Sécuriser les postes clients Windows 11 d'un domaine AD avec les GPO et AppLocker

Création automatisée de VM avec Vagrant, sécurisation de postes de travail sous Windows 11 via les GPO et AppLocker

Référence : TP-WINDOWS-CLIENT-2220

Auteur :

Nicolas

Destinataires :

Formateurs

Apprenants

Date de dernière modification : 05/01/23

Version : 1.0

1 Introduction

Dans ces travaux pratiques vous allez tout d'abord voir comment déployer une machine virtuelle Windows sous VMware Workstation automatiquement avec l'outil Vagrant.

Vous apprendrez ensuite comment sécuriser les postes clients Windows d'un domaine Active Directory en respectant les *best-practices* recommandées par Microsoft à l'aide d'outils natifs tels que les GPO et AppLocker.

Une approche dans la lutte contre les virus et les logiciels malveillants consiste à mettre sur liste blanche les logiciels considérés comme sûrs à exécuter et de bloquer tous les autres.

C'est exactement ce que AppLocker vous permettra de faire dans ces travaux pratiques.

Ce TP a été en partie basé sur des ressources non publiques, en cas de difficulté vous pouvez vous renseigner sur des tutoriels similaires[1] sur internet.

1.1 Consigne

Vous serez invités à réaliser des exercices pratiques tout au long de ce document.

Si vous êtes un ou une stagiaire en formation et que votre organisme de formation demande au formateur de vous évaluer vous devrez lui prouver que vous avez bien participé aux exercices. Dans ce but, vous devrez effectuer des captures d'écran démontrant votre investissement.

Vous devrez envoyer vos captures **en fin de module** par mail à l'adresse que vous recevrez ou, si vous savez le faire, via un lien de partage *cloud* (OneDrive, Google Drive, etc.) **en respectant bien les consignes suivantes** sous peine de pénalités :

- Il faudra coller vos captures dans un document texte (.doc, .docx) que vous enverrez au formateur. Cette solution est celle qui est recommandée car cela vous permettra de revenir à votre document plus tard quand vous aurez besoin de vous souvenir de ce que vous avez appris.

- Vous pouvez aussi choisir de ne pas faire de document, dans ce cas il faudra :
    - renommer chaque image (.png, .jpg) de capture d'écran obtenue par votre prénom ou vos initiales suivi d'un numéro, par ex. « **prénom01** » ou « **pn02** »

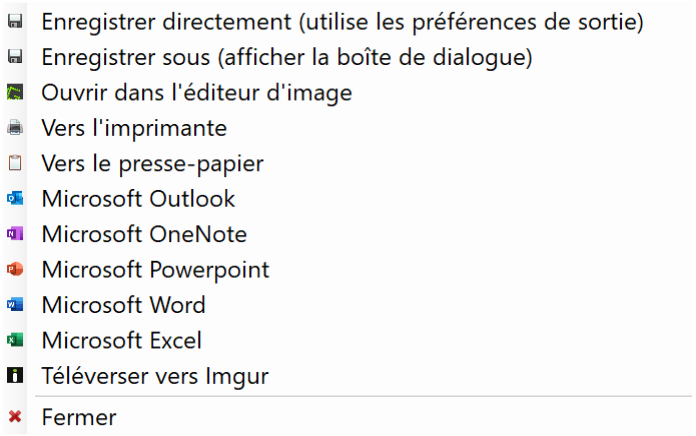
[1] https://www.it-connect.fr/gpo-comment-configurer-applocker-pour-securiser-vos-postes-windows/ ; https://rdr-it.com/applocker-configuration-environnement-active-directory/ ; https://www.youtube.com/watch?v=vOTTZpb0mjY ; https://www.malekal.com/windows-applocker-bloquer-les-executables-et-scripts/ ; https://blog.netwrix.fr/2020/08/25/6-parametres-de-strategie-de-groupe-que-vous-devez-configurer-correctement/

- envoyer vos captures au formateur **en une seule fois** dans une archive (.zip, .rar, .7zip) **renommée avec votre prénom** et **contenant toutes vos captures** (= ne pas envoyer les captures une à une dans un mail)

Merci de respecter ces consignes cela permettra à votre formateur de gérer plus efficacement la partie correction et notation.

L'outil Greenshot : https://getgreenshot.org/downloads/

Je vous conseille d'utiliser Greenshot (un logiciel libre & open source) pour les prises de capture d'écran (il est plus pratique que « Outil capture d'écran » de Windows). Une fois installé et lancé en arrière-plan, utilisez la touche « *Impr écran* » de votre clavier pour prendre une capture d'écran rapide puis choisissez « Enregistrer directement » pour qu'elle arrive immédiatement sur votre bureau ou « Enregistrer sous » pour la renommer avant de l'enregistrer où vous voulez. Il propose aussi d'autres actions rapides comme envoyer la capture directement dans un éditeur d'image (pour faire des cadres, des flèches, du floutage, de la numérotation) ou dans le presse-papier (pour pouvoir coller la capture d'écran dans un document sans avoir besoin de l'enregistrer en tant que fichier au préalable) :



2 Mise en place des prérequis

Pour la réalisation de ce TP j'ai utilisé un ordinateur physique sous Windows 10 Education. J'y ai installé l'hyperviseur VMware Workstation 17 Pro avec lequel j'ai virtualisé une

machine sous Windows Server 2022 Standard et une autre sous Windows 11 Entreprise. J'ai aussi utilisé PowerShell 7 et Vagrant 2.3.4 pour automatiser la création de machine virtuelle.

2.1 Avoir une machine virtuelle Windows 11 Entreprise

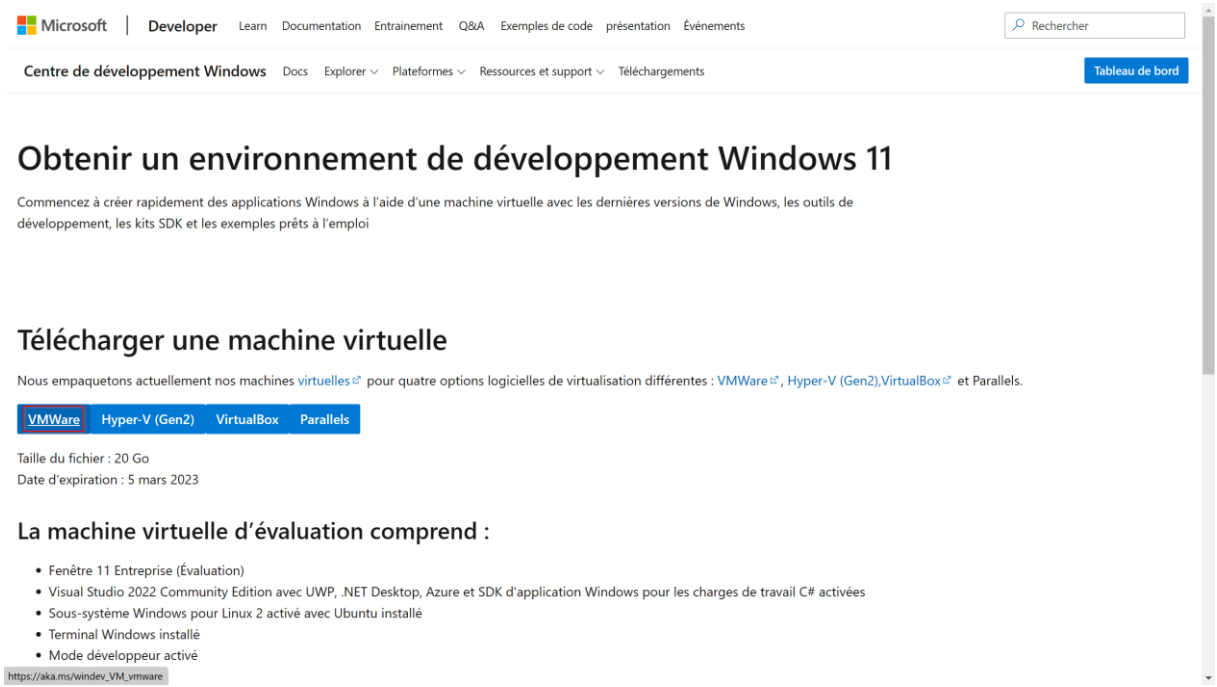
Vous devez avoir la version **Entreprise** ou **Education** de Windows 11 ou 10 pour utiliser AppLocker.

2.1.1 Première option : installer manuellement

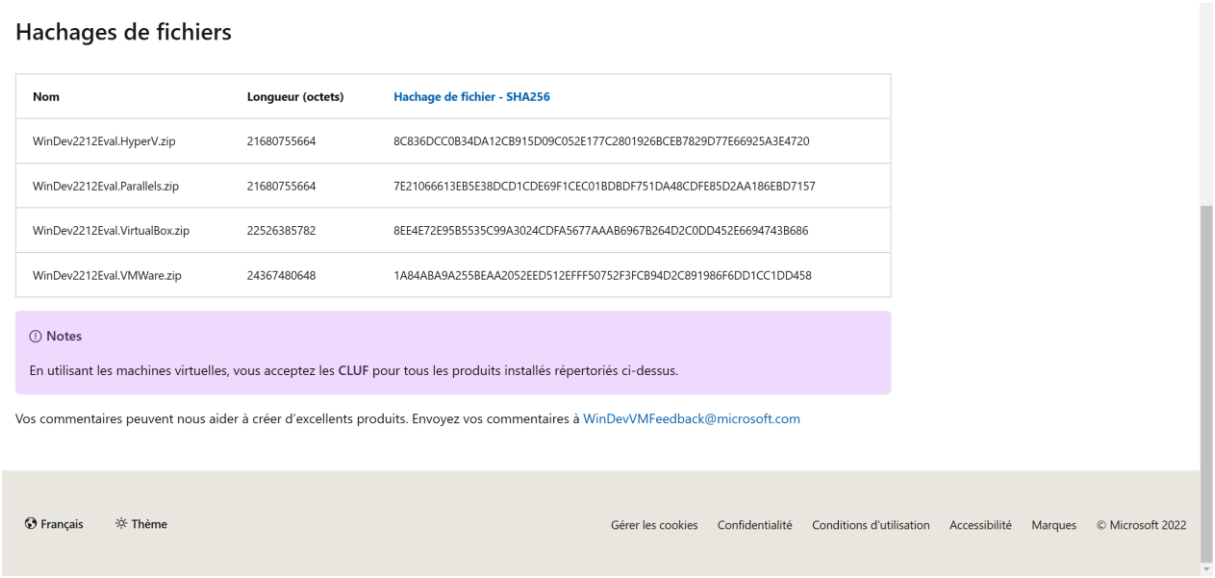
Vous pouvez le faire manuellement comme vous êtes habitué à le faire. Cette méthode « classique » ne sera pas expliquée dans ce document.

2.1.2 Deuxième option : télécharger une VM toute prête

Pour vous éviter d'installer manuellement une machine virtuelle, sachez qu'il est possible d'en récupérer une prête-à-l 'emploi, sous Windows 11 Entreprise, de manière officielle et gratuitement sur le site de Microsoft depuis ce lien : https://developer.microsoft.com/fr-fr/windows/downloads/virtual-machines/ [2]



[2] Si le lien ne fonctionne plus à l'heure où vous lisez ces lignes, n'hésitez pas à demander à votre formateur qui peut vous fournir une copie du fichier original (environ 23 Go).



Hachages de fichiers

Nom	Longueur (octets)	Hachage de fichier - SHA256
WinDev2212Eval.HyperV.zip	21680755664	8C836DCC0B34DA12CB915D09C052E177C2801926BCEB7829D77E66925A3E4720
WinDev2212Eval.Parallels.zip	21680755664	7E21066613EB5E38DCD1CDE69F1CEC01BDBDF751DA48CDFE85D2AA186EBD7157
WinDev2212Eval.VirtualBox.zip	22526385782	8EE4E72E95B5535C99A3024CDFA5677AAAB6967B264D2C0DD452E6694743B686
WinDev2212Eval.VMWare.zip	24367480648	1A84ABA9A255BEAA2052EED512EFFF50752F3FCB94D2C891986F6DD1CC1DD458

Notes

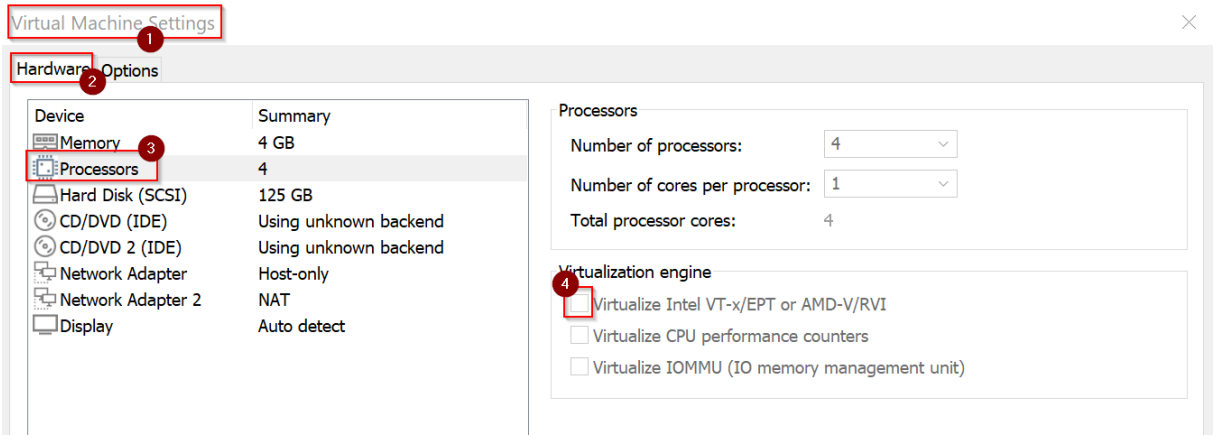
En utilisant les machines virtuelles, vous acceptez les CLUF pour tous les produits installés répertoriés ci-dessus.

Vos commentaires peuvent nous aider à créer d'excellents produits. Envoyez vos commentaires à WinDevVMFeedback@microsoft.com

Français Thème Gérer les cookies Confidentialité Conditions d'utilisation Accessibilité Marques © Microsoft 2022

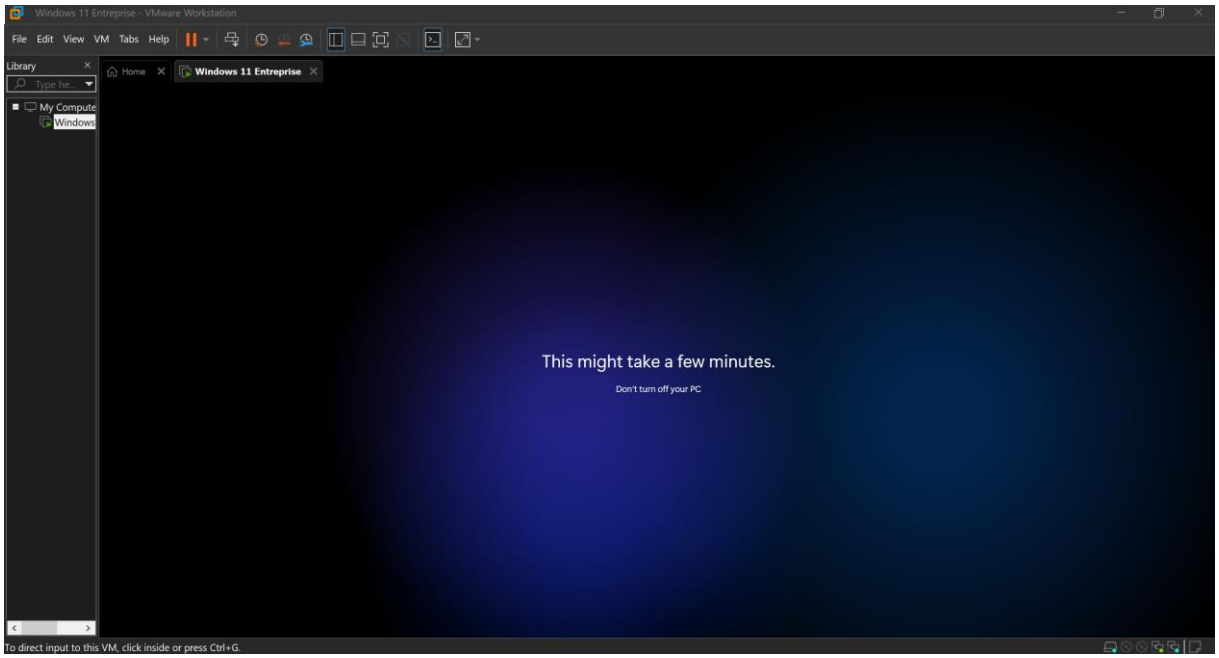
Téléchargez la version pour VMware et ensuite il vous suffira juste de l'importer dans VMware Workstation en pointant sur le fichier « .ovf ».

Démarrez ensuite votre VM. Si vous avez un message d'erreur bloquant au lancement de la VM, désactivez « Virtualize Intel VT-x/EPT or AMD-V/RVI » dans les paramètres de la VM :

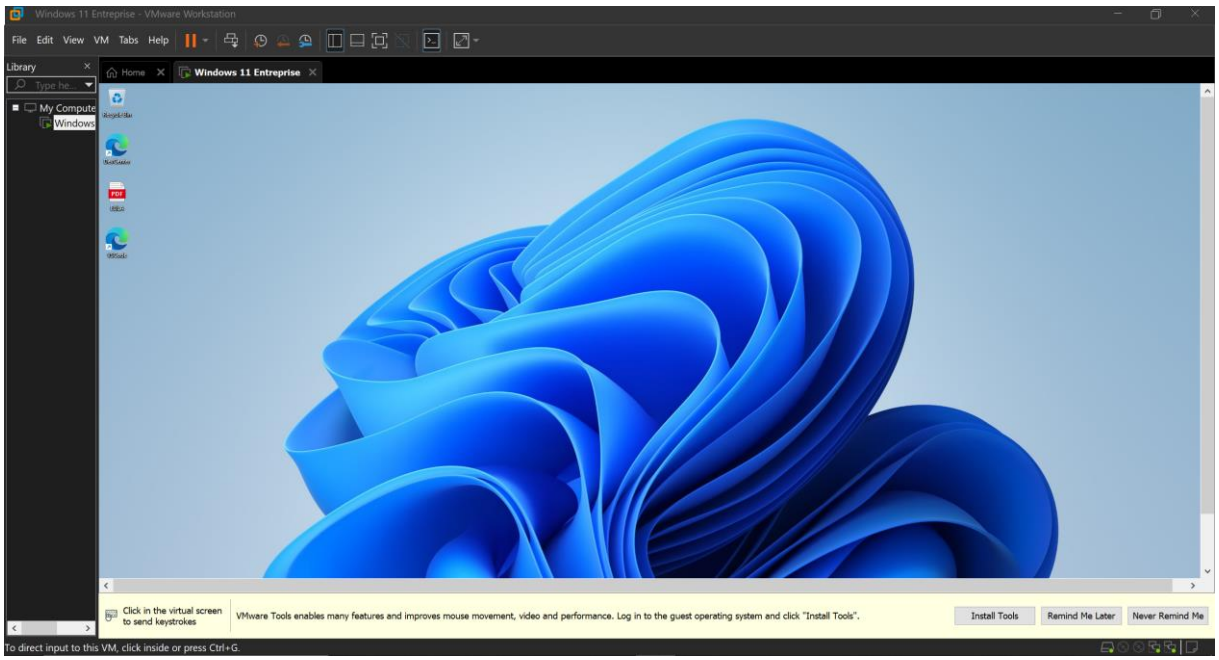


Vous pouvez constater au passage qu'elle est configurée par défaut avec 4 Go de RAM, 4 vCPU, 125 Go de stockage, une NIC dans votre réseau virtuel Host-Only (vmnet1) et une autre dans le réseau NAT (vmnet8). Vous pouvez laisser cette configuration.

Après avoir décoché la case vous pourrez démarrer votre VM avec succès et elle prendra quelques minutes à se configurer :



Puis vous arriverez sur le bureau Windows 11 :

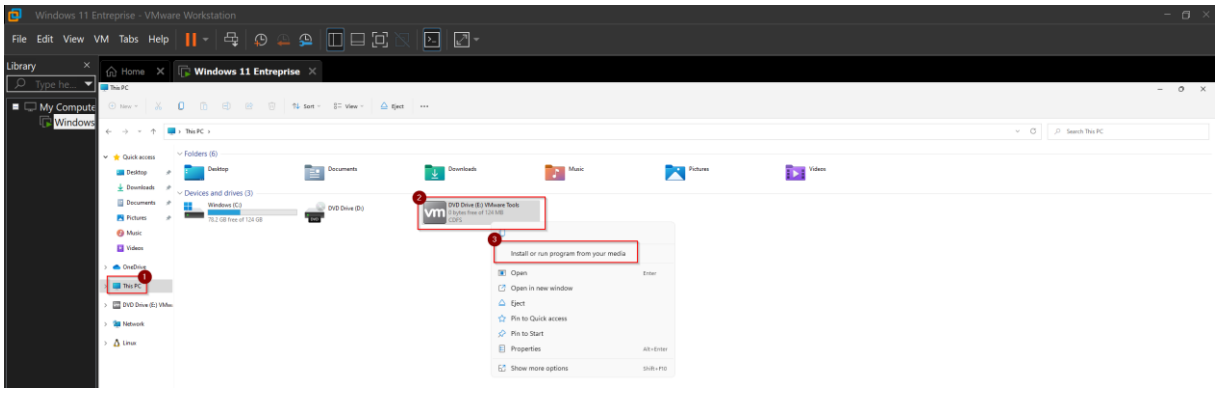


2.1.3 Configurer votre VM client

L'utilisateur local « User » est créé par défaut, il a tous les droits d'administration et il n'a pas de mot de passe.

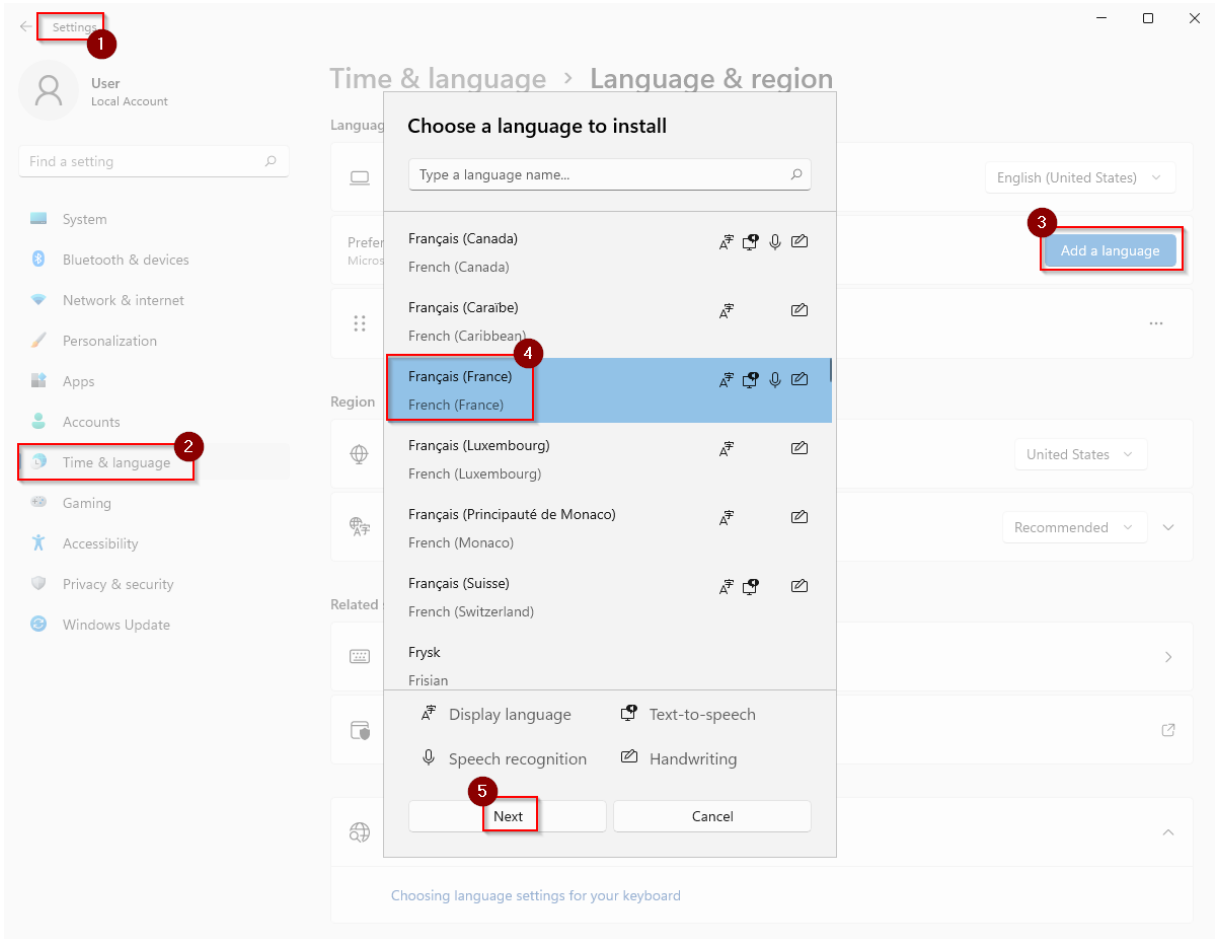
Installer les VMware Tools (facultatif)

Vous pouvez installer les VMware Tools si vous souhaitez de meilleures performances et une plus grande facilité d'utilisation. Pour cela cliquez sur le bouton « Install Tools » sur le bandeau jaune en bas de l'écran et ensuite rendez-vous dans l'Explorateur Windows et suivez les étapes illustrées ci-dessous :



Activer la langue française (facultatif)

Vous pouvez aussi activer la langue française dans les paramètres en suivant les étapes illustrées ci-dessous :

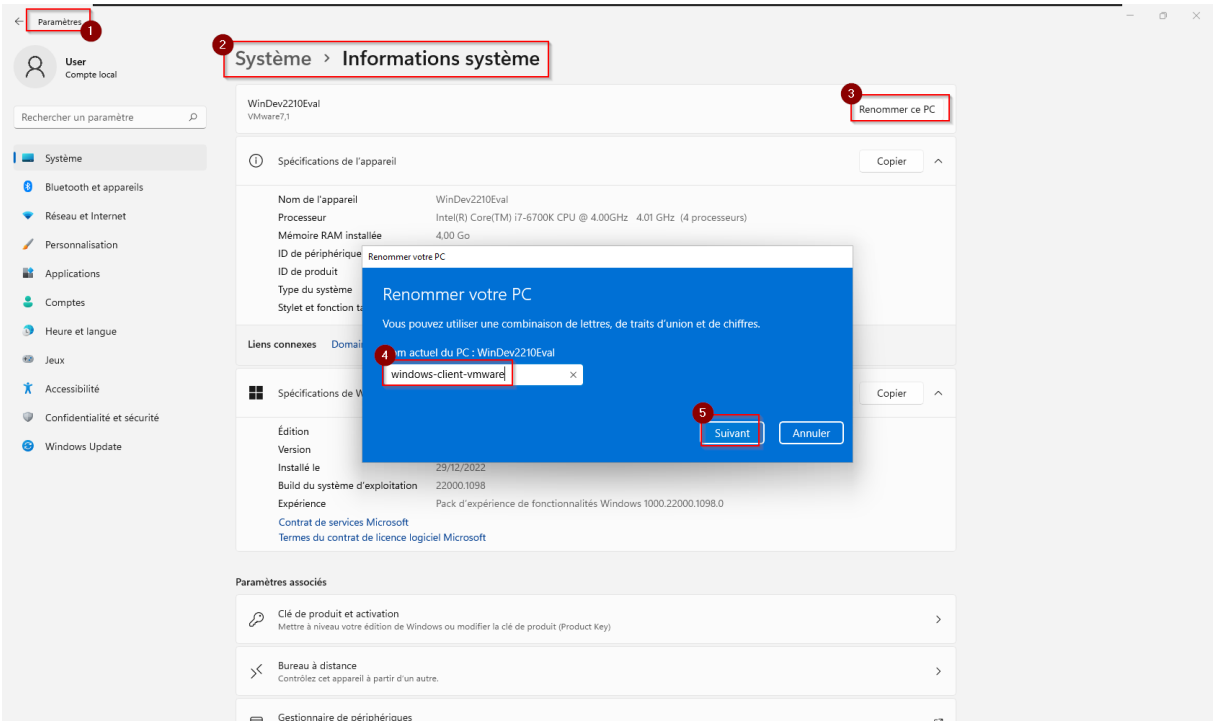


Vous devrez vous déconnecter de votre session pour que le changement de langue soit pris en compte.

Pour vous reconnecter, utilisez le compte par défaut « User » qui n'a pas de mot de passe.

Changer le nom de la machine (facultatif)

Vous pouvez aussi changer le nom d'hôte par défaut « WinDev2210Eval » pour qu'il réponde aux critères de votre convention de nommage des machines, moi j'ai choisi de la renommer en « windows-client-vmware » mais en production ne dépassez jamais les 15 caractères pour éviter des problèmes[3] :



Configurer les paramètres réseau

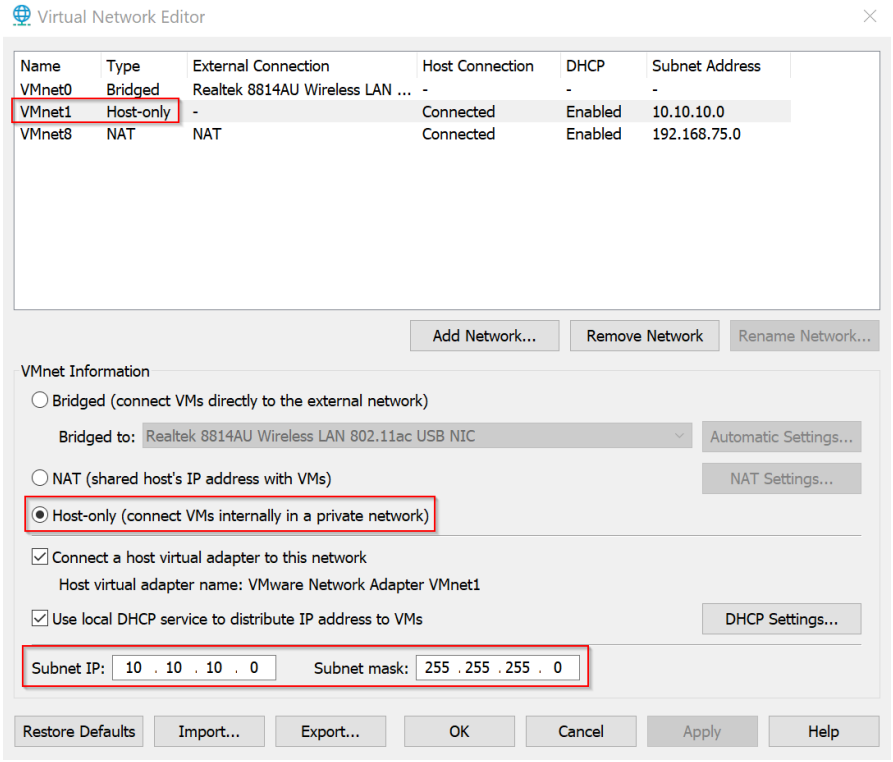
Concernant la configuration réseau, j'ai laissé les interfaces Ethernet1 (qui est dans le réseau NAT) et Ethernet0 (qui est dans le réseau Host-only) en configuration automatique par le protocole DHCP.

[3] Certains logiciels ne prennent en compte que les 15 premiers caractères des noms de machine ce qui provoque des conflits puisque certaines machines auront le même nom. Cela arrive par exemple dans une arborescence Active Directory comme nous le verrons un peu plus bas ou dans l'interface d'un serveur GLPI (service qui permet entre autres d'inventorier les différentes machines d'un parc informatique).

Cependant pour pouvoir par la suite joindre cette machine cliente Windows 11 à votre futur domaine Active Directory, vous devrez ajouter en « Serveur DNS préféré » l'adresse IP de l'interface LAN du contrôleur de domaine que vous allez créer juste après.

Autant le faire tout de suite.

Pour cela allez dans le « Virtual Network Editor » de votre hyperviseur VMware Workstation et affichez ou modifiez à votre convenance le réseau Host-only que vous allez utiliser dans ce TP (par exemple le « vmnet1 »). Ce réseau sera votre réseau local (LAN).

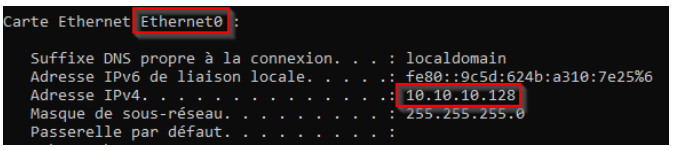


Dans ce LAN, choisissez une adresse IP pour l'interface LAN de votre futur serveur DNS/contrôleur de domaine. Par exemple : 10.10.10.130

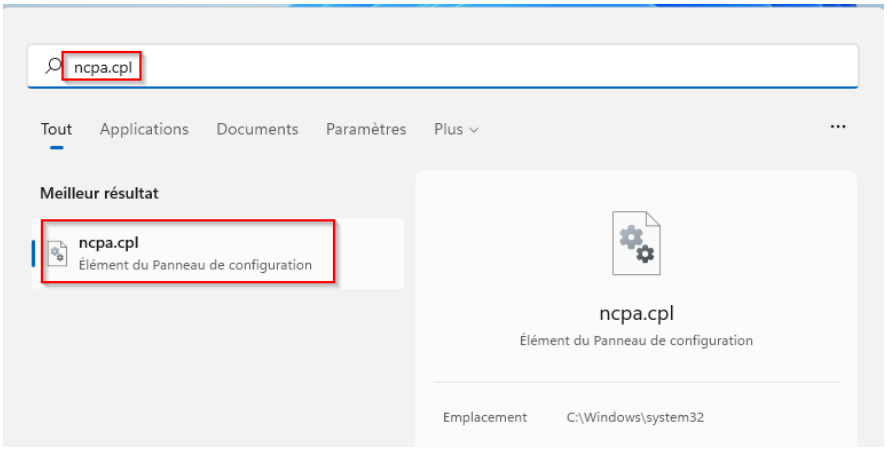
Identifiez le nom de l'interface réseau de votre Windows 11 qui est dans le réseau Host-only que vous avez choisi avec la commande :

```
ipconfig
```

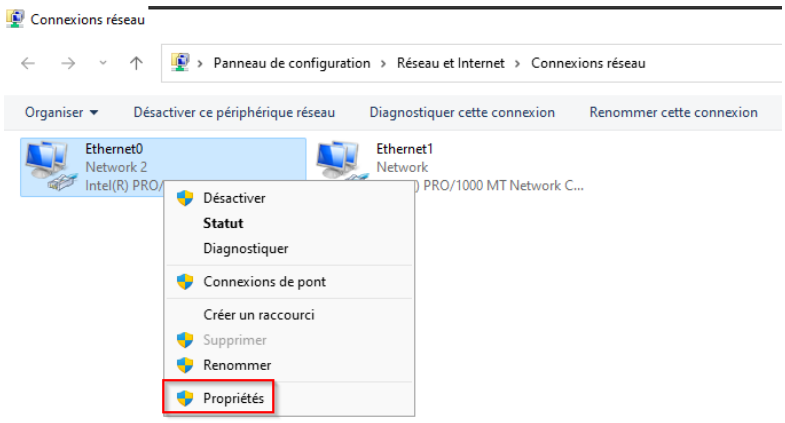
Vous devriez obtenir une sortie similaire à celle-ci :



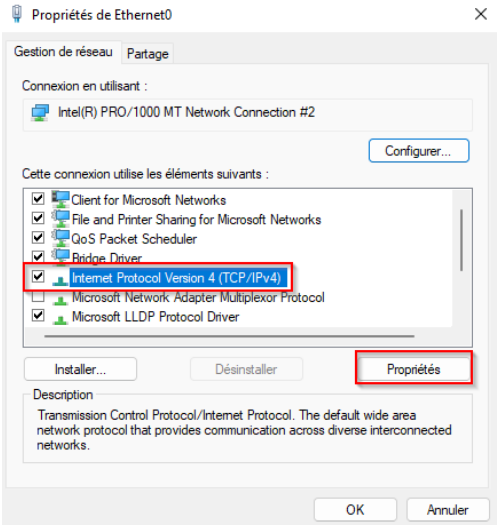
Ensuite tapez dans la barre de recherche Windows « ncpa.cpl » pour afficher le menu des « Connexions réseau » :

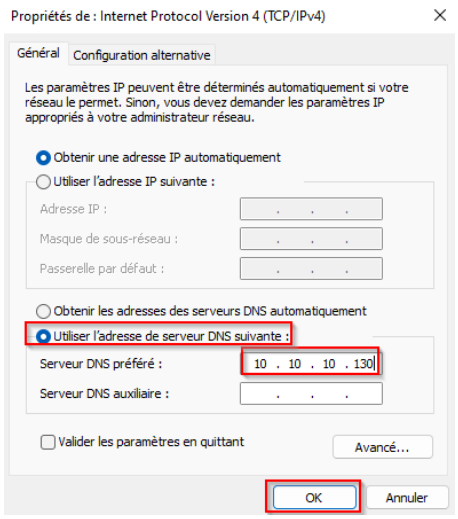


Faites un clic droit sur la bonne NIC (Network Interface Card), puis cliquez sur ses « Propriétés » :



Modifiez ses paramètres IPv4 en ajoutant l'adresse IP de votre futur serveur :

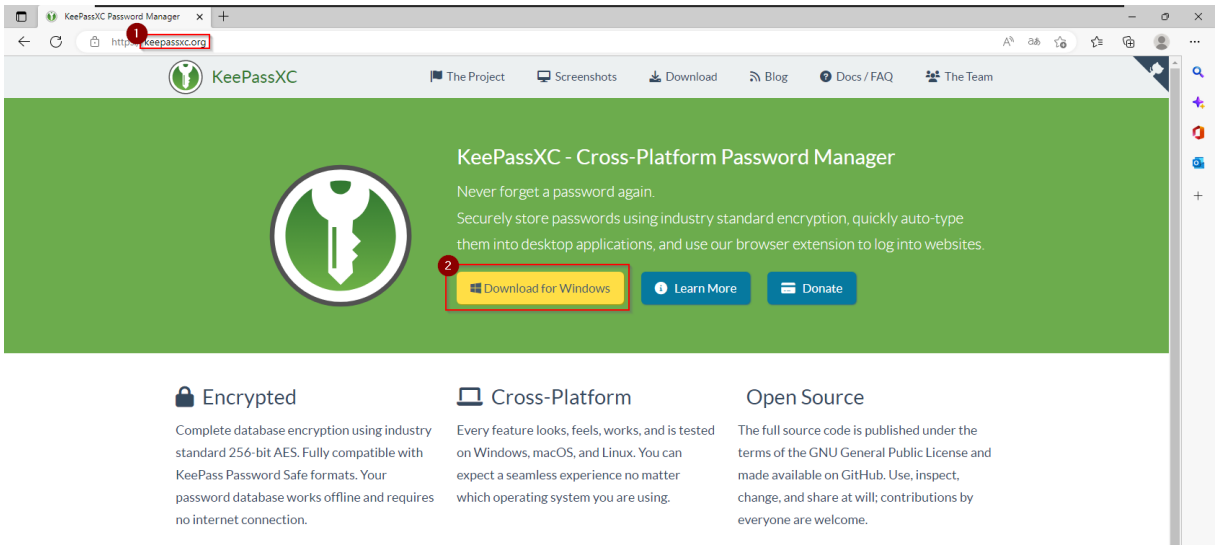


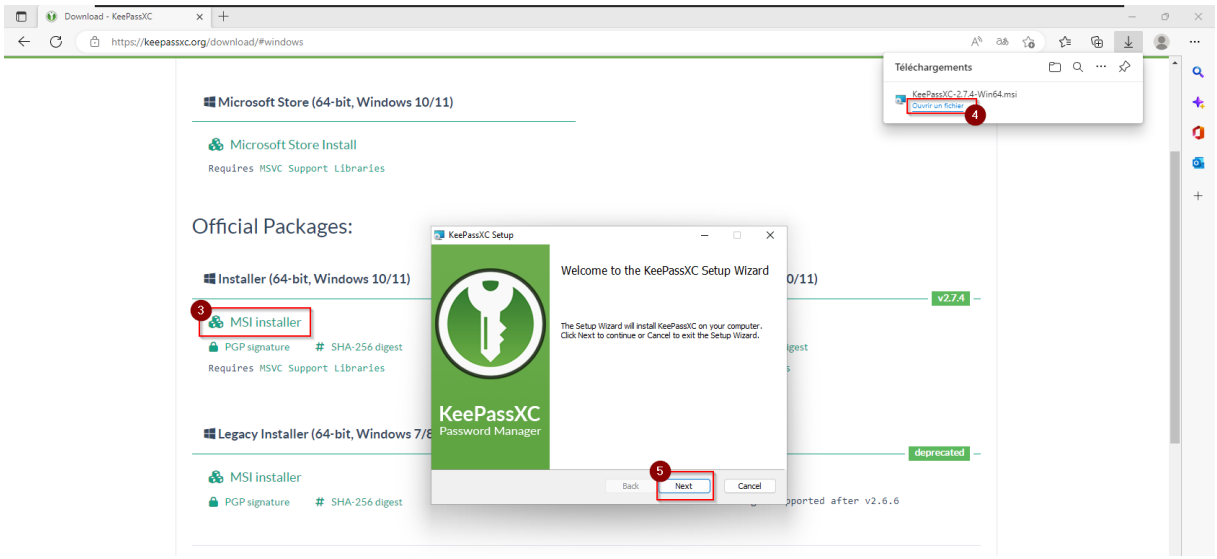


Voilà une bonne chose de faite. Passons à la création du serveur maintenant.

Télécharger et installer KeePassXC

Dans la suite de ce TP vous allez avoir besoin d'un programme tiers afin d'y appliquer des règles. Téléchargez et installez le gestionnaire de mots de passe KeePassXC sur « keepassxc.org » en suivant les étapes illustrées ci-dessous puis celles de l'assistant d'installation :





2.2 Avoir une machine virtuelle Windows Server 2022

Vous allez devoir installer une machine virtuelle Windows Server 2022 avec VMware Workstation.

2.2.1 Première option : installer manuellement

Vous pouvez le faire manuellement comme vous êtes habitué à le faire. Cette méthode « classique » ne sera pas expliquée dans ce document.

2.2.2 Deuxième option : automatiser le déploiement

Vous pouvez aussi automatiser cette tâche avec Vagrant. Si vous ne connaissez pas encore cet outil, c'est l'occasion d'apprendre à l'utiliser.

Vagrant est un outil de HashiCorp qui permet de déployer une ou plusieurs machines virtuelles automatiquement. Savoir le maîtriser vous fera gagner beaucoup de temps au cours de vos études.

Installation de Vagrant et de ses prérequis

Vous allez utiliser l'hyperviseur VMware Workstation pour virtualiser les machines dans ce TP, pour automatiser le déploiement il vous faut donc installer tous ces prérequis en plus de VMware Workstation :

1) Vagrant, que vous pouvez télécharger gratuitement ici : https://developer.hashicorp.com/vagrant/downloads

2) Vagrant VMware Utility, que vous pouvez télécharger gratuitement ici : https://developer.hashicorp.com/vagrant/downloads/vmware
3) le module Vagrant pour VMware en exécutant la commande Powershell suivante :

```
vagrant plugin install vagrant-vmware-desktop
```

Préparation du fichier de déploiement

Une fois ces prérequis installés[4] vous allez devoir préparer votre déploiement en éditant un fichier de configuration « Vagrantfile ». Il ne devra pas être renommé autrement et ne comportera pas d'extension (attention donc à l'extension « .txt » d'un document texte qui n'est pas affichée par défaut sous Windows).

Vous pouvez éditer le Vagrantfile avec le « Bloc-notes » natif de Windows ou n'importe quel autre éditeur de texte comme NotePad++ par exemple.

La VM que vous allez déployer sera créée dans un dossier « .vagrant\machines\ » qui sera lui-même créé à l'emplacement où vous placerez votre fichier Vagrantfile.

Choisissez donc votre emplacement dès maintenant pour savoir où seront déployées vos VMs. Moi j'ai choisi de le créer dans : « C:\VMs\ ».

Toute la configuration de Vagrant va se faire ci-dessous[5]. Veuillez la copier-coller dans votre Vagrantfile. Prenez le temps de lire les commentaires pour comprendre ce que fait chaque paramètre. Il en existe d'autres mais sachez que parfois ils ne fonctionneront pas comme ils le devraient et qu'ils peuvent différer selon l'hyperviseur utilisé, le système d'exploitation déployé, etc.

ATTENTION : C'EST DU LANGAGE RUBY DONC LE RESPECT DE L'INDENTATION EST IMPORTANT !

```
# -*- mode: ruby -*-
# vi: set ft=ruby :

Vagrant.configure("2") do |config| # Le "2" dans Vagrant.configure indique la
version de la configuration. Ne le modifiez pas, sauf si vous savez ce que vous
faites.
```

[4] En cas de difficultés pour l'installation, voici un tuto datant de 2021 en anglais décrivant les étapes pour tout installer depuis un système Linux (mais sous Windows c'est encore plus simple) : https://linuxhint.com/vagrant-vmware-workstation-pro-16/

[5] En cas de problème vous pouvez générer un autre Vagrantfile tout propre avec la commande PowerShell « vagrant init » et vous pouvez aussi consulter la documentation officielle ici : https://developer.hashicorp.com/vagrant/docs et plus particulièrement la partie sur VMware ici : https://developer.hashicorp.com/vagrant/docs/providers/vmware


```
  config.vm.box = "dstoliker/winserver2022-max" # Cela va utiliser une box Vagrant de Windows Server 2022 qui fonctionne avec VMware. Pour en trouver d'autres compatibles VMware consultez le catalogue des boxes : https://app.vagrantup.com/boxes/search?provider=vmware (ATTENTION TOUT DE MEME AUX BOXES MALVEILLANTES NON-OFFICIELLES !)

  config.vm.hostname = "windows-server-vmware" # Cela va configurer le nom d'hôte. Il ne faut pas mettre un FQDN pour un système Windows.

  config.vm.base_address = "192.168.75.120" # Cela va faire une réservation DHCP pour l'adresse IP de l'interface NAT sur la machine invité. Adaptez la configuration à votre propre réseau virtuel NAT. Notez que l'adresse configurée doit faire partie de l'étendue DHCP autorisée (voir cela dans le Virtual Network Editor de votre hyperviseur VMware Workstation).

  config.vm.network "private_network", ip: "10.10.10.120", :hostonly => "vmnet1" # Cela va ajouter une NIC dans le réseau host-only spécifié et devrait lui attribuer l'adresse IP spécifiée.

  # La directive config.vm.provider permet de configurer les paramètres spécifiques au fournisseur de VMs (ici VMware Workstation)
  config.vm.provider "vmware_workstation" do |v|

    v.vmx["displayName"] = "Windows Server 2022" # Cela va configurer le nom d'affichage de la machine virtuelle dans VMware Workstation.

    v.vmx["memsize"] = "2048" # Cela va configurer la taille de la RAM de la VM.

    v.vmx["numvcpus"] = "2" # Cela va configurer le nombre de CPU de la VM.

    v.vmx["ethernet0.pcislotnumber"] = "33" # Ceci est un paramètre réseau de la box qui est automatiquement écrasé par Vagrant au démarrage. Dans une prochaine version, Vagrant cessera d'écraser ce paramètre ce qui pourrait empêcher une configuration réseau correcte. Il convient donc de l'appliquer manuellement pour éviter de futurs problèmes avec cette configuration.

    v.gui = true # Cela va afficher l'interface graphique de VMware peu après le processus de création de la machine avec la commande vagrant up. Vous pouvez remplacer true par false pour ne pas l'afficher mais en cas de problème vous ne verrez pas ce qui se passe dans la VM. (La configuration de ce paramètre est obligatoire sinon message d'erreur bloquant)

  end


end
```

Enregistrez votre fichier Vagrantfile.

Déploiement

Vous êtes maintenant prêt à déployer votre VM.

Lancez PowerShell.

Rendez-vous dans le dossier où se trouve le Vagranfile. Utilisez pour cela la commande « cd » (pour « Change Directory ») suivie d'un espace et du chemin d'accès complet vers votre fichier Vagrantfile ; dans mon exemple c'est :

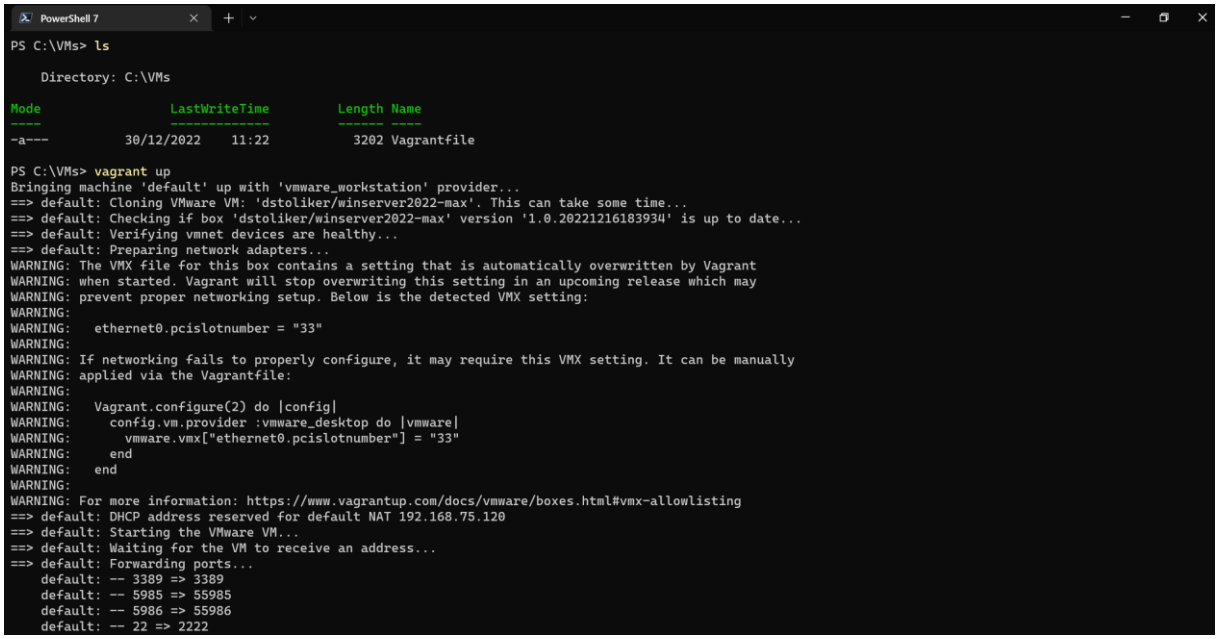
```
cd C:\VMs\
```

Attention, il ne faut pas qu'il y ait d'espace dans le chemin d'accès vers le fichier Vagrantfile sinon la commande « vagrant » ne fonctionnera pas.

Lancez maintenant la commande PowerShell suivante :

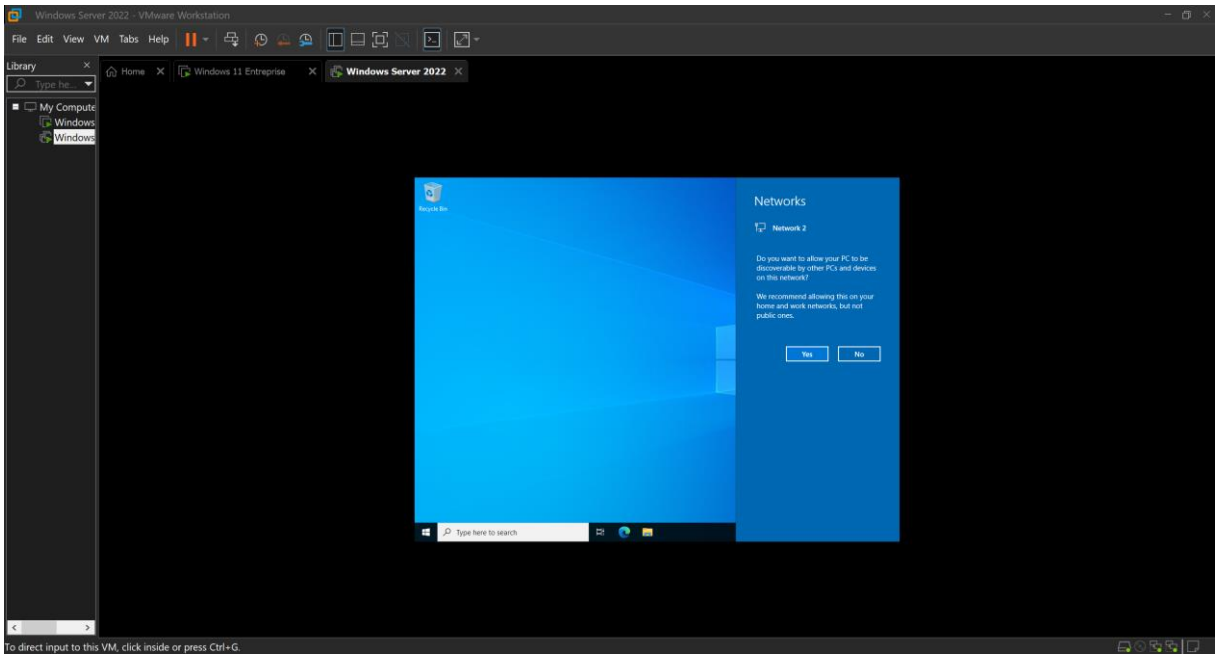
```
vagrant up
```

Attendez ensuite quelques minutes car il faut que Vagrant télécharge la box Windows Server et qu'il déploie la VM donc soyez patients. A la fin vous devriez obtenir une sortie similaire à celle-ci :




```
==> default: Waiting for machine to boot. This may take a few minutes...
    default: WinRM address: 127.0.0.1:55985
    default: WinRM username: vagrant
    default: WinRM execution_time_limit: PT2H
    default: WinRM transport: negotiate
==> default: Machine booted and ready!
==> default: Setting hostname...
==> default: Waiting for machine to reboot...
==> default: Configuring network adapters within the VM...
==> default: Configuring secondary network adapters through VMware
==> default: on Windows is not yet supported. You will need to manually
==> default: configure the network adapter.
==> default: Enabling and configuring shared folders...
    default: -- C:/VMs: /vagrant
PS C:\VMs>
```

Après ces quelques minutes vous arriverez automatiquement sur cet écran avec votre VM toute prête :



2.2.3 Configurer votre VM serveur

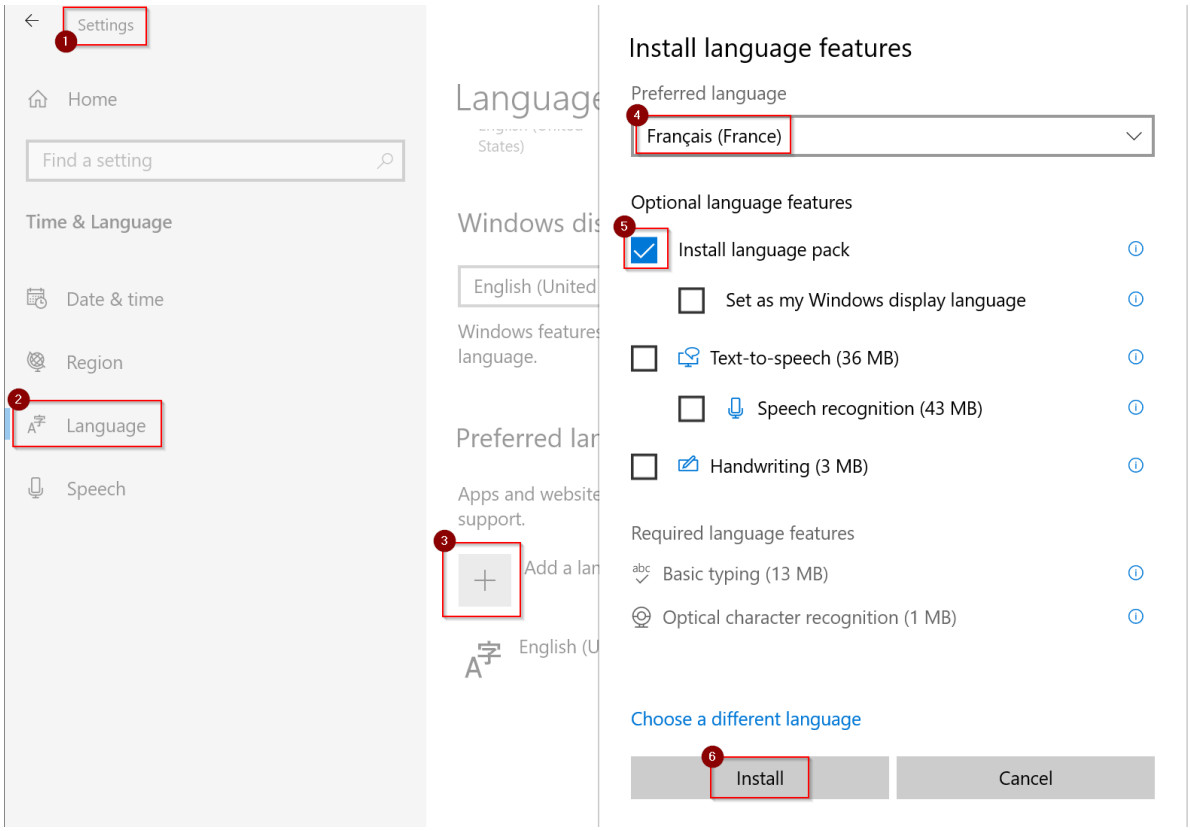
Installer les VMwware Tools (facultatif)

Profitez-en pour installer directement les VMware Tools puis redémarrez.

Pour vous reconnecter, utilisez le compte « Administrator » et le mot de passe « vagrant » qui a été configuré par défaut.

Activer la langue française (facultatif)

Si vous le voulez, mettez le système en français et le clavier en AZERTY en recherchant « Language settings » dans la barre de recherche :



Vous devrez vous déconnecter de votre session pour que le changement de langue soit pris en compte.

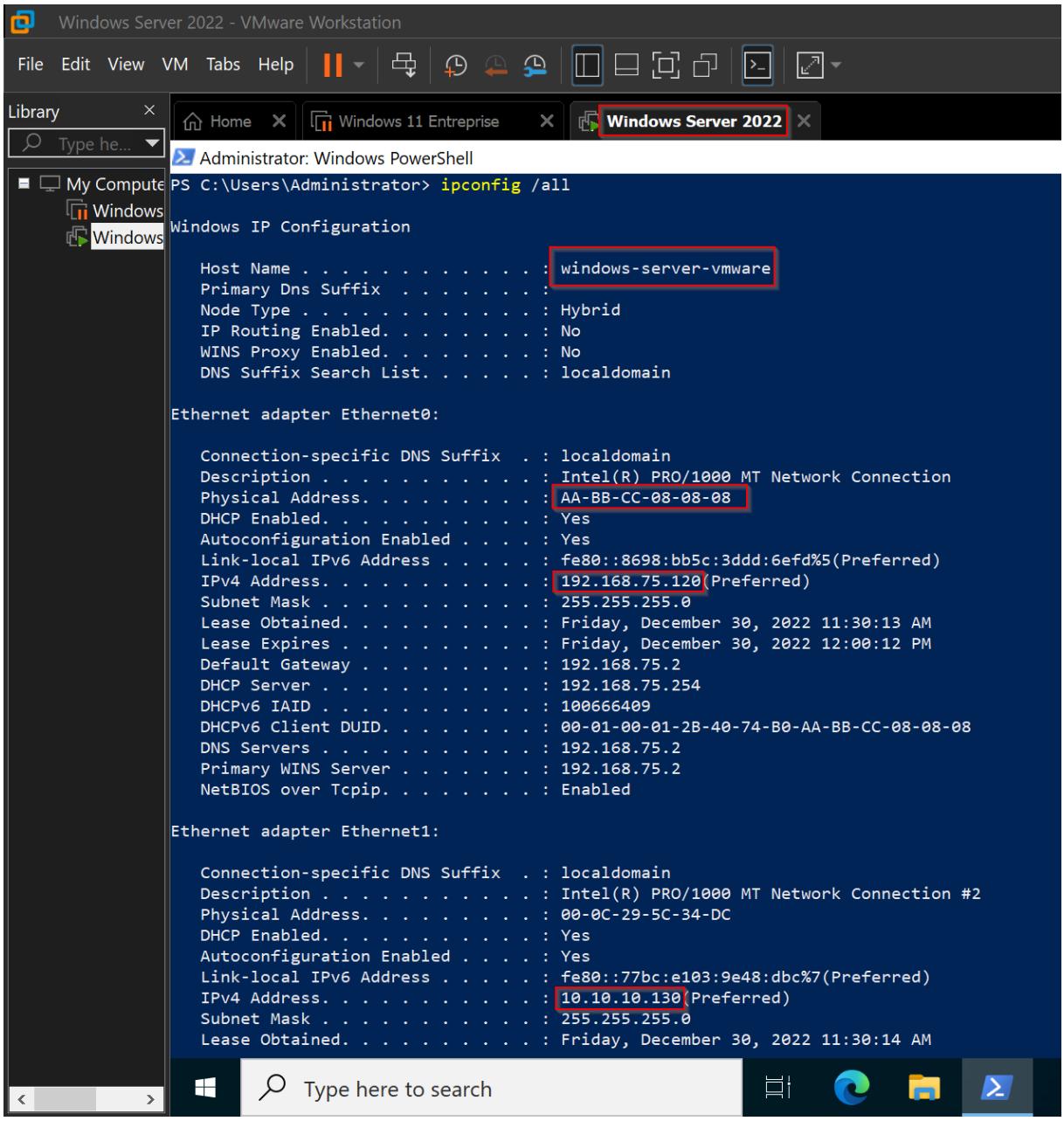
Configurer les paramètres réseau

Une fois revenu, lancez la commande PowerShell suivante pour afficher la configuration réseau[6] :

```
ipconfig /all
```

Vous obtiendrez une sortie similaire à celle-ci :

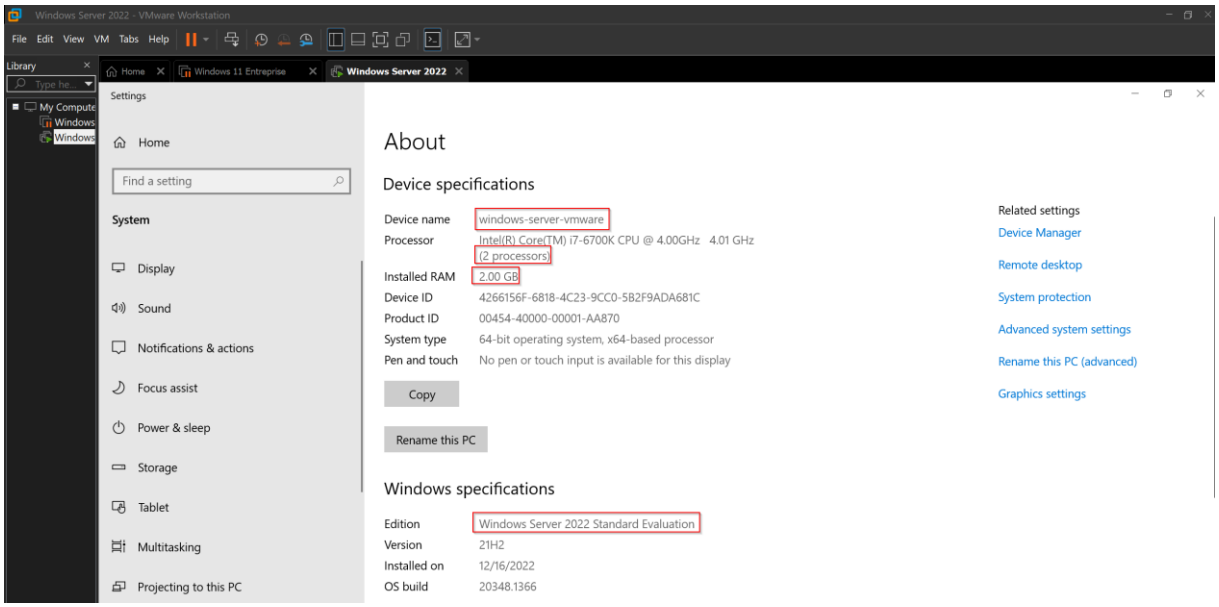
[6] Si vous n'avez pas changé le clavier en QWERTY par défaut, il faut remplacer « / » par « ! » et « a » par « q » sur un clavier AZERTY.



Je constate que le paramètre pour fixer l'IP de l'interface réseau dans le vmnet1 (Host-only) n'a pas complètement fonctionné mais qu'il a au moins créé l'interface réseau. Je fixerai l'IP manuellement dans l'étape suivante.

Je constate aussi que les autres paramètres ont bien été configurés comme le nom d'affichage dans l'interface VMware, le nom d'hôte, l'IP de l'interface réseau dans le vmnet8 (NAT) et son adresse MAC.

Je peux aussi vérifier si les autres paramètres comme la RAM et le nombre de vCPUs ont bien été pris en compte :



C'est bien le cas.

D'autres options de la commande « vagrant » :

Sachez que vous pouvez aussi vous connecter à votre VM en SSH avec la commande « vagrant ssh » (puis vous déconnecter avec « exit ») ou détruire très facilement la VM créée précédemment avec « vagrant destroy ».

2.3 Avoir un contrôleur de domaine

2.3.1 Qu'est-ce qu'un contrôleur de domaine ?

Un **contrôleur de domaine** (**DC**) est **un serveur qui répond aux demandes d'authentification de sécurité au sein d'un domaine de réseau informatique**.

Il est chargé d'autoriser l'accès de l'hôte aux ressources du domaine. Il authentifie les utilisateurs, stocke les informations de compte d'utilisateur et applique la politique de sécurité pour un domaine.

Lorsque l'on crée un domaine, le serveur depuis lequel on effectue cette création est promu au rôle de « contrôleur de domaine » du domaine créé.

Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine. De ce fait, il devra vérifier les identifications des objets, traiter les demandes d'authentification, veiller à l'application des stratégies de groupe ou encore stocker une copie de l'annuaire Active Directory.

Un contrôleur de domaine est indispensable au bon fonctionnement du domaine, si l'on éteint le contrôleur de domaine ou qu'il est corrompu, le domaine devient inutilisable.

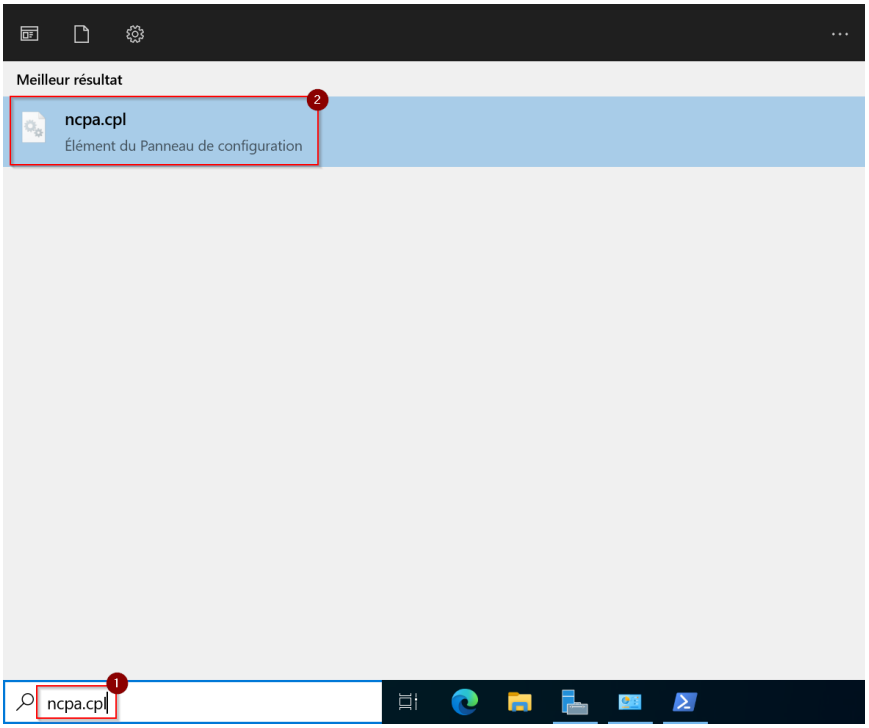
De plus, lorsque vous créez le premier contrôleur de domaine dans votre organisation, vous créez également le premier domaine, la première forêt, ainsi que le premier site.

Le rôle du serveur de contrôleur de domaine est l'un des rôles les plus importants à sécuriser dans n'importe quel environnement d'ordinateurs fonctionnant avec Windows Server et le service d'annuaire Active Directory. Toute atteinte à l'intégrité d'un contrôleur de domaine ou la perte de ce dernier dans ce type d'environnement pourrait entraîner des conséquences graves pour les ordinateurs clients, serveurs et applications s'appuyant sur les contrôleurs de domaine pour l'authentification, la stratégie de groupe et un annuaire LDAP central.

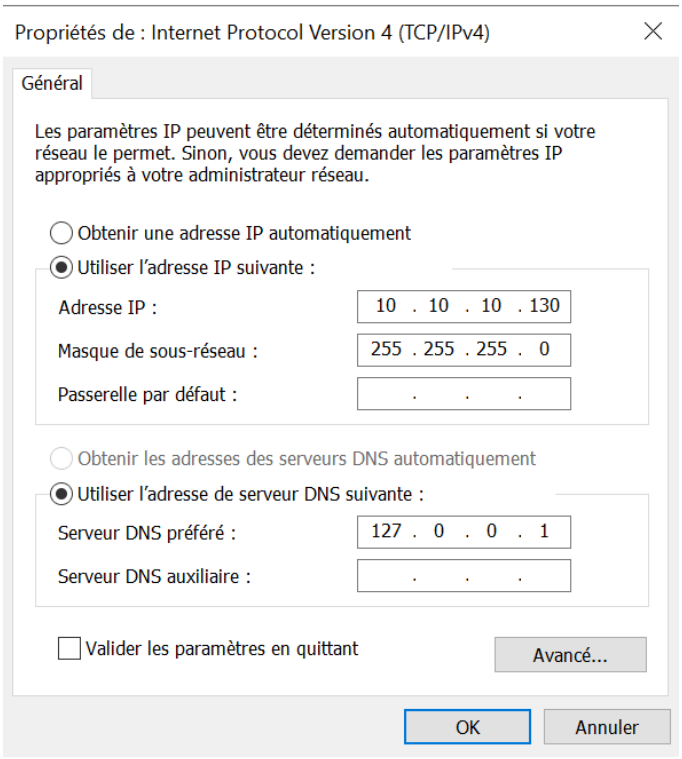
Plus d'infos sur : https://www.it-connect.fr/chapitres/controleur-de-domaine-et-domaine/ et https://en.wikipedia.org/wiki/Domain_controller

2.3.2 Promouvoir le serveur Windows en contrôleur de domaine

Avant de le promouvoir, vous devez d'abord fixer l'adresse IP de son interface dans le réseau Host-only (Ethernet1 dans mon cas) qui est notre réseau local. Utilisez l'astuce « ncpa.cpl » vue précédemment pour vous rendre sur la page des « Connexions réseau » :

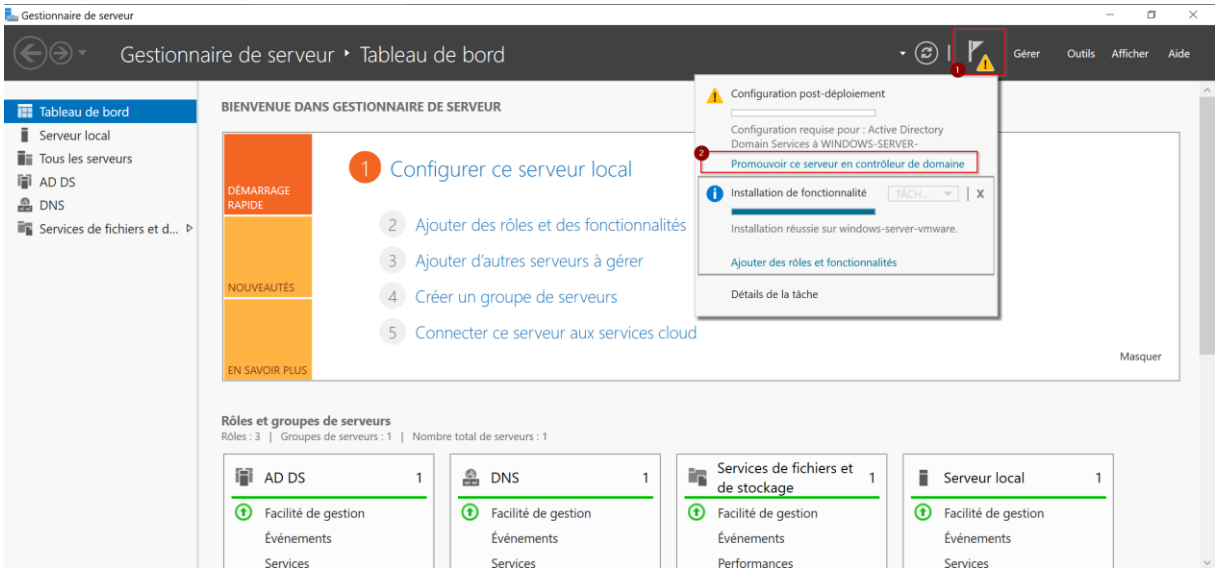


Choisissez la bonne interface et attribuez-lui une IP. J'ai choisi « 10.10.10.130 » sur un réseau en /24. Mettez « 127.0.0.1 » en adresse IP de « Serveur DNS préféré » car il sera le résolveur DNS une fois promu en contrôleur de domaine.

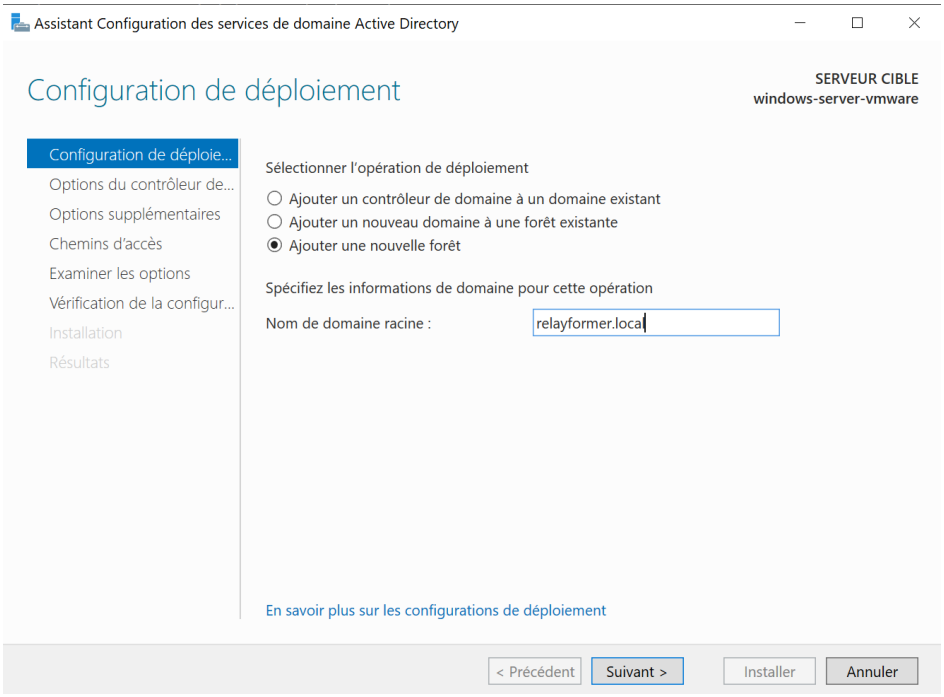


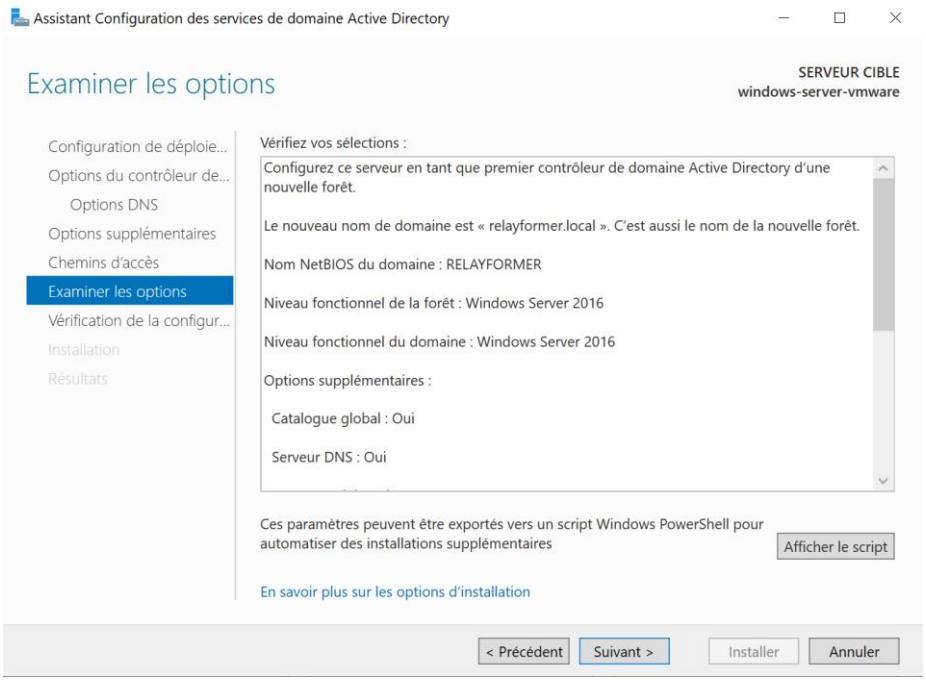
Ensuite installez les services AD DS et DNS. Les étapes pour cela ne seront volontairement pas très détaillées car vous devez savoir le faire en autonomie. De plus, c'est très intuitif car l'assistant détaille tout.

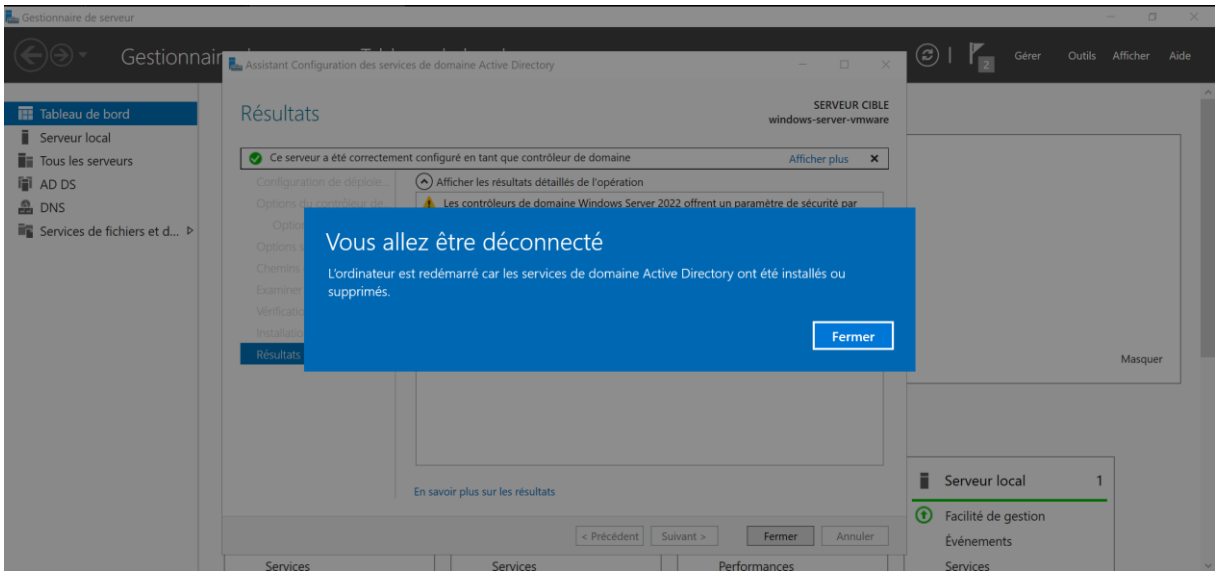
Une fois cela fait, il vous restera à promouvoir le serveur en contrôleur de domaine.

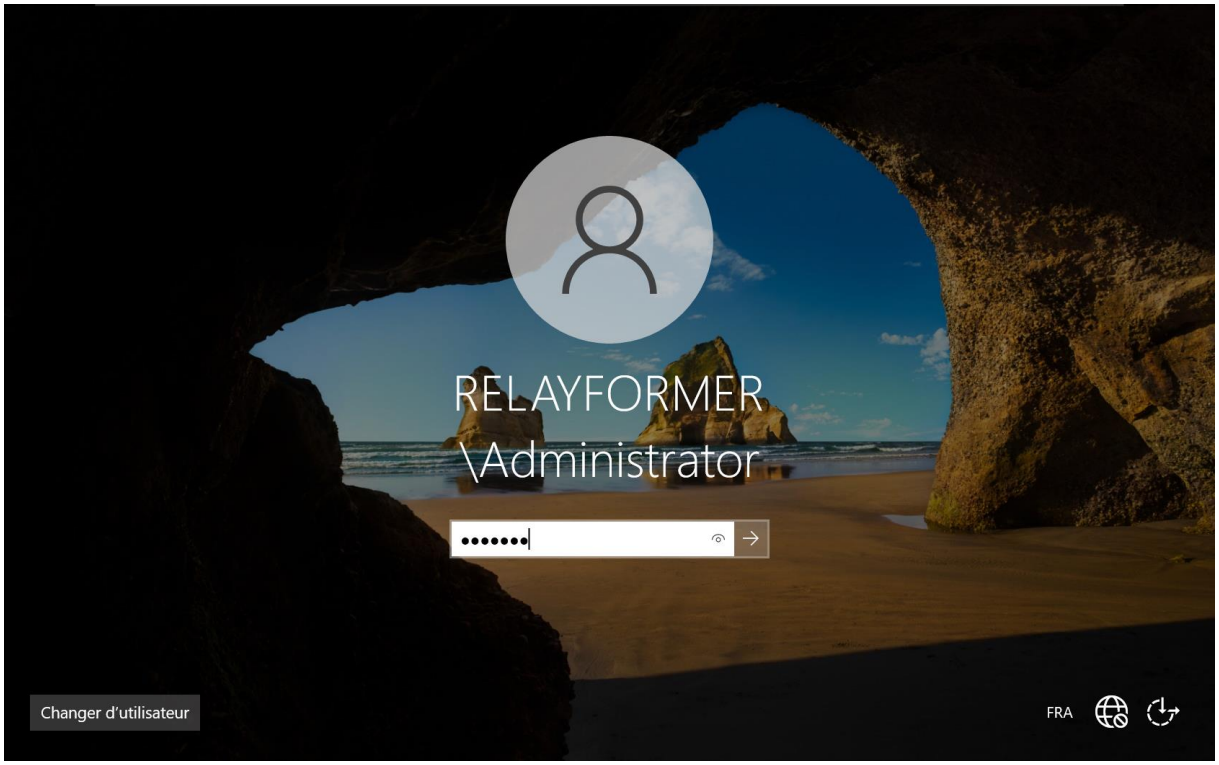


Vous pouvez choisir le nom de domaine de votre choix. Par exemple « monorganisation.local » ou « tp-windows.lab ».









2.4 Avoir une connectivité réseau entre les machines

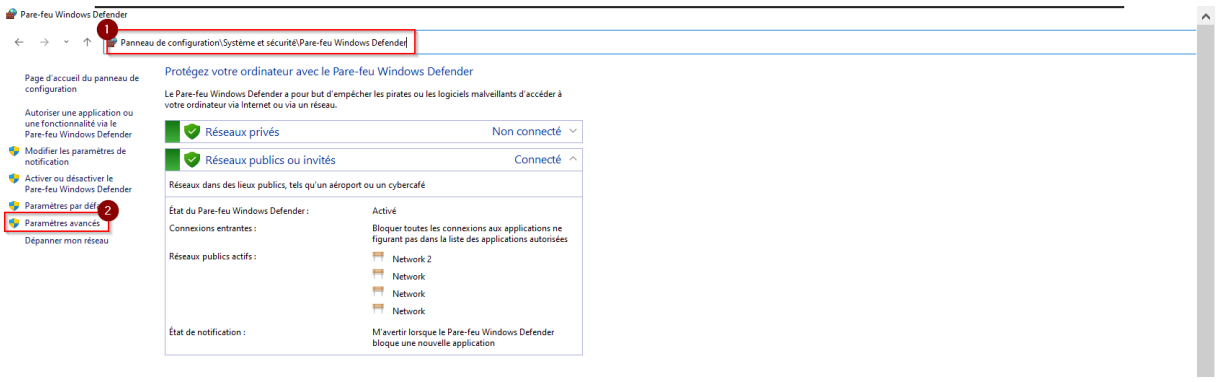
Pour vous assurer que tout va bien, essayez de pinguer votre serveur Windows 2022 avec votre client Windows 11 en forçant l'utilisation de l'interface du réseau local avec l'option « -S » :

```
PS C:\Users\User> ping -S 10.10.10.128 windows-server-vmware

Envoi d'une requête 'ping' sur windows-server-vmware.localdomain [10.10.10.130] de 10.10.10.128 avec 32 octets de données :
Réponse de 10.10.10.130 : octets=32 temps<1ms TTL=128
Réponse de 10.10.10.130 : octets=32 temps=2 ms TTL=128
Réponse de 10.10.10.130 : octets=32 temps=2 ms TTL=128
Réponse de 10.10.10.130 : octets=32 temps=3 ms TTL=128

Statistiques Ping pour 10.10.10.130:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 3ms, Moyenne = 1ms
```

Dans l'autre sens, essayez maintenant de pinguer votre Windows 11 client depuis votre Windows Server sur le réseau Host-only (l'option « - a » résout les adresses en noms d'hôtes) :

```
PS C:\Users\Administrator> ping -S 10.10.10.130 -a 10.10.10.128

Envoi d'une requête 'ping' sur WINDOWS-CLIENT- [10.10.10.128] de 10.10.10.130 avec 32 octets de données :
Réponse de 10.10.10.128 : octets=32 temps<1ms TTL=128
Réponse de 10.10.10.128 : octets=32 temps=3 ms TTL=128
Réponse de 10.10.10.128 : octets=32 temps=1 ms TTL=128
Réponse de 10.10.10.128 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 10.10.10.128:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 3ms, Moyenne = 1ms
```

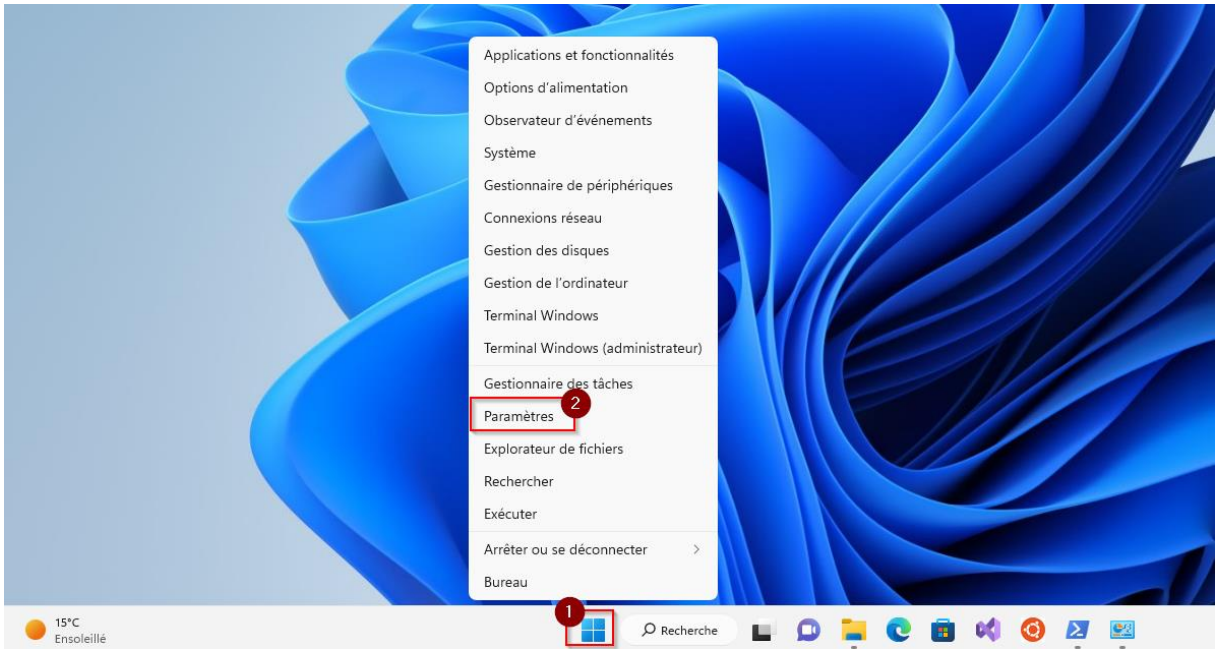
Si vous n'y arrivez pas vérifiez bien toute votre configuration réseau. Vous pouvez aussi retourner sur le client Windows 11 et regarder du côté de votre pare-feu Windows Defender et si besoin le configurer (ou, plus radicalement, le désactiver ce qui n'est pas très grave puisque nous ne sommes pas dans un environnement de production).

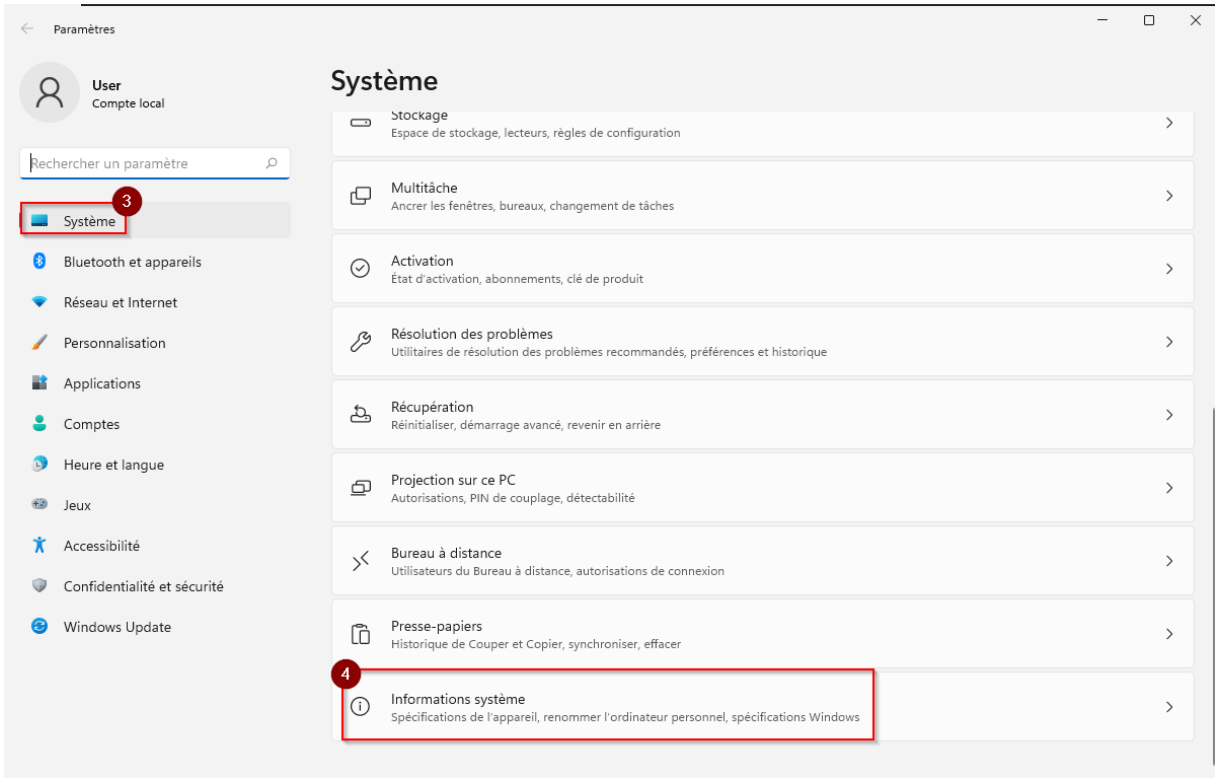


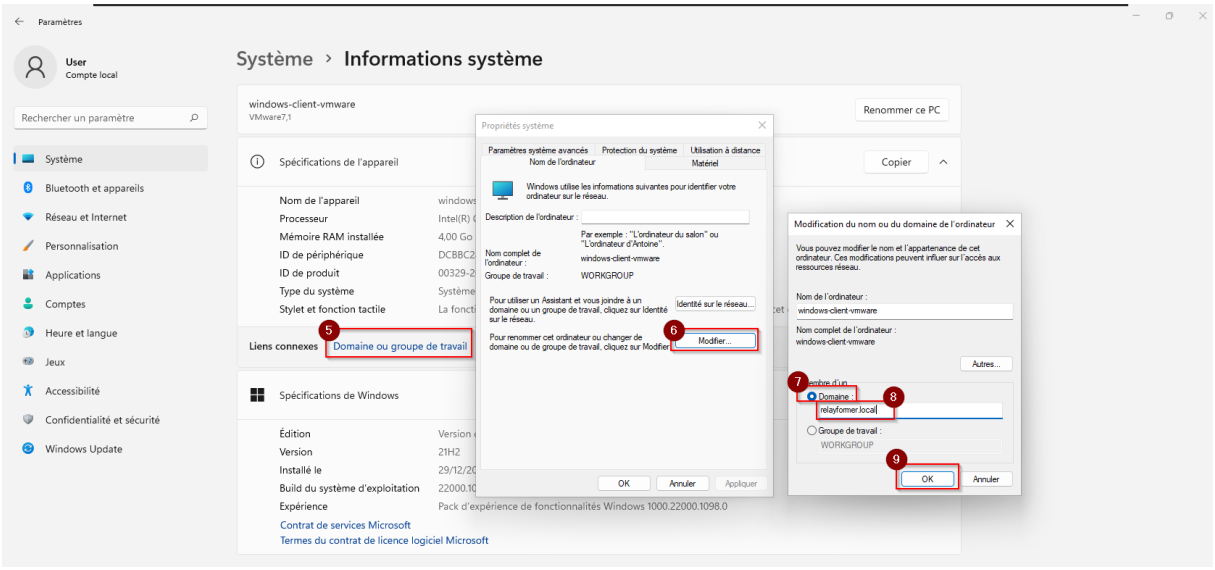
3 Joindre le poste client au domaine Active Directory

Vous allez maintenant pouvoir joindre votre machine cliente à un domaine Active Directory.

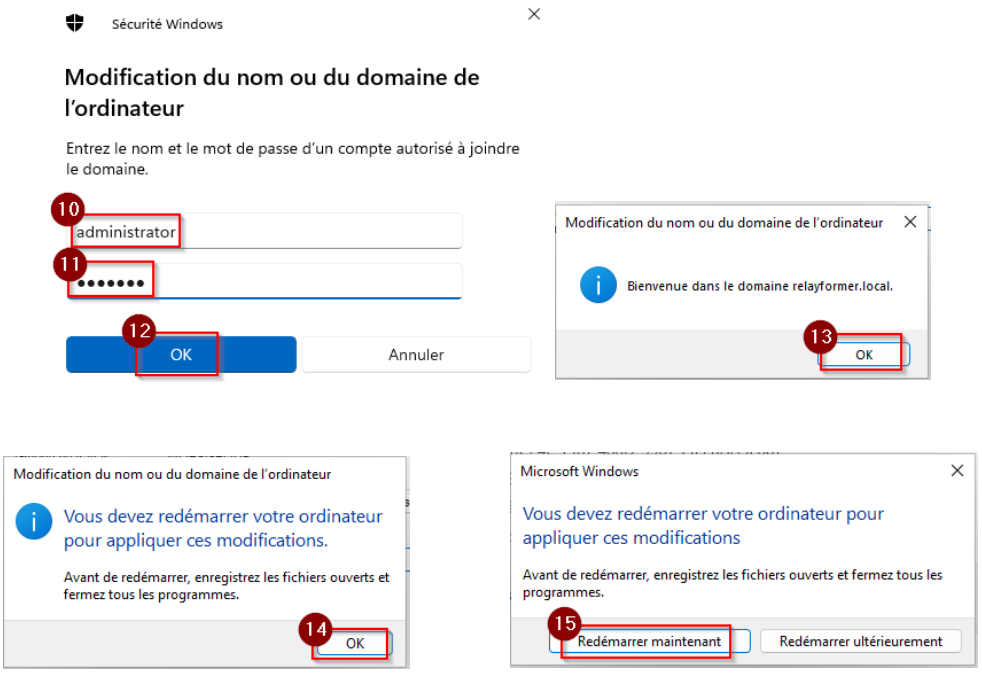
Faites un clic droit sur l'icône du menu Démarrer puis choisissez « Paramètres » :



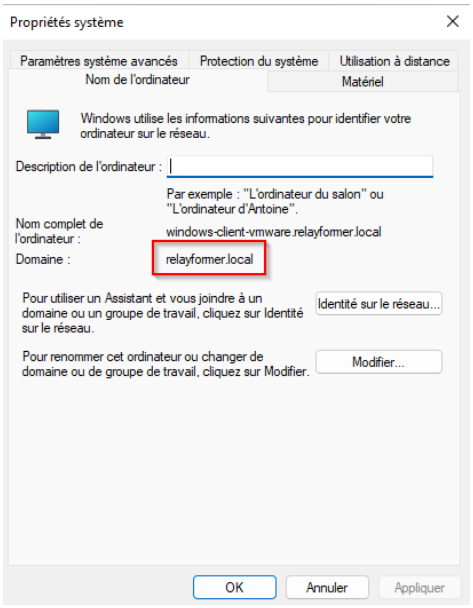




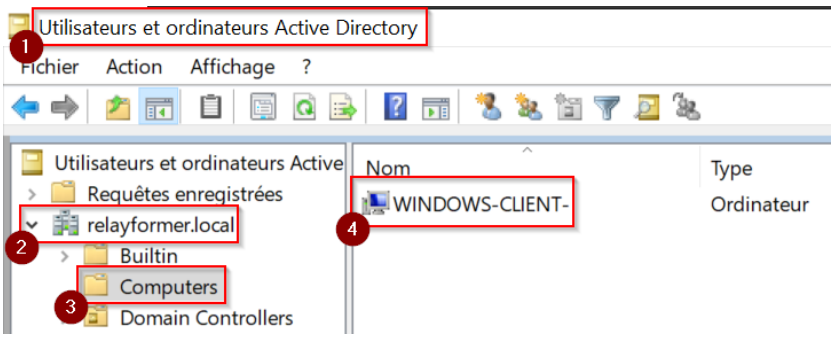
Identifiez-vous avec votre compte administrateur qui se nomme en réalité « administrator » puisque le système était en anglais à sa création :



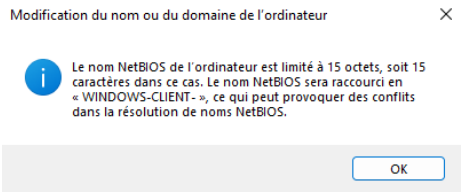
Une fois reconnecté avec l'utilisateur local « User » vous pouvez constater que le poste a bien été joint au domaine :



Si vous retournez sur votre contrôleur de domaine, vous verrez qu'il s'affiche aussi dans l'arborescence Active Directory :



Remarquez que son nom a été automatiquement raccourci à 15 caractères lors de la jonction au domaine :

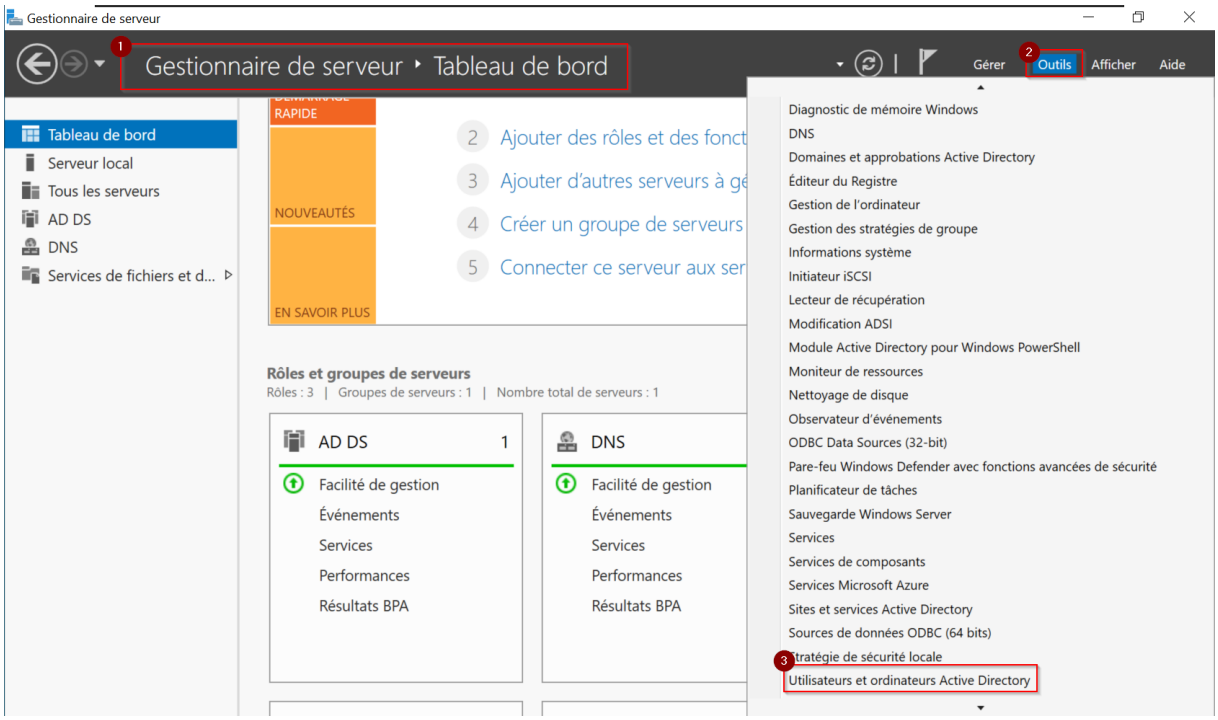


4 Gérer des objets dans l'annuaire Active Directory

Vous allez appliquer un ensemble de règles à des objets Active Directory.

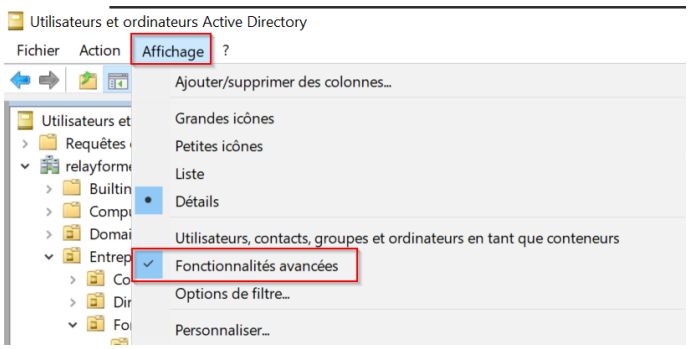
Mais pour cela il faut déjà organiser votre arborescence Active Directory.

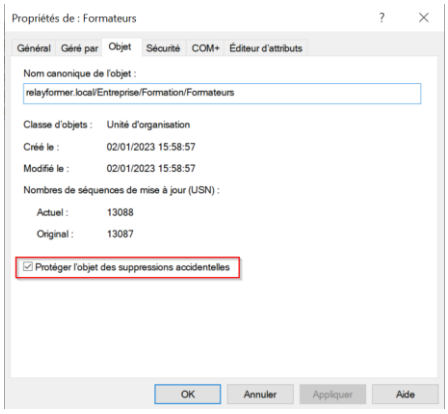
Retournez sur votre contrôleur de domaine et rendez-vous dans « Utilisateurs et groupes Active Directory » :



Suppression d'objets protégés

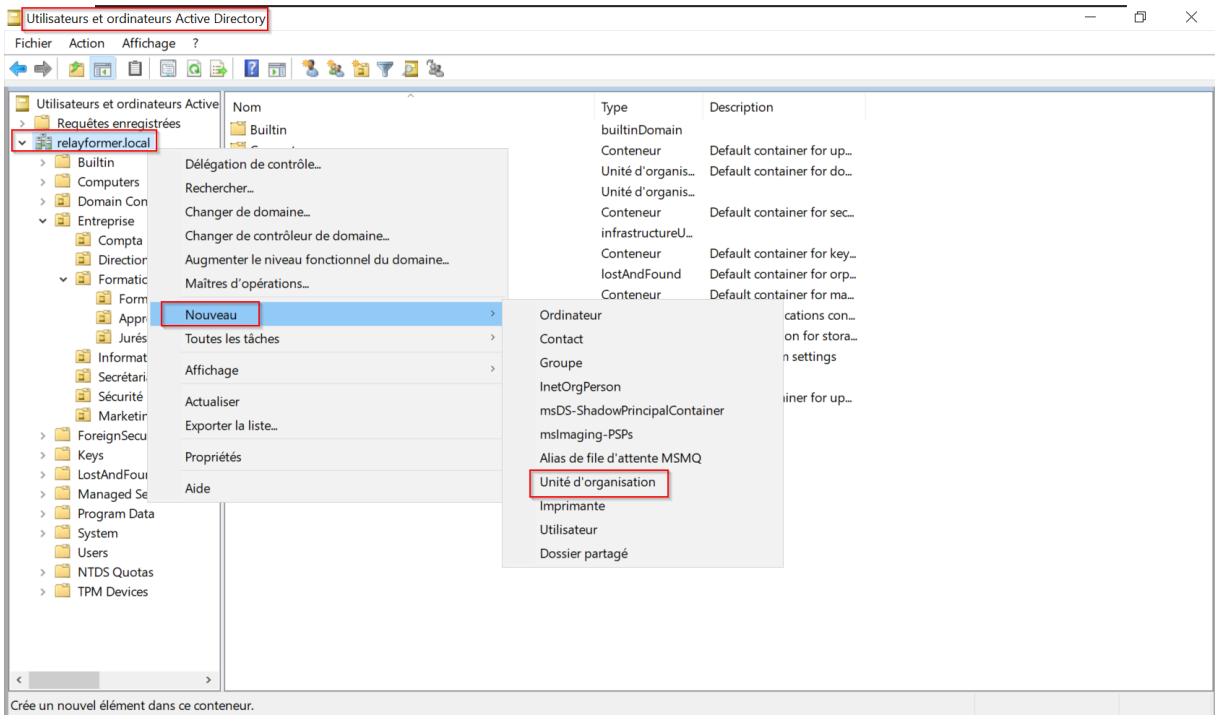
Si vous avez besoin de supprimer un objet (groupe, UO, ordinateur, etc.) que vous avez protégé contre la suppression accidentelle lors de sa création, vous devrez activer l'affichage des « Fonctionnalités avancées » pour pouvoir retirer cette protection dans les propriétés de l'objet comme illustré ci-dessous :



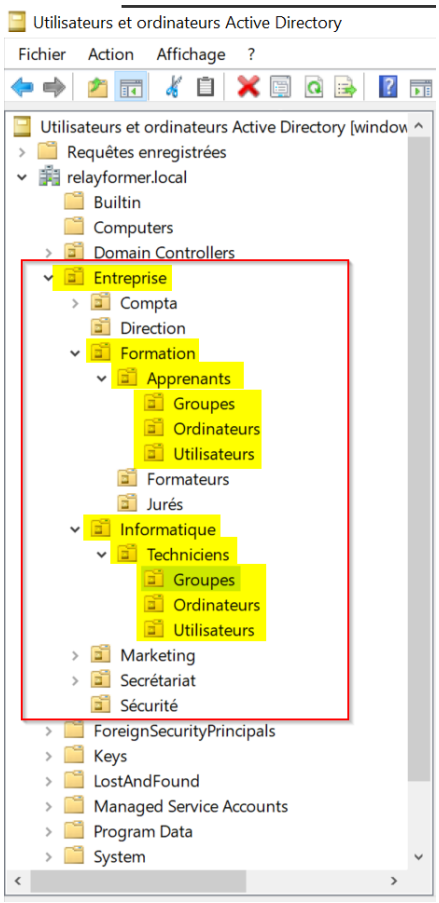


4.1 Créer des unités d'organisation (UO)

Ensuite créez une arborescence d'UO (Unités d'Organisation) pour votre domaine :



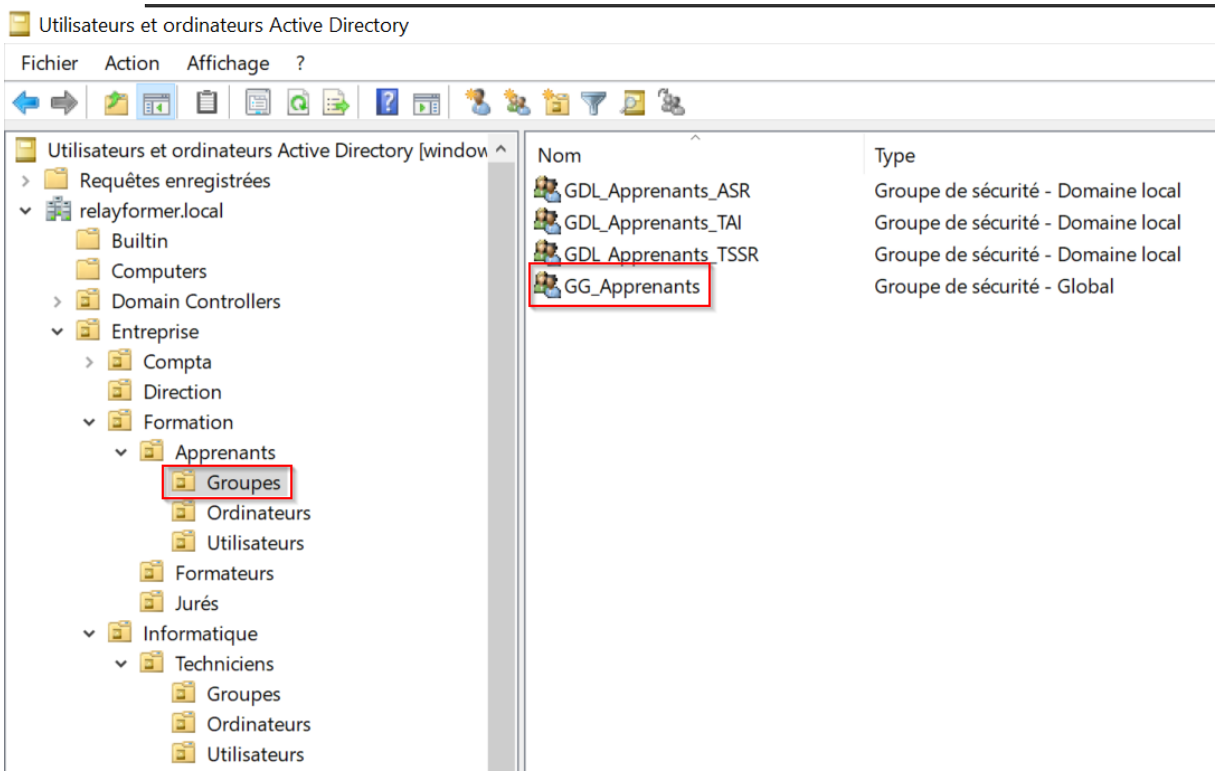
Disons que vous travaillez dans un centre de formation. Vous trouverez ci-dessous l'organisation d'arborescence AD que j'ai créée pour ce centre. Je vous demande de recréer au moins les conteneurs surlignés en jaune dans la capture d'écran ci-dessous (« Entreprise », qui contient les conteneurs « Informatique », « Techniciens », « Formation », « Apprenants », etc.) :

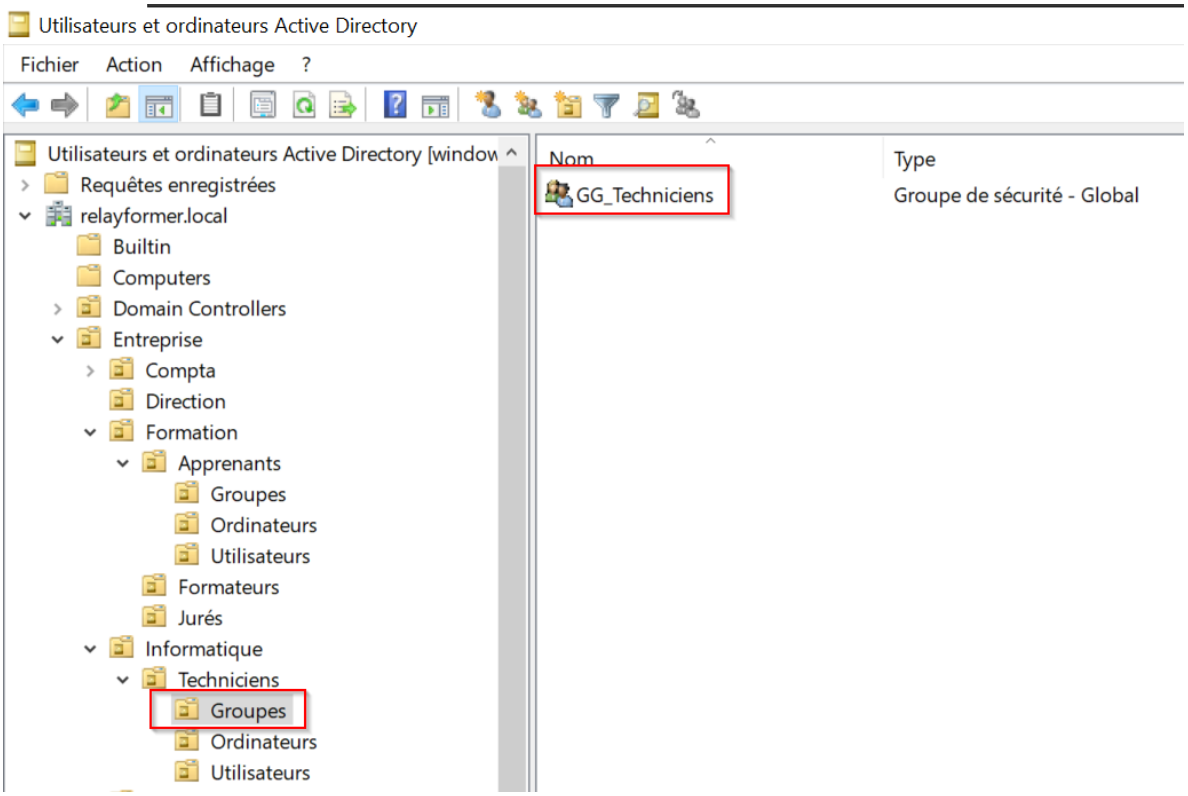


4.2 Créer des groupes

Une fois votre structure en place, vous pouvez y créer quelques groupes Active Directory[7]. Créez au moins un groupe global « GG_Apprenants » et un groupe global « GG_Techniciens ».

[7] Pour en savoir un plus sur les groupes Active Directory : https://learn.rdr-it.io/Le%C3%A7on/groupes-active-directory/

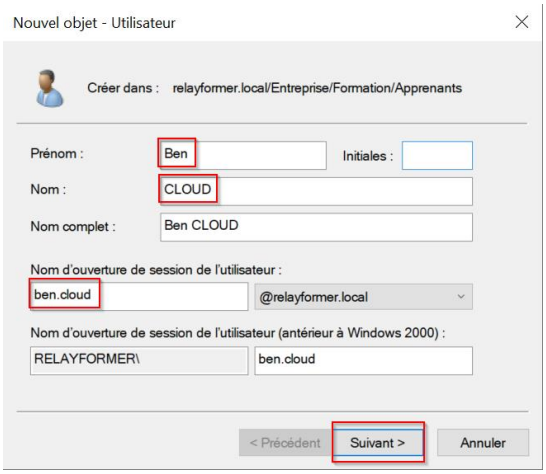


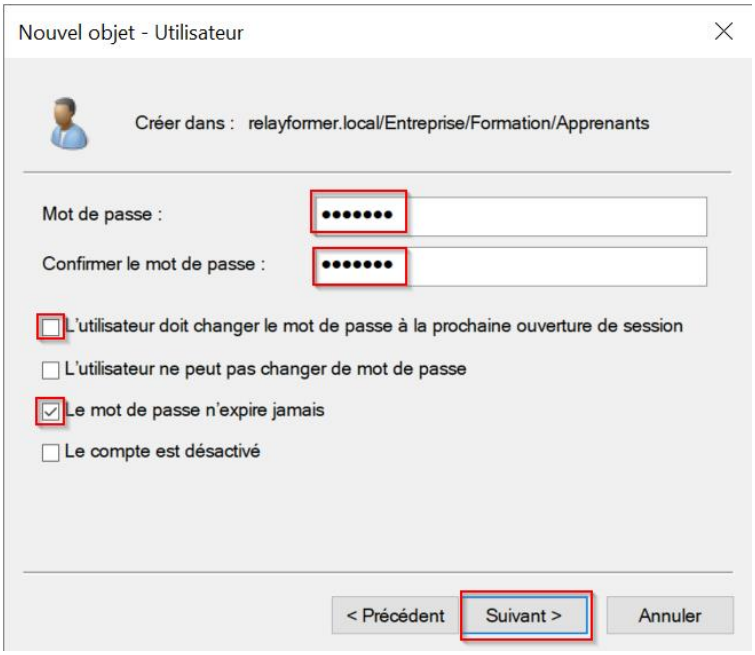


Une fois vos groupes créés vous pouvez passer à la suite.

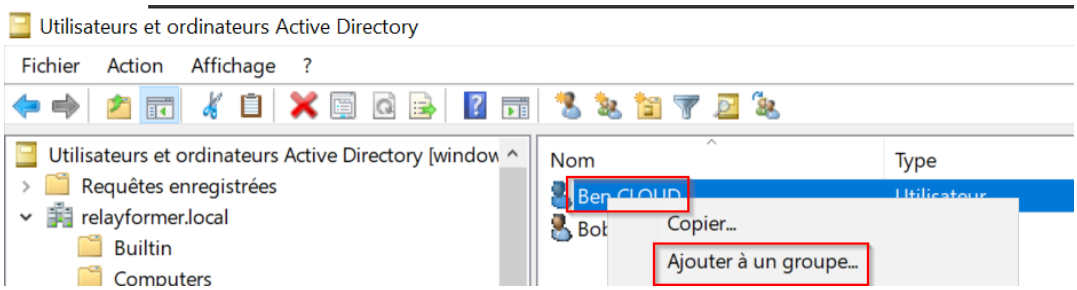
4.3 Créer des utilisateurs

Créez deux utilisateurs dans votre domaine Active Directory : « Ben CLOUD » que vous ajouterez au groupe global « GG_Apprenants » et « Bill TECH » que vous ajouterez au groupe global « GG_Techniciens ».

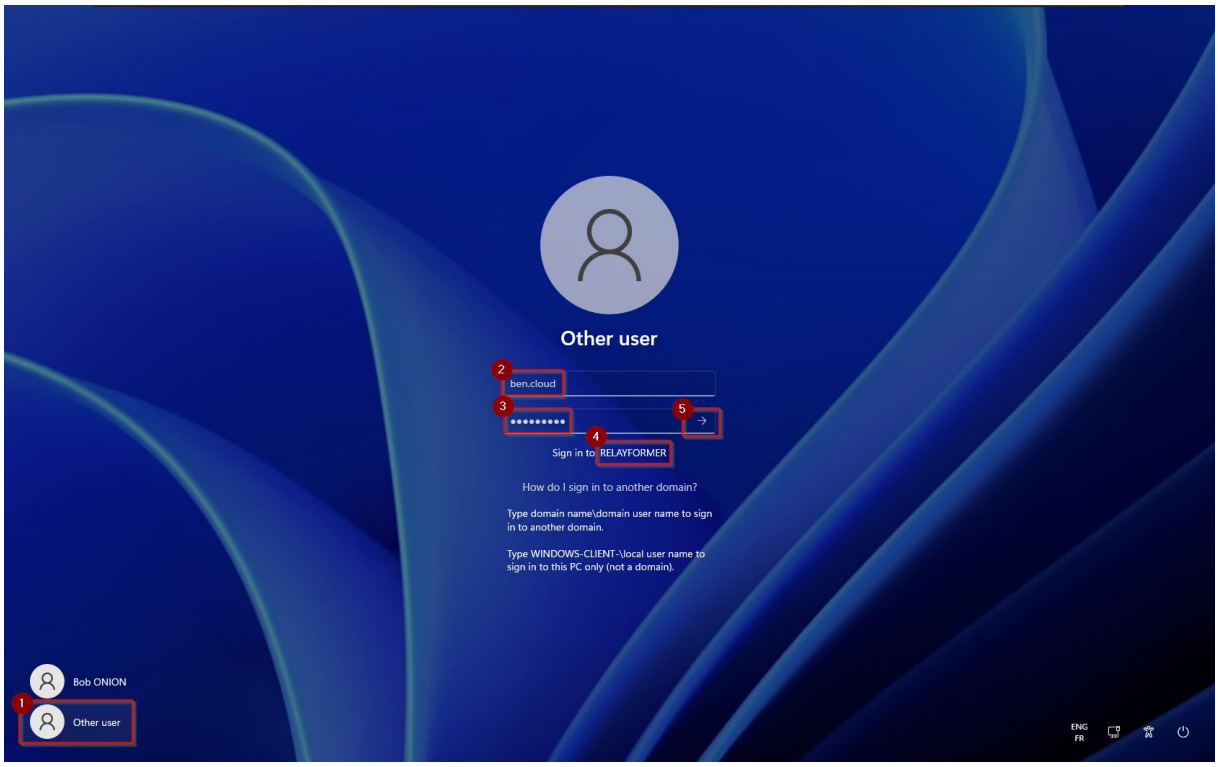




Pour être sûr de ne pas oublier le mot de passe de vos utilisateurs par la suite vous pouvez utiliser celui-ci : « Password123! ».

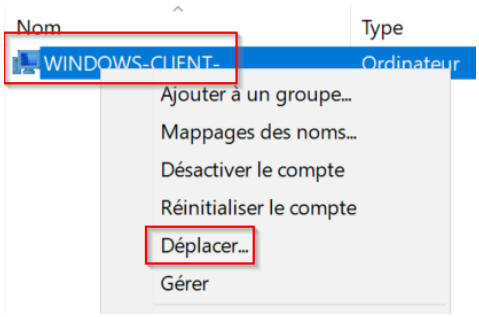


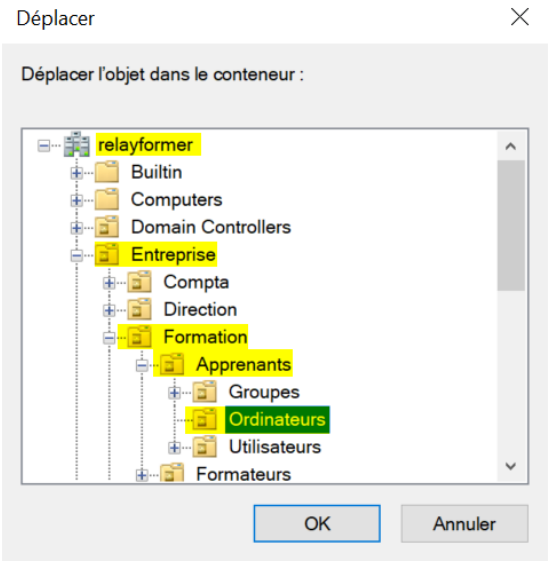
Il sera ensuite possible de se connecter avec les utilisateurs AD créés en utilisant leur nom d'ouverture de session comme illustré ci-dessous :



4.4 Gérer des ordinateurs

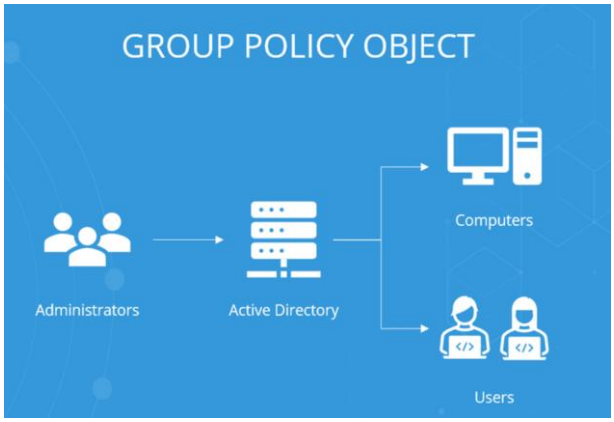
La représentation dans Active Directory de votre VM Windows 11 s'est retrouvée automatiquement dans l'UO par défaut « Computers » après la jonction au domaine AD. Vous allez maintenant la déplacer dans l'UO « Ordinateurs » de l'UO « Apprenants ». Pour cela effectuez un simple glisser-déposer dans l'arborescence ou bien un clic-droit sur l'objet et sélectionnez « Déplacer… »





5 Mettre en place des stratégies de groupe

5.1 Qu'est-ce qu'une stratégie de groupe (GPO) ?



Une **stratégie de groupe** (**Group Policy Object**, ou **GPO**) est **un ensemble d'outils intégrés à Windows Server qui permet au service informatique de centraliser la gestion de l'environnement utilisateur et la configuration des machines grâce à l'application de politiques**.

Chaque stratégie dispose de ses propres paramètres, définis par l'administrateur système, et qui seront appliqués ensuite à des postes de travail, des serveurs ou des utilisateurs.

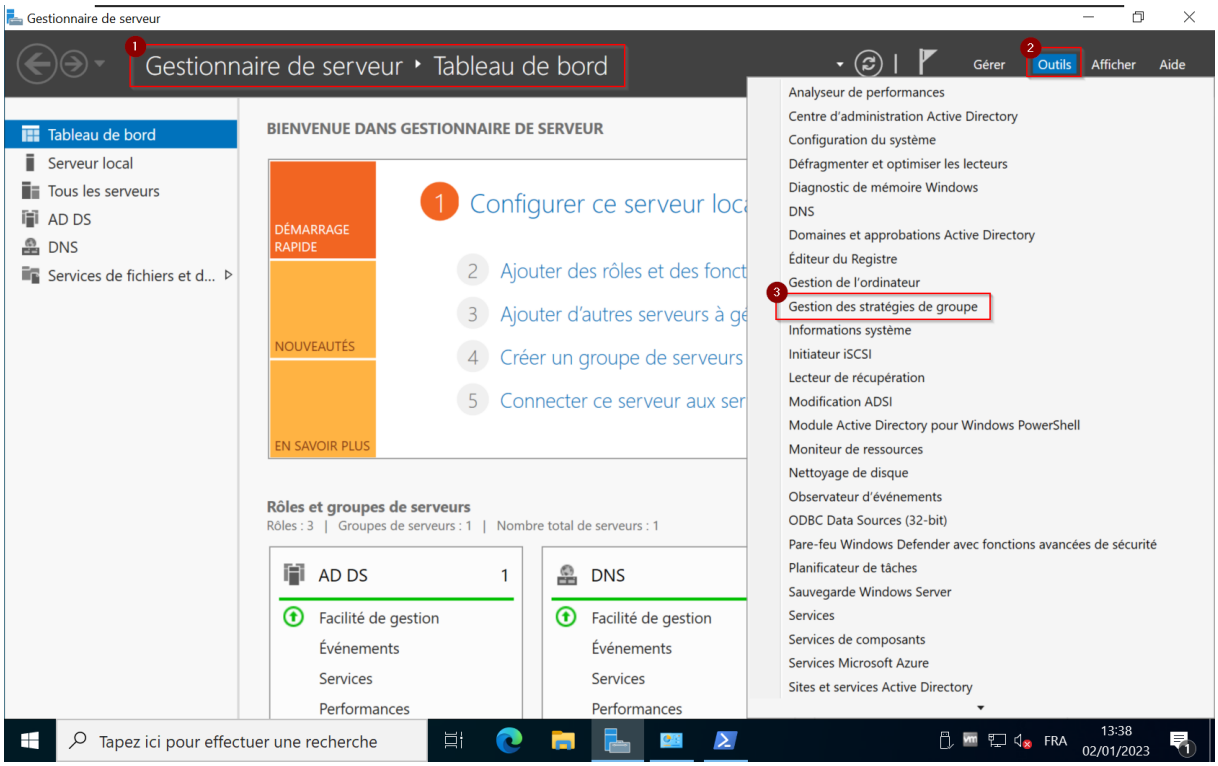
La GPO peut être appliquée au domaine ou à une unité d'organisation (UO) de l'arborescence Active Directory.

Pour en savoir plus sur les GPO : https://www.it-connect.fr/chapitres/quest-ce-quune-strategie-de-groupe-ou-gpo/ ; https://fr.wikipedia.org/wiki/Strat%C3%A9gie_de_groupe ; https://en.wikipedia.org/wiki/Group_Policy ; https://www.netwrix.fr/group_policy_best_practices.html

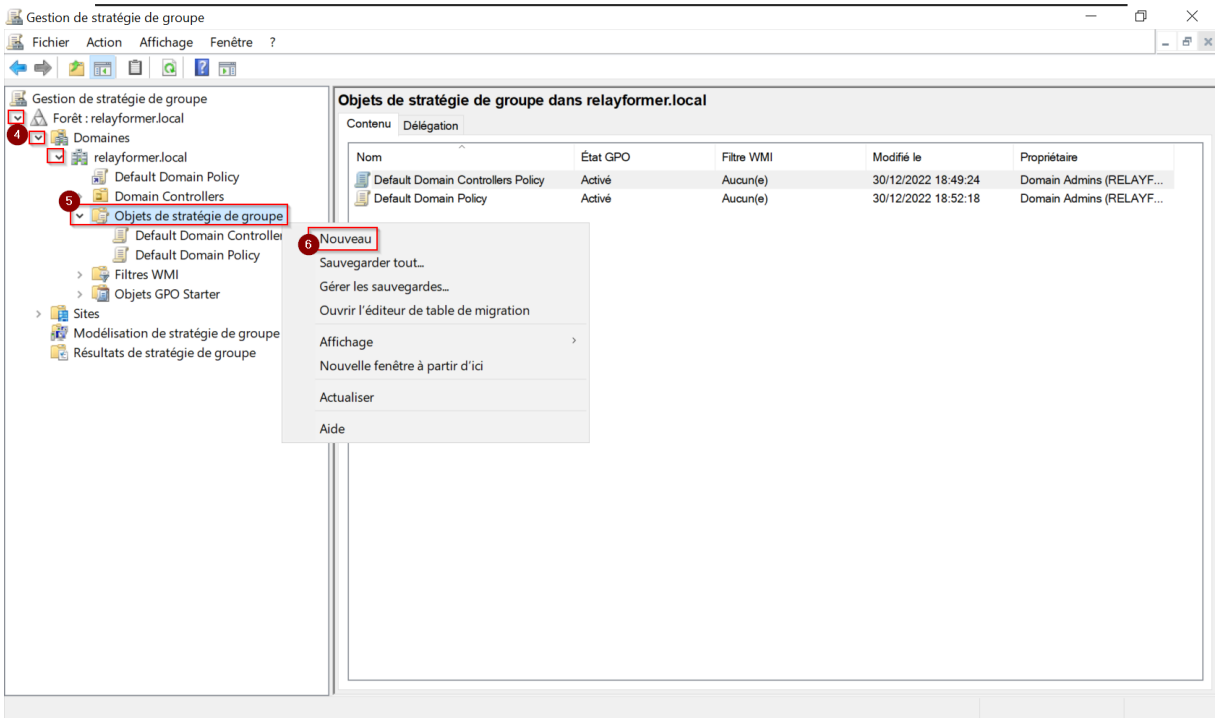
5.1 Créer une GPO simple

Scénario fictif : disons que vous êtes le nouvel administrateur système d'un centre de formation.

Vous allez devoir créer une stratégie de groupe qui forcera les apprenants à respecter votre politique de mots de passe. Pour cela allez dans l'outil de « Gestion des stratégies de groupe » :



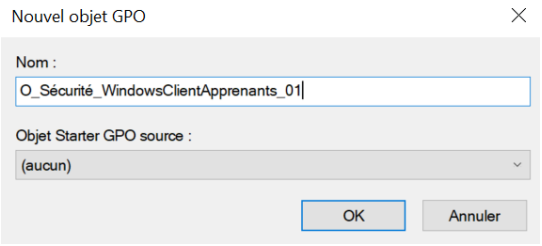
Déroulez l'arborescence jusqu'à « Objets de stratégie de groupe » faites un clic-droit dessus et sélectionnez « Nouveau » :



Une bonne pratique dans la gestion des GPO est de leur donner des noms descriptifs afin qu'il soit possible d'identifier rapidement à quoi sert une GPO simplement en lisant son nom.

L'administration des stratégies de groupe s'en trouvera grandement simplifiée. En donnant à une GPO un nom générique de type « paramètres pc », vous compliquez la tâche aux administrateurs systèmes qui passeront derrière vous. Vous pouvez par exemple mettre en place la convention de nommage suivante :

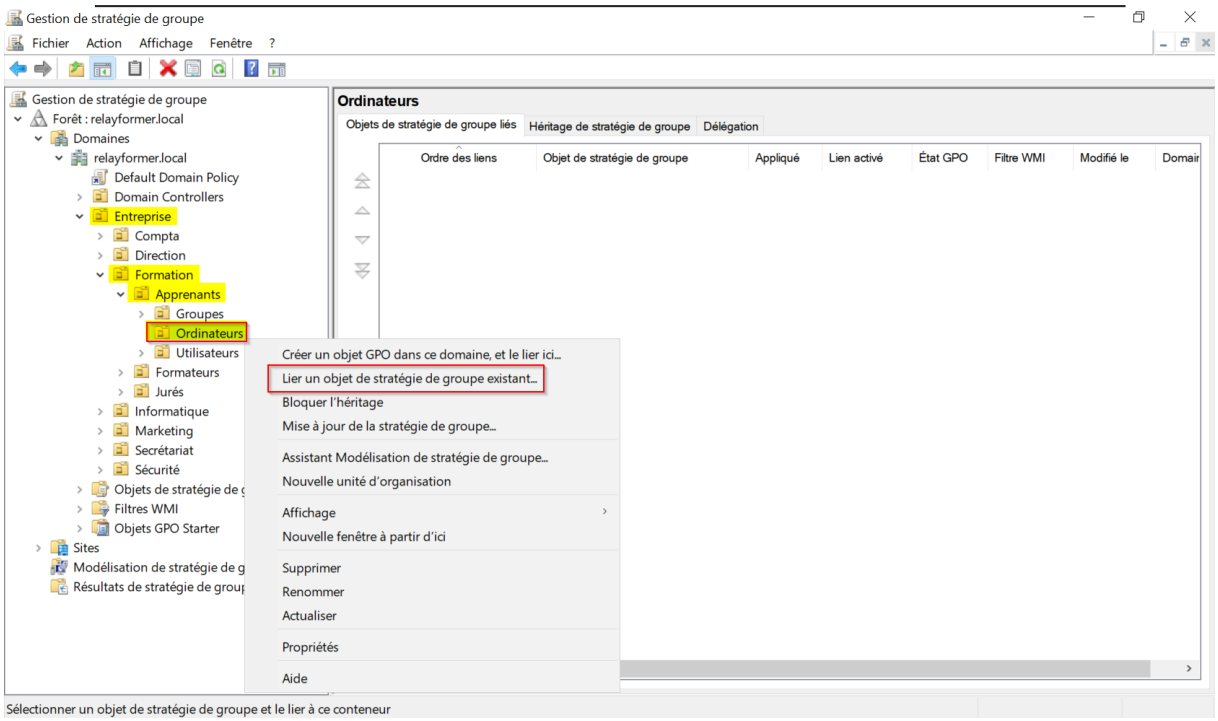
Commencer par un « O » pour spécifier que la GPO va s'appliquer sur des ordinateurs, utiliser des « _ » pour les séparations, puis « Sécurité » pour spécifier que la GPO va appliquer des paramètres de sécurité, puis « WindowsClientApprenants » pour spécifier qu'elle s'applique à des postes clients sous Windows utilisés par les apprenants, puis un numéro « 01 ».

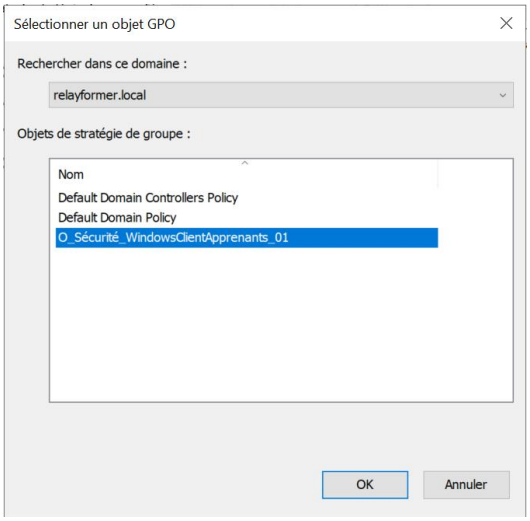


Pour le moment la GPO est vide mais vous allez configurer ses paramètres par la suite pour pouvoir l'appliquer aux postes de travail Windows 11 du centre de formation.

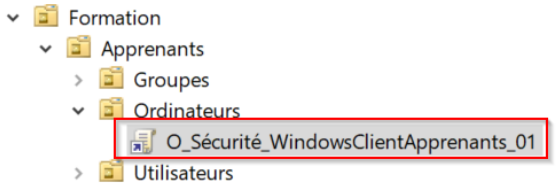
5.1.1 Lier la GPO à une UO

Vous allez maintenant lier votre GPO à l'unité d'organisation « Ordinateurs » de l'UO « Apprenants » qui est censée contenir tous les ordinateurs en liens avec les apprenants de votre centre de formation.



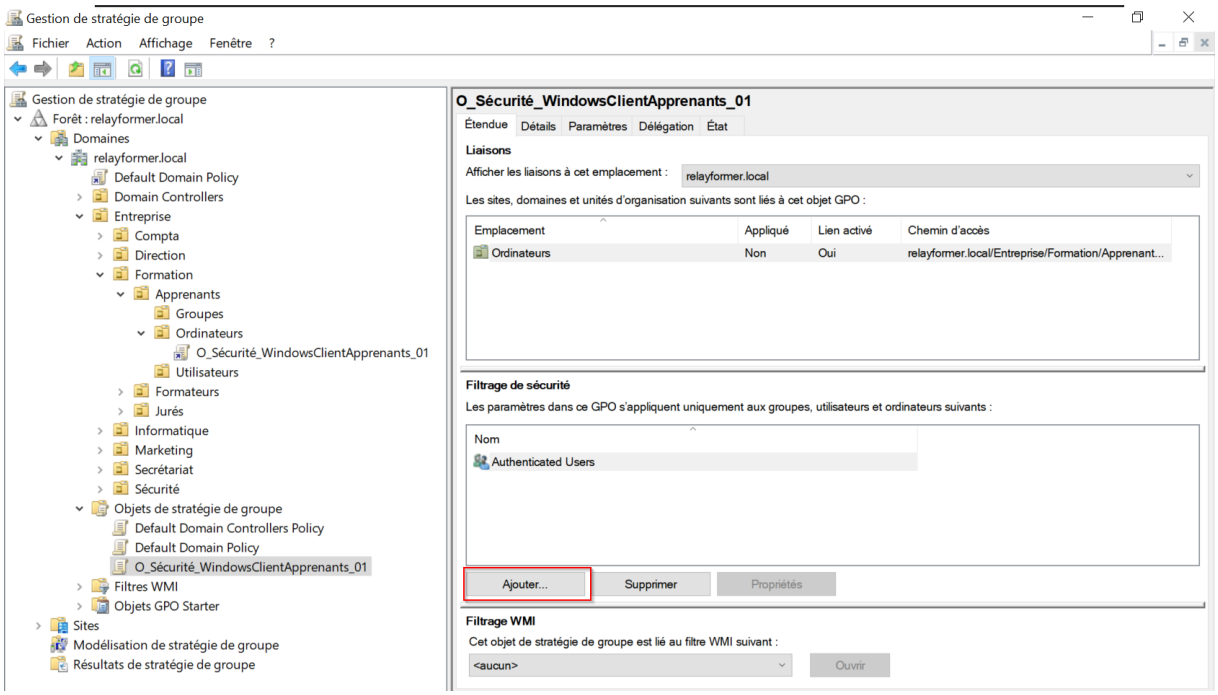


Votre GPO est maintenant liée à votre UO et vous pouvez remarquer qu'un raccourci vers cette GPO s'est ajouté juste sous l'UO.

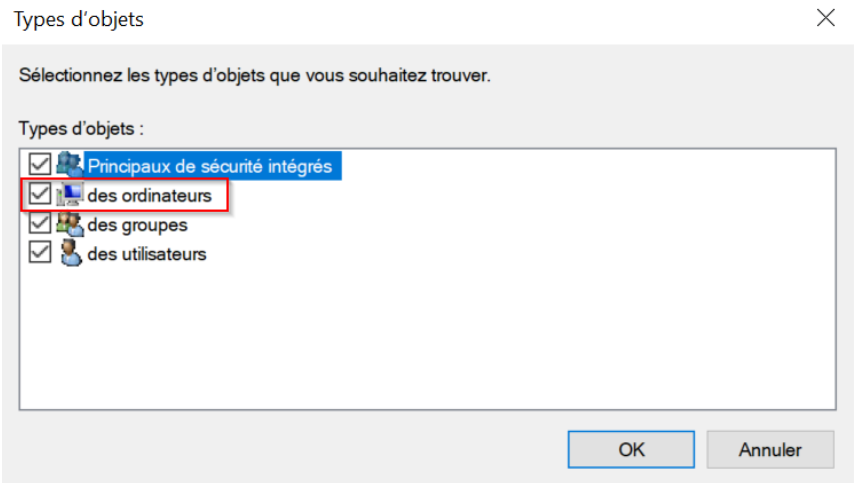


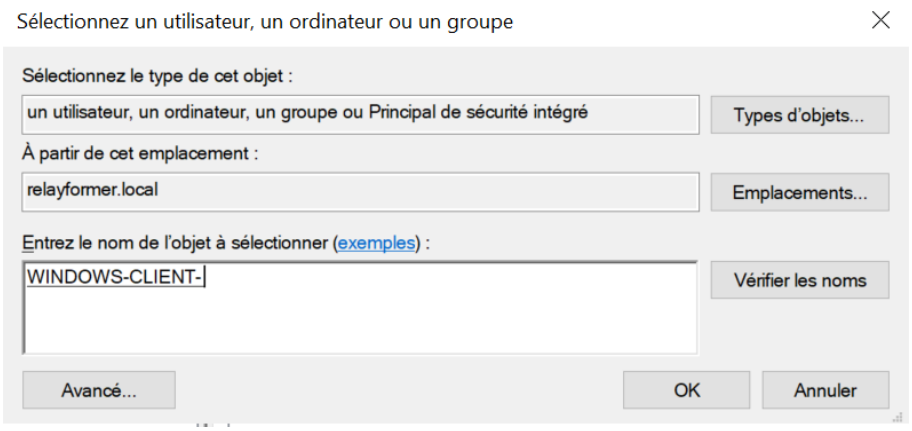
5.1.2 Filtrer l'application des paramètres de la GPO

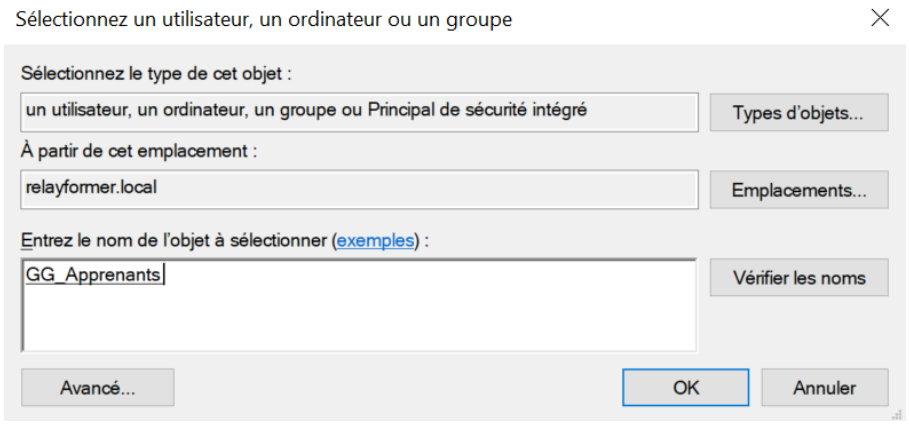
Vous pouvez faire en sorte que les paramètres de cette GPO ne s'appliquent qu'à certains groupes, utilisateurs ou ordinateurs en utilisant le filtrage de sécurité. C'est ce que nous allons faire en spécifiant le groupe « GG_Apprenants » et l'ordinateur « WINDOWS-CLIENT- ». Pour cela cliquez sur « Ajouter » dans le cadre « Filtrage de sécurité » :

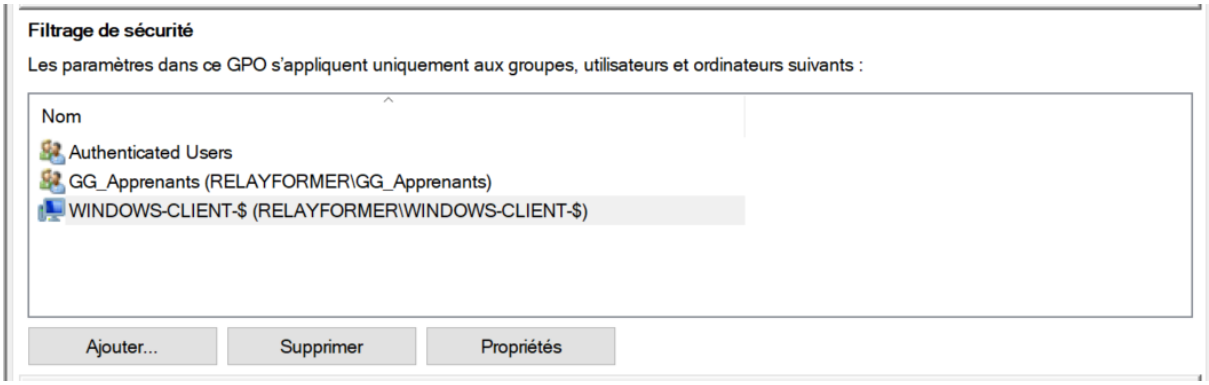


Pour rechercher un ordinateur il faut cliquer sur « Types d'objets… » et cocher « des ordinateurs » :



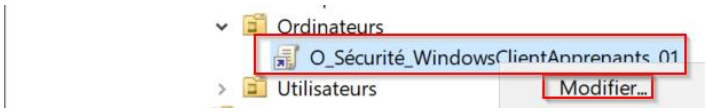






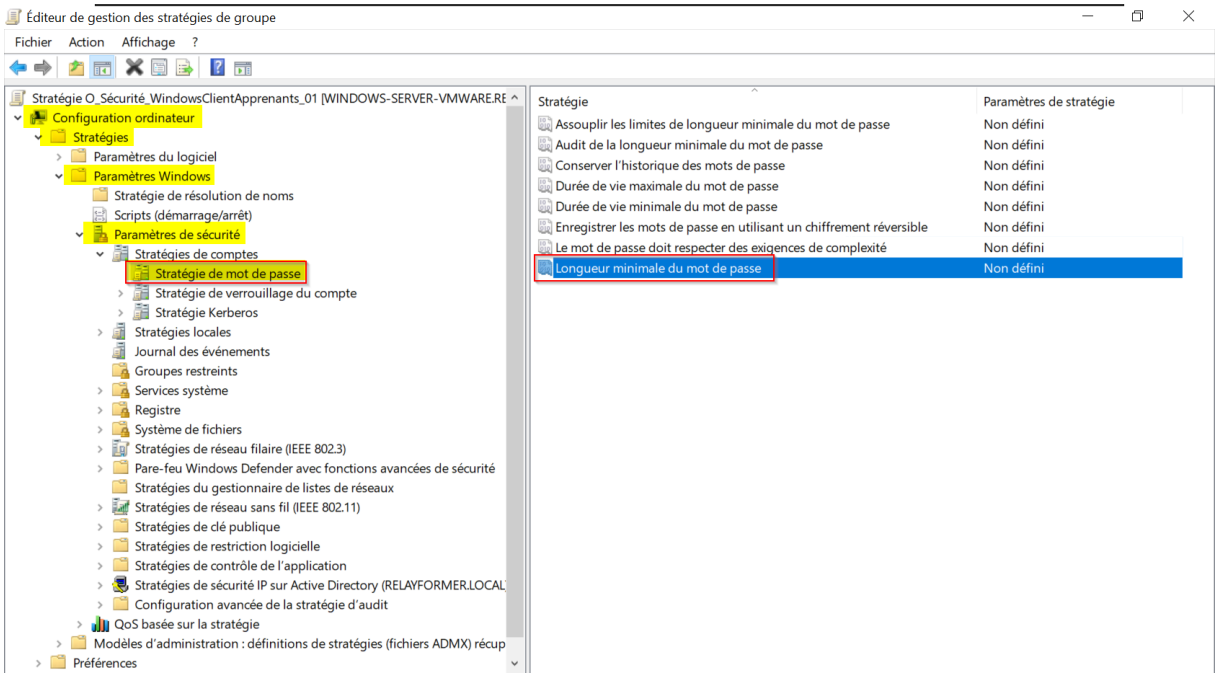
5.1.3 Configurer les paramètres de la GPO

Faites un clic-droit dessus et sélectionnez « Modifier »

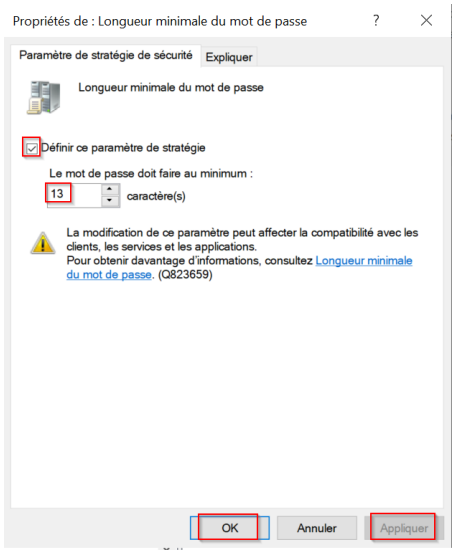


Prenez le temps d'explorer l'arborescence et de regarder les différents paramètres de stratégie disponibles.

Ensuite parcourez l'arborescence comme illustré ci-dessous et vous arriverez aux paramètres de « Stratégie de mot de passe » :

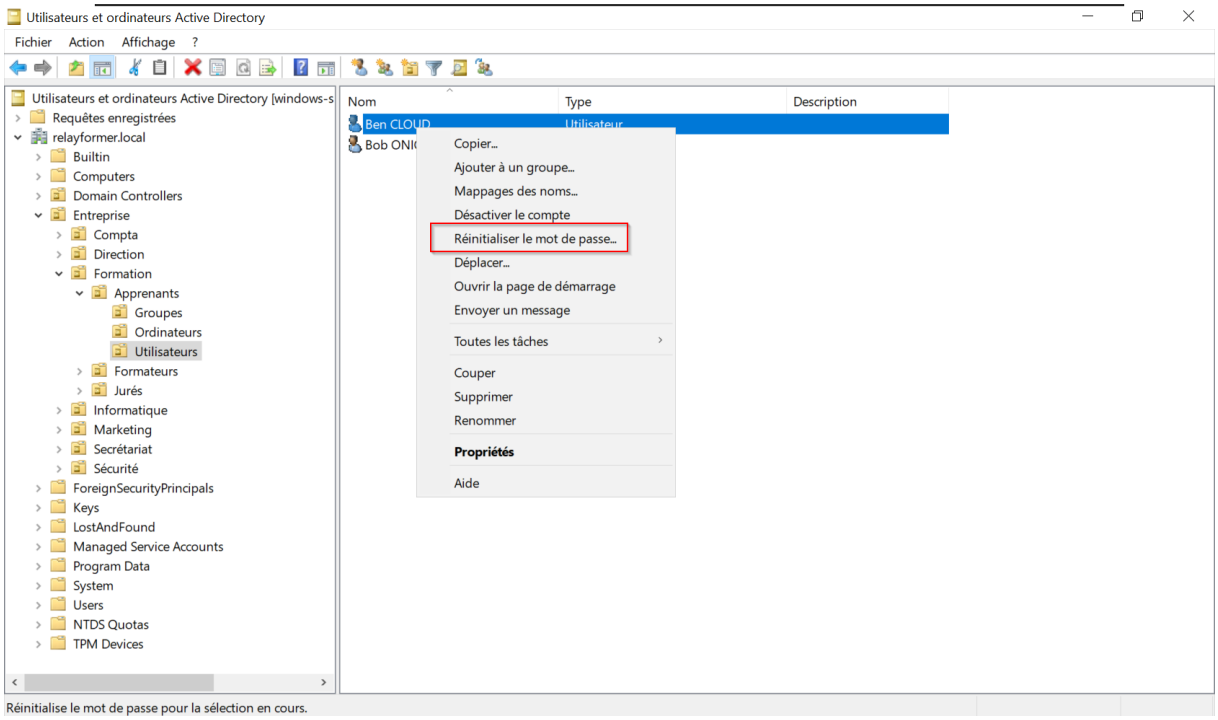


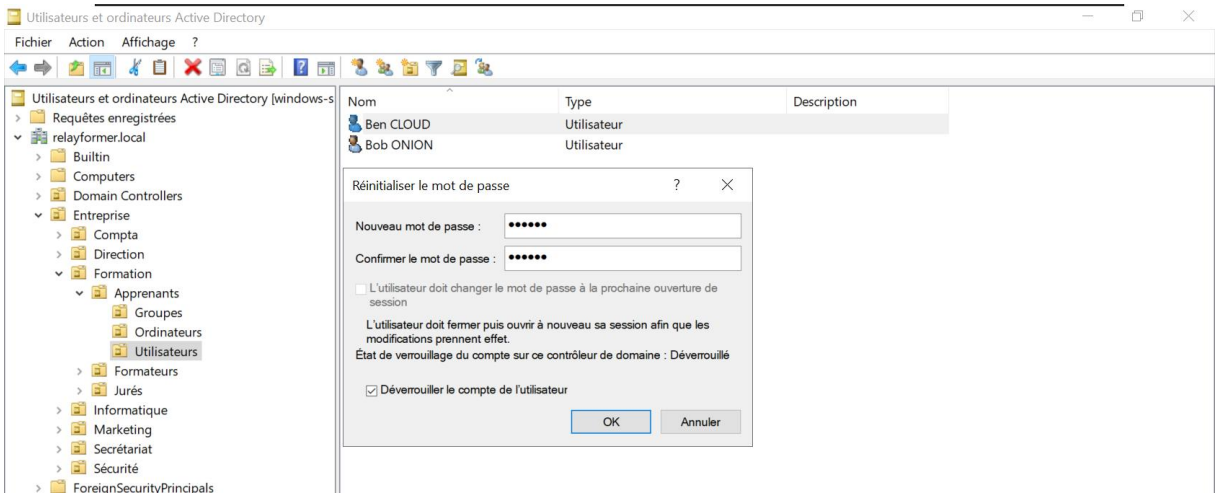
Double-cliquez sur le paramètre de stratégie « Longueur minimale du mot de passe » et configurez-le à 13 caractères.

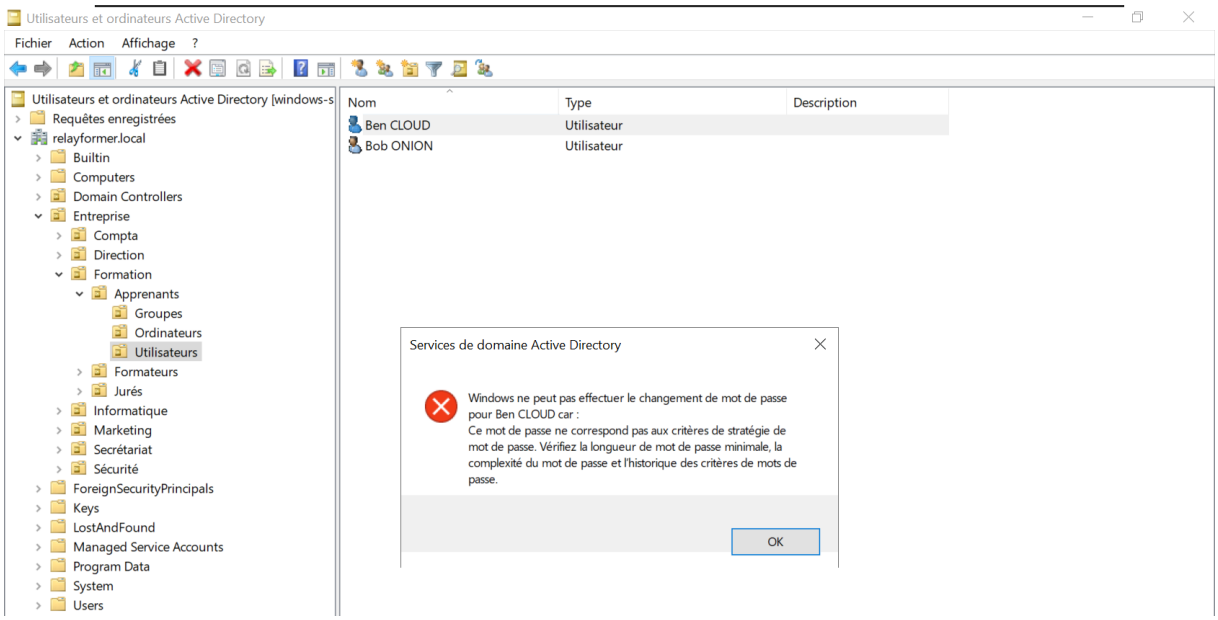


5.2 Tester la bonne application de la GPO

Une fois cela fait vous pouvez tester la bonne application de ce paramètre. Réinitialisez le mot de passe d'un de vos utilisateurs en mettant moins de 13 caractères :

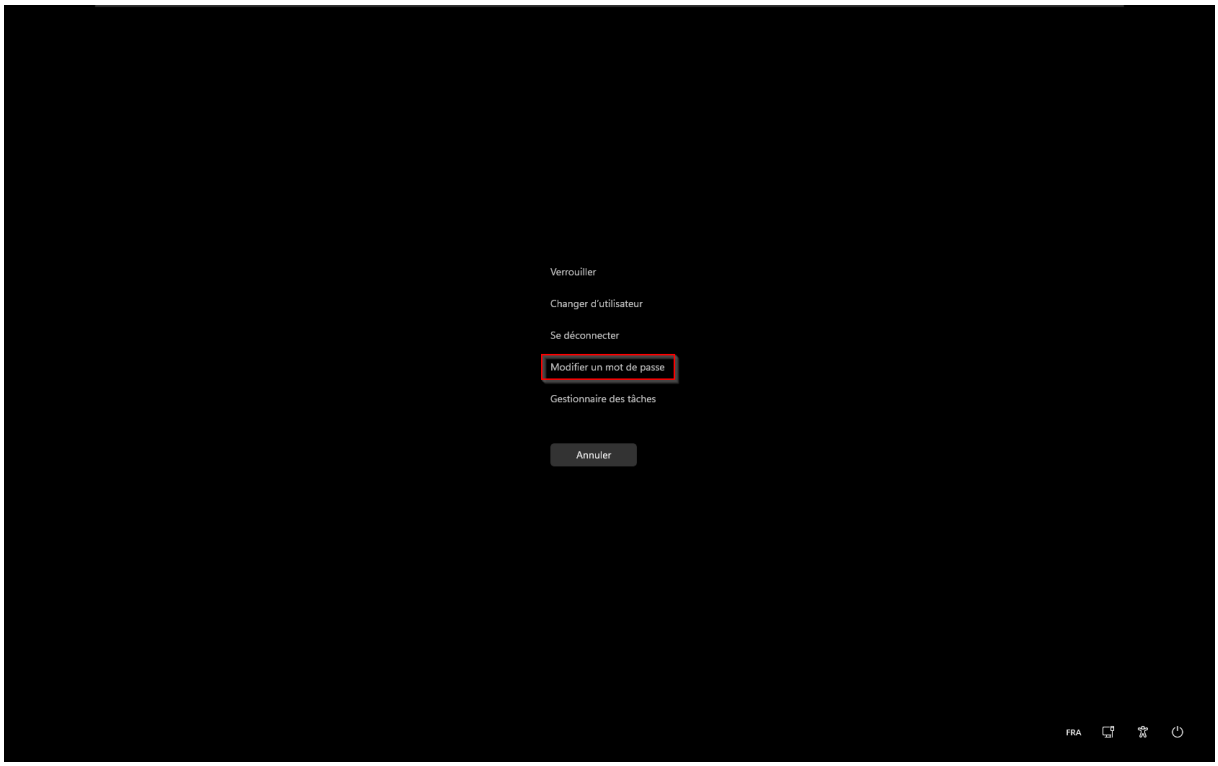




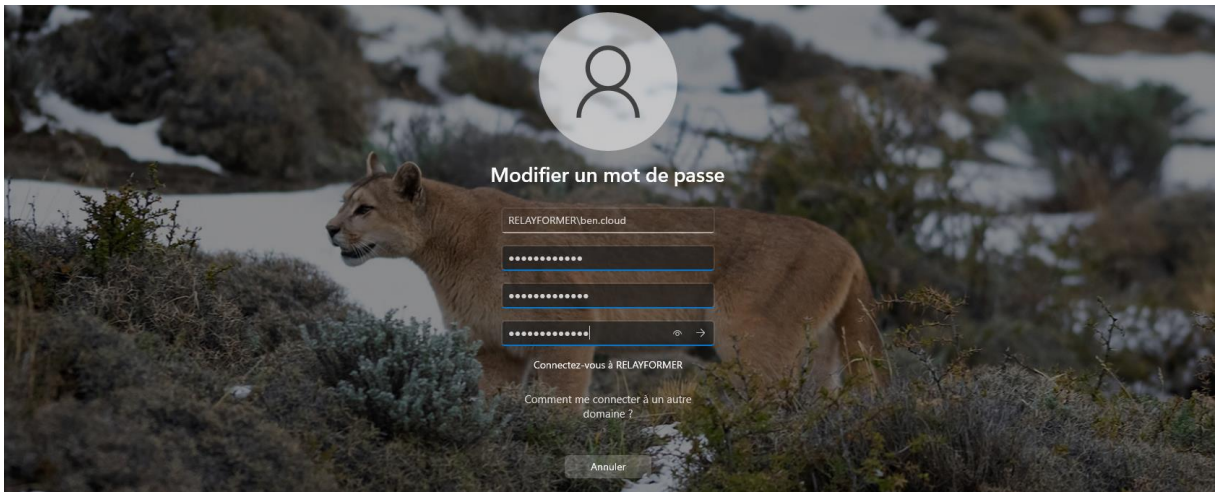


Vous pouvez aussi cliquer sur ce bouton dans l'interface de VMware Workstation depuis votre Windows client :

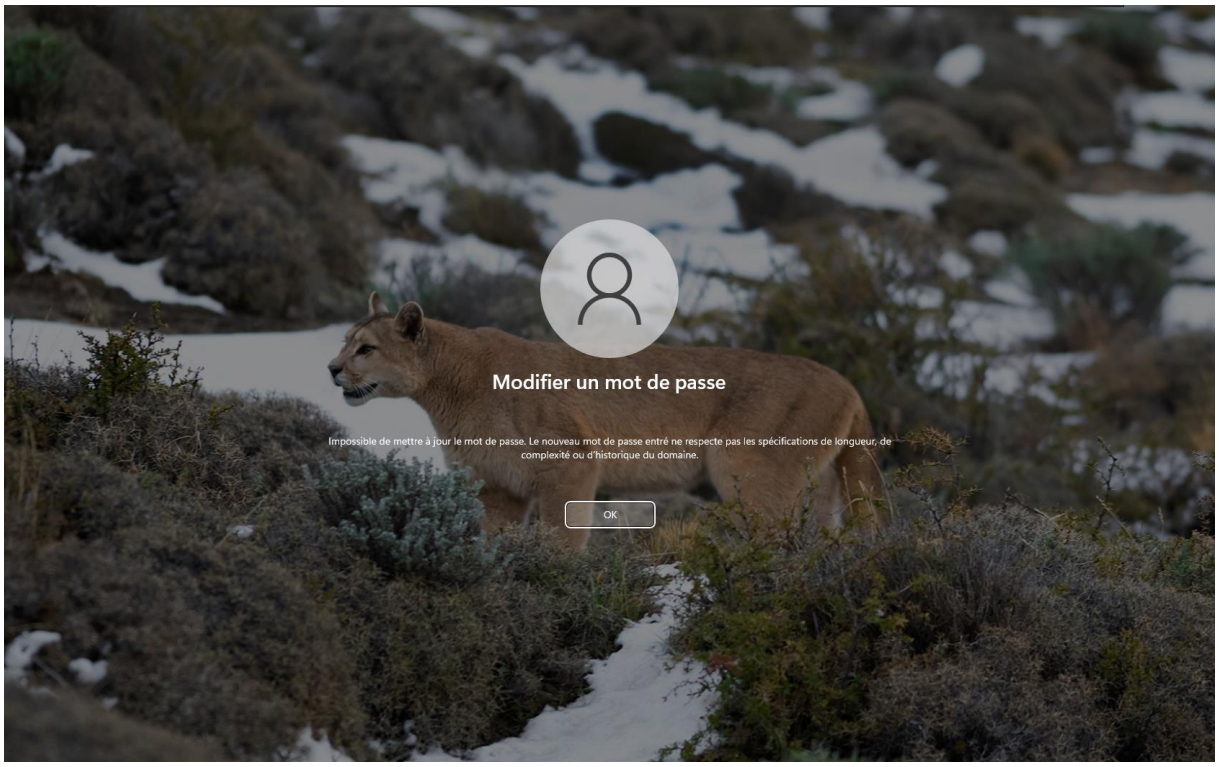
Pour arriver ici et cliquer sur « Modifier un mot de passe » :



Essayer de mettre un mot de passe ne respectant pas les nouvelles exigences, tel que « Password456! » :



Vous devriez obtenir ce message d'erreur :



Votre GPO est bien active.

5.3 Créer une GPO plus complexe

Vous avez créé et configuré la GPO précédente depuis le serveur mais sachez qu'il est possible aussi de faire tout cela depuis le poste client puis d'exporter la GPO pour l'importer sur le serveur. C'est ce que vous allez faire en mettant en place une autre GPO qui utilisera AppLocker pour empêcher les apprenants d'exécuter des logiciels non autorisés sur leurs postes.

5.3.1 Qu'est-ce qu'AppLocker ?

AppLocker est **une technologie de liste blanche d'applications qui permet de restreindre les programmes que les utilisateurs peuvent exécuter** en fonction du chemin d'accès, de l'éditeur ou du hachage du programme et, dans une entreprise, peut être configuré via la stratégie de groupe (GPO).

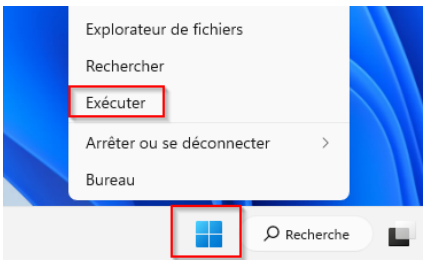
AppLocker permet donc de créer des règles pour définir les applications autorisées à être exécutées par les utilisateurs lambdas sur les machines du domaine. Grâce à ces restrictions, vous allez pouvoir lutter contre l'installation de logiciels non approuvés par le service informatique, de logiciels crackés en version portable, des logiciels portables au sens large, mais cela va permettre aussi de limiter l'installation de malwares sur les postes de travail.

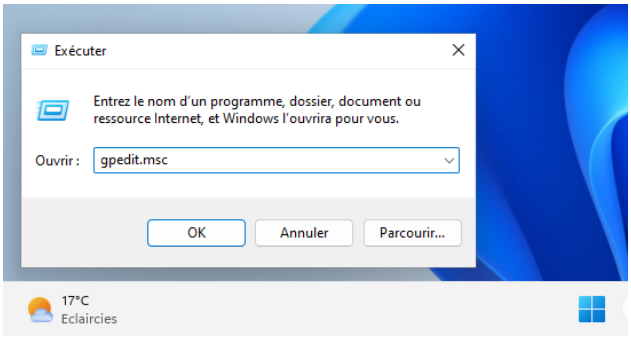
AppLocker va permettre d'agir sur quatre types d'éléments : les exécutables, les installeurs au format Windows Installer (package MSI), les scripts et les applications modernes au format APPX.

Pour en savoir plus sur AppLocker : https://learn.microsoft.com/fr-fr/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

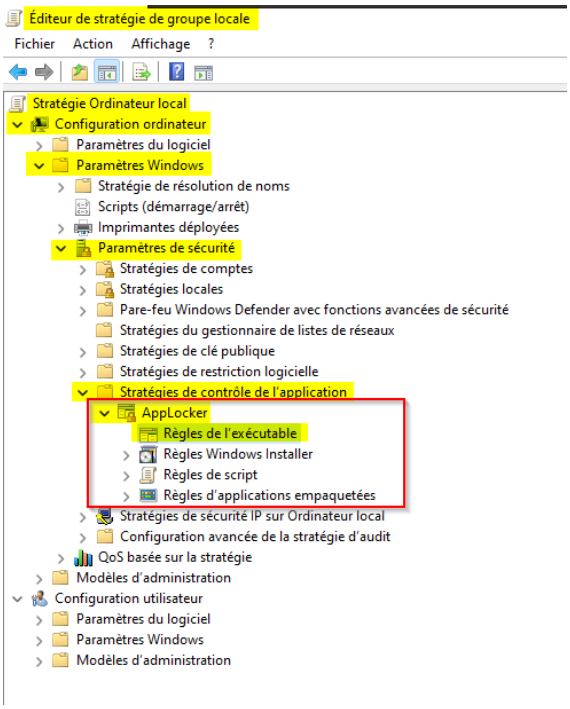
5.3.2 Créer et paramétrer la GPO AppLocker

Depuis votre Windows 11 client, connectez-vous avec le compte local « User » qui possède les droits d'administration et allez dans l'outil « Editeur de stratégie de groupe locale » :

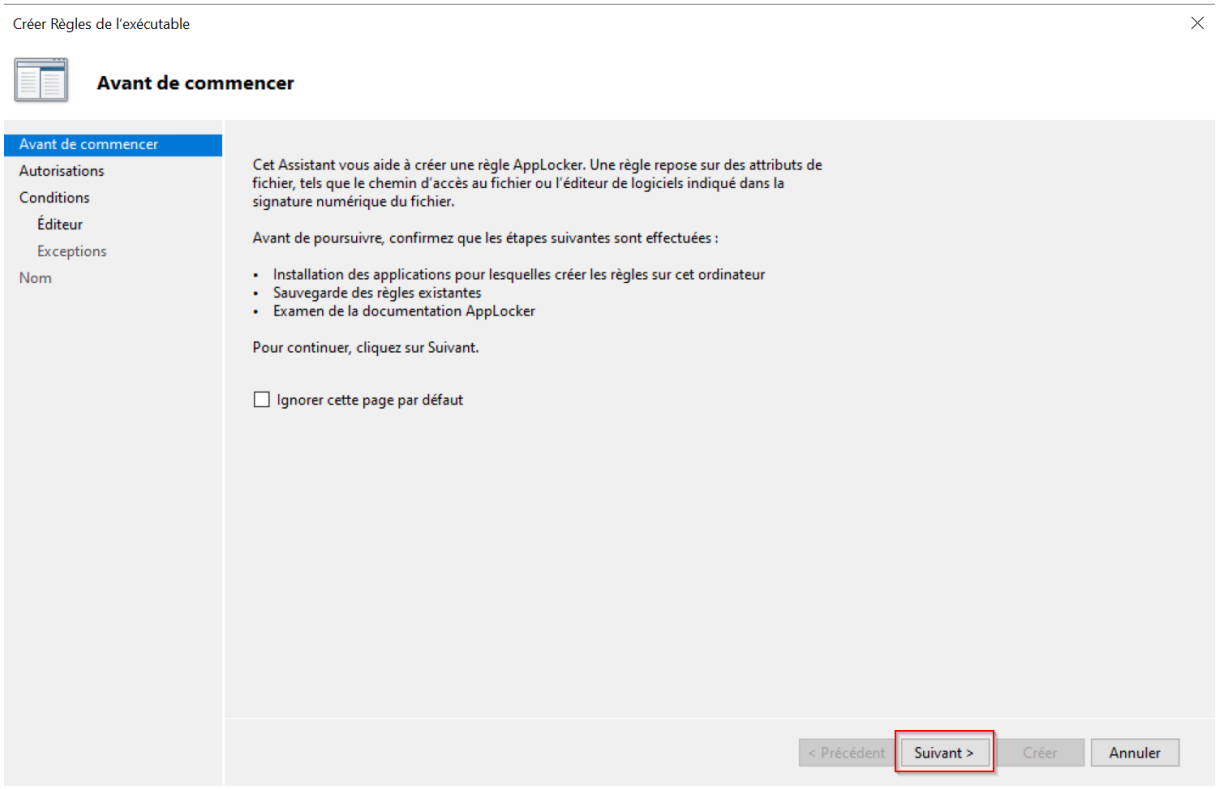




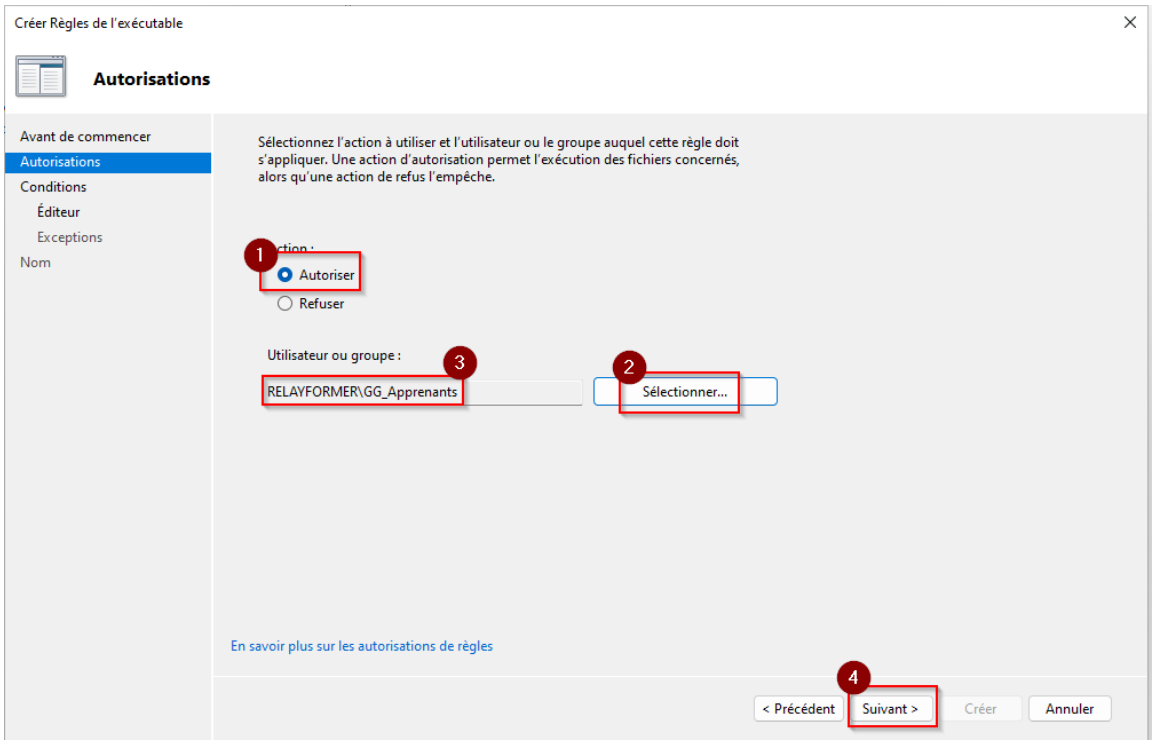
Parcourez l'arborescence comme illustré ci-dessous et vous arriverez aux paramètres d'AppLocker :



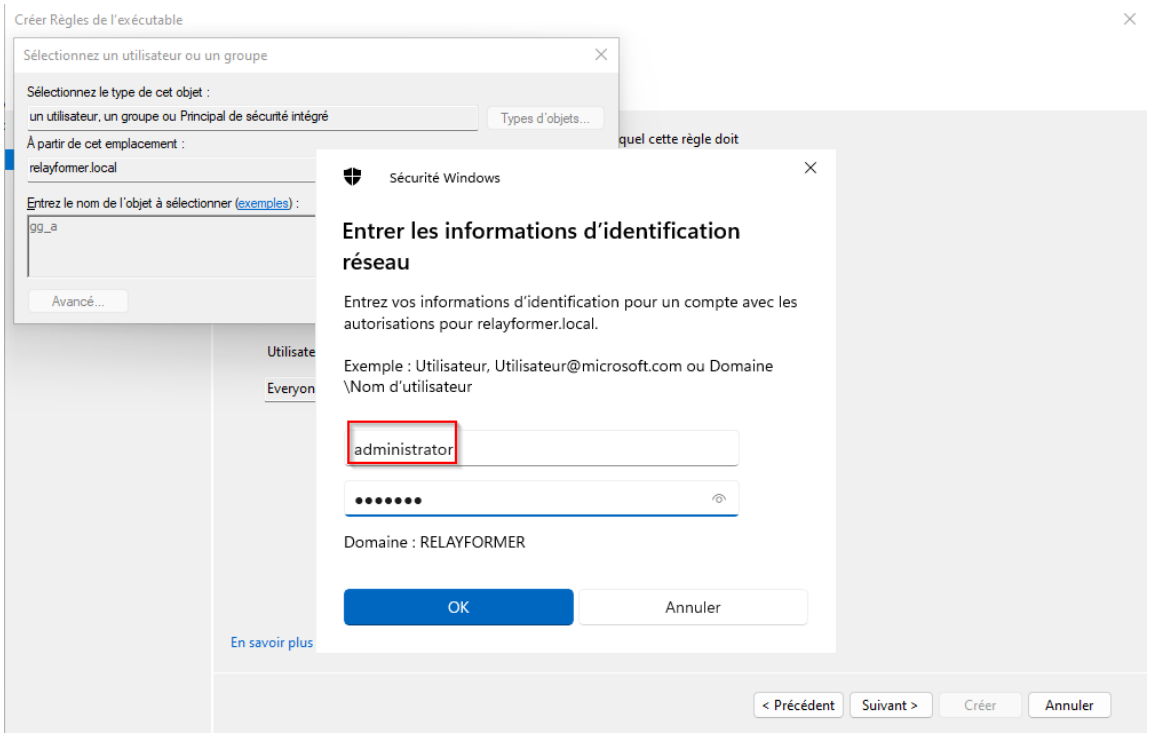
Faites un clic-droit sur « Règles de l'exécutable » puis cliquez sur « Créer une règle ».

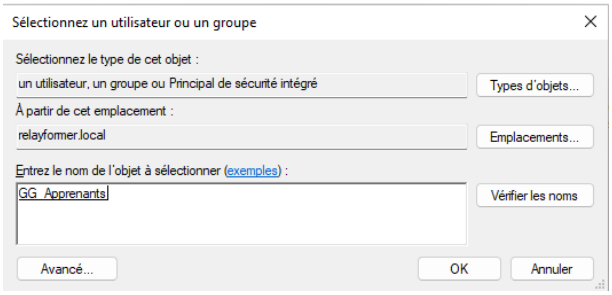


Vous allez ici définir l'action : soit « Autoriser » (principe de la liste blanche où tout ce qui n'est pas explicitement autorisé est interdit) soit « Refuser » (principe de la liste noire où tout ce qui n'est pas explicitement interdit est autorisé). Vous allez mettre en place une liste blanche car c'est plus sécurisé et puisque que vous voulez limiter la liberté d'utilisation des apprenants ciblez uniquement leur groupe.



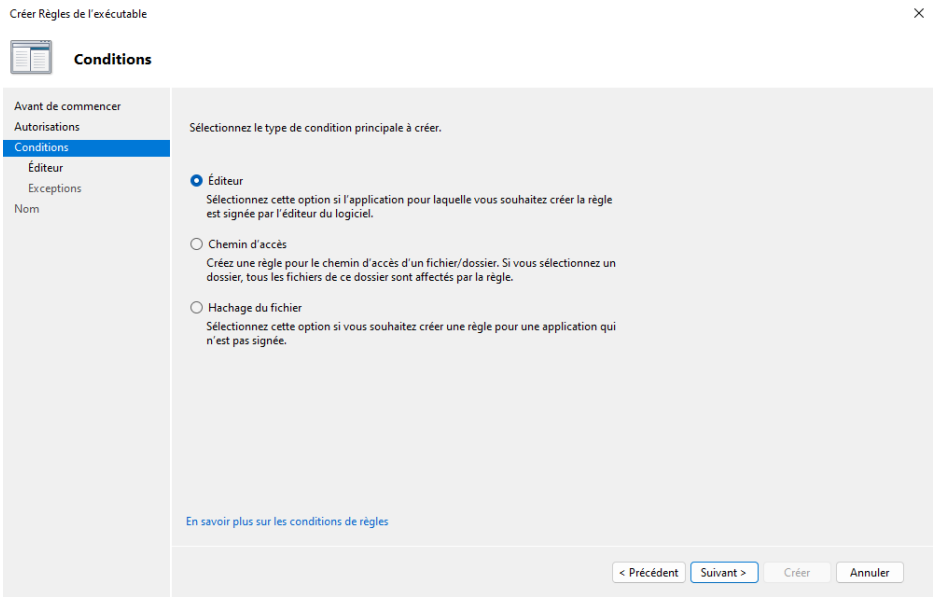
Authentifiez-vous avec le compte « administrator » pour valider l'action :



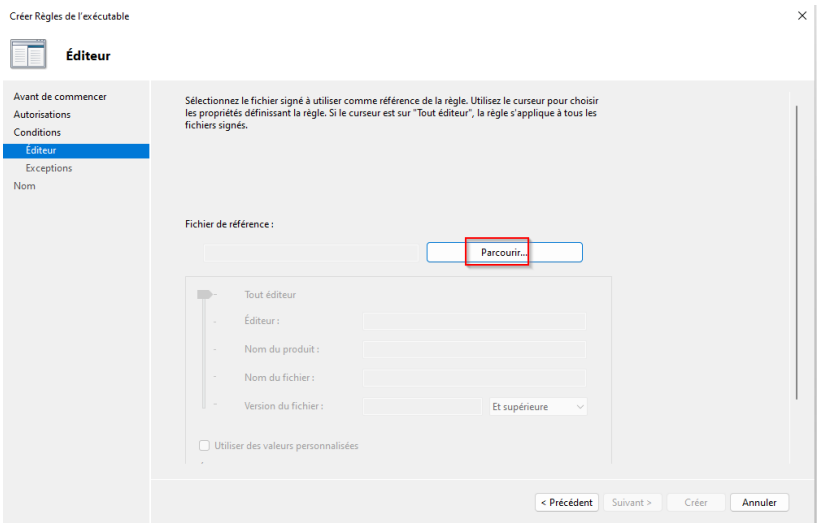


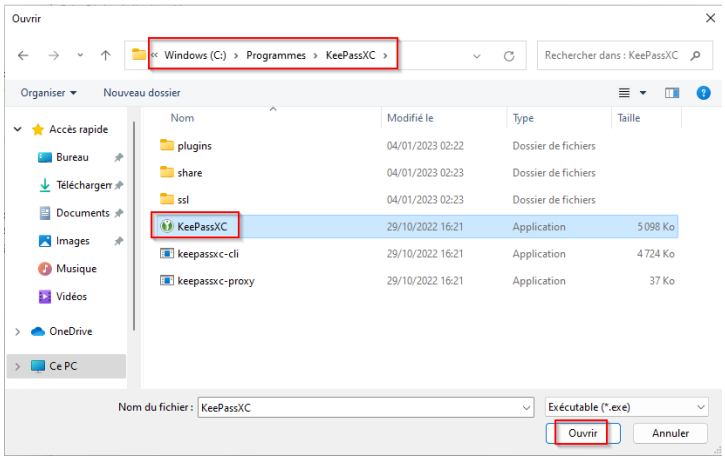
Vous avez ensuite trois types de condition principale à disposition pour créer votre règle :

1. Celle basée sur l'éditeur se base sur la signature du certificat de l'éditeur de l'exécutable et c'est celle que vous allez choisir car la règle sera dans ce cas effective quelque soit l'emplacement où se trouve l'exécutable.
2. La condition du chemin d'accès peut être ennuyeuse car si vous prenez l'exécutable et le changez d'endroit la règle ne s'appliquera plus et vous ne pourrez donc plus lancer l'application.
3. Enfin la condition du hachage du fichier peut aussi poser problème car lors des mises à jour du logiciel le hash peut changer et il faudra mettre à jour la règle à chaque fois.

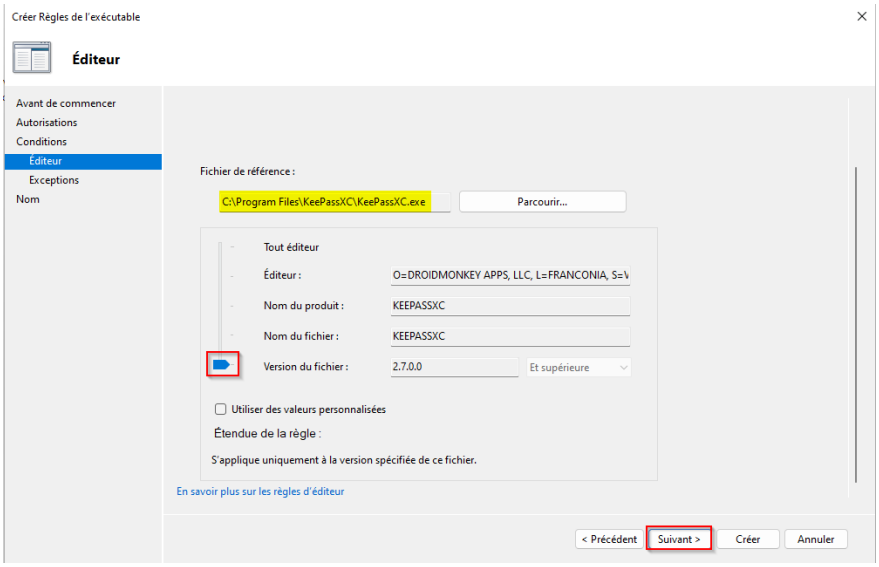


Vous devez ensuite sélectionner l'exécutable concerné (en général dans le dossier « Program Files »)

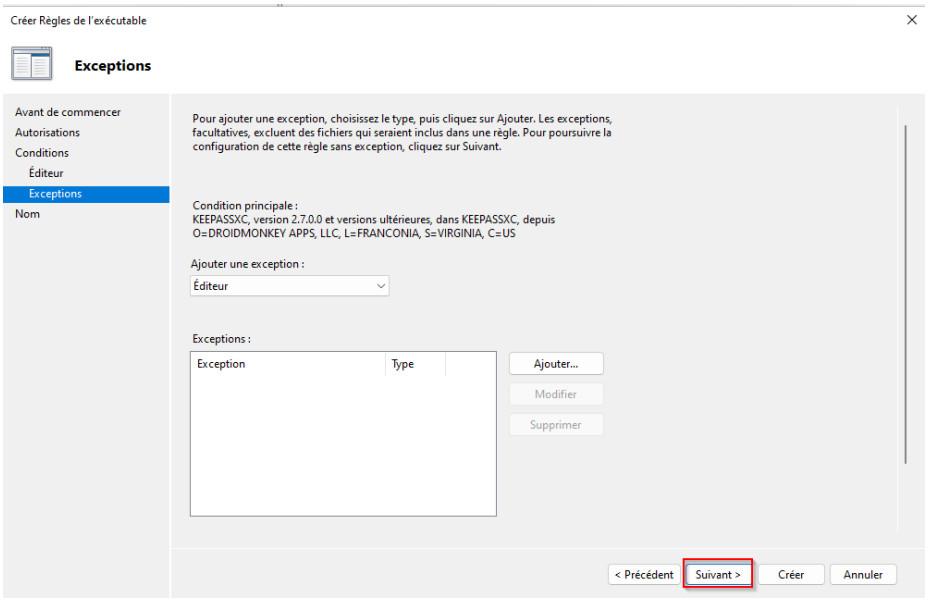




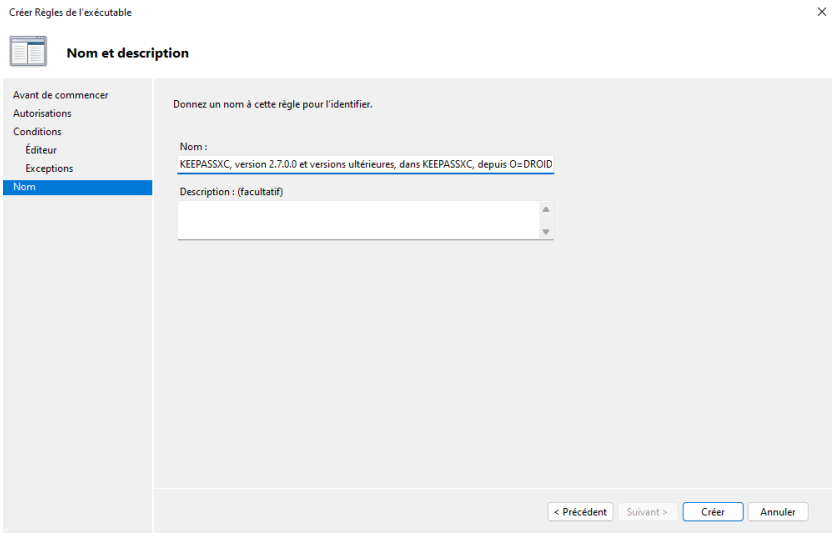
Vous remarquerez que vous pouvez jouer avec le curseur pour cibler toutes les versions du logiciel y compris celles à venir ou une seule en particulier.



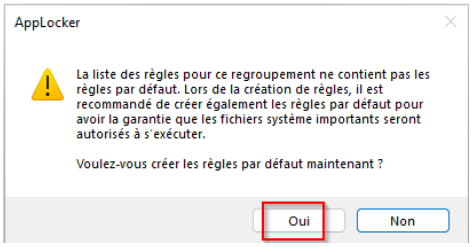
Vous pouvez ensuite mettre des exceptions à la règle. Vous n'en avez pas besoin, cliquez sur « Suivant »



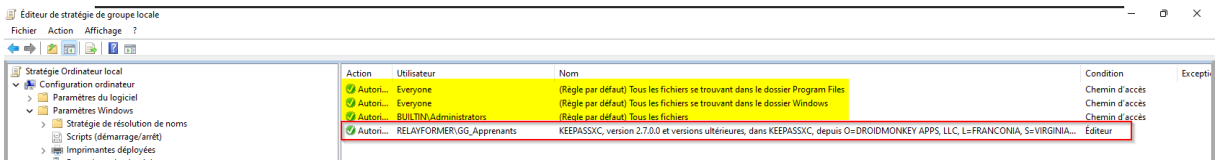
Vous pouvez ensuite renommer la règle et lui donner une description si vous le souhaitez, puis cliquez sur « Créér » :



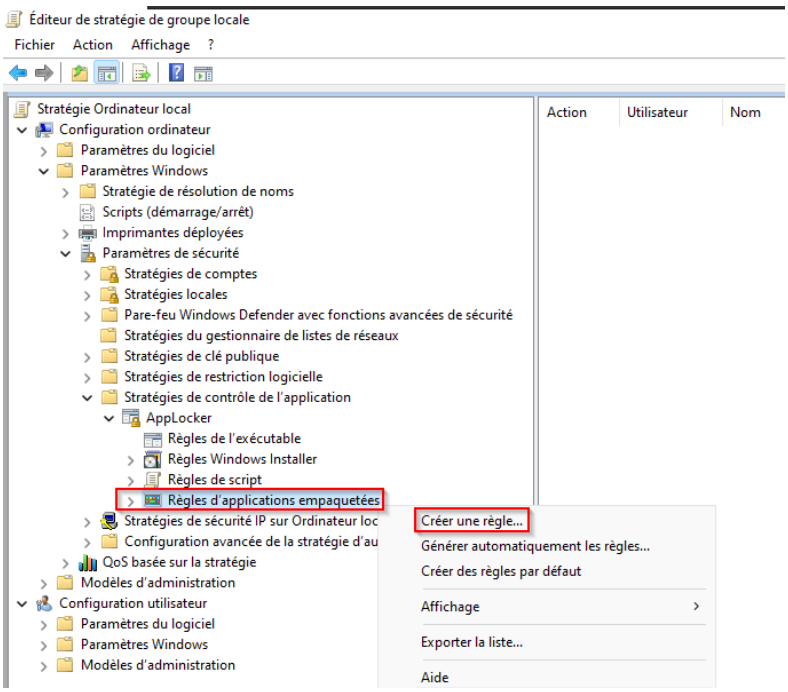
L'assistant vous propose ensuite de mettre en place des règles par défaut qui permettent aux membres du groupe « Tout le monde » (*Everyone*) d'exécuter les applications se trouvant dans les dossiers *Program Files* et *Windows* et qui permettent aux membres du groupe « Administrateurs » local d'exécuter toutes les applications. Vous pouvez les accepter.

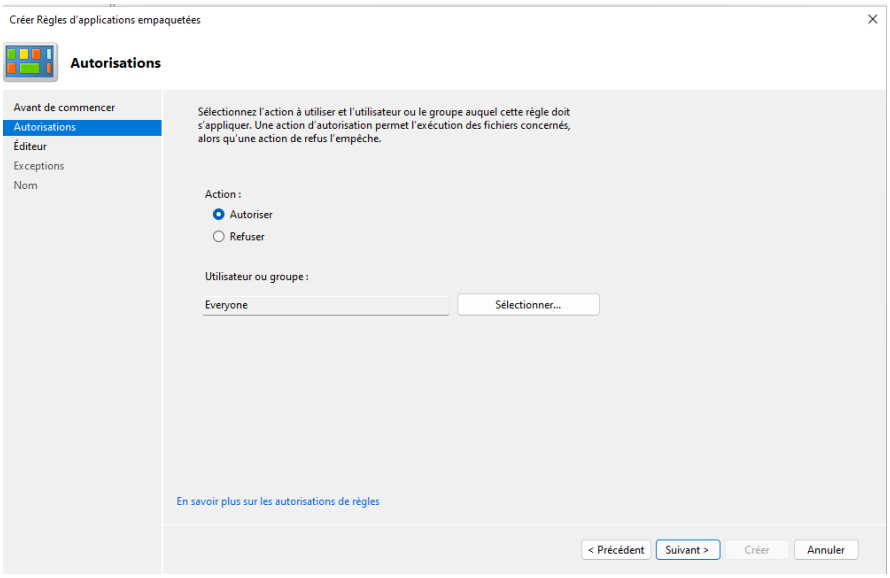


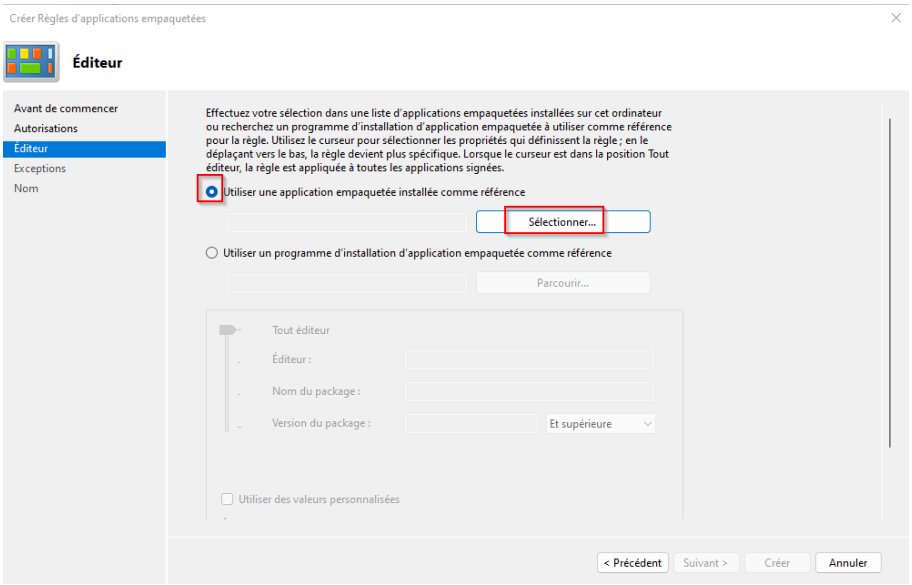
Vous retrouvez ensuite vos règles :

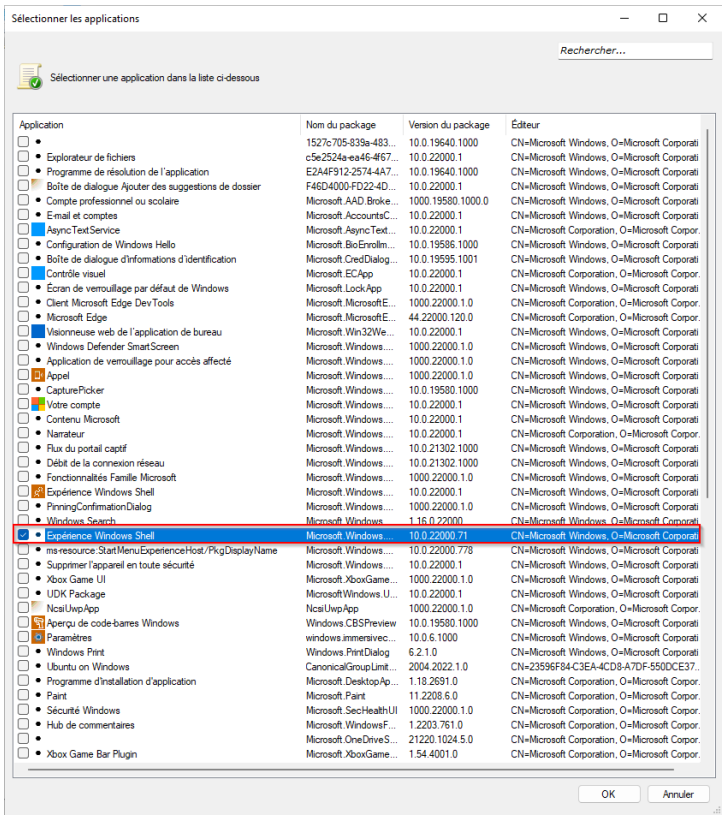


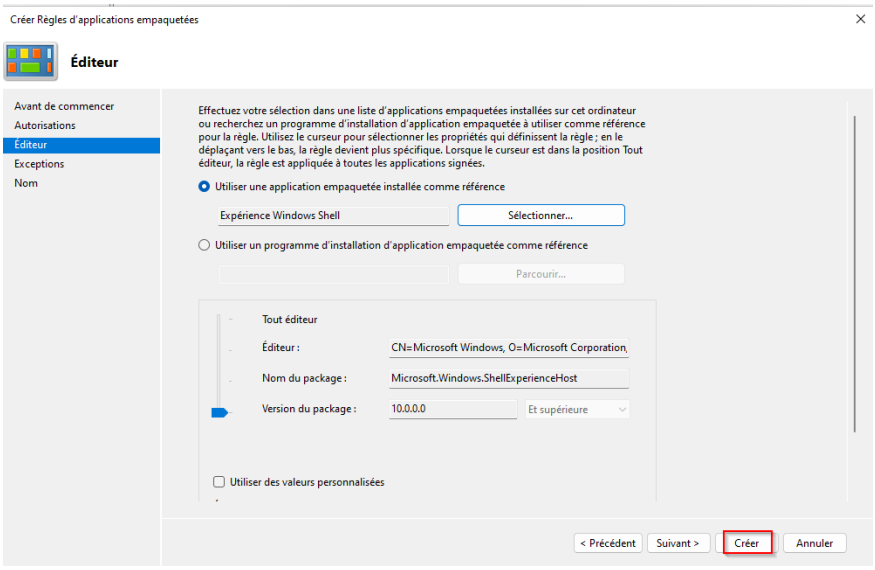
Vous devez aussi créer une règle pour « Expérience Windows Shell » sinon vous aurez des dysfonctionnements en appliquant vos stratégies AppLocker sur vos postes Windows 10 et 11. Il est donc important d'autoriser cette application. Cliquez sur « Règles d'applications empaquetées » et sur « Créer une règle… » :

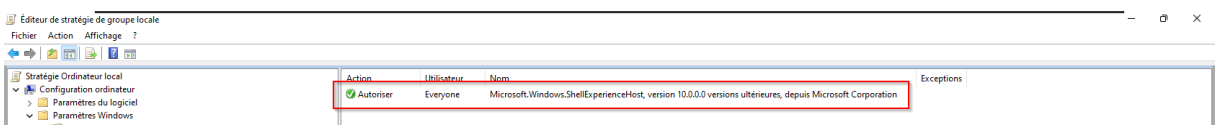






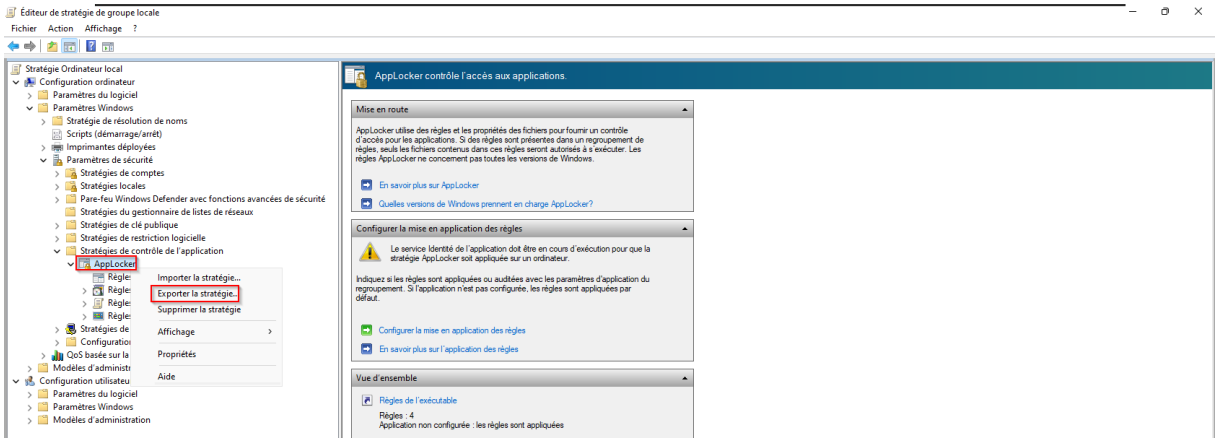


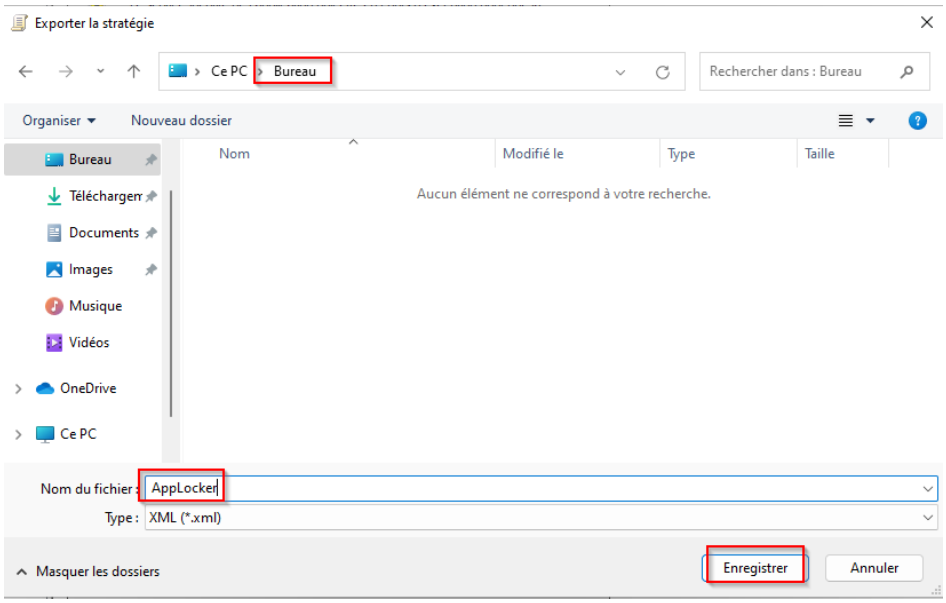




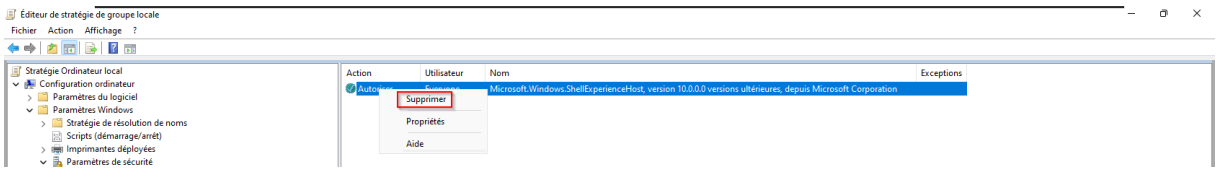
5.3.3 Exporter la GPO AppLocker

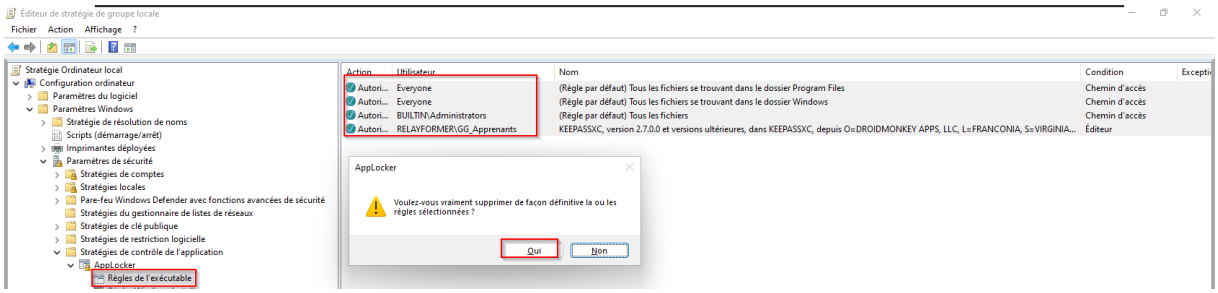
Faites un clic droit sur le paramètre AppLocker, puis cliquez sur « Exporter la stratégie… »





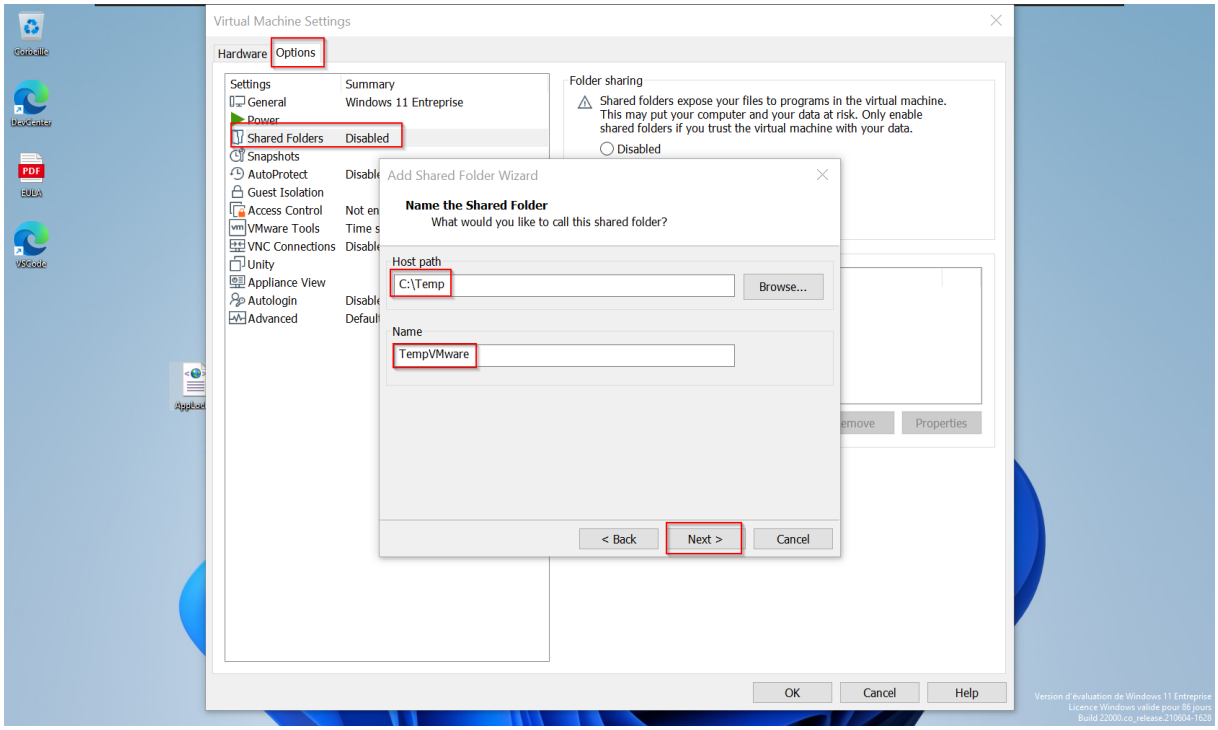
Une fois vos règles locales exportées vous devez toutes les supprimer du poste Windows 11 car elles vont être importée dans le serveur et appliquées via la stratégie de groupe.



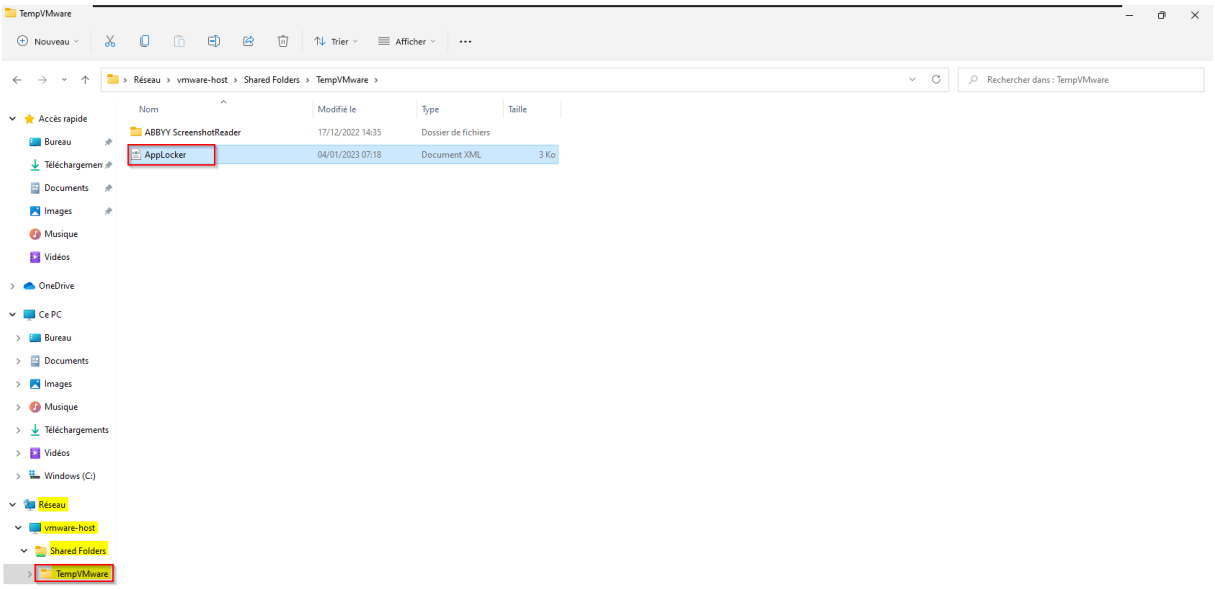


5.3.4 Importer la GPO AppLocker

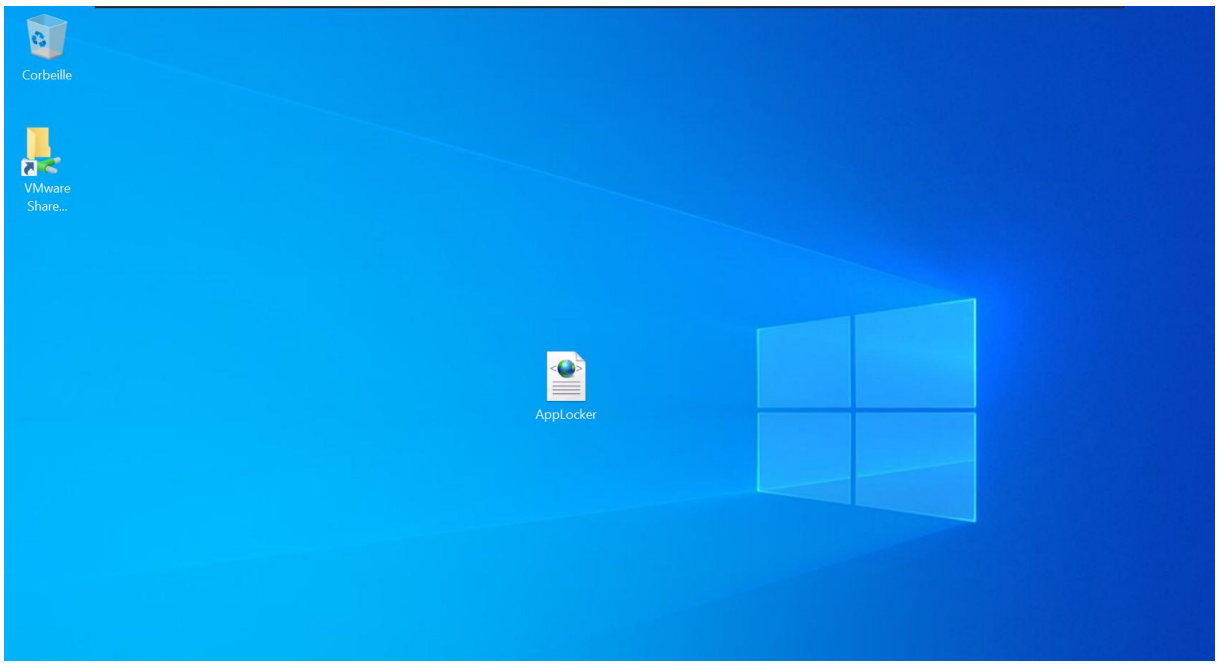
Ensuite vous pouvez copier le fichier .xml sur votre serveur en utilisant les dossiers partagés de VMware par exemple :



Collez votre fichier dans votre dossier partagé :



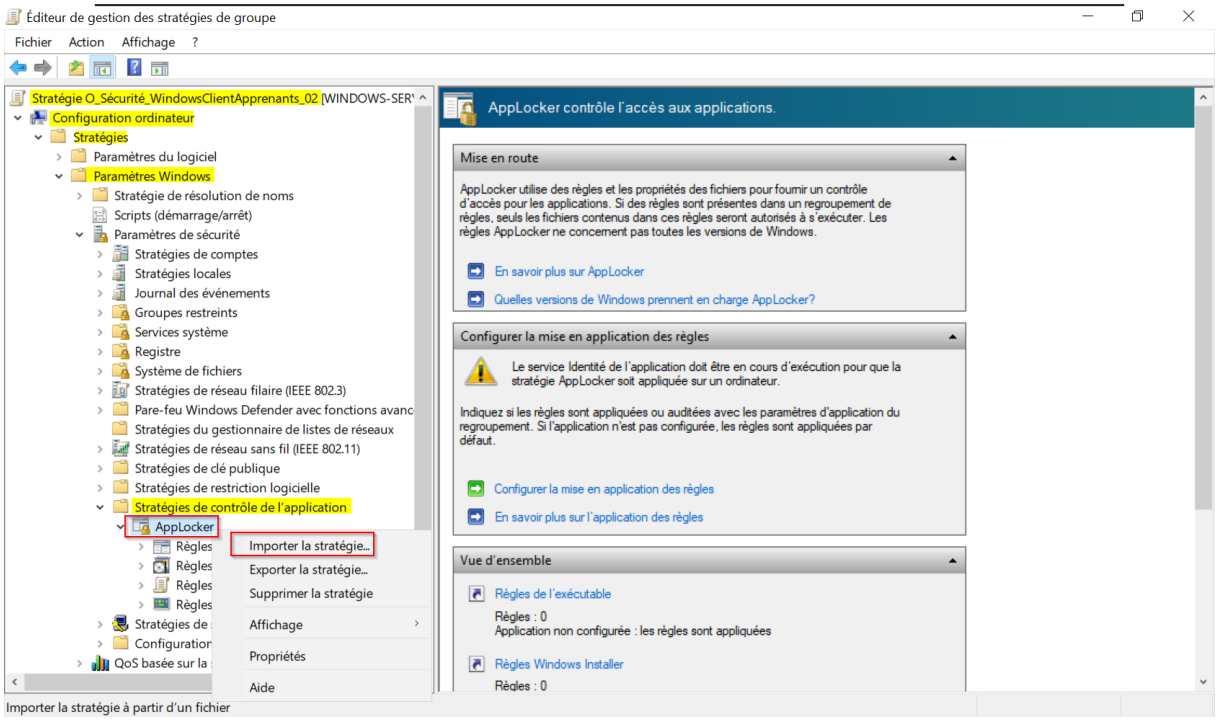
Puis glissez-le depuis le dossier de votre machine hôte vers le bureau de votre VM Windows Server par exemple :

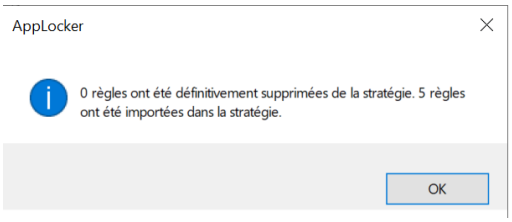


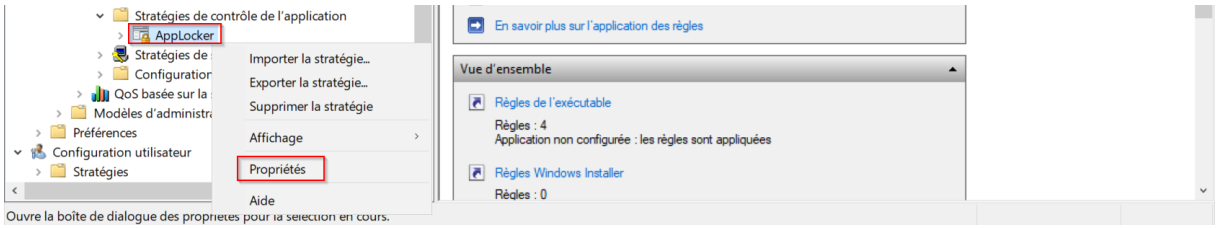
Ensuite vous ouvrez l'outil « Gestion des stratégies de groupe »

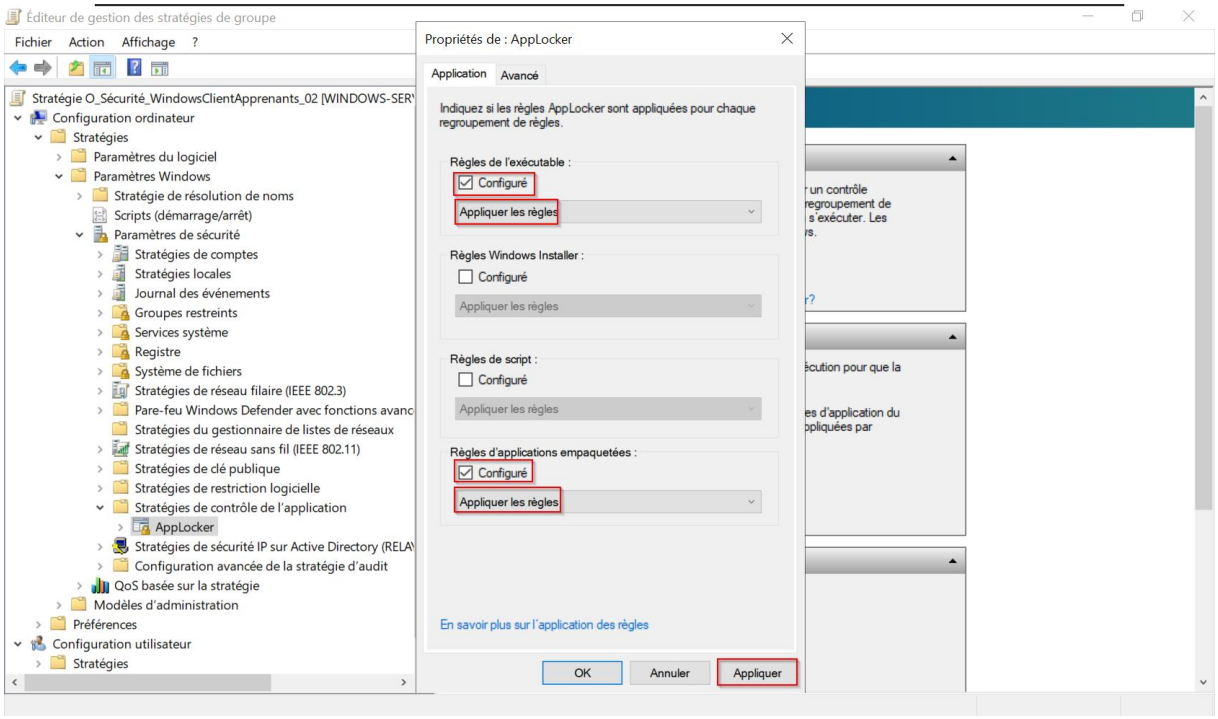
Retrouvez le conteneur « Apprenants » puis créez-y une GPO que vous nommerez « O_Sécurité_WindowsClientApprenants_02 » :

Une fois créée effectuez un clic-droit dessus et sélectionnez « Modifier ». Retrouvez AppLocker dans l'arborescence :



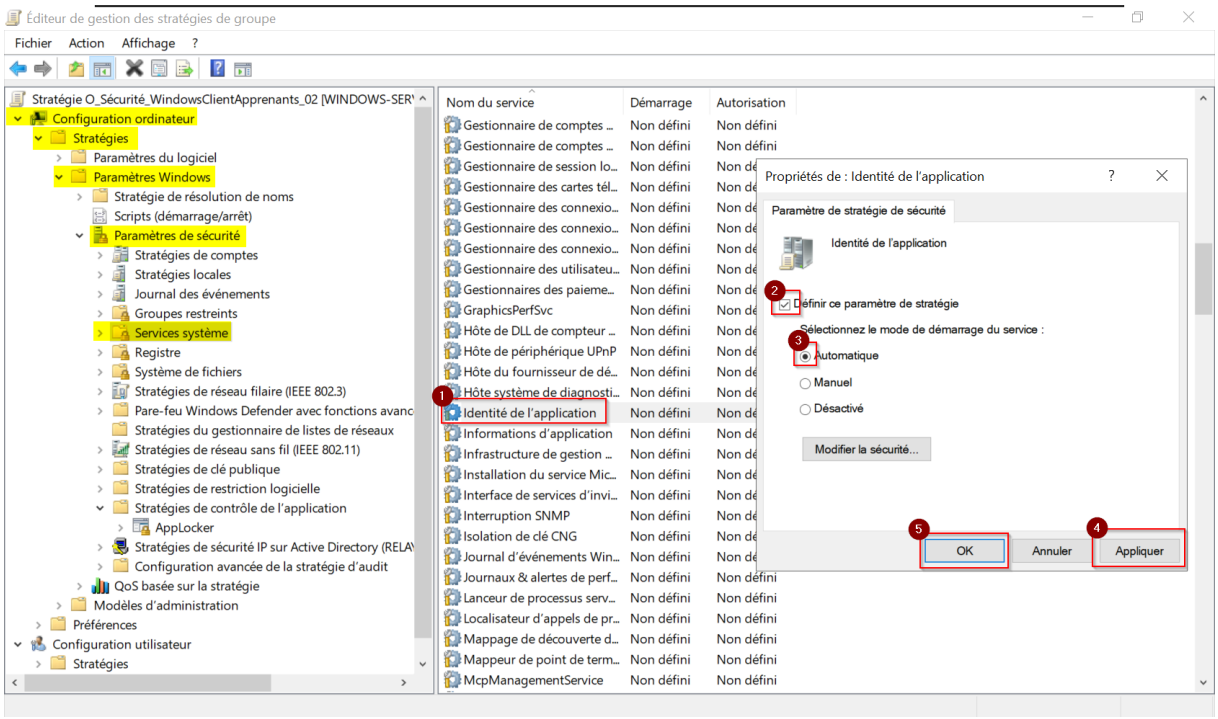






5.3.5 Configurer le service « Identité de l'application »

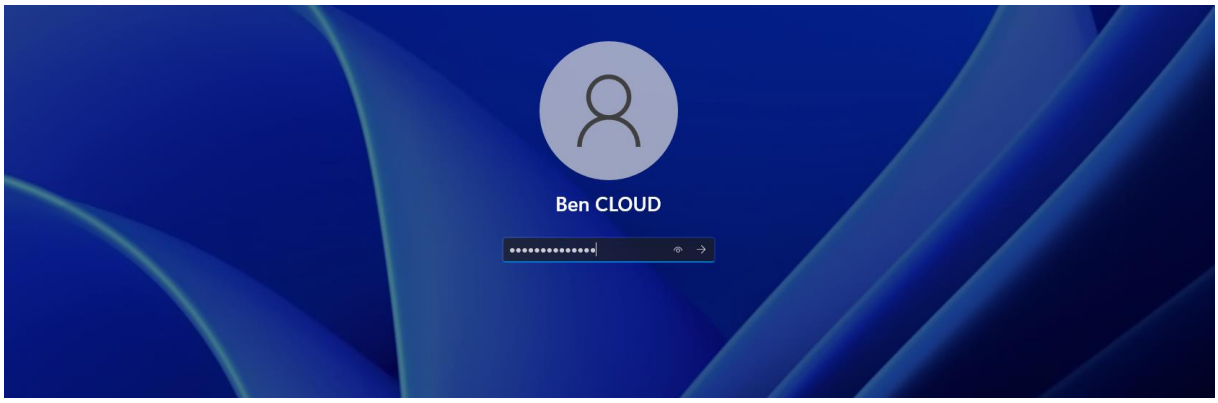
AppLocker s'appuie sur le service « Identité de l'application » pour fonctionner, il faut donc activer le démarrage automatique de ce service :



A partir de ce moment-là AppLocker est correctement configuré et va s'appliquer sur votre poste Windows 11.

5.4 Tester la bonne application de la GPO

Retournez sur votre poste client Windows 11, redémarrez votre machine et connectez-vous avec un compte utilisateur du domaine AD (c'est-à-dire celui d'un apprenant sur lequel s'applique la GPO et non pas le compte local « User ») :

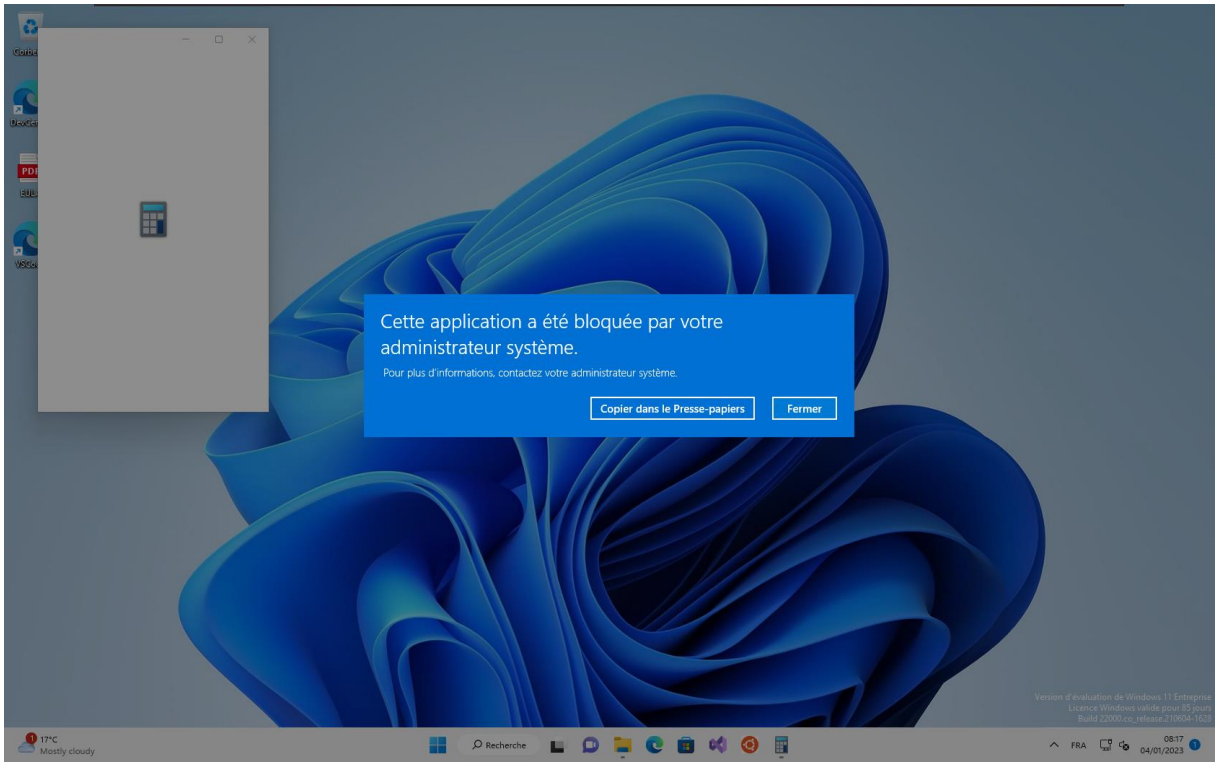


Cela peut prendre un peu de temps pour que la GPO s'applique sur les objets AD. Pour forcer la mise à jour des GPO sur un poste client vous pouvez utiliser la commande dans l'invite de commande :

```
gpupdate /force
```

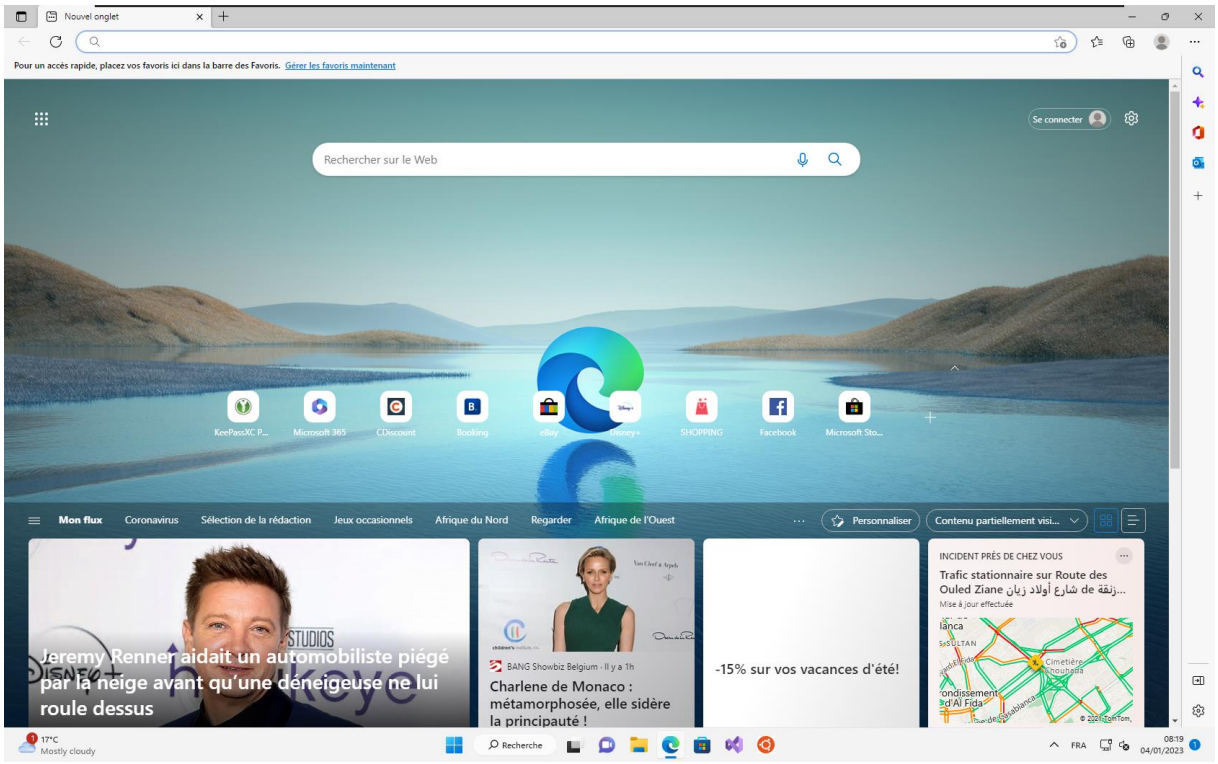
```
C:\Users\ben.cloud>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

Maintenant essayez de lancer une application qui n'est pas préalablement autorisée comme « Microsoft Store », « Caméra », « Editeur de vidéo », « Bloc-Notes », « Paint » ou « Calculatrice » par exemple. Vous obtiendrez ce message d'erreur :

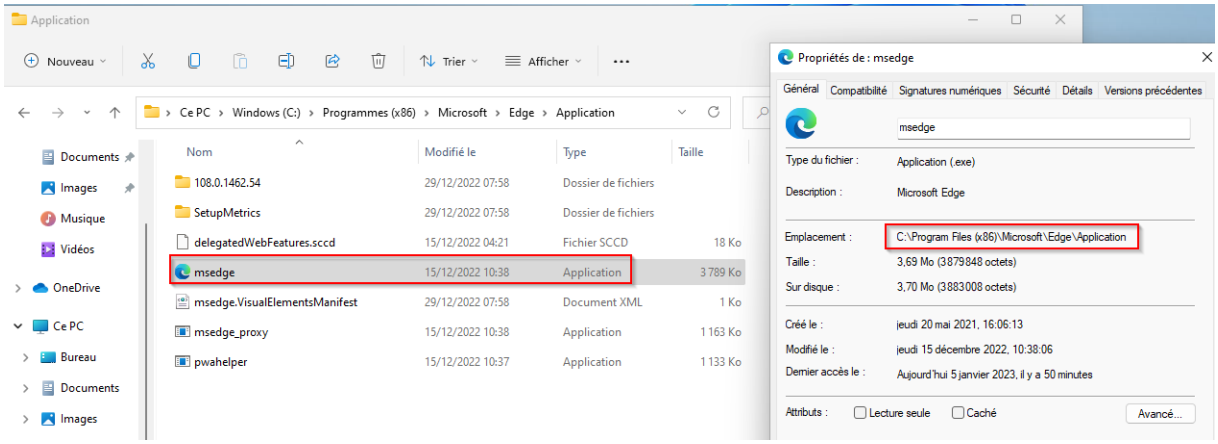


En effet ces applications Windows ne sont pas concernées par les règles par défaut que nous avons importées et qui autorisent uniquement les programmes installés dans le dossier « Windows » et le dossier « Program Files ».

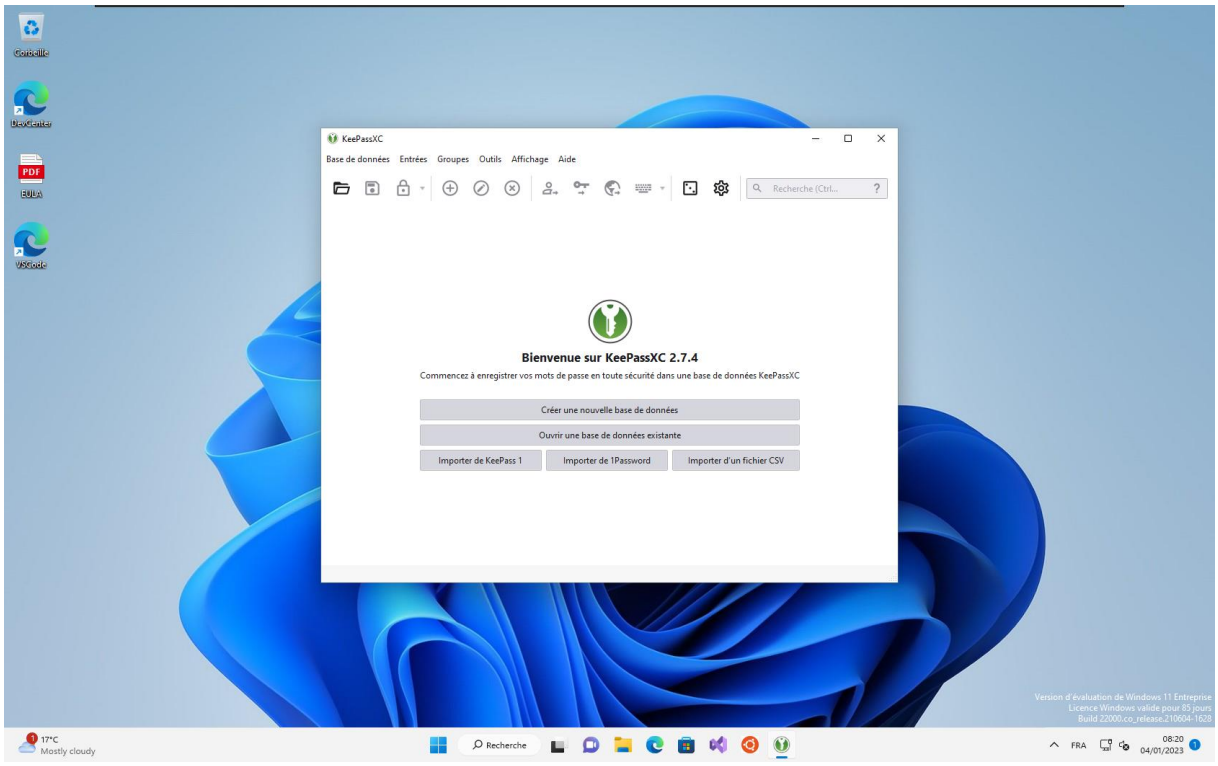
Essayez de lancer Microsoft Edge maintenant :



C'est autorisé car Edge est installé dans le dossier « Program Files » :



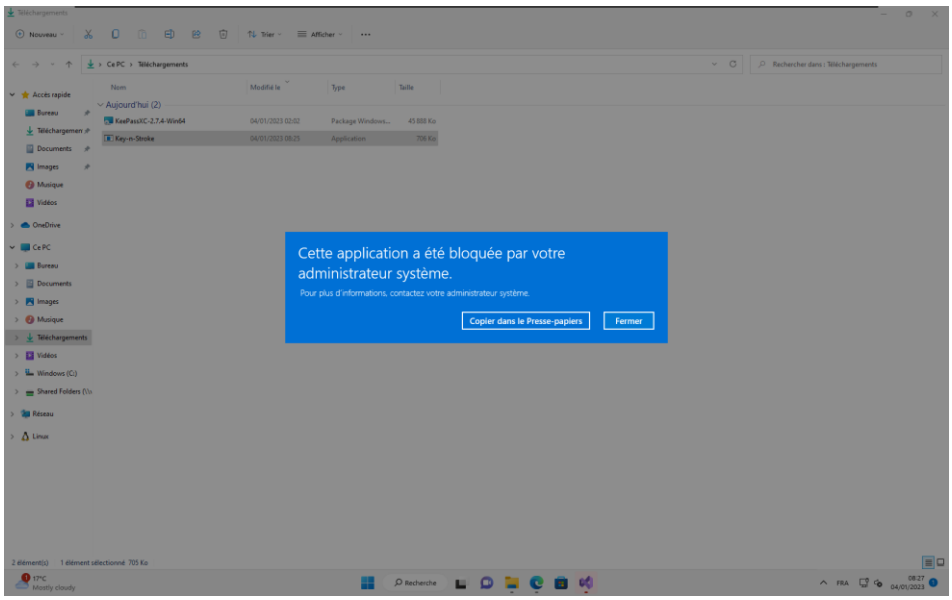
Lancez KeePassXC :



C'est aussi autorisé par notre GPO AppLocker puisqu'il a été sécifiquement autorisé et qu'il fait en plus partie des logiciels installés dans le dossier « Program Files ».

Essayez maintenant de télécharger et d'exécuter une application portable qui pourrait être un logiciel malveillant (mais qui n'en est pas un dans notre exemple) telle que Key-n-Stroke (qui permet d'afficher à l'écran nos frappes de clavier et nos clics de souris) :

https://github.com/Phaiax/Key-n-Stroke/raw/master/Releases/v1.1.0/Key-n-Stroke.exe



L'exécutable n'est pas autorisé. Vous avez réussi à sécuriser un poste Windows 11 via les GPO et Active Directory.