

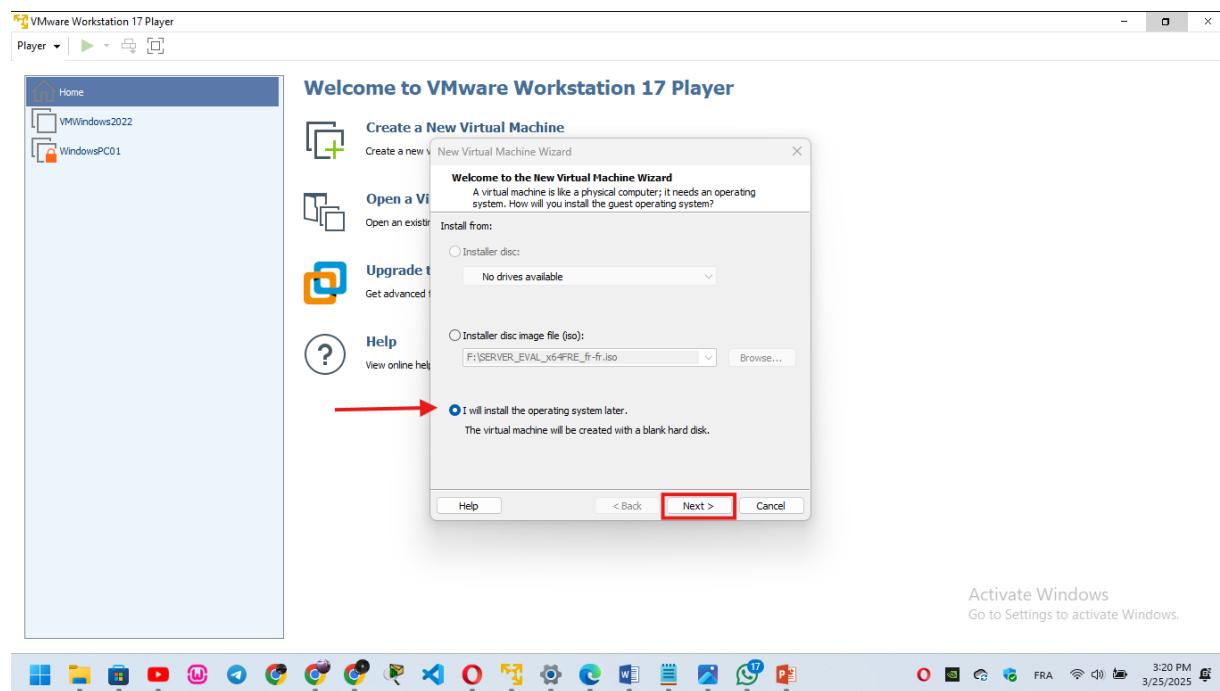
Installation Centralisée de Kaspersky Endpoint Security (KES) avec Kaspersky Security Center (KSC)

Environnement Technique

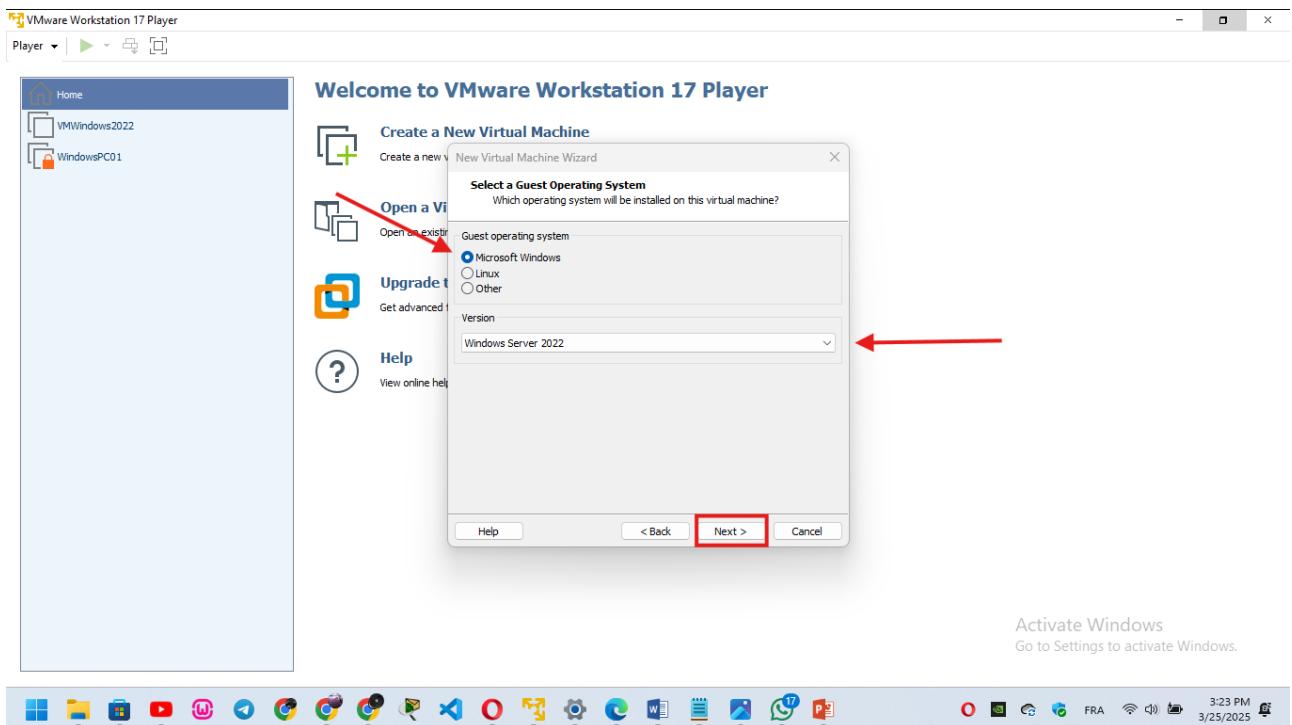
- Hyperviseur : VMware Workstation 17 Player
- Serveur de Gestion : Windows Server 2022
- Solution : Kaspersky Endpoint Security (KES)
- Console d'administration : Kaspersky Security Center (KSC)

Prérequis Système

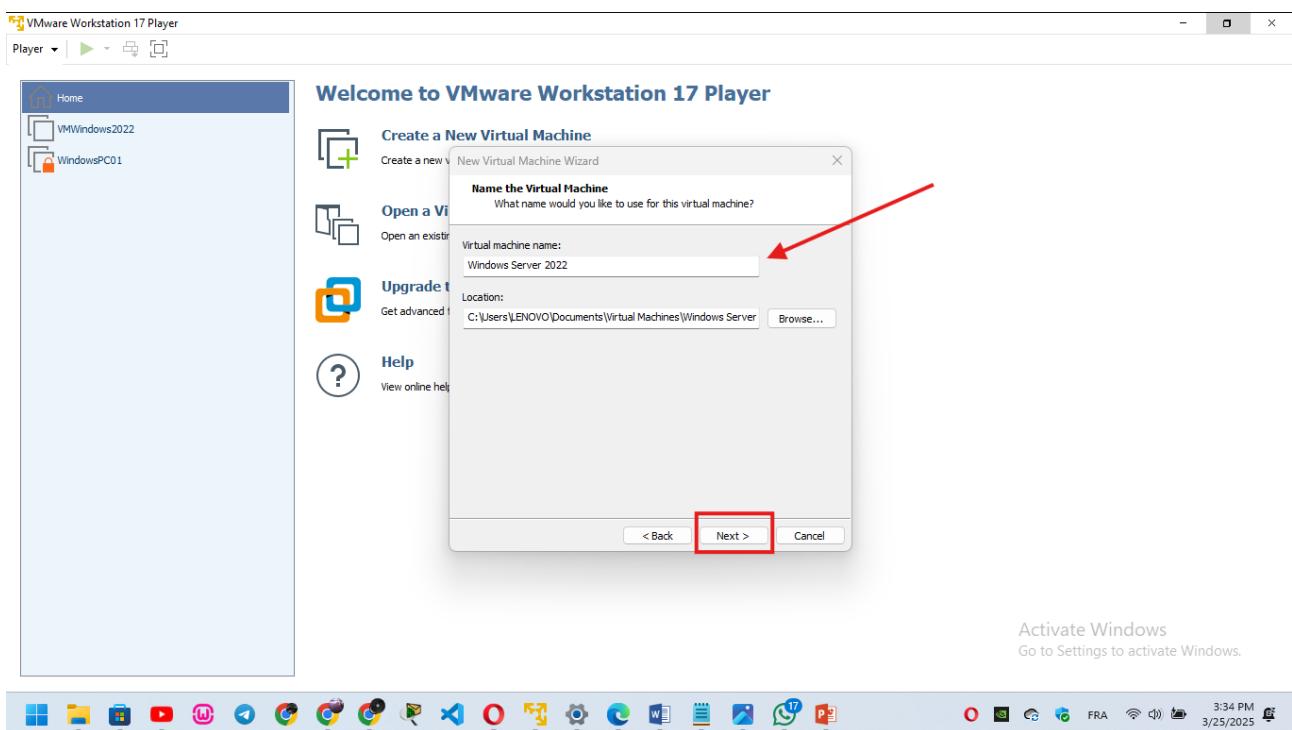
Configuration Serveur KSC



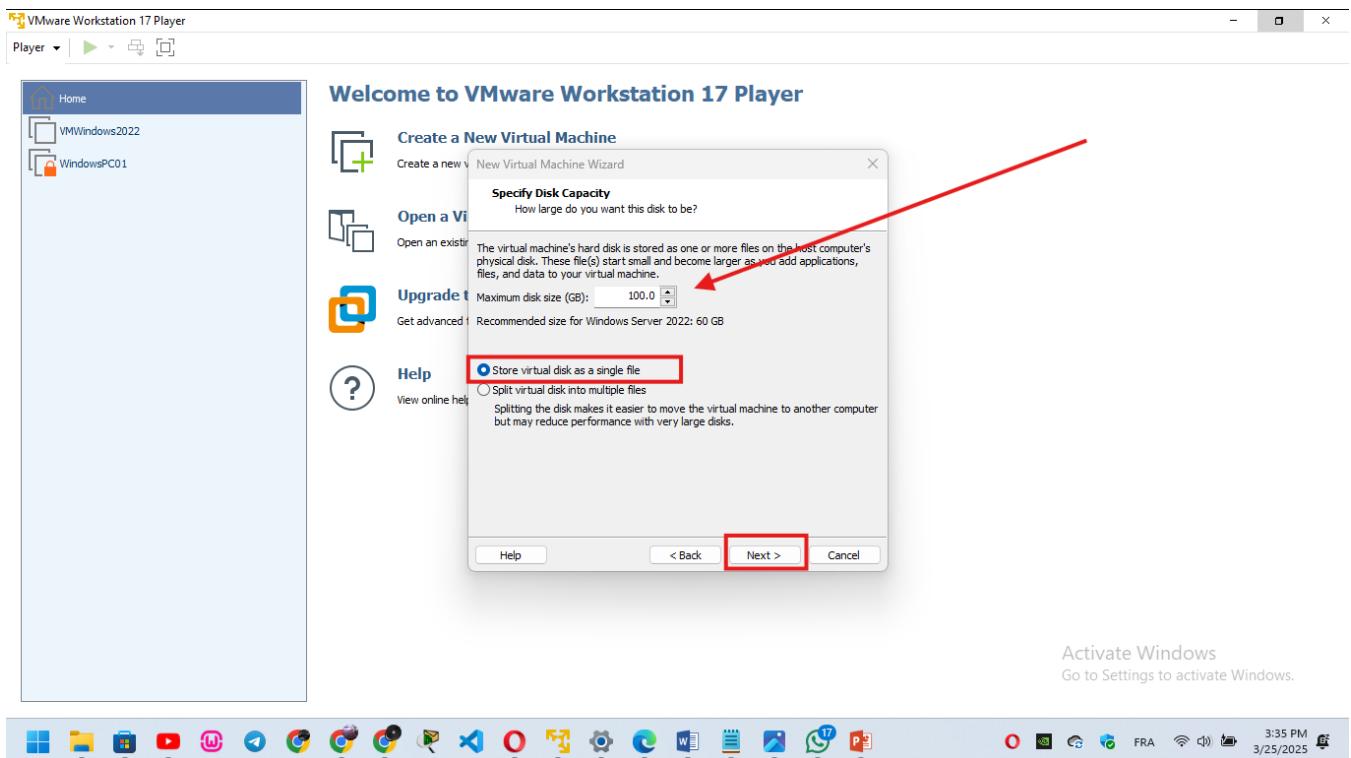
Étape 1: Cliquez sur j'installerai le système d'exploitation plus tard.



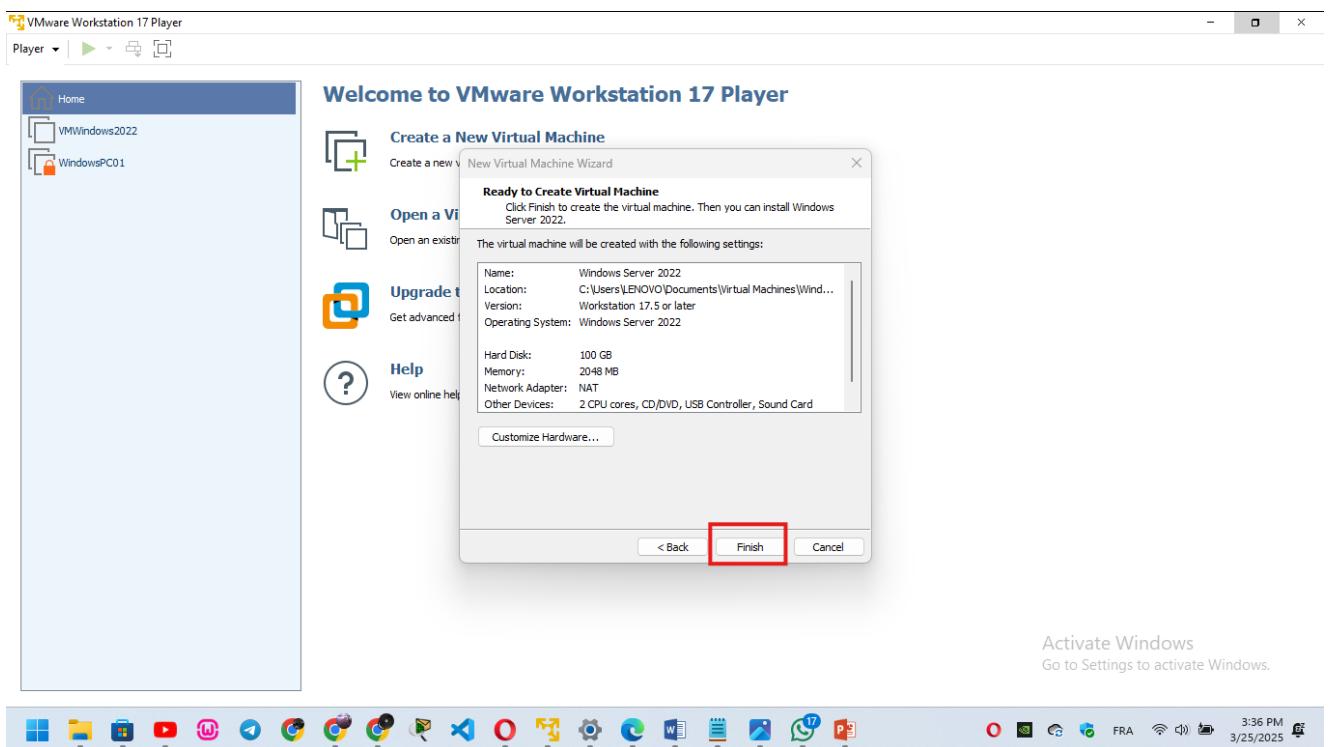
Étape 2: Sélectionnez l'option Microsoft Windows puis faites défilez la barre jusqu'à Windows server 2022.



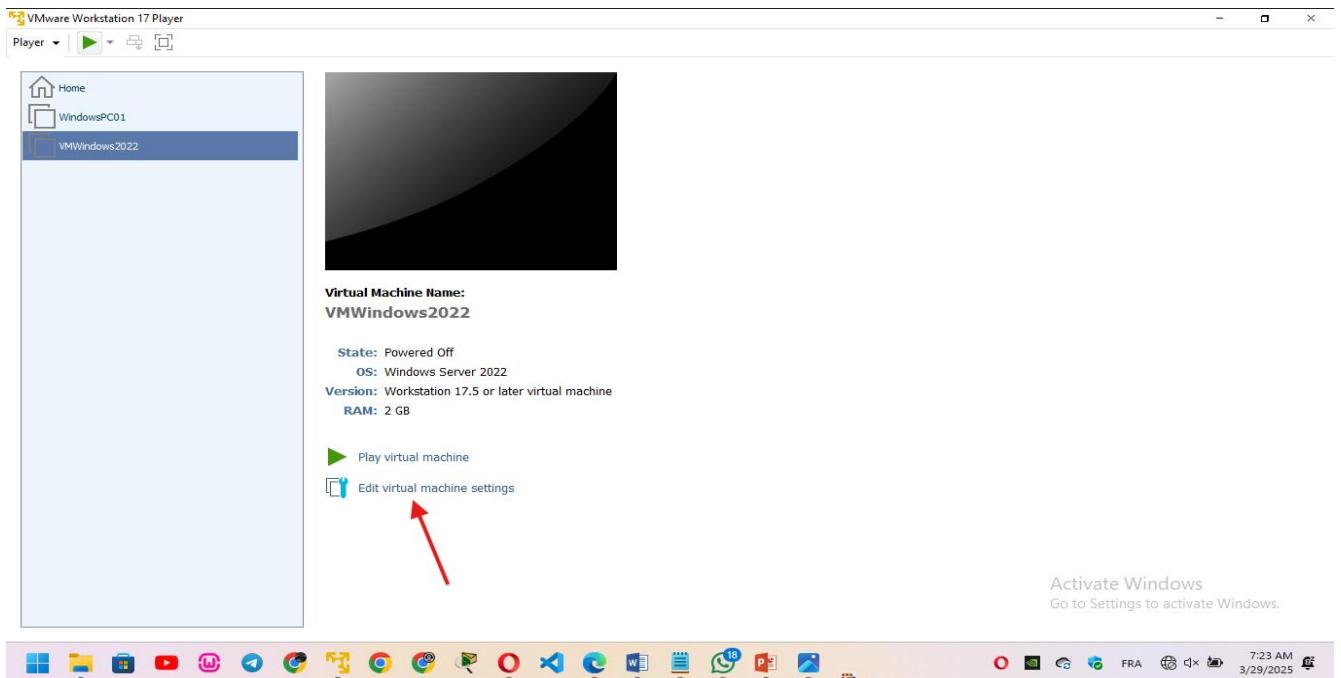
Étape 3: Donner un nom à votre VM et sélectionner un emplacement dans votre disque sinon laissez les valeurs par défaut et cliquez sur suivant.



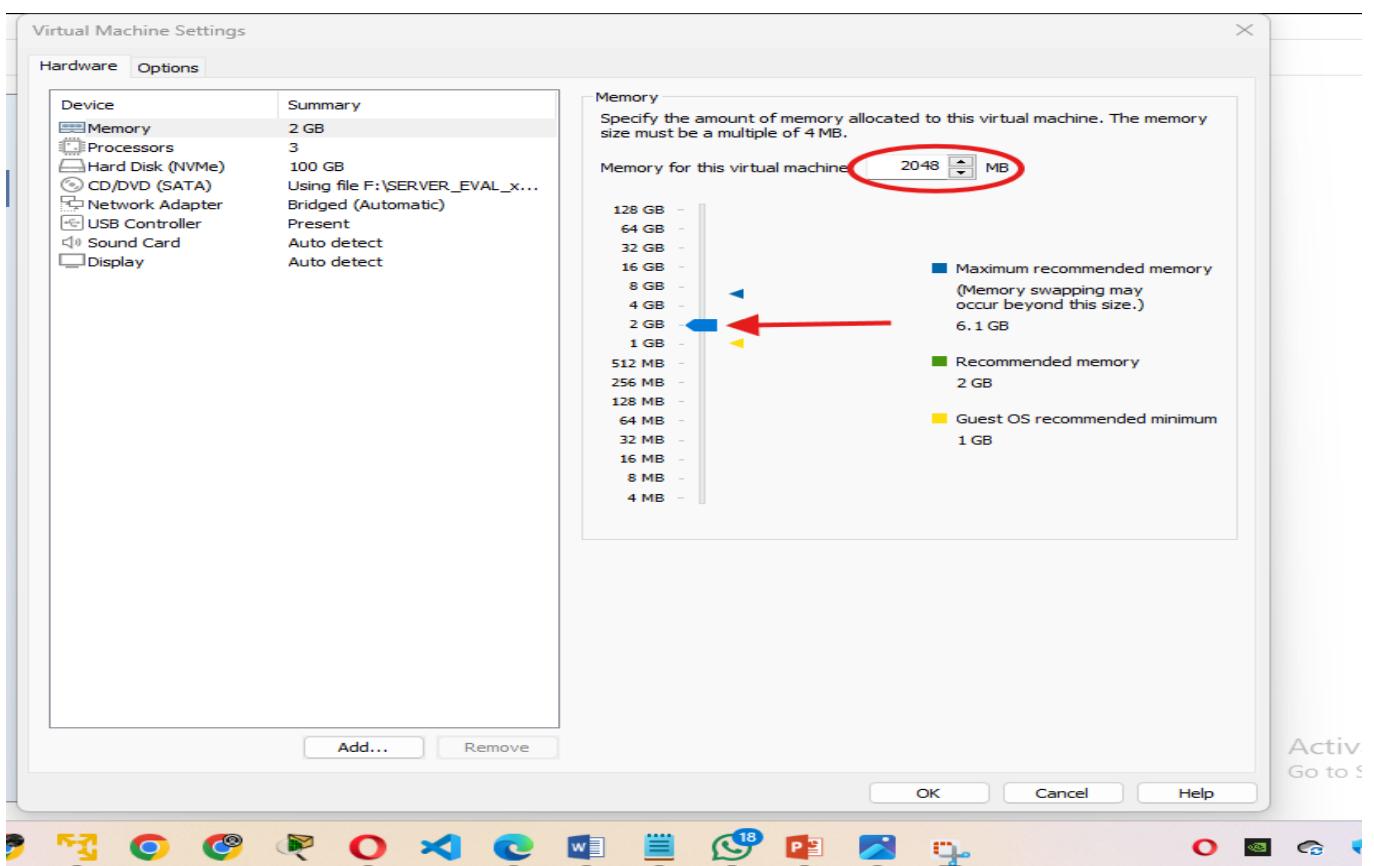
Étape 4: Donnez à la VM serveur minimum 100.0 GB d'espace disque puis sélectionnez la première option



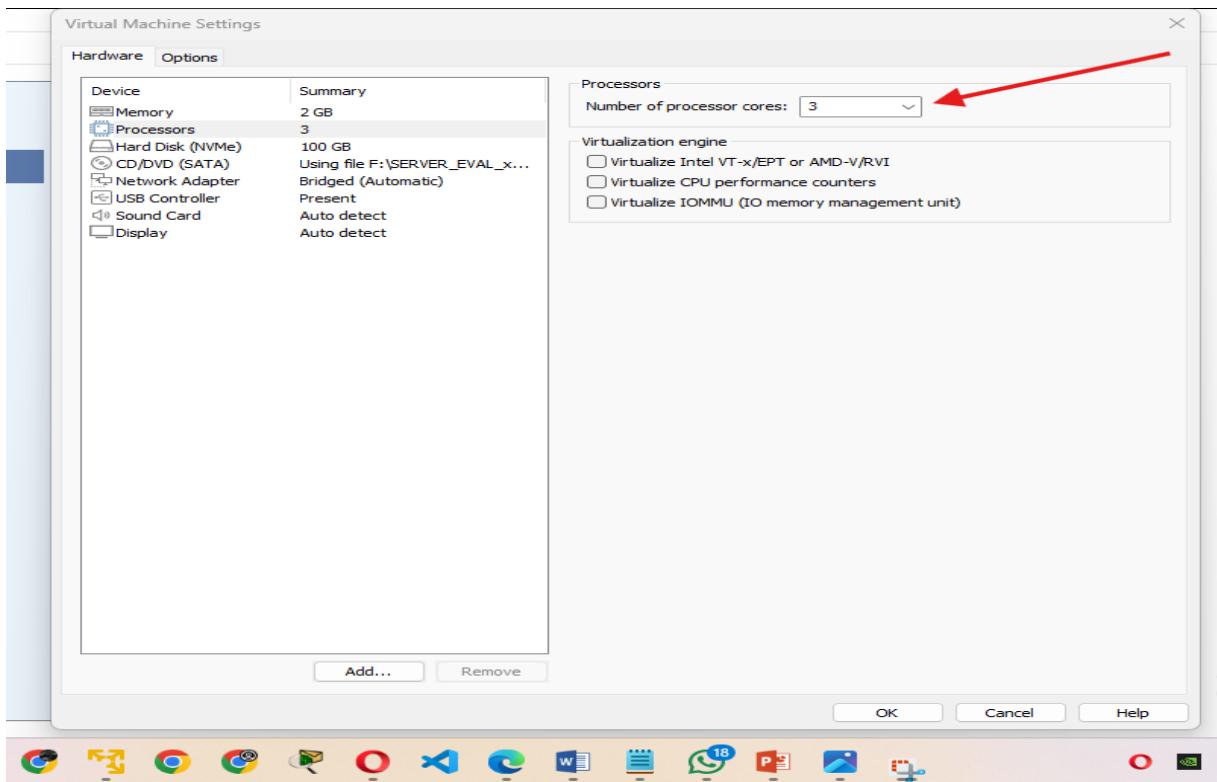
Étape 5: Si vous avez bien suivie les étapes cliquez sur terminée sinon revenez en arrière pour corrigez les problèmes.



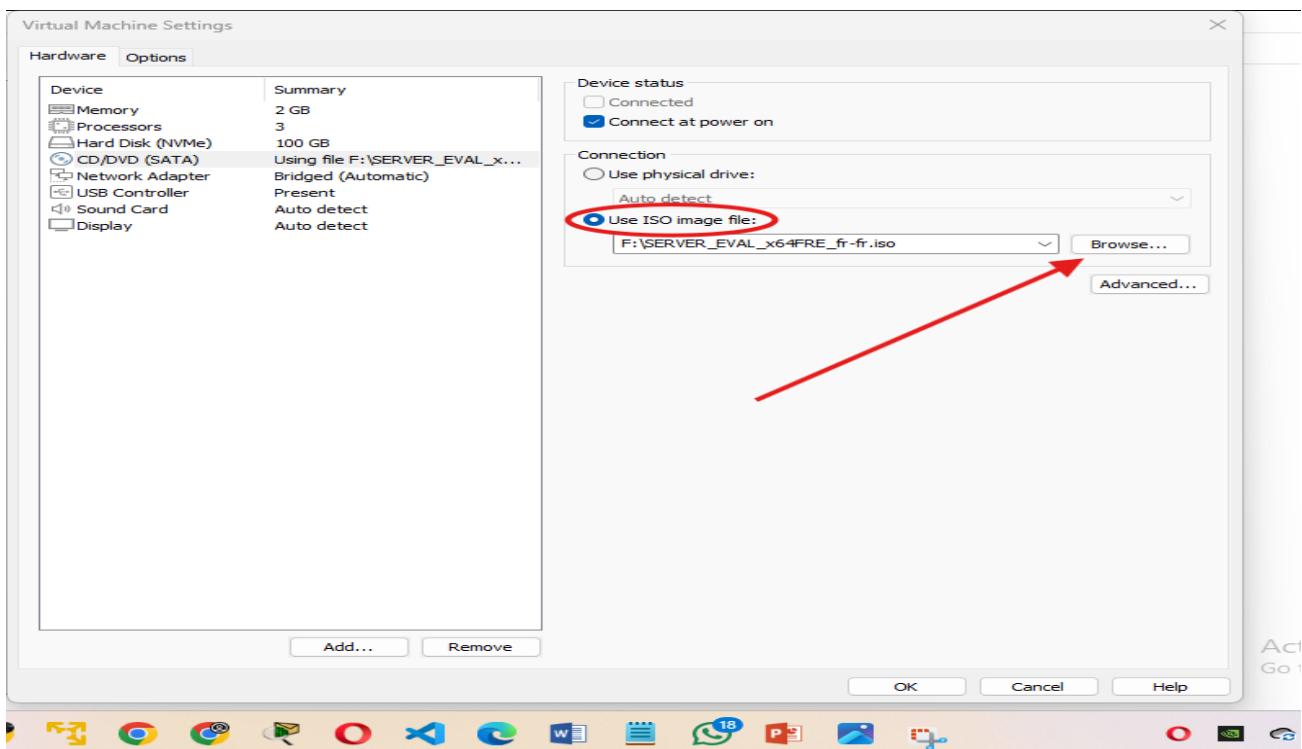
Étape 6: Après la création de votre VM cliquez sur modifier les paramètres de la machine virtuelle



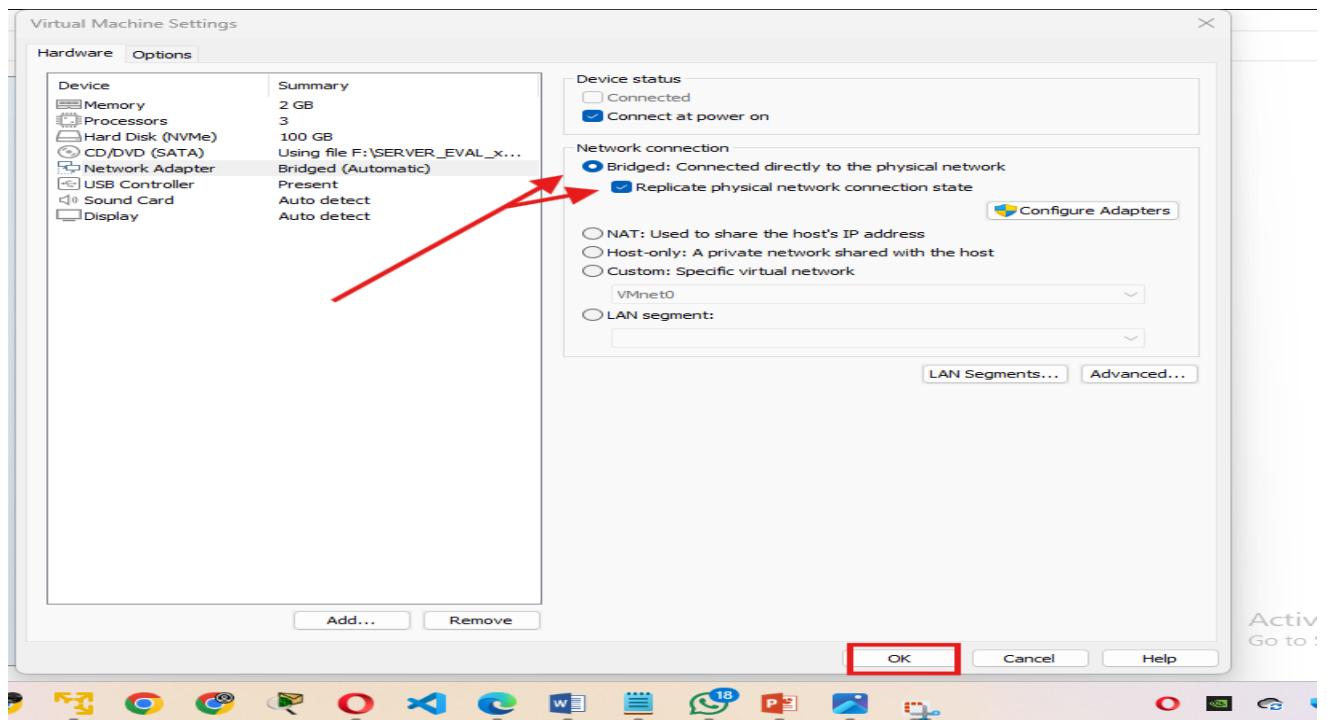
Étape 7: Dans cette section augmentez la mémoire RAM de votre VM à minimum 8GB



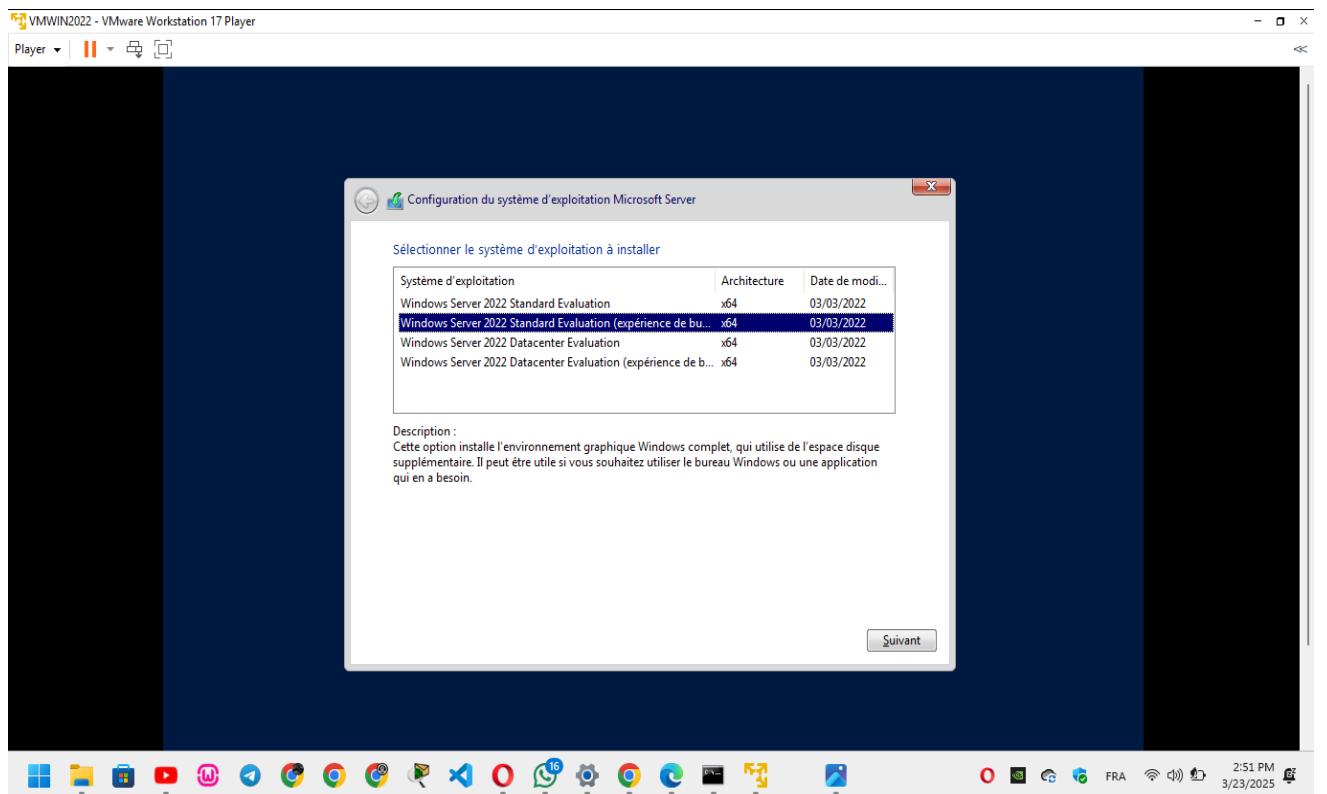
Étape 8: Puis dans cette section donnez 3 coeurs de processeurs à votre VM



Étape 9: Dans cette partie cliquez sur parcourir et sélectionner l'emplacement de votre image ISO.

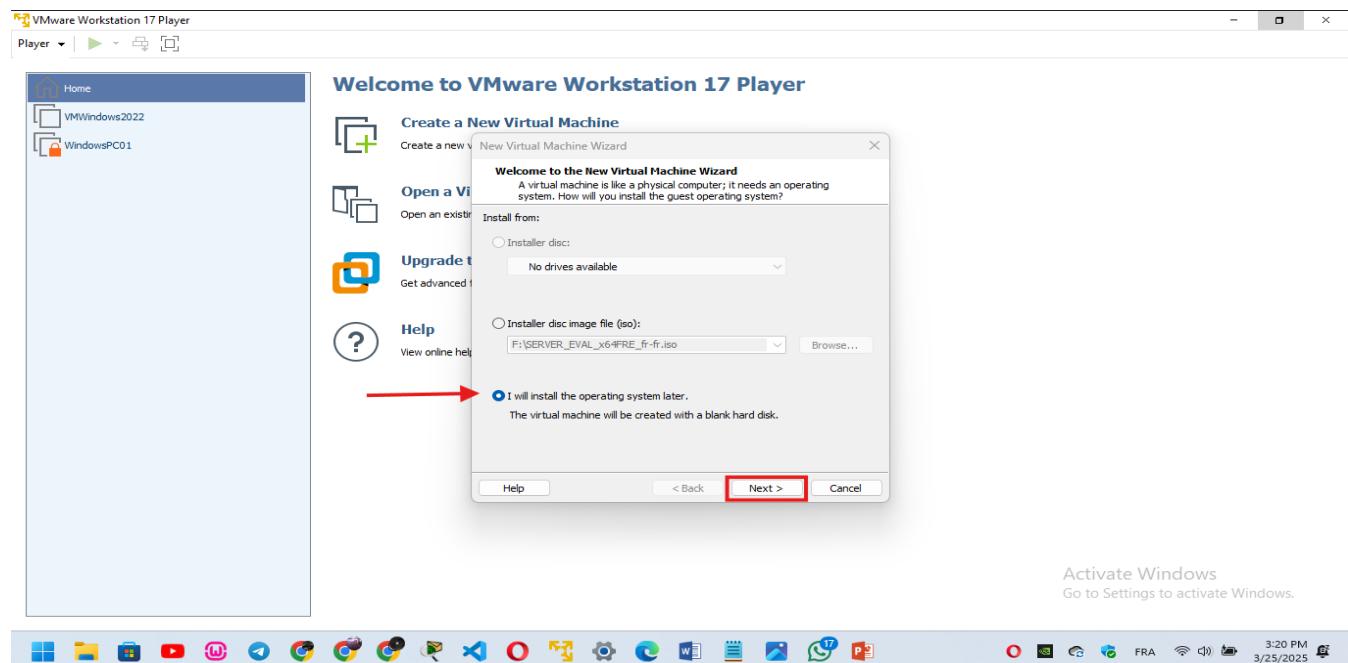


Étape 10: Sélectionnez le mode réseau Bridged

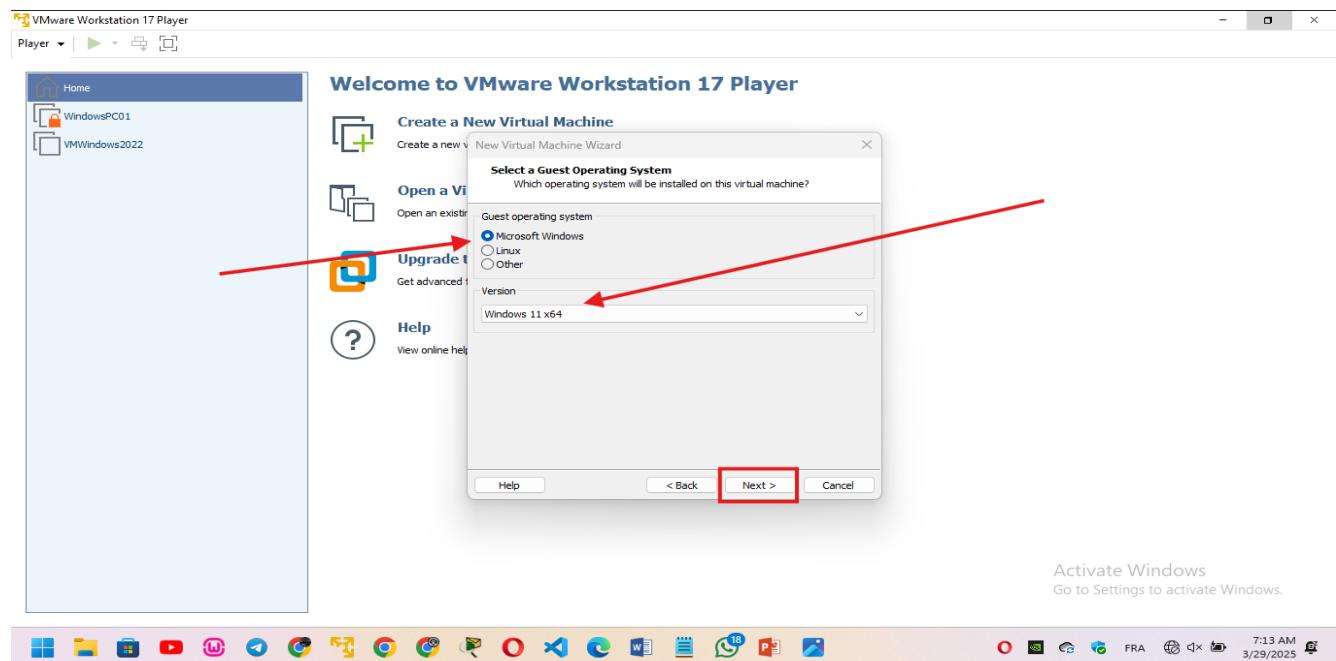


Étape 11:Lancez votre VM et cliquez sur cette option pour démarrez l'installation de Windows server 2022.

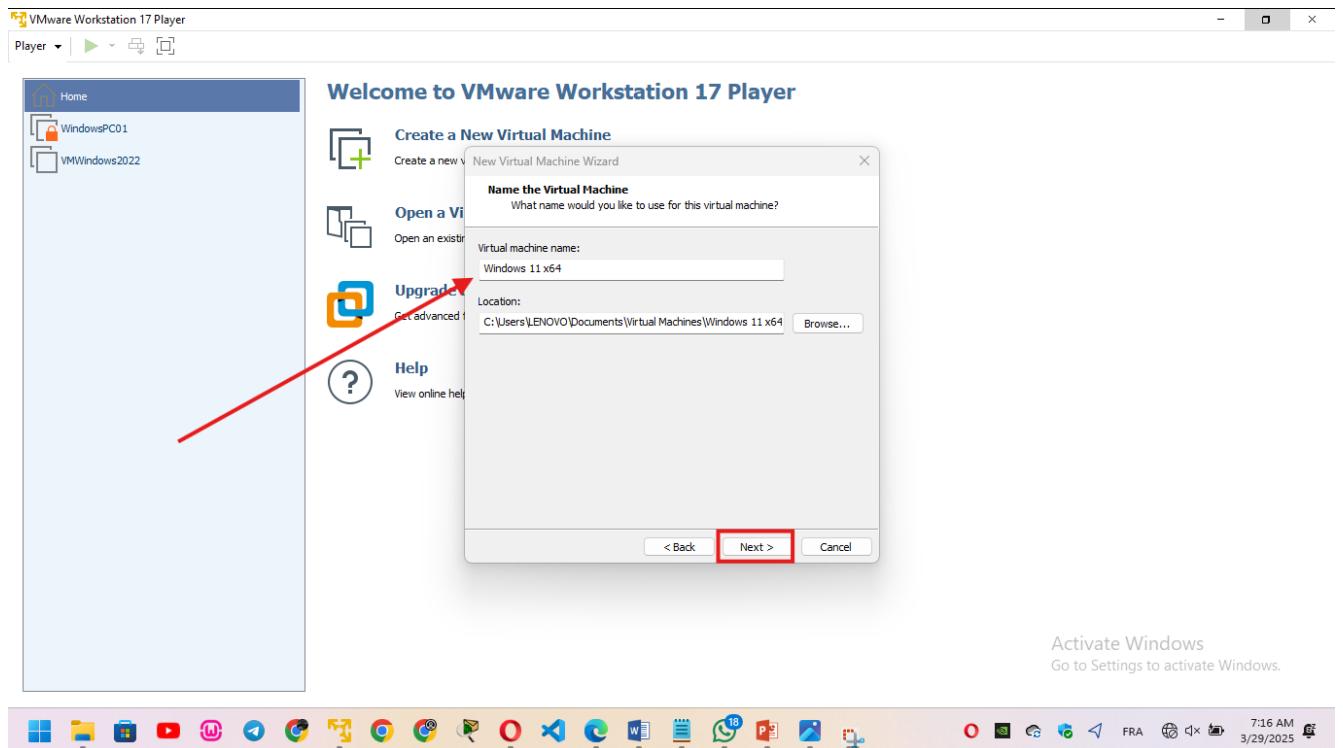
Configuration Poste Client



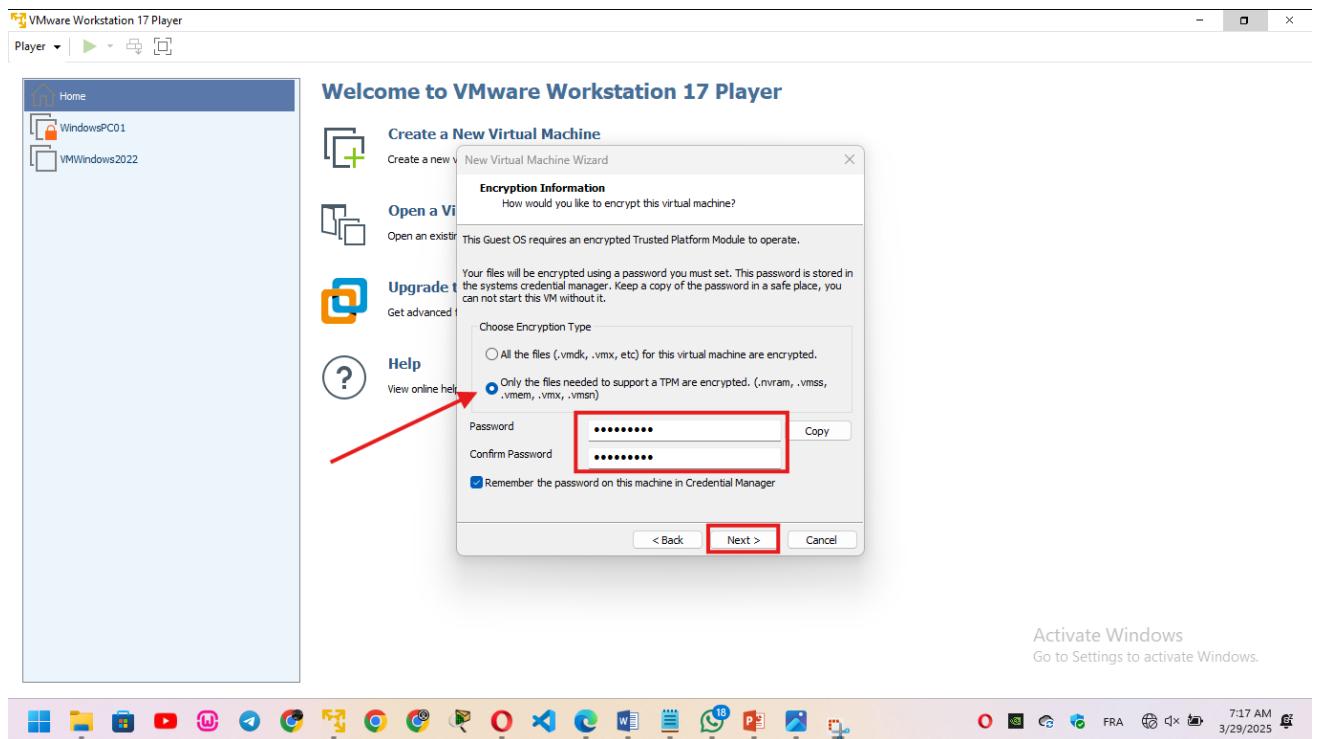
Étape 12: Comme précédent cliquez sur j'installerai le système d'exploitation plus tard.



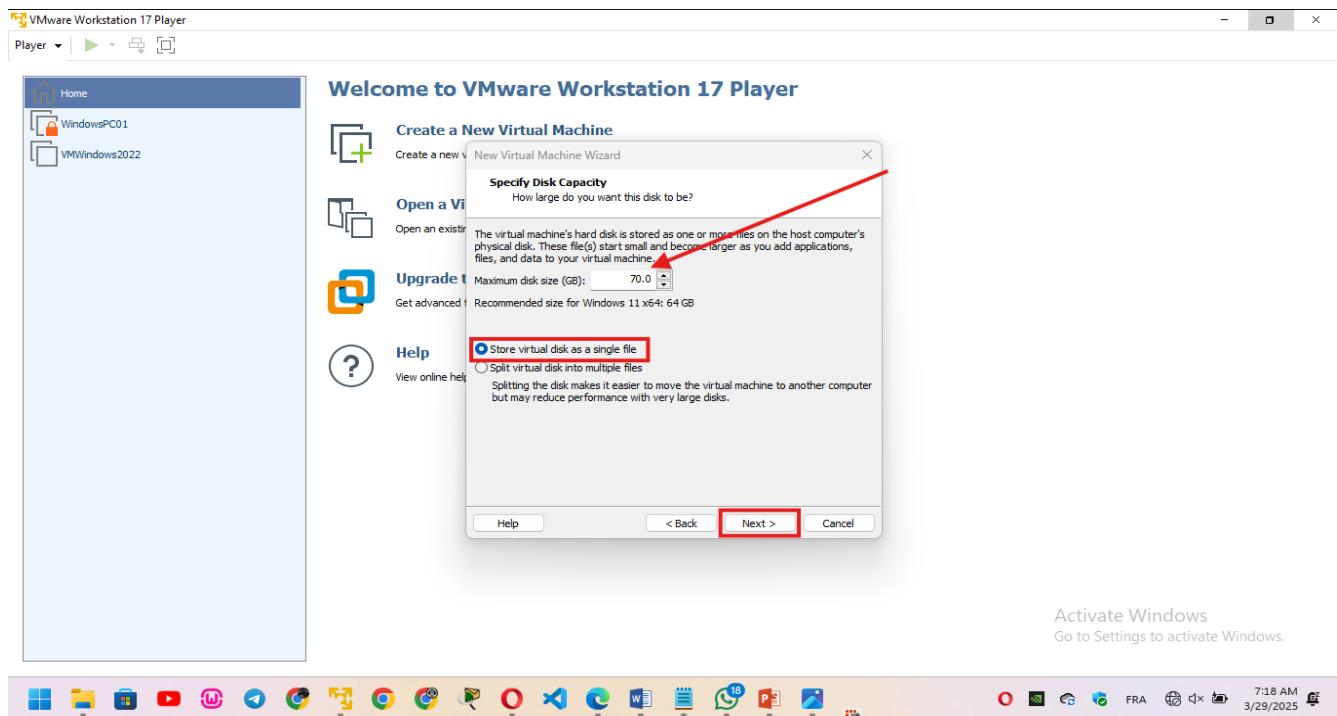
Étape 13: Sélectionnez l'option Microsoft Windows et défilez la barre jusqu'à Windows 11 x64.



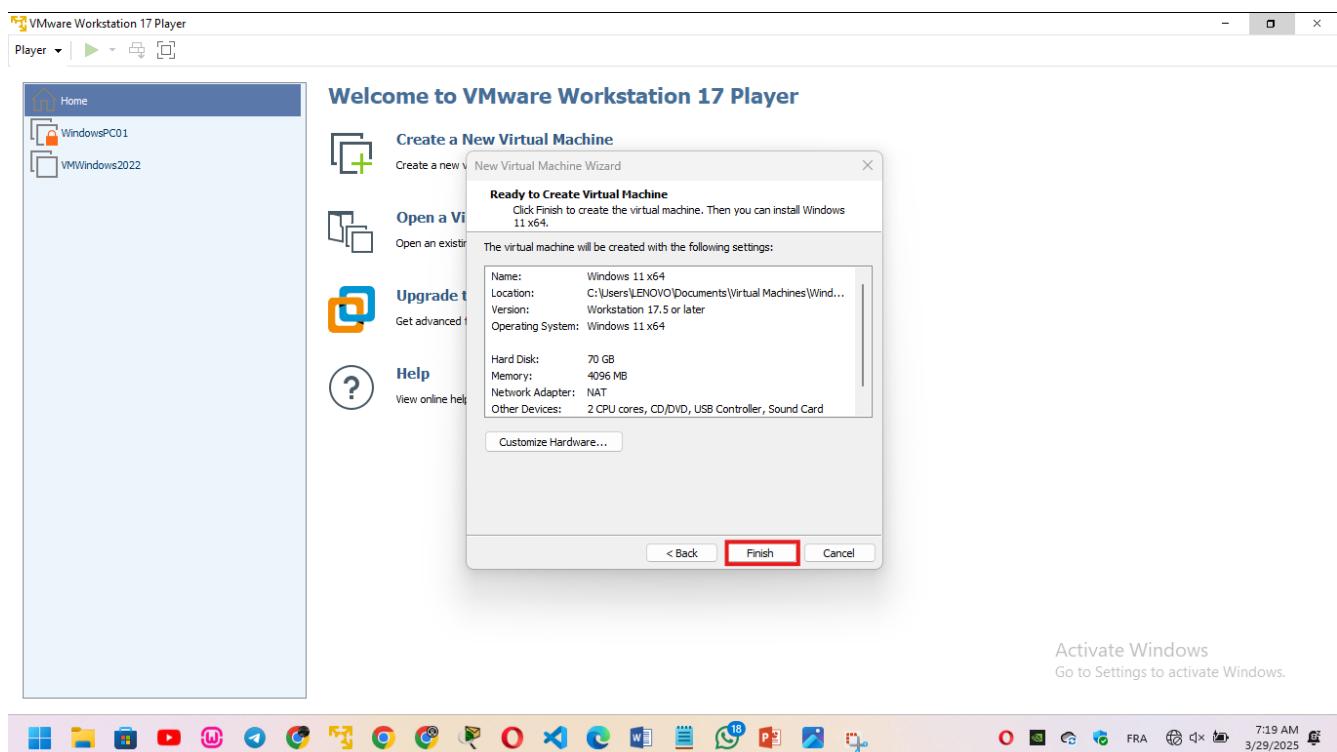
Étape 14: Donnez un nom à votre VM et définissez un emplacement de stockage sinon laissez les valeurs par défaut et cliquez sur suivant.



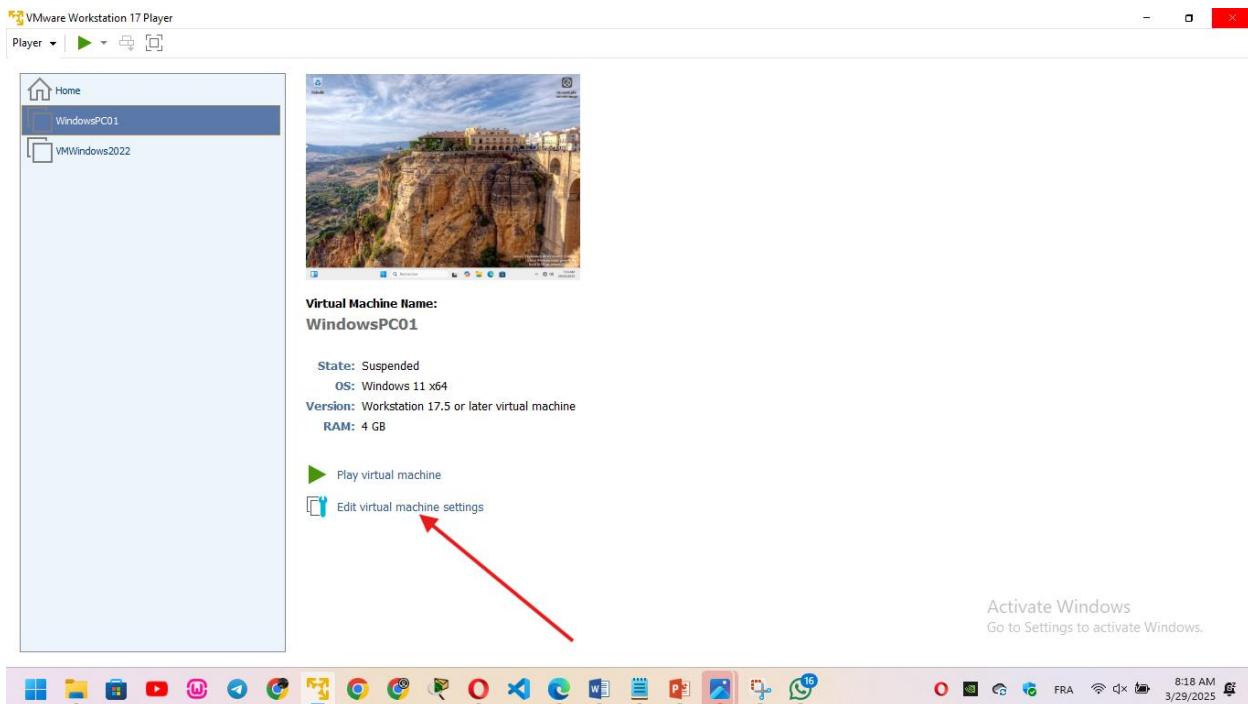
Étape 15: Définissez un mot de passe pour votre VM cliente et laissez les valeurs par défauts.



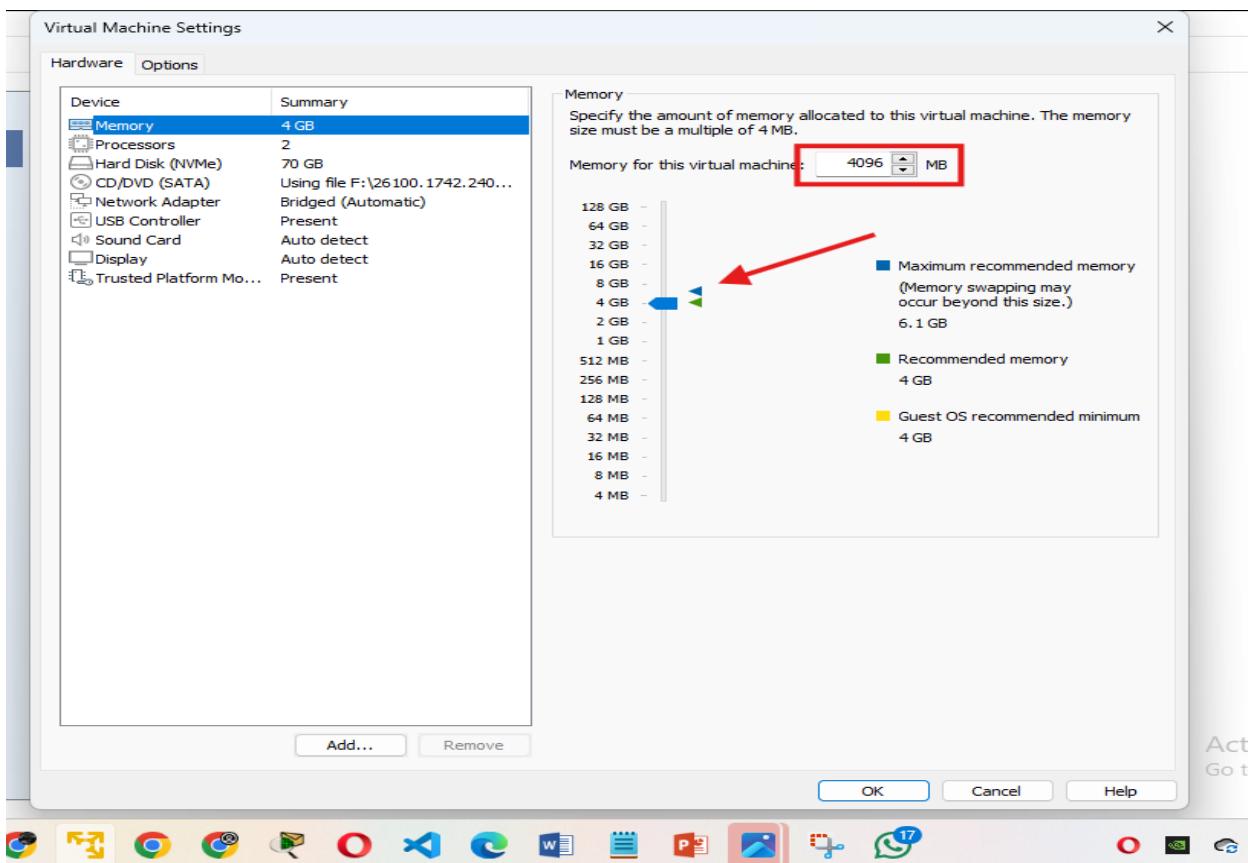
Étape 16: Allouez à votre VM minimum 64GB ou 70.0GB idéalement puis choisissez la première option.



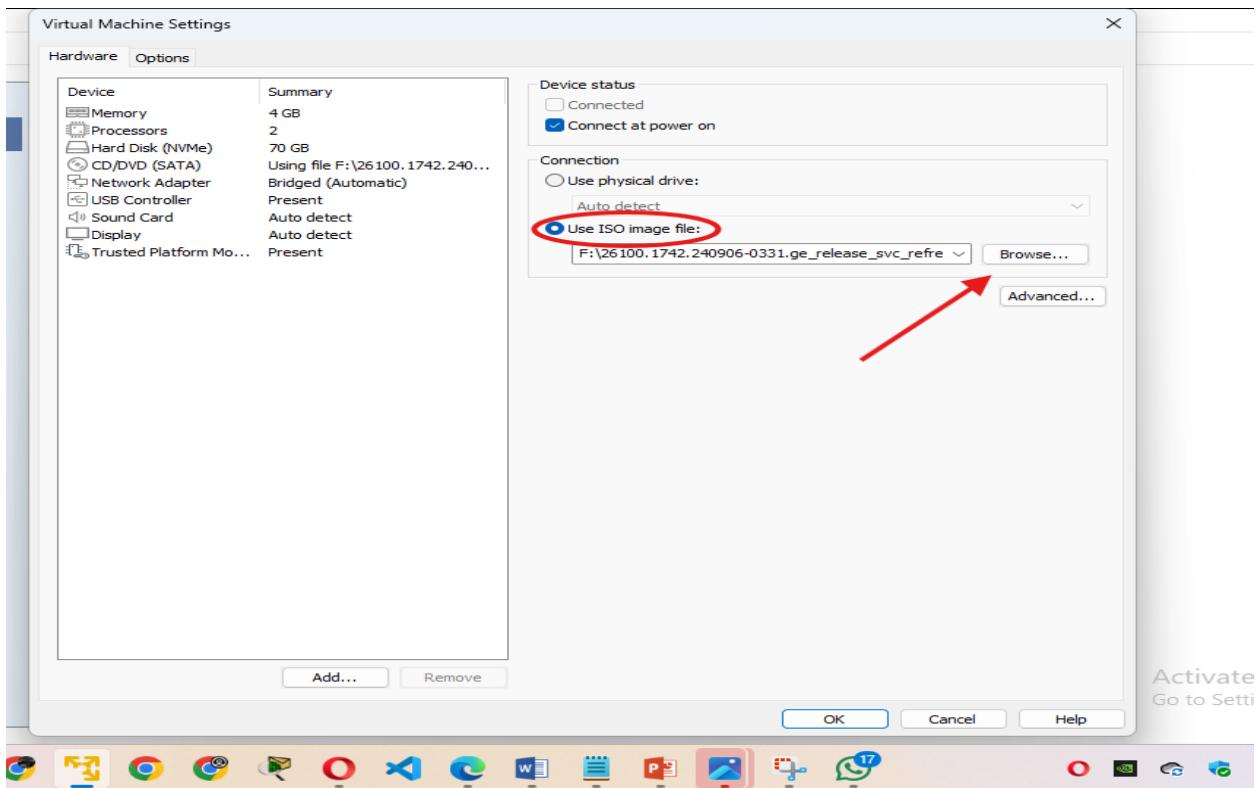
Étape 17: Si vous avez bien suivie les étapes cliquez sur terminée sinon revenez en arrière pour corrigez les problèmes.



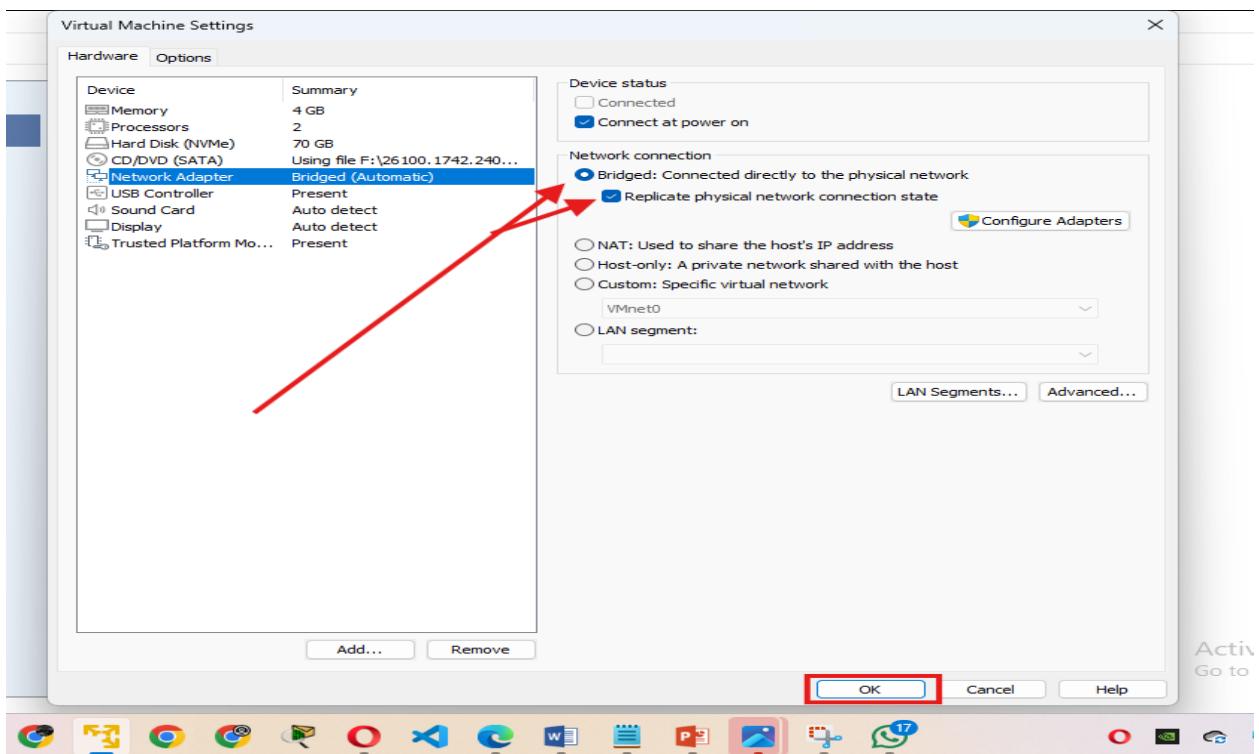
Étape 18:Cliquez sur modifiez les paramètres de ma VM.



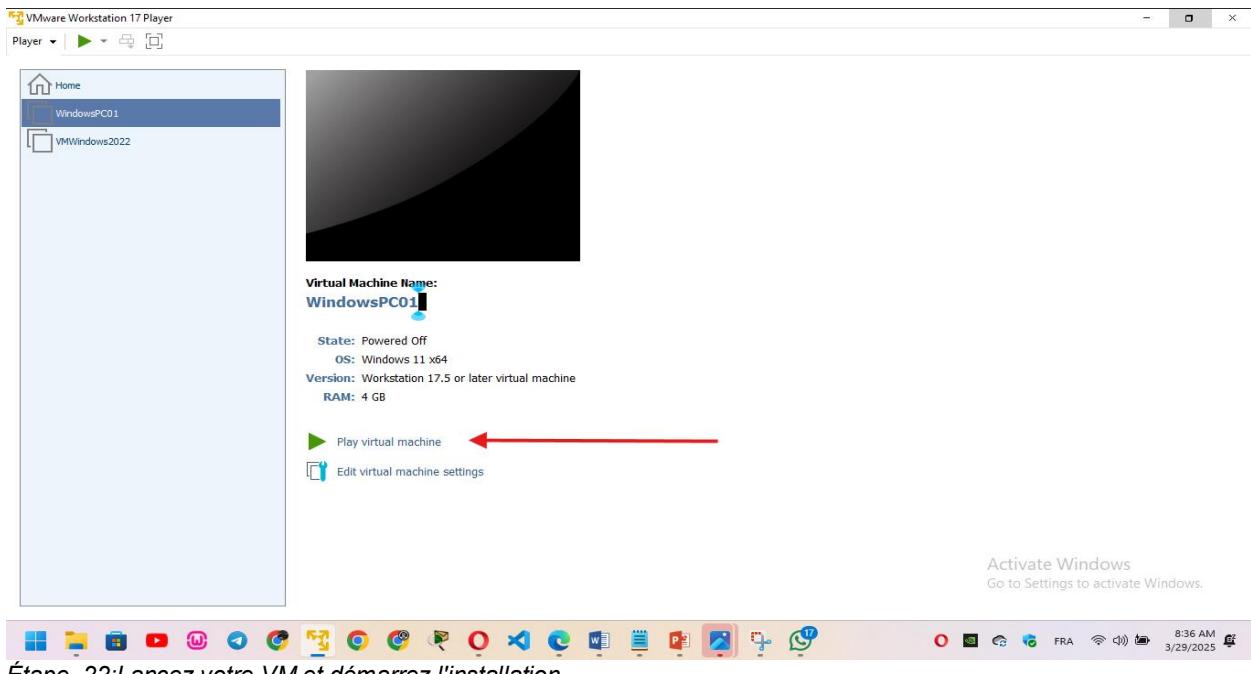
Étape 19:Augmentez la RAM de votre VM à 4GB.



Étape 20:Sélectionnez l'emplacement de votre image ISO



Étape 21:Sélectionnez le mode réseau Bridged et cliquez sur OK.



Étape 22:Lancez votre VM et démarrez l'installation.

Configuration Réseau

Sur le Serveur KSC

```

Administrator : C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.20348.587]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig
Configuration IP de Windows

Carte Ethernet Ethernet0 :
    Suffixe DNS propre à la connexion . . . . . : fe80::1:9991%0
    Adresse IPv6 de liaison locale . . . . . : fe80::1:9991%0
    Adresse IPv4 . . . . . : 192.168.1.38
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 192.168.1.1

NetAdaptation C:\Users\Administrateur>ping 192.168.1.40
Envoi d'une requête 'Ping' à 192.168.1.40 avec 32 octets de données :
Réponse de 192.168.1.40 : octets=32 temps=8 ms TTL=128
Réponse de 192.168.1.40 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.1.40 : octets=32 temps=17 ms TTL=128
Réponse de 192.168.1.40 : octets=32 temps=1 ms TTL=128

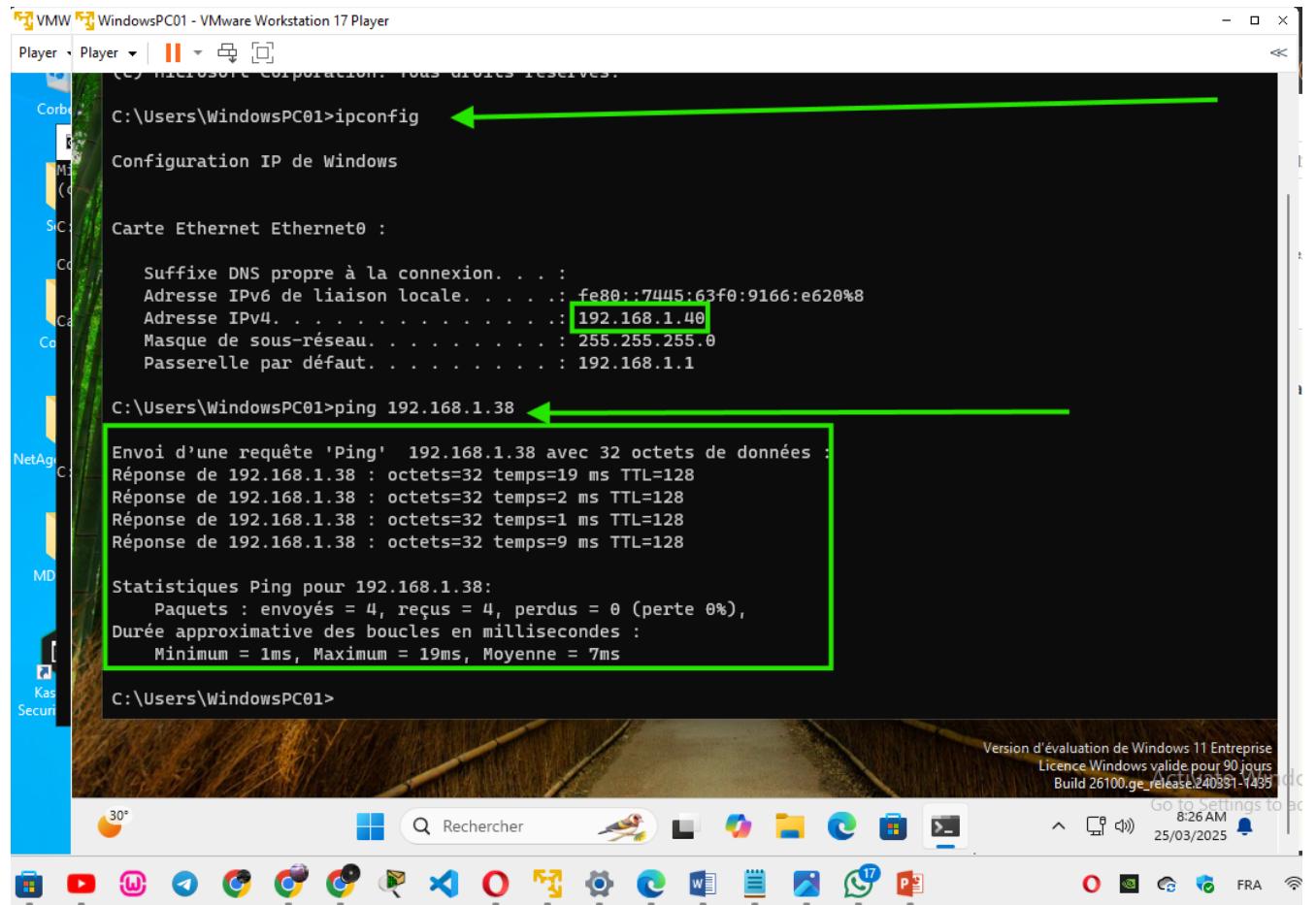
Statistiques Ping pour 192.168.1.40:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 17ms, Moyenne = 7ms

C:\Users\Administrateur>

```

Étape 23:Dans votre VM serveur lancez l'invite de commandes cmd vérifiez l'adresse IP de votre serveur à l'aide de la commande ipconfig puis lancez la commande ping pour pinger votre VM windows cliente.

Sur le Poste Client



```
C:\Users\WindowsPC01>ipconfig
Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffrage DNS propre à la connexion. . . . . : fe80::7445:63f0:9166:e620%8
    Adresse IPv6 de liaison locale. . . . . : fe80::7445:63f0:9166:e620%8
    Adresse IPv4. . . . . : 192.168.1.40
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.1

C:\Users\WindowsPC01>ping 192.168.1.38
Envoi d'une requête 'Ping' 192.168.1.38 avec 32 octets de données :
Réponse de 192.168.1.38 : octets=32 temps=19 ms TTL=128
Réponse de 192.168.1.38 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.1.38 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.38 : octets=32 temps=9 ms TTL=128

Statistiques Ping pour 192.168.1.38:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 19ms, Moyenne = 7ms

C:\Users\WindowsPC01>
```

Étape 24: Dans votre VM Windows11 lancez l'invite de commande cmd vérifiez l'adresse IP de votre poste à l'aide de la commande ipconfig puis lancez la commande ping pour pinger votre VM serveur.

NB : Pour que le ping fonctionne les deux VMs doivent être allumée en même temps.

Mises à Jour et Préparation

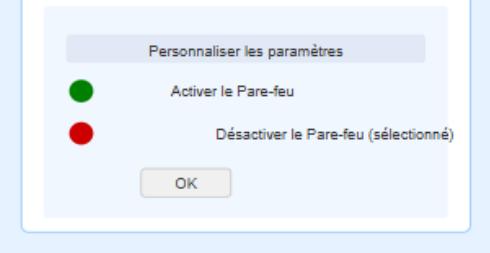
1. Installer les dernières mises à jour Windows

2. Désactiver temporairement les pare-feu antivirus

Désactiver temporairement les pare-feu Windows

Windows 10/11

- 1 Ouvrir le menu Démarrer
- 2 Taper "Pare-feu Windows"
- 3 Cliquer sur "Pare-feu Windows Defender"
- 4 Dans le menu gauche, cliquer sur "Activer ou désactiver le Pare-feu"
- 5 Sélectionner "Désactiver le Pare-feu" pour chaque type de réseau
- 6 Cliquer sur "OK"



Windows Server 2022

- 1 Ouvrir le "Gestionnaire de serveur"
- 2 Cliquer sur "Outils" dans le menu
- 3 Sélectionner "Pare-feu Windows avec sécurité avancée"
- 4 Dans le volet gauche, cliquer droit sur "Pare-feu Windows avec sécurité avancée"
- 5 Sélectionner "Propriétés"
- 6 Pour chaque profil (Domaine, Privé, Public), modifier "État du pare-feu" à "Désactivé"



⚠️ N'oubliez pas de réactiver le pare-feu après vos opérations pour garantir la sécurité du système.

3. Vérifier la connectivité Internet