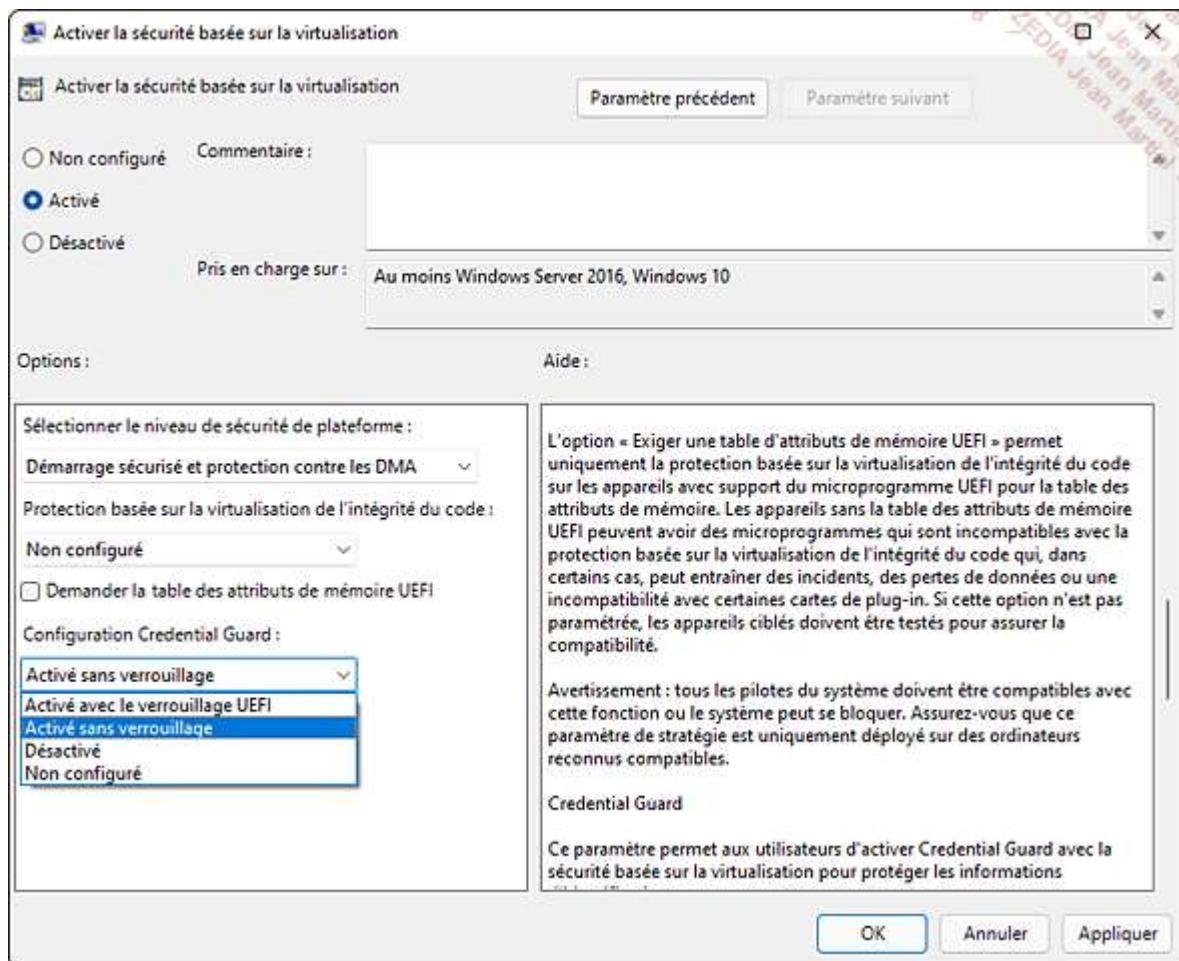
- La stratégie de groupe locale (gpedit.msc) utilise le nœud **Activer la sécurité basée sur la virtualisation** pour activer la prise en charge du mode **Secure-Boot** depuis le chemin ci-dessous : **Configuration Ordinateur - Modèles d'administration - Système - Device Guard**.

Windows Defender Credential Guard

- Windows Defender Credential Guard apporte une couche de sécurité supplémentaire car, couplée avec Device Guard, les utilisateurs d'un domaine Active Directory auront leur mot de passe stocké dans un conteneur virtuel et non dans LSA (*Local Security Authority*). Credential Guard a pour fonction de protéger les données confidentielles d'un ordinateur virtuel Hyper-V, comme il le ferait pour un ordinateur physique.
- Une architecture 64 bits avec Windows 11 Entreprise installé sur un ordinateur physique, ainsi qu'un microprogramme UEFI 2.3.1 minimum et une infrastructure Hyper-V avec les extensions Intel VT-x/AMD-V et SLAT (*Second Level Address Translation*), sont nécessaires.

La stratégie de groupe locale (gpedit.msc) utilise le nœud **Activer la sécurité basée sur la virtualisation** pour activer la prise en charge du mode **Secure-Boot** depuis le chemin ci-dessous : **Configuration ordinateur - Modèles d'administration - Système - Device Guard**.

Cliquez sur la case **Activé** et, dans le champ **Configuration Credential Guard**, sélectionnez **Activé sans verrouillage**.



Configuration du Pare-feu Windows Defender avec fonctions avancées de sécurité

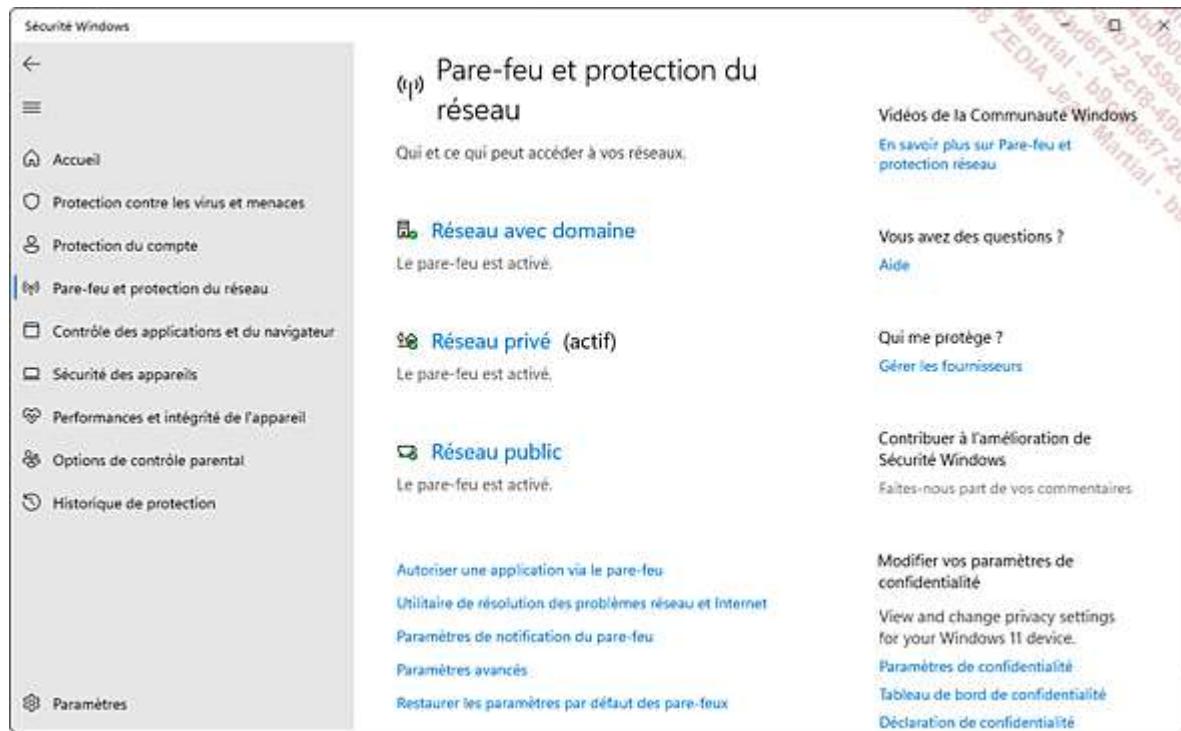
- Un pare-feu est l'équivalent d'un verrou apposé sur une porte, il complique la tâche d'une personne mal intentionnée, sans protéger complètement l'ensemble de l'habitation. Il doit être utilisé en conjonction d'autres mesures, comme l'utilisation d'un antivirus ou la gestion des mises à jour de sécurité.
- Il a pour fonction la protection du poste de travail Windows 11 contre les accès non autorisés d'ordinateurs présents sur un réseau (Internet, local...).
- Le pare-feu fourni avec Windows XP était considéré comme peu sûr, car il ne filtrait que les communications entrantes. Le pare-feu avec fonctions avancées de sécurité livré avec Windows 11 vérifie que les paquets qui circulent sont sûrs grâce à une connexion initiée (pare-feu avec état) et procure un filtrage dans les deux sens des flux transitant.
- Windows 11 gère des profils réseau, en référence au lieu dans lequel se trouve l'utilisateur. À chaque première connexion, celui-ci est invité à définir son emplacement actuel : privé (domicile), domaine (entreprise) et public (cybercafé). Par exemple, l'administrateur peut autoriser l'accès au Bureau à distance (port par défaut 3389 en TCP) lorsque l'utilisateur se trouve sur le domaine de la société, et refuser son utilisation lorsqu'il est connecté depuis un réseau moins sécurisé, comme celui d'un cybercafé. Pour chaque emplacement, le pare-feu possède un ensemble de règles par défaut appliquée.
- Windows 11 est livré avec deux pare-feu, l'un proposant des actions simples, comme autoriser ou non un programme, c'est le **Pare-feu Windows Defender**, l'autre offrant une gestion plus précise des paramètres, c'est le **Pare-feu Windows Defender avec fonctions avancées de sécurité**.

258 Le Pare-feu Windows est accessible depuis les **Paramètres, Confidentialité et sécurité, Sécurité Windows**.

259 Cliquez sur le bouton **Ouvrir Sécurité Windows**.



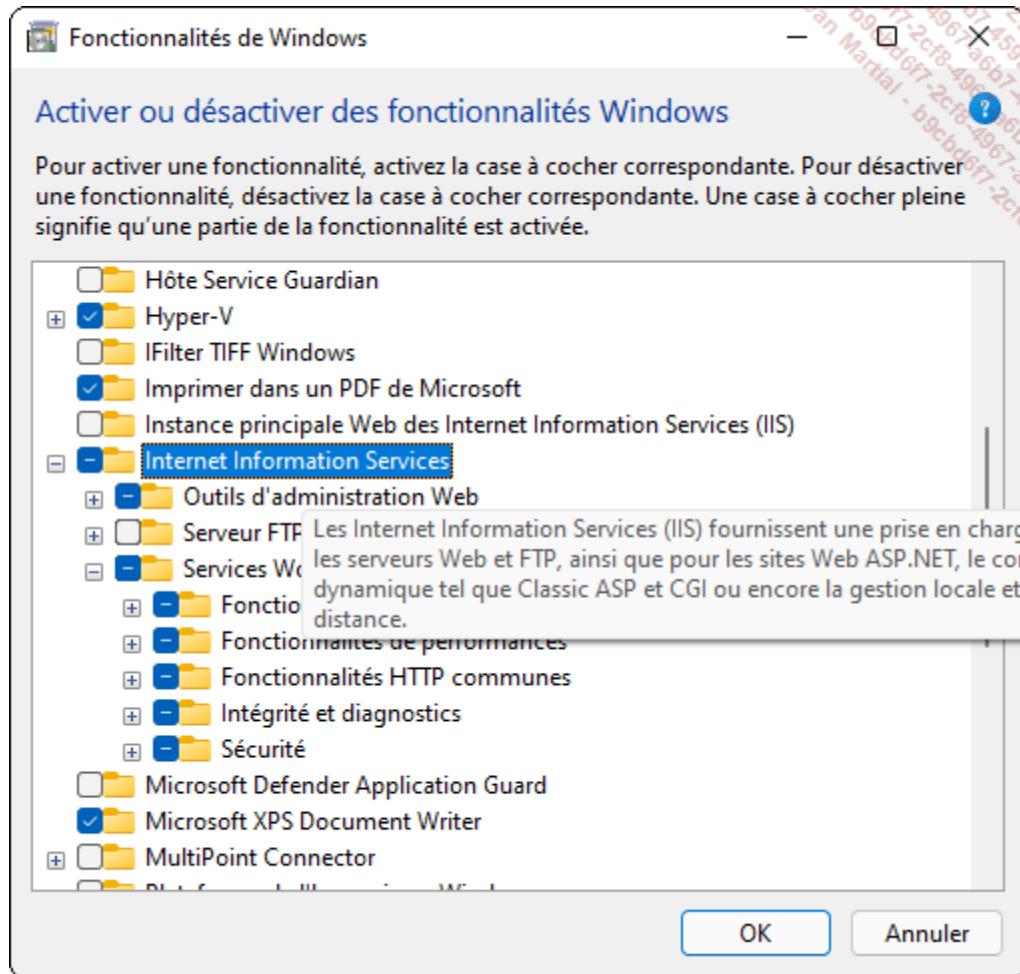
260 Dans la fenêtre **Sécurité Windows**, cliquez sur **Pare-feu et protection du réseau**, puis **Paramètres avancés**. Validez par **Oui** le message de contrôle de compte utilisateur.



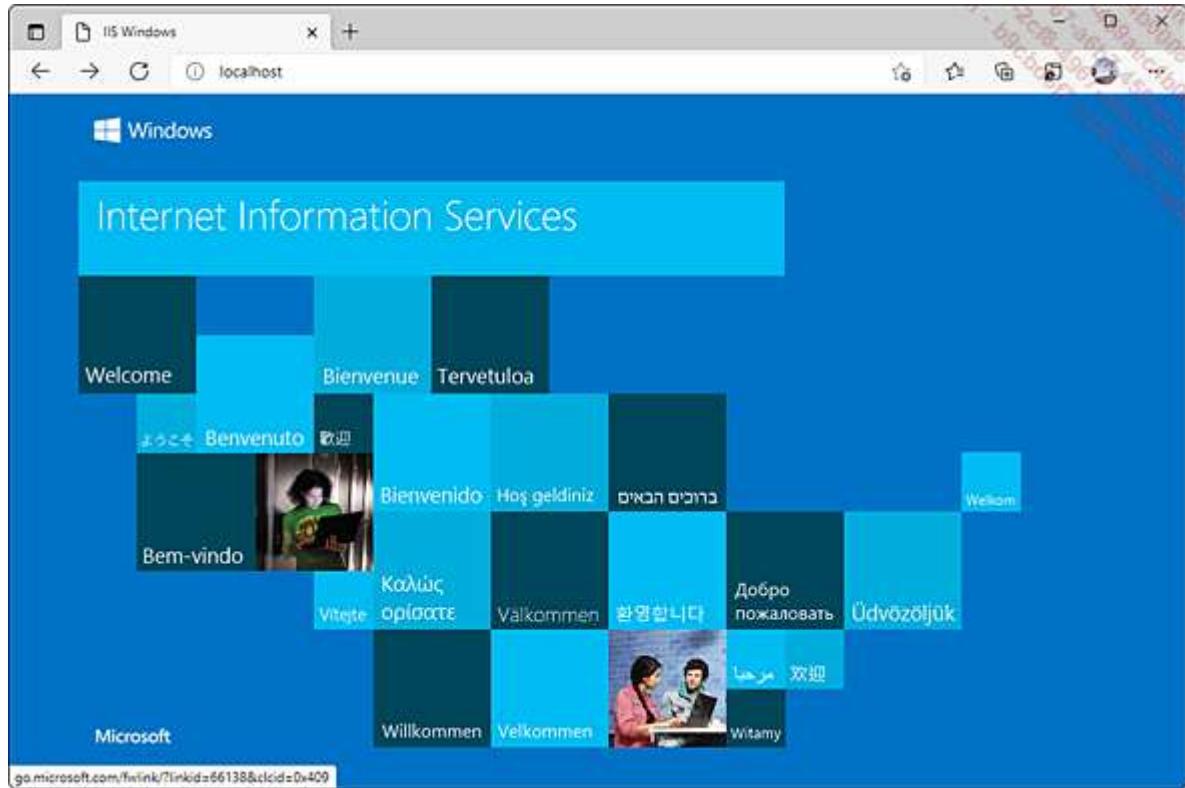
- Il est possible d'accéder au pare-feu depuis le **Panneau de configuration**, et au Pare-feu avec fonctions avancées de sécurité depuis les **Outils Windows** ou depuis **Paramètres avancés** de l'interface Pare-feu Windows.
- Le pare-feu Windows 11 propose de créer des exceptions manuellement, permettant ainsi à des programmes ou des ports de communiquer avec l'extérieur. En cas de problème de sécurité lié à l'utilisation du pare-feu, les notifications sont affichées dans le Centre de notifications.
- Par exemple, pour créer une règle de trafic entrant refusant l'accès à votre serveur web Windows 11 sur le Pare-feu avec fonctions avancées de sécurité, il est dans un premier temps nécessaire d'installer la fonctionnalité IIS, qui est le serveur web de Microsoft :

261 Ouvrez les **Paramètres** depuis le menu **Démarrer**. Cliquez sur **Applications, Fonctionnalités facultatives**. Cliquez ensuite sur **Plus de fonctionnalités Windows**.

262 Dans la fenêtre **Fonctionnalités de Windows**, cochez la case **Internet Information Services** et validez par **OK**.

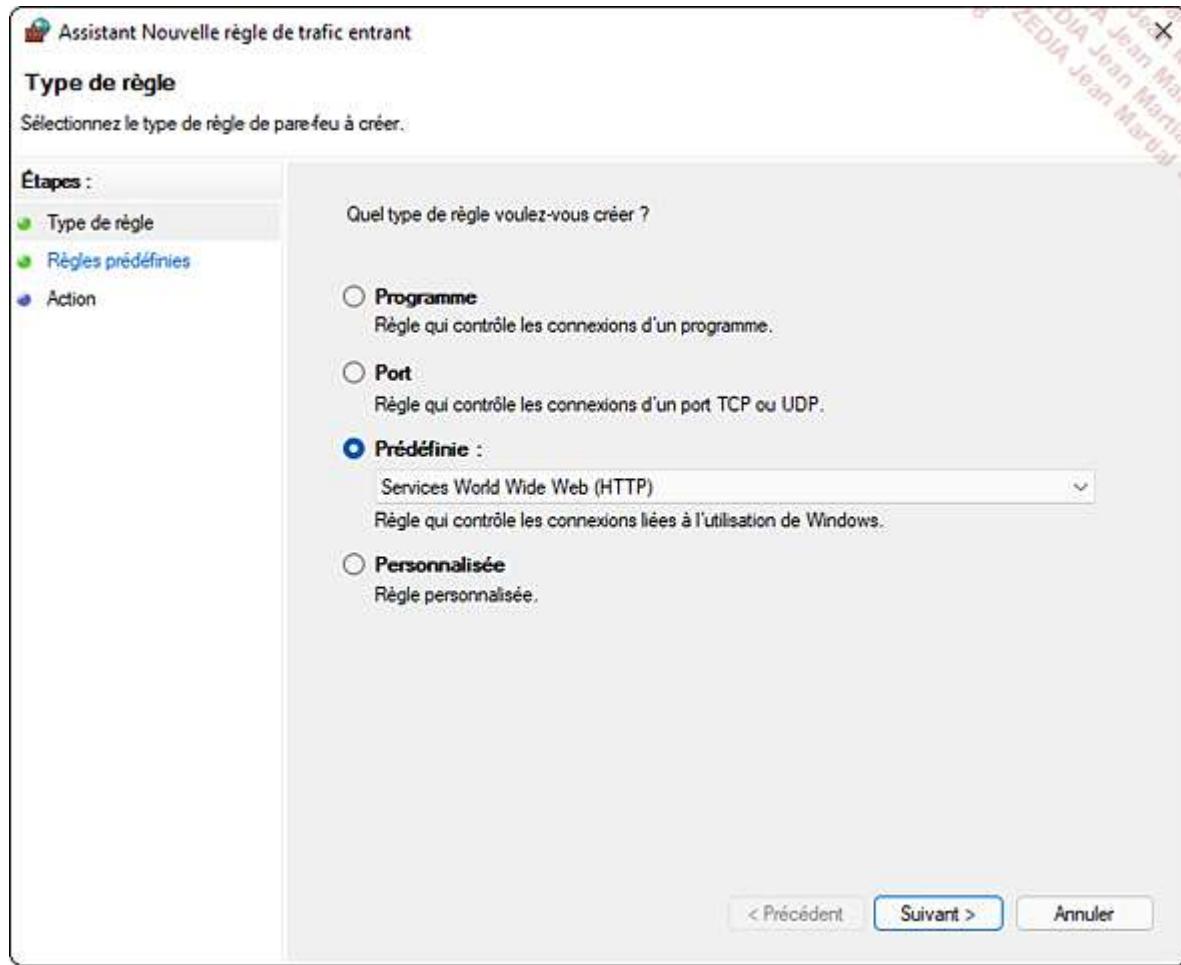


263 Une fois l'installation terminée, cliquez sur le bouton **Fermer**. Exécutez le navigateur **Microsoft Edge** depuis l'icône située dans la barre des tâches, et saisissez l'URL <http://localhost/> dans la barre d'adresse. Le logo IIS apparaît :



- Il faut maintenant configurer le pare-feu pour empêcher l'accès à ce site IIS :

- 264 Depuis l'écran d'accueil, pressez les touches + R puis saisissez wf.msc dans la fenêtre **Exécuter** et validez par la touche [Entrée]. Il s'agit d'une autre manière d'accéder aux paramètres avancés du pare-feu.
- 265 Dans le volet de gauche de la fenêtre **Pare-feu Windows Defender avec fonctions avancées de sécurité**, effectuez un clic avec le bouton droit sur **Règles de trafic entrant**, puis cliquez sur **Nouvelle règle**.
- 266 Choisissez le type de règle à créer : **Programme, Port** (UDP ou TCP), **Prédefinie** (liée aux fonctionnalités de Windows 11) ou **Personnalisée** (combine programme, protocole et ports).
- 267 Dans cet exemple, choisissez **Prédefinie** et sélectionnez **Services World Wide Web (HTTP)** dans la liste déroulante.



268 Cliquez sur le bouton **Suivant** puis cochez la case **Services World Wide Web (trafic http-entrant)** et une nouvelle fois sur **Suivant**.

269 Cochez la case **Bloquer la connexion**. Notez que vous pourriez **Autoriser la connexion si elle est sécurisée** (protocole IPsec). Validez le choix en cliquant sur le bouton **Terminer**.

- En PowerShell, la commande New-NetFirewallRule permet de créer des règles entrantes ou sortantes sur un ensemble de postes :

- Pour bloquer le port TCP 80 en flux entrant sur le poste de travail Windows 11, cela donne :

```
New-NetFirewallRule -DisplayName "Blocage IIS" -Direction Inbound  
-LocalPort 80 -Protocol TCP -Action Block
```

- Pour modifier une règle existante, utilisez la commande PowerShell :

```
Set-NetFirewallRule
```

- La suppression d'une règle de pare-feu s'effectue à l'aide de la commande :

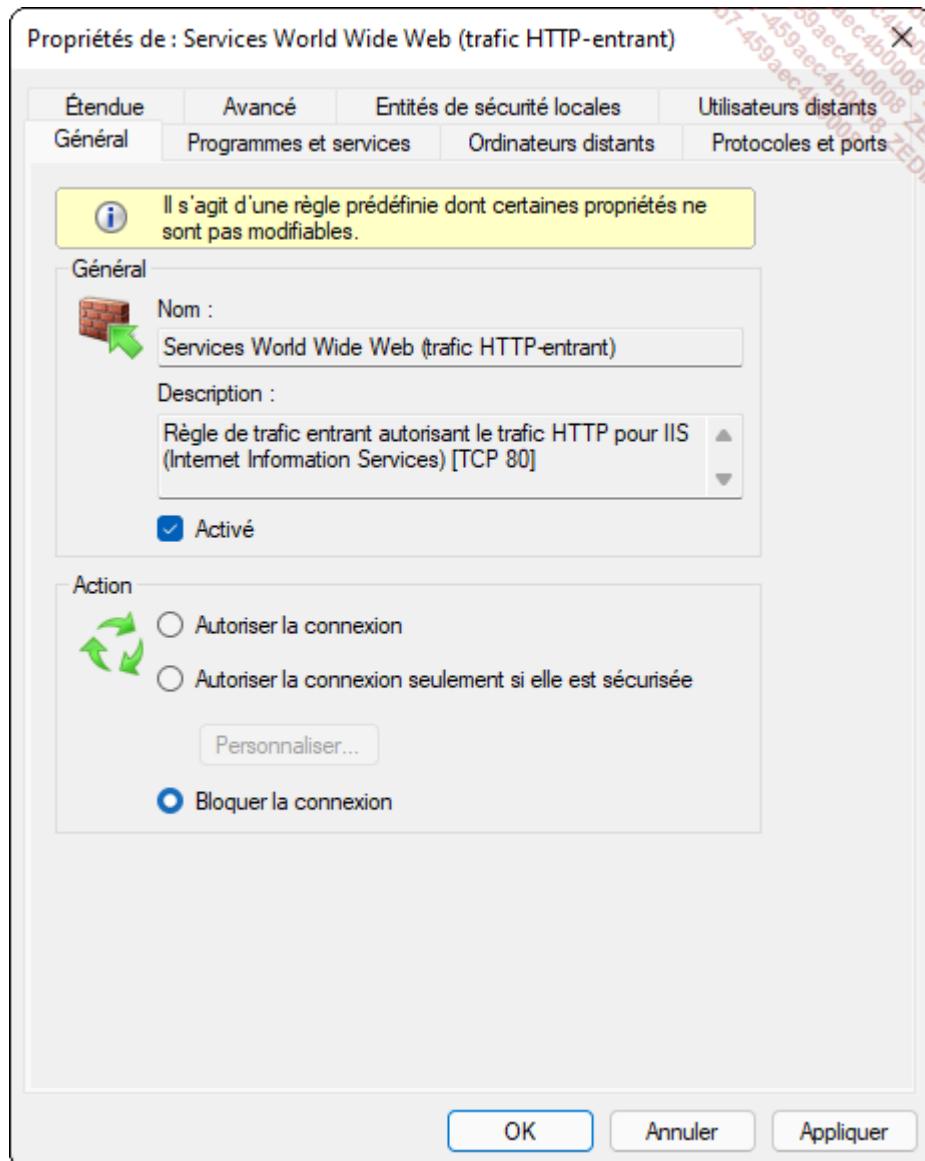
```
Remove-NetFirewallRule
```

- Testez maintenant la connexion au site interne IIS :

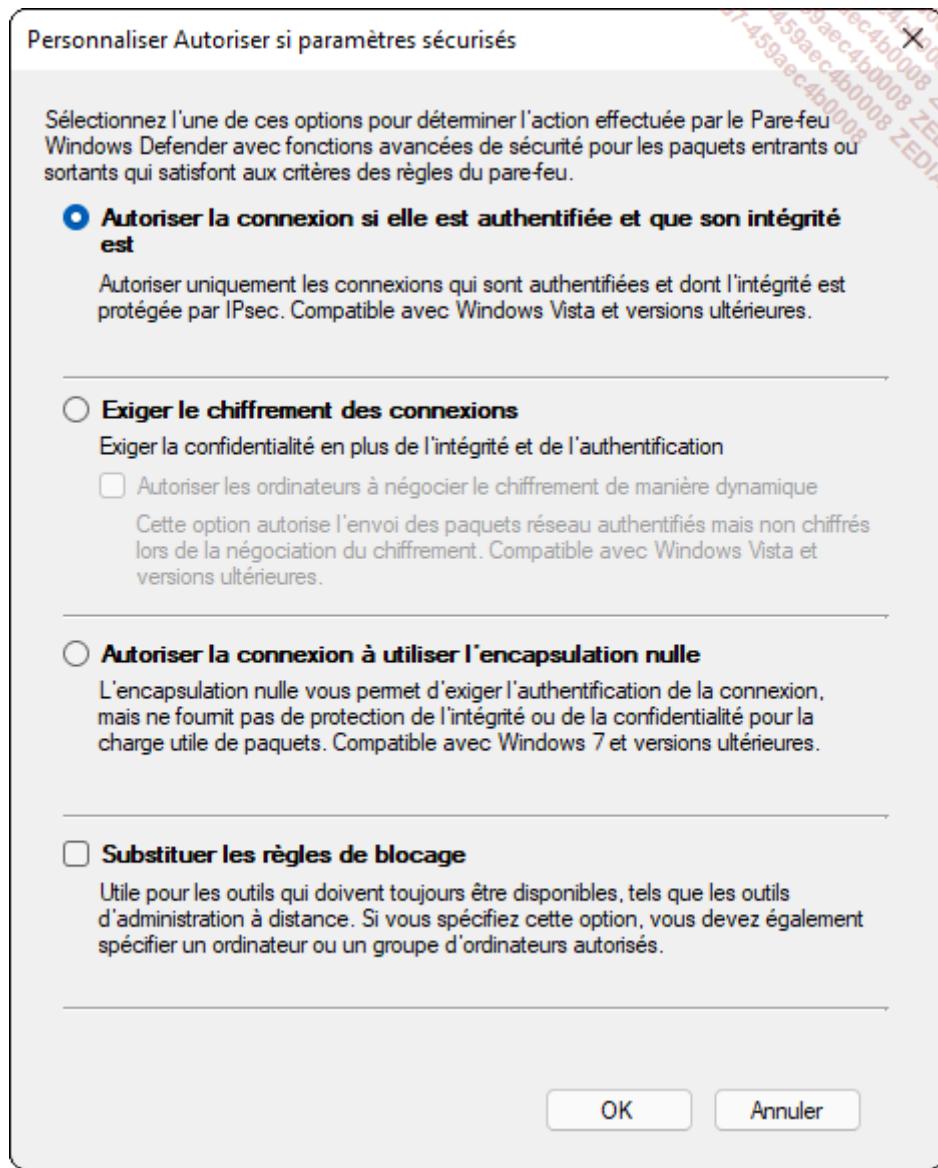
270 Saisissez une nouvelle fois l'URL <http://localhost> dans le navigateur Microsoft Edge. Le site IIS ne s'affiche plus.

- Une fois la règle créée, il est possible de lui définir des paramètres avancés en la sélectionnant avec le bouton droit et en éditant ses **Propriétés**. Par exemple, l'onglet **Étendue** spécifie les adresses IP locales et distantes

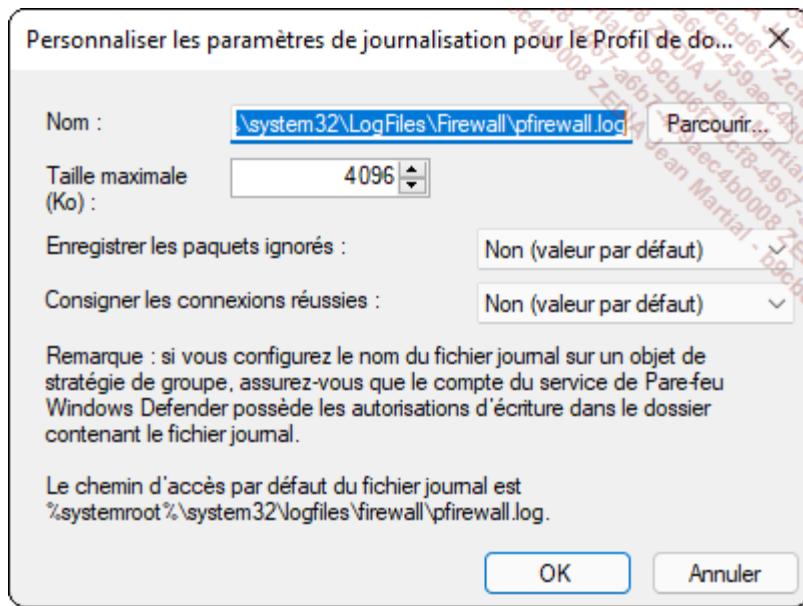
auxquelles la règle doit s'appliquer. L'administrateur peut aussi définir une règle de connexion sécurisée entre deux ressources dans l'onglet **Général**, section **Action**.



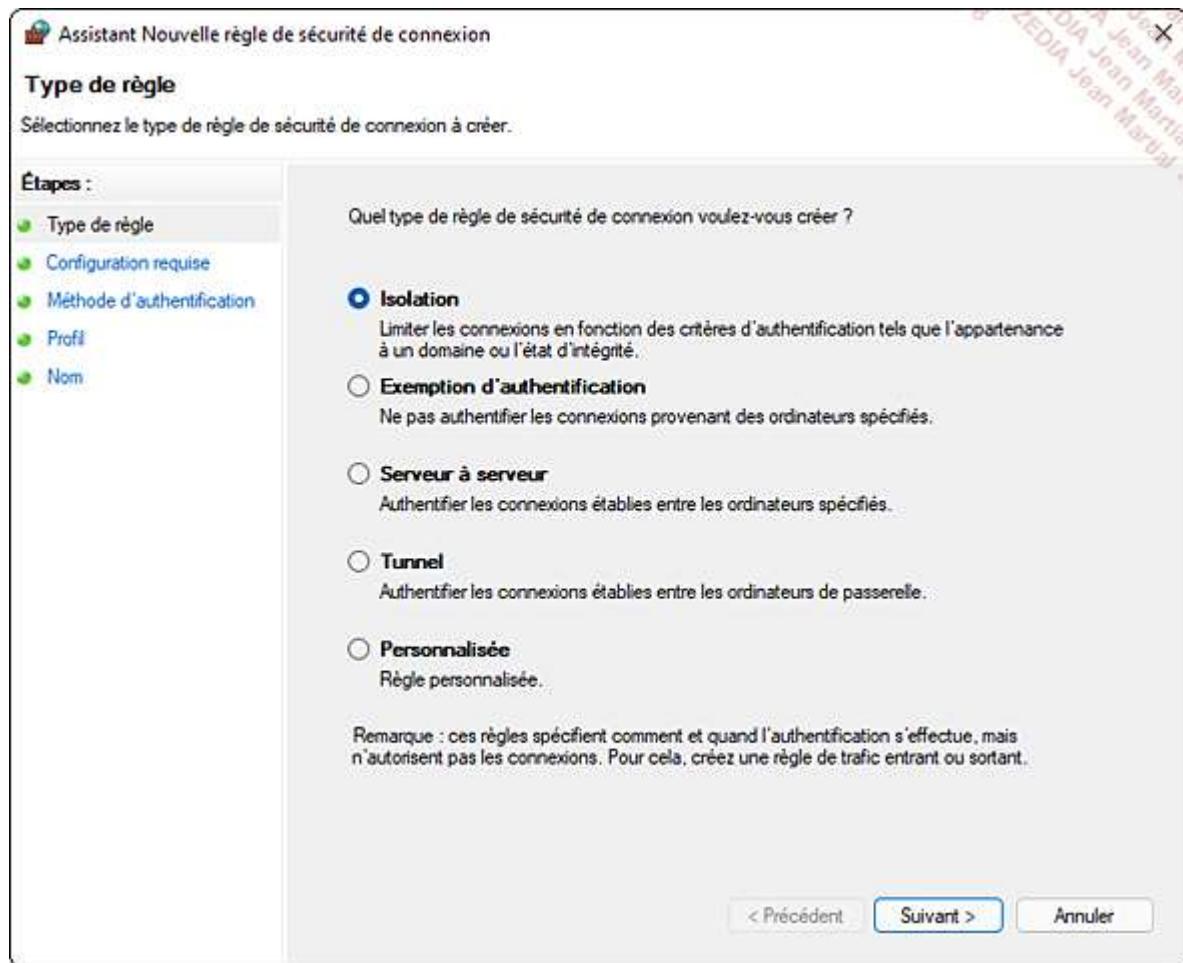
- Ainsi, il est possible de s'assurer qu'un serveur de fichiers ne répondra à des requêtes clientes que si la connexion initiée l'est de façon sécurisée. Les options, accessibles via le bouton **Personnaliser...**, sont les suivantes :
 - **Autoriser la connexion si elle est authentifiée et que son intégrité est protégée par IPsec** : cette option nécessite un système Windows Vista ou supérieur.
 - **Exiger le chiffrement des connexions** : l'administrateur peut autoriser les ordinateurs à négocier le chiffrement de manière dynamique. Cette règle est applicable uniquement au trafic entrant.
 - **Autoriser la connexion à utiliser l'encapsulation nulle** : cette option est disponible uniquement pour un client Windows 7 ou supérieur. Elle exige que le client s'authentifie, sans toutefois assurer de contrôle d'intégrité ou de chiffrement de la connexion entre les parties.
 - **Substituer les règles de blocage** : dans la règle par défaut du pare-feu Windows, une règle qui bloque explicitement est toujours prioritaire sur une règle qui laisse passer. En sélectionnant cette option, la connexion sera autorisée même si une autre règle la bloque. Elle nécessite de spécifier les ordinateurs autorisés dans l'onglet **Ordinateurs distants** des propriétés de la règle.



- Il est possible de définir le comportement du pare-feu en fonction de l'emplacement de la machine :
- 271 Cliquez avec le bouton droit sur le nœud **Pare-feu Windows avec fonctions avancées de sécurité sur l'ordinateur local** puis choisissez **Propriétés**.
- 272 Choisissez l'onglet correspondant au profil que vous souhaitez modifier : connexion à un domaine, à un réseau privé ou public.
- 273 Dans la section **Enregistrement**, cliquez sur le bouton **Personnaliser**.
- 274 Configurez les paramètres de journalisation relatifs à chaque profil : nom du journal, taille maximale en Ko et les types d'événement à enregistrer (**paquets ignorés, connexions réussies**).
- 275 Par défaut, les enregistrements sont stockés dans le dossier **%systemroot%\system32\LogFiles\Firewall\pfirewall.log**.



- Pour vérifier que le port 80 est bien ouvert sur le pare-feu Windows 11, exécutez dans une invite de commandes la commande : netstat -an | find "80" et vérifiez la ligne **LISTENING**.
- Dans la console d'administration du pare-feu avec fonctions avancées de sécurité, le nœud **Règles de sécurité de connexion** propose un ensemble de règles prédéfinies pour améliorer la sécurité d'une communication. Quatre types de règles sont proposés, plus un cinquième que vous pouvez personnaliser :
 - **Isolation** : l'ordinateur n'acceptera que les connexions d'ordinateurs ou d'utilisateurs membres de son domaine. Toute autre connexion sera rejetée.
 - **Exemption d'authentification** : les ordinateurs spécifiés n'auront pas besoin de s'authentifier lors de la connexion.
 - **Serveur à serveur** : fonctionne de façon analogue à l'isolation, mais ne s'applique finalement qu'à un ensemble défini d'adresses IP dont les hôtes sont membres d'un domaine.
 - **Tunnel** : sécurise les communications sans utiliser le mode de transport IPsec mais plutôt le mode tunnel.



- En créant un objet stratégie de groupe, l'administrateur du domaine a la possibilité de forcer l'activation du pare-feu et de créer des règles personnalisées homogènes sur son réseau : ces paramètres prévaudront même si l'utilisateur final est administrateur local de son poste Windows 11. Cette action s'effectue en éditant un objet stratégie de groupe et en sélectionnant le nœud **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Pare-feu Windows Defender avec fonctions avancées de sécurité** et **Pare-feu avec fonctions avancées de sécurité**.
- Pour rendre inactif un profil ou plusieurs profils du pare-feu, il existe plusieurs manières de procéder.
- Il est possible de passer par la fenêtre des **Paramètres**, menu **Confidentialité et Sécurité, Sécurité Windows**.

276 Cliquez sur **Ouvrir Sécurité Windows**, puis sur **Pare-feu et protection du réseau**.

277 Cliquez sur votre réseau actuel (**Réseau avec domaine, Réseau privé ou Réseau public**) et désactivez le pare-feu.

- Vous pouvez utiliser la console **Pare-feu Windows Defender avec fonctions avancées de sécurité** (wf.msc) :

278 Cliquez avec le bouton droit sur **Pare-feu Windows Defender avec fonctions avancées de sécurité** sur **Ordinateur local**, puis choisissez **Propriétés**.

279 Cliquez sur l'onglet du profil à désactiver, et sélectionnez **Inactif** dans le champ **État du pare-feu**.

- Ou encore la ligne de commande :

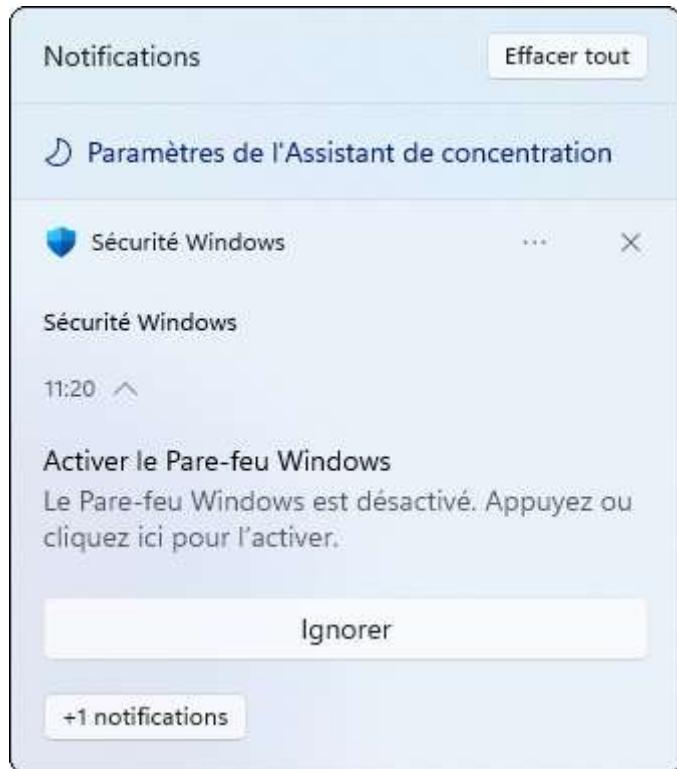
280 Pour désactiver tous les profils, ouvrez un Terminal Windows en tant qu'administrateur puis saisissez :
netsh advfirewall set allprofiles state off

281 La désactivation du pare-feu sur tous les profils d'un poste Windows 11 est également possible grâce à la commande PowerShell :

```
Set-NetFirewallProfile -Profile Domain,Public,Private
```

-Enabled false

- Un message apparaît dans la zone de notification située en bas à droite, vous avertissant de la désactivation du pare-feu.



- Dans la console d'administration du pare-feu avec fonctions avancées de sécurité, le nœud **Analyse**, puis **Pare-feu** affiche les règles de pare-feu et de sécurité en vigueur, les profils actifs ainsi que leurs paramètres, et les associations de sécurité.
- Son utilisation prend tout son sens lorsque l'administrateur a besoin d'avoir une vue globale des ports ouverts. Les colonnes **Port local** et **Port distant** affichent ceux-ci en fonction de la règle du pare-feu. Le menu **Affichage** et **Ajouter/Supprimer des colonnes...** permet à l'administrateur de personnaliser l'interface.

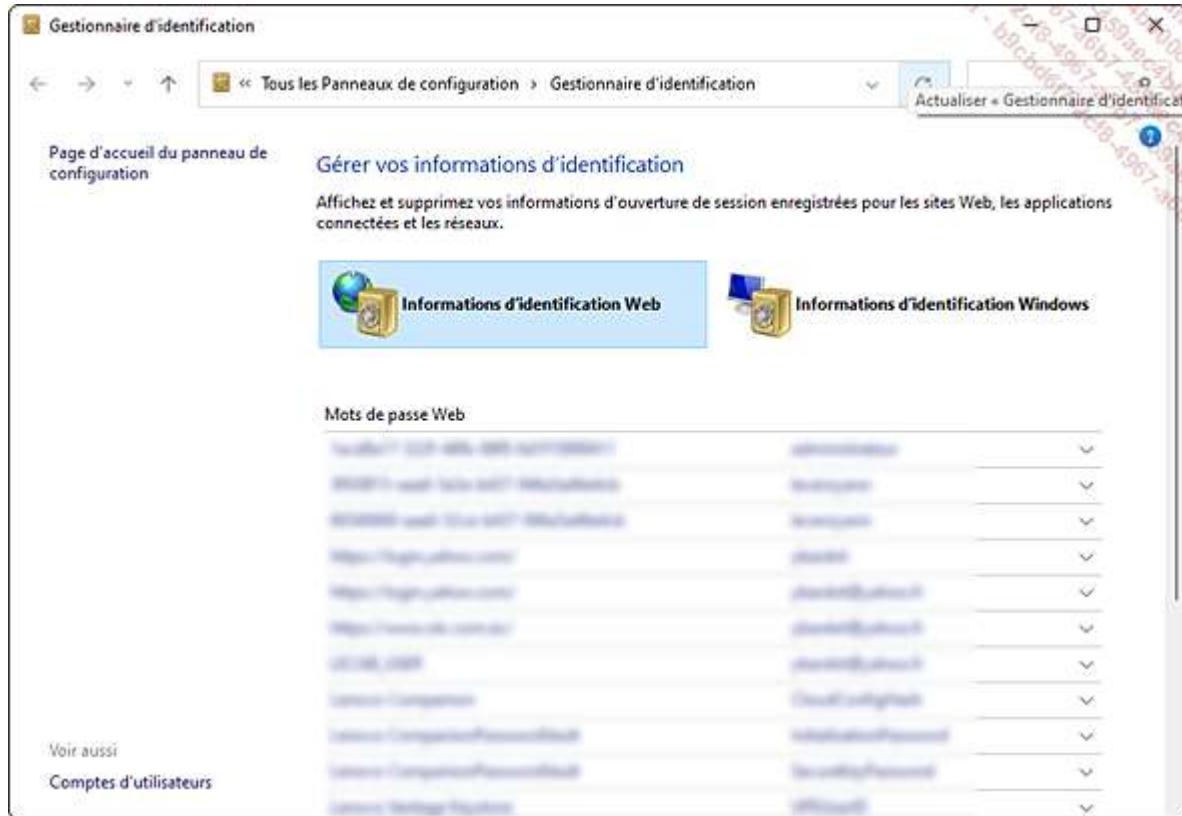
Règles de connexion								
Nom	Profil	Action	Remplacer	Direction	Programme	Adresse locale	Adresse distante	Protocole
0@Microsoft.Todos_0.48.41972.0_x64_Bea...	Dome...	Autoriser	Non	Entrant	Tout	Tout	Tout	Tous
0@Microsoft.Todos_0.48.41972.0_x64_Bea...	Dome...	Autoriser	Non	Entrant	Tout	Tout	Tout	Tous
0@Microsoft.windowscommunications...	Tout	Autoriser	Non	Entrant	Tout	Tout	Tout	Tous
0@Microsoft.windowscommunications...	Tout	Autoriser	Non	Entrant	C:\Users\yb...	Tout	Tout	TCP
0@Microsoft.windowscommunications...	Tout	Autoriser	Non	Entrant	C:\Users\yb...	Tout	Tout	UDP
Alltoys Router (TCP-In)	Dome...	Autoriser	Non	Entrant	C:\WINDOW...	Tout	Tout	TCP
Alltoys Router (UDP-In)	Dome...	Autoriser	Non	Entrant	C:\WINDOW...	Tout	Tout	UDP
App Installer	Dome...	Autoriser	Non	Entrant	Tout	Tout	Tout	Tous
App Installer	Dome...	Autoriser	Non	Entrant	Tout	Tout	Tout	Tous
App Installer	Dome...	Autoriser	Non	Entrant	Système	Tout	Sous-réseau local	TCP
Bureau à distance Microsoft	Tout	Autoriser	Non	Entrant	C:\WINDOW...	Tout	Sous-réseau local	UDP
Cast to Device streaming server (HTTP-St...)	Print	Autoriser	Non	Entrant	C:\WINDOW...	Tout	Sous-réseau local	TCP
Cast to Device streaming server (HTTP-St...)	Print	Autoriser	Non	Entrant	C:\WINDOW...	Tout	Sous-réseau local	UDP
Compte professionnel ou scolaire	Dome...	Autoriser	Non	Entrant	Tout	Tout	Tout	Tous
Compte professionnel ou scolaire	Dome...	Autoriser	Non	Entrant	Tout	Tout	Tout	Tous
Compte professionnel ou scolaire	Dome...	Autoriser	Non	Entrant	Tout	Tout	Tout	Tous
Connected Devices Platform (TCP-In)	Dome...	Autoriser	Non	Entrant	C:\WINDOW...	Tout	Tout	TCP
Connected Devices Platform (UDP-In)	Dome...	Autoriser	Non	Entrant	C:\WINDOW...	Tout	Tout	UDP
Core Networking - Destination Unreache...	Tout	Autoriser	Non	Entrant	Système	Tout	Tout	ICMPv6
Core Networking - Destination Unreache...	Tout	Autoriser	Non	Entrant	Système	Tout	Tout	ICMPv6
Core Networking - Dynamic Host Config...	Tout	Autoriser	Non	Entrant	C:\WINDOW...	Tout	Tout	UDF
Core Networking - Dynamic Host Config...	Tout	Autoriser	Non	Entrant	C:\WINDOW...	Tout	Tout	UDP
Core Networking - Infrastructure Manag...	Tout	Autoriser	Non	Entrant	Système	Tout	Tout	ICMP
Core Networking - IPv6 (Pv6-In)	Tout	Autoriser	Non	Entrant	Système	Tout	Tout	IPv6
Core Networking - Multicast Listener Du...	Tout	Autoriser	Non	Entrant	Système	Tout	Sous-réseau local	ICMPv6
Core Networking - Multicast Listener Du...	Tout	Autoriser	Non	Entrant	Système	Tout	Sous-réseau local	ICMPv6
Core Networking - Multicast Listener Du...	Tout	Autoriser	Non	Entrant	Système	Tout	Sous-réseau local	ICMPv6
Core Networking - Multicast Listener Du...	Tout	Autoriser	Non	Entrant	Système	Tout	Sous-réseau local	ICMPv6

Seules les règles qui s'appliquent aux profils actuellement actifs sont affichées par le nœud **Analyse**.

- Le noeud **Associations de sécurité** affiche des informations sur les moyens mis en œuvre pour protéger les communications entre deux ordinateurs, y compris les points de terminaison.

Gestionnaire d'identification

- L'authentification unique, ou SSO (*Single Sign-On*), permet à un utilisateur d'un système Windows 11 de ne procéder qu'à une seule authentification pour accéder à plusieurs ressources (serveurs, sites internet...). Une personne utilise souvent le même mot de passe pour accéder à des sites internet différents (Facebook, LinkedIn, messagerie électronique comme Windows Live) réduisant ainsi le niveau de sécurité de ces services : si le mot de passe partagé était subtilisé, l'ensemble des ressources qu'il protège serait compromis.
 - Face à cette problématique, Microsoft propose le **Gestionnaire d'identification**, qui est un coffre-fort électronique dont la principale fonction est le stockage sécurisé des identifiants et mots de passe utilisés régulièrement par un compte utilisateur. Windows 11 se charge ensuite de les saisir automatiquement lors de l'accès à une ressource précise.
 - Les mots de passe deviennent complexes car le travail de mémorisation n'est plus nécessaire : ce que nous ignorons ne peut être dévoilé.
 - En utilisant un compte Microsoft pour s'authentifier, l'utilisateur peut ouvrir des sessions sur d'autres postes Windows 11 et ainsi accéder à ses applications protégées par des mots de passe stockés dans le coffre-fort. Cette fonctionnalité est activée par défaut lorsque l'ordinateur est membre d'un groupe de travail, mais automatiquement désactivée lorsqu'il est joint à un domaine Active Directory, afin d'éviter la fuite de données sensibles.
 - Le Gestionnaire d'identification est associé à la protection des utilisateurs :
- Depuis le champ de recherche situé dans la barre des tâches, saisissez gestionnaire d'identification et sélectionnez **Gestionnaire d'identification**. Vous pouvez aussi y accéder depuis le **Panneau de configuration**.



- Deux catégories sont proposées :
 - **Informations d'identification Web** : lorsque l'utilisateur souhaite accéder à une page internet demandant une authentification de type nom d'utilisateur et mot de passe, Microsoft Edge affiche un bandeau en bas de la fenêtre permettant de sauvegarder ces informations.

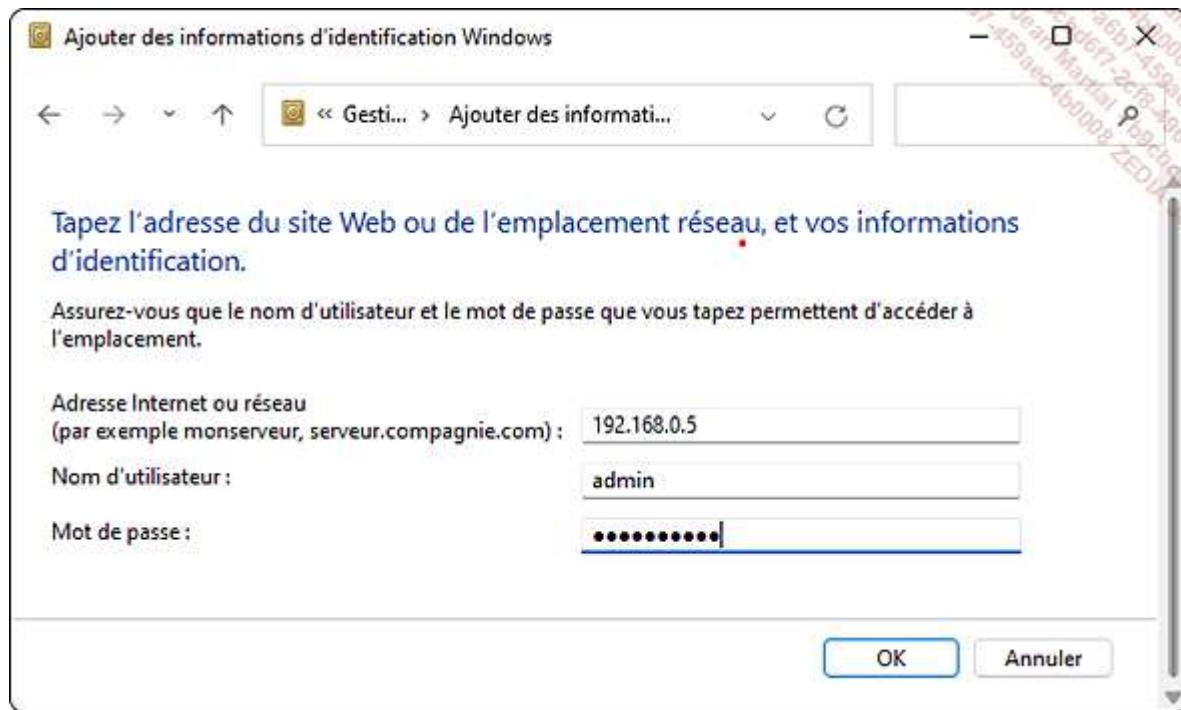


Ainsi, lors du prochain accès au site internet, les identifiants seront automatiquement saisis. Microsoft Edge gère la création de la sauvegarde des identifiants. Le Gestionnaire d'identification gère la lecture et la suppression de ces informations.

- **Informations d'identification Windows** : Windows 11 propose de sauvegarder l'identifiant et le mot de passe utilisés lors de la connexion à un serveur distant. Lorsque l'authentification s'effectue à l'aide d'une carte à puce, les **Informations d'identification à base de certificat** peuvent être stockées. La section **Informations d'identification génériques** sauvegarde les identifiants liés à des applications comme le service Windows Live. Contrairement à la catégorie Informations d'identification Web, la catégorie Informations d'identification Windows propose à l'utilisateur l'ajout ou la modification manuelle d'identifications.
- Pour sauvegarder l'accès à un serveur Windows, suivez la procédure ci-dessous :

Dans la fenêtre **Gestionnaire d'identification**, cliquez sur **Informations d'identification Windows** puis **Ajouter des informations d'identification Windows**.

Entrez l'adresse IP du serveur distant, dans l'exemple 192.168.0.5, puis saisissez un nom d'utilisateur et un mot de passe pouvant y accéder.

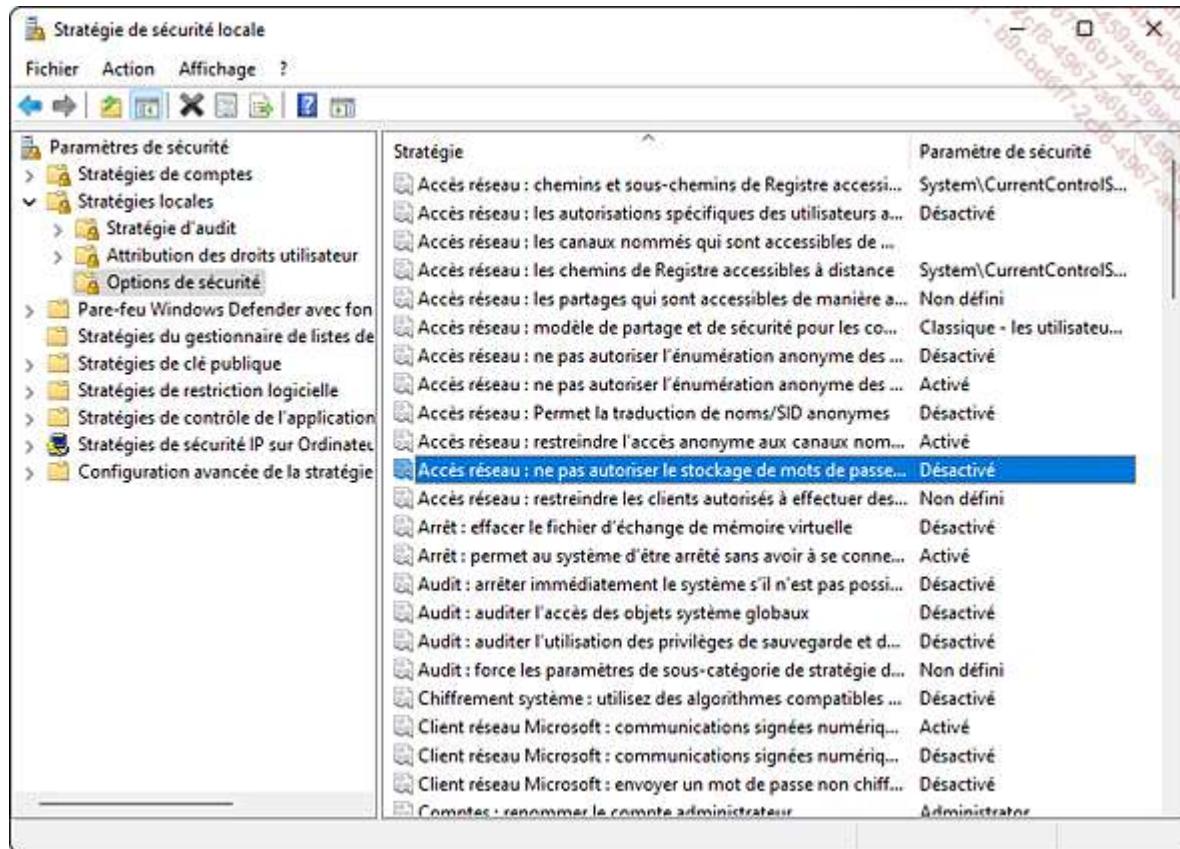


Validez en cliquant sur le bouton **OK**.

- Vous pourrez ensuite **Modifier** ou **Supprimer** les informations saisies précédemment depuis la section nommée 192.168.0.5 du **Gestionnaire d'identification**.
- Pour désactiver le stockage des identifiants liés à une authentification réseau, l'édition de la stratégie de sécurité locale est nécessaire :

Depuis l'écran d'accueil, pressez les touches + R puis saisissez secpol.msc dans la fenêtre **Exécuter** et validez par la touche [Entrée].

Depuis l'arborescence de la console **Stratégie de sécurité locale**, développez les nœuds **Stratégies locales** et **Options de sécurité**.



Double cliquez sur le paramètre **Accès réseau : ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'authentification du réseau** et cochez la case **Activé**.

Audit

- L'audit dans un domaine Active Directory ou un groupe de travail permet de suivre les actions effectuées par les utilisateurs et les ordinateurs. En fonction des informations journalisées, l'administrateur pourra visualiser et corriger un problème, mais aussi détecter une intrusion et ainsi anticiper un nouveau type d'attaque.
- Généralement, les événements des échecs sont plus instructifs que ceux liés aux réussites. Tout ne doit pas être audité, car l'utilisation de cette fonctionnalité entraîne une charge de traitement supplémentaire (CPU, RAM, espace disque) auprès des postes de travail, serveurs et contrôleurs de domaine.
- Un attaquant possédant des priviléges administrateur pourra supprimer ses traces, donc les événements stockés dans les journaux répertoriant ses actions malveillantes : il peut être intéressant de séparer les rôles, en octroyant par exemple le droit à un compte de service de générer les événements sur un serveur distant dédié au stockage, mais ce compte ne pourrait pas les supprimer ou les modifier. Un compte d'audit aurait accès aux journaux en lecture à des fins d'expertise. Ces actions peuvent être effectuées grâce aux événements transmis (cf. chapitre Protection et récupération du système, section Dépannage du système).
- La stratégie d'audit a été étendue avec Windows Server 2012 et Windows 11. Elle porte le nom de Configuration avancée de la stratégie d'audit. Ce ne sont plus neuf catégories d'événements pouvant faire l'objet d'un audit, mais 53 (en comptant les sous-catégories), classées dans les catégories suivantes :
 - Connexion de compte.
 - Gestion du compte.

- Suivi détaillé.
 - Accès DS.
 - Ouvrir/Fermer la session.
 - Accès à l'objet.
 - Changement de stratégie.
 - Utilisation de privilège.
 - Système.
 - Audit de l'accès global aux objets.
- Pour afficher la liste des catégories et des sous-catégories disponibles, saisissez la commande suivante dans un Terminal Windows exécuté en tant qu'administrateur :

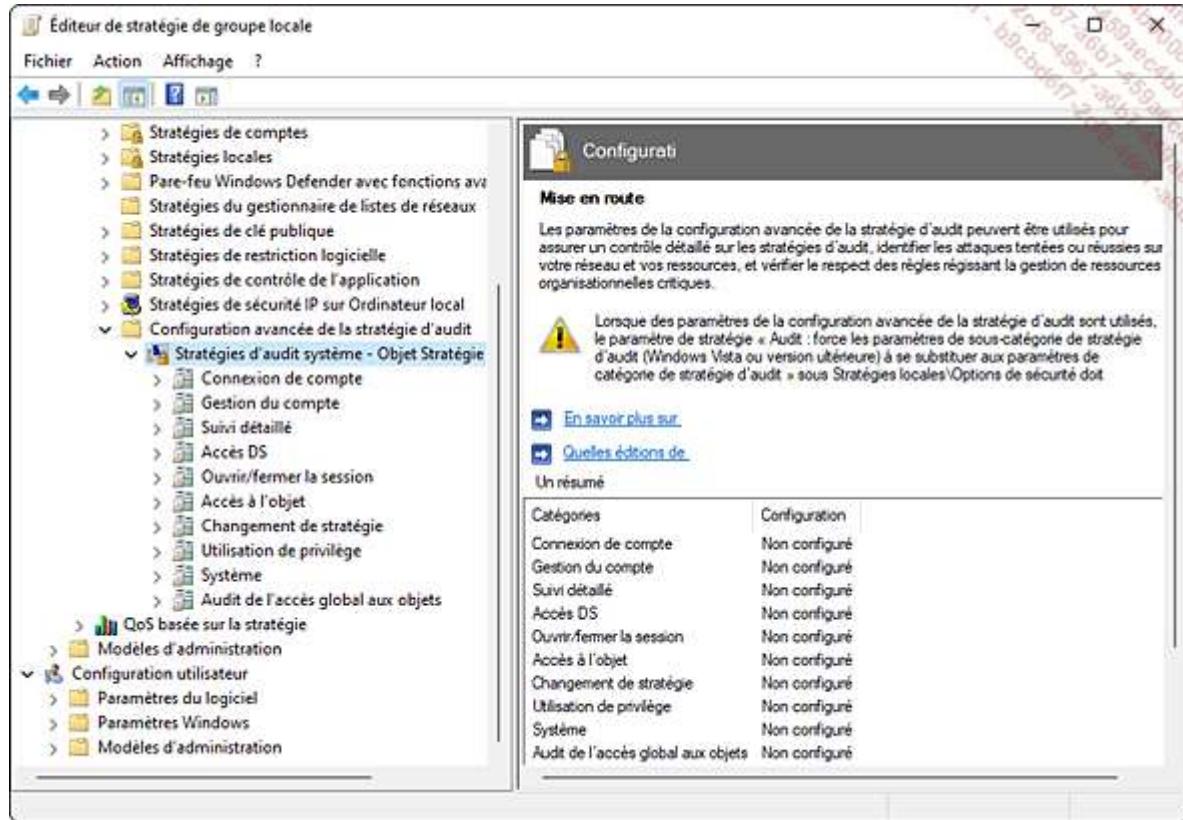
```
auditpol /get /category:*
```

```
PS C:\Users\ybard> auditpol /get /category:*
Stratégie d'audit système
Catégorie/Sous-catégorie           Paramètre
Système
  Extension système de sécurité      Pas d'audit
  Intégrité du système              Succès et échec
  Pilote IPSEC                      Pas d'audit
  Autres événements système         Succès et échec
  Modification de l'état de la sécurité Réussite
Ouverture/Fermeture de session
  Ouvrir la session                 Succès et échec
  Fermer la session                 Réussite
  Verrouillage du compte            Réussite
  Mode principal IPsec             Pas d'audit
  Mode rapide IPsec                Pas d'audit
  Mode étendu IPsec                Pas d'audit
  Ouverture de session spéciale    Réussite
  Autres événements d'ouverture/fermeture de session Pas d'audit
  Serveur NPS                      Succès et échec
  Revendications utilisateur/de périphérique Pas d'audit
  Appartenance à un groupe          Pas d'audit
Accès aux objets
  Système de fichiers               Pas d'audit
  Registre                          Pas d'audit
```

- Par exemple, si vous souhaitez auditer les modifications réussies sur les groupes de sécurité sur un client Windows 11 membre d'un groupe de travail, effectuez les opérations suivantes :

Pressez les touches + R. Saisissez gpedit.msc dans la fenêtre Exécuter puis validez par la touche [Entrée].

Dans la fenêtre Éditeur de stratégie de groupe locale, développez les nœuds Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Configuration avancée de la stratégie d'audit et Stratégies d'audit système - Objet Stratégie de groupe local.



Cliquez sur la catégorie **Gestion du compte** et double cliquez sur **Auditer la gestion des groupes de sécurité**. Dans la fenêtre de propriétés, cochez les cases **Configurer les événements d'audit suivants** et **Succès**.

282 La configuration avancée de la stratégie d'audit peut être configurée dans un objet stratégie de groupe et appliquée à des membres spécifiques du domaine.

- Un journal d'événements intéressant est celui concernant la **raison de l'accès** : lorsqu'un événement se produit, la raison pour laquelle l'opération a été autorisée ou refusée est consignée.
- **L'audit d'accès aux fichiers** contient désormais des informations précises sur les attributs du fichier auquel un utilisateur a accédé (événements numéros 4656 et 4663).
- Si un administrateur souhaite connaître l'utilisation des périphériques de stockage amovibles dans le réseau de l'entreprise, il en a la possibilité grâce à l'**Audit de périphériques de stockage amovibles**. Un événement d'audit est créé lorsqu'un utilisateur accède à une mémoire flash USB :
 - Écriture ou lecture réussies (événement numéro 4663).
 - Échecs d'accès (événement numéro 4656).
- Cette stratégie d'audit se configure depuis le nœud **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Configuration avancée de la stratégie d'audit - Stratégies d'audit système - Objet stratégie de groupe locale et Accès à l'objet**. Le paramètre se nomme **Auditer le stockage amovible**.
- Les anciennes stratégies d'audit de base sont toujours disponibles mais peuvent entrer en conflit avec l'audit avancé. Dans ce cas :

Activez le paramètre **Audit : force les paramètres de sous-catégorie de stratégie d'audit (Windows Vista ou version ultérieure)** à se substituer aux paramètres de catégorie de stratégie d'audit dans le nœud **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Options de sécurité**.

- L'audit de sécurité de base sera ainsi systématiquement ignoré au profit de l'audit avancé.
- Un autre ajout important est la journalisation des modifications du service d'annuaire. Avec les anciennes versions serveur de Windows, l'audit des services Active Directory enregistrait le nom de l'attribut modifié, mais pas son ancienne ni sa nouvelle valeur. Depuis Windows Server 2008, la sous-catégorie **Auditer les modifications du service d'annuaire** comble ce manque.
- La gestion des journaux d'événements (archivage, suppression, etc.) est importante dans un environnement d'entreprise, tout comme la compréhension des événements générés. La commande wevtutil.exe gère les événements Windows et les messages associés.
- wevtutil el affiche tous les journaux Windows.
- Pour connaître la liste des fournisseurs d'événements, la commande suivante liste tous les événements liés aux applications serveur du fournisseur Microsoft :

```
wevtutil gp "Microsoft-Windows-Application  
Server-Applications" /ge:true /gm:true
```

Sécurité dans Microsoft Edge

283 Microsoft Edge est le navigateur internet livré avec Windows 11. Il ne prend plus en charge les barres d'outils, les scripts Visual Basic et ActiveX qui étaient souvent exploités par les hackers. Les extensions utiliseront uniquement HTML5 et JavaScript.

284 De plus, Microsoft Edge héberge chaque onglet de site visité dans un bac à sable, constituant un conteneur totalement indépendant.

285 Une autre fonctionnalité intéressante est la possibilité de s'authentifier sur un site internet via son compte Microsoft (code PIN et identification biométrique).

286 Edge apporte des améliorations sur la sécurité, telles que **Navigation InPrivate**, qui permet de visiter des sites internet sans laisser de traces ou encore **SmartScreen** qui vérifie le site visité par rapport à une liste de sites répertoriés comme malveillants. On trouve également la protection contre le suivi (fonctionnalité de *tracking*) visant à empêcher un site de récupérer vos habitudes de navigation afin de vous proposer des annonces publicitaires ciblées.

287 Le navigateur de Microsoft a été créé en utilisant le cycle de vie du développement de la sécurité (SDL) : Microsoft Edge empêche par exemple un code malveillant de s'exécuter dans une mémoire définie comme non exécutable. Désormais, le blocage des fenêtres contextuelles est activé, limitant ainsi l'affichage intempestif de publicités.

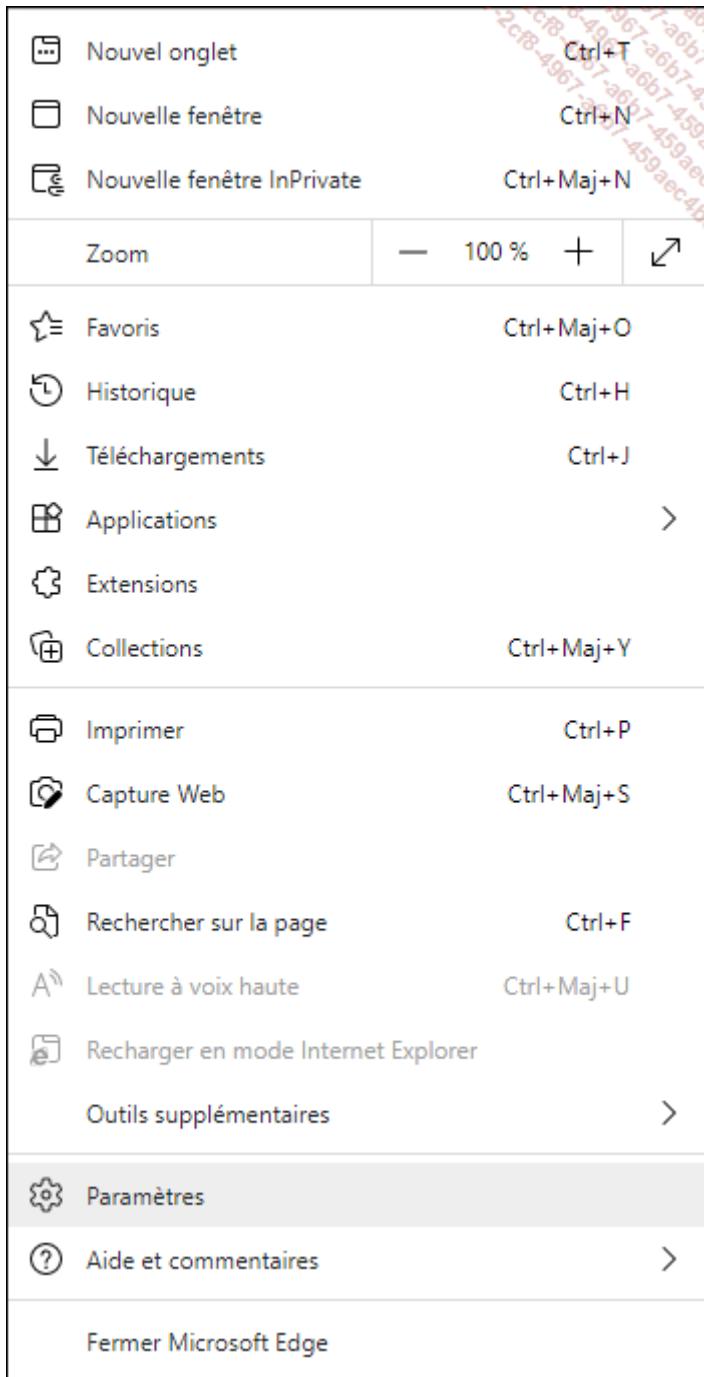
1. Protection contre le suivi

288 Lorsque l'utilisateur visite un site internet, du contenu publicitaire ciblé en fonction de ses habitudes et de son comportement peut être affiché dans le navigateur, et ainsi être exploité à des fins commerciales.

289 Microsoft part du principe que c'est à l'utilisateur de choisir les informations qu'il souhaite communiquer pour exploitation par des sites tiers, et non l'inverse.

290 La fonctionnalité de protection contre le suivi est activée par défaut. Voici comment y accéder :

Depuis le bureau, exécutez le navigateur **Microsoft Edge** en cliquant sur l'icône située dans la barre des tâches. Sélectionnez ensuite le menu **Paramètres et plus** , puis choisissez **Paramètres**.



Cliquez ensuite sur le bouton **Confidentialité, recherche et services**. Activez l'option **Envoyer des demandes Do Not Track**.

Dans la section **Protection contre le suivi, Prévention de suivi** est activé par défaut. Choisissez le niveau qui vous convient entre **Basique**, **Usage normal** ou **Strict**.

291 La protection contre le tracking reste active quels que soient les sites internet visités.

292 Microsoft Edge renforce la confidentialité des habitudes des utilisateurs, en envoyant des en-têtes DNT (*Do Not Track*) aux sites pour qu'ils ne suivent pas ces derniers. Néanmoins, un site peut demander une exception en requérant l'autorisation de suivre les utilisateurs qui le parcourent. Si l'utilisateur approuve la demande, Microsoft Edge enregistre une exception et envoie les en-têtes DNT au site internet qui autorise le suivi.

2. Filtre Microsoft Defender SmartScreen

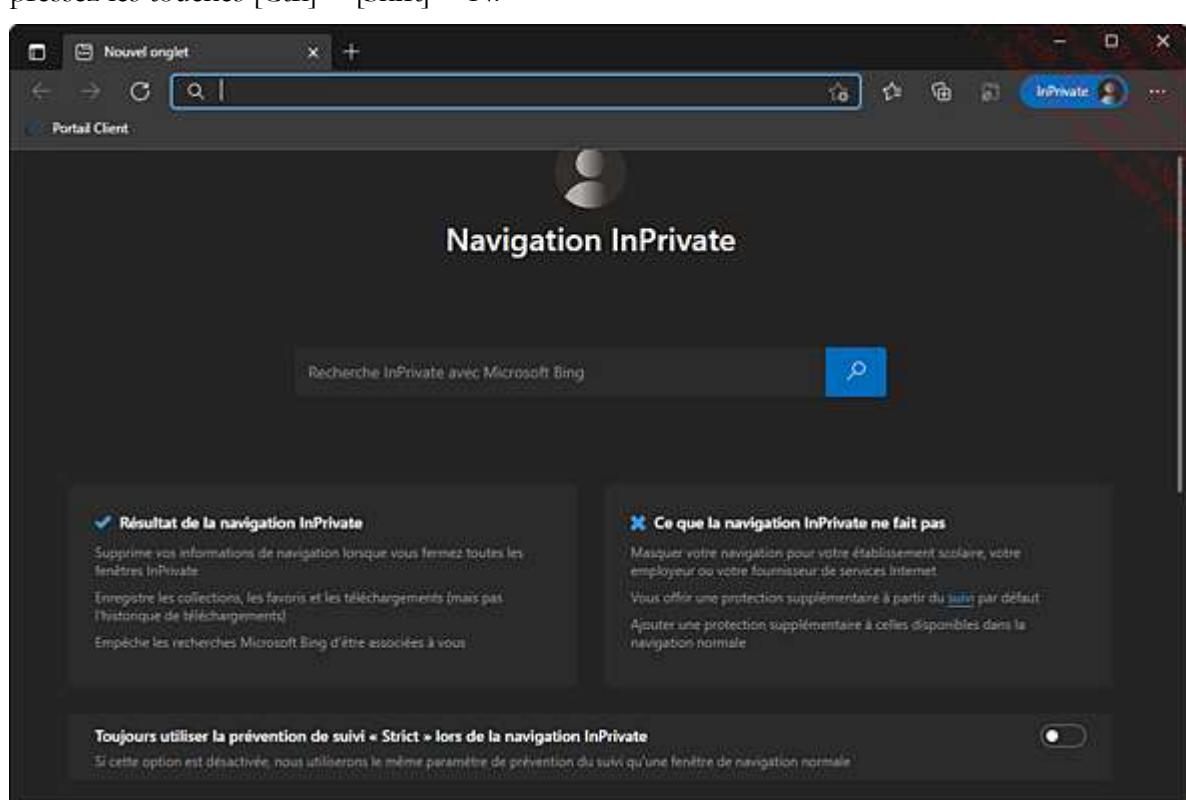
- 293 Le filtre SmartScreen vérifie les sites internet visités par rapport à une liste de sites connus pour être potentiellement dangereux (comme les sites de phishing ou hameçonnage) maintenue à jour.
- 294 Le phishing est utilisé pour récupérer des informations confidentielles (numéro de carte de crédit, nom d'utilisateur et mot de passe) auprès d'internautes en usurpant l'identité de sites ciblés, afin de faire croire à la victime qu'elle s'adresse à un tiers de confiance. La majorité des sites falsifiés font référence aux banques ou aux moyens de paiement associés, tels que Paypal.fr.
- 295 Si un site internet falsifié est détecté, Microsoft Edge bloque l'intégralité dudit site. Le filtre SmartScreen est combiné avec le module de téléchargement pour contrôler les logiciels téléchargés.

Le filtre SmartScreen est activé par défaut. Pour le désactiver, il suffit de cliquer sur le menu puis de sélectionner **Paramètres** et **Confidentialité, recherche et services**. Désactivez le paramètre **Microsoft Defender SmartScreen**.

3. Navigation InPrivate

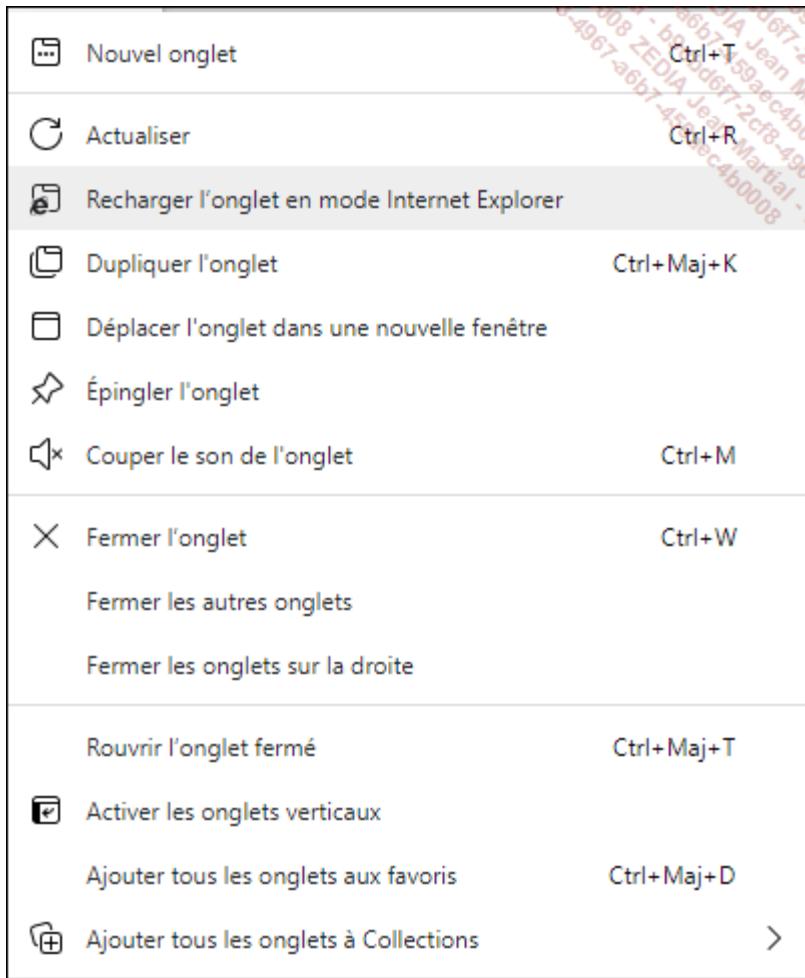
- 296 La Navigation InPrivate répond à un besoin croissant de protection de la vie privée des internautes ; cette fonctionnalité efface les traces laissées sur un poste de travail Windows 11 lorsque des sites internet sont visités.
- 297 Les cookies, les fichiers internet temporaires, l'historique des pages web visitées, les données de formulaires, la saisie semi-automatique pour la recherche, sont supprimés lorsque la fenêtre de Navigation In Private est fermée par l'utilisateur. Ainsi, les traces de l'utilisateur sont effacées sur le système hôte.
- 298 Pour activer la navigation InPrivate :

Depuis le navigateur **Microsoft Edge**, cliquez sur le menu puis sur **Nouvelle fenêtre InPrivate** ou bien pressez les touches [Ctrl] + [Shift] + N.



La navigation InPrivate n'est valable que durant la période où l'onglet est ouvert.

- 299 Enfin, sachez que l'ancien navigateur Microsoft Internet Explorer n'est plus disponible directement mais reste accessible depuis Edge, en cliquant avec le bouton droit sur un onglet lorsqu'une page compatible est visitée.



Cette option doit être activée dans les **Paramètres, Apparence, Personnaliser la barre d'outils**.

Sécurité Windows et antivirus

- Pour aider l'administrateur à protéger Windows 11 contre les logiciels espions et malveillants, Microsoft fournit gratuitement un antivirus. Le logiciel peut vérifier les postes de travail physiques ou virtuels et offre les fonctions communes aux programmes concurrents :
 - Mise à jour automatique des définitions virales via le service Windows Update.
 - Scan rapide, complet, manuel ou planifié : exclusion possible de fichiers, de dossiers, de partitions et de processus.
 - Alertes affichées dans le Centre de notifications lors de l'installation ou l'exécution d'un programme indésirable. Selon son niveau, quatre actions sont proposées : ignorer, mettre en quarantaine, supprimer ou toujours autoriser.
 - Protection en temps réel des composants critiques du système : un agent contrôle les programmes démarrés automatiquement, les paramètres de Windows 11, les composants additionnels et téléchargements de Microsoft Edge, les services et pilotes, l'inscription et l'exécution d'applications.
 - L'antivirus peut maintenant détecter les virus exécutés dans le kernel (noyau) et la mémoire vive, afin de traiter ceux-ci même lorsqu'ils sont de type 0-day : en effet, une vulnérabilité zero-day (en français : jour zéro) ne fait l'objet d'aucun correctif connu le jour de sa découverte.

- De plus, grâce aux données de télémétrie récoltées par Microsoft, un apprentissage des habitudes et comportements des utilisateurs permet de réduire les faux positifs et de mieux détecter les menaces.
- Le logiciel est accessible depuis la barre des tâches en recherchant le mot-clé antivirus, cliquez ensuite sur **Protection contre les virus et menaces**.



- Le logiciel gérant la sécurité adopte désormais une interface épurée. Le menu situé à gauche est composé comme suit :
 - Le bouton **Accueil** affiche l'état de la sécurité du poste de travail.
 - Le bouton **Protection contre les virus et les menaces** symbolisé par un bouclier affiche l'historique des menaces et permet d'obtenir les mises à jour de l'antivirus. De plus, les menaces potentielles nécessitant une action de l'utilisateur sont affichées.
 - Le bouton **Protection du compte** permet de sécuriser les informations de connexion et de configurer le verrouillage dynamique.
 - L'antenne **Pare-feu et protection du réseau** liste les connexions réseau, leur état (connecté/déconnecté), et permet de configurer le pare-feu du système.
 - Le bouton **Contrôle des applications et du navigateur** affiche les paramètres du filtre Windows Defender SmartScreen pour les applications installées ainsi que le navigateur Edge. Il est possible d'installer Microsoft Defender Application Guard, une fonctionnalité qui isole des sites web ou des fichiers Office non fiables dans un conteneur virtuel isolé. C'est également dans cette rubrique que vous pourrez paramétrier **Exploit Protection**, une fonctionnalité à l'origine dans Microsoft EMET (*Enhanced Mitigation Experience Toolkit*) qui empêche le fonctionnement de nombreuses techniques d'attaque.
 - Le bouton **Sécurité des appareils** symbolisé par un ordinateur portable gère la sécurité de la couche virtualisation Hyper-V.
 - Le bouton **Performances et intégrité de l'appareil** (cœur) génère des rapports d'intégrité sur les mises à jour du système, la capacité de stockage, les pilotes de périphériques ainsi que l'autonomie de la batterie.

- Le bouton **Options de contrôle parental** permet d'obtenir une vue synthétique des paramètres liés à la vie en ligne des enfants de la famille.
- Le bouton **Historique de protection** qui regroupe les dernières actions de protection engagées par le système.
- Le bouton **Paramètres** affiche les réglages de sécurité vis-à-vis des notifications créées par une activité malveillante et permet de sélectionner un autre antivirus.
- Microsoft Defender for Endpoint est une option payante de Microsoft Defender Antivirus à destination des entreprises et qui permet, via un capteur comportemental, de consigner les événements de sécurité afin de les analyser dans le cloud de manière centralisée. L'évaluation du service est possible depuis l'adresse : <https://aka.ms/MDEp2OpenTrial>

The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a sidebar with various dashboard options: Dashboards, Incidents, Device inventory, Alerts queue, Automated investigations, Advanced hunting, Reports, Partners & APIs, Threat & Vulnerability Management, Evaluation and tutorials, Service health, Configuration management, and Settings. The main area has a dark theme with a large 'Security operations' section featuring a lock icon. To the right, a prominent message says 'Microsoft Defender for Endpoint is moving'. It explains that starting July 6th, users will be gradually redirected from securitycenter.windows.com to the newly unified Microsoft 365 Defender portal. A blue button labeled 'Take me there' is present. Below this are two cards: 'Active alerts' (30 days) and 'Active automated investigations' (30 days). The 'Active alerts' card shows a count of 0. The 'Active automated investigations' card shows a donut chart with 0 pending action, 0 waiting for device, and 0 running.

- Une fois les conditions du contrat acceptées et les informations concernant l'entreprise demanduse saisies, le parc informatique peut bénéficier de cette technologie.
- Le service sera par la suite disponible depuis le Centre de sécurité Windows accessible depuis le lien : <https://security.microsoft.com/homepage>

Résumé du chapitre

- Windows 11 offre un large éventail d'outils de sécurité, afin de couvrir l'intégralité des besoins de l'utilisateur. Concernant la protection des postes de travail, l'UAC contribue à empêcher les programmes malveillants de s'installer sur le poste de travail en utilisant des priviléges élevés, et le Centre de notifications propose dans une vue centrale les messages récents relatifs à la sécurité.
- EFS, quant à lui, chiffre les fichiers et dossiers choisis de manière transparente sur une partition NTFS. Il n'est pas possible de chiffrer et compresser un fichier ou un dossier en même temps. L'agent de récupération est un compte d'utilisateur pouvant déchiffrer n'importe quel fichier chiffré. Il doit être créé afin d'éviter la perte définitive de données chiffrées.
- BitLocker chiffre l'intégralité des partitions, en mode hors connexion. BitLocker To Go fait de même sur les périphériques amovibles USB.
- Tout comme les versions précédentes des systèmes Microsoft, il est important d'installer les mises à jour de sécurité pour Windows 11, afin que le système reste stable et sécurisé. L'entreprise peut utiliser un serveur WSUS, placé dans le réseau local pour gérer les correctifs de sécurité, et ainsi économiser la bande passante Internet. Grâce à un objet stratégie de groupe, l'administrateur du domaine définira des paramètres standards de gestion des correctifs, et les appliquera à l'intégralité du parc informatique dont il a la responsabilité.
- AppLocker restreint l'exécution et l'installation de logiciels définis, ainsi que des applications Windows 11.
- Le Pare-feu Windows Defender avec fonctions avancées de sécurité procure un filtrage dans les deux sens des flux transitant. Device Guard représente un ensemble de fonctionnalités liées à la sécurité matérielle et logicielle qui, lorsqu'elles sont définies simultanément, obligent l'utilisateur à n'utiliser que des applications préapprouvées par l'administrateur. Credential Guard apporte une couche de sécurité supplémentaire car, couplée avec Device Guard, les utilisateurs d'un domaine Active Directory auront leur mot de passe stocké dans un conteneur virtuel et non dans LSA (*Local Security Authority*).
- Le Gestionnaire d'identification est un coffre-fort électronique dont la principale fonction est le stockage sécurisé des identifiants et mots de passe utilisés régulièrement par un compte utilisateur. Windows 11 se charge ensuite de les saisir automatiquement lors de l'accès à une ressource précise.
- L'audit a été amélioré ; l'accès aux périphériques amovibles est par exemple journalisé.
- Concernant la sécurité liée à la navigation sur internet, Microsoft Edge propose un filtrage des sites de phishing (SmartScreen) et une meilleure prise en compte de la vie privée des internautes (navigation InPrivate).
- Enfin, Microsoft fournit gratuitement Protection contre les virus et les menaces, outil protégeant Windows 11 en temps réel contre les logiciels espions et malveillants. Couplé à Sécurité Windows, l'ensemble de la sécurité du poste de travail Windows 11 est désormais géré dans une seule et même interface.

Connectivité réseau

Protocoles IPv4 et IPv6

Que l'utilisateur soit dans un environnement réseau domestique ou professionnel, la connectivité est une partie essentielle pour assurer la communication. Les ordinateurs communiquent entre eux à l'aide du protocole IP (*Internet Protocol*). Les techniciens de support doivent posséder une bonne compréhension des protocoles IPv4 et IPv6, qui assurent la transmission de l'information, pour résoudre les problèmes réseau.

L'épuisement des adresses IPv4 publiques disponibles a favorisé l'utilisation de techniques de traduction d'adresses (NAT, *Network Address Translation*) ainsi que la propagation du protocole IPv6, successeur d'IPv4.

Tout comme ses prédecesseurs, Windows 11 fournit des fonctionnalités de mise en réseau avancées, que nous allons détailler dans ce chapitre.

1. Adressage IPv4

IPv4 est une version d'Internet Protocol qui forme la base du réseau internet. Elle s'appuie sur un modèle d'adressage pour la transmission des données entre des systèmes d'exploitation identiques ou différents.

L'adresse IPv4 unique d'un ordinateur permet aux autres ordinateurs placés sur le même réseau de communiquer avec lui. Chaque interface d'un hôte IPv4 peut posséder une ou plusieurs adresses IP.

Cette adresse IPv4 codée sur 32 bits est divisée en 4 octets de 8 bits représentés par des nombres décimaux.

Exemple : 172.16.1.2 est une adresse IPv4 dont le masque de sous-réseau est 255.255.0.0.0.

Comme l'adressage IPv4 est défini sur 32 bits, il peut y avoir au maximum 2^{32} adresses, soit 4 294 967 296.

L'adresse est composée de deux parties : l'ID hôte, qui représente l'adresse unique de l'ordinateur, et l'ID réseau, qui indique le sous-réseau d'appartenance de ce même ordinateur.

Le masque de sous-réseau, composé de 4 octets, indique la démarcation entre l'ID hôte et l'ID réseau. Il définit la plage d'adresses IP avec laquelle une carte réseau peut communiquer. Il est ainsi possible de segmenter le trafic en créant des sous-réseaux en fonction d'emplacements physiques. Les routeurs permettent aux réseaux ou sous-réseaux de communiquer entre eux.

Par exemple, les adresses IP de classe A (de 1 à 127) possèdent le masque de sous-réseau par défaut 255.0.0.0, et permettent d'utiliser 126 réseaux pour gérer 16 777 214 hôtes par réseau.

Deux grands types d'adresses IP sont utilisées quotidiennement par les particuliers et entreprises :

- Adresse publique : reçue du fournisseur d'accès à Internet pour les systèmes qui se connectent directement à Internet, l'IP publique est unique, routable et attribuée par l'ICANN (*Internet Corporation for Assigned Names and Numbers*), dont le site internet est accessible à l'adresse <http://www.icann.org/>.
- Adresse privée : non routable sur Internet, cette adresse IP est attribuée localement par l'organisation, généralement à l'aide d'un serveur DHCP. Elle doit être convertie pour communiquer avec des adresses IP publiques internet, à l'aide de mécanismes de translation d'adresses (NAT). Quatre plages d'adresses IP sont non routables, donc non accessibles directement depuis Internet :
 - Adresses IP de classe A : 10.0.0.1 à 10.255.255.254 pour les réseaux conséquents supportant un grand nombre d'hôtes.
 - Adresses IP de classe B : 172.16.0.1 à 172.31.255.254 permettant de créer des réseaux privés de taille moyenne.
 - Adresses IP de classe C : 192.168.0.1 à 192.168.255.254 pour les réseaux privés de petite taille.

- APIPA (*Automatic Private Internet Protocol Addressing*) : 169.254.0.0 à 169.254.255.255, adresse que le client Windows 11 s'attribuera automatiquement en cas d'absence du serveur DHCP.

Pour découvrir l'adresse IP utilisée par un adaptateur réseau :

Ouvrez les **Paramètres, Réseau et Internet**.

Cliquez sur la carte réseau dont vous voulez connaître la configuration, puis sur **Propriétés matériel**.



Vous pouvez voir ses adresses IPv4 et IPv6, ses serveurs DNS... Pour une carte Wi-Fi, le SSID, le protocole et d'autres informations sont également affichées. Les mêmes informations peuvent se retrouver dans **Paramètres réseau avancés**.

La commande ipconfig /all permet d'afficher la configuration IP d'un poste Windows 11.

Grâce à PowerShell, de nombreuses informations sur la configuration réseau peuvent être visualisées :

- Pour afficher les interfaces réseau ainsi que des informations sur le statut, la vitesse du lien et le VLAN associé, tapez : get-netadapter | ft Name, Status, LinkSpeed, VlanID

Pour des informations plus précises, saisissez : get-netadapter | format-list -property *

- Pour visualiser des informations détaillées sur la configuration IP du poste Windows 11, essayez : get-netadapter | Get-NetIpAddress
- L'adresse du serveur DNS n'est pas affichée. Utilisez la commande : Get-DnsClientServerAddress

```

Administrator : 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:\Users\ybard> Get-NetAdapter

Name      InterfaceDescription      ifIndex Status      MacAddress      LinkLayer
----      ----
kspeed
-----
Cellular 13      Ericsson H5321 gw      35 Not Present
0 bps
Cellular 15      Ericsson H5321 gw      34 Not Present
0 bps
Cellular 7       Ericsson H5321 gw      30 Not Present
0 bps
Cellular 18      Ericsson H5321 gw      29 Not Present
0 bps
Cellular 17      Ericsson H5321 gw      28 Not Present
0 bps
Cellular        Ericsson H5321 gw      27 Disconnected 84-89-9F-5C-58-5D
0 bps

```

- Pour définir une adresse IP sur un ensemble de postes, utilisez la commande PowerShell : New-NetIPAddress
- Pour modifier l'adresse IP existante d'une interface Wi-Fi, saisissez la commande : Set-NetIPAddress -InterfaceAlias "Wi-Fi" -IPv4Address 192.168.10.5 -PrefixLength "24"

La liste des commandes PowerShell liées au protocole TCP/IP est disponible à l'adresse ci-dessous : <https://docs.microsoft.com/en-us/powershell/module/nettcip/?view=win11-ps>

Passerelle

Une passerelle, généralement un routeur, assure le routage des paquets dans le cas où les ordinateurs communiquent depuis des réseaux différents (intranet/extranet).

Elle sert souvent de relais pour former un intranet. La passerelle fait transiter les paquets d'une interface réseau vers une autre à l'aide d'un ensemble de règles. Lorsqu'un client Windows 11 souhaite communiquer avec un autre ordinateur, il utilise un processus simple pour la transmission des données :

1. Le poste expéditeur utilise son masque de sous-réseau pour calculer son adresse de réseau logique. Il va ensuite appliquer son masque de sous-réseau sur l'adresse du poste de destination afin de calculer l'adresse du réseau logique de celui-ci. Si les adresses de réseau logique des deux postes sont identiques, il lui remet le paquet. Sinon, il passe à l'étape 2.
2. Le poste va vérifier qu'il possède une passerelle par défaut, un routeur par exemple, et va effectuer la même procédure qu'à l'étape 1 pour contrôler si la passerelle par défaut et lui-même sont sur le même réseau. Si c'est le cas, le paquet est envoyé à la passerelle par défaut ; sinon, il est abandonné.
3. La passerelle par défaut reçoit le paquet et l'analyse. Celle-ci consulte alors sa table de routage à la recherche d'informations permettant de connaître où est situé le réseau de l'hôte de destination. S'il y a une correspondance, le paquet va transiter jusqu'à l'hôte en passant par un ou plusieurs autres routeurs. Le paquet peut être abandonné par n'importe quel routeur si aucune route concordante n'est trouvée.

Pour connaître l'adresse IP de la passerelle par défaut du client Windows 11, exécutez la commande :

netsh interface ipv4 show address

ou :

ipconfig/all

et visualisez l'adresse IP correspondante à la ligne Passerelle par défaut.

2. Adressage IPv6

La version 6 du protocole IP est la conclusion de travaux dirigés par l'IETF (*Internet Engineering Task Force*) pour pallier l'épuisement inévitable des adresses publiques IPv4. Les adresses ne sont plus définies sur 32 bits, mais sur 128 bits (par blocs de 16 bits, séparés par :) exprimés en notation hexadécimale. La taille du sous-réseau est désormais fixée à 64 bits et utilise un préfixe (barre oblique /) pour définir l'ID réseau.

Le protocole IPv6 permet d'utiliser 3.4×10^{38} adresses pour définir des hôtes.

Les 64 derniers bits d'une adresse IPv6 sont l'identificateur de l'interface, qui est l'équivalent de l'ID hôte dans une adresse IPv4. Chaque interface d'un réseau IPv6 doit posséder un identificateur d'interface unique, ce qui permet de s'affranchir de l'adresse MAC (*Media Access Control*) de la carte réseau.

Le gain d'espace d'adressage est donc conséquent.

Une adresse IPv6 serait par exemple : fe80:0053:0000:0000:4804:0db0:479d:f61e/64

Pour simplifier sa lecture, il est possible de remplacer "0000" par "0" : fe80:0053:0:0:4804:0db0:479d:f61e/64

Puis, de supprimer les premiers "0" de chaque bloc : fe80:53:0:0:4804:db0:479d:f61e/64

Et enfin, nous remplaçons les blocs consécutifs de "0" par "::" : fe80::4804:db0:479d:f61e/64

Trois types d'adresses IPv6 sont proposés :

- Monodiffusion : utilisée pour la communication directe entre hôtes, l'adresse de monodiffusion identifie une interface unique. C'est la plus usitée. Quatre adresses similaires à l'adressage IPv4 sont disponibles :
- Adresse globale : équivalente à une adresse publique IPv4, cette adresse est accessible depuis Internet IPv6 et commence toujours par "001".
- Adresse locale de liaison : similaire à l'adressage privé automatique (APIPA), cette adresse commence toujours par "fe80".
- Adresse locale de site : adresse commençant par "fec0", elle correspond à l'adressage privé IPv4 et nécessite un serveur DHCPv6. Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 et Windows Server 2012 R2 offrent ce rôle.
- Adresses spéciales : ces adresses sont équivalentes à l'adresse indéfinie ("::" ou 0:0:0:0:0:0:0) et à l'adresse de bouclage ("::1" ou 0:0:0:0:0:0:1).
- Multidiffusion : identifie plusieurs interfaces. Ce type d'adresse est utilisé pour la communication un-à-plusieurs entre des hôtes définis comme utilisant la même adresse. Les paquets IPv6 sont livrés sur toutes les interfaces qui sont définies par cette adresse.
- Anycast : plusieurs interfaces sont utilisées mais les paquets sont livrés sur la plus proche en matière de distance de routage (nombre de sauts). Ce type d'adresse sert principalement à localiser des services ou des routeurs.

Un client Windows 11 peut obtenir une adresse IP d'un serveur DHCPv6 (configuration avec état), ou s'en attribuer une de lui-même automatiquement (configuration sans état) en l'absence de ce dernier. La configuration manuelle reste toujours d'actualité, grâce à l'écran de configuration **Réseau et Internet** de la fenêtre des **Paramètres** ou bien avec la commande netsh.

Le langage PowerShell contient également un lot de commandes permettant d'effectuer les opérations courantes :

- Set-NetIPv6Protocol pour modifier la configuration du protocole IPv6.
- Get-NetIPv6Protocol pour obtenir des informations sur celui-ci.

L'enregistrement DNS d'un hôte IPv6 est de la forme "AAAA" : permet d'établir la correspondance entre le nom d'hôte pleinement qualifié d'une machine et son adresse IPv6.

Le protocole est utilisé par différentes fonctionnalités, telles que DirectAccess, la reconnexion VPN ou le partage de fichiers sécurisé...

Côté sécurité, IPv6 prend nativement en charge le protocole IPsec, garantissant ainsi le chiffrement des données qui transitent entre les hôtes.

IPv6 implémente la livraison par ordre de priorité : l'en-tête du paquet contient un champ définissant le temps de traitement de l'information. Cette amélioration est particulièrement utile lorsque l'utilisateur se connecte à une vidéo diffusée en streaming, les données devant lui parvenir rapidement.

Le principal point négatif de ce protocole est l'incompatibilité entre les adresses IPv4 et IPv6, du fait d'une conception différente des en-têtes.

Il est dans ce cas nécessaire d'utiliser un protocole de tunnelisation comme 6to4, ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) ou Teredo, qui encapsulent les paquets IPv6 dans des paquets IPv4, ou vice versa, pour traverser des routeurs IPv4.

Pour pallier le problème de communication entre un client IPv4 et un client IPv6, Windows 11 implémente par défaut une configuration à double pile, qui consiste à attribuer à l'ordinateur deux adresses IP, une IPv4, l'autre IPv6 et qui fournit une couche transport et une trame partagée pour ces deux protocoles.

En outre, Windows 11 propose d'établir des connexions Bureau à distance (cf. chapitre Gestion des clients Windows, section Accès à distance) sur des hôtes possédant des adresses IPv6.

Windows 11 supporte les nouvelles fonctionnalités introduites par Windows 10 lors de l'utilisation du protocole IPv6 :

- Meilleure gestion de la connectivité internet : dans les anciennes versions du système d'exploitation Windows, lorsqu'un hôte distant IPv6 était inaccessible en raison d'un chemin de routage défaillant, la connexion s'effectuait avec le protocole IPv4, ralentissant l'accès à la ressource. Windows 11 s'assure désormais de la connectivité d'une adresse IPv6 connue pour être disponible. Si elle ne l'est pas, le système désactive l'utilisation du protocole IPv6 pour l'hôte recherché et se connecte directement avec le protocole IPv4.
- NAT64/DNS64 : lorsqu'un trafic entrant IPv6 à destination d'un hôte IPv4 survient, NAT64 assure la translation d'adresse. DNS64 résout le nom d'un ordinateur IPv4 vers une adresse IPv6 translatée. NAT64/DNS64 est utilisé par la fonctionnalité DirectAccess fournie avec Windows Server 2012 (ou supérieur).
- Support de PowerShell : dans les précédentes versions de Windows, la commande Netsh était utilisée pour effectuer des actions sur le protocole IPv6. Désormais, PowerShell offre de nouvelles possibilités, comme la gestion de l'adressage IPv6.

Visualiser la configuration IPv6 d'un client Windows 11 est simple grâce à la commande ipconfig /all.

Il est aussi possible d'utiliser la commande :

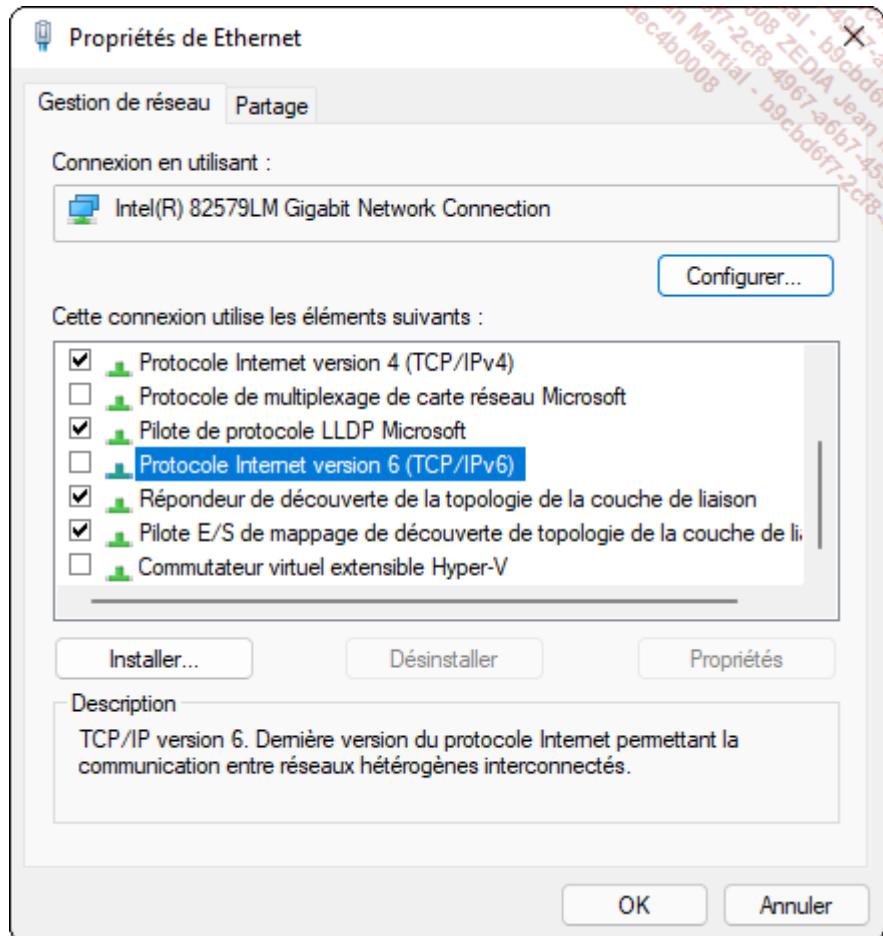
```
netsh interface ipv6 show address
```

Pour désactiver IPv6, il suffit d'utiliser le **Centre Réseau et partage** et de désactiver le protocole dans les propriétés de la carte réseau :

Cliquez sur le menu **Démarrer** puis saisissez ncpa.cpl et validez par la touche [Entrée].

Dans la fenêtre **Connexions réseau**, sélectionnez la carte réseau sur laquelle vous souhaitez désactiver le protocole IPv6, effectuez un clic avec le bouton droit puis choisissez **Propriétés**.

Dans la fenêtre **Propriétés de Ethernet**, décochez la case **Protocole Internet version 6 (TCP/IPv6)**.



Validez en cliquant sur le bouton **OK**.

Dans la fenêtre vue précédemment, il est possible de définir manuellement une adresse IPv6, ainsi que la longueur du préfixe de sous-réseau, la passerelle par défaut et les serveurs DNS. Sélectionnez **Protocole Internet version 6 (TCP/IPv6)** et cliquez sur le bouton **Propriétés**.

La commande netsh peut aussi être utilisée.

3. Dépannage IP

La résolution des problèmes liés à la connectivité réseau peut s'effectuer de plusieurs façons avec Windows 11, avec le panneau **Paramètres, Réseau et Internet**, au travers du Centre Réseau et partage ou bien à l'aide de commandes telles qu'ipconfig ou netsh.

Des outils de résolution des problèmes réseau sont intégrés à Windows 11 :

- Le journal **Système**, accessible depuis l'**Observateur d'événements**, répertorie les erreurs ou les avertissements associés aux services réseau.
- **IPconfig** affiche la configuration réseau TCP/IP, mais permet aussi de renouveler un bail DHCP (commandes ipconfig /release, ipconfig /renew) ou de vider le cache de résolution DNS (ipconfig /flushdns).
- **Ping** vérifie la connexion à un ordinateur distant grâce au protocole ICMP (*Internet Control Message Protocol*).
- **Nslookup** interroge les DNS référencés et l'existence des enregistrements recherchés.
- **Tracert** affiche les chemins empruntés par un paquet de données IP transmis d'une machine Windows 11 vers une autre machine connectée au réseau IP.

- **Résoudre les problèmes** : Windows 11 exécute un ensemble de commandes réseau de diagnostics et vous propose un rapport de résolution (cf. Diagnostics réseau de Windows, plus bas dans ce chapitre).

Pour tester la connectivité d'un client Windows 11 dans un réseau d'entreprise, il suffit de respecter la procédure suivante dans un Terminal Windows :

1. Visualiser la configuration IP : ipconfig /all ou pour les informations concernant IPv6 : netsh interface ipv6 show address
2. ping 127.0.0.1 ou ping ::1 (test de l'adresse de bouclage).
3. Vérifier la présence d'adresse APIPA commençant par 169.254 (IPv4) ou fe80 ou fec0 (IPv6) et tester l'adresse privée du client avec un ping vers cette adresse.
4. Facultatif : ping 0.0.0.1 (adresse publique internet du système Windows 11 local).
5. ping de l'adresse IP de la passerelle par défaut.
6. ping de la machine distante connectée à Internet.

a. Netsh

La commande ipconfig, bien connue des administrateurs, reste toujours implémentée avec Windows 11. Elle affiche la configuration IPv4 ou IPv6 par interface physique ou virtuelle. Toutefois, elle n'est exécutable que localement. Microsoft propose l'utilitaire de script de ligne de commande netsh, qui permet d'afficher ou modifier la configuration réseau d'un ordinateur Windows 11, localement et à distance.

La configuration du DHCP, des interfaces IPv4, IPv6, d'IPsec, du routage, du service RPC (*Remote Procedure Call*) ou WINS est ainsi grandement facilitée.

Pour exécuter netsh, il suffit d'ouvrir un Terminal, de saisir netsh puis de valider par la touche [Entrée].

Par exemple, pour visualiser la configuration IPv6 du client Windows 11 :

Depuis un **Terminal Windows**, saisissez : netsh interface ipv6 show address

```

Réponse de ::1 : temps<1ms
PS C:\Users\ybard> netsh interface ipv6 show address

Interface 1 : Loopback Pseudo-Interface 1

Addr Type  État DAD    Vie valide Pers. Fav. Adresse
----- -----
Autre      Préféré     infinite   infinite ::1

Interface 22 : Teredo Tunneling Pseudo-Interface

Addr Type  État DAD    Vie valide Pers. Fav. Adresse
----- -----
Public    Préféré     infinite   infinite 2001:0:1428:8f18:873:332e:a907:dd82
Autre      Préféré     infinite   infinite fe80::873:332e:a907:dd82%22

Interface 5 : Wi-Fi

Addr Type  État DAD    Vie valide Pers. Fav. Adresse
----- -----
Public    Préféré     29m44s    9m44s  2a01:cb14:137:6800:316b:5dc8:4ace:16e7
Temporaire Préféré     29m44s    9m44s  2a01:cb14:137:6800:cd6a:29da:c846:90fb
Autre      Préféré     infinite   infinite fe80::316b:5dc8:4ace:16e7%5

```

La commande suivante définira l'interface nommée "Privee" avec une adresse IPv6 fixe anycast : netsh interface ipv6 set address "Privée" FE80::5 anycast

La commande netsh permet aussi de configurer des règles de pare-feu ou encore BranchCache. Consultez l'aide pour connaître les commandes disponibles : netsh /?.

Pour vider le cache du client Windows 11, saisissez la commande netsh interface ipv6 delete neighbors en tant qu'administrateur local.

b. Résolution des problèmes de Windows

Windows 11 propose une série d'utilitaires permettant de résoudre certains problèmes, dont ceux liés au réseau. Ces outils peuvent corriger par exemple un accès infructueux à un site web, l'impossibilité d'utiliser DirectAccess, ou encore la connexion défaillante à un réseau (filaire, sans fil...). Après avoir entrepris les actions correctives, un rapport de résolution des problèmes est généré à l'intention de l'administrateur, contenant dans des fichiers au format texte les opérations effectuées (exemple : ipconfig ou tracert).

L'utilisateur peut retrouver ces outils de la manière suivante :

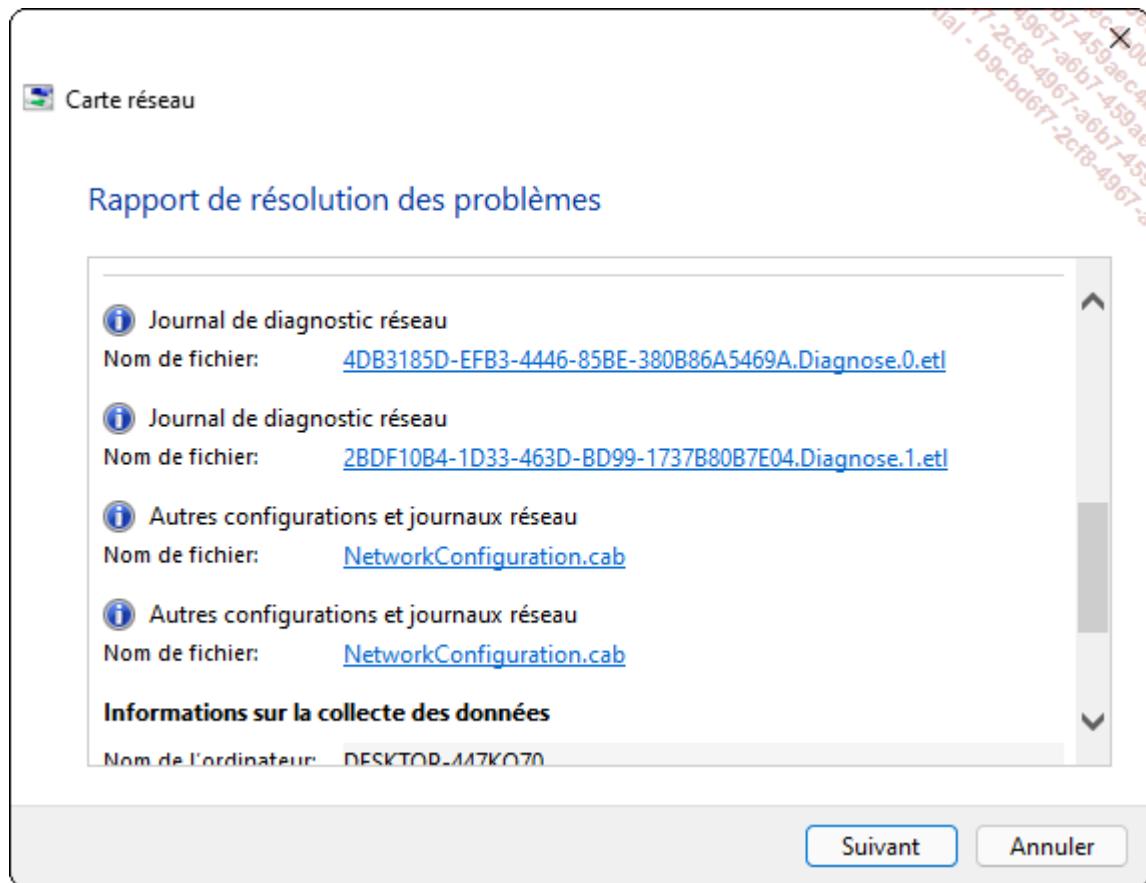
Cliquez sur **Démarrer, Paramètres, Système et Résolution des problèmes**.

Cliquez sur **Autres utilitaires de résolution des problèmes**.



Cherchez les lignes **Connexion Internet** ou **Carte réseau** et cliquez sur le bouton **Exécuter**.

Un assistant guide l'utilisateur en lui posant des questions sur la nature des problèmes puis tente de le corriger automatiquement.



Réseau et Internet

Windows 11, comme son prédecesseur, centralise la majorité des fonctionnalités réseau dans le panneau des **Paramètres**, dans la rubrique **Réseau et Internet**.



L'utilisateur peut y trouver les éléments suivants :

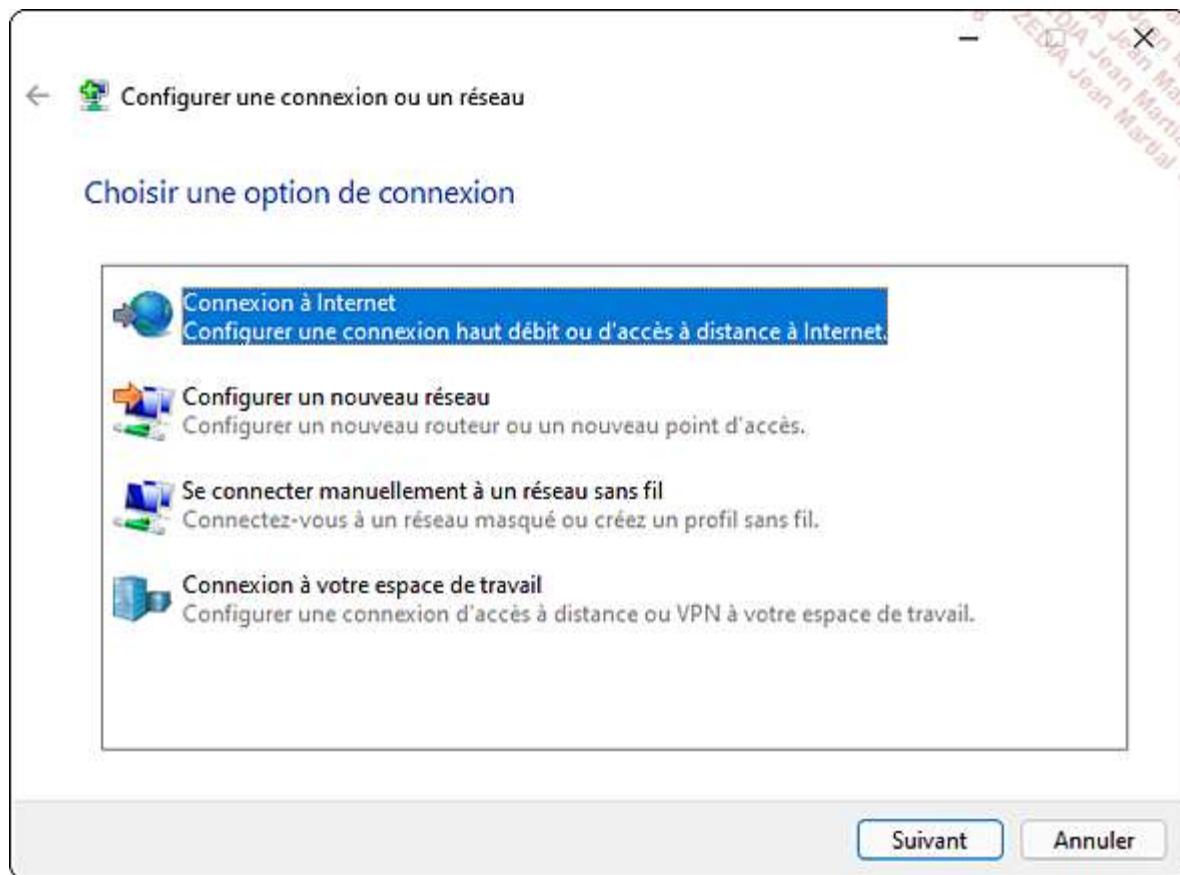
- L'état de ses différentes connexions réseau, que ce soit filaire, Wi-Fi ou cellulaire, la consommation de données...
- Le paramétrage de connexions spécifiques comme un VPN, un proxy, un accès distant...
- Des paramètres réseau supplémentaires.

Ce panneau de commande remplace le **Centre Réseau et partage**, toujours accessible depuis **Accès à distance**, par l'intermédiaire du **Panneau de configuration** ou à l'aide de la commande :

control.exe /name Microsoft.NetworkAndSharingCenter

Pour configurer une nouvelle connexion réseau grâce à un assistant :

Cliquez sur le lien **Configurer une nouvelle connexion** de la section **Accès à distance** :



Choisissez le type de connexion à créer parmi les quatre choix suivants :

- **Connexion à Internet** : configure une connexion haut débit PPoE (*Point-to-Point Protocol over Ethernet*), ADSL ou câble. Une connexion bas débit peut être définie en présence d'un modem RTC (réseau téléphonique commuté) ou RNIS (réseau numérique à intégration de services) dans l'ordinateur.
- **Configurer un nouveau réseau** : affiche la liste des points d'accès ou routeurs qui peuvent être paramétrés par l'intermédiaire de Windows 11.
- **Se connecter manuellement à un réseau sans fil** (cf. section Gestion des réseaux sans fil).
- **Connexion à votre espace de travail** : crée une nouvelle connexion VPN (SSTP, PPTP...) ou bas débit par l'intermédiaire d'un modem RTC.

Les paramètres de profil sont affichés et définissables pour chaque périphérique.

Dans **Réseau et Internet**, cliquez sur la mention **Propriétés** d'une carte réseau.

Réseau et Internet



The screenshot shows the Windows Control Panel under 'Réseau et Internet'. It displays a summary of network connections:

- Wi-Fi (Livebox-D5D6)**: Status is "Connecté, sécurisé".
- Propriétés**: Type is "Réseau privé" at "5 GHz".

Below this, there are two links:

- Wi-Fi**: Connecter, gérer des réseaux connus, connexion réseau limitée.
- Réseau cellulaire**: Données cellulaires, options d'itinérance, paramètres de l'opérateur mobile.

Vous pouvez ensuite sélectionner le type de profil réseau parmi :

- **Public** : cette option assure une certaine protection en empêchant votre machine d'être détectable.
- **Privé** : votre appareil est détectable sur le réseau et vous pouvez partager des fichiers.
- **Domaine** : votre machine est intégrée à un domaine... Ce type de profil n'est affiché que si un domaine a été détecté.

Il est possible d'obtenir le profil actuel avec la commande PowerShell Get-NetConnectionProfile

Pour modifier le profil en public (Public) :

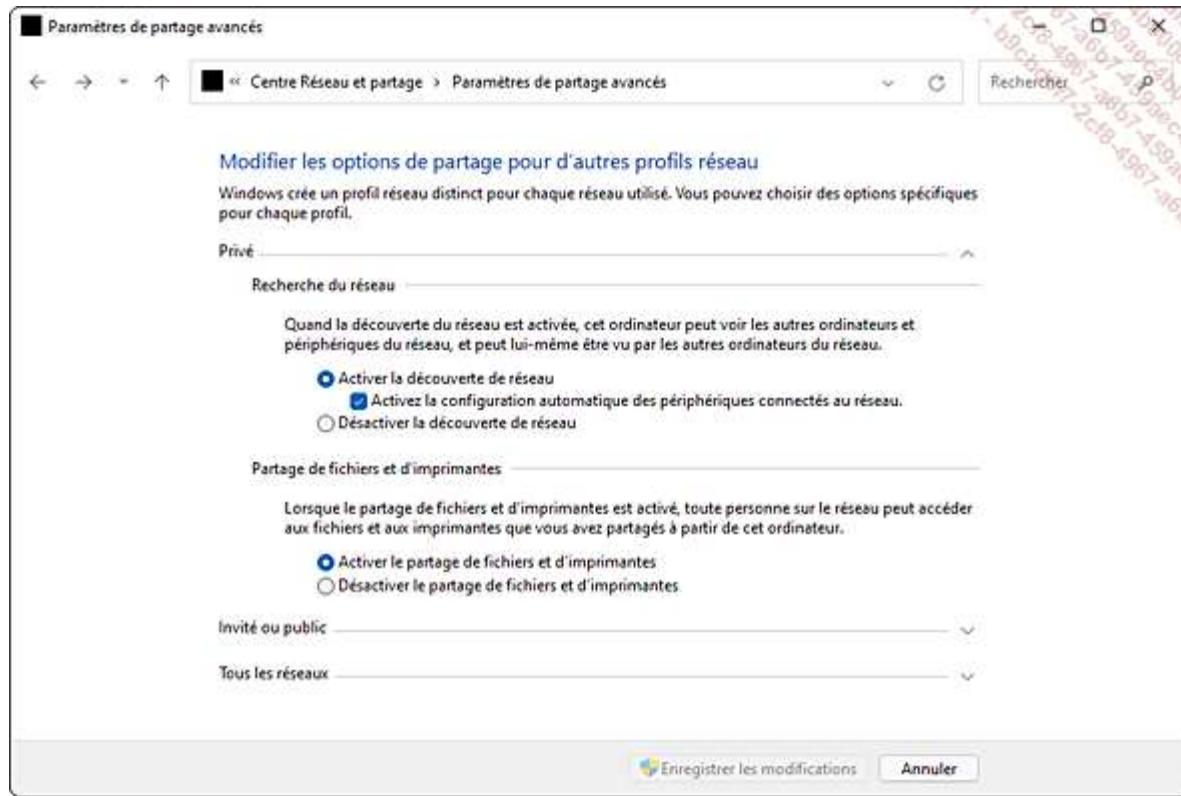
```
Set-NetConnectionProfile -Name "NOM CONNEXION"
```

```
-NetworkCategory Public
```

Le comportement des partages réseau peut être configuré par type de profil réseau. Il est ainsi possible :

- d'activer ou non la découverte du réseau ;
- d'activer ou non le partage ;
- de protéger les partages réseaux.

Ces options sont configurables dans **Modifier les paramètres de partage avancés** de la page principale du **Centre Réseau et partage**.



300 Les partages sont ensuite initiés depuis l'Explorateur de fichiers (cf. chapitre Gestion des disques et des pilotes) ou les paramètres des imprimantes (cf. chapitre Gestion des clients Windows).

301 Notez que les groupes résidentiels ont été supprimés depuis Windows 10 version 1803.

1. Création d'un serveur VPN

302 Tout comme les anciennes versions clientes de Microsoft, Windows 11 peut remplir les fonctions basiques d'un serveur VPN : chiffrement des communications et création d'un tunnel sécurisé. Le service Routage et accès distant, quant à lui, permet de recevoir les connexions entrantes. L'utilisateur distant voulant se connecter sur un poste de travail Windows 11 doit posséder un compte local sur celui-ci et être explicitement autorisé.

303 Pour créer un serveur VPN, ouvrez une session en tant qu'administrateur sur un ordinateur équipé de Windows 11 et suivez la procédure ci-dessous :

Cliquez sur le menu **Démarrer** puis saisissez services.msc. Cliquez sur **Services**.

Dans la fenêtre **Services**, cliquez avec le bouton droit sur **Routage et accès distant**, puis cliquez sur **Propriétés**.

Dans le champ **Type de démarrage**, choisissez **Automatique** et validez en cliquant sur le bouton **Appliquer**.

Cliquez ensuite sur les boutons **Démarrer** et **OK**. Fermez la fenêtre **Services**.

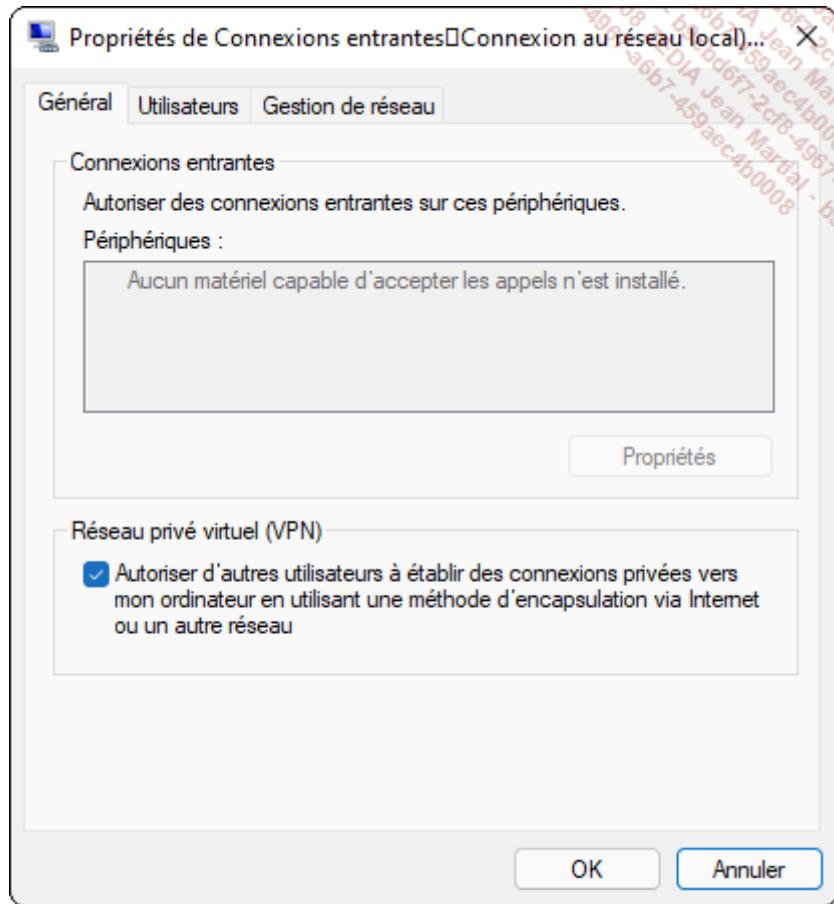
Le service de routage et accès distant est en service et se lancera automatiquement au prochain démarrage de la machine.

304 Dans le Centre Réseau et partage, nous allons maintenant configurer le serveur VPN :

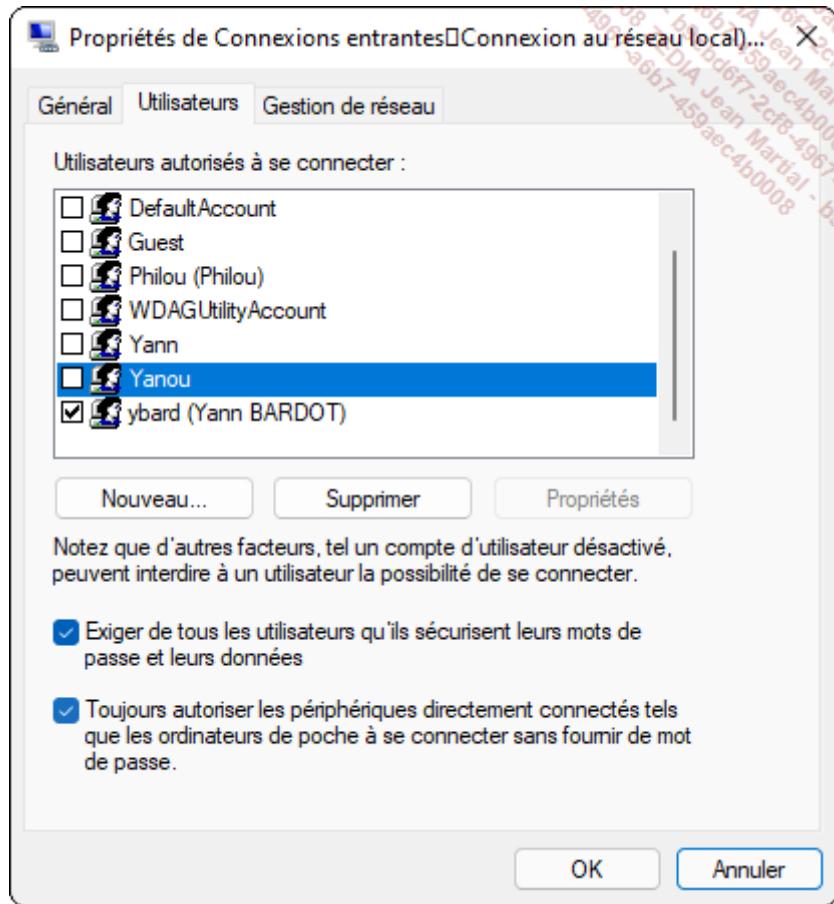
Cliquez sur le menu **Démarrer** puis saisissez ncpa.cpl. Cliquez sur **ncpa.cpl** (**Elément du Panneau de configuration**).

Dans la fenêtre **Connexions réseau**, l'icône **Connexions entrantes** est désormais visible. Cliquez avec le bouton droit dessus, puis choisissez **Propriétés**.

Cochez la case **Autoriser d'autres utilisateurs à établir des connexions privées vers mon ordinateur en utilisant une méthode d'encapsulation via Internet ou un autre réseau**.

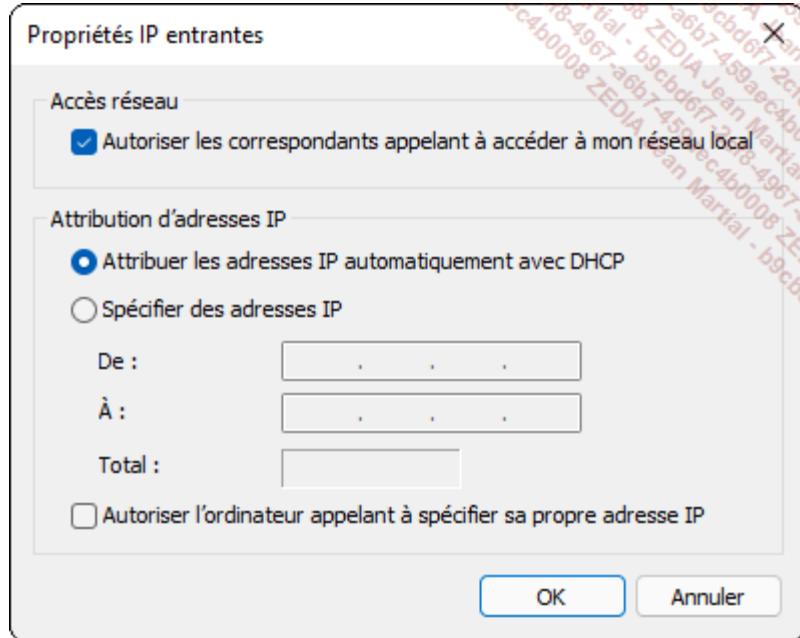


Sélectionnez ensuite l'onglet **Utilisateurs** puis cochez les utilisateurs locaux autorisés à se connecter à votre poste de travail Windows 11. Assurez-vous qu'un mot de passe est défini pour ces comptes, sinon un message d'erreur apparaîtra lors de la tentative d'initialisation du tunnel VPN. Vous pouvez **Exiger des utilisateurs** qu'ils sécurisent leurs mots de passe et leurs données pour pouvoir se connecter, ou bien **Toujours autoriser les périphériques directement connectés tels que les ordinateurs de poche à se connecter sans fournir de mot de passe**.



Cliquez sur l'onglet **Gestion de réseau**, sélectionnez **Protocole Internet version 4 (TCP/IPv4)** et cliquez sur le bouton **Propriétés**.

Dans le champ **Accès réseau**, assurez-vous que la case **Autoriser les correspondants appelant à accéder à mon réseau local** soit cochée. Cliquez sur **Spécifier des adresses IP** et définissez la plage d'adresses IP conforme à votre réseau qui sera allouée aux connexions VPN distantes.



Validez en cliquant sur le bouton **OK**.

La configuration du serveur VPN Windows 11 est maintenant terminée.

Notez qu'il est tout à fait possible d'établir une connexion VPN depuis un poste en Windows 10 ou 11, en reprenant la procédure de création d'un VPN abordée dans le chapitre Gestion des clients Windows.

Gestion des réseaux sans fil

Souvent utilisé pour fournir un accès à Internet dans des lieux publics, un réseau sans fil est un ensemble d'ordinateurs interconnectés par signaux radio, à la différence d'un réseau filaire qui utilise des connecteurs RJ45. La norme IEEE (*Institute of Electrical and Electronics Engineers*) 802.11 décrit les spécifications pour implémenter des réseaux locaux à liaison sans fil.

La gestion des réseaux sans fil est une tâche importante pour un administrateur, car cela engendre des problèmes de sécurité, du fait de la disparition du périmètre réseau, et est sujet aux interférences. Néanmoins, les réseaux sans fil facilitent la mobilité et la flexibilité des utilisateurs itinérants.

Il existe deux modes de connexion à un réseau sans fil : le mode ad hoc et le mode infrastructure. Avec le premier, la connexion d'un ordinateur Windows 11 s'effectue de sa carte réseau sans fil à celle de l'autre ordinateur, à l'aide d'un mot de passe partagé : c'est l'équivalent du concept de groupe de travail.

Dans le mode infrastructure, le client Windows 11 se connecte directement à un point d'accès sans fil, qui se charge du transfert et de la sécurisation des données échangées ; l'architecture est similaire à un domaine Microsoft. Un réseau sans fil, en mode ad hoc ou infrastructure, porte toujours un nom, visible ou caché, le SSID (*Service Set Identifier*).

Windows 11 fournit une prise en charge complète de toutes les normes du marché :

- Wi-Fi 1 appelée également 802.11b (débit maximal théorique de 11 Mbits/s)
- Wi-Fi 2 ou 802.11a (54 Mbits/s)
- Wi-Fi 3 ou 802.11g (54 Mbits/s)
- Wi-Fi 4 ou 802.11n (600 Mbits/s)
- Wi-Fi 5 ou 802.11ac (5,3 Gbits/s)
- Wi-Fi 6 ou 802.11ax (10,5 Gbits/s)
- Wi-Fi 6E (E pour *Extended*) la dernière norme validée, avec pour particularité et nouveauté la possibilité d'utiliser la bande des 6 GHz en plus des bandes 2,4 GHz et 5 GHz.

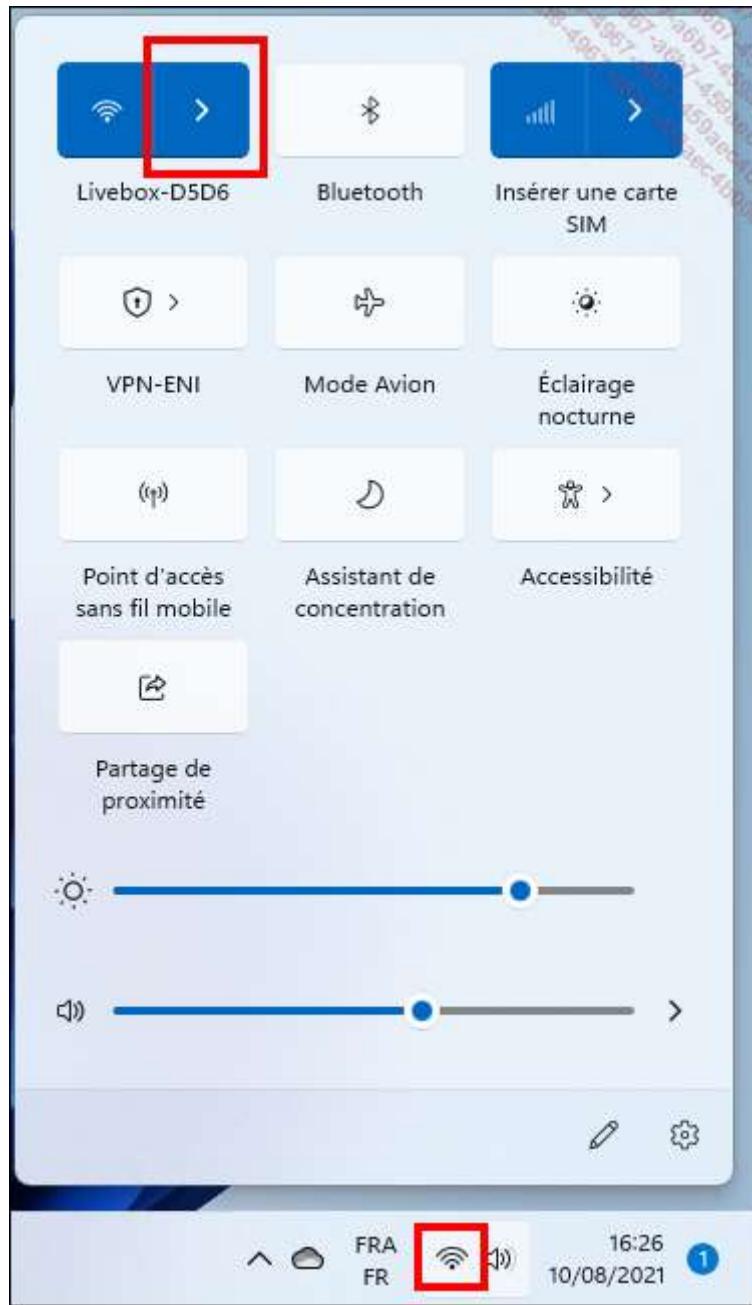
Bien entendu, la qualité d'utilisation d'un réseau sans fil dépend de la carte réseau disponible sur la machine et du pilote associé.

La sécurité du réseau sans fil combine des méthodes d'authentification et de chiffrement. Windows 11 peut se connecter au point d'accès sans fil à l'aide d'une authentification par système ouvert, clé partagée (WEP), 802.1 X ou PSK. Côté chiffrement, les clés WEP (*Wired Equivalent Privacy*), WPA et WPA2 (*Wi-Fi Protected Access*) Entreprise (TKIP, AES) sont disponibles.

Même si la sécurité du client est essentielle, celle du point d'accès est primordiale : pensez à désactiver la publication du SSID, à activer le filtrage d'adresses MAC ou encore à utiliser des logiciels qui diffusent de faux SSID. Ces actions s'effectuent depuis les paramètres avancés de votre modem ADSL (Freebox, Livebox...).

La connexion à un réseau sans fil, délicate pour un néophyte, est désormais simplifiée avec Windows 11 : une seule vue permet de gérer les connexions, distantes (VPN, RTC...), sans fil ou filaire.

Cliquez simplement sur l'icône de réseau située dans la barre des tâches, puis sur la flèche à droite de l'icône **Wi-Fi**, pour afficher tous les réseaux sans fil.



Cliquez sur le réseau choisi, entrez la clé de sécurité, cochez **Se connecter automatiquement** et cliquez sur le bouton **Se connecter**.



La connexion d'un client à un point d'accès sans fil nécessite de connaître le nom du réseau (SSID) et d'entrer une clé (WEP, WPA...) pour s'authentifier.

Lorsque le réseau ne nécessite pas de clé pour se connecter (réseau ouvert) mais impose à l'utilisateur de saisir un nom d'utilisateur et un mot de passe sur une page internet, Windows 11 détecte cette méthode d'identification et peut entrer les identifiants automatiquement.

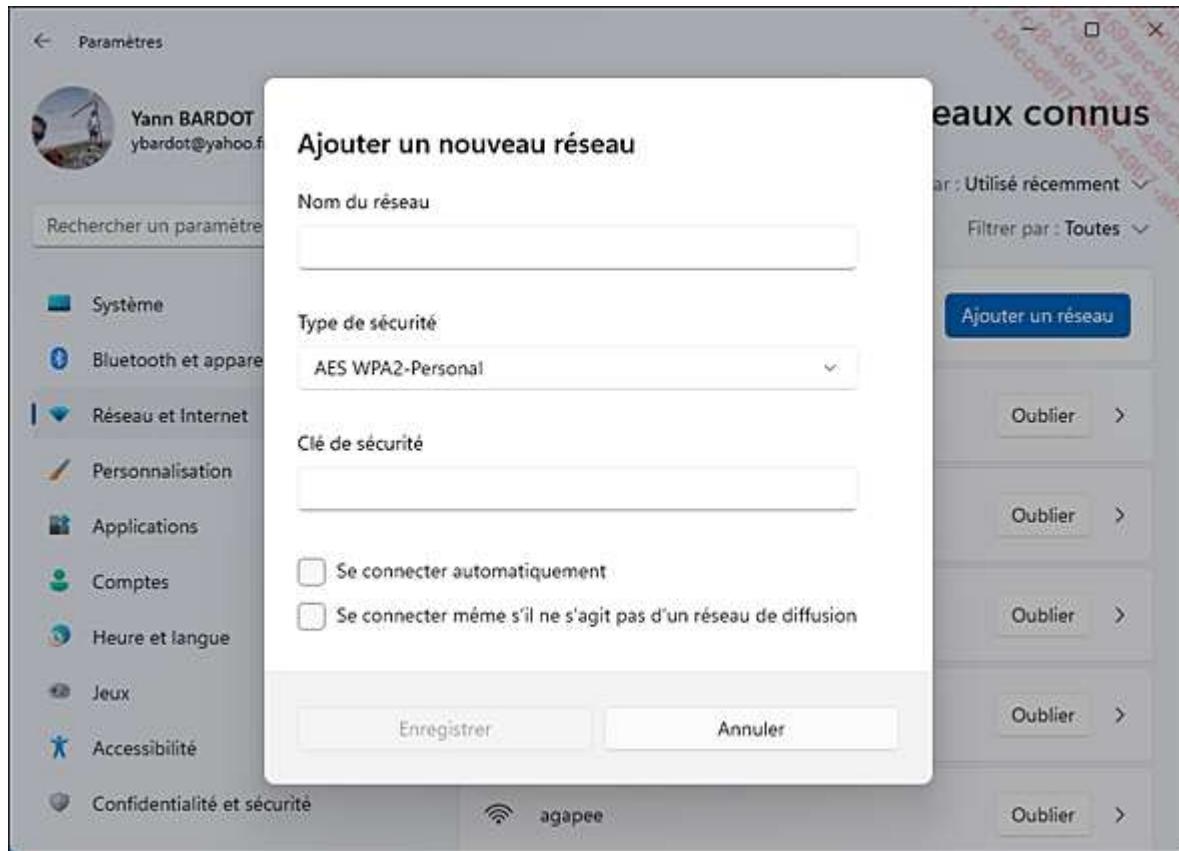
La configuration d'un réseau sans fil peut s'effectuer de trois manières différentes :

- Depuis les **Paramètres, Réseau et Internet, Wi-Fi**, en cliquant sur **Afficher les réseaux disponibles**.

The screenshot shows the Windows Settings interface under 'Réseau et Internet > Wi-Fi'. The left sidebar has 'Réseau et Internet' selected. The main area shows the 'Wi-Fi' tab is active, indicated by a blue toggle switch. A list of available networks is shown: 'Livebox-D5D6 propriétés' (Connected, secured), 'Livebox-D5D6' (Connected), 'Bbox-849FC5B6' (Secured, checked for automatic connection), and 'Livebox-893a'. A 'Connecter' button is visible next to the Bbox network. At the bottom, there's a link to 'Gérer les réseaux connus'.

- Sélectionnez le réseau Wi-Fi et cliquez sur le bouton **Conneter**. Lorsque cela vous est demandé, saisissez la clé de sécurité et cliquez sur le bouton **Suivant**.

Si vous souhaitez ajouter un réseau manuellement, cliquez sur **Gérer les réseaux connus**, puis sur le bouton **Ajouter un réseau**.

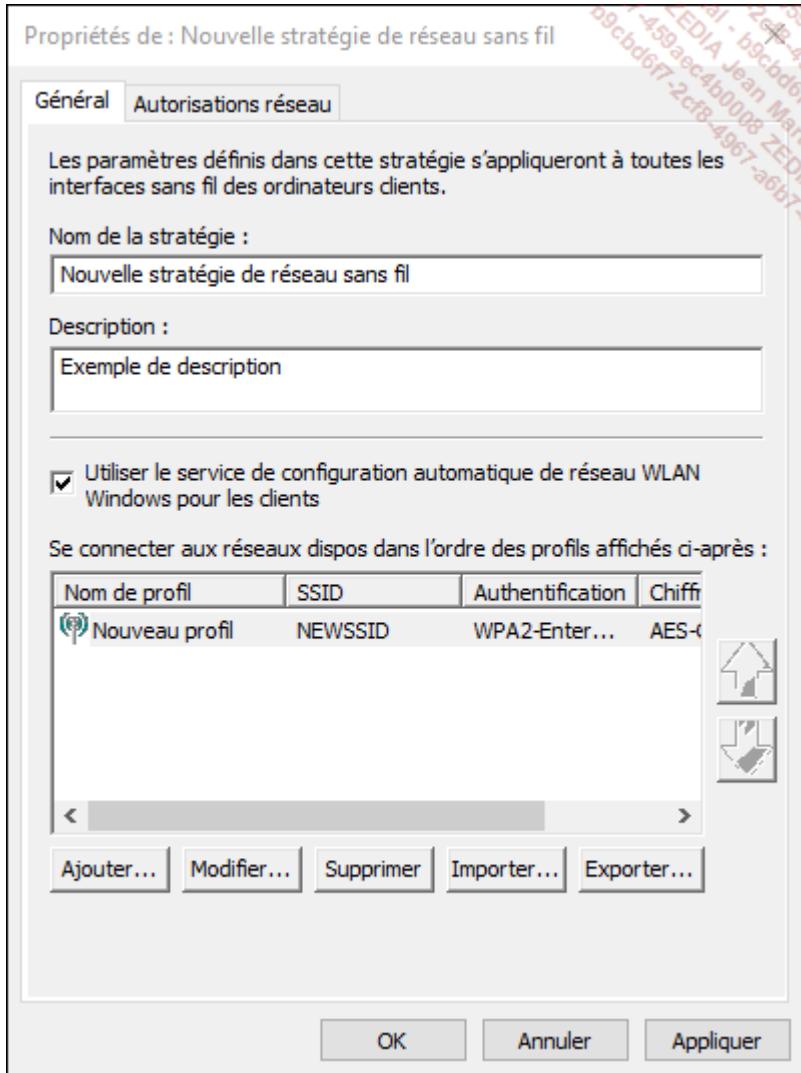


- Saisissez le **Nom du réseau** (SSID), sélectionnez son **Type de sécurité**, entrez la **Clé de sécurité** et cochez **Se connecter automatiquement**. Confirmez les paramètres en cliquant sur le bouton **Enregistrer**.

Avec la ligne de commande : la commande netsh wlan permet de configurer localement ou à distance des réseaux sans fil.

Par exemple, la commande netsh wlan connect name=Profile1 ssid=mytraining interface="wi-fi" créera une connexion au réseau "mytraining" depuis la carte sans fil nommée Wi-Fi du client Windows 11.

Avec la stratégie de groupe, depuis un serveur : dans un environnement Active Directory, l'administrateur peut configurer de manière homogène des réseaux sans fil sur ses postes Windows 11. Cela s'effectue au travers du nœud **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité et Stratégies de réseau sans fil (IEEE 802.11)**. Vous pourrez définir des réseaux sans fil préférés, définir les paramètres de sécurité appropriés, ou encore empêcher la connexion à des réseaux spécifiques.



Auparavant, un ordinateur en veille qui sortait de celle-ci nécessitait un temps d'attente avant la reconnexion au réseau Wi-Fi utilisé. Avec Windows 11, il faut une à deux secondes pour que l'utilisateur y soit connecté, les informations de connexion étant appliquées une nouvelle fois rapidement par le système.

Lorsqu'une connexion à un réseau sans fil est lente ou impossible, l'administrateur recherche la cause du problème et entreprend les actions correctives. Plus le signal est fort, meilleures sont les performances. Un point d'accès situé à une grande distance du poste de travail peut expliquer un temps de latence conséquent. La présence d'un composant Bluetooth peut interférer avec le signal du réseau sans fil.

Une armoire en métal ou un mur épais peut expliquer la faiblesse du signal, de même que les interférences créées par des téléphones sans fil. Dans certains cas, envisagez de définir un numéro de canal différent sur le point d'accès.

Si le réseau sans fil auquel le client veut se connecter ne s'affiche pas, vérifiez que la carte réseau sans fil est activée et dispose du pilote approprié. Certains points d'accès sans fil ne publient pas leur SSID pour améliorer la sécurité. De plus vérifier la compatibilité Wi-Fi : un PC disposant d'une carte Wi-Fi 802.11n (Wi-Fi 5) ne pourra pas se connecter à un réseau sans fil 802.11ac (Wi-Fi 6).

1. Réseau cellulaire

Les réseaux 4G et 5G représentent des débits compris entre quelques dizaines jusqu'à plusieurs centaines de mégabytes. Ils sont généralement rapides malgré un temps de latence élevé. Ils utilisent le réseau cellulaire géré par un opérateur mobile (SFR, Orange, Bouygues Telecom...). Ces réseaux imposent généralement des seuils de données avec des coûts de dépassement élevés.

Avec Windows 7, les utilisateurs devaient installer les pilotes et les logiciels fournis par les fournisseurs d'accès puis configurer les connexions. Windows 10 a simplifié ces exigences en proposant un pilote intégré nativement et mis à jour via Windows Update. Windows 11 dispose donc d'un pilote natif et d'une interface remaniée pour configurer ce type de réseau.

L'opérateur mobile est automatiquement identifié puis la carte SIM liée est configurée. Le cas échéant, l'application propriétaire est téléchargée depuis le Microsoft Store, permettant ainsi de payer sa facture, visualiser la consommation des données ou utiliser l'assistance technique !

L'utilisateur peut choisir directement un forfait mobile gérant les données sur le site internet de l'opérateur, il sera ensuite appliqué aux paramètres de connexion.

Grâce à la norme MBIM (*Mobile Broadband Interface Model*), Windows 11 peut exploiter les périphériques haut débit mobiles depuis une seule interface. Il est ainsi possible d'activer ou de désactiver les différentes cartes (Bluetooth, haut débit, Wi-Fi...) :

Cliquez sur le menu **Démarrer, Paramètres, Réseau et Internet**. Vérifiez que **Réseau cellulaire** est activé et cliquez sur ce menu.



Dans les **Paramètres, Réseau et Internet**, les premières lignes affichent quelques informations sur les réseaux, dont la consommation des données Wi-Fi et Cellulaire des 30 derniers jours.

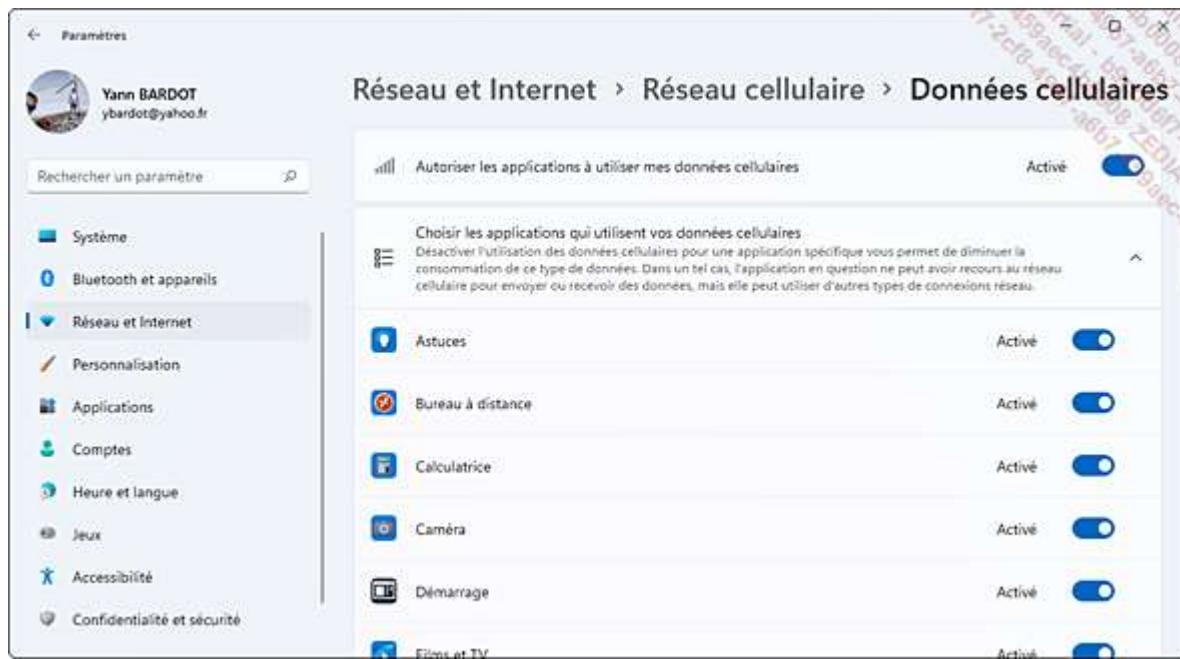
The screenshot shows the Windows 11 Settings interface under the 'Réseau et Internet' section. On the left, a sidebar lists various settings categories. The 'Réseau et Internet' category is selected and expanded, showing sub-options like 'Wi-Fi', 'Cellular', 'Ethernet', and 'VPN'. Each option has a status bar at the top right indicating connectivity and data usage over the last 30 days. A search bar is at the top left.

Vous pouvez retrouver ces informations détaillées et configurer une limite en cliquant sur **Consommation des données** ou en vous rendant dans **Paramètres réseau avancés**, **Consommation des données**.

This screenshot shows the 'Advanced network data consumption' settings page. It displays the total data usage ('5.14 Go') over the last 30 days and provides a breakdown of usage by application. At the top right, there's a button to 'Enter a limit'. Below the usage summary, a chart shows the data consumption of various applications: Système (2.45 Go), msedge.exe (961 Mo), OneDrive.exe (353 Mo), Windows Web Experience Pack (81 Mo), and Microsoft Store (80 Mo).

Windows 11 permet de déterminer les applications consommatrices de données (dans l'exemple, sur le réseau Wi-Fi) et de fixer une limite en cliquant sur le bouton **Entrer une limite**.

De plus, Windows 11 permet de sélectionner les applications pouvant utiliser les données cellulaires, depuis **Paramètres**, **Réseau et Internet**, **Réseau cellulaire** et **Données cellulaires**. Il suffit d'activer ou de désactiver l'application désirée. Par défaut, elles sont toutes activées.



Le suivi de la consommation réseau en direct par les applications est disponible depuis le **Gestionnaire des tâches**, onglet **Processus**.

Avec Windows 11, le système analyse le comportement de l'utilisateur (déconnexion manuelle d'un réseau sans fil, type de réseau) puis crée une liste de ses habitudes qu'il maintient à jour. Par exemple, si l'utilisateur est connecté à un réseau "A" puis qu'il se déconnecte de celui-ci pour se lier à un réseau "B", Windows 11 placera le réseau "B" plus haut dans la liste de ses réseaux préférés.

Lorsqu'un utilisateur connecté à un réseau haut débit mobile se trouve à proximité d'un réseau Wi-Fi préféré, Windows 11 le déconnecte automatiquement du premier réseau afin de privilégier la rapidité offerte par le Wi-Fi. Le cas échéant, le périphérique haut débit est désactivé, afin de préserver la batterie.

Le Mode Avion est toujours présent ; il permet d'activer ou de désactiver rapidement, depuis la barre des tâches, toutes les interfaces gérant les réseaux sans fil, à la manière d'un smartphone.

2. Affichage sans fil Miracast

Face au Airplay d'Apple ou WiDi d'Intel, le consortium Wi-Fi Alliance a développé une technologie permettant de projeter des images et sons entre un périphérique mobile (tablette tactile, ordinateur portable...) et un téléviseur, vidéoprojecteur ou moniteur, grâce à un réseau sans fil. Ainsi, l'utilisateur peut afficher une présentation PowerPoint ou encore jouer à un jeu sur un écran plus grand que celui de son périphérique.

Windows 11 supporte cette fonctionnalité sur toutes les éditions du système, et propose le Wi-Fi Direct, le protocole WPA2 pour sécuriser les flux, le support du codec H.264 matériel pour le codage vidéo, ainsi que le Wi-Fi 802.11n pour la connectivité. Notez que la résolution théorique est de 1080p Full HD.

Pour pouvoir utiliser l'affichage sans fil, la machine doit disposer d'une carte graphique prenant en charge la version 2 de *Windows Display Driver Model*(WDDM) et d'une carte Wi-Fi gérant le Wi-Fi Direct.

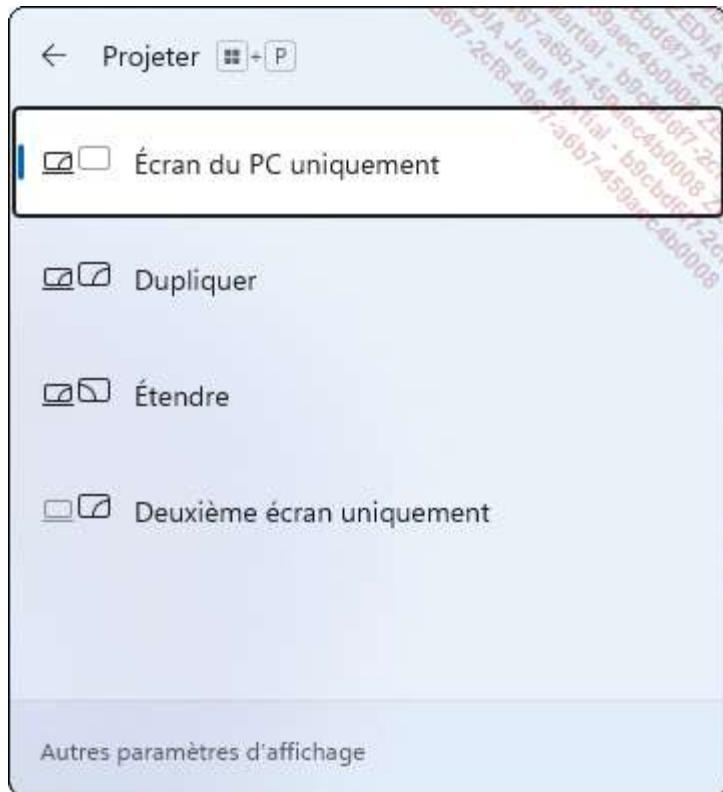
Si votre écran cible ne supporte pas la technologie Miracast, il sera nécessaire d'acquérir un adaptateur qui sera branché sur le port HDMI du périphérique d'affichage.

Pour ajouter l'écran sans fil compatible Miracast à votre tablette ou votre PC, suivez la procédure ci-dessous :

Depuis le menu **Démarrer**, cliquez sur **Paramètres** et sur **Système**. Dans la section **Affichage**, déroulez **Plusieurs affichages** et dans la section **Se connecter à un affichage sans fil**, cliquez sur le bouton **Se connecter** ou bien appuyez sur les touches + K.

Maintenant que l'écran sans fil a été ajouté, partager son écran est simple :

Choisissez le type de configuration de l'affichage parmi ces quatre choix : afficher l'**Écran du PC uniquement**, **Duplicer** l'affichage de manière identique sur les deux écrans, **Étendre** l'affichage ou afficher sur le **Deuxième écran uniquement**.



Notez qu'il est nécessaire que l'écran sans fil soit situé à proximité de votre périphérique Windows 11.

Lorsque votre PC Windows 11 bascule en mode veille, ou bien s'il est déplacé hors de portée de votre écran sans fil, il sera automatiquement déconnecté de ce dernier.

3. Wi-Fi tethering

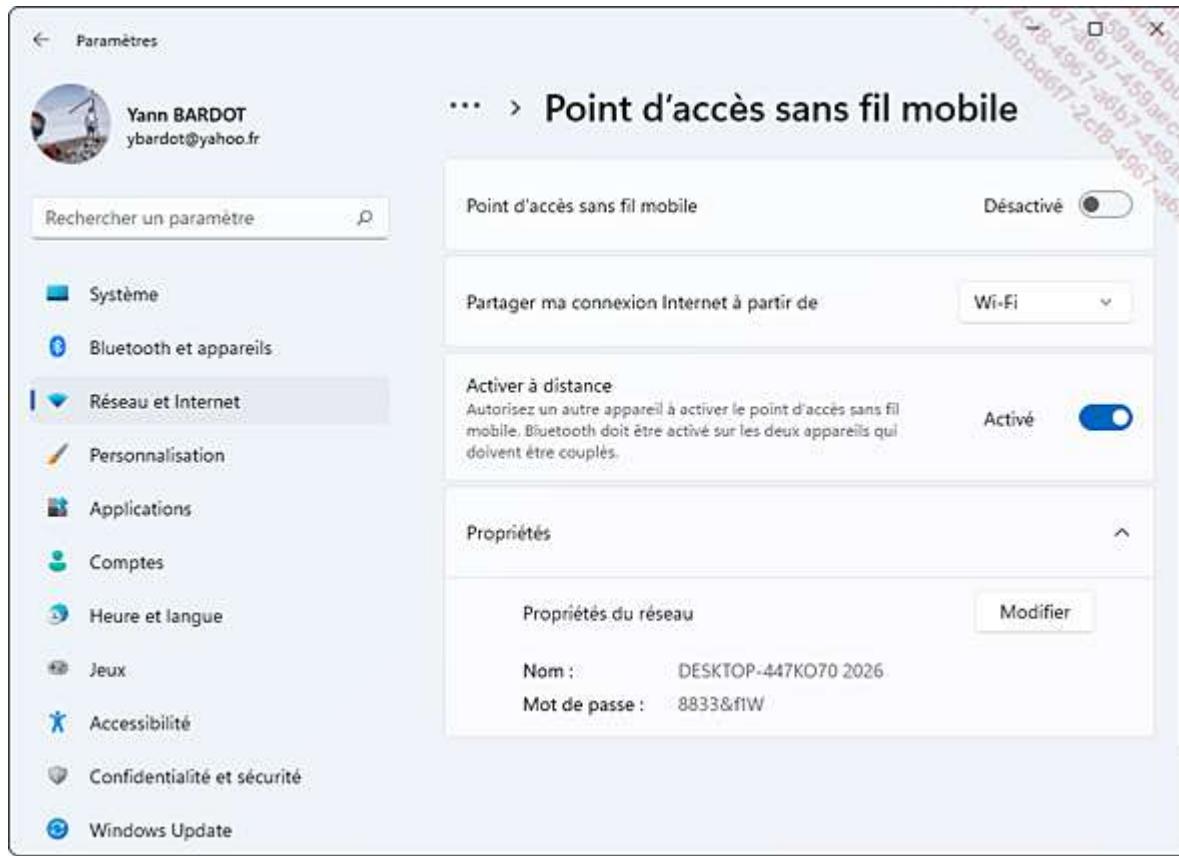
Le partage d'une connexion de données cellulaires (3G, 4G ou 5G) avec un autre périphérique est quelquefois appelé « *tethering* » (connexion d'un périphérique à un autre). La connexion par tethering transforme ainsi le smartphone en point d'accès sans fil mobile. Cette fonctionnalité est souvent facturée à l'utilisateur par l'opérateur téléphonique, si celui-ci franchit une quantité de données transmises.

Donc, en insérant une carte SIM ou en se connectant au réseau d'un opérateur téléphonique, Windows 11 peut partager sa connexion internet à d'autres périphériques. Néanmoins, les mises à jour de sécurité et des applications ne seront pas téléchargées par ce biais, afin de limiter l'utilisation de la bande passante allouée.

Désormais, il est possible de convertir l'ordinateur portable ou la tablette tactile Windows 11 en point d'accès sans fil afin de partager avec au maximum dix périphériques la connexion internet.

Pour activer le partage de connexion, suivez la procédure ci-dessous :

Cliquez sur le bouton **Démarrer**, puis **Paramètres, Réseau et Internet**. Activez le **Point d'accès mobile**.



Vous pouvez définir depuis quel périphérique partager votre connexion (Wi-Fi, Bluetooth) et autoriser l'activation à distance depuis un autre appareil couplé en Bluetooth.

Dorénavant, en connectant votre périphérique au réseau sans fil diffusé par le poste de travail Windows 11, vous pourrez utiliser la connexion internet de ce dernier.

Allocation automatique d'adresses IP

- Windows 11 supporte, comme tout système d'exploitation, l'obtention d'une adresse IP depuis un serveur DHCPv4 ou DHCPv6. Le bénéfice pour un administrateur est important, car il n'a plus à s'occuper de gérer les adresses IP allouées sur le réseau de l'entreprise. Répertorier les adresses IP statiques consomme du temps et augmente le risque d'erreur.
- Le service Client DHCP gère l'inscription et la mise à jour des adresses IP auprès du serveur DHCP, ainsi que les enregistrements DNS correspondants.
- En cas de défaut du serveur DHCP, le client s'octroiera automatiquement une adresse IP APIPA, sur le réseau 169.254.0.0/16. Néanmoins, cette configuration ne permettra pas d'utiliser les services Active Directory ou Internet, car aucune passerelle, aucun serveur DNS ou WINS ne sont configurés dans ce réseau. Pour pallier cette limitation, Microsoft propose d'utiliser la configuration alternative.

305 Un bon moyen d'éviter l'utilisation de l'APIPA est de mettre en place la résilience DHCP : deux serveurs DHCP proposent des étendues différentes (50 % des adresses disponibles pour l'un, 50 % l'autre) aux clients DHCP. Ainsi, si l'un devient inaccessible, l'autre continuerait à distribuer les adresses IP.

Configuration alternative

- L'onglet **Configuration alternative**, disponible dans les propriétés d'une carte réseau IPv4, permet de spécifier le comportement du client Windows 11 en cas d'indisponibilité d'un serveur DHCP. L'utilisateur peut au choix utiliser l'adressage IP privée automatique ou bien spécifier une adresse IP alternative manuellement.

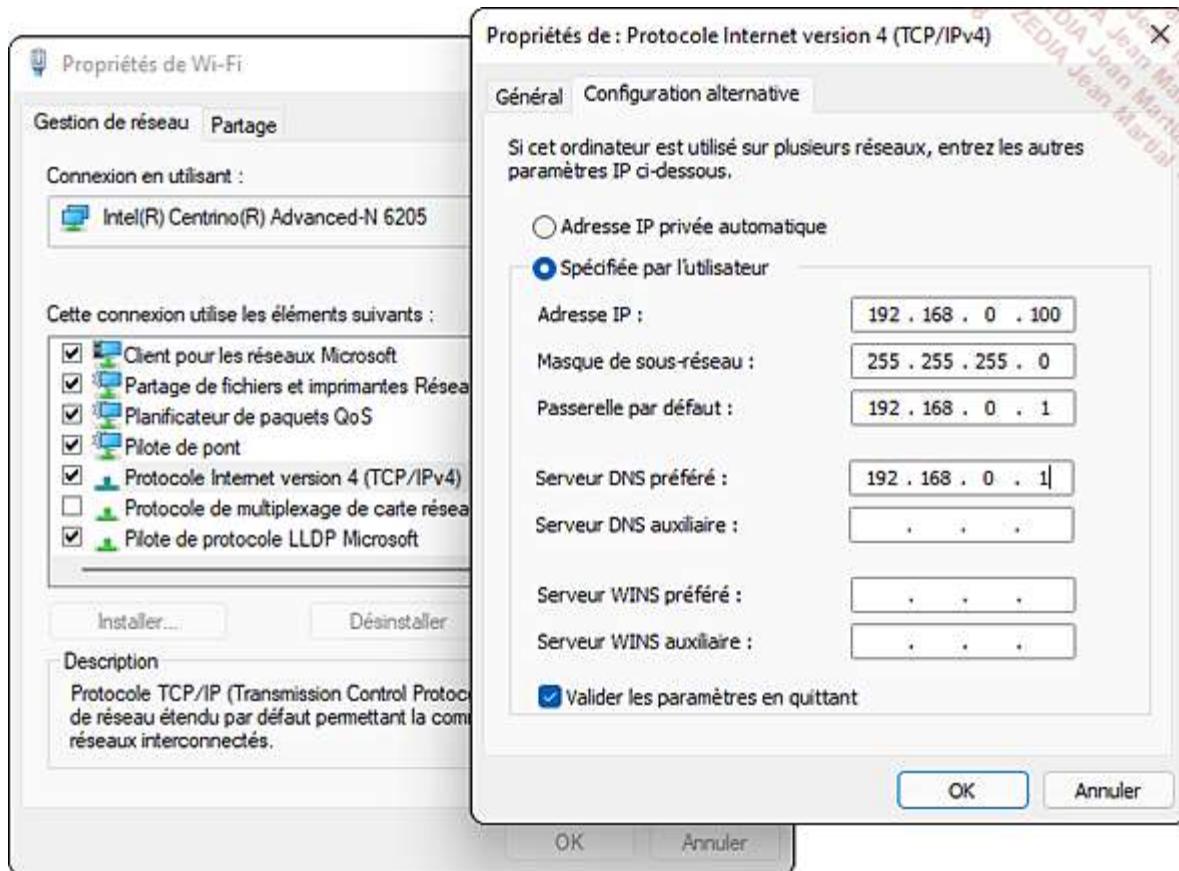
- Pour définir une configuration IP alternative, suivez la procédure ci-dessous :

Depuis le bureau, pressez les touches  + R puis saisissez ncpa.cpl dans la fenêtre **Exécuter** et validez par la touche [Entrée].

Dans la fenêtre **Connexions réseau**, sélectionnez la carte réseau sur laquelle vous souhaitez définir une configuration IP alternative, effectuez un clic avec le bouton droit puis choisissez **Propriétés**.

Dans la fenêtre **Propriétés de Ethernet**, sélectionnez **Protocole Internet version 4 (TCP/IPv4)** et cliquez sur le bouton **Propriétés**.

Sélectionnez l'onglet **Configuration alternative**, puis cochez la case **Spécifiée par l'utilisateur** et renseignez les champs **Adresse IP**, **Masque de sous-réseau**, **Passerelle par défaut**, **Serveur DNS préféré**. Cochez ensuite la case **Valider les paramètres en quittant** pour tester la configuration.



Confirmez en cliquant sur le bouton **OK**.

Résolution des noms

Il est plus facile de se rappeler le nom d'un site plutôt que son adresse IP sur 4 octets : par exemple, l'adresse IP 173.194.66.94 correspond actuellement au nom de domaine google.fr, plus facilement mémorisable. Un processus de résolution consiste simplement à convertir une adresse IP en nom.

Un nom d'ordinateur (ou nom d'hôte), utilisant le système de noms de domaine, peut comporter jusqu'à 255 caractères, avec des caractères alphanumériques, des points et des traits d'union. C'est le système utilisé sur Internet au travers d'une résolution DNS (*Domain Name System*).

Windows 11 prend en charge la résolution des noms DNS.

1. Système de noms de domaine

Inventé dans les années 80, le système de noms de domaine (ou DNS) est un service qui résout les noms d'hôte conviviaux en adresses IP, et inversement. Windows 11 utilise DNS pour rechercher des contrôleurs de domaine dans l'Active Directory, des ressources comme des serveurs de messagerie (enregistrement MX (*Mail eXchanger*)) et pour se connecter à d'autres clients.

Lorsqu'un client Windows 11 essaie de résoudre un nom d'ordinateur DNS, il suit les étapes suivantes :

1. Le nom demandé est-il son propre nom ?
2. Vérification du nom d'hôte et de sa correspondance dans le fichier hosts local stocké dans le dossier %systemroot%\System32\drivers\etc\.
3. Tentative de résolution depuis le cache DNS : commande ipconfig /displaydns pour l'afficher, ipconfig /flushdns pour vider son contenu.
4. Interrogation des serveurs DNS.
5. Si le nom n'est pas encore résolu, la requête est éventuellement adressée au serveur WINS.

Le système DNS est une partie essentielle d'un domaine Active Directory Windows Server 2008 ou supérieur, il s'intègre parfaitement avec le service DHCP auquel peut être confiée la tâche d'enregistrer auprès du serveur DNS les nouvelles IP des ordinateurs.

Pour définir l'adresse IP d'un serveur DNS primaire (serveur préféré pour la résolution de noms) sur un poste Windows 11, vous pouvez utiliser la commande netsh dans un Terminal :

```
netsh interface ipv4 set dnsservers "Ethernet" static
```

```
192.168.0.2 primary
```

Vous pouvez aussi utiliser l'interface graphique des propriétés de la carte réseau depuis les **Paramètres, Réseau et Internet, Paramètres réseau avancés** :

Cliquez sur l'adaptateur réseau que vous souhaitez modifier, puis sur **Afficher les propriétés supplémentaires**.

Sur la ligne **Attribution d'adresse IP**, cliquez sur le bouton **Modifier** et sélectionnez **Manuel**.

Cochez **IPv4** dans le cas présent, et inscrivez les paramètres IP.

Modifier les paramètres IP

Manuel

IPv4

Activé

Adresse IP

192.168.0.100

Masque de sous-réseau

255.255.255.0

Passerelle

192.168.0.1

DNS préféré

192.168.0.2

X

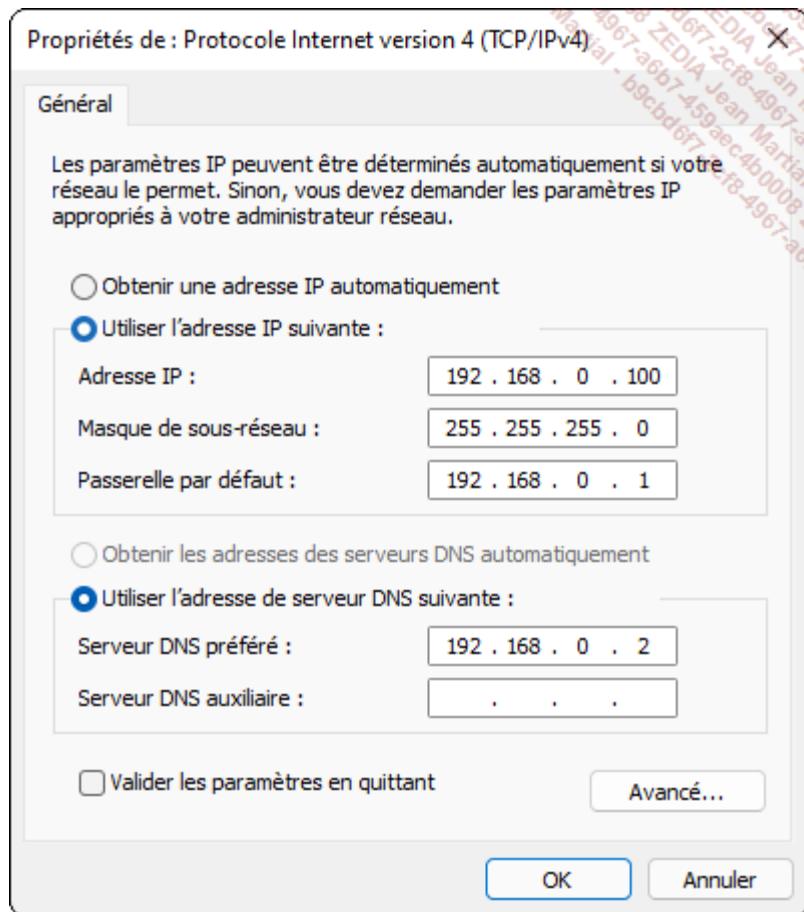
Chiffrement DNS préféré

Non chiffré uniquement

Enregistrer

Annuler

306 Vous pouvez également passer par les propriétés vues dans la partie précédente :



Pour accéder à un dossier partagé nommé **Cours**, situé sur un serveur distant **SRV1** (adresse IP **192.168.0.10**) géré par le système DNS dans un domaine **mytraining.fr**, utilisez au choix la convention ci-dessous :

- \\SRV1.mytraining.fr\Cours
- \\192.168.0.10\Cours
- File:///192.168.0.10/Cours

Si le serveur distant fait aussi fonction de serveur web (rôle IIS) :

- <http://SRV1.mytraining.fr/Cours/>

Résumé du chapitre

- Windows 11 implémente en standard les protocoles IPv4 et IPv6. La commande netsh permet de configurer le réseau d'un client distant. L'administrateur peut utiliser les utilitaires de résolution des problèmes pour résoudre les problèmes réseau les plus courants.
- Avec Windows 11, la configuration réseau s'effectuera généralement depuis les **Paramètres**, dans la rubrique **Réseau et Internet** : état de celui-ci, configuration, création d'une nouvelle connexion et réparation. Les paramètres supplémentaires seront accessibles dans **Connexions réseau**.
- Tout comme les anciennes versions clientes de Microsoft, Windows 11 peut remplir les fonctions basiques d'un serveur VPN : chiffrement des communications et création d'un tunnel sécurisé. Le service Routage et accès distant permet la réception de connexions entrantes VPN.
- Windows 11 fournit une prise en charge complète des normes actuelles (Wi-Fi 4, 5, 6 et 6E) et supporte deux modes de connexion : ad hoc et infrastructure. La configuration d'un réseau sans fil s'effectue de trois manières différentes : graphiquement par le panneau Wi-Fi, par la commande netsh ou grâce à un objet stratégie de groupe.
- Les réseaux 4G et 5G sont désormais gérés nativement grâce à un pilote intégré et mis à jour régulièrement via Windows Update. Leur disponibilité est affichée dans la même interface que celle gérant les réseaux Wi-Fi.
- Windows 11 supporte la technologie Miracast, permettant de projeter des images et sons entre un périphérique mobile et un téléviseur, vidéoprojecteur ou moniteur, grâce à un réseau sans fil.
- Désormais, il est possible de convertir l'ordinateur portable ou la tablette tactile Windows 11 en point d'accès sans fil afin de partager avec au maximum dix périphériques la connexion internet : c'est le Wi-Fi tethering.
- La configuration alternative permet de spécifier le comportement du client Windows en cas d'indisponibilité d'un serveur DHCPv4.
- DNS est un service qui résout les noms d'hôte conviviaux (255 caractères maximum) en adresses IP, et inversement.

Protection et récupération du système

Sauvegarde et restauration

Planifier une sauvegarde discrète et sécurisée des données importantes permet d'assurer une continuité de service en cas de sinistre informatique. Que vous copiez vos données grâce au réseau, sur DVD, sur média amovible USB, localement ou sur le cloud public Microsoft Azure, l'important est de sauvegarder. C'est en quelque sorte l'assurance-vie de vos données.

Lorsque vous planifiez un processus de sauvegarde, il est important de tenir compte de sa taille et du temps nécessaire à son exécution. Le support de sauvegarde (durée de vie, vitesse de copie), la durée de conservation ainsi que le lieu de conservation sont autant d'éléments majeurs à prendre en considération.

Le coût de stockage des données peut vite devenir problématique : par exemple, la sauvegarde des données sur réseau SAN (*Storage Area Network*) génère un coût élevé par mégaoctet (Mo) alors que la sauvegarde sur disque externe USB est plus compétitive, mais en assure une sécurité moindre.

1. OneDrive

Microsoft propose par défaut un espace de stockage privé de 5 Go dans le cloud Microsoft pour sauvegarder automatiquement ses données. Cet outil a été abordé précédemment au chapitre Gestion des disques et des pilotes, section Partitionnement et gestion des fichiers.

Les avantages de cet outil sont les suivants : pas de supports à gérer, sauvegarde automatique, historique des versions, restauration simplifiée.

2. Réinitialiser ce PC

Un administrateur peut réattribuer un ordinateur inutilisé à une personne de l'entreprise. Un particulier peut vouloir vendre son ordinateur, en s'assurant qu'aucune de ses données personnelles n'est encore présente sur le disque dur et ainsi fournir les logiciels préinstallés avec le PC.

Dans ces cas-là, Microsoft introduit la fonctionnalité **Réinitialiser ce PC** ; les partitions sont formatées et une nouvelle copie de Windows 11 est installée. L'utilisateur peut avant cette action choisir de conserver ses fichiers personnels.

Pour réinitialiser le PC, l'administrateur peut effectuer la manipulation depuis les paramètres de Windows 11 :

Cliquez sur le menu **Démarrer** puis sur **Paramètres**. Cliquez sur **Système** puis **Récupération**.

Choisir une option

Conserver mes fichiers

Avec cette option, vous supprimez les applications et les paramètres, mais vous conservez les fichiers personnels.

Supprimer tout

Avec cette option, vous supprimez l'ensemble des fichiers personnels, des applications et des paramètres.

[Comment choisir ?](#)

[Annuler](#)

Sélectionnez une de ces deux options : **Conserver mes fichiers** ou **Supprimer tout**.

Une fois le choix effectué, l'utilisateur doit insérer le support d'installation puis redémarrer l'ordinateur.

Si Windows 11 ne peut plus démarrer, suite par exemple à la corruption du secteur d'amorce par un virus, l'administrateur ne parviendra pas à exécuter une actualisation de PC depuis l'interface. Il est dans ce cas possible d'exécuter Windows RE depuis le support d'installation Windows 11, ou bien d'utiliser une mémoire flash USB (cf. chapitre Installation du client Windows 11).

3. Historique des fichiers

Dans les anciennes versions de Microsoft Windows, environ 5 % des utilisateurs sauvegardaient régulièrement leurs données, ce qui est peu, en comparaison des sinistres informatiques (virus, défaillance matérielle, mauvaise manipulation) qui apparaissent... au plus mauvais moment !

Les données de l'utilisateur doivent être sauvegardées, quel que soit le lieu où l'ordinateur est connecté.

Pour aider l'administrateur, Microsoft a développé la fonctionnalité **Historique des fichiers** : chaque heure, les fichiers modifiés sont copiés à un emplacement déterminé, créant ainsi un historique des différentes versions, tout ceci en arrière-plan et sans intervention de l'utilisateur.

La sauvegarde peut être stockée dans un dossier partagé situé sur un serveur ou sur un NAS (*Network Attached Storage*), mais aussi sur un périphérique externe, comme un disque dur externe USB.

Désormais, il n'est plus nécessaire d'être administrateur du poste de travail pour configurer une sauvegarde, n'importe quel utilisateur le peut.

Par défaut, Historique des fichiers sauvegarde les données présentes dans les dossiers Documents, Images, Contacts, Bureau, Favoris... L'utilisateur peut bien entendu ajouter manuellement les répertoires à sauvegarder.

Contrairement au composant Sauvegarder et restaurer (Windows 7) Historique des fichiers ne sauvegarde pas le système d'exploitation ou les applications, mais uniquement les fichiers personnels.

Grâce au journal des modifications NTFS, la fonctionnalité cible rapidement les données modifiées et exécute la sauvegarde correspondante. En cas de mise en veille, coupure de courant ou saturation du processeur, Historique

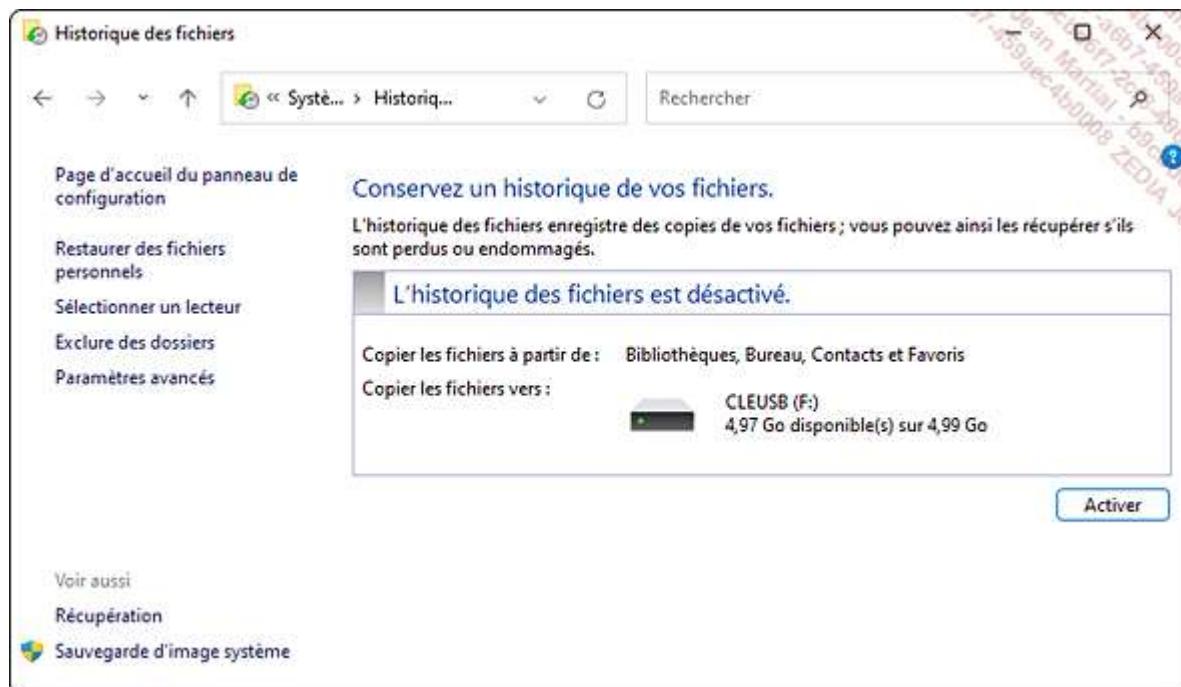
des fichiers suspend son activité et la reprend plus tard au point arrêté. À l'aide d'un cache local situé sur la partition système, si le lecteur dédié à la sauvegarde devenait indisponible, les données y seraient temporairement copiées, en attendant la reconnexion du lecteur.

Le fait qu'un lecteur chiffré à l'aide de BitLocker (cf. chapitre Configuration de la sécurité Windows, section Sécurisation des données hors connexion) soit utilisé comme source ou destination de sauvegarde n'a aucune incidence sur la fonctionnalité **Historique des fichiers**, elle le prend en charge de manière transparente.

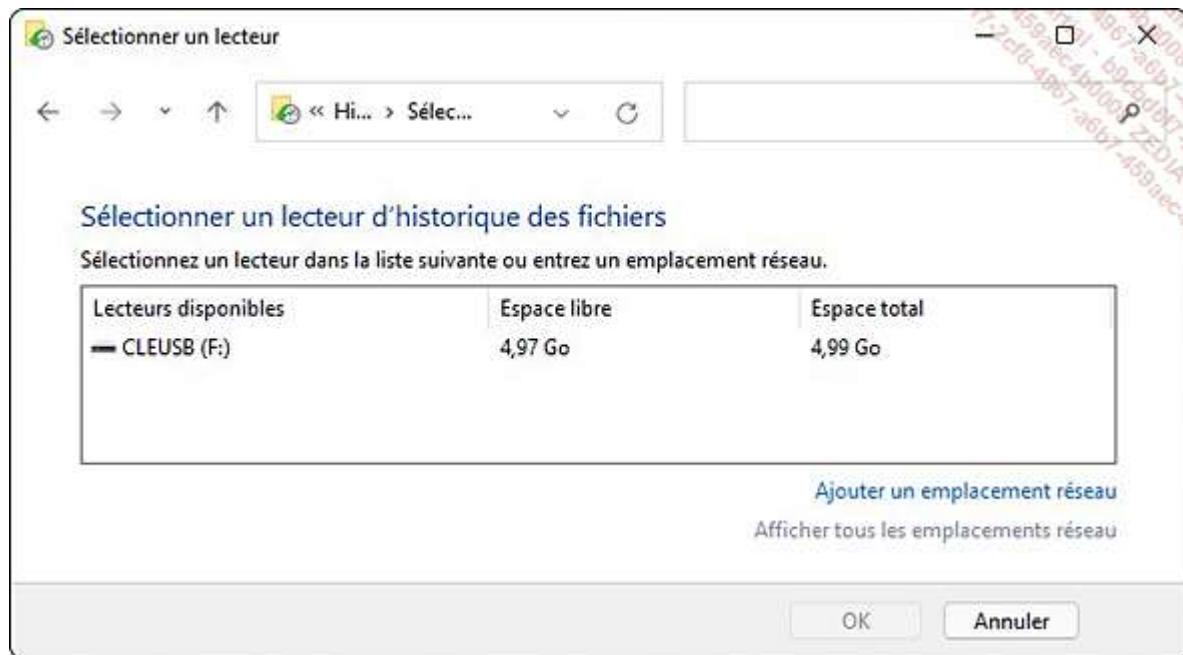
a. Configurer une sauvegarde

Pour activer la fonctionnalité **Historique des fichiers**, suivez la procédure ci-dessous :

Branchez un périphérique externe sur le poste de travail Windows 11. Cliquez sur le menu **Démarrer**, puis saisissez historique et cliquez sur **Historique des fichiers - Panneau de configuration**.



L'étape suivante consiste à ajouter un lecteur (clé USB ou partage réseau) qui sauvegardera les fichiers cibles. Cliquez sur **Sélectionner un lecteur**. La liste des cibles de stockage disponibles s'affiche. Sélectionnez le lecteur de votre choix et cliquez sur le bouton **OK**.



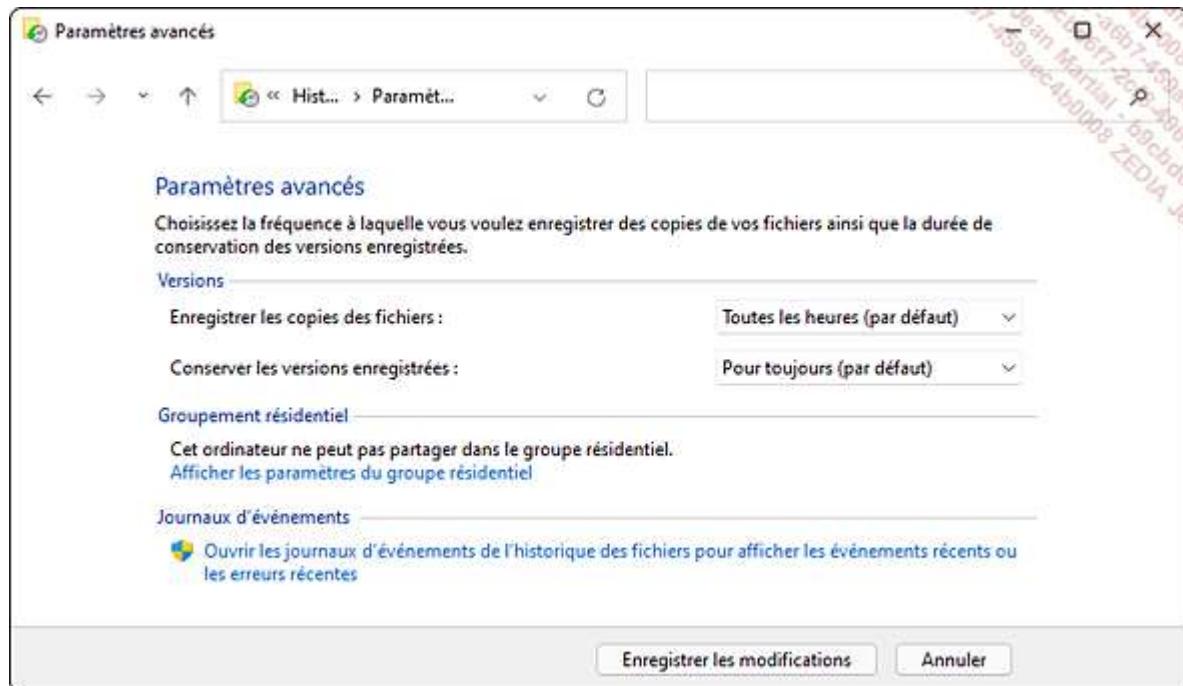
Cliquez sur le bouton **Activer**. Les données sont sauvegardées automatiquement et un dossier nommé **FileHistory** est créé sur le média de destination. Celui-ci peut être parcouru depuis l'**Explorateur de fichiers** comme n'importe quel répertoire.

En cliquant sur **Sélectionner un lecteur** dans la fenêtre **Historique des fichiers**, l'utilisateur peut visualiser les emplacements contenant les sauvegardes.

Grâce à cette interface, lorsqu'un lecteur est saturé, l'utilisateur peut changer la destination des sauvegardes en déplaçant les données existantes vers le nouveau lecteur, ou bien ne rien faire en créant ainsi un nouveau jeu de sauvegarde. Cette action s'effectue en cliquant sur le bouton **Ajouter un emplacement réseau**.

Pour modifier les paramètres de la sauvegarde, procédez comme suit :

Dans la fenêtre **Historique des fichiers**, cliquez sur **Paramètres avancés**.



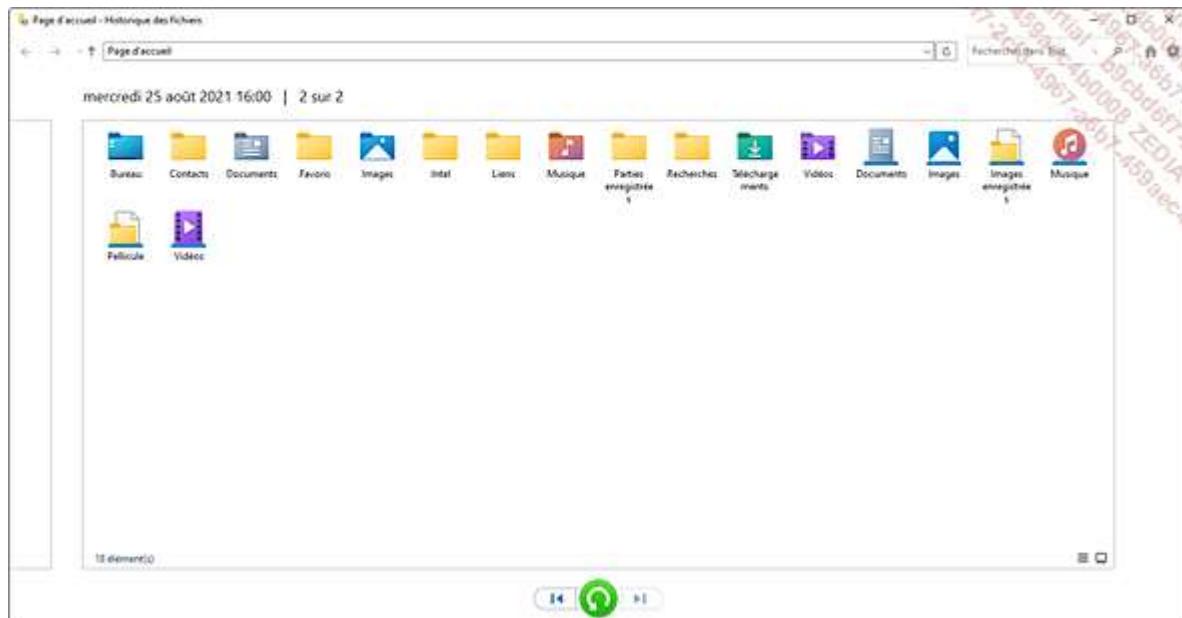
Modifiez la fréquence des copies (**Toutes les heures (par défaut)**) et la durée de rétention des données (**Pour toujours (par défaut)**) et cliquez sur le bouton **Enregistrer les modifications**.

Les événements liés à la fonctionnalité **Historique des fichiers** sont disponibles depuis l'**Observateur d'événements**, dans le nœud **Journaux des applications et des services - Microsoft - Windows - FileHistory - Engine** et **Journal de sauvegarde de l'historique des fichiers**.

Pour désactiver la fonctionnalité sur les postes de travail d'un domaine, éditez un objet de stratégie de groupe puis développez le nœud **Configuration ordinateur - Stratégies - Modèles d'administration - Composants Windows** et **Historique des fichiers**. Éditez ensuite le paramètre **Désactiver l'historique des fichiers**.

b. Restaurer les données

Une fois la sauvegarde configurée, une corruption ou perte de données peut survenir, l'application de restauration permettra d'y remédier simplement. Il suffit de cliquer sur **Restaurer des fichiers personnels** dans la fenêtre principale **Historique des fichiers**, puis de sélectionner l'heure et la date de sauvegarde grâce aux flèches de défilement et de cliquer sur le bouton pour restaurer les données visées.

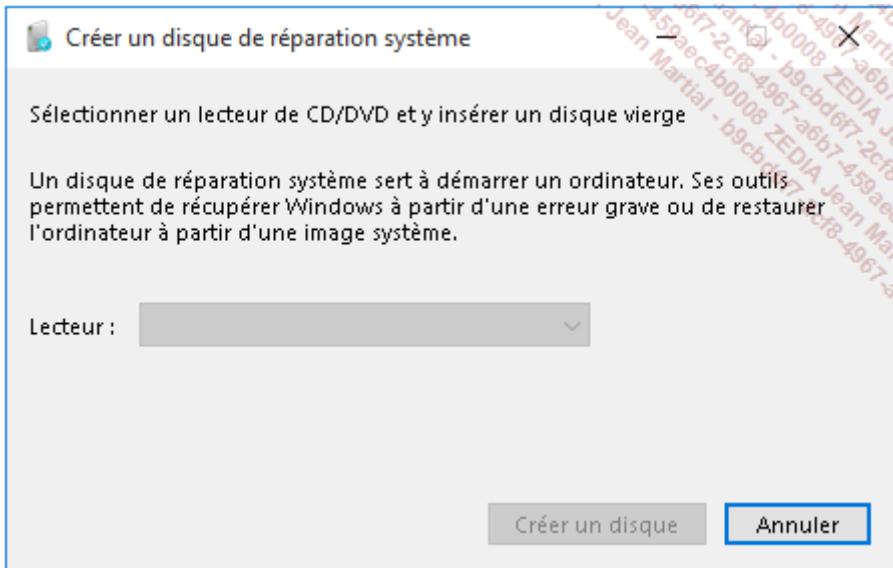


4. Sauvegarde de fichiers et volumes

a. Sauvegarder et restaurer (Windows 7)

Windows 7 a introduit la fonctionnalité **Sauvegarder et restaurer**. Elle est accessible depuis le panneau de configuration et propose trois types de sauvegarde :

- **Créer une image système** : contient une sauvegarde complète de toutes les partitions utilisées par Windows pour fonctionner, ainsi que celles mentionnées par l'utilisateur. Utile en cas de dysfonctionnement total d'un ordinateur, lors de la panne d'un disque dur par exemple. Les volumes EFI et systèmes sont automatiquement sélectionnés.
- **Sauvegarder des fichiers** : crée des copies des fichiers de données en planifiant une occurrence. Windows peut de lui-même lister les fichiers importants, ou bien l'utilisateur peut le faire manuellement. Ce type de sauvegarde est remplacé par la fonctionnalité **Historique des fichiers** fournie avec Windows 10.
- **Créer un disque de réparation système** : grave sur un CD ou un DVD l'environnement de récupération Windows RE avec des outils de restauration des sauvegardes ou de vérification du matériel. La commande `reldrive.exe` livrée avec Windows permet aussi de lancer l'assistant de création. Cette commande ne fonctionne pas si vous n'avez pas de graveur.



- Le système peut vous demander d'insérer le DVD d'installation du produit si les fichiers nécessaires à la création du disque de réparation ne sont pas présents sur le disque dur.

Cette fonctionnalité est abordée un peu plus loin dans ce chapitre (cf. section Dépannage du système).

D'autres méthodes de sauvegarde sont proposées par Windows 11 pour assurer une disponibilité des données, parmi lesquelles la commande robocopy permettant de copier des dossiers et des fichiers de manière industrielle, en reprenant par exemple une opération là où elle s'est arrêtée, en respectant les attributs... robocopy c:\users\philou e:\sauvegarde /MIR /Z copiera exactement (MIR pour copie miroir) le contenu du profil de l'utilisateur « philou » dans le dossier de sauvegarde situé sur le lecteur E:, en supprimant tout fichier présent dans ce dossier de destination. Le commutateur /Z reprendra la copie en cas de perte de connexion réseau.

- Notez l'option /MT[:n] qui permet d'exploiter le multithread lors de la copie des fichiers en indiquant le nombre (n) de threads.

Sauvegarder les données critiques est vital, mais tester la restauration, avant d'en avoir vraiment besoin, l'est tout autant. Réaliser fréquemment une restauration d'essai vous permettra de connaître la durée du processus et les éventuels problèmes rencontrés.

b. Commande wbadmin

Les opérations de sauvegarde sont disponibles en ligne de commande, à l'aide de la commande wbadmin, qui remplace l'ancienne commande ntbackup. La version de l'utilitaire wbadmin livrée avec Windows 11 est plus limitée que celle fournie avec Windows Server 2019. Par exemple, il n'est pas possible de créer une récupération en l'état du système.

- Les sauvegardes effectuées avec ntbackup ne peuvent pas être restaurées avec wbadmin.

Pour configurer une sauvegarde planifiée en ligne de commande, il faut appartenir au groupe Administrateurs. Pour restaurer ou créer une sauvegarde, être membre du groupe Opérateurs de sauvegarde suffit.

L'utilitaire wbadmin nécessite donc d'être exécuté depuis un Terminal avec des priviléges élevés. Dans l'exemple qui suit, l'objectif est de sauvegarder le volume C: sur le volume D: sans modifier le calendrier de sauvegarde :

Cliquez avec le bouton droit sur le menu **Démarrer** puis sur **Terminal Windows (administrateur)**.

Validez en cliquant sur le bouton **Oui** lorsque la fenêtre de contrôle de compte d'utilisateur apparaît.

Dans la fenêtre **Administrateur : Windows PowerShell** saisissez la commande suivante :

```
wbadmin start backup -backuptarget:D: -include:C: -vsscopy
```

```
PS C:\Users\ybard> wbadmin start backup -backuptarget:D: -include:C: -vsscopy
wbadmin 1.0 - Outil en ligne de commande de sauvegarde
(C) Copyright Microsoft Corporation. Tous droits réservés.

Récupération des informations de volume...
Cette opération va sauvegarder (C:) sur D:.
Voulez-vous démarrer l'opération de sauvegarde ?
[O] Oui [N] Non o

Remarque : la liste des volumes inclus pour la sauvegarde n'englobe pas tous
les volumes qui contiennent des composants du système d'exploitation. Cette
sauvegarde ne peut pas être utilisée pour effectuer une récupération du
système. Vous pouvez toutefois récupérer d'autres éléments si le type du média de dest
ination prend en charge cette opération.

L'opération de sauvegarde sur D: démarre.
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'une sauvegarde du volume (C:) en cours, (0%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (0%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (1%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (2%) copiés.
```

Un dossier nommé WindowsImageBackup est créé sur le volume de destination de la sauvegarde.

À tout moment, vous pouvez arrêter une opération de sauvegarde en cours d'exécution : wbadmin stop job.

Pour obtenir un état des opérations en cours : wbadmin get status.

Visualiser les sauvegardes disponibles s'effectue à l'aide de la commande get versions : wbadmin get versions.

Dans les grands réseaux d'entreprise, il peut être intéressant d'investir dans une solution telle que DPM (*Microsoft System Center Data Protection Manager*), qui permet de centraliser dans une console la gestion des sauvegardes et des restaurations des postes Windows sur disque, bande ou cloud Microsoft Azure.

5. Points de restauration système

L'outil de restauration du système enregistre les modifications apportées au système Windows puis propose de le restaurer à un état antérieur grâce aux points de restauration. Plus rapide qu'une restauration complète, cette méthode ne sauvegarde pas les données personnelles de l'utilisateur (documents, images...). En effet, les points de restauration système sauvegardent uniquement le registre, certains fichiers utilisés par Windows 11 et les programmes.

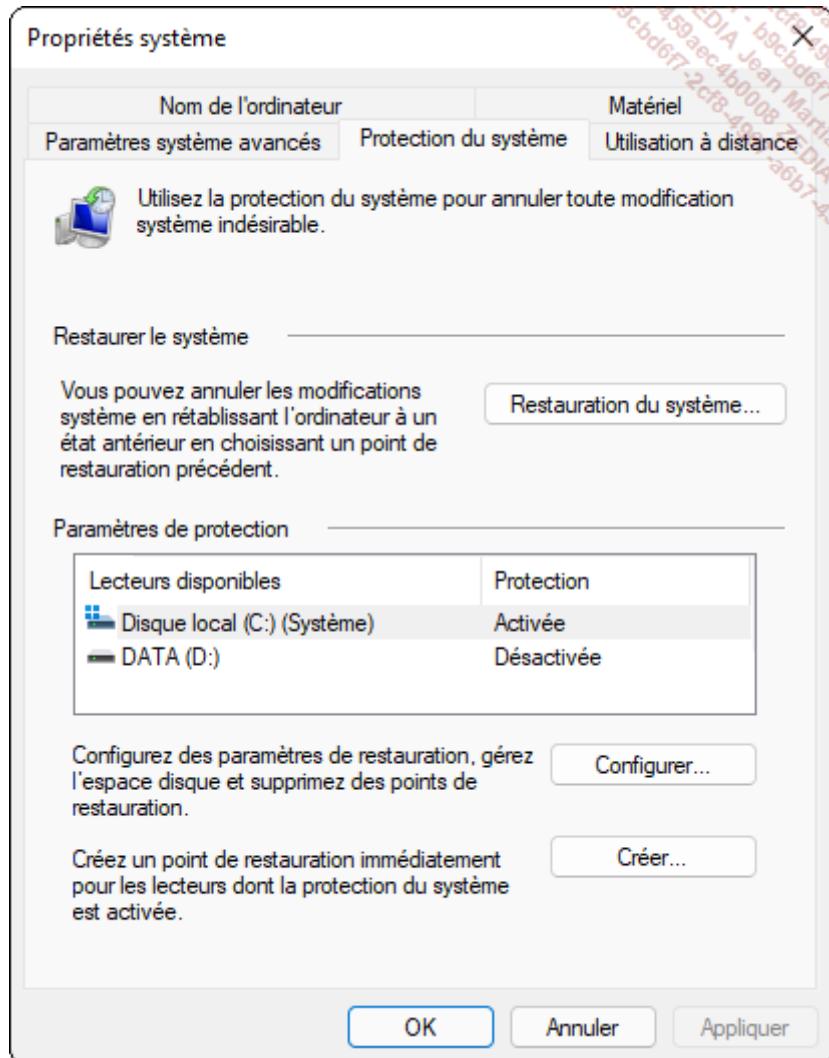
Une fois par jour et à chaque événement important survenu sur le client Windows 11, comme l'installation d'un pilote de périphérique ou la désinstallation d'un logiciel, un point de restauration est créé. Néanmoins, l'utilisateur peut à tout moment en créer un manuellement.

Avant d'exécuter la restauration du système, fermez tous les programmes et documents, car Windows 11 redémarrera l'ordinateur. Notez qu'il est possible d'annuler les modifications effectuées par une restauration du système, sauf si l'utilisateur a effectué cette procédure en mode sans échec. De plus, les points de restauration créés sont conservés jusqu'à ce que la limite qui leur est allouée soit atteinte : dans ce cas, ils seront supprimés pour permettre aux plus récents d'être générés.

Par défaut, Windows 11 n'active pas la fonctionnalité sur la partition où il est installé.

Pour configurer la protection du système, ouvrez une session en tant qu'administrateur local et suivez la procédure suivante :

Cliquez sur le menu **Démarrer**, allez sur **Paramètres, Système** et **Informations système**. Cliquez sur le lien **Protection du système**.



Dans les paramètres de protection, sélectionnez le lecteur sur lequel vous souhaitez activer la création des points de restauration, puis cliquez sur le bouton **Configurer**. Cochez la case **Activer la protection du système** puis choisissez la quantité d'espace disque allouée à la protection du système. Validez par le bouton **OK**.

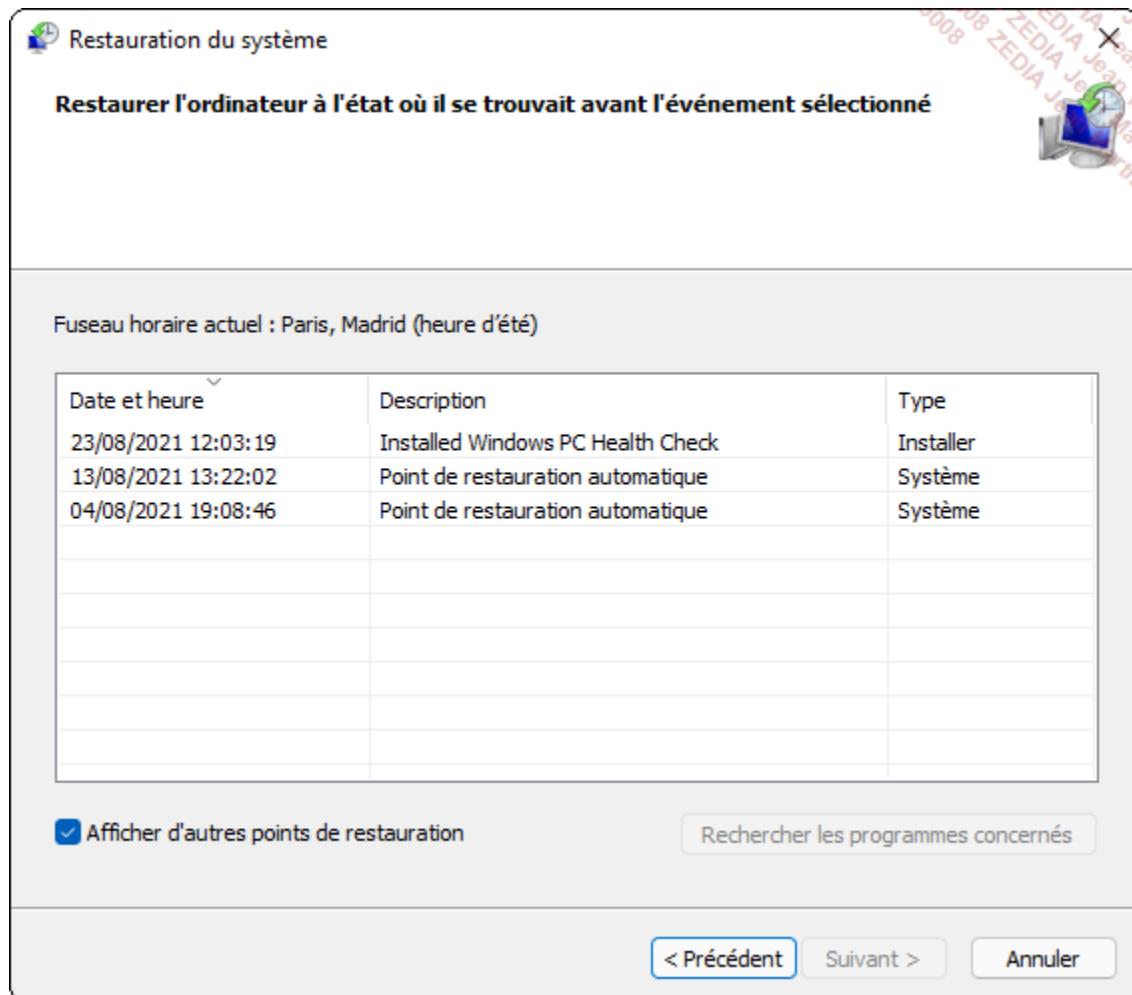
Pour revenir à un point de restauration, procédez comme suit :

Cliquez sur le menu **Démarrer**, allez sur **Paramètres, Système** et **Informations système**. Cliquez sur le lien **Protection du système**.

Cliquez sur le bouton **Restauration du système** pour restaurer le système à une date précise.

- L'option **Restauration recommandée** restaure le système dans l'état où il était avant l'installation la plus récente. Choisir un autre point de restauration permet de sélectionner une autre date.

Cliquez sur le bouton **Suivant** et sélectionnez le point de restauration souhaité en fonction de la date ou du libellé :



En cliquant sur **Rechercher les programmes concernés**, la liste des programmes qui seront supprimés ou restaurés suite à l'activation du point de restauration est affichée.

Cliquez sur le bouton **Terminer**. Le processus de restauration nécessite de redémarrer la machine. Prenez soin d'enregistrer votre travail avant de lancer cette tâche.

La fonctionnalité Restauration du système ne fonctionne que sur une partition NTFS. Le système de fichiers FAT n'est pas supporté.

Les fonctionnalités de restauration sont également disponibles depuis le Panneau de configuration - Récupération.

Résumé du chapitre

- Windows 11 offre différentes fonctionnalités permettant de sauvegarder votre système, mais également de le restaurer à un état antérieur en cas de problème.
- La fonctionnalité Réinitialiser ce PC supprime les partitions en sauvegardant les données, puis installe une nouvelle copie de Windows 11.
- Microsoft a développé la fonctionnalité Historique des fichiers : chaque heure, les fichiers modifiés sont copiés à un emplacement externe déterminé, créant ainsi un historique des différentes versions, tout ceci en arrière-plan et sans intervention de l'utilisateur.
- Grâce à la fonctionnalité Sauvegarder et restaurer (Windows 7), l'administrateur peut créer une sauvegarde de plusieurs volumes.
- L'outil de restauration du système enregistre les modifications apportées au système Windows puis propose de les restaurer à un état antérieur grâce aux points de restauration système.
- La commande BCDEDIT configure les magasins BCD pour faciliter le démarrage de Windows 11 ou d'un autre système d'exploitation, tandis que BCDBOOT configure la partition système.
- Des fonctionnalités de récupération sont implémentées dans Windows 11, grâce au système d'exploitation minimal Windows RE.
- Le Gestionnaire des tâches affiche désormais l'historique d'utilisation des logiciels. Une fonctionnalité intéressante est l'action Recherche en ligne : l'administrateur peut rechercher sur Internet des informations sur un processus, un service, ou une application.
- Windows 11 peut récupérer les journaux d'événements d'autres ordinateurs Windows en tant que collecteur.
- Le Moniteur de fiabilité est un indicateur de la stabilité du système dans le temps pourvu d'une échelle de 1 à 10.
- L'Analyseur de performances est l'outil référent pour étudier l'impact d'un programme ou du matériel sur les ressources du système, que ce soit en temps réel ou grâce à un récapitulatif historique.
- Enfin, l'Enregistreur d'actions utilisateur permet, lorsqu'un utilisateur est confronté à un problème sur sa session, d'enregistrer les actions effectuées dans un fichier au format ZIP, et d'annoter par des commentaires le résultat produit, pour transmission au support.