

BTS 2 option SISR

Renouvellement par masterisation des postes clients d'une PME

I.	Contexte.....	4
II.	NTLite.....	4
A.	Intégration des mises à jour.....	6
1.	Première méthode.....	6
2.	Deuxième méthode.....	6
B.	Intégration driver.....	7
C.	Configuration de l'éditeur de registre.....	8
1.	Paramètres biométriques et d'écran de verrouillage.....	9
2.	DNS et sécurisation du réseau.....	9
3.	Sécurisation des mots de passe et d'authentifications.....	11
4.	Protection du Réseau.....	13
5.	Paramètre de Windows Defender.....	14
6.	Journalisation des évènements Windows.....	15
7.	Mesure de sécurité avancées.....	15
D.	Configuration Post-Installation.....	16
E.	Configuration Composant.....	17
F.	Configuration Tâches planifiées.....	18
G.	Configuration Fonctionnalités.....	18
1.	Fonctionnalités principales de Windows.....	18
2.	Outils et services.....	19
3.	Capacités réseau.....	19
4.	Fonctionnalités liées à la sécurité.....	19
H.	Configuration Paramètre.....	19
I.	Configuration Services.....	20
1.	Désactiver les services inutiles.....	20
2.	Configurer des services essentiels.....	20
J.	Configuration Services cachées.....	20
K.	Configuration Unattended.....	21
L.	Création de l'ISO personnaliser de Windows 11.....	22
III.	Déploiement par Clé USB.....	24
A.	Création d'une Clé USB bootable.....	24
B.	Installation de l'ISO sur la VM.....	26
IV.	Déploiement par le réseau avec un serveur Fog.....	29
A.	Téléchargement et installation d'une VM Ubuntu.....	29

B.	Configuration de la VM.....	32
1.	Configuration de l'interface réseau.....	32
2.	Mise à jour et mise à niveau.....	37
3.	Téléchargement et installation du logiciel Fog Projet.....	37
C.	Création d'une image.....	42
1.	Enregistrement d'une machine dans l'inventaire du serveur Fog.....	42
2.	Création d'une image.....	43
D.	Déploiement de l'ISO.....	47
1.	Enregistrement de la nouvelle machine à déployer.....	47
2.	Affectation d'une tâche de déploiement à la machine.....	47
3.	Déploiement de la nouvelle machine.....	47
V.	Déploiement par le réseau avec un serveur WDS.....	49
A.	Téléchargement, installation et configuration de Windows Server 2022.....	49
1.	Téléchargement de Windows Server 2022.....	49
2.	Installation de Windows Server 2022.....	49
3.	Configuration de Windows Server 2022.....	52
4.	Configurer le réseau de la VM.....	53
B.	Installation et configurer le serveur AD DS.....	57
1.	Installation du serveur AD DS.....	58
2.	Configurer le serveur AD DS.....	59
C.	Installation et configurer le serveur DNS.....	62
1.	Installation serveur DNS.....	62
2.	Configurer le serveur DNS.....	63
D.	Installation et configurer le serveur DHCP.....	68
1.	Installation du serveur DHCP.....	68
2.	Configurer le serveur DHCP.....	69
3.	DHCP : déclarer les classes de fournisseurs.....	73
4.	Créer les stratégies DHCP pour le BIOS et l'UEFI.....	74
E.	Installation et configuration du serveur WDS.....	75
1.	Installation du serveur WDS.....	75
2.	Configuration du Serveur WDS.....	77
F.	Déploiement avec le couple WDS - MDT.....	81
1.	Installation Windows ADK, Windows PE et MDT.....	81
2.	Créer le Deployment Share.....	82

3.	Créer un utilisateur local dédié à MDT.....	84
4.	Importer une image Windows 11 dans MDT.....	85
5.	Créer une séquence de tâches pour Windows 11.....	88
G.	Configurer MDT pour Windows 11 (et éviter des problèmes).....	91
1.	Bug de la console MMC avec l'onglet Windows PE.....	91
H.	Personnaliser le bootstrap.ini et le CustomSettings.ini.....	93
I.	Générer l'image Lite Touch et l'importer dans WDS.....	95
1.	MDT : générer l'image Lite Touch.....	95
2.	WDS : importer l'image Lite Touch.....	96
J.	Déploiement de l'image de démarrage.....	97

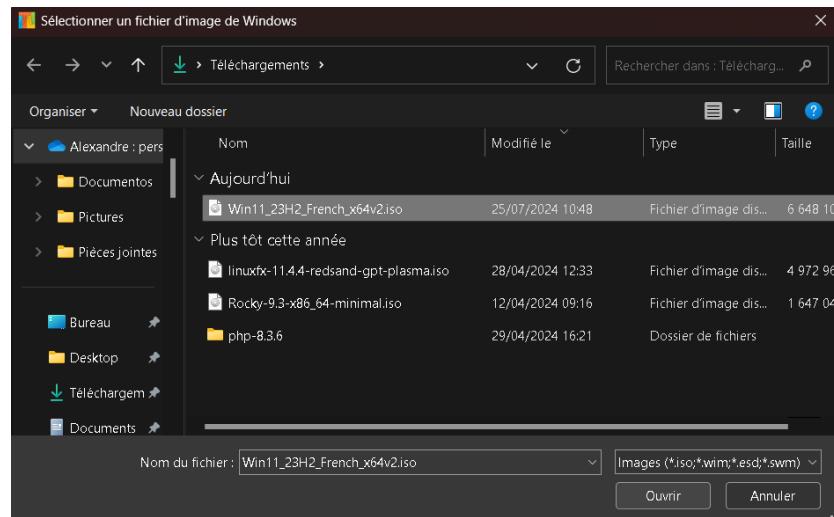
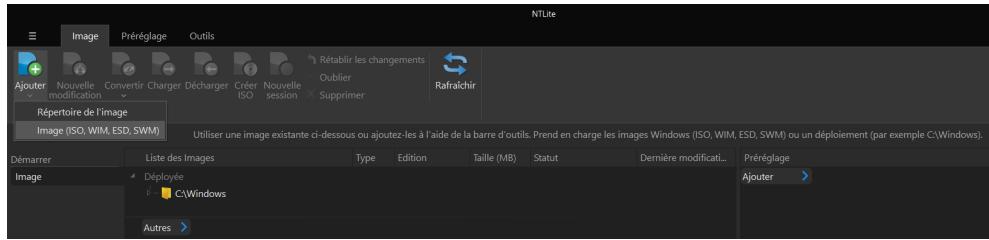
I. Contexte

L'entreprise EXPERTY souhaite renouveler intégralement son parc informatique de 80 postes sous Windows 11. Nous allons utiliser un logiciel de personnalisation d'image pour répondre au mieux à la sécurité et au besoin de l'entreprise avec NTLite. Utiliser 3 méthodes de déploiement de cette image avec une clé USB, un serveur Fog et un serveur WDS.

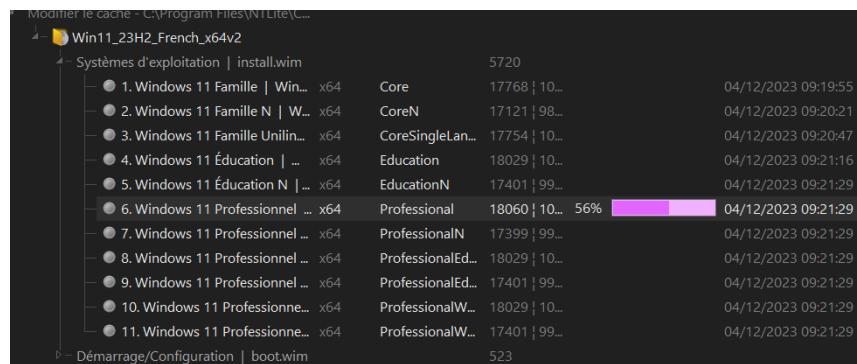
II. NTLite

NTLite est un logiciel de personnalisation d'ISO Windows par l'ajout ou suppression des composant inutiles, le paramétrage de la sécurité par l'éditeur de registre, l'intégration de logiciel indispensable, de pilote ou de mise à jour. C'est un outil parfait pour la création d'une image de déploiement.

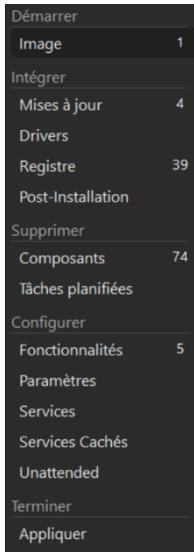
- Télécharger la version 64 bits du logiciel NTLITE avec le lien <https://www.ntlite.com/>
- Téléchargement de l'image de disque Windows 11 sur le site de Microsoft (<https://www.microsoft.com/fr-fr/software-download/windows11>)
- Ouvrez NTLite, cliquez sur Ajouter > Image (ISO, WIM, ESO, SWM) > sélectionnez l'ISO téléchargé précédemment :



- Sélectionnez Windows 11 Professionnel avec un double clique > confirmez le répertoire racine et l'image va se charger :



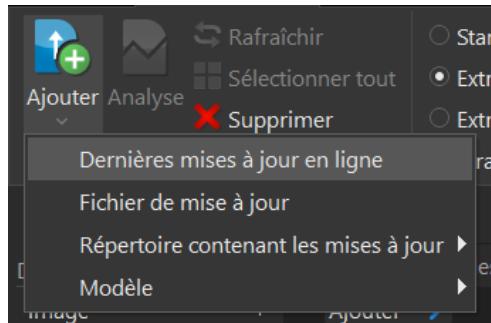
- Le menu déroulant permet d'intégrer, supprimer et configurer des composants dans l'ISO Windows 11 :



A. Intégration des mises à jour

- Dans le menu Mise à jour, intégrez les dernières mises à jour de Windows Update à votre ISO Windows 11 :

 1. Première méthode
 - Ajouter > Dernières mise à jour en ligne :



- Cochez les mises à jour non intégrer dans l'image :

1. Sélectionner une liste de mise à jour					Plus d'infos
	Date de ...	Version	État	Chemin	Taille (MB)
Windows 11 23H2 x64 [Chargé]
File d'attente des mises à jour
Taper ici pour filtrer
KB2267602 - Microsoft Defender Antivirus update (Engine v1.1.24060.5)	07/21/24	1.415.215.0	Manquant	[Cache]\11.23H2.x64\mpam-fe.exe	...
KB5040442 - Cumulative Update	07/03/24	22621.3880...	Manquant	[Cache]\11.23H2.x64\windows11-kb5040442-x64_c1ba0e4607fd0ee46254a6255...	728.70
KB4052623 - Microsoft Defender Antivirus update (Platform)	06/25/24	4.18.24060.7	Manquant	[Cache]\11.23H2.x64\updateplatform\md64fre_b15ba1fac832628f6273887773f63cd...	12.80
KB5039895 - .NET Framework 3.5 and 4.8.1 Cumulative Update	06/14/24	100.9256.3	Manquant	[Cache]\11.23H2.x64\windows11-kb5039895-x64_ndp481_880d33530d0e5e1423c9...	71.70
KB5040709 - Dynamic Update for Windows setup	06/11/24	100.25398.1...	Manquant	[Cache]\11.23H2.x64\windows11-kb5040709-x64_a7998d59ed342398fb0b3264d...	9.80
KB5036212 - Out of Box Experience update	02/14/24	22621.3227...	Manquant	[Cache]\11.23H2.x64\windows11-kb5036212-x64_a89863be944faaa267b7315ccdd...	1.20
Windows Package Manager (App Installer, WinGet)	2024.709.23...	Manquant	[Cache]\11.23H2.x64\Microsoft.DesktopAppInstaller_0wekyb3d8bbwe.msixbundle	252.50	
Microsoft.UI.Xaml 2.8.6	8.2310.3000...	Manquant	[Cache]\11.23H2.x64\Microsoft.UI.Xaml.2.8.x64.appx	4.90	
Microsoft Visual C++ + UWP Runtime v14.00 (Microsoft.VCLibs.140.00.UWPDesktop)	14.0.33321.0	Manquant	[Cache]\11.23H2.x64\Microsoft.VCLibs.x64.14.00/Desktop.appx	6.50	

2. Deuxième méthode

- Installez les mises à jour Windows manuellement en les téléchargeant sur le site Catalogue Microsoft Update (<https://www.catalog.update.microsoft.com/home.aspx>) :

Catalogue Microsoft Update

FAQ | aide

"kb5040709"

Mises à jour : 1 - 1 sur 1 (page 1 sur 1)

Titre	Produits	Classification	Dernière mise à jour	Version	Taille	Télécharger
2024_07_Setup_Dynamic_Update_for_Microsoft_server_operating_system_version_23H2_for_x64-based_Systems_(KB5040709)	Windows 10 and later Dynamic Update	Critical Updates	09/07/2024	n.a.	9.8 MB	Télécharger

- Téléchargez dans un dossier prévu à cet effet puis ajoutez les dans la file d'attente des mises à jour, Ajouter > Fichier > Répertoire :

File d'attente des mises à jour Date de ... Version Chemin Taille (MB)

Ajouter > Fichier Répertoire Dernières mises à jour en ligne

Répertoire
Rechercher et ajouter tous les éléments d'un répertoire à la file d'attente d'intégration

Taper ici pour filtrer

Ajouter >

KB5040709 - Mise à jour...	06/11/24	10.0.25398.1...	C:\Users\alexr\Downloads\windows11.0-kb...	9.84
KB5040442 - Mise à jour Cumulative	22621.3880...		C:\Users\alexr\Downloads\windows11.0-kb...	728.67
Mise à jour de l'antivirus...	06/25/24	4.18.24060.7	C:\Users\alexr\Downloads\updateplatform....	12.77
KB5039895 - .NET Fram...	06/14/24	10.0.9256.3	C:\Users\alexr\Downloads\windows11.0-kb...	71.70

B. Intégration driver

- Le menu Driver permet d'ajouter ou de supprimer des pilotes essentiels pour le bon fonctionnement du système. Cliquez Ajouter > Fichier ou Répertoire pour ajouter les pilotes manquants :

Ajouter Importer Exporter les hôtes inutiles Supprimer Machine Machine hôte (LAP...) Afficher les périphériques cachés Réutilisation du cache du pilote

Important liste HW Exporter la liste HW Liste du matériel Options

Démarre... File d'attente du pilote Ajouter > Version

Ajouter des pilotes à la liste et examiner les besoins matériels

Liste du matériel État

- audio inputs and outputs Trouvé
- Batteries Trouvé
- Lecteurs de DVD/CD-ROM Trouvé
- Ordinateur Trouvé
- disk drives Trouvé
- display adapters Trouvé
- firmware Trouvé
- Pérophériques d'interface utilisateur Trouvé
 - Pérophérique d'acquisition d'images Trouvé
- Claviers Trouvé
- sound, video and game controllers Trouvé
 - NVIDIA High Definition Audio Trouvé
 - NVIDIA Virtual Audio Device (Wave Extensible) (WDM) Trouvé
 - Realtek(R) Audio Trouvé
 - Son Intel(R) pour écrans Trouvé
- Modems Trouvé
- monitors Trouvé
- Souris et autres périphériques de pointage Trouvé
- Cartes réseau Trouvé
 - Intel(R) Wi-Fi 6 AX201 160MHz Trouvé
 - Microsoft Kernel Debug Network Adapter Trouvé
 - Microsoft Wi-Fi Direct Virtual Adapter #3 Trouvé
 - Microsoft Wi-Fi Direct Virtual Adapter #4 Trouvé
 - Realtek PCIe GBE Family Controller Trouvé
 - Microsoft VHD Disk Reference Adapter Trouvé

C. Configuration de l'éditeur de registre

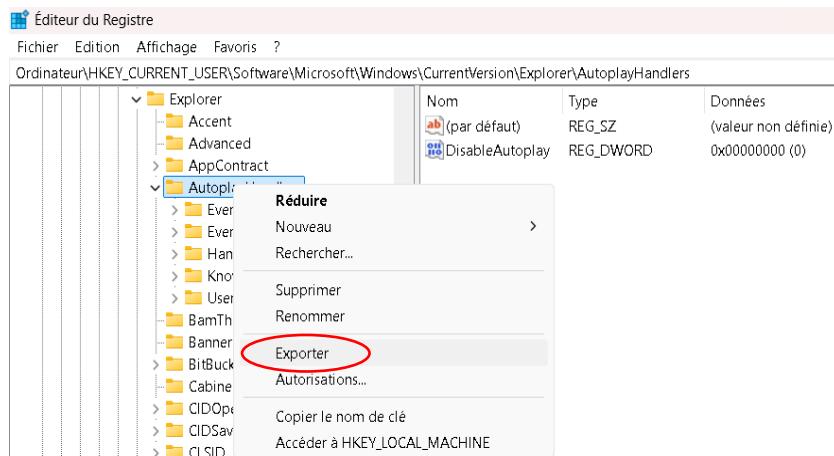
Le menu **Registre** permet d'activer ou désactiver des processus et des services Windows essentiel ou de les configurer.

L'éditeur de registre est une base de données hiérarchique centralisée qui stocke les informations essentielles à la configuration du système pour tous les utilisateurs, applications et périphériques matériels. La modification de paramètre dans le registre peut provoquer des dysfonctionnements de Windows si elle est mal configurée.

Cette base de données est composée de 5 ruches de registre structurées en arborescence :

- HKEY_LOCAL_MACHINE (HKLM) : contient les informations de configuration du système d'exploitation Windows, de démarrage, des logiciel et application installé pour n'importe quel utilisateur. Elle inclut aussi les informations du matériel et des pilotes détectés. L'arborescence de HKLM contient 5 clés prédefinies de registre principales : SOFTWARE, SYSTEM, SECURITY, SAM et HARDWARE.
- HKEY_CURRENT_USER (HCKU) : stocke la configuration de Windows et logiciel spécifiques de compte utilisateur actuellement connecté, les dossiers, les couleurs d'écran et les paramètres du panneau de configuration.
- HKEY_CLASSES_ROOT (HKCR) : contient les informations des associations d'extensions nom de fichier et d'inscription de classe COM.
- HKEY_USERS (HKU) : contient tous les profils utilisateur actifs chargés sur l'ordinateur.
- HKEY_CURRENT_CONFIG (HKCC) : comporte des informations sur le profil matériel utilisé par l'ordinateur local au démarrage du système.

Il est conseillé d'exporter le fichier registre « .reg » et d'effectuer le modifier dans un fichier bloc note. Il faudra créer des sous-clés ou valeurs dans la base de données :



1. Paramètres biométriques et d'écran de verrouillage

Service Biométriques permet d'autres méthodes d'authentification par exemple la reconnaissance d'empreintes digitales ou la reconnaissance faciale. Malheureusement ces méthodes sont facilement contournées par des hackers, le mieux est de les désactiver.

- Désactiver le service biométrique :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Biometrics > Enable > DWORD (32-bit) > 0
- Activer l'anti-spoofing contre usurpation d'identité :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeature > Enable > DWORD (32-bit) > 1

La caméra peut-être aussi hacker et utiliser pour surveiller et récupérer des informations sensibles.

- Désactiver la caméra :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Camera > AllowCamera > DWORD (32-bit) > 0
- Désactiver l'authentification faciale Windows :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticati on\LogonUI\FaceLogon > ShouldForbidExternalCameras > DWORD (32-bit) > 0

Les commandes vocales peuvent être utiliser même si le post est verrouillé ce qui compromet sa sécurité. Mais aussi la collecte des données vocale peut être utiliser pour du spoofing.

- Désactivé la reconnaissance vocale en ligne et la collecte des données vocales :
 - HKEY_CURRENT_USER\Software\Microsoft\Speech_OneCore\Settings\OnlineSpe echPrivacy > HasAccepted > DWORD (32-bit) > 0
- Désactivé la reconnaissance vocale hors ligne :
 - HKEY_CURRENT_USER\Software\Microsoft\Speech_OneCore\Settings\VoiceActivatio n > VoicActivationEnableAboveLockscreen > DWORD (32-bit) > 0
- Désactivé l'assistance vocale personnelle de Microsoft :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search > AllowCortana > DWORD (32-bit) > 0

2. DNS et sécurisation du réseau

Le mDNS (Multicast DNS) est un protocole qui bénéficie des fonctionnalités de DNS sans avoir de serveur DNS sur le réseau. Il représente un risque dans la sécurité de réseau car dans certain cas le mDNS est ouvert donc répond aux demandes externes au réseau. Les hackers peuvent l'utiliser pour effectuer des attaques DDoS, de détourner le réseau, récupérer des données sensibles et les adresses MAC des appareils connectés.

- Désactiver mDNS:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
 > EnableMDNS > DWORD (32-bit) > 0

Le pare-feu sécurise un pc par le contrôle les communications entre les ports utiliser pour interagir avec un réseau interne sécurisé et un réseau externe non sécurisés. Il surveille et filtre les paquets entrants et sortants par le biais de règles de sécurité prédéfinies, autorisant ou bloquant des connexions spécifiques en fonction de critères tels que l'adresse IP, le port, ou le protocole.

- Activer le pare-feu et les notifications des profils existants :
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile > EnableFirewal > DWORD (32-bit) > 1

Le protocole d'authentification NTLM est utilisé pour vérifier l'identité d'un utilisateur ou une machine sur un réseau en se basant sur un système de challenge-response. Le chiffrement utilisé est faible ce qui le rend vulnérable avec un hash de mot de passe pouvant être extrait de la mémoire du service LSA. L'hacker peut récupérer les mots de passes pour s'authentifier dans le réseau.

- Désactiver NTLM :
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 > NtLmMinClientSec et NtLmMinServerSec > DWORD (32-bit) > 20080000

Activation de la signature SMB/LDAP

Le protocole SMB (Server Massage Block) est un protocole réseau utilisé principalement pour le partage de fichiers, d'imprimantes et d'autres ressources réseau de manière sécuriser entre appareils connecter au même réseau. SMB prend en charge l'authentification des utilisateurs et le contrôle des accès pour garantir que seules les personnes autorisées peuvent accéder à certaines ressources. Il offre des fonctionnalités de verrouillage de fichiers pour empêcher plusieurs utilisateurs de modifier simultanément un même fichier, réduisant ainsi le risque de conflits ou de corruption de données.

- Désactiver SMBv1 :
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters > SMB1 > DWORD (32-bit) > 0.
- Activer SMBv2/SMBv3 :
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters > SMB1 > DWORD (32-bit) > 0.

UAC (User Account Protection) est une **fonctionnalité de sécurité intégrée** de Windows qui consiste à limiter les actions sur le **système** d'un utilisateur ou d'un programme. Si un programme ou une action **nécessite** des droits administrateurs, une **fenêtre UAC** demande l'autorisation de l'utilisateur si elle n'est pas **validée** l'action ne se produira pas. L'UAC contribue au renforcement de la **sécurité** en **empêchant** des logiciels malveillants de modifier le **système** sans autorisation et de **limité** les dégâts si l'utilisateur en a exécuté.

- Activer l'UAC :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System > EnableLUA > DWORD (32-bit) > 1

3. Sécurisation des mots de passe et d'authentifications

Le mot de passe en clair est un mot de passe non **sécuriser** qui peut **être stocké** dans la mémoire du **système** pouvant **être récupérer** par des hackers. En **désactivant** l'enregistrement des mots de passe en claire, les hackers auront plus de mal à récupérer des informations d'identification sensible.

- Désactiver l'enregistrement des mots de passe en claire :
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest > UseLogonCredential > DWORD (32-bit) > 0

Kerberos est un protocole de chiffrement **renforcé** et authentification externe permettant d'identifier l'utilisateur par tickets temporaires qui **empêche la réutilisation** de ces derniers et aussi de chiffrer les échanges d'informations bloquant ainsi l'interception et la modification des données.

Dans les environnements Windows, Kerberos est le protocole d'authentification par **défaut** pour les domaines Active Directory. Lorsque vous vous connectez à un domaine Windows, Kerberos est utilisé pour valider votre identité et gérer l'accès aux ressources réseau.

- Paramétriser Kerberos :
 - Accédez au différent nom de la valeur de type **DWORD (32-bit)** dans HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters
 - **SkewTime** est la différence de temps maximale autorisée entre l'ordinateur client et le serveur qui accepte l'authentification Kerberos ou le KDC (Key Distribution Center) : 5 min
 - **LogLevel** indique les événements sont enregistrés dans le journal des événements système : 0

- StartupTime est le temps pendant lequel Windows attend que le KDC démarre avant que Windows abandonne : 120 sec
- KdcWaitTime correspond à l'heure à laquelle Windows attend une réponse d'un KDC, modifier 10 sec
- KdcBackoffTime correspond à la durée entre les appels successifs au KDC si l'appel précédent a échoué : 12 sec
- MaxPacketSize correspond à la taille des paquets UDP (User Datagram Protocol). Si la taille du paquet dépasse cette valeur, TCP est utilisé : 1465 octets
- KdcSendRetries indique le nombre de tentative que le client peut faire pour contacter un KDC : 3 tentatives
- DefaultEncryption indique le type de chiffrement par défaut pour la pré-authentification : 0x00000017
- MaxReferralCount correspond au nombre de références KDC d'un client poursuit avant l'abandonner : 6

PowerShell est un outil permettant d'effectuer changements dans les **paramètres**, résoudre plusieurs **problèmes**, gérer des **fonctionnalités** et automatiser votre travail avec des lignes de commande. Les hackers peuvent l'utiliser pour lancer des scripts malveillants sur le post infecter. Mshta.exe est un autre **exécutable** de fichiers Microsoft HTML Application (HTA) qui est aussi sensible aux attaques de malware.

- Ne pas autoriser le PowerShell :
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
r > DisallowRun > DWORD (32-bit) > 1
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun > DWORD (32-bit) > créez des valeurs de chaîne REG_SZ pour restreindre des applications en les nommant 1 et 2

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"DisallowRun"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun]
"1"="mshta.exe"
"2"="powershell.exe"
```

- Désactiver exécution de script :
 - HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\Windows\System > EnableScript > DWORD (32-bit) > 0

L'AutoRun permet d'automatiser le lancement de certains programmes lors de l'insertion d'un périphérique de stockage ce qui peut être très dangereux si une personne malveillante à un accès directe à un poste dans le but de l'infecter et d'infecter le réseau de l'entreprise.

- Désactiver l’Autorun :
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers > DisableAutoplay > DWORD (32-bit) > 1

4. Protection du Réseau

Le service Netlogon permet d’authentifier des utilisateurs et des ordinateurs dans le domaine Active Directory (AD). Il sécurise et journalise les connexions entre les clients et les contrôleurs de domaines.

- Configurer Netlogon :
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters > type DWORD (32-bit)
 - DisablePasswordChange surveille si l’ordinateur membre du domaine change automatiquement son mot de passe : 0
 - Require SignOrSeal contrôle si la communication entre un client et un contrôleur de domaine doit être signée ou cryptée : 1
 - SignSecureChannel définie si les messages sur le canal sécurisé doivent être signés pour garantir leur intégrité : 1
 - MaximumPasswordAge détermine la durée maximale, en jours, avant qu’un ordinateur membre du domaine doive changer son mot de passe : 30

SmartScreen est un composant anti-phishing et anti-malware qui vérifie la présence de menace sur les sites visités, les fichiers téléchargés et les applications non reconnues.

- Activer SmartScreen :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System > EnableSmartScreen > DWORD (32-bit) > 1
 -
- Activer SmartScreen dans Microsoft Edge :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter > EnabledV9 > DWORD (32-bit) > 1

5. Paramètre de Windows Defender

Windows Defender est un composant antivirus de Microsoft Windows qui protège en temps réel plusieurs zones de Windows.

- Activer Windows Defender :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager > DisableAntispyware > DWORD (32-bit) > 0

- Activer l’analyse planifiée de Windows Defender :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Scan > DisablesScheduleScan > DWORD (32-bit) > 0
 - ScanScheduleDay effectue des analyses planifiées pour détecter des éventuelles menaces sur le système durant la semaine : 1 (analyse le dimanche)
 - ScanScheduleTime programme l’heure d’analyse, modifiez la valeur par 540 (9h00 x 60 minutes + 0 minute)
 - DisablesScanningMappedNetworkDrivesForFullScan analyse des lecteurs réseau mappés lors d’une analyse complète : 0
 - DisableRemovableDriveScanning analyse les disques amovibles lors des analyses régulières : 1
- Activer la protection contre les applications potentiellement indésirables (PUA) :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\MpEngine > MpEnablePus > DWORD (32-bit) > 1
 - DisableScanningNetworkFiles analyse les fichiers partagés sur un réseau : 1
- Activer la protection contre la modification de dossier par des applications non autorisé (Accès contrôlé aux dossiers) :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender Exploit Guard\Controlled Folder Access > EnableControlledFolderAccess > DWORD (32-bit) > 1
 - AuditMode journalise les tentatives d’accès non autorisé sans les bloquer réellement : 1
- Activer les règles ASR (Attack Surface Reduction) pour limiter les actions effectuer par des applications malveillantes ou non approuvées :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Exploit Guard\ASR > ExploitGuard_ASR_Rules > DWORD (32-bit) > 1

6. Journalisation des évènements Windows

Ce journal permet de lister tous les événements qui ont eu lieu depuis le démarrage du PC, voir qui a été connecté, quand et pendant combien de temps.

- Activer le seuil en pourcentage pour le journal des évènements de sécurité auquel le système générera un avertissement
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security > WarningLevel > DWORD (32-bit) > 60

- Augmenter sa taille permet d'avoir plus d'informations à enregistrer :
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security > MaxSize > DWORD (32-bit) > 20480 (Ko)
- Activer l'audit met dans le journal des évènements tous les nouveaux processus créer :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit > ProcessCreationIncludeCmdLine_Enabled > DWORD (32-bit) > 1

7. Mesure de sécurité avancées

Credential Guard est une fonctionnalité de Windows basée sur la virtualisation pour LSASS qui bloque les attaquants spoofing.

- Activer Credential Guard et la sécurité basée sur la virtualisation :
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceGuard > EnableVirtualizationBasedSecurity > DWORD (32-bit) > 1

Configurer des politiques de sécurité avancé au niveau du mot de passe :

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa > MinimumPasswordLength > DWORD (32-bit) > 16 pour définir une longueur minimale du mot de passe
- PasswordComplexity permet d'exiger des mots de passe complexes (caractères spéciaux, nombre, alphabet) : 1
- MaximumPasswordAge définit le nombre de jour avant modification de mot de passe : 90 (jours)

Configurer des politiques de sécurité avancé au niveau du verrouillage de compte :

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon > MaxConsecutiveLogonFailures de type DWORD (32-bit) > 3 pour définir nombre de tentative
- AccountLockoutDuration définie la durée de verrouillage du compte en minutes : 30

LSASS (Local Security Authority Subsystem Service) est une mesure de sécurité indispensable pour sécuriser les informations d'identification stockées en mémoire sur un système Windows. LSASS est responsable de l'authentification des utilisateurs et protège contre le vol d'informations d'identification.

- Activer LSASS contre le vol d'identifications :

- Accédez au nom de la valeur RunAsPPL de type DWORD (32-bit) dans HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
- Modifiez la valeur par 1

- Activer mise à jour automatique de Windows :
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU > NoAutoUpdate > DWORD (32-bit) > 0
 - ScheduledInstallDay définit le jours de la semaine pour installer la mise à jour : 1 (dimanche)
 - ScheduledInstallTime définit l'heure de la mise à jour : 10 (heure)

D. Configuration Post-Installation

Post-Installation permet de gérer les commandes et installation des applications qui s'exécutent à la fin de la configuration de l'installation de Windows.

Pour ajouter une application, il faut charger le Setup que vous avez téléchargé sur le site officiel du logiciel. Il peut lui indiquer d'effectuer une installation en mode silencieux avec le paramètre /S et sans intervention d'un utilisateur avec /qn au lancement du Setup :

- Cliquez sur le bouton ajouter en haut à gauche > Fichier > Ajoutez le setup de 7zip, Adobe Reader, OpenOffice et Chrome Entreprise qui s'ouvre en automatique à l'ouverture d'une session utilisateur et afficher la page www.intranet.local avec un fichier .bat avec la commande ci-dessous :

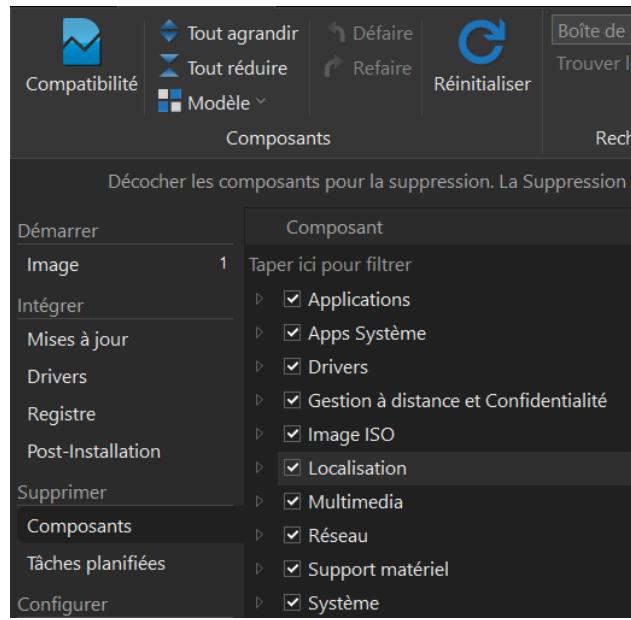
```
schtasks /create /tn "Launch Chrome" /tr "C:\Program Files\Google\Chrome\Application\chrome.exe www.intranet.local" /sc onlogon /rl highest
/f
```

- Et enfin ajouter dans Paramètre /S et /qn

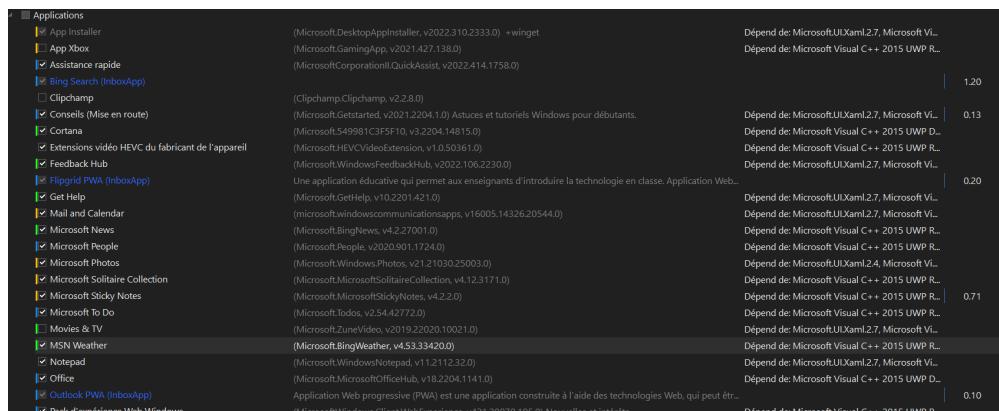
	Exécuter	7z2408-x64.exe	/qn /S	ISO	Temporaire	Existant - Insta...
	Exécuter	Reader_fr_install.exe	/qn /S	ISO	Temporaire	Existant - Insta...
	Exécuter	Apache_OpenOffice_4.1.15_Win_x86_instal...	/qn /S	ISO	Temporaire	Existant - Insta...
	Exécuter	C:\Users\alex\Downloads\GoogleChrom...	/qn /S	ISO	Temporaire	Nouveau - Insta...
	Exécuter	C:\Users\alex\Documents\ConfChrome.bat	/qn /S	ISO	Temporaire	Nouveau - Bat...

E. Configuration Composant

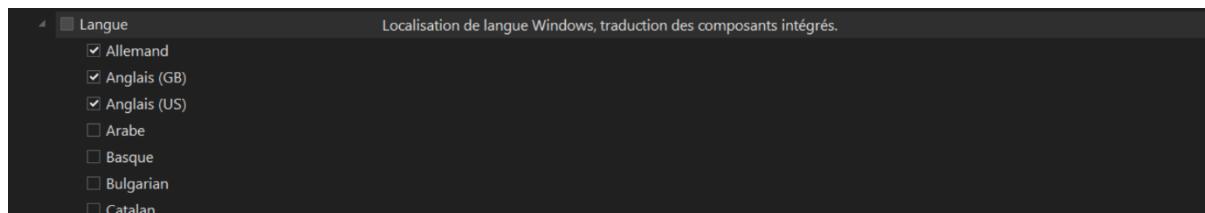
Dans le menu Composant, on trouve différents composants à intégrer ou à supprimer de l'ISO de Windows 11 qui va permettre de l'alléger :



- Le premier composant Application, permet de retirer les applications préinstallées par Microsoft qui ne sont pas nécessaire (App Xbox, Clipchamp, Xbox Game Bar) :

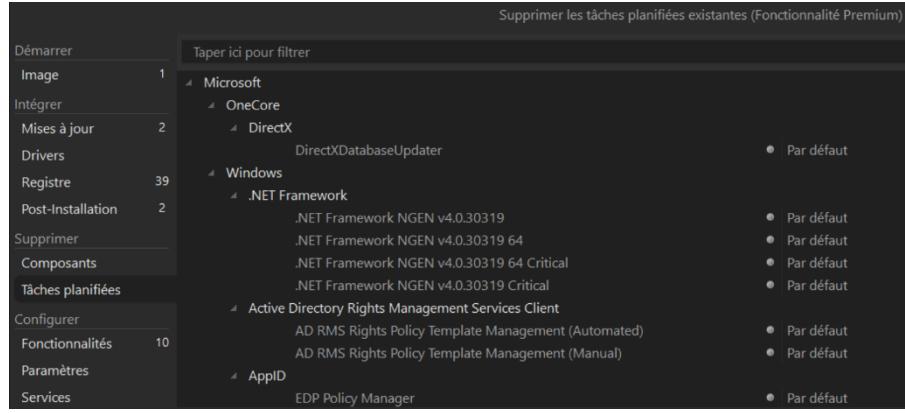


- Retirez les langues non essentielles pour alléger ISO Windows :



F. Configuration Tâches planifiées

Le menu tâches planifiées permet d'automatiser certains processus au démarrage, lors de la connexion ou à des moments spécifiques sur le système. Cette méthode est utile pour configurer des tâches qui s'exécutent automatiquement lors de l'installation ou de l'utilisation du système d'exploitation.



G. Configuration Fonctionnalités

Le menu Fonctionnalités permet d'activer ou désactiver des fonctionnalités de Windows.

Démarrer	Fonctionnalité	Description	État
Image	Taper ici pour filtrer	...	
Intégrer	> Fonctionnalités à la demande (capacités)	La désactivation des fonctionnalités supprimera la fonctionnalité, y compris la configuration...	
Mises à jour	> <input checked="" type="checkbox"/> .NET Framework 4.8 Advanced Services	Cette opération installe les services AD LDS (Active Directory Lightweight Direct...	Activé
Drivers	> Services AD LDS (Active Directory Lightweight Directory Services)	Provides services and tools to create and manage Windows Server Containers and their...	Désactivé
Registre	> Containers	IEEE Data Center Bridging	Désactivé
Post-Installation	> Data Center Bridging	Services and tools to provide a controlled and specialized experience for the end user of...	Désactivé
Supprimer	> Device Lockdown	Provides services and management tools for creating and running virtual machines and...	Désactivé
Composants	> Hyper-V	Program your application to serve HTTP requests by using core IIS functionality.	Désactivé
Tâches planifiées	> Internet Information Services Hostable Web Core	Internet Information Services provides support for Web and FTP servers, along with sup...	Désactivé
Configurer	> Internet Information Services	Controls legacy components in Windows.	Désactivé
Fonctionnalités	> Legacy Components	Controls media features such as Windows Media Player.	Activé
Paramètres	> Media Features	Windows Media Player Legacy (App)	Activé
Services	> Microsoft Defender Application Guard	Offers a secure container for internet browsing	Désactivé
Services Cachés	> Microsoft Message Queue (MSMQ) Server	Microsoft Message Queue (MSMQ) Server.	Désactivé
Unattended	> <input checked="" type="checkbox"/> Imprimer dans un PDF de Microsoft	Fournit des fichiers binaires sur le système pour créer la file d'attente Imprimer dans un...	Activé
Terminer	> Microsoft XPS Document Writer	Fournit des fichiers binaires au système pour la création de la file d'attente d'impresso...	Désactivé
Appliquer	> MultiPoint Connector	Allows your computer to be monitored and managed by the MultiPoint Manager and M...	Désactivé
	> Print and Document Services	Enable print, fax, and scan tasks on this computer.	Activé

1. Fonctionnalités principales de Windows

- .NET Framework 3.5 et 4.8 permet à certaines applications qui requièrent cette fonctionnalité donc à activer
- Services AD LDS permet la gestion des identités, maintient l'intégrité et de la sécurité des données donc à activer
- Hyper-V permet de créer et gérer des machines virtuelles donc à désactiver
- Windows Subsystem for Linux (WSL) permet de faire fonctionner des distributions Linux directement dans Windows donc à désactiver
- DirectPlay est un ancien composant pour le support de jeux plus anciens donc à désactiver

2. Outils et services

- Outils d'administration système comme l'outil de gestion des disques, le gestionnaire de périphériques, gestion d'authentification donc la plupart à activer
- Windows PowerShell est une interface ne ligne de commande pour automatiser des tâches, donc à activer

3. Capacités réseau

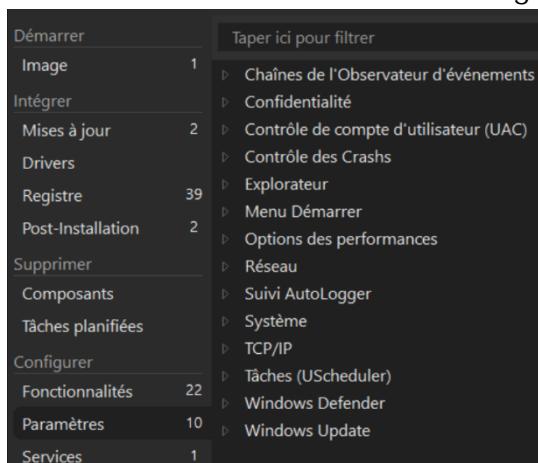
- Client SMB 1.0/CIFS est un protocole de partage de fichiers très peu sécurisé donc à désactiver
- Services de fédération Active Directory (AD FS) est environnements Active Directory complexes nécessitant des fonctionnalités de fédération donc à activer

4. Fonctionnalités liées à la sécurité

- BitLocker permet le cryptage de disque BitLocker pour sécuriser les données
- Windows Defender Application Guard permet de sécuriser les applications donc à activer
- Windows Defender permet de sécuriser le système donc à activer

H. Configuration Paramètre

Le menu Paramètre permet des modifications visuelles sur le post mais aussi de désactiver des applications promotionnelles préinstallées par Windows, d'activer ou désactiver certains services, fonction et applications de Windows comme la barre de tâche Widget.



I. Configuration Services

Le menu Service permet de gérer et de personnaliser le type de démarrage des services Windows qui seront activés ou désactivés au démarrage ou encore lorsqu'une application se lance. Les services Windows sont des processus en arrière-plan qui permettent à certaines fonctionnalités du système ou à des applications de fonctionner correctement.

Démarrer	Taper ici pour filtrer
Image	1
Intégrer	
Mises à jour	2
Drivers	
Registre	39
Post-Installation	2
Supprimer	
Composants	
Tâches planifiées	
Configurer	
Fonctionnalités	22
Paramètres	10
Services	1
Taper ici pour filtrer	
	Accès aux données utilisateur
	Acquisition d'image Windows (WIA)
	Agent Activation Runtime
	Agent de stratégie IPsec
	Alimentation
	Appel de procédure distante (RPC)
	Application Host Helper Service
	Application système COM+
	Assistance IP
	Assistance NetBIOS sur TCP/IP
	Assistant Connectivité réseau
	Assistant Connexion avec un compte Microsoft
	Audio Windows
	Authentification naturelle
	BranchCache
	Manuel
	Manuel
	Manuel
	Manuel
	Automatique
	Automatique
	Automatique
	Manuel

1. Désactiver les services inutiles

Tous les services utilisent des ressources au processeur ce qui peut ralentir le pc, certains services ne sont pas essentiels pour le bon fonctionnement du système. Leur désactivation va permettre d'alléger le système et d'améliorer les performances.

- Le service Hyper-V si vous n'utilisez pas le service de virtualisation
- Le service de Biométrie si vous ne voulez pas utiliser la reconnaissance faciale ou digital
- Le service de géolocalisation si vous ne voulez pas utiliser des applications nécessaires la géolocalisation
- Le service de démo du magasin

2. Configurer des services essentiels

Vous pouvez également configurer des services critiques pour garantir que le système fonctionne comme prévu :

- Windows Update permet de mettre Windows à jour automatiquement
- Pare-feu Windows permet la sécurisation du système

J. Configuration Services cachées

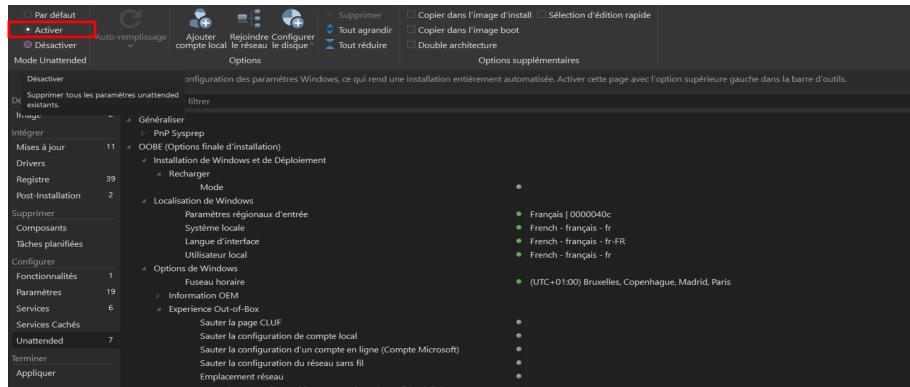
Le menu Service cachée permet de gérer et de personnaliser les services Windows qui ne sont pas visible.

Démarrer	Taper ici pour filtrer
Image	1
Intégrer	
Mises à jour	2
Drivers	
Registre	39
Post-Installation	2
Supprimer	
Composants	
Tâches planifiées	
Configurer	
Fonctionnalités	22
Paramètres	10
Services	1
Services Cachés	
Taper ici pour filtrer	
	1394 ohci compliant host controller
	3ware
	acpi devices driver
	acpi power meter driver
	acpi processor aggregator driver
	acpi wake alarm driver
	Acx01000
	adaptec sas/sata-ii raid storport's miniport driver
	ADP80XX
	afunix
	amd gpio client driver
	amd i2c controller service
	amd k8 processor driver
	amd processor driver
	amdsata
	amdsbs
	Manuel
	Démarrer
	Manuel
	Démarrer
	Démarrer
	Système
	Manuel
	Manuel
	Manuel
	Démarrer
	Démarrer

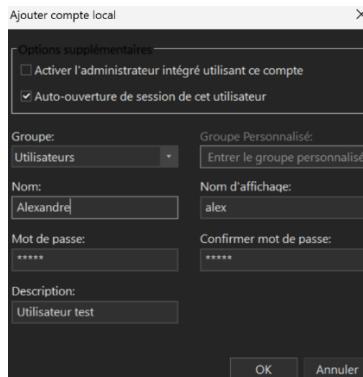
K. Configuration Unattended

Le menu Unattended permet configurer l'installation de Windows 11 sans l'intervention de l'utilisateur et même sauté des étapes comme configuration du compte local et du compte Microsoft.

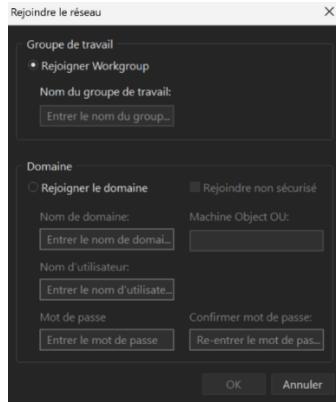
- Cliquez sur « Activer » en haut à gauche :



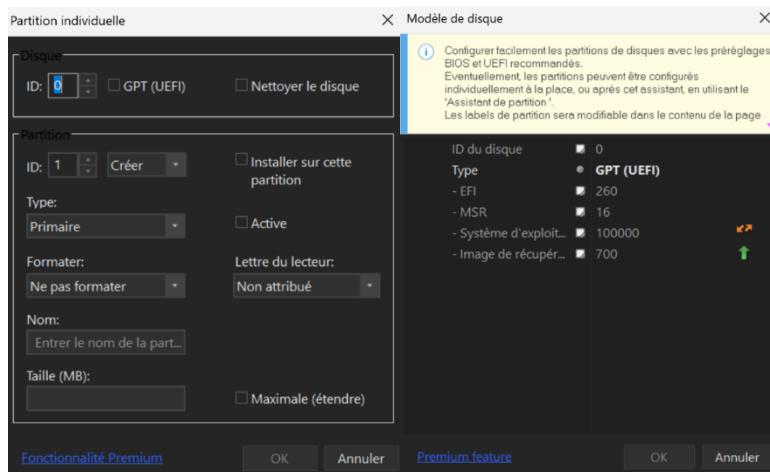
- En cliquant sur « Ajouter compte local » vous pouvez configurer un compte utilisateur personnalisé qui sera automatiquement créé lors de l'installation :



- En cliquant sur « Rejoindre le réseau » vous permet de rejoindre durant l'installation un réseau :

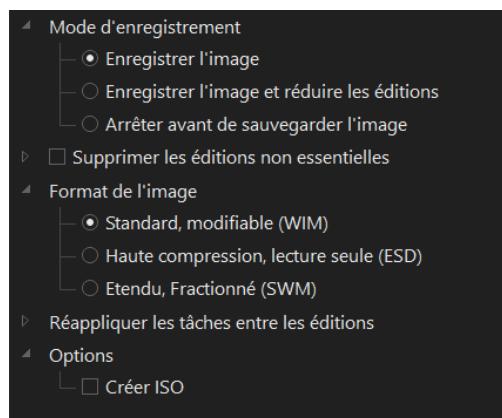


- En cliquant sur « Configurer le disque » vous permet de configurer automatiquement le partitionnement et formatage des disques lors de l'installation :

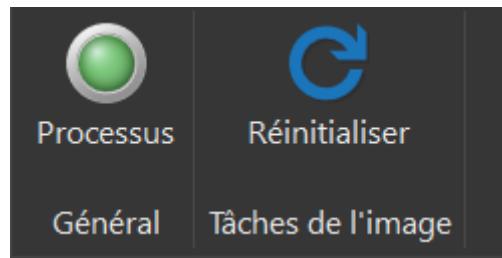


L. Création de l'ISO personnaliser de Windows 11

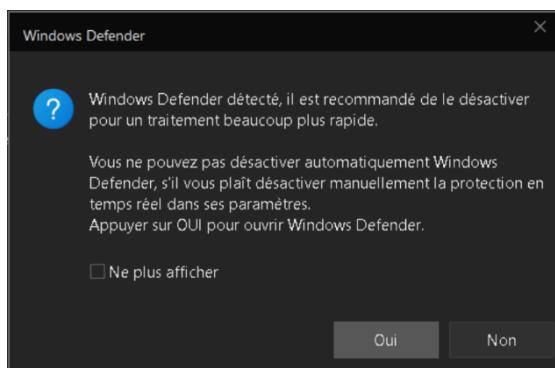
- Lorsque tout a été bien paramétré, cliquez sur Appliquer > Options > Crée l'ISO > indiquez l'emplacement et le nom de l'ISO :



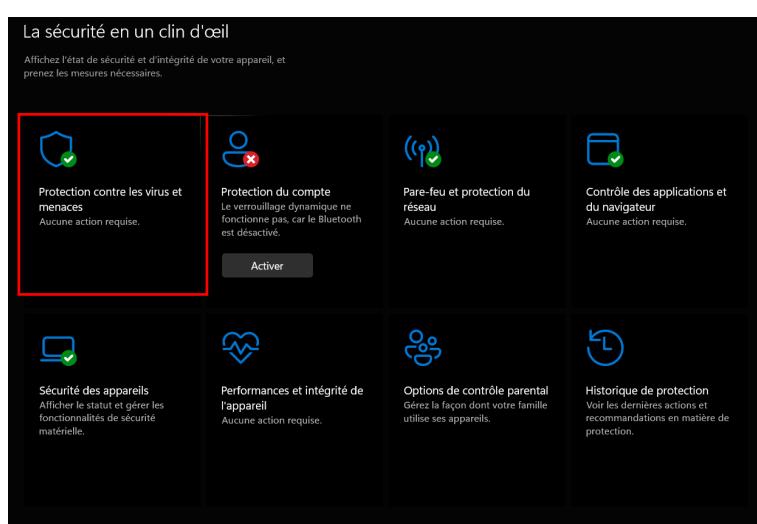
- Cliquez-en haut à droit « Processus » sur le bouton lancer la création de l'ISO personnalisée de Windows 11 :



- NTLite vous demande de désactiver Windows Defender pour gagner en ressource, cliquez sur « Oui » :



- Windows Defender s'ouvre cliquez sur « Protection contre les virus et menaces » :



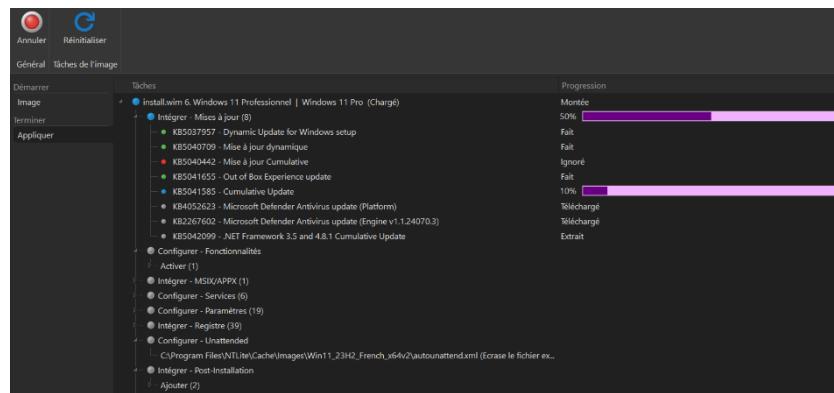
- Allez sur la rubrique « Paramètre de protection de protection contre les virus et menaces » cliquez sur « Gérer les paramètres » :



- Allez sur la rubrique « Protection en temps réel » cliquez sur « Activé » pour le désactivé :



- La création de l'ISO débute et prend énormément de temps puis une fenêtre vous indique la fin de la création de l'ISO :



III. Déploiement par Clé USB

A. Création d'une Clé USB bootable

- Insérez votre clé USB
- Ouvrez l'invite de commande en mode administrateur et lancez « Diskpart » pour le partitionner l'USB :

```
C:\Windows\System32>diskpart

Microsoft DiskPart version 10.0.22621.1

Copyright (C) Microsoft Corporation.

Sur l'ordinateur : LAPTOP-CTJMFVFG

DISKPART>
```

- Tapez les lignes de commandes ci-dessous pour connaitre le numéro du disque à préparer :

```
DISKPART> list disk

  N° disque  Statut          Taille    Libre     Dyn  GPT
  -----  -----  -----  -----  -----  -----
  Disque 0   En ligne       476 G octets  1024 K octets
  Disque 1   En ligne      7455 M octets    0 octets
```

- Tapez les lignes de commandes ci-dessous sur la ligne **select disk** tapez le numéro de votre clé USB puis tapez la commande **clean** :

```
DISKPART> select disk 1

Le disque 1 est maintenant le disque sélectionné.

DISKPART> clean

DiskPart a réussi à nettoyer le disque.
```

- Tapez les lignes de commandes ci-dessous pour créer le partitionnement du disk puis tapez la commande **exit** :

```
DISKPART> create partition primary
DiskPart a réussi à créer la partition spécifiée.

DISKPART> select partition 1
La partition 1 est maintenant la partition sélectionnée.

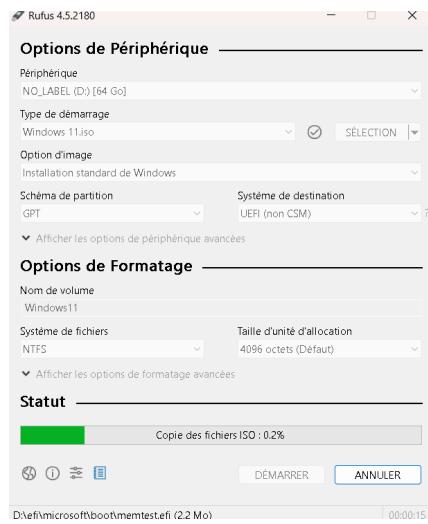
DISKPART> format fs=ntfs quick
 100 pour cent effectués
DiskPart a formaté le volume.

DISKPART> active
DiskPart a indiqué la partition actuelle comme étant active.

DISKPART> assign
DiskPart a correctement assigné la lettre de lecteur ou le point de montage.

DISKPART> exit
```

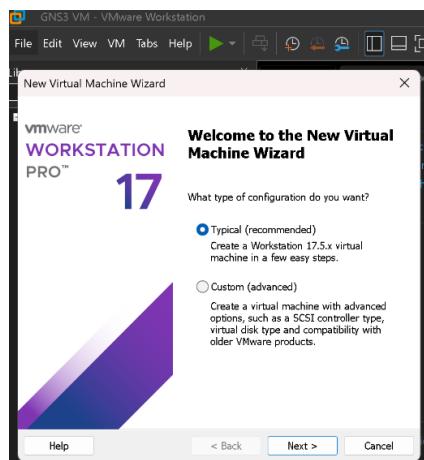
- Vous pouvez aussi utiliser le logiciel Rufus (https://rufus.ie/fr/#google_vignette) pour créer une clé USB bootable avec la configuration ci-dessous :



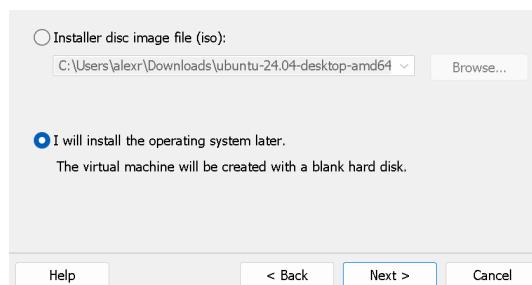
B. Installation de l'ISO sur la VM

Installer de la VM sur VMware Workstation :

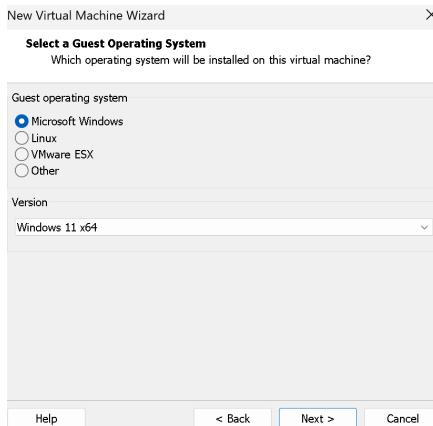
- Cliquez-en haut à gauche sur File puis sur « New Virtual Machine »
- Choisissez « Typical » puis cliquez sur « Next » :



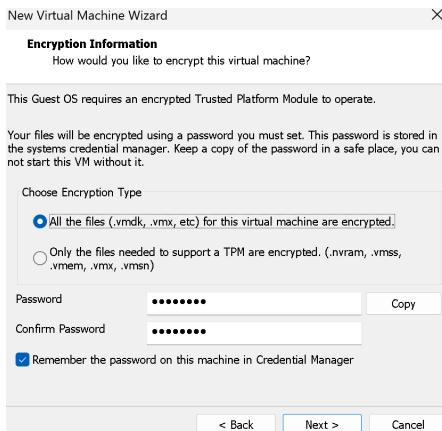
- Sélectionnez « I will install the operating system later » puis cliquez sur « Next »:



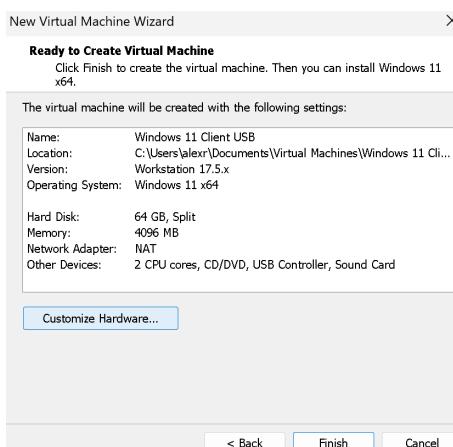
- Sélectionnez le système d'exploitation Microsoft Windows et sa version Windows 11 puis cliquez sur « Next » :



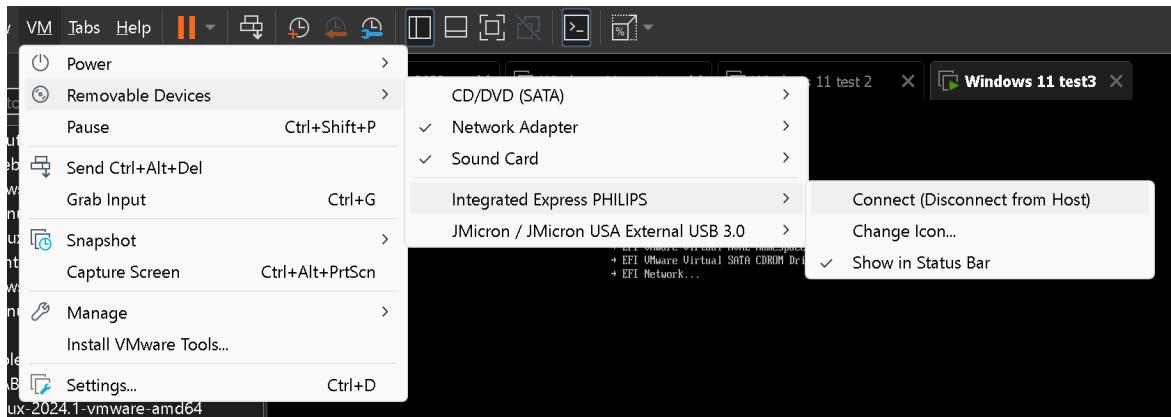
- Sélectionnez « All the files » pour le type d'encryptions et mettez un mot puis cliquez sur « Next » :



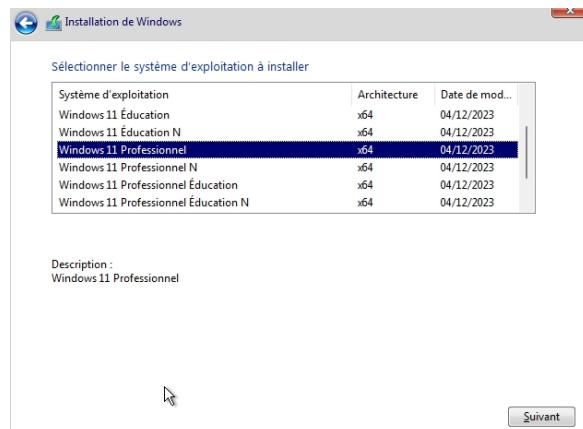
- Une fenêtre de récapitulation des informations s'affiche grâce au bouton « Customize Hardware », puis cliquez sur « Finish » si toutes les informations sont correctes :



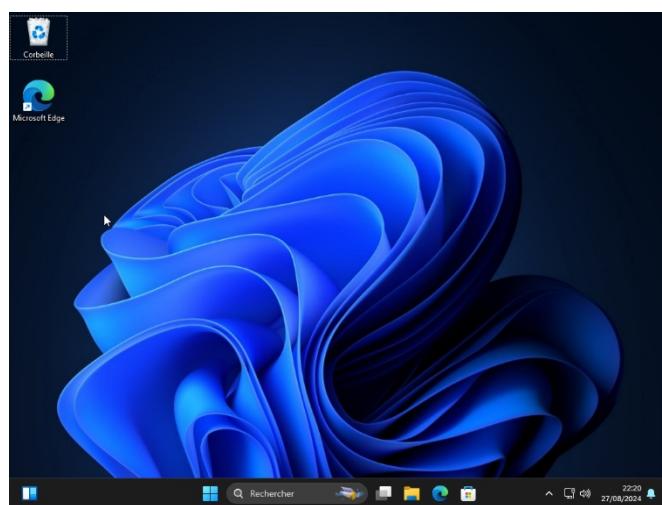
- Insérez la Clé USB Bootable, lancez la VM, cliquez sur VM puis cliquez sur « Removable Devices », sélectionnez la clé puis cliquez sur « Connect (Disconnect from Host) » :



- Le menu d'installation de Windows va s'afficher automatiquement puis sélectionnez une version Windows et cliquez sur « Suivant » :



- A la fin du déploiement la machine va se redémarrer et se mettre sur un système parfaitement fonctionnel et configurer en fonction de votre ISO :



IV. Déploiement par le réseau avec un serveur Fog

Fog (Free OpenSource Ghost) est un logiciel gratuit de capture et de déploiement d'images systèmes. Fog utilise un serveur PXE (Preboot eXecution Environnement) qui permet aux postes de démarrer sur le réseau sans avoir besoin de CD, de Clé USB ou disque dur local. Il inclut une interface web de gestion des machines et d'images avec des outils pour réinitialiser les mots de passe Windows, installer des logiciels à distance et effectuer des tâches de maintenance. Le serveur sera installé sur une VM Ubuntu.

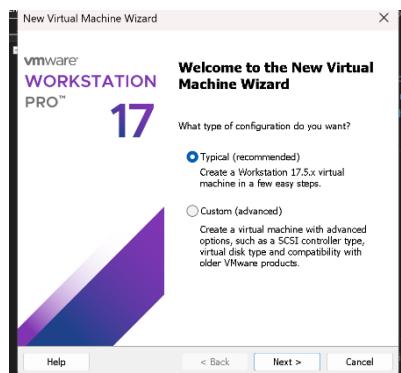
A. Téléchargement et installation d'une VM Ubuntu

- Télécharger l'ISO d'Ubuntu avec le lien <https://www.ubuntu-fr.org/download/> :

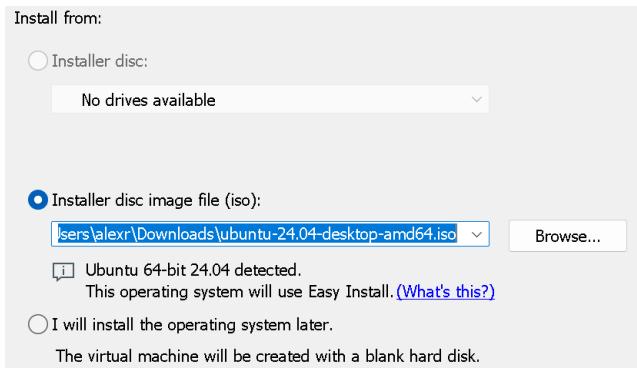


Installer de la VM sur VMware Workstation :

- Cliquez-en haut à gauche sur File puis sur New Virtual Machine
- Choisissez « Typical » puis cliquez sur « Next » :



- Sélectionnez « Installer disc image file (iso) » puis sélectionner l'ISO Ubuntu téléchargé précédemment et cliquez sur « Next » :



- Saisissez les informations de votre utilisateur puis cliquez sur « Next » :

Full name:	alexg
User name:	admin
Password:	*****
Confirm:	*****

- Renommez le nom de la VM et sélectionnez son emplacement puis cliquez sur « Next » :

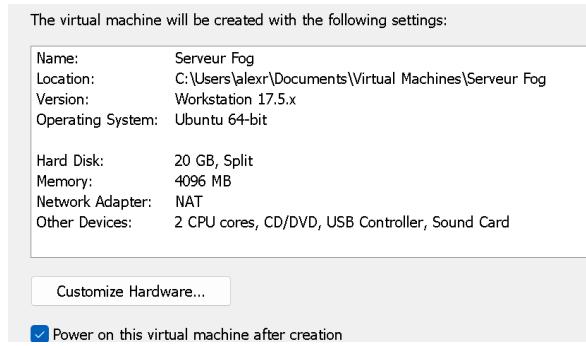
Virtual machine name:	Serveur Fog
Location:	C:\Users\alexr\Documents\Virtual Machines\Serveur Fog
The default location can be changed at Edit > Preferences.	

- Modifiez la taille du disque si vous avez besoin de plus d'espace puis cliquez sur « Next » :

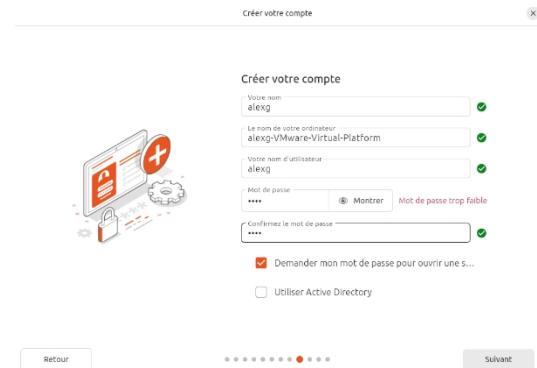
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):	20.0
Recommended size for Ubuntu 64-bit: 20 GB	
<input type="radio"/> Store virtual disk as a single file <input checked="" type="radio"/> Split virtual disk into multiple files	
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.	

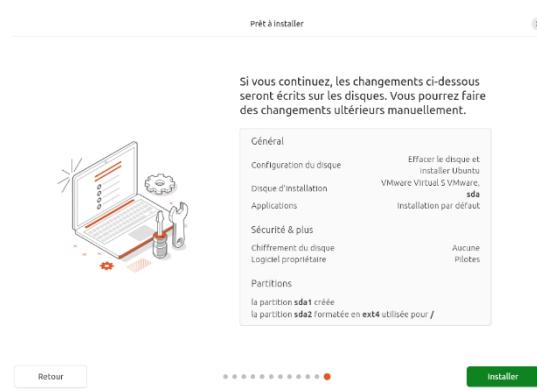
- Une fenêtre de récapitulation des informations s'affiche grâce au bouton « Customize Hardware » vous pouvez rajouter ou paramétré les composants de votre vm comme ajouter une adaptateur réseau supplémentaire essentiel pour le serveur Fog expliquer dans « B. Configuration de la VM ». Cliquez sur « Finish » si toutes les informations sont correctes :



- La machine virtuelle va ensuite démarrer sur le système d'exploitation Ubuntu. Une fenêtre d'installation va vous demander de choisir votre configuration pour la langue, l'accessibilité d'Ubuntu, du clavier, de la connexion, des mises à jour disponible, du type d'installation par défaut avec ou sans application préinstallée, du fuseau horaire.
- Créez votre compte puis cliquez sur « Suivant » :



- Une fenêtre de récapitulation des informations s'affiche puis cliquez sur « Installer » si toutes les informations sont correctes :



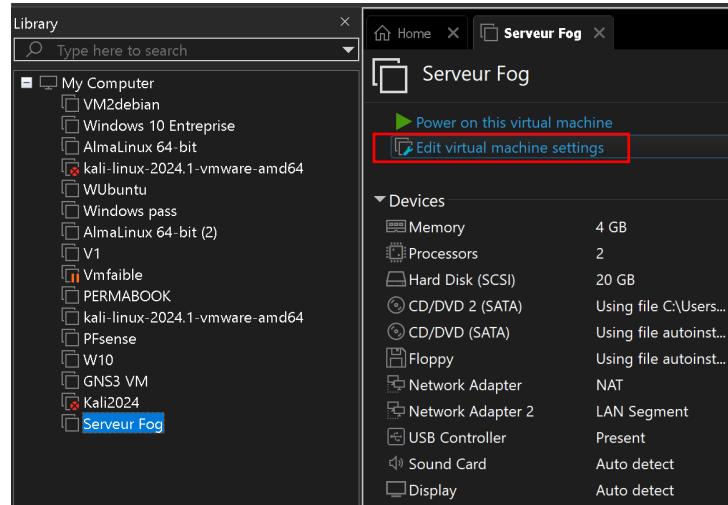
B. Configuration de la VM

1. Configuration de l'interface réseau

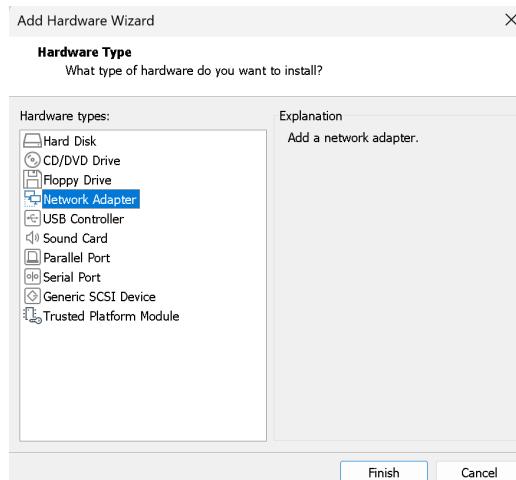
LAN segment est un réseau isolé principalement utilisés pour créer des environnements de test ou des configurations réseau spécifiques sans interférence avec le réseau physique de l'hôte.

Vmware Workstation permet de modifier la configuration matérielle de la vm comme ajouter des interfaces réseau en NAT pour avoir internet via l'hôte ou créer des réseaux isolés.

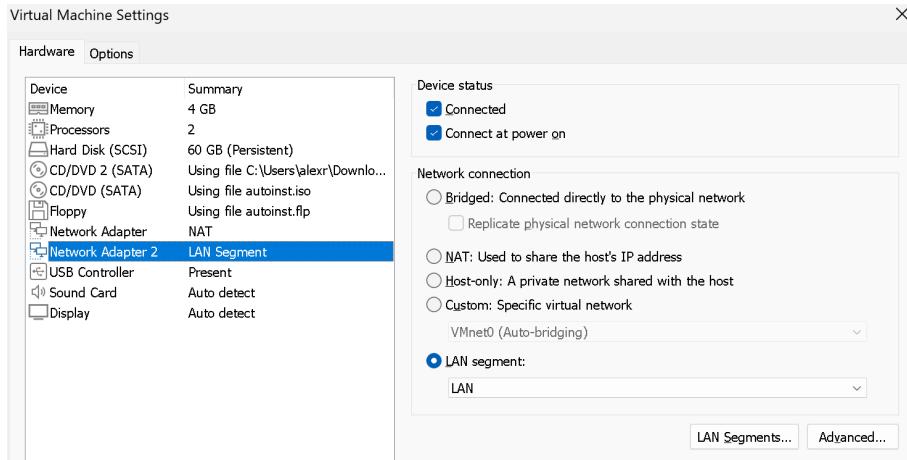
- Fermez la VM Ubuntu, cliquez sur « Edit Virtual Machine Settings » :



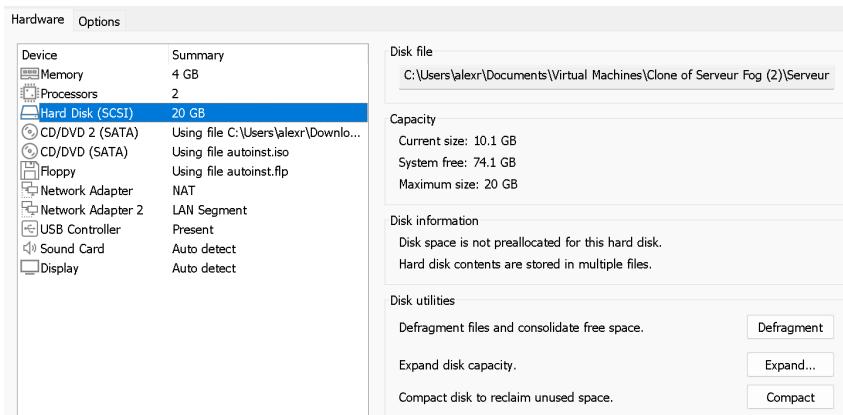
- Ajoutez une nouvelle interface réseau en Cliquez sur « Add », sélectionnez « Network Adapter » puis « Finish » et validez les modifications :



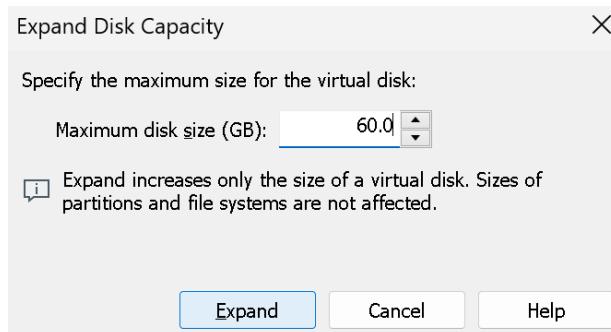
- Cliquez sur l'interface ajouté, sélectionnez « LAN segment » puis « LAN » :



- Ajoutez aussi plus d'espace disque car l'image de la machine Windows risque pèse autour des 10Go. Cliquez sur « Hard Disk (SCSI) » puis sur « Expand Disk Capacity » :



- Tapez la taille maximum de l'espace disque, cliquez sur « Expand » puis sur « OK ». Il faut redimensionner la partition dans Ubuntu pour utiliser cet espace supplémentaire :



- Maintenant entrez dans la vm, lancez l'invite d'Ubuntu puis tapez la commande ci-dessous pour être en root pour avoir tous les priviléges :

```

root@alexg-VMware-Virtual-Platform: /home/alexg
alexg@alexg-VMware-Virtual-Platform: ~ $ sudo su
[sudo] Mot de passe de alexg :
root@alexg-VMware-Virtual-Platform: /home/alexg#

```

- Installez « gparted » est un logiciel d'édition de partition avec une interface graphique en tapant la commande ci-dessous :

```

root@alexg-VMware-Virtual-Platform:/home/alexg# sudo apt install gparted
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  gparted-common libatkmm-1.6-1v5 libcairomm-1.0-1v5 libglibmm-2.4-1t64 libgtkmm-3.0-1t64 libpangomm-1.4-1v5
  libparted-fs-resize0t64 libsigc++-2.0-0v5
Paquets suggérés :
  dmraid gpart jfsutils kpartx mtools reiser4progs reiserfsprogs udf-tools xfsprogs exfatprogs libparted-dev
Les NOUVEAUX paquets suivants seront installés :
  gparted gparted-common libatkmm-1.6-1v5 libcairomm-1.0-1v5 libglibmm-2.4-1t64 libgtkmm-3.0-1t64 libpangomm-1.4-1v5
  libparted-fs-resize0t64 libsigc++-2.0-0v5
0 mis à jour, 9 nouvellement installés, 0 à enlever et 23 non mis à jour.
Il est nécessaire de prendre 2 311 ko dans les archives.
Après cette opération, 10,9 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o

```

- Tapez « sudo gparted » pour ouvrir le logiciel graphique :

```

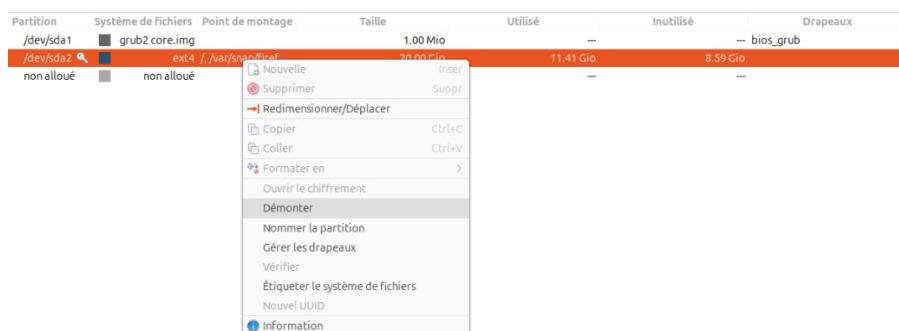
root@alexg-VMware-Virtual-Platform:/home/alexg# sudo gparted

```

- L'espace surligné en orange représente l'espace utilisé par la VM et celle juste en-dessous est l'espace appelé « non alloué », elle n'est pas utilisée par la VM car elle vient d'être ajouté :



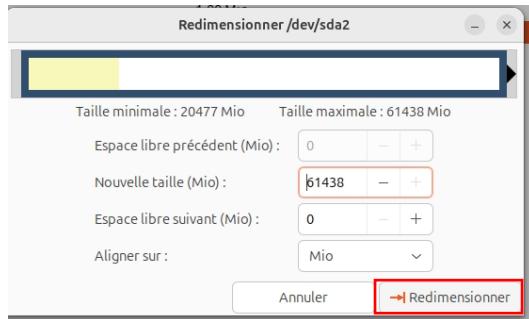
- Clic droit sur la partition, en orange puis cliquez sur « Démonter » :



- Clic sur « Redimensionner/déplacer » :



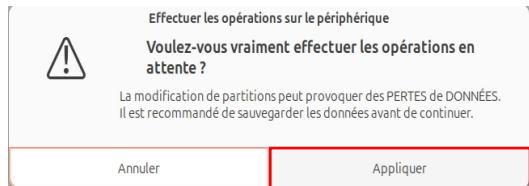
- Redimensionnez l'espace et cliquez sur « Redimensionner » :



- Clic sur le bouton validé :



- Clic sur « Appliquer » :

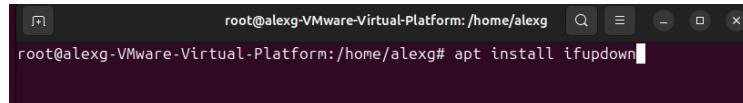


- L'espace disque sera afficher à la bonne taille :



Commande optionnelle :

- Tapez la commande ci-dessous pour installer ifupdown qui est un outil simple et efficace pour gérer les interfaces réseau sur Linux et Ubuntu :



```
root@alexg-VMware-Virtual-Platform:/home/alexg# apt install ifupdown
```

- Tapez la commande ci-dessous pour installer net-tools qui contient un ensemble de programme de contrôle de sous-système réseau sur Linux et Ubuntu comme netstat -tuln pour afficher les connexions réseau actives, les tables de routage ou encore route -n pour afficher ou manipuler la table de routage :

```
root@alexg-VMware-Virtual-Platform:/home/alexg# apt install net-tools
```

- Tapez la commande ip a pour connaître le nom des interfaces :

```
alexg@alexg-VMware-Virtual-Platform:~$ sudo su
[sudo] Mot de passe de alexg :
root@alexg-VMware-Virtual-Platform:/home/alexg# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:c9:70:a6:4d brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.254.132/24 brd 172.16.254.255 scope global dynamic noprefixroute ens3
        valid_lft 1106sec preferred_lft 1106sec
        inet6 fe80::20c:29ff:fe70:a64d/64 scope link
            valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:c9:70:a6:57 brd ff:ff:ff:ff:ff:ff
    altname enp2s2
root@alexg-VMware-Virtual-Platform:/home/alexg#
```

- Pour configurer les 2 interfaces réseaux, tapez la commande ci-dessous pour accéder au fichier des interfaces réseaux :

```
root@alexg-VMware-Virtual-Platform:/home/alexg# nano /etc/netplan/*.yaml
```

- Faites un Ctrl+X pour accéder au fichier /etc/netplan/50-cloud-init.yaml:

```
[1/2]                                     /etc/netplan/01-networ
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
```

- Tapez les informations spécifiques des différentes interfaces ci-dessous, puis pour sauvegarder et quitter le fichier faites Ctrl+X :

```
[ 1/1] /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        ens33:
            dhcp4: true
        ens34:
            addresses: [192.168.1.1/25]
            dhcp4: false
    version: 2
```

- Pour appliquer les modifications effectuer précédent, tapez la commande ci-dessous. S'il y a des erreurs dans la configuration, netplan vous le signalera :

```
root@alexg-VMware-Virtual-Platform:/home/alexg# sudo netplan apply
```

- Une la commande effectuer, NetworkManager va mettre à jour les interfaces configurer. Vous pouvez vérifier si les modifications ont bien été pris en compte en tapant la commande ip a :

```
root@alexg-VMware-Virtual-Platform:/home/alexg# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:70:a6:4d brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.254.132/24 brd 172.16.254.255 scope global dynamic noprefixroute ens3
        valid_lft 1778sec preferred_lft 1778sec
    inet6 fe80::20c:29ff:fe0:a64d/64 scope link
        valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:70:a6:57 brd ff:ff:ff:ff:ff:ff
    altname enp2s2
    inet 192.168.1.1/25 brd 192.168.1.127 scope global noprefixroute ens34
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe0:a657/64 scope link
        valid_lft forever preferred_lft forever
root@alexg-VMware-Virtual-Platform:/home/alexg#
```

2. Mise à jour et mise à niveau

- Tapez la commande ci-dessous pour mettre à jours les paquets :

```
root@alexg-VMware-Virtual-Platform:/home/alexg# apt update && apt upgrade -y
```

3. Téléchargement et installation du logiciel Fog Projet

- Téléchargez le logiciel Fog Projet en format TAR.GZ avec le lien <https://fogproject.org/download.php> :

Downloading

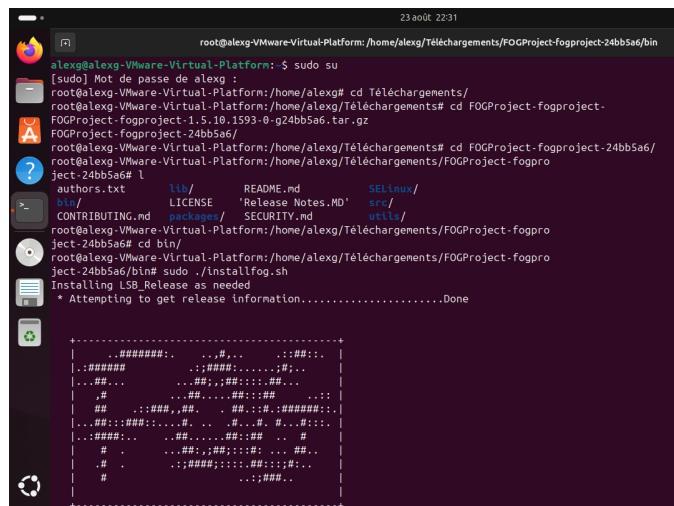
You can download a pre-packaged tarball of the latest release of FOG Project, v1.5.10.1593, from [TAR.GZ](#) or [ZIP](#). Please verify that your download matches one of the following checksums:

md5: 30c7aa471c0122bc05a7fd1330e292c	fogproject-1.5.10.1593.tar.gz
sha1: fe0e7f052069483cbe970f70a9339e327bfae647	fogproject-1.5.10.1593.tar.gz

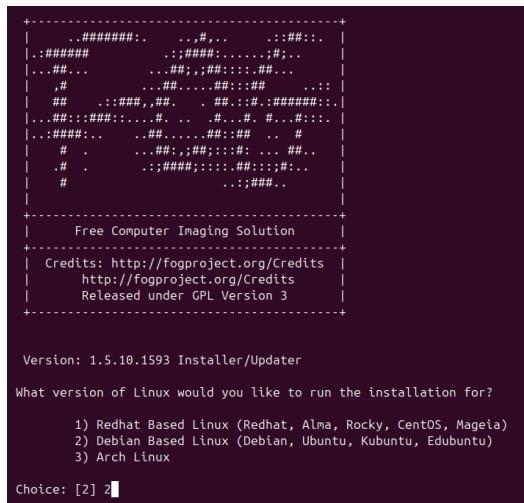
- Utilisez le terminal d'Ubuntu, accédez au dossier compressez en allant dans « Téléchargements » avec la commande **cd Téléchargements** puis décompresser le dossier avec la commande « Téléchargements » :

```
root@alexg-VMware-Virtual-Platform:/home/alexg# cd Téléchargements/
root@alexg-VMware-Virtual-Platform:/home/alexg/Téléchargements# ls
FOGProject-fogproject-1.5.10.1593-0-g24bb5a6.tar.gz
root@alexg-VMware-Virtual-Platform:/home/alexg/Téléchargements# tar xvzf FOGProject-fogproject-1.5.10.1593-0-g24bb5a6.tar.gz
```

- Accédez au fichier bin du dossier décompresser avec la commande **cd fogproject-1.5.10.1593/bin** puis installer le logiciel Fog avec la commande **sudo ./installfog.sh** :



- L'installation se lance et nous demandé de choix la distribution dans notre cas c'est Ubuntu donc tapez 2 :



- Demande de type d'installation, tapez « N » pour avoir « Normal Server » :

```
FOG Server installation modes:  
* Normal Server: (Choice N)  
    This is the typical installation type and  
    will install all FOG components for you on this  
    machine. Pick this option if you are unsure what to pick.  
  
* Storage Node: (Choice S)  
    This install mode will only install the software required  
    to make this server act as a node in a storage group  
  
More information:  
http://www.fogproject.org/wiki/index.php?title=InstallationModes  
  
What type of installation would you like to do? [N/s (Normal/Storage)] n
```

- Demande si la carte réseau par défaut est bien celle indiquer, tapez « N » pour choisir une autre interface puis tapez l'autre la **ens34** :

```
We found the following interfaces on your system:  
* ens33 - 172.16.254.132/24  
* ens34 - 192.168.1.1/25  
  
Would you like to change the default network interface from ens33?  
If you are not sure, select No. [y/N] y  
What network interface would you like to use? ens34
```

- Demande s'il faut configurer l'adresse du routeur comme serveur DHCP, tapez « N » :

```
Would you like to setup a router address for the DHCP server? [Y/n] n
```

- Demande s'il faut utiliser le serveur DHCP pour gérer DNS, tapez « N » :

```
Would you like DHCP to handle DNS? [Y/n] n
```

- Demande s'il faut utiliser le serveur Fog comme service DHCP, tapez « Y » :

```
Would you like to use the FOG server for DHCP service? [y/N] y
```

- Demande s'il faut activer Secure HTTPS sur serveur Fog, tapez « N » :

```
Using encrypted connections is state of the art on the web and we  
encourage you to enable this for your FOG server. But using HTTPS  
has some implications within FOG, PXE and fog-client and you want  
to read https://wiki.fogproject.org/HTTPS before you decide!  
Would you like to enable secure HTTPS on your FOG server? [y/N] n
```

- Demande s'il faut garder le nom de domaine indiquer, tapez « Y » :

```

Which hostname would you like to use? Currently is: alexg-VMware-Virtual-Platform
Note: This hostname will be in the certificate we generate for your
FOG webserver. The hostname will only be used for this but won't be
set as a local hostname on your server!
Would you like to change it? If you are not sure, select No. [y/N]
FOG would like to collect some data:
  We would like to collect the following information:
    1. OS Name (CentOS, RedHat, Debian, etc....)
    2. OS Version (8.0.2004, 7.2.1409, 9, etc....)
    3. FOG Version (1.5.9, 1.6, etc....)

```

- Demande si les informations afficher sont correctes, si oui tapez « Y » :

```

* Here are the settings FOG will use:
* Base Linux: Debian
* Detected Linux Distribution: Ubuntu
* Interface: ens34
* Server IP Address: 192.168.1.1
* Server Subnet Mask: 255.255.255.128
* Hostname: alexg-VMware-Virtual-Platform
* Installation Type: Normal Server
* Internationalization: Yes
* Image Storage Location: /images
* Using FOG DHCP: Yes
* DHCP router Address:
* Send OS Name, OS Version, and FOG Version: Yes

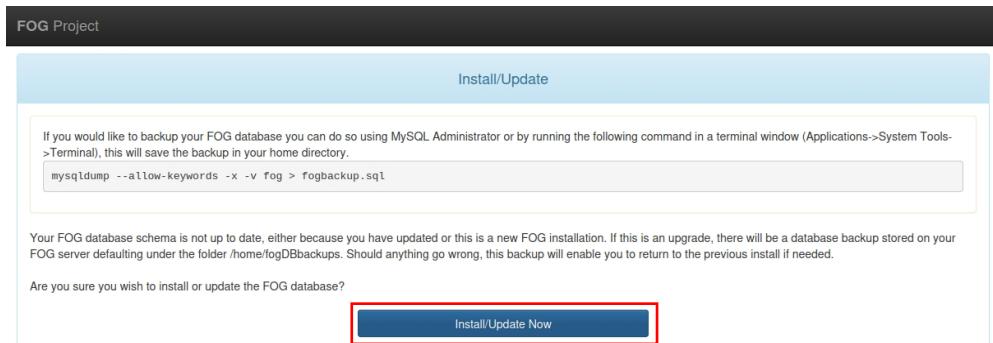
* Are you sure you wish to continue (Y/N) y

```

- L'installation du serveur Fog va télécharger et installer de nombreux paquet essentiel à son utilisation. Une fois le processus terminé, connecter vous avec le lien donné pour accéder à l'interface web de management de Fog :

<http://192.168.1.1/fog/management>

- Après avoir ouvert le lien, cliquez sur le bouton « Install/update Now » :



- Retournez sur votre invite de commande et appuyer sur la touche « Entrée » pour confirmer l'initiation de votre serveur Fog :

```
* Press [Enter] key when database is updated/installed.█
```

- A la fin du processus, vous obtenez un récapitulatif complet avec l'adresse IP de Fog et les identifiants à une première connexion :

```
* Setup complete

You can now login to the FOG Management Portal using
the information listed below. The login information
is only if this is the first install.

This can be done by opening a web browser and going to:
http://192.168.1.1/fog/management

Default User Information
Username: fog
Password: password

* Changed configurations:

The FOG installer changed configuration files and created the
following backup files from your original files:
* /etc/dhcp/dhcpd.conf <=> /etc/dhcp/dhcpd.conf.1724445105
* /etc/vsftpd.conf <=> /etc/vsftpd.conf.1724445105
* /etc/exports <=> /etc/exports.1724445105
```

- Retournez la page web pour entrer les informations nécessaires pour une première connexion puis cliquez sur « Login » :

FOG Project

Username: fog

Password: *****

Language: Français

Login

Estimated FOG Sites: 3506

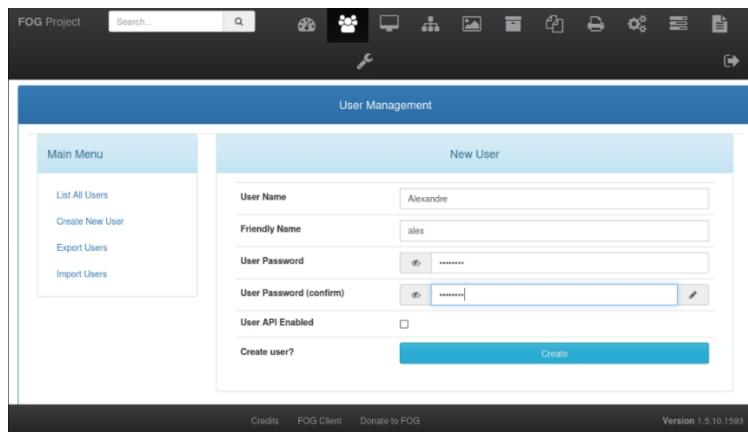
Latest Version: 1.5.10.1593

Latest Development Version: 1.5.10.1593

- Vous accédez à l'écran principal de Fog » :



- Créez un utilisateur en cliquant sur l'icône de « User Management Edit » puis sur « Create New User » :

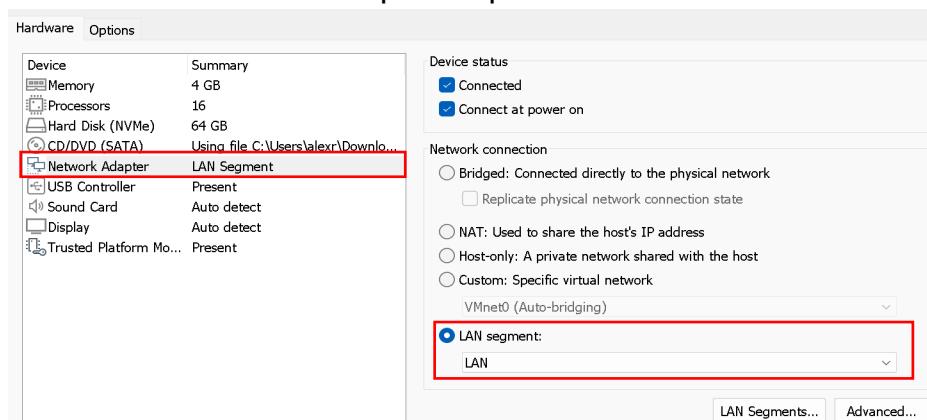


C. Création d'une image

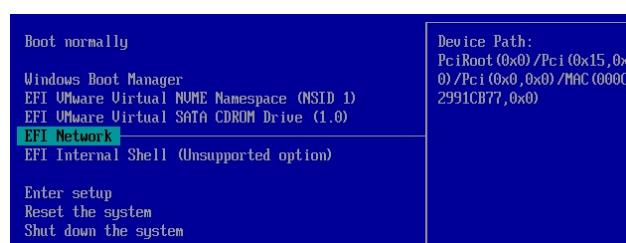
1. Enregistrement d'une machine dans l'inventaire du serveur Fog

Vous allez enregistrer la machine utiliser pour le déploiement par clé USB dans l'inventaire afin de la capturer et de pouvoir la déployer :

- Changez le type de carte réseau de votre machine en la mettant dans le même réseau que le server Fog en cliquant sur « Edit virtual machine settings » puis sur « Network Adapter » et sélection le bon réseau puis cliquez sur « OK » :



- Lancez la machine en appuyant sur F12 pour aller dans le menu Boot et choisir l'ordre d'amorçage « EFI Network » :



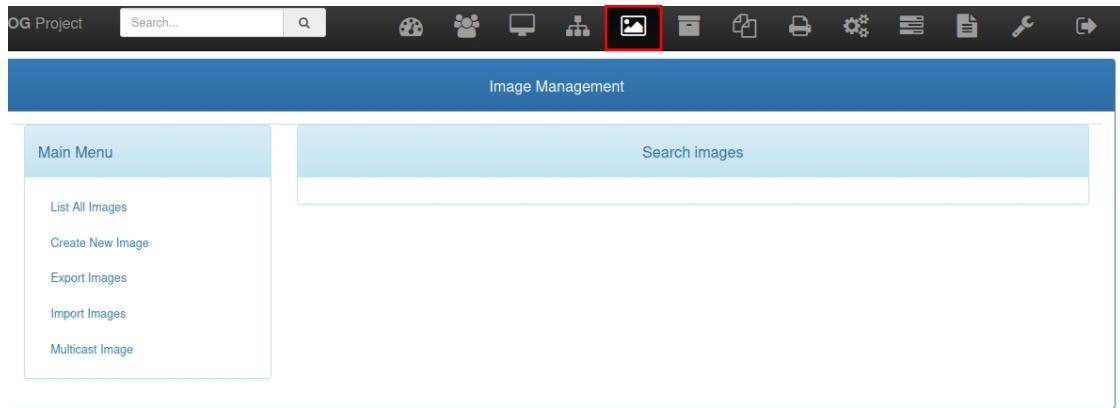
- Attendez l'affichage du menu d'accueil de Fog et sélectionnez l'option « Quick Registration and Inventory » ce qui va l'enregistrer sur le serveur :



- La machine s'enregistre et redémarre une fois finie :

2. Creation d'une image

- Retournez sur l'interface du serveur Fog et allez dans « Image Management » :



- Cliquez sur « Create New Image » puis complétez les rubriques comme ci-dessous et cliquez sur « Ajoutez » :

Image Name	img-W11
Image Description	
Operating System	Windows 10 - (9)
Image Path	/images/img-W11
Image Type	Multiple Partition Image - Single Disk (Not Resizable) - (2)
Partition	Everything - (1)
Protected	<input type="checkbox"/>
Image Enabled	<input checked="" type="checkbox"/>
Replicate?	<input checked="" type="checkbox"/>
Compression	6
Image Manager	Partclone Zstd
Make Changes?	Update

- Dans l'interface du serveur Fog et allez sur « Host Management » puis cliquez sur « List All Hosts » pour nommer l'hôte et affecter la future image :

Host	Imaged	Task	Assigned Image
000c2991cb77 00:0c:29:91:cb:77	No Data		

- Cliquez sur le nom de l'hôte qui est dans notre cas l'adresse mac de la vm en bleu puis complétez les rubriques comme ci-dessous avec l'image créée et cliquez sur « Update » :

Host general

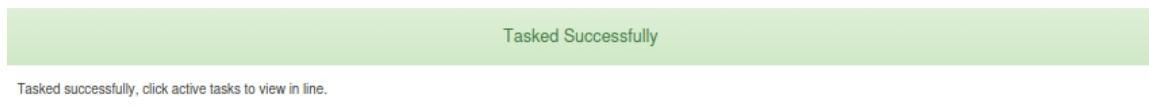
Host Name	Win_11		
Primary MAC	00:0C:29:91:CB:77	Lead MAC Vendors	LM.C. I.M.I.
Host description	Created by FOG Reg on August 27, 2024, 4:25 pm		
Host Product Key			
Host Image	img-W11 - (2)		
Host Kernel			
Host Kernel Arguments			
Host Init			
Host Primary Disk			
Host Bios Exit Type	- Please Select an option -		
Host EFI Exit Type	- Please Select an option -		
Make Changes?	<input type="button" value="Update"/>		

- Dans l'interface du serveur Fog et allez sur « Task Manger » puis cliquez sur « List All Hosts », sélectionner la machine enregistrée avec la bonne image, puis cliquez sur la petite icône orange « Capture » pour créer la tâche de capture :

All Hosts

Host Name	Assigned Image	Tasking
Windows_11_Depl 00:0C:29:90:68:61	img-W11	
Win_11 00:0C:29:91:CB:77	img-W11	

- Un message de confirmation s'affiche pour confirmer la création de la tâche de capture :

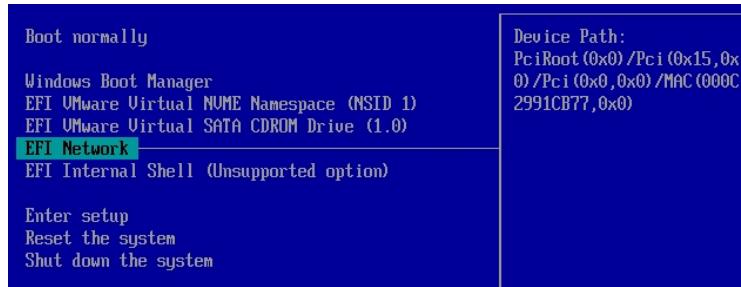


- Cliquez sur « Active Task » pour voir le statut de la tâche :

Active Tasks

Started By:	Hostname MAC	Image Name	Start Time	Working with node	Status
fog	Win_11	img-W11	2024-08-27 19:59:57	DefaultMember	

- Relancez la machine Windows en appuyant sur F12 ou échappe pour aller dans le menu Boot et choisir l'ordre d'amorçage « EFI Network » :



- Le serveur Fog va cloner automatiquement l'ISO de la vm :

Started By:	Hostname MAC	Image Name	Start Time	Working with node	Status
fog	Win_11	img-W11	2024-08-27 16:31:18	DefaultMember	In Progress
00:01:21/00:03:04	31%	8.880 GiB of 65.121			

Cancel selected tasks?

- L'extraction prend du temps et la vm vous indiquera si le clonage a réussi et redémarra :

```
Partclone
Reading Super Block
Calculating bitmap... Please wait...
done!
File system: NTFS
Device size: 818.9 MB = 199935 Blocks
Space in use: 725.7 MB = 177180 Blocks
Free Space: 93.2 MB = 22755 Blocks
Block size: 4096 Byte
Syncing... OK!
Partclone successfully cloned the device (/dev/nume0n1p4) to
the image (/tmp/pigz1)

Total Time: 00:00:05 Remaining: 00:00:00
Ave. Rate: 8.71GB/min

Data Block Process:
[██████████] 100.00%

Total Block Process:
[██████████] 100.00%
```

- Retournez sur votre serveur Fog dans la section « Image Management », puis « Liste All Image ». Si tout s'est bien passé, l'image de la machine Windows vous indiquera quel pèse 64 Go car c'est l'espace que j'ai allouer à cette vm :

Image Name	Storage Group	Image Size:	Captured
img-W11 - 2 Multiple Partition Image - Single Disk (Not Resizable) ZSTD Compressed	default	64.01 GiB	2024-08-27 16:43:09

D. Déploiement de l'ISO

1. Enregistrement de la nouvelle machine à déployer

- Refaire les mêmes manipulations effectuer précédemment pour son enregistrement en la nommant autrement dans « Host Management » :

All Hosts						
		Host	Imaged	Task	Assigned Image	
?	□	Windows_11_Depl 00:0c:29:90:e6:6f	2024-08-27 16:21:59	▲ ▲ □ □		
?	□	Win_11 00:0c:29:91:cb:77	No Data	▲ ▲ □ □	img-W11	

- Cliquez sur le nom de l'hôte puis ajouter l'image à assigner puis cliquez sur « Update » :

Host general

Host Name	Windows_11_Depl
Primary MAC	Load MAC Vendors 00:0c:29:90:e6:6f <input checked="" type="radio"/> I.M.C. <input type="checkbox"/> I.M.I.
Host description	Created by FOG Reg on August 27, 2024, 4:18 pm
Host Product Key	
Host Image	img-W11 - (2) <input checked="" type="radio"/>
Host Kernel	
Host Kernel Arguments	
Host Init	
Host Primary Disk	
Host Bios Exit Type	- Please Select an option -
Host EFI Exit Type	- Please Select an option -
Make Changes?	<input type="button" value="Update"/>

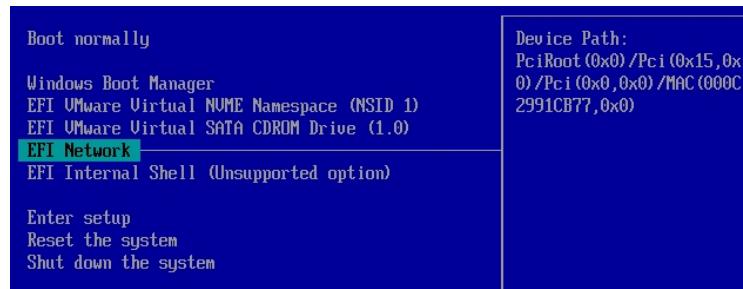
2. Affectation d'une tâche de déploiement à la machine

- Allez sur « Task Manger » puis cliquez sur « List All Hosts », sélectionner la machine enregistrée avec la bonne image cliquez sur la petite icône verte « Deploy » pour déployer l'ISO :

All Hosts		
Host Name	Assigned Image	Tasking
Windows_11_Depl 00:0c:29:90:e6:6f	img-W11	
Win_11 00:0c:29:91:cb:77	img-W11	

3. Déploiement de la nouvelle machine

- Lancez la machine vierge en appuyant sur F12 pour aller dans le menu Boot et choisir l'ordre d'amorçage « EFI Network » :



- Le déploiement va se lancer automatiquement :

A screenshot of a terminal window titled 'Partclone'. The window displays the progress of a disk cloning operation. The text output includes:

```
Partclone v0.3.27 http://partclone.org
Starting to restore image (-) to device (/dev/nvme0n1p3)
note: Storage Location 192.168.1.1:/images/, Image name img-W11
Calculating bitmap... Please wait...
done!
File system: NTFS
Device size: 67.8 GB = 16546815 Blocks
Space in use: 23.2 GB = 5665103 Blocks
Free Space: 44.6 GB = 10881712 Blocks
Block size: 4096 Byte

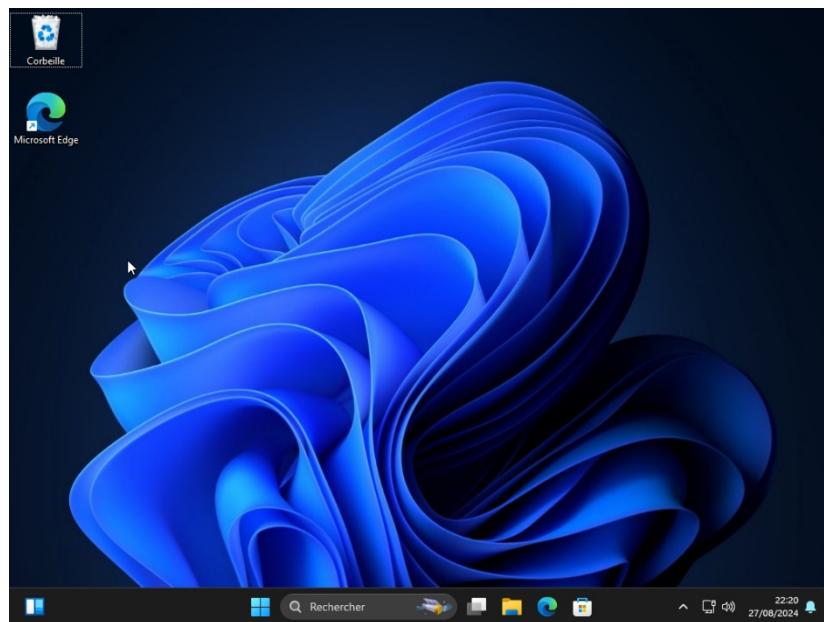
Elapsed: 00:00:48 Remaining: 00:01:48 Rate: 8.92GB/min
Current Block: 1803620 Total Block: 16546815

Data Block Process:
[██████████] 30.75%

Total Block Process:
[██████████] 10.90%
```

The progress bar for 'Data Block Process' is at 30.75%, and the total progress bar is at 10.90%.

- A la fin du déploiement la machine va se redémarrer et se mettre sur un système parfaitement fonctionnel et configurer en fonction de votre ISO :



V. Déploiement par le réseau avec un serveur WDS

Windows Deployment Service (WDS) est un service de Windows serveur qui permet de stocker déploiement d'ISO sur plusieurs machine sans à avoir besoin de supports physique comme CD, DVD ou clés USB mais par le réseau. Pour fonctionner, il a besoin d'un serveur DHCP conformer au principe de boot PXE qui peut être intégrer sur Windows Serveur. Le serveur WDS peut en mode groupe de travail (autonome) ou enregistré dans l'Active Directory. Il aura aussi besoins d'un serveur DNS et AD DS pour fonctionner.

WDS peut charger 2 types d'image :

- Une image de démarrage qui va être charger par le boot PXE quand la machine client va démarrer sur le réseau (boot.wim)
- Une image d'installation qui va permettre de déployer un système d'exploitation par le réseau (install.wim)

A. Téléchargement, installation et configuration de Windows Server 2022

1. Téléchargement de Windows Server 2022

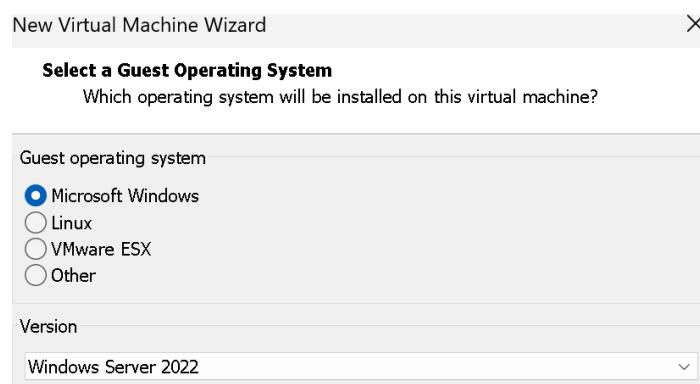
Windows server 2022 est un système d'exploitation optimiser pour la gestion des rôles de serveur tels l'hébergement de sites web, la gestion des utilisateurs via Active Directory, le partage de fichier NTFT, le serveur DHCP, le serveur WDS et bien d'autre services.

- Téléchargez l'ISO avec le lien de téléchargement <https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-server-2022> :

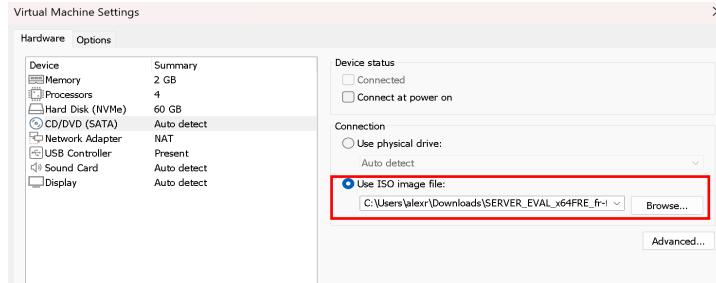
The screenshot shows the Microsoft Evaluation Center page for Windows Server 2022. At the top, there's a navigation bar with links like 'Centre d'évaluation', 'Windows', 'Windows Server', 'SQL Server', 'System Center', 'Sécurité Microsoft', 'Plus', and 'Tout Microsoft'. Below the navigation, the title 'Windows Server 2022' is displayed. Underneath it, there are tabs for 'Vue d'ensemble', 'Démarrez gratuitement', 'Description', 'Conditions préalables', 'Ressources', and 'Prise en charge de produits'. A section titled 'Vue d'ensemble' contains text about adding more languages and features by downloading the ISO file. A red box highlights the link 'Téléchargez ce fichier ISO.'

2. Installation de Windows Server 2022

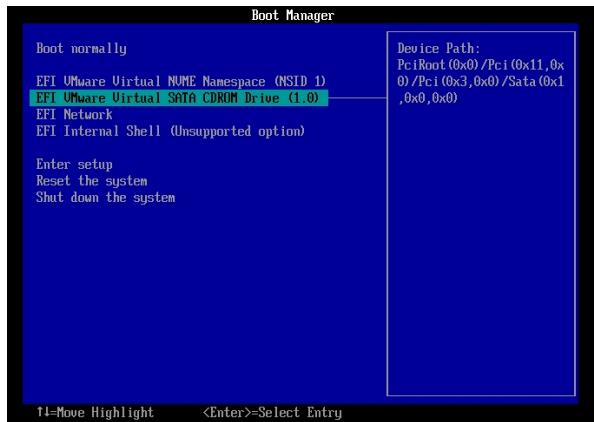
- Lors de la création de la VM, sélectionnez la version « Windows server 2022 » :



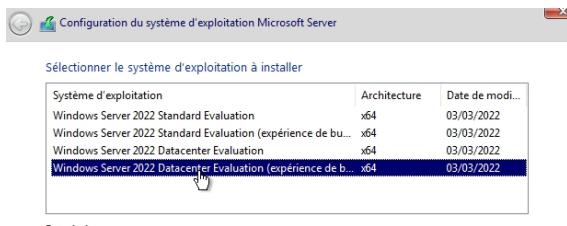
- Sélectionnez l'ISO télécharger précédemment dans « CD/DVD (SATA) » :



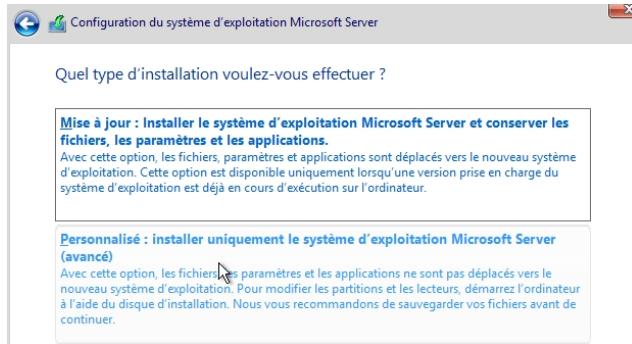
- Lancez la machine Windows serveur 2022 en appuyant sur F12 ou échappe pour accéder au menu Boot et choisir l'ordre d'amorçage « EFI VMware Virtual SATA CDROM Drive (1.0) » :



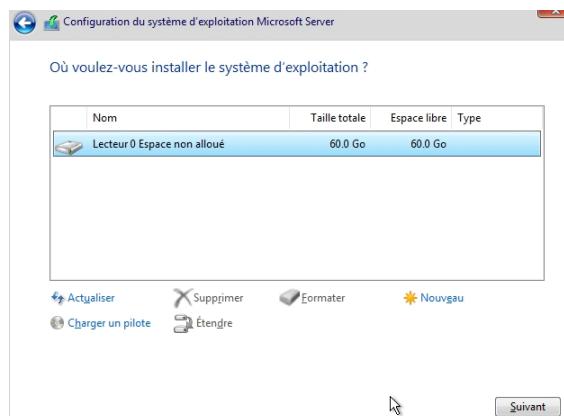
- L'installation de Windows serveur 2022 va vous demandez de choisir entre différentes versions du serveur en mode graphique ou non. Sélectionnez la dernière version pour avoir un environnement graphique Windows Complet :



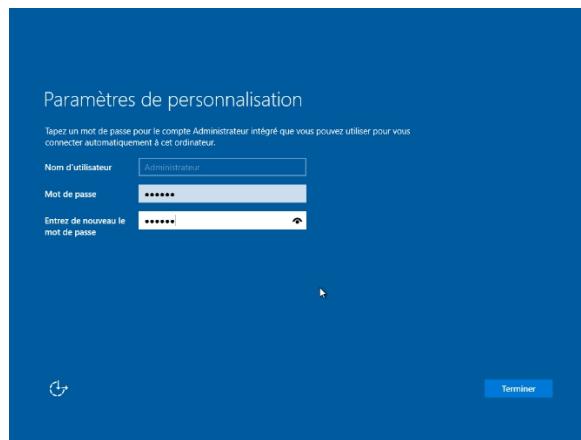
- Cliquez sur l'installation personnalisé :



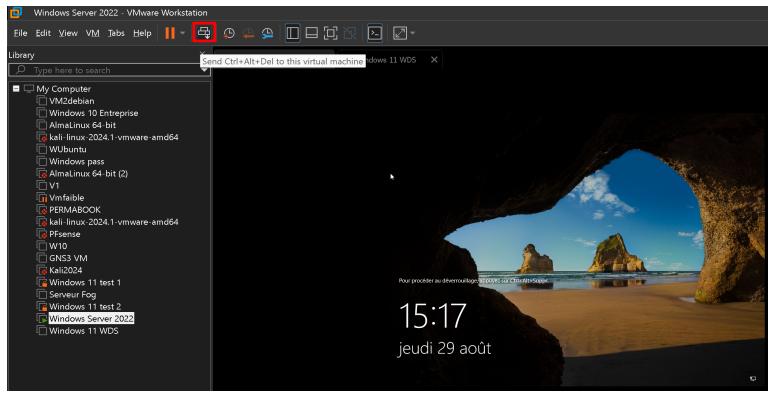
- Sélectionnez le disque sur de la vm puis cliquez sur « Suivant » :



- Après l'installation, Windows vous demande le mot de passe de l'administrateur qui est minimum 8 caractères avec des majuscules, minuscule et caractères spéciaux. Puis cliquez sur « Terminer » :

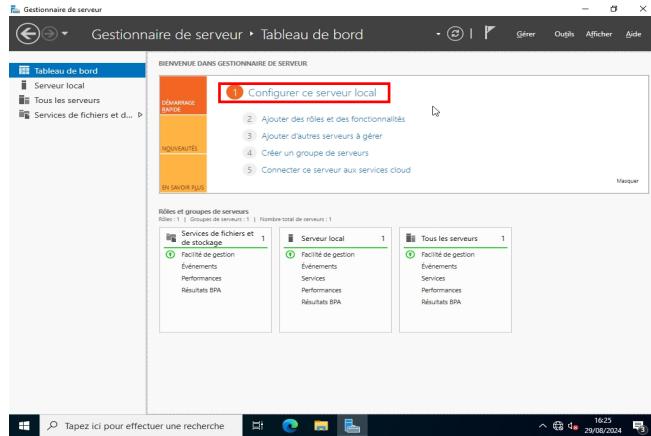


- L'écran de verrouillage vous demande de taper la combinaison de touche « Ctrl+Alt+Suppr », cliquez sur l'icône encadrer en rouge pour effectuer cette combinaison et accéder à la session administrateur :



3. Configuration de Windows Server 2022

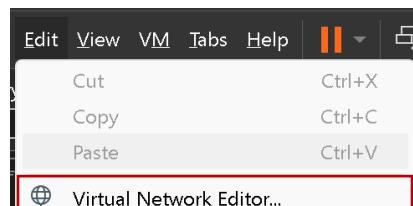
- En ouvrant la session administrateur, le tableau de bord du gestionnaire de serveur s'affiche automatiquement. Pour configurer le serveur, cliquez sur « Configurer ce serveur local » :



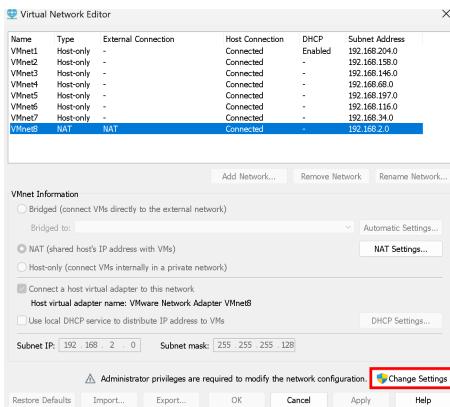
4. Configurer le réseau de la VM

Le serveur doit avoir un adresse IP en statique et internet pour que tous les services essentiels dans **le déploiement** fonctionnent. Le NAT permet d'avoir une connexion internet par le biais de l'hôte mais malheureusement un serveur DHCP est prédefini par Vmware donc nous allons le personnaliser pour avoir notre propre réseau.

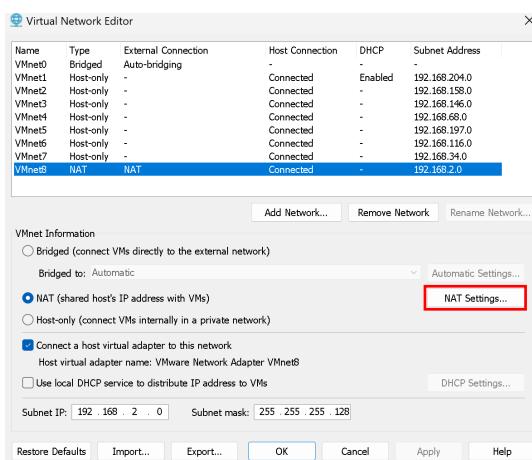
- Dans Vmware cliquez sur « Edit » puis « Virtual Network Editor » :



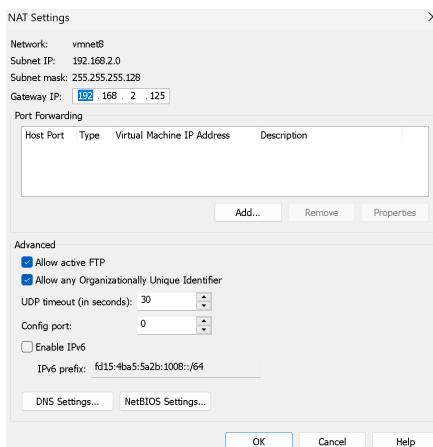
- La fenêtre de « Virtual Network Editor » présente tous les réseaux personnalisés, cliquez sur « Change Settings », une fenêtre de « Demande de contrôle de compte de l'utilisateur » clique sur « Oui » :



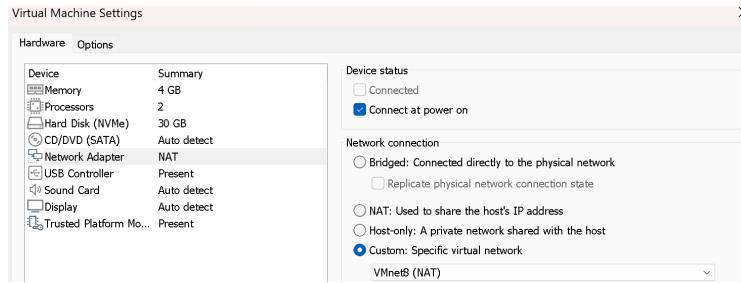
- Sélectionnez le réseau que vous voulez personnaliser, modifiez le sous-réseau et le masque. Puis cliquez sur « NAT Settings » :



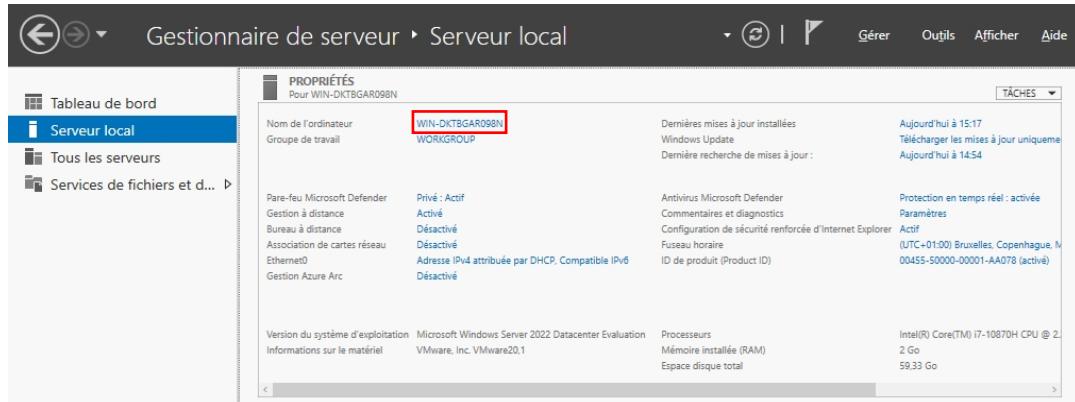
- Modifiez la passerelle puis cliquez sur « Apply » et sur « OK » :



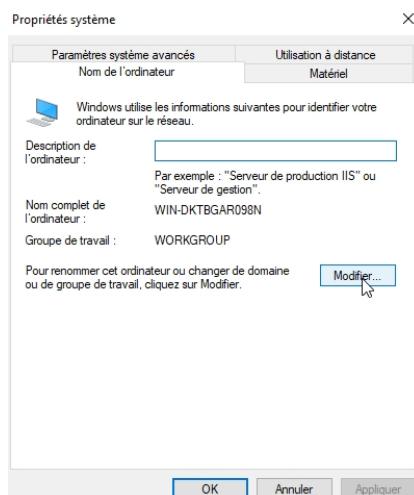
- Sur la VM cliquez sur « Virtual Machine Settings », puis sur « Network Adapter ». Cliquez sur « Custom », puis sélectionnez le réseau configuré et cliquez sur « OK » :



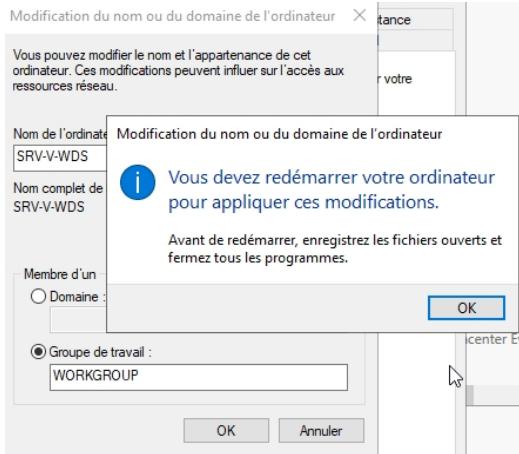
- Dans Propriété vous pouvez renommer l'ordinateur, cliquez sur « WIN-DKTBGAR098N » :



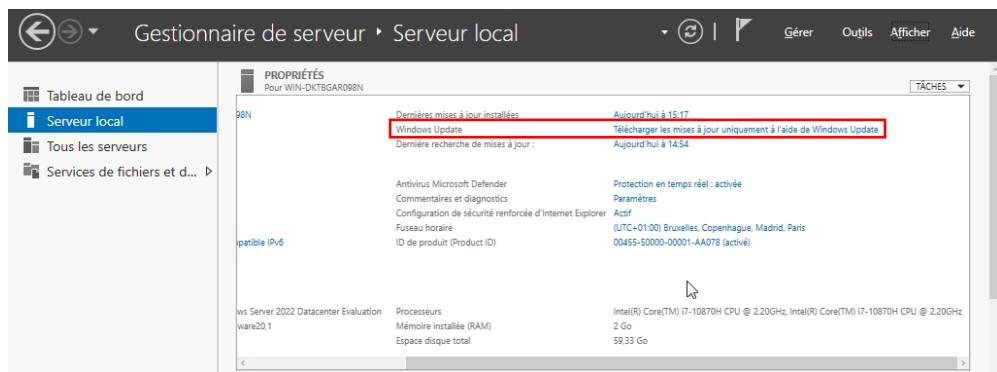
- Puis cliquez modifiez :



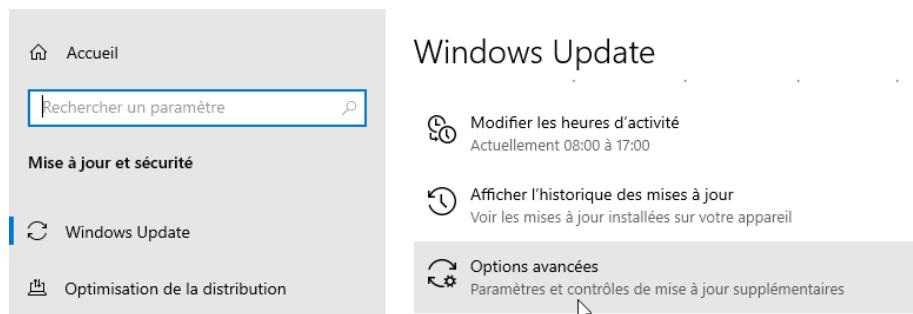
- Renommez l'ordinateur, puis cliquez sur « OK ». Une fenêtre vous indique qu'il faut redémarrer l'ordinateur pour appliquer ces modifications :



- Pour installer les mises à jour, cliquez sur « Télécharger les mises à jour uniquement à l'aide Windows Update ». Elles vont s'installer et certaines vont demander de redémarrer le système, cliquez sur « Installer maintenant » :



- Pour recevoir les mises à jour des services installer retourner sur Windows Update, cliquez sur « Options avancées » :



- Puis cliquez sur « Désactivé » en dessous de la première option :

⇒ Options avancées

*Votre organisation gère certains paramètres (Consulter les politiques)

Options de mise à jour

Recevoir les mises à jour d'autres produits Microsoft lors de la mise à jour de Windows



Téléchargez les mises à jour via des connexions limitées (des frais supplémentaires peuvent s'appliquer).



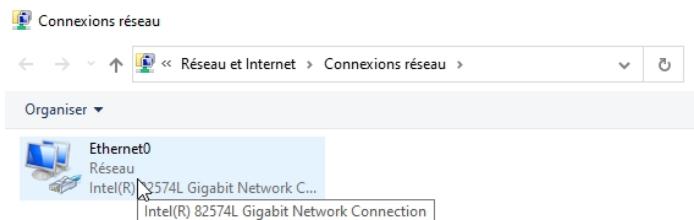
Redémarrez cet appareil dès que possible lorsqu'un redémarrage est nécessaire pour installer une mise à jour. Windows affiche un avertissement avant le redémarrage et l'appareil doit être allumé et branché.



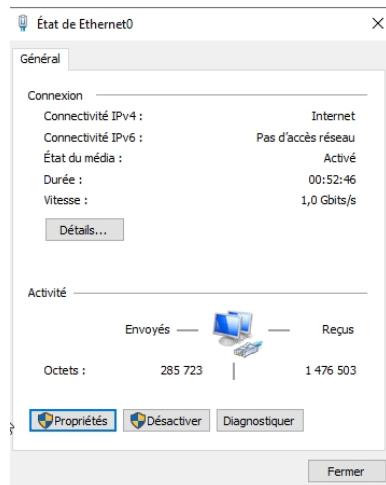
- Pour mettre l'adresse IP en statique, allez dans le menu « Serveur local » cliquez sur « Adresse IPv4 attribuée par DHCP » :

Pare-feu Microsoft Defender	Privé : Actif	Antivirus Microsoft Defender	Protection en temps réel : activée
Gestion à distance	Activé	Commentaires et diagnostics	Paramètres
Bureau à distance	Désactivé	Configuration de sécurité renforcée d'Internet Explorer	Actif
Association de cartes réseau	Désactivé	Fuseau horaire	(UTC+01:00) Bruxelles, Copenhague, M
Ethernet0	Adresse IPv4 attribuée par DHCP, Compatible IPv6	ID de produit (Product ID)	00455-50000-00001-AA078 (activé)
Gestion Azure Arc	Désactivé		

- Cliquez sur « Ethernet0 » :

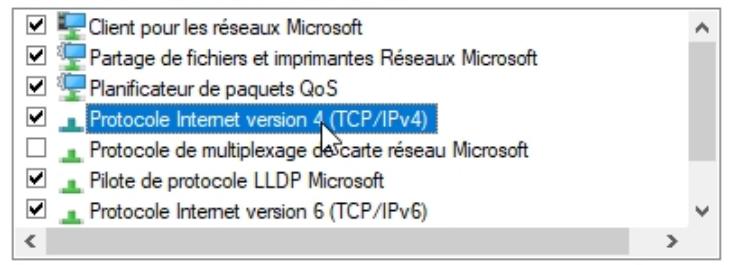


- Cliquez sur « Propriétés » :

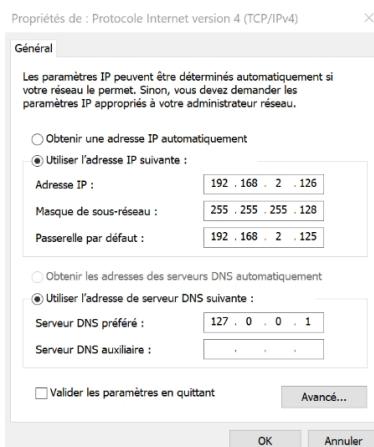


- Cliquez sur « Protocole internet version 4 (TCP/IPv4) » :

Cette connexion utilise les éléments suivants :



- Remplissez les paramètres demandés et cliquez sur « OK » :

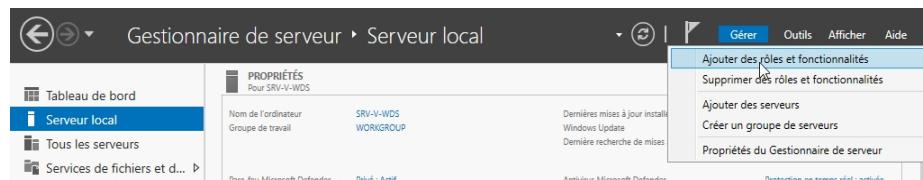


B. Installation et configurer le serveur AD DS

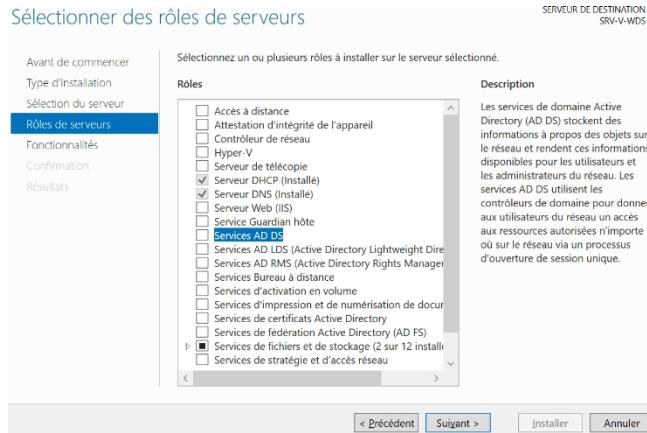
Serveur AD DS (Active Directory Domain Services) est un serveur qui permet aux administrateurs réseau de créer et gérer des domaines, des utilisateurs et définir des stratégies de groupe.

1. Installation du serveur AD DS

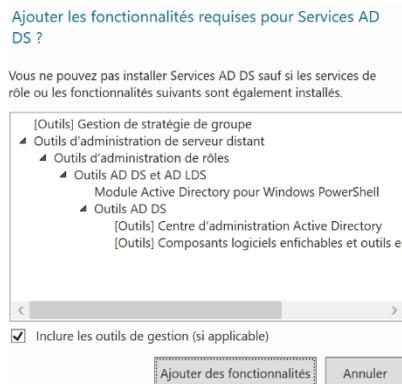
- Pour installer le rôle AD DS, cliquez-en haut à droit sur « Gérer » puis « ajoutez des rôles et fonctionnalités »



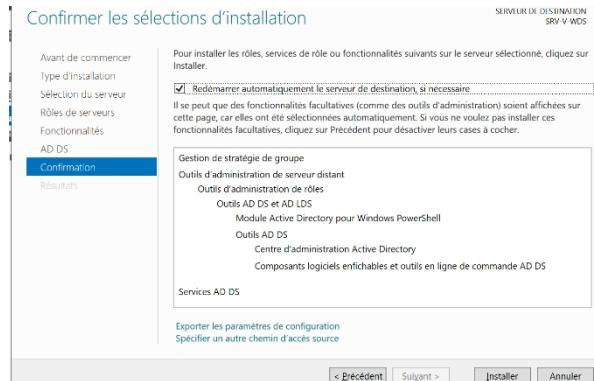
- Cliquez sur « Suivant » jusqu'à arriver sur la page « sélection des rôles de serveurs », Sélectionnez « Serveur AD DS » puis cliquez sur « Suivant » :



- Cliquez sur « Ajouter des fonctionnalités » :

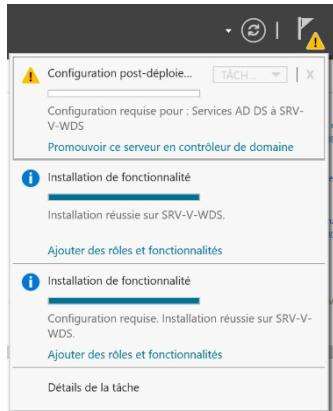


- Cliquez sur « Installer » :

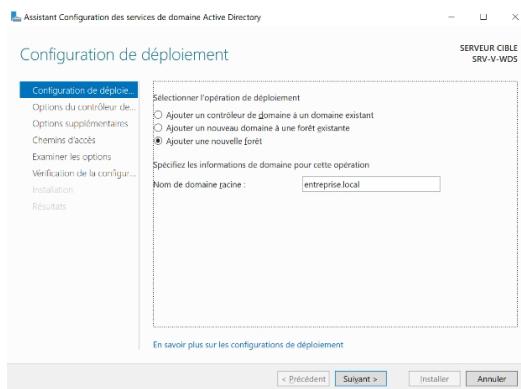


2. Configurer le serveur AD DS

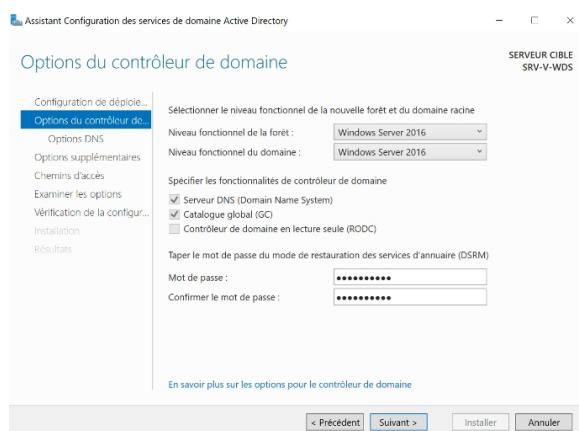
- Il va falloir promouvoir notre serveur en contrôleur de domaine (serveur qui répond aux requêtes au sein AD), cliquez sur le drapeau puis cliquez sur « Promouvoir ce serveur en contrôle de domaine » :



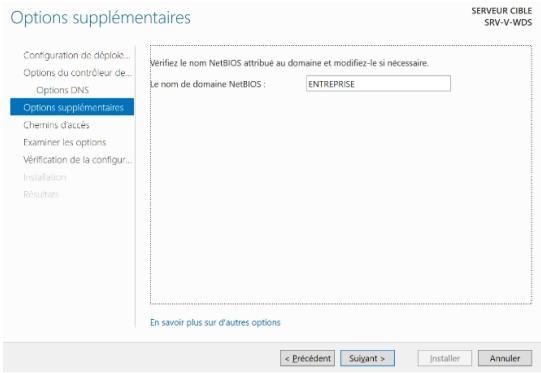
- Cliquez sur « Ajouter une nouvelle forêt » (ensemble de domaine) puis donnez un nom à votre premier nom de domaine avec une terminaison « en .local » pour qu'il ne soit pas confondu avec un de domaine public et cliquez sur « Suivant » :



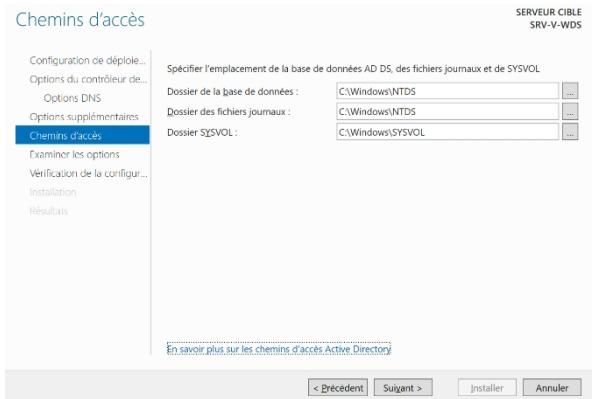
- Laissez le niveau fonctionnel le plus élevé, le serveur DNS et catalogue global (AD stocke les objets au sein de l'annuaire), puis spécifiez un mot de passe de secours (il permet de récupérer les objectés de l'annuaire si AD est en panne) et cliquez sur « Suivant » :



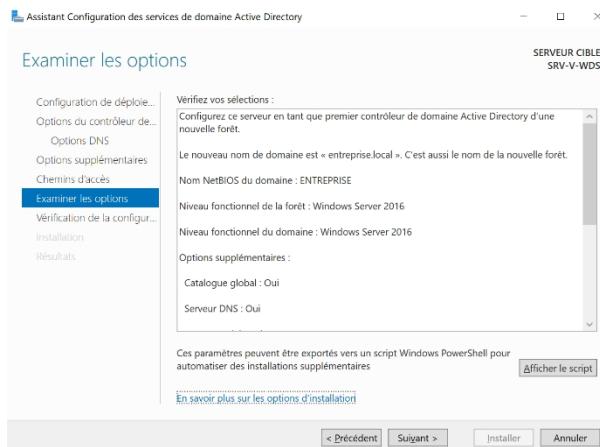
- On vous attribue un nom de domaine NetBIOS est une alternative DNS et vous pouvez le modifier puis cliquez sur « Suivant » :



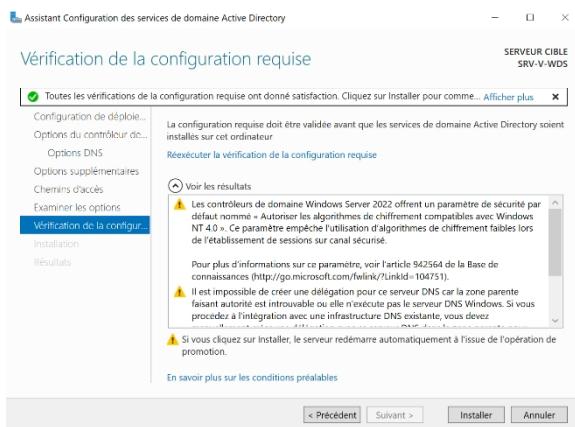
- Affichage de l'emplacement de stockage des données d'AD, cliquez sur « Suivant » :



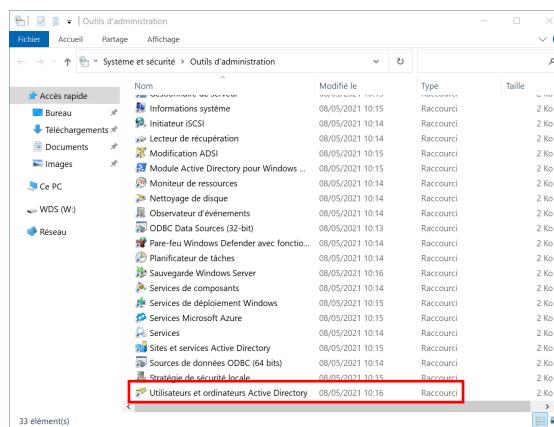
- Affichage du récapitulatif, si tout est bon cliquez sur « Suivant » :



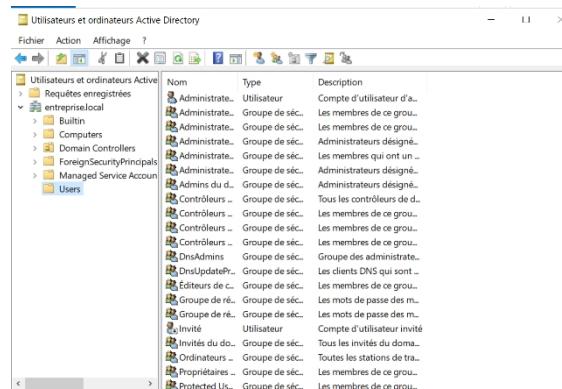
- Affichage de 2 avertissements, l'un pour la délégation et l'autre pour la compatibilité avec les anciens serveurs, cliquez sur « Installer » et la machine va redémarrer :



- Vérifiez que votre serveur AD DS est fonctionnel en allant dans « Outil d'administration », puis cliquez sur « Utilisateurs et ordinateurs Active Directory » :



- L'AD est activé et vous pouvez visualiser vos utilisateurs et vos domaines :

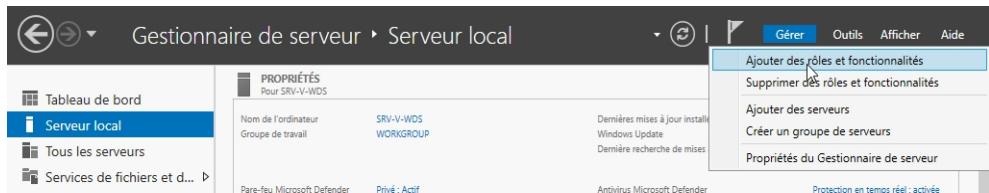


C. Installation et configurer le serveur DNS

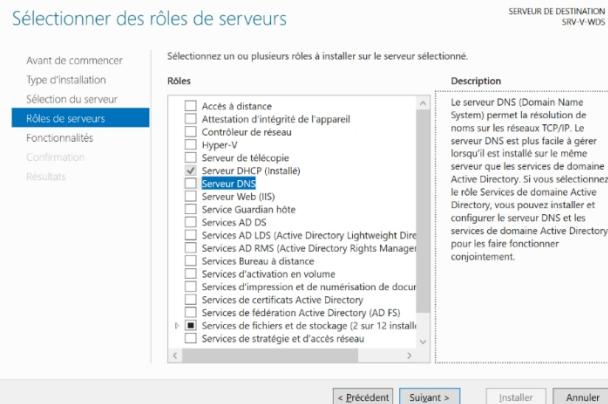
Le serveur DNS (Domain Name system) permet de faire le lien entre le nom d'hôte et l'adresse IP donc de traduire le nom de domaine en adresse IP.

1. Installation serveur DNS

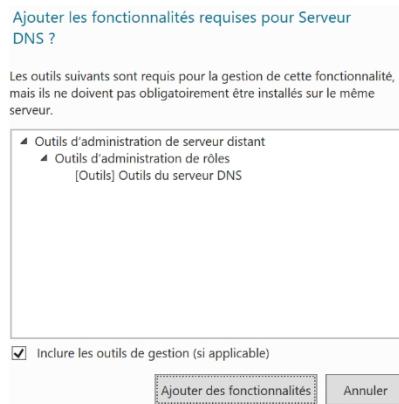
- Pour installer le rôle DNS, cliquez-en haut à droit sur « Gérer » puis « ajoutez des rôles et fonctionnalités »



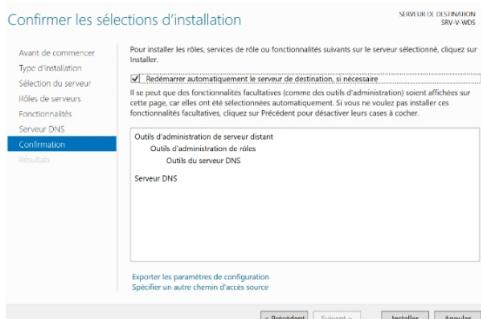
- Cliquez sur « Suivant » jusqu'à arriver sur la page « sélection des rôles de serveurs », Sélectionnez « Serveur DNS » puis cliquez sur « Suivant » :



- Cliquez sur « Ajouter des fonctionnalités » :

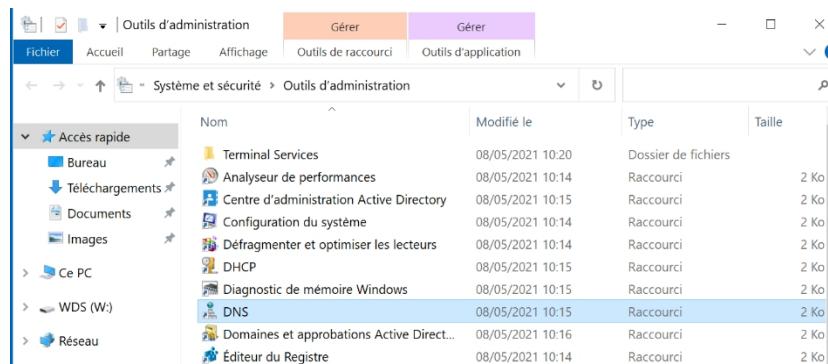


- Cliquez sur « Installer » :

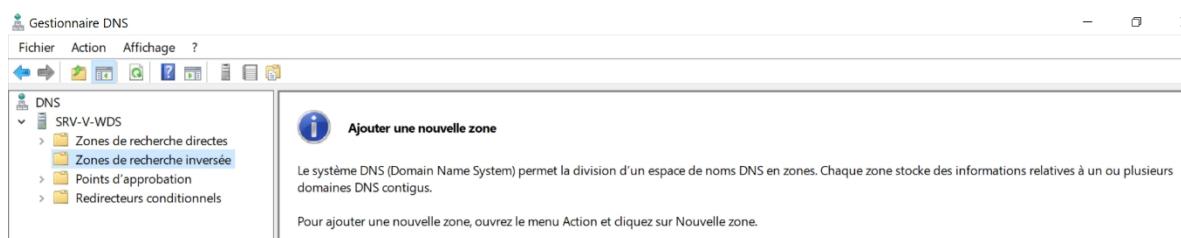


2. Configurer le serveur DNS

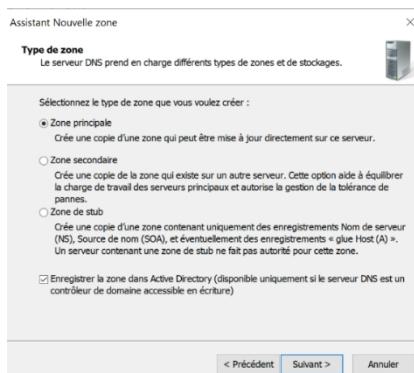
- Allez dans « Outil d'administration », puis cliquez sur « DNS » :



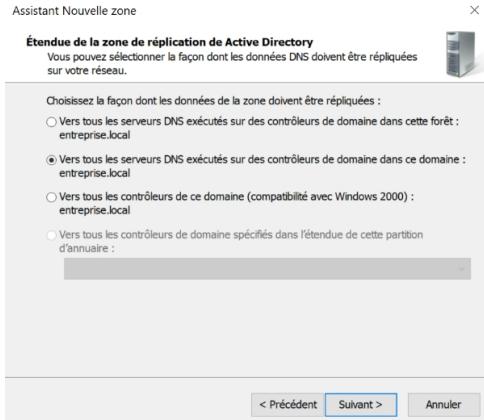
- Créez une zone de recherche inversé consiste de faire la liaison entre une IP et un nom, clic droit sur « Zone de recherche inversé » puis sur « Nouvelle zone » :



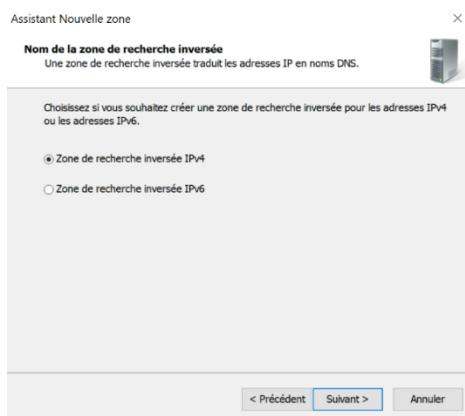
- Laissez-la en « Zone principale » et register la zone dans AD, puis cliquez sur « Suivant » :



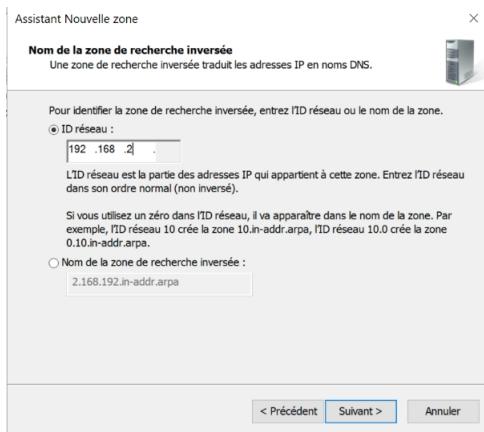
- Laissez l'option cocher de base, puis cliquez sur « Suivant » :



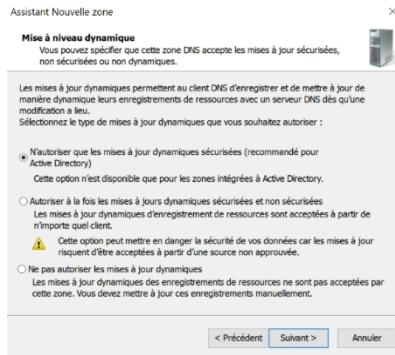
- Laissez l'option cocher de base car on travaille en IPv4, puis cliquez sur « Suivant » :



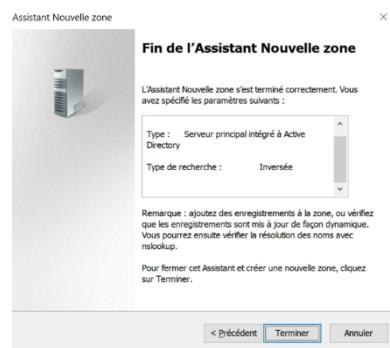
- Entrez l'ID du réseau, puis cliquez sur « Suivant » :



- Autorisez que les mises à jour sécurisé, puis cliquez sur « Suivant » :



- Affichage du récapitulatif, si tout est bon cliquez sur « Terminer » :



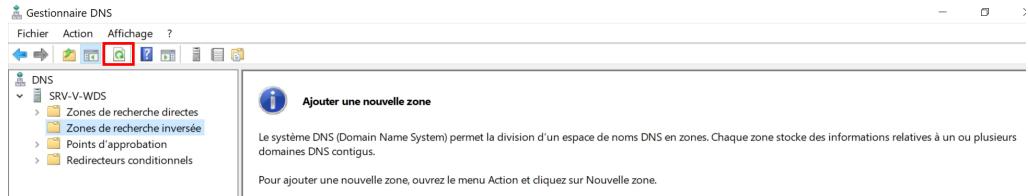
- Les enregistrements préalables à la création de la zone ne se mettent pas à jour automatiquement dans la « Zone de recherche inversé ». Cliquez sur votre serveur puis votre nom de domaine puis double clics sur le dernier fichier :

Nom	Type	Données	Horodateur
_msdc\$	Source de nom (SOA)	[19], srv-v-wds.entreprise.lo...	statique
_sites	Serveur de noms (NS)	srv-v-wds.entreprise.local.	statique
_tcp	Hôte (A)	192.168.2.126	30/08/2024 18:00:00
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[19], srv-v-wds.entreprise.lo...	statique
(identique au dossier parent)	Serveur de noms (NS)	srv-v-wds.entreprise.local.	statique
(identique au dossier parent)	Hôte (A)	192.168.2.126	30/08/2024 18:00:00
srv-v-wds	Hôte (A)	192.168.2.126	statique

- Cochez la case enregistrement puis cliquez sur « Appliquer » et sur « OK » :



- Actualisez avec l'icône entourer en rouge ci-dessous :



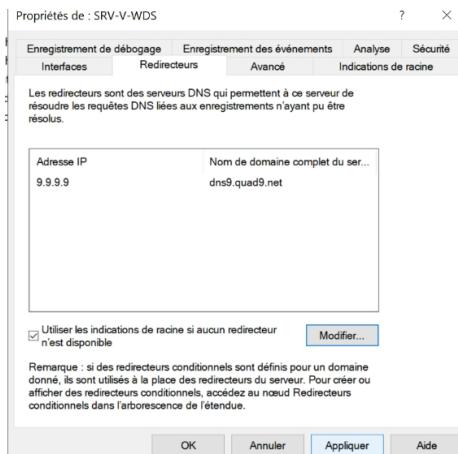
- Retournez dans la « Zone de recherche inversé » puis sur l'ID pour voir apparaître l'enregistrement inverse :

Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[6, srv-v-wds.entreprise.local]	statique
(identique au dossier parent)	Serveur de noms (NS)	srv-v-wds.entreprise.local.	statique
192.168.2.126	Pointeur (PTR)	srv-v-wds.entreprise.local.	statique

- Désactivez l'écoute sur IPv6, clic droit sur votre serveur puis sur « Propriété ». Cochez « Uniquement les adresses IP suivantes », décochez IPv6 puis cliquez sur « Appliquer » et sur « OK » :



- Cliquez sur « Redirecteurs » dans le cas où le serveur DNS ne sait pas faire la résolution de nom demander c'est à se redirecteurs qu'il va demander. Cliquez sur « Modifier », tapez la même adresse ci-dessous puis « Appliquer » et « OK » :



- Pour savoir s'il marche, allez dans invite de commande et asseyez de ping le nom de domaine :

```
C:\Users\Administrateur>ping entreprise.local

Envoi d'une requête 'ping' sur entreprise.local [192.168.2.126] avec 32 octets de données :
Réponse de 192.168.2.126 : octets=32 temps<1ms TTL=128
Réponse de 192.168.2.126 : octets=32 temps<1ms TTL=128
Réponse de 192.168.2.126 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.2.126 : octets=32 temps<1ms TTL=128

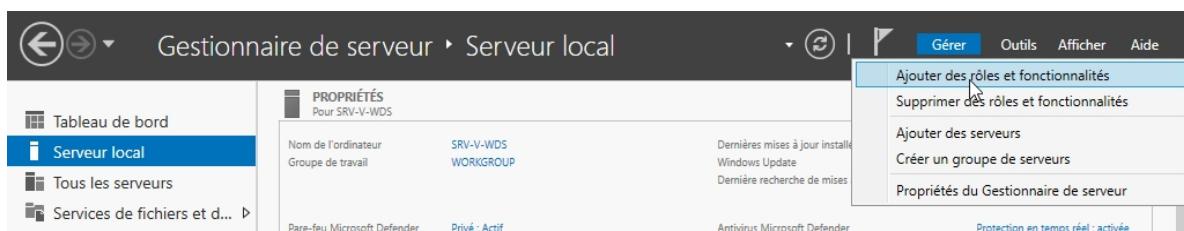
Statistiques Ping pour 192.168.2.126:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

D. Installation et configurer le serveur DHCP

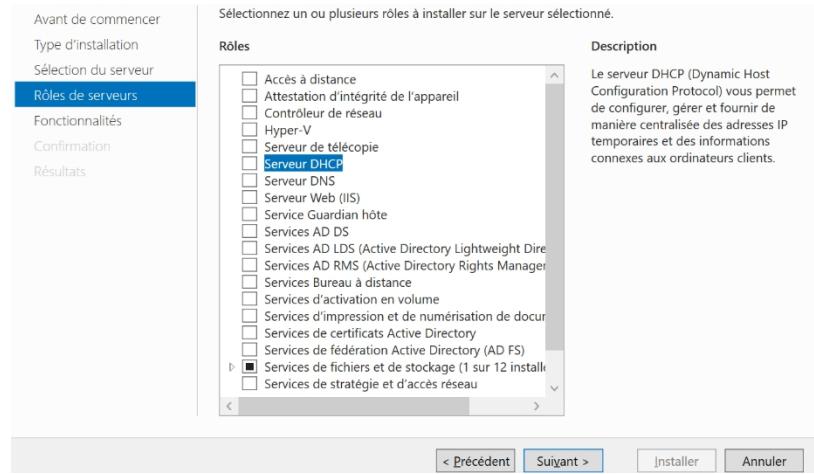
Le serveur DHCP (Dynamic Host Configuration Protocol) est un serveur qui utilise le protocole **DHCP de couche applicative du modèle OSI**, permettant à un administrateur **système à affecter des paramètres d'adressage à plusieurs hôtes dans le réseau de façon simultané et automatique**.

1. Installation du serveur DHCP

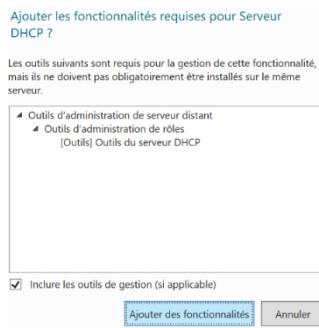
- Pour installer le rôle DHCP, cliquez-en haut à droit sur « Gérer » puis « ajoutez des rôles et fonctionnalités »



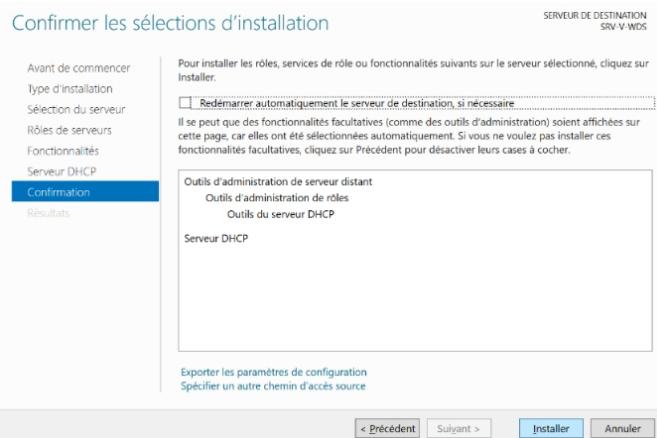
- Cliquez sur « Suivant » jusqu'à arriver sur la page « sélection des rôles de serveurs », Sélectionnez « Serveur DHCP » puis cliquez sur « Suivant » :



- Cliquez sur « Ajouter des fonctionnalités » :

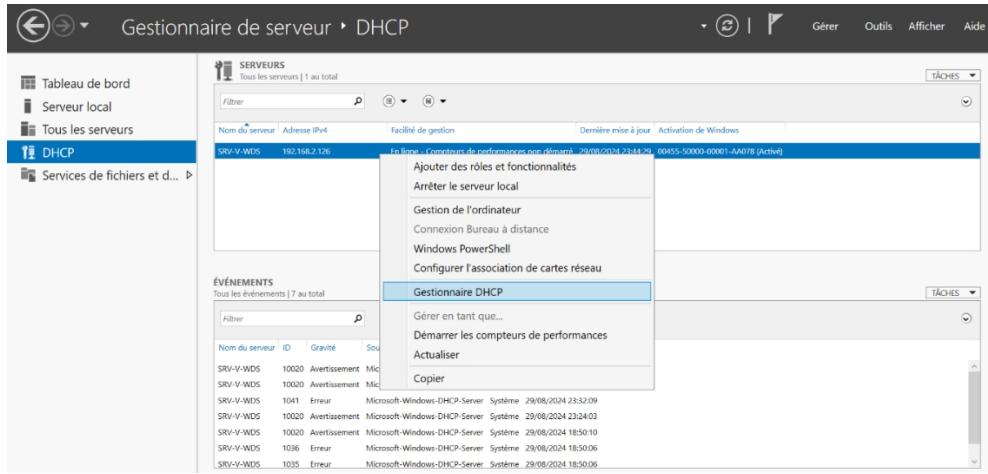


- Cliquez sur « Installer » :

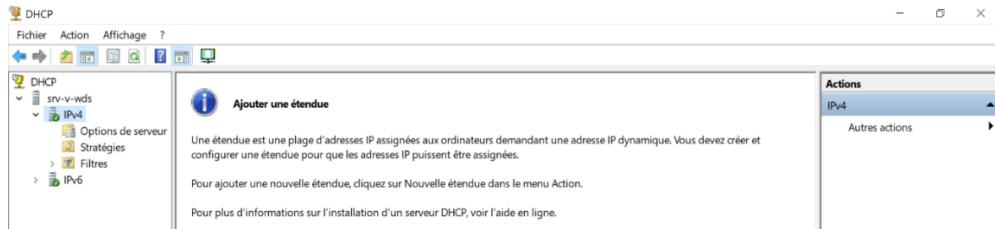


2. Configurer le serveur DHCP

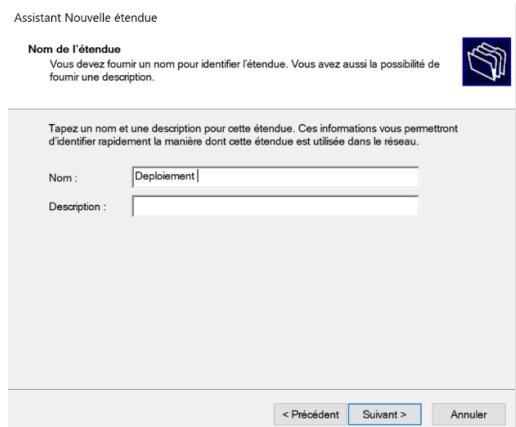
- Dans DHCP, cliquez droit sur « SRV-V-WDS » puis sur « Gestionnaire DHCP » :



- Cliquez droit sur « IPv4 » puis sur « Nouvelle étendue » :



- Cliquez sur « Suivant » et vous pouvez donner un nom pour cette étendue puis cliquez sur « Suivant » :



- Configurez les plages d'adressage avec l'adresse IP de début/fin, préfixe et masque de sous-réseau, puis cliquez sur « Suivant » :

Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.



Paramètres de configuration pour serveur DHCP
Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :	192 . 168 . 2 . 1
Adresse IP de fin :	192 . 168 . 2 . 80

Paramètres de configuration qui se propagent au client DHCP.

Longueur :	25
Masque de sous-réseau :	255 . 255 . 255 . 128

< Précédent Suivant > Annuler

- Vous pouvez paramétriser les adresses à exclure, puis cliquez sur « Suivant » :

Ajout d'exclusions et de retard
Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCP OFFER.



Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début :	Adresse IP de fin :	Ajouter
-----------------------	---------------------	---------

Plage d'adresses exclue :

Supprimer

Retard du sous-réseau en millisecondes :

0

< Précédent Suivant > Annuler

- Modifiez la durée du bail, puis cliquez sur « Suivant » :

Assistant Nouvelle étendue

Durée du bail
La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.



La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

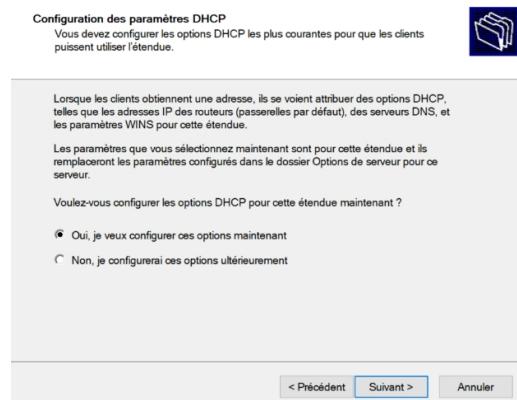
Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

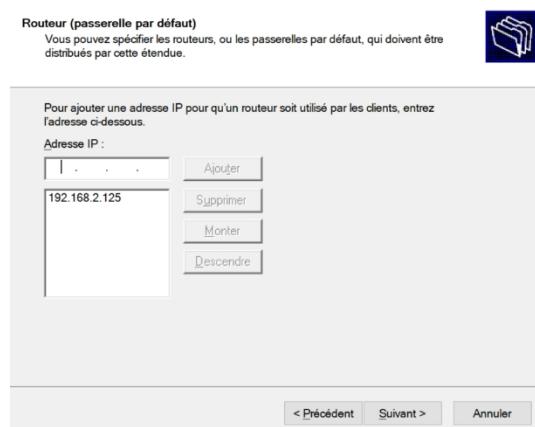
Jours :	Heures :	Minutes :
0	3	0

< Précédent Suivant > Annuler

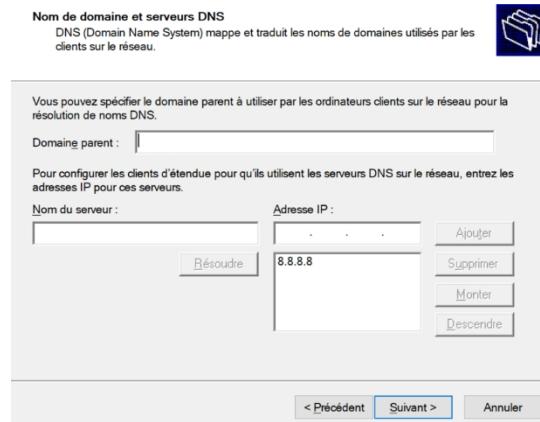
- Cliquez sur « Suivant » :



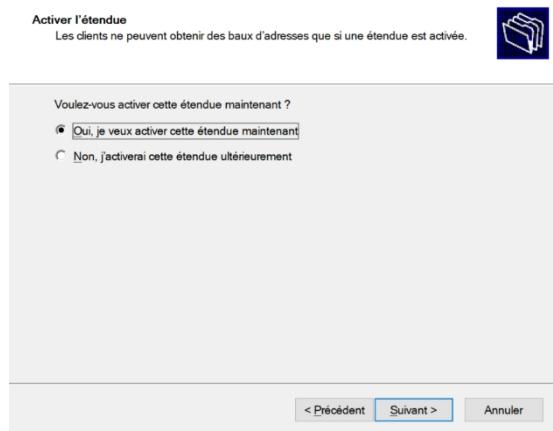
- Tapez l'adresse IP de la passerelle, puis cliquez sur « Suivant » :



- Tapez l'adresse IP du DNS, puis cliquez sur « Suivant » :



- Cliquez sur « Suivant » :



3. DHCP : déclarer les classes de fournisseurs

- Dans « PowerShell ISE » tapez les commandes :

Nom d'hôte du serveur DHCP

```
$DhcpServerName = "SRV-V-WDS"
```

Adresse IP du serveur WDS (PXE)

```
$PxeServerIp = "192.168.2.125"
```

Adresse réseau de l'étendue DHCP ciblée

```
$Scope = "192.168.2.0"
```

Administrateur : Windows PowerShell ISE

Fichier Modifier Afficher Outils Déboguer Composants additionnels Aide

File New Open Save Cut Copy Paste Find Replace Run Stop Help

```
PS C:\Users\Administrateur> # Nom d'hôte du serveur DHCP
$DhcpServerName = "SRV-V-WDS"
# Adresse IP du serveur WDS (PXE)
$PxeServerIp = "192.168.2.125"
# Adresse réseau de l'étendue DHCP ciblée
$Scope = "192.168.2.0"
```

- Définissez les trois classes de fournisseurs DHCP correspondantes à des architectures différentes avec les trois commandes suivantes :

```

Add-DhcpServerv4Class -ComputerName $DhcpServerName -Name "PXEClient - UEFI x64" -Type Vendor -Data "PXEClient:Arch:00007" -Description "PXEClient:Arch:00007"
Add-DhcpServerv4Class -ComputerName $DhcpServerName -Name "PXEClient - UEFI x86" -Type Vendor -Data "PXEClient:Arch:00006" -Description "PXEClient:Arch:00006"
Add-DhcpServerv4Class -ComputerName $DhcpServerName -Name "PXEClient - BIOS x86 et x64" -Type Vendor -Data "PXEClient:Arch:00000" -Description "PXEClient:Arch:00000"

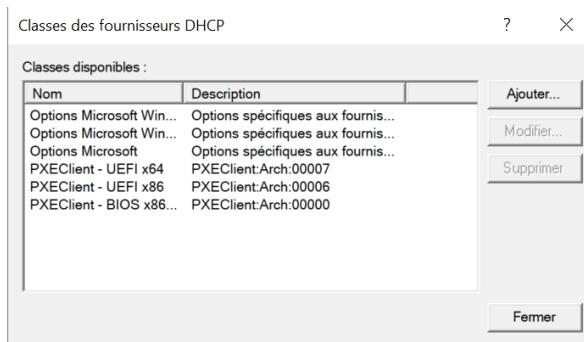
```

```

PS C:\Users\Administrateur> Add-DhcpServerv4Class -ComputerName $DhcpServerName -Name "PXEClient - UEFI x64" -Type Vendor -Data "PXEClient:Arch:00007" -Description "PXEClient:Arch:00007"
Add-DhcpServerv4Class -ComputerName $DhcpServerName -Name "PXEClient - UEFI x86" -Type Vendor -Data "PXEClient:Arch:00006" -Description "PXEClient:Arch:00006"
Add-DhcpServerv4Class -ComputerName $DhcpServerName -Name "PXEClient - BIOS x86 et x64" -Type Vendor -Data "PXEClient:Arch:00000" -Description "PXEClient:Arch:00000"

```

- Les modifications effectuées par ces commandes sont visibles dans, clic gauche sur IPv4 > Définir les classes des fournisseurs :



4. Créer les stratégies DHCP pour le BIOS et l'UEFI

- Créez les stratégies DHCP qui s'appliqueront sur l'étendue ciblée pour le mode BIOS x86/x64, UEFI x86 et UEFI x64 :

\$PolicyNameBIOS = "PXEClient - BIOS x86 et x64"

```

Add-DhcpServerv4Policy -Computername $DhcpServerName -ScopId $Scope -Name $PolicyNameBIOS -Description "Options DHCP pour boot BIOS x86 et x64" -Condition Or -VendorClass EQ, "PXEClient - BIOS x86 et x64**"

```

```

Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 066 -Value $PxeServerIp -PolicyName $PolicyNameBIOS

```

```

Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 067 -Value boot\x64\wdsnbp.com -PolicyName $PolicyNameBIOS

```

\$PolicyNameUEFIx86 = "PXEClient - UEFI x86"

```

Add-DhcpServerv4Policy -Computername $DhcpServerName -ScopId $Scope -Name $PolicyNameUEFIx86 -Description "Options DHCP pour boot UEFI x86" -Condition Or -VendorClass EQ, "PXEClient - UEFI x86**"

```

```
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 060 -Value PXEClient -PolicyName $PolicyNameUEFIx86
```

```
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 066 -Value $PxeServerIp -PolicyName $PolicyNameUEFIx86
```

```
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 067 -Value boot\x86\wdsmgfw.efi -PolicyName $PolicyNameUEFIx86
```

\$PolicyNameUEFIx64 = "PXEClient - UEFI x64"

```
Add-DhcpServerv4Policy -Computername $DhcpServerName -ScopId $Scope -Name $PolicyNameUEFIx64 -Description "Options DHCP pour boot UEFI x64" -Condition Or -VendorClass EQ, "PXEClient - UEFI x64"
```

```
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 060 -Value PXEClient -PolicyName $PolicyNameUEFIx64
```

```
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 066 -Value $PxeServerIp -PolicyName $PolicyNameUEFIx64
```

```
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 067 -Value boot\x64\wdsmgfw.efi -PolicyName $PolicyNameUEFIx64
```

```
PS C:\Users\Administrateur> # Nom d'hôte du serveur DHCP
$dhcpServerName = "SRV-V-WDS"
# Adresse IP du serveur WDS (PXE)
$PxeServerIp = "10.10.3.30"
# Adresse réseau de l'étendue DHCP ciblee
$Scope = "10.10.3.0"

PS C:\Users\Administrateur> $PolicyNameBIOS = "PXEClient - BIOS x86 et x64"
Add-DhcpServerv4Policy -Computername $DhcpServerName -ScopId $Scope -Name $PolicyNameBIOS -Description "Options DHCP pour boot BIOS x86 et x64" -Condition Or -VendorClass EQ, "PXEClient - BIOS x86 et x64"
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 066 -Value $PxeServerIp -PolicyName $PolicyNameBIOS
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 067 -Value boot\x64\wdsnbp.com -PolicyName $PolicyNameBIOS

PS C:\Users\Administrateur> $PolicyNameUEFIx86 = "PXEClient - UEFI x86"
Add-DhcpServerv4Policy -Computername $DhcpServerName -ScopId $Scope -Name $PolicyNameUEFIx86 -Description "Options DHCP pour boot UEFI x86" -Condition Or -VendorClass EQ, "PXEClient - UEFI x86"
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 060 -Value PXEClient -PolicyName $PolicyNameUEFIx86
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 066 -Value $PxeServerIp -PolicyName $PolicyNameUEFIx86
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 067 -Value boot\x86\wdsmgfw.efi -PolicyName $PolicyNameUEFIx86

PS C:\Users\Administrateur> $PolicyNameUEFIx64 = "PXEClient - UEFI x64"
Add-DhcpServerv4Policy -Computername $DhcpServerName -ScopId $Scope -Name $PolicyNameUEFIx64 -Description "Options DHCP pour boot UEFI x64" -Condition Or -VendorClass EQ, "PXEClient - UEFI x64"
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 060 -Value PXEClient -PolicyName $PolicyNameUEFIx64
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 066 -Value $PxeServerIp -PolicyName $PolicyNameUEFIx64
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopId $Scope -OptionId 067 -Value boot\x64\wdsmgfw.efi -PolicyName $PolicyNameUEFIx64
```

- Allez dans IPv4 > 2tendue [192.168.2.0] Deploiement > Stratégie :

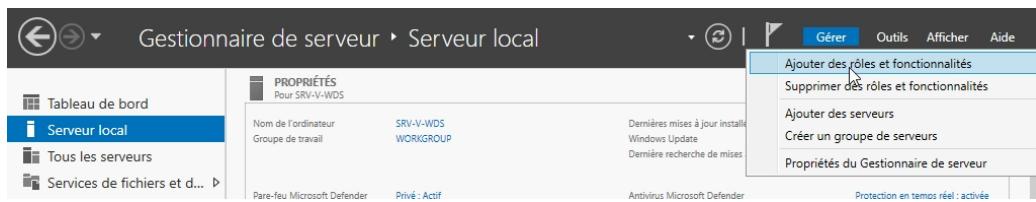
Nom de la stratégie	Description	Ordre de t...	Niveau	Plage d'adresses	État
PXEClient - BIOS x...	Options DHCP pour ...	1	Étendue		Activé
PXEClient - UEFI x...	Options DHCP pour ...	2	Étendue		Activé
PXEClient - UEFI x...	Options DHCP pour ...	3	Étendue		Activé

Nom d'option	Fournisseur	Valeur	Nom de la stratégie
003 Routeur	Standard	10.10.3.254	Aucun
006 Serveurs DNS	Standard	10.10.3.30	Aucun
015 Nom de domaine DNS	Standard	entreprise.local	Aucun
060 PXEClient	Standard	PXEClient	PXEClient - UEFI x86
060 PXEClient	Standard	PXEClient	PXEClient - UEFI x64
066 Nom d'hôte du serveur..	Standard	10.10.3.30	PXEClient - BIOS x86 et x64
066 Nom d'hôte du serveur..	Standard	10.10.3.30	PXEClient - UEFI x86
066 Nom d'hôte du serveur..	Standard	10.10.3.30	PXEClient - UEFI x64
067 Nom du fichier de dém..	Standard	boot\x64\wdsnbp.com	PXEClient - BIOS x86 et x64
067 Nom du fichier de dém..	Standard	boot\x86\wdsmgfw.efi	PXEClient - UEFI x86
067 Nom du fichier de dém..	Standard	boot\x64\wdsmgfw.efi	PXEClient - UEFI x64

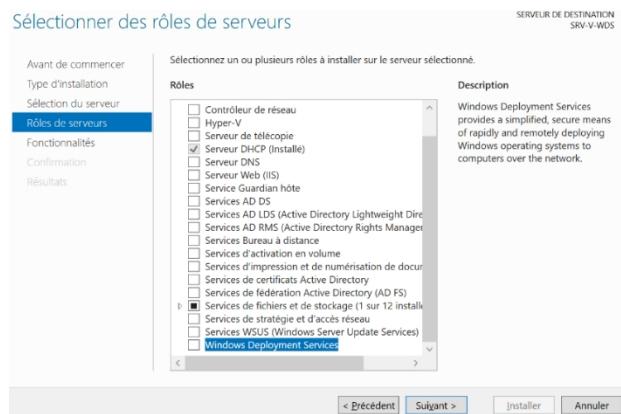
E. Installation et configuration du serveur WDS

1. Installation du serveur WDS

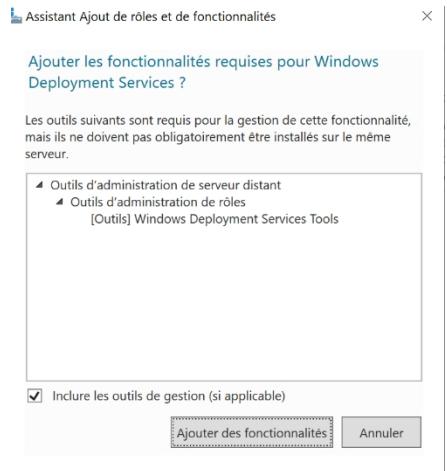
- Pour installer le rôle WDS, cliquez-en haut à droit sur « Gérer » puis « ajoutez des rôles et fonctionnalités » :



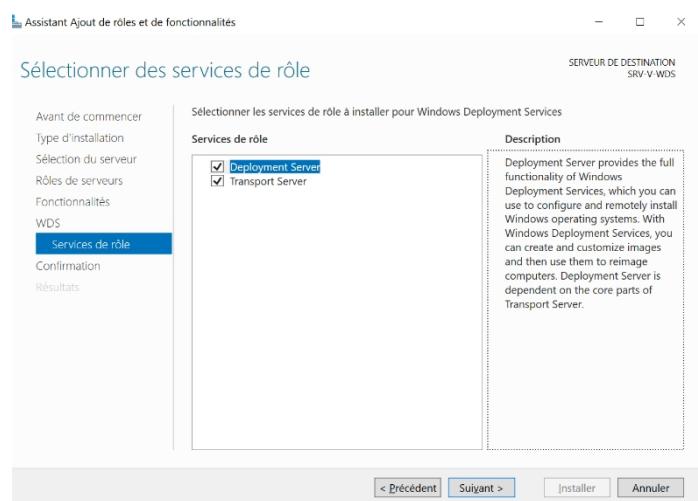
- Cliquez sur « Suivant » jusqu'à arriver sur la page « sélection des rôles de serveurs », Sélectionnez « Windows Deployment Services » puis cliquez sur « Suivant » :



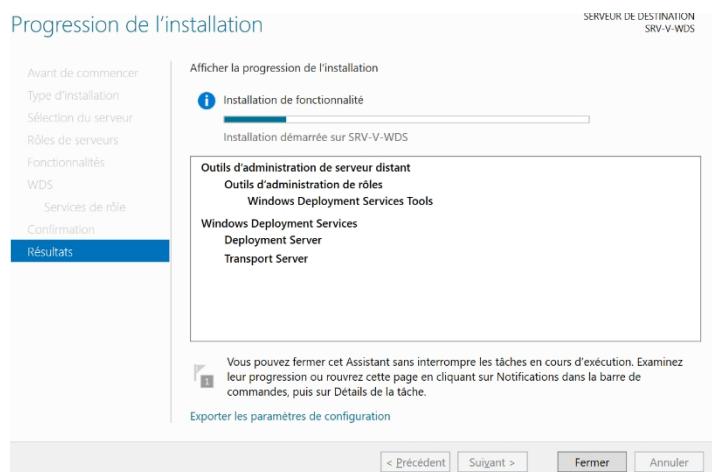
- Cliquez sur « Ajouter des fonctionnalités » :



- Cliquez sur « Suivant » :

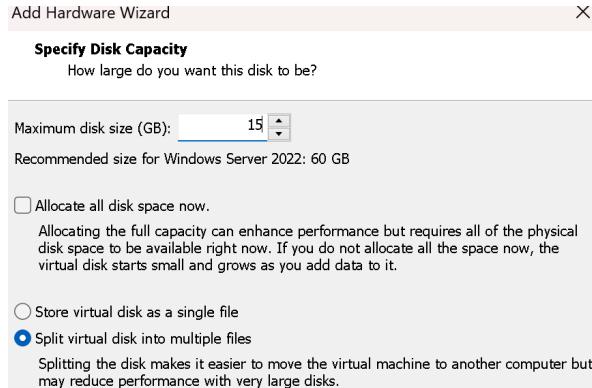


- Cliquez sur « Installer » :

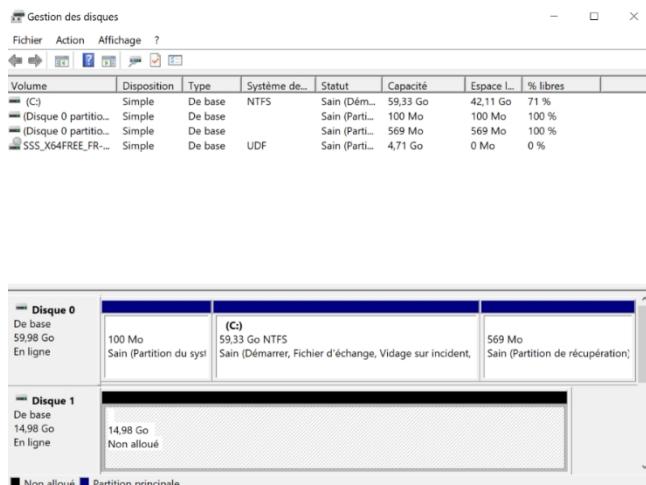


2. Configuration du Serveur WDS

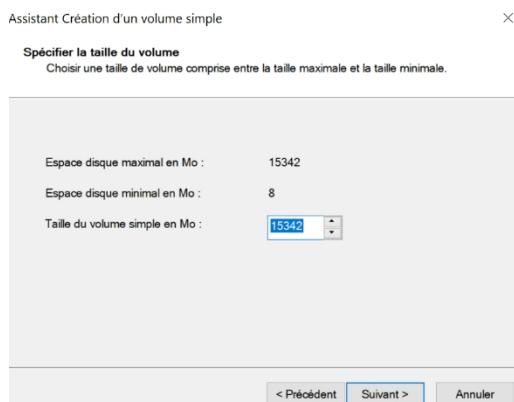
- Eteignez la VM et ajoutez un espace disque pour stocker les images du service WDS en cliquant sur « Ctrl+D », cliquez sur « Add » puis « Hard Disk » et sélectionner l'espace du disque :



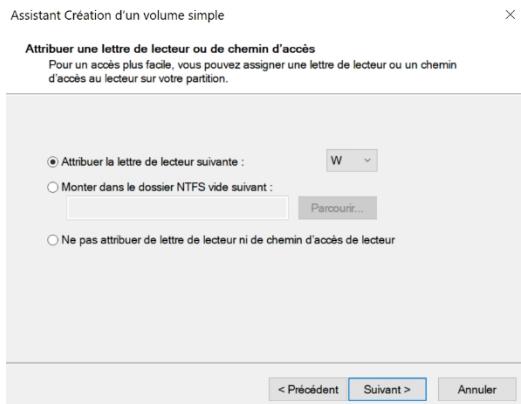
- Rallumez la VM, tapez « Windows+X », cliquez sur « Gestionnaire des disques » puis clic droit sur le disque avec un volume « Non alloué » et cliquez sur « nouveau volume simple » :



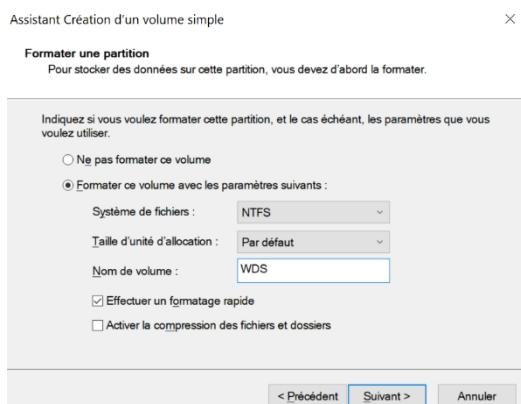
- Indiquez la taille que vous voulez mettre puis cliquez sur « Suivant » :



- Vous pouvez modifier la lettre du lecteur puis cliquez sur « Suivant » :



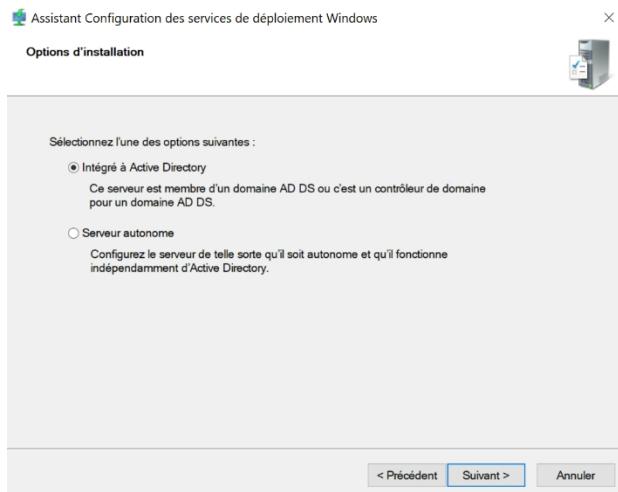
- Vous pouvez modifier le système de fichiers et le nom du volume puis cliquez sur « Suivant » :



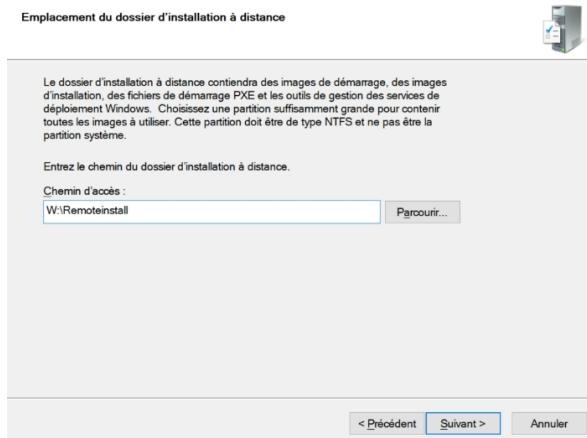
- Accédez au « Services de déploiement Windows », cliquez sur « Servers » puis sur « SRV-V-WDS » et sur « Configurer le serveur » :



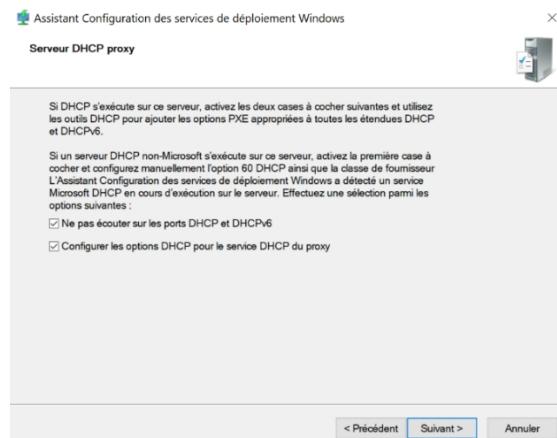
- Cliquez sur « Suivant » une première fois car nous avons un serveur DHCP et un DNS, puis cliquez sur « Suivant » pour l'intégrer à Active Directory :



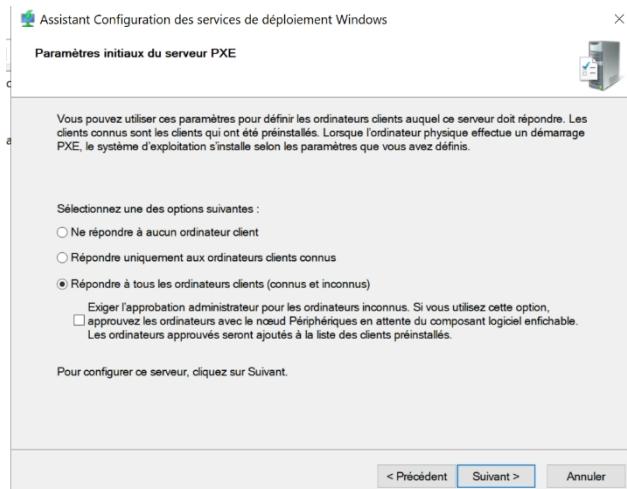
- Sélectionnez le volume créer précédemment puis cliquez sur « Suivant » :



- Sélectionnez le volume créer précédemment puis cliquez sur « Suivant » :



- Sélectionnez « Répondre à tous les ordinateurs clients (connus et inconnus) » puis cliquez sur « Suivant » :



F. Déploiement avec le couple WDS - MDT

La console MDT va permettre de créer des séquences de tâches pour personnaliser le déploiement de systèmes d'exploitation Microsoft sur des machines :

- Gérer le nom de la machine et son appartenance à un domaine Active Directory
- Gérer le partitionnement des disques de la machine
- Gérer le chiffrement BitLocker sur des volumes
- Installer les pilotes correspondants au matériel de la machine
- Exécuter des scripts pour réaliser des tâches diverses et variés

1. Installation Windows ADK, Windows PE et MDT
 - Téléchargez-le avec le lien <https://learn.microsoft.com/fr-fr/windows-hardware/get-started/adk-install> les logiciels ci-dessous :
 - Télécharger le Windows ADK 10.1.26100.2454 (décembre 2024) ↗
 - Télécharger le module complémentaire Windows PE pour l'ADK Windows 10.1.26100.2454 (décembre 2024) ↗
 - Sélectionnez les 4 fonctionnalités pour ADK :



- Téléchargez la version x64 de MDT avec le lien <https://www.microsoft.com/en-us/download/details.aspx?id=54259> :

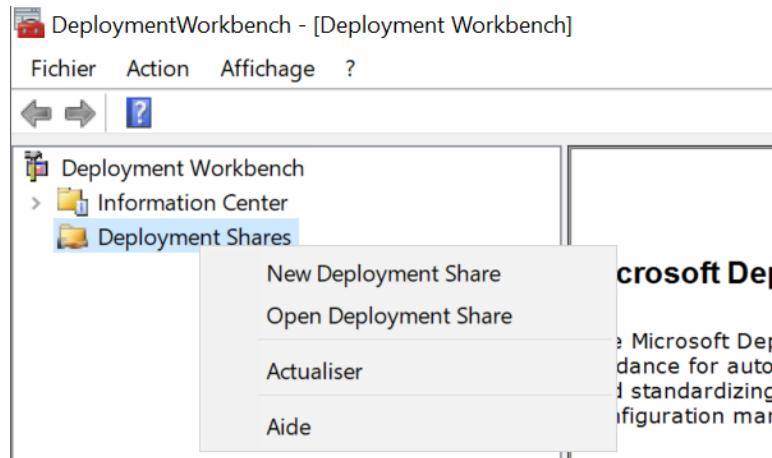
The screenshot shows the Microsoft Download Manager interface. It has a header 'Choose the download you want' and a note 'File Name' and 'Size'. Below is a table with two rows:

File Name	Size
<input type="checkbox"/> MicrosoftDeploymentToolkit_x86.msi	20.1 MB
<input checked="" type="checkbox"/> MicrosoftDeploymentToolkit_x64.msi	20.6 MB

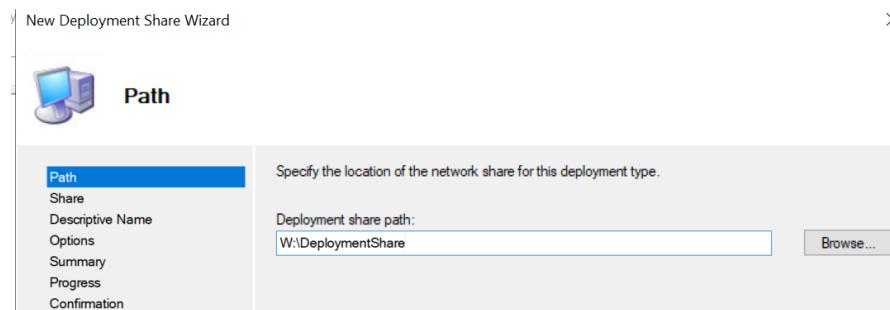
At the bottom, there is a 'Download' button and a note 'Total size: 20.6 MB'. Below this is a screenshot of the Windows Start Menu showing the 'Windows Server' desktop icon and various administrative tools like Gestionnaire de serveur, Windows PowerShell, and Panneau de configuration.

2. Créer le Deployment Share

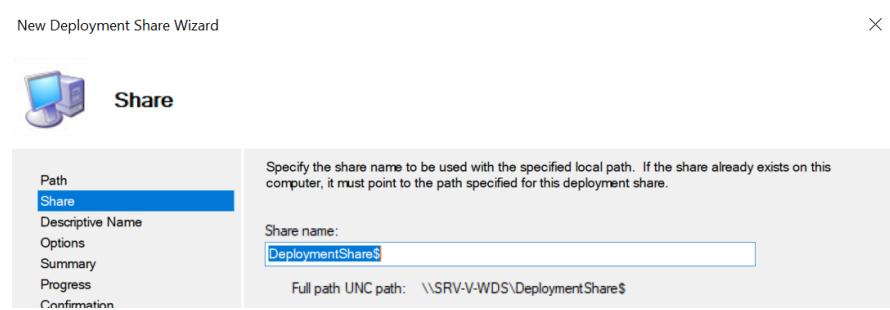
- Ouvrez la console "Deployment Workbench", effectuez un clic droit sur "Deployment Shares" > "New Deployment Share" :



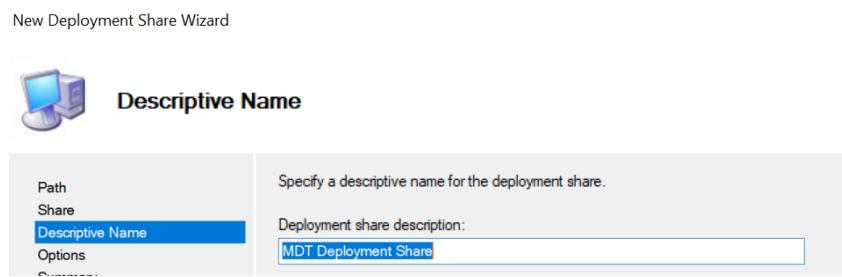
- Indiquez l'emplacement du Deployment Share. Ce dossier sera partagé et il va contenir l'ensemble des données de MDT :



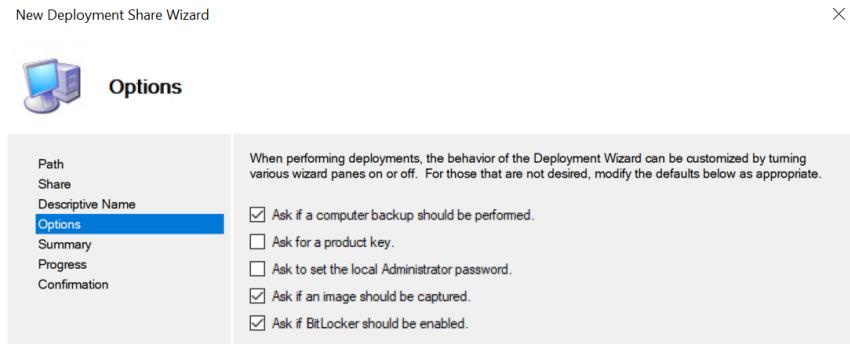
- Laissez la valeur par défaut qui est un partage caché "DeploymentShare\$" :



- Mettez « MDT Deployment Share » comme description :



- Conservez les étapes de l'assistant de déploiement par défaut :



3. Créer un utilisateur local dédié à MDT

Au lancement de la machine en boot PXE. Elle va charger une image de démarrage qui va établir une connexion au MDT. La machine doit utiliser un compte utilisateur pour s'authentifier sur le partage et accéder aux données (images, pilotes, séquences de tâches, etc.).

- Créez un compte utilisateur qui n'est pas administrateur du serveur avec des attributions des droits de lecture et exécution sur le partage. Tapez cette commande dans le PowerShell ISE :

Sur le serveur MDT, exéutez le script PowerShell suivant :

```
# Spécifier le nom et le mot de passe du compte de service
```

```
$ServiceAccountName = "Service_MDT"
```

```
$ServiceAccountPassword = ConvertTo-SecureString "Adm.2022" -AsPlainText -Force
```

```
# Créer le compte local
```

```
New-LocalUser $ServiceAccountName -Password $ServiceAccountPassword -FullName "MDT" -Description "Compte de service pour MDT"
```

```
# Ajouter les droits en lecture sur le partage
```

```
Grant-SmbShareAccess -Name "DeploymentShare$" -AccountName "Service_MDT" -AccessRight Read -Force
```

```
# Attribuer au compte de service les permissions nécessaires pour accéder aux fichiers de déploiement MDT
```

```

$MDTSharePath = "\$env:COMPUTERNAME\DeploymentShare\$"

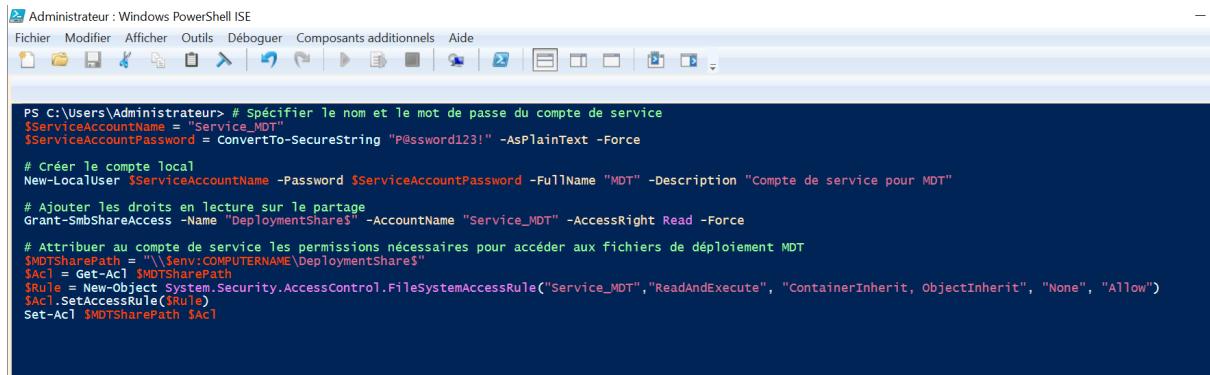
$Acl = Get-Acl $MDTSharePath

$Rule = New-Object
System.Security.AccessControl.FileSystemAccessRule("Service_MDT", "ReadAndExecute",
"ContainerInherit, ObjectInherit", "None", "Allow")

$Acl.SetAccessRule($Rule)

Set-Acl $MDTSharePath $Acl

```



The screenshot shows a Windows PowerShell ISE window. The code in the editor is:

```

PS C:\Users\Administrateur> # Spécifier le nom et le mot de passe du compte de service
$ServiceAccountName = "Service_MDT"
$ServiceAccountPassword = ConvertTo-SecureString "P@ssword123!" -AsPlainText -Force

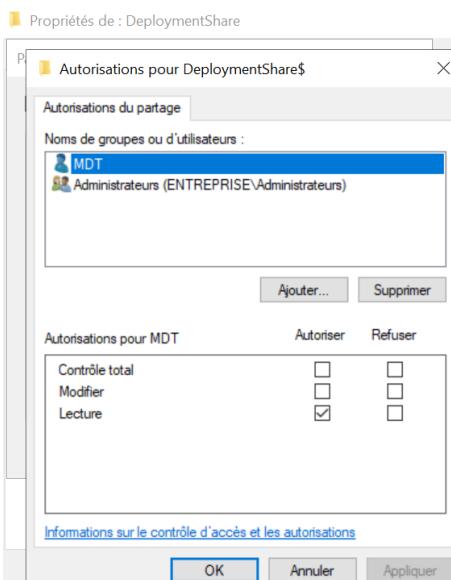
# Créer le compte local
New-LocalUser $ServiceAccountName -Password $ServiceAccountPassword -FullName "MDT" -Description "Compte de service pour MDT"

# Ajouter les droits en lecture sur le partage
Grant-SmbShareAccess -Name "DeploymentShare$" -AccountName "Service_MDT" -AccessRight Read -Force

# Attribuer au compte de service les permissions nécessaires pour accéder aux fichiers de déploiement MDT
$MDTSharePath = "\$env:COMPUTERNAME\DeploymentShare$"
$Acl = Get-Acl $MDTSharePath
$Rule = New-Object System.Security.AccessControl.FileSystemAccessRule("Service_MDT", "ReadAndExecute", "ContainerInherit, ObjectInherit", "None", "Allow")
$Acl.SetAccessRule($Rule)
Set-Acl $MDTSharePath $Acl

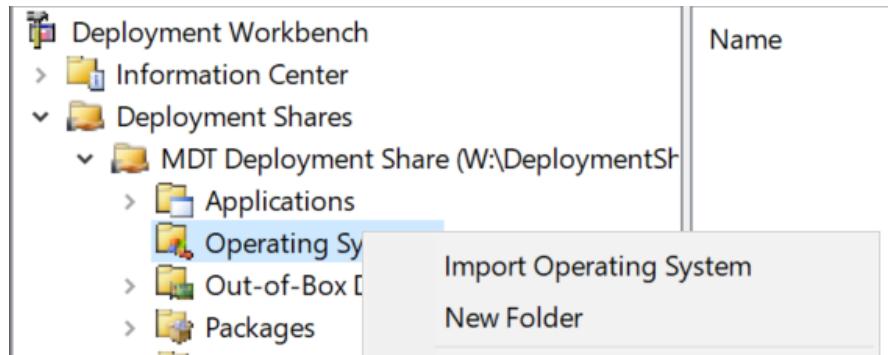
```

- L'utilisateur "Service_MDT" possède l'accès en lecture seule sur le Deployment Share :

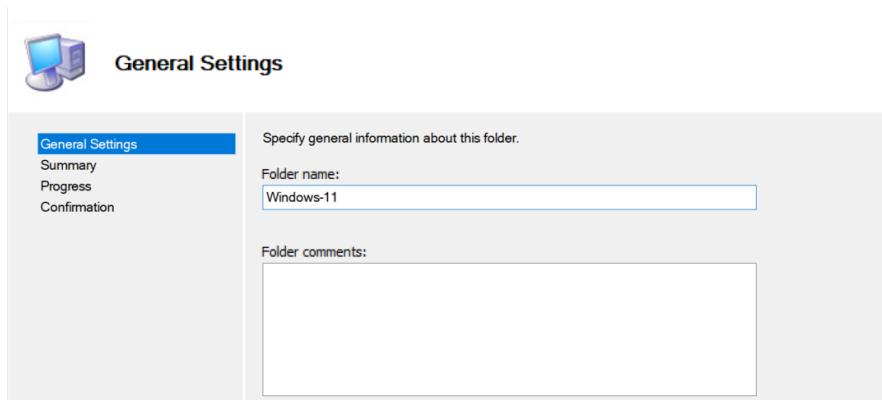


4. Importer une image Windows 11 dans MDT

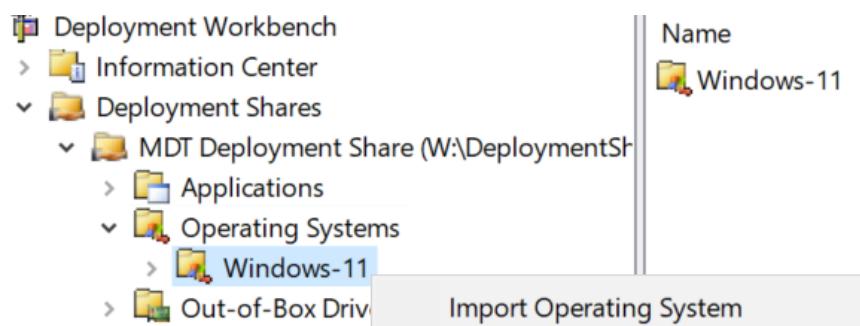
- Effectuez un clic droit sur Operating Systems > Import Operating System > New Folder pour créer un dossier afin d'organiser vos images :



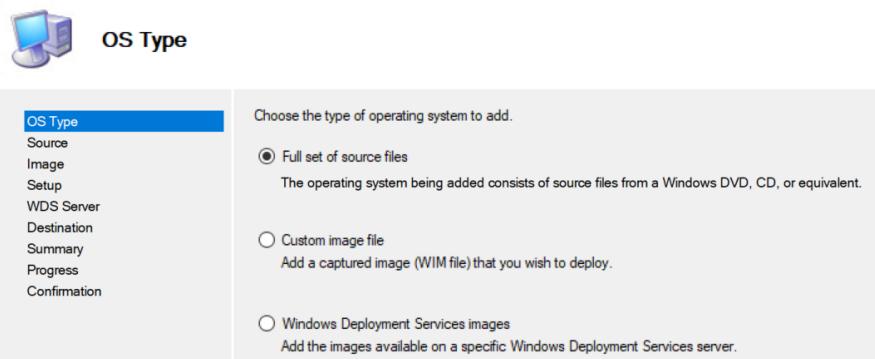
- Nommez le dossier :



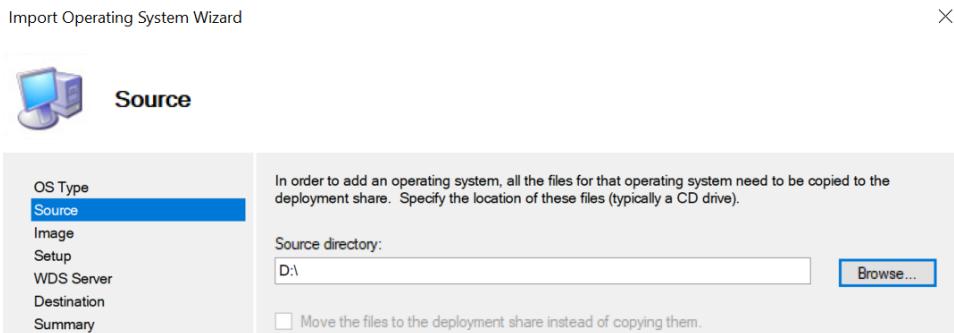
- Importez l'image avec Operating Systems > Windows-11 > Import Operating System :



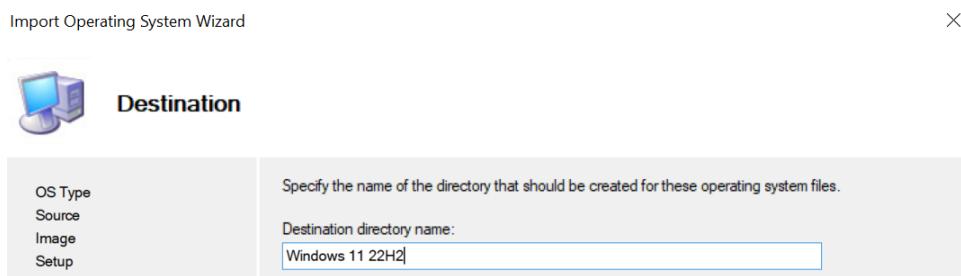
- Choisissez "Full set of source files" :



- Sélectionnez le lecteur DVD « D:\ » :



- Nommez cette image :

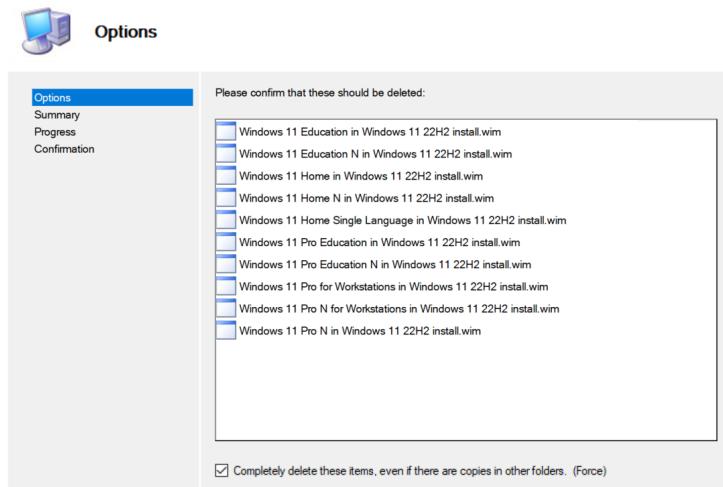


- Dans la liste "Operating Systems", gardez la version « Windows 11 Pro » et supprimer les autres :

A screenshot of the Deployment Workbench interface. On the left is a navigation tree with 'Deployment Workbench' expanded, showing 'Information Center', 'Deployment Shares' (selected), 'MDT Deployment Share (W:\DeploymentShare)', 'Applications', 'Operating Systems' (selected), 'Windows-11', 'Out-of-Box Drivers', 'Packages', 'Task Sequences', 'Advanced Configuration', and 'Monitoring'. On the right is a table listing various Windows 11 installation files. A context menu is open over the last few items in the list, showing options: 'Couper', 'Copier', 'Supprimer', and 'Aide'. The table columns are 'Name', 'Description', 'Platform', 'Build', and 'OSType'.

Name	Description	Platform	Build	OSType
Windows 11 Education in Windows 11 22H2 install.wim	Windows 11 Education	x64	100.26100.1742	Wind
Windows 11 Education N in Windows 11 22H2 install.wim	Windows 11 Education N	x64	100.26100.1742	Wind
Windows 11 Home in Windows 11 22H2 install.wim	Windows 11 Home	x64	100.26100.1742	Wind
Windows 11 Home N in Windows 11 22H2 install.wim	Windows 11 Home N	x64	100.26100.1742	Wind
Windows 11 Home Single Language in Windows 11 – Wind	Windows 11 Home Single Language	x64	100.26100.1742	Wind
Windows 11 Pro Education in Windows 11 22H2 inst...	Wind	x64	100.26100.1742	Wind
Windows 11 Pro Education N in Windows 11 22H2 ...	Wind	x64	100.26100.1742	Wind
Windows 11 Pro for Workstations in Windows 11 22H2 ...	Wind	x64	100.26100.1742	Wind
Windows 11 Pro in Windows 11 22H2 install.wim	Wind	x64	100.26100.1742	Wind
Windows 11 Pro N for Workstations in Windows 11 – Wind	Wind	x64	100.26100.1742	Wind
Windows 11 Pro N in Windows 11 22H2 install.wim	Windows 11 Pro N	x64	100.26100.1742	Wind

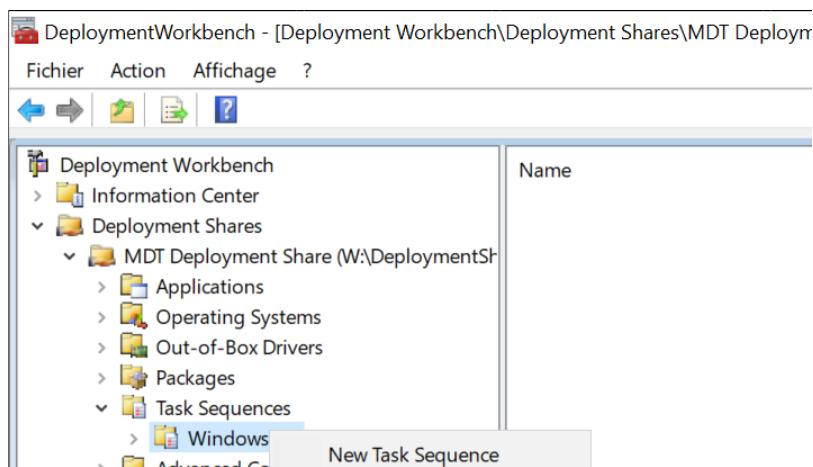
- Cochez force :



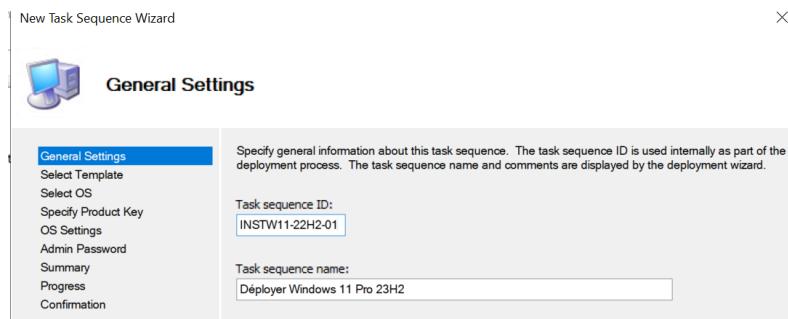
5. Créer une séquence de tâches pour Windows 11

Il faut l'ajouter à une séquence de tâches pour que l'image d'installation de Windows 11 22H2 soit déployée sur une machine.

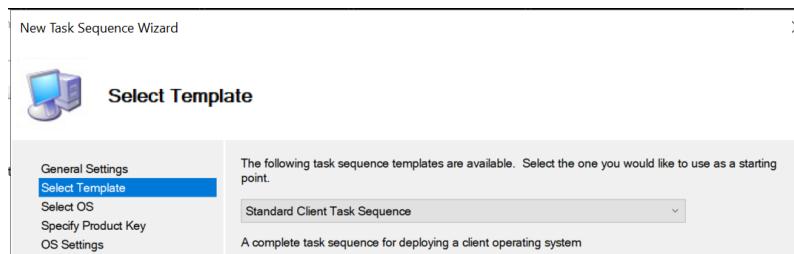
- Effectuez un clic droit sur "Task Sequences > New Task Sequence :



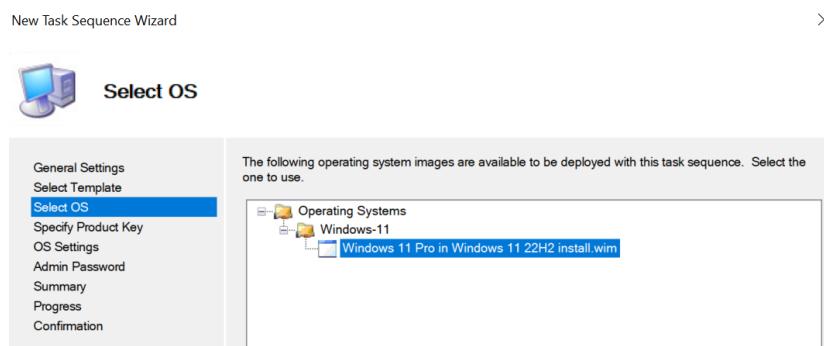
- Indiquez le nom qui fera office d'ID (identifiant unique) pour cette séquence de tâches, puis indiquez un nom "Déployer Windows 11 Pro 23H2" :



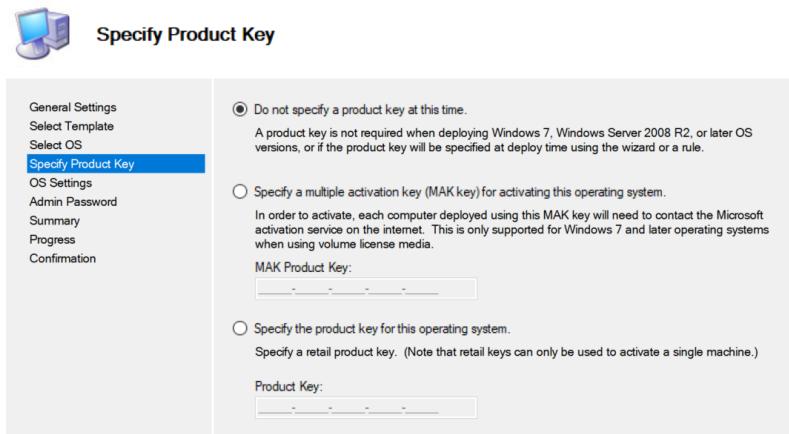
- Sélectionnez le template "Standard Client Task Sequence" pour que l'on puisse déployer l'OS :



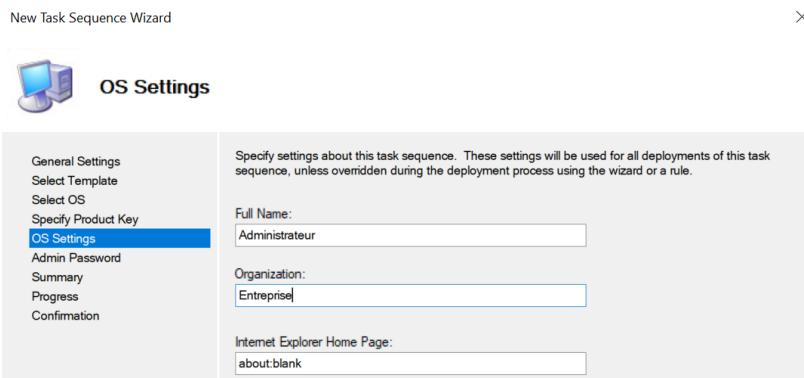
- Sélectionnez l'image Windows 11 importer précédemment :



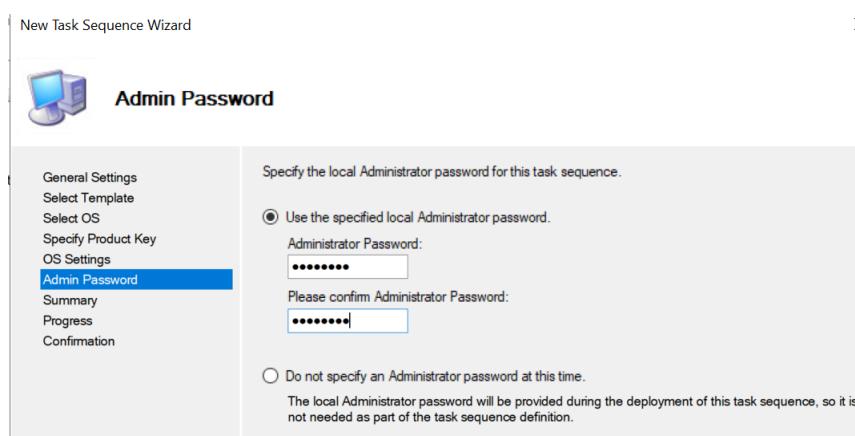
- Laissez par défaut :



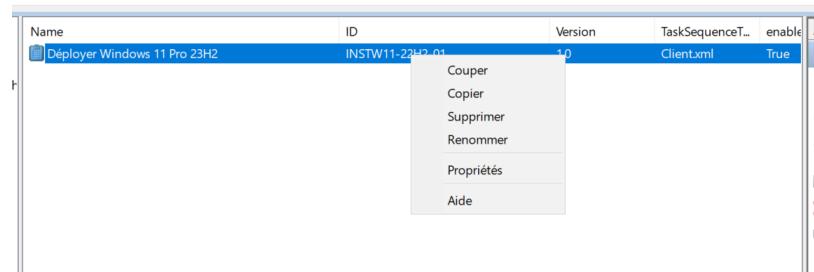
- Indiquez le nom du compte utilisateur qui sera créé par défaut sur la machine déployée, ainsi que le nom de l'organisation. Ce compte sera administrateur de la machine :



- Définissez un mot de passe pour le compte Administrateur local de cette machine :

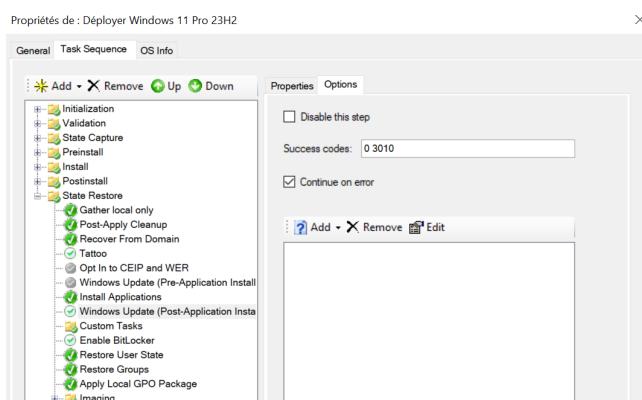


- Vous pouvez éditer la task avec clic droit dessus puis "Propriétés" :



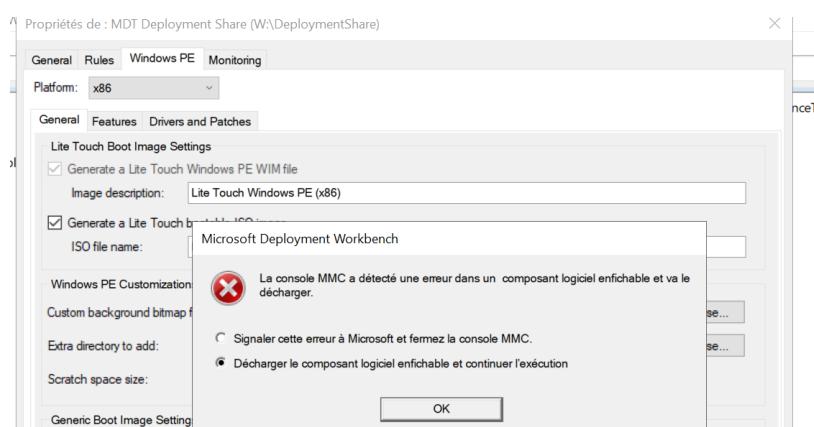
L'onglet "Task Sequence" contient l'ensemble des tâches qui seront exécutées pendant le déploiement de la machine comme le partitionnement du disque et configuration post-installation. Elles peuvent être activée ou désactivée, et si une tâche est considérée comme critique, on peut arrêter le déploiement si elle échoue.

- Activer la tâche "Windows Update (Post-Application Installation)", cliquez dessus > Options > décochez la case "Disable this step" :



G. Configurer MDT pour Windows 11 (et éviter des problèmes)

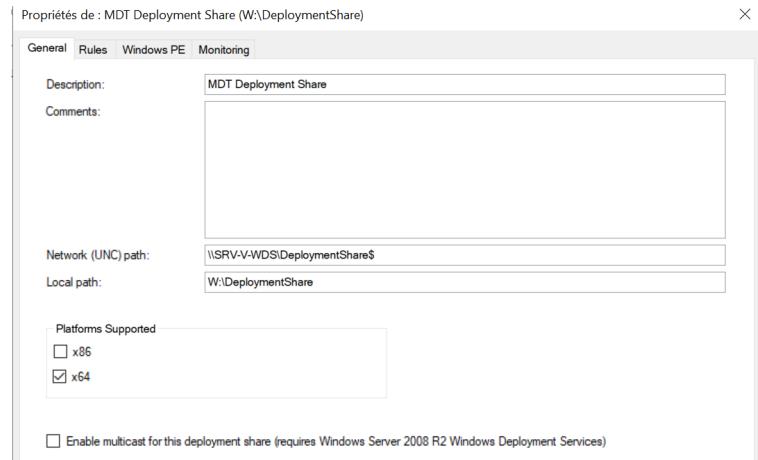
- Bug de la console MMC avec l'onglet Windows PE
- Allez dans Deployment Share > Windows PE, une erreur apparait et plus rien ne fonctionne :



- Créez un dossier vide avec la commande :

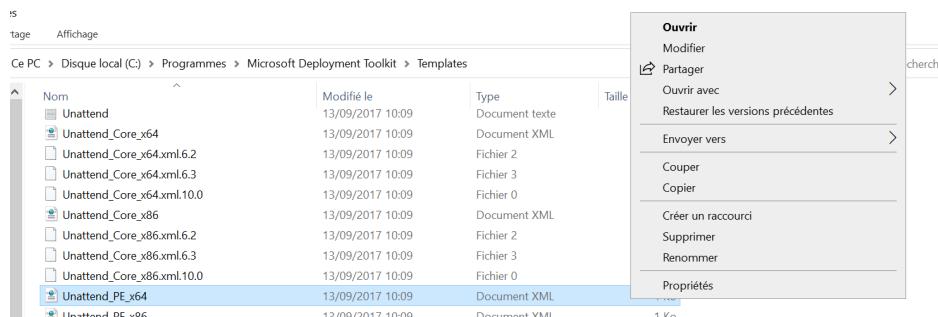
```
mkdir "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\WinPE_OCs"
```

- Dans General, décochez le support du x86 :



L'erreur Script Error avec le texte "An error has occurred in the script on this page" au moment de lancer un déploiement (ou une capture) sur une machine.

- Modifiez le fichier "Unattend_PE_x64.xml" en allant dans C:\Program Files\Microsoft Deployment Toolkit\Templates :



- Supprimez le contenu de ce fichier et mettez à la place le contenu du lien https://learn.microsoft.com/en-us/mem/configmgr/mdt/known-issues?WT.mc_id=AZ-MVP-5004580#hta-applications-report-script-error-after-upgrading-to-adk-for-windows-11-version-22h2?WT.mc_id=AZ-MVP-5004580 :

```
apide Unattend 13/09/2017 10:09 Document texte 20 Ko
iu Fichier Edition Format Affichage Aide
vargeme <unattend xmlns="urn:schemas-microsoft-com:unattend">
ments <settings pass="windowsPE">
es <component name="Microsoft-Windows-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" l
inistrations <Display>
je local (C: <ColorDepth>32</ColorDepth>
m32 <HorizontalResolution>1024</HorizontalResolution>
<RefreshRate>60</RefreshRate>
<VerticalResolution>768</VerticalResolution>
</Display>
<RunSynchronous>
<RunSynchronousCommand wcm:action="add">
<Description>Fix HTA scripts error Windows 11 ADK 22H2</Description>
<Order>1</Order>
<Path>reg.exe add "HKLM\Software\Microsoft\Internet Explorer>Main" /t REG_DWORD /v JscriptRepla
</RunSynchronousCommand>
<RunSynchronousCommand wcm:action="add">
<Description>Lite Touch PE</Description>
<Order>2</Order>
<Path>wscript.exe X:\Deploy\Scripts\LiteTouch.wsf</Path>
</RunSynchronousCommand>
</RunSynchronous>
</component>
</settings>
</unattend>
```

H. Personnaliser le bootstrap.ini et le CustomSettings.ini

La configuration globale de MDT et de l'environnement de déploiement s'effectue au travers de deux fichiers de configuration bootstrap.ini et CustomSettings.ini.

- Pour accéder au contenu du fichier "CustomSettings.ini", clic droit sur le Deployment Share > Propriétés > Rules :

[Settings]

Priority=Default

Properties=MyCustomProperty

[Default]

OSInstall=Y

SkipCapture=NO

SkipAdminPassword=YES

SkipProductKey=YES

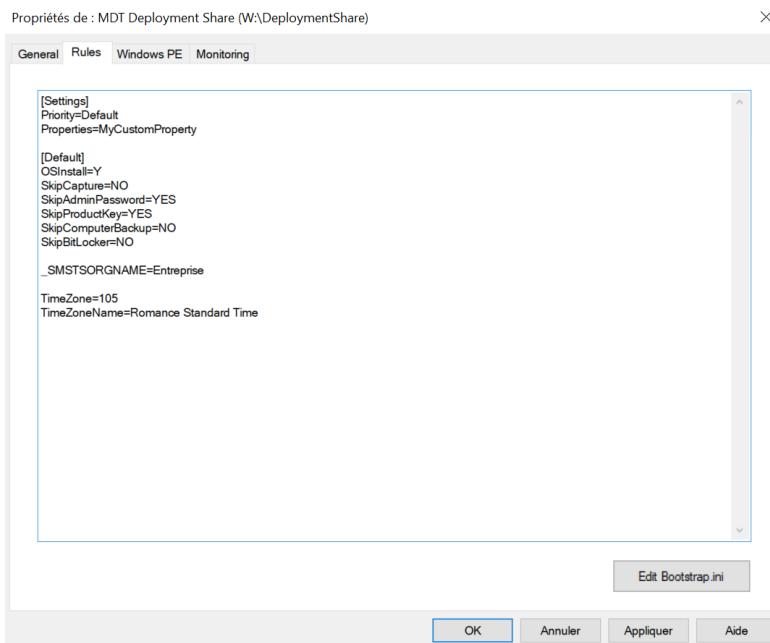
SkipComputerBackup=NO

SkipBitLocker=NO

_SMSTSORGNAME=Enterprise

TimeZone=105

TimeZoneName=Romance Standard Time



- Pour le fichier "Bootstrap.ini", cliquez sur "Edit Bootstrap.ini". Dans ce fichier mettez **le chemin réseau vers le Deployment Share, le nom de l'utilisateur et le mot de passe à utiliser pour se connecter à ce partage** :

DeployRoot=\SRV-WDS\DeploymentShare\$: Chemin UNC vers le partage Deployment Share

UserID=Service_MDT : nom du compte utilisateur

UserPassword= Adm.2022 : mot de passe du compte utilisateur

UserDomain=SRV-WDS : nom de domaine Active Directory ou nom du serveur s'il s'agit d'un compte local

On ajoutera aussi une option pour disposer du clavier en français. Ce qui donne :

[Settings]

Priority=Default

[Default]

DeployRoot=\SRV-WDS\DeploymentShare\$

UserID=Service_MDT

UserPassword=Adm.2022

UserDomain=SRV-WDS

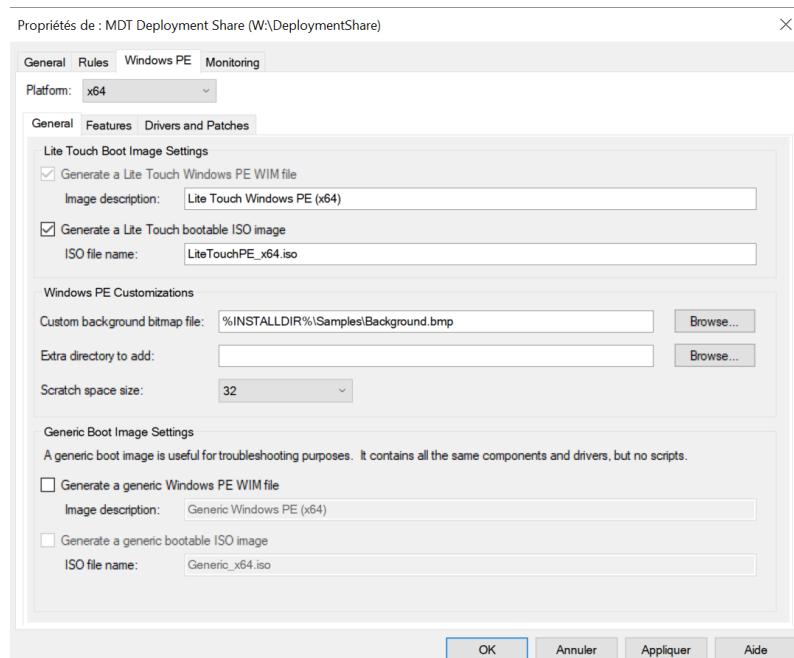
SkipBDDWelcome=YES

KeyboardLocalePE=040c : 0000040c

```
Bootstrap - Bloc-notes
Fichier Edition Format Affichage Aide
[Settings]
Priority=Default

[Default]
DeployRoot=\SRV-WDS\DeploymentShare$
UserID=Service_MDT
UserPassword=Adm.2022
UserDomain=SRV-WDS
SkipBDDWelcome=YES
KeyboardLocalePE=040c : 0000040c
```

- Dans « Windows PE », choisissez la "Platform" en "x64" :

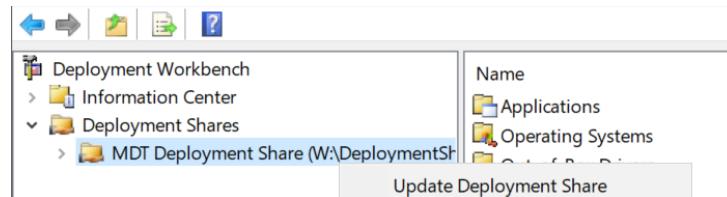


I. Générer l'image Lite Touch et l'importer dans WDS

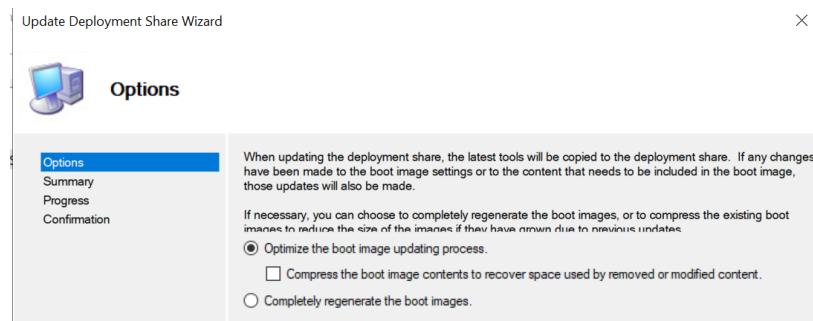
1. MDT : générer l'image Lite Touch

L'image Lite Touch correspond à l'environnement de démarrage en boot PXE : elle doit être générée avec la console MDT pour intégrer notre configuration, notamment les identifiants de connexion au Deployment Share.

- Effectuez un clic droit sur le Deployment Share > Update Deployment Share :



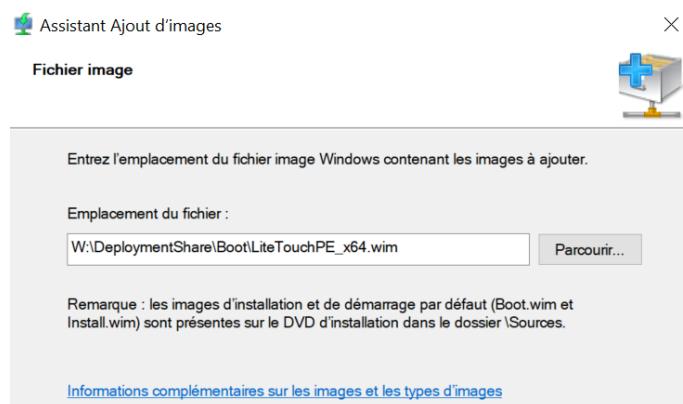
- Laissez « Optimize the boot image updating process » :



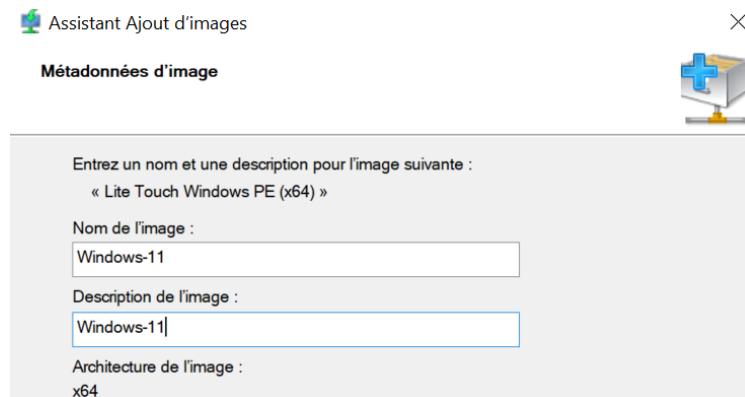
2. WDS : importer l'image Lite Touch

Comme évoqué précédemment, c'est cette image que nous devons charger en boot PXE. Ainsi, sur le serveur WDS, il faut l'ajouter en tant qu'image de démarrage.

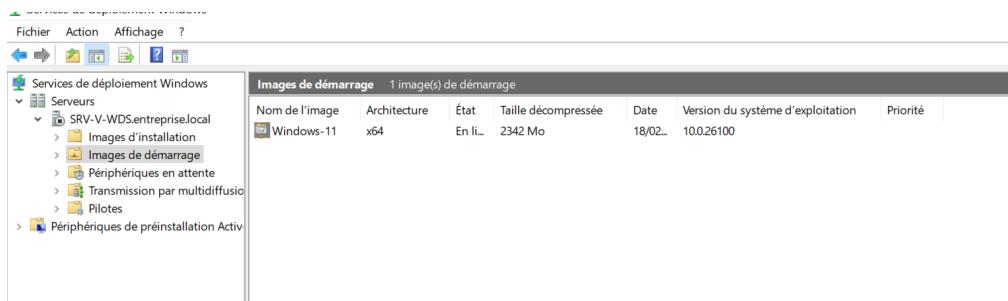
- À partir de la console WDS, ajoutez une nouvelle image et chargez le fichier suivant :



- Renommez-le :



- L'image Lite Touch est bien ajoutée et elle est en ligne :



J. Déploiement de l'image de démarrage

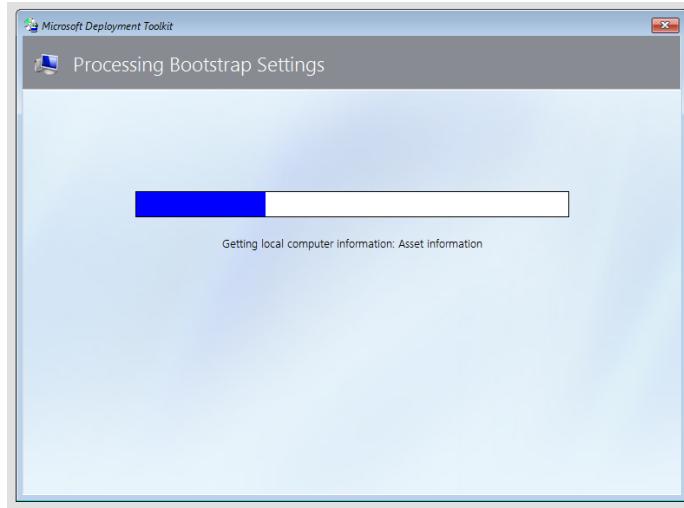
- Lancez la VM vierge et pressez « ENTER » :



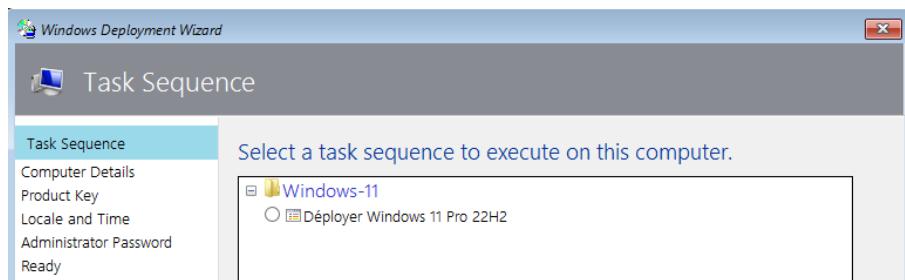
- La VM va installer l'image de démarrage, l'installation peut prendre du temps :



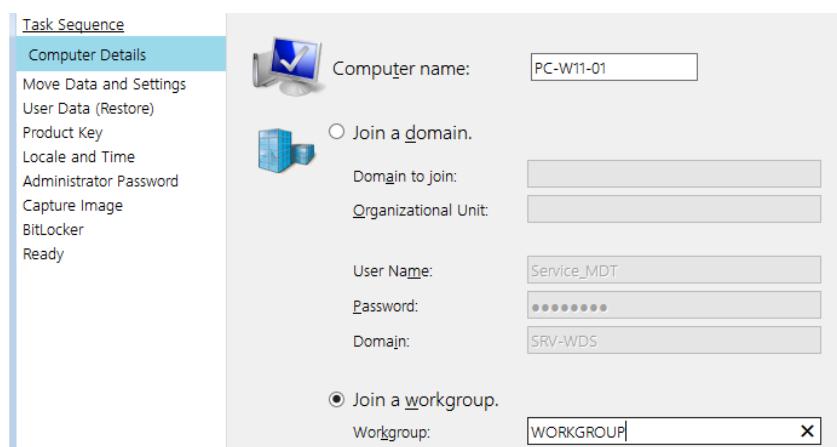
- Après avoir chargé l'image, une fenêtre "Microsoft Deployment Toolkit" :



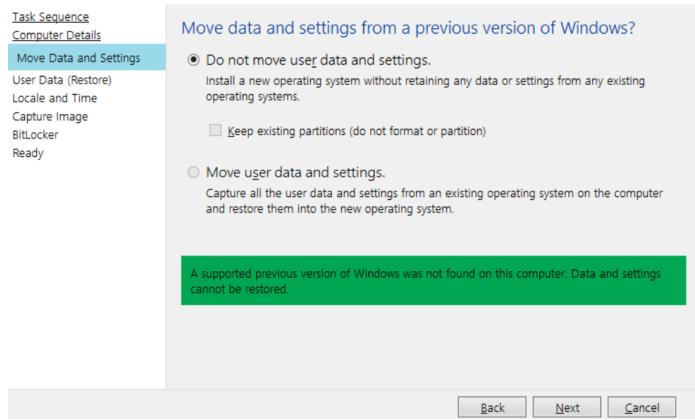
- Dans l'onglet "Task Sequence", sélectionnez la séquence de tâches à exécuter > Déployer Windows 11 pro 22H2 :



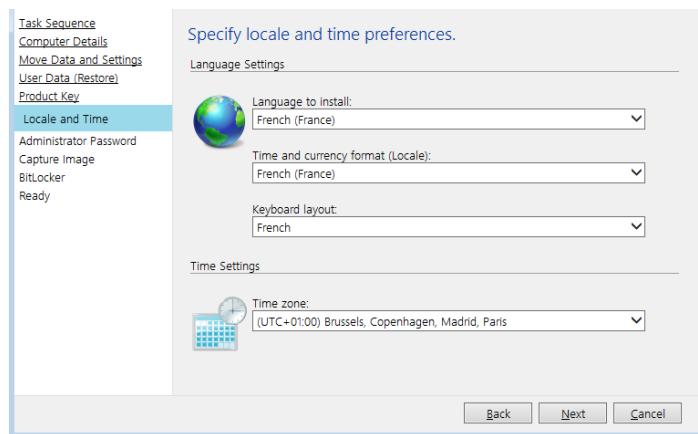
- Nommez la machine :



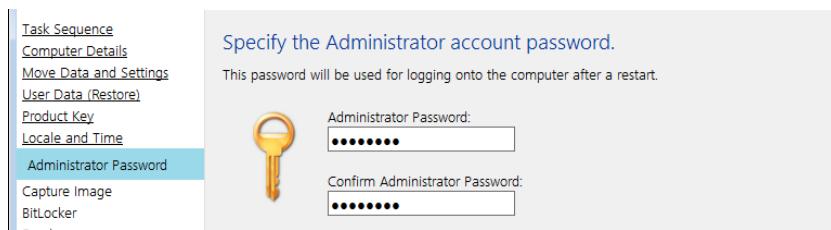
- Next :



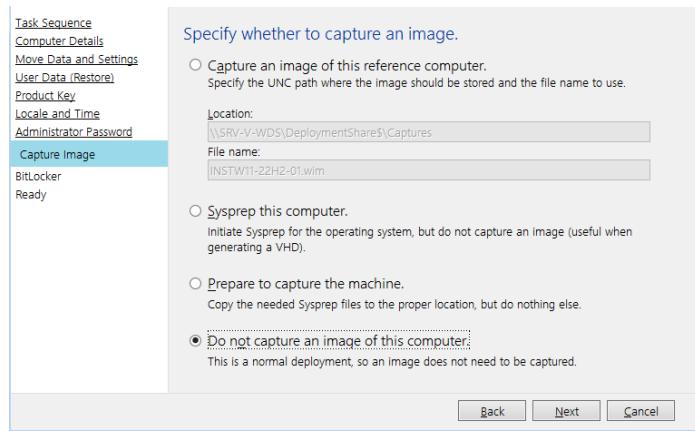
- L'étape "Locale and Time" permet de définir la langue, la disposition du clavier et le fuseau horaire. Tout est déjà correct grâce à la configuration effectuée dans les fichiers INI de MDT.



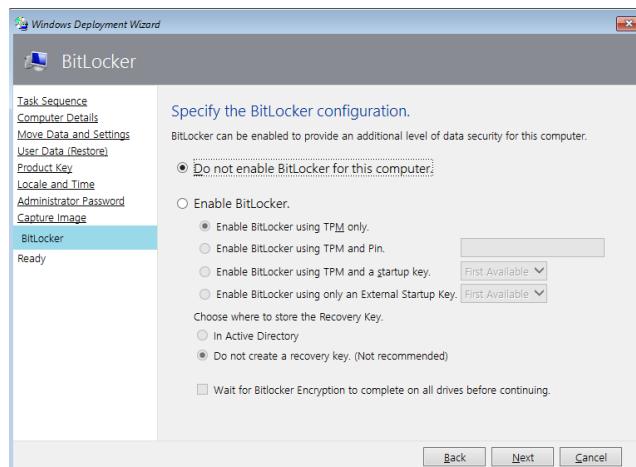
- Mettez le mot de passe de l'administrateur :



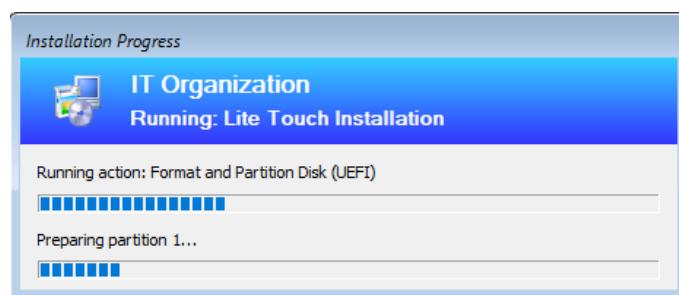
- Next :



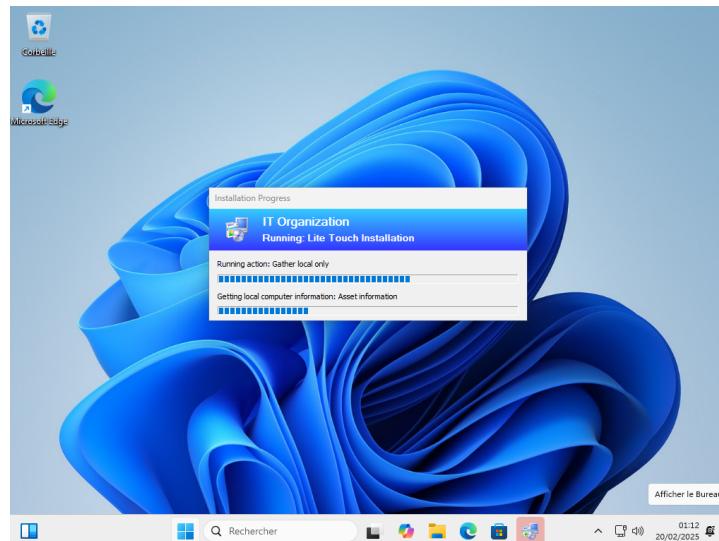
- Next :



- MDT va enchaîner toutes les étapes configurées dans la séquence de tâches sélectionnée. Cela intègre notamment l'installation de l'image Windows 11 Pro 23H2 :



- MDT fini d'installer les mises à jour Windows :



- Une fenêtre s'affiche et cliquez sur « Finish » :

