

Mémoire de stage

BTS SIO Option SISR

Renouvellement par masterisation des postes clients d'une PME

Colin MONTERASTELLI

30 Août 2024

I. Introduction	6
II. Création de l'image de déploiement avec NTLITE	6
2.1 Présentation de NTLITE	6
2.2 Téléchargement et installation de NTLITE	7
2.3 Préparation de l'image Windows 11	7
2.4 Chargement de l'image dans NTLITE	8
2.5 Personnalisation de l'image	8
2.5.1 Suppression des composants inutiles	9
2.5.2 Intégration des applications requises	9
2.5.3 Configuration de Google Chrome	11
2.6 Application des paramètres de sécurité	12
2.7 Création de l'image finale	12
2.8 Vérification de l'image	13
III. Déploiement par clé USB de l'image NTLITE	14
3.1 Introduction au déploiement par clé USB	14
3.2 Préparation de la clé USB	14
3.2.1 Téléchargement et installation de Rufus	14
3.2.2 Création de la clé USB bootable	15
3.3 Procédure de déploiement	17
3.3.1 Configuration du BIOS/UEFI	17
3.3.2 Installation de l'image	18
3.3.3 Configuration post-installation	19
3.4 Avantages et inconvénients du déploiement par clé USB	20
3.5 Considérations de sécurité	20
IV. Déploiement par le réseau avec un serveur FOG	22

4.1 Introduction à FOG Project	22
4.2 Installation du serveur FOG	22
4.2.1 Prérequis	22
4.2.2 Installation d'Ubuntu Server	23
4.2.3 Installation de FOG	23
4.3 Configuration du serveur FOG	27
4.3.1 Accès à l'interface web	27
4.3.2 Configuration initiale	28
4.4 Création et upload de l'image	28
4.4.1 Préparation de l'image de référence	28
4.4.2 Création de l'image dans FOG	29
4.4.3 Upload de l'image	29
4.5 Déploiement de l'image	30
4.5.1 Enregistrement des postes clients	30
4.5.2 Création d'une tâche de déploiement	31
4.5.3 Lancement du déploiement	32
4.6 Post-déploiement	32
4.6.1 Vérification	32
4.6.2 Mise à jour de l'inventaire	32
4.7 Avantages et inconvénients du déploiement avec FOG	33
4.8 Considérations de sécurité	33
V. Déploiement par le réseau avec un serveur WDS	34
5.1 Introduction à Windows Deployment Services (WDS)	34
5.2 Installation et configuration de WDS	34
5.2.1 Prérequis	34

5.2.2 Installation du rôle WDS	34
5.2.3 Configuration initiale de WDS	35
5.3 Préparation des images pour WDS	36
5.3.1 Conversion de l'image NTLITE en format WIM	36
5.3.2 Ajout de l'image à WDS	36
5.4 Configuration des options de déploiement	39
5.4.1 Création d'un fichier de réponse	39
5.4.2 Association du fichier de réponse à l'image	39
5.5 Préparation des postes clients	39
5.5.1 Configuration du BIOS/UEFI	39
5.6 Processus de déploiement	40
5.6.1 Démarrage PXE et sélection de l'image	40
5.6.2 Installation automatisée	41
5.6.3 Finalisation et vérification	41
5.7 Gestion post-déploiement	42
5.7.1 Mise à jour de l'image	42
5.7.2 Surveillance et maintenance	42
5.8 Avantages et inconvénients du déploiement avec WDS	42
5.9 Considérations de sécurité	42
VI. Configuration de sécurité selon les recommandations de l'ANSSI et Microsoft	44
6.1 Introduction à la sécurisation des postes clients	44
6.2 Guides de référence	44
6.3 Configuration des paramètres de sécurité	44
6.3.1 Gestion des comptes utilisateurs	44
6.3.2 Restriction des droits d'administration	45

6.3.3 Configuration du pare-feu Windows	45
6.3.4 Mise à jour automatique	46
6.3.5 BitLocker	46
6.3.6 Désactivation des services inutiles	47
6.3.7 Configuration de Microsoft Defender	47
6.3.8 Désactivation des protocoles obsolètes	48
6.3.9 Restriction des autorisations PowerShell	48
6.4 Application des paramètres via les stratégies de groupe (GPO)	49
6.5 Audit et surveillance	49
6.5.1 Configuration de l'audit	49
6.5.2 Centralisation des journaux	50
6.6 Gestion des vulnérabilités	50
6.6.1 Analyse régulière des vulnérabilités	50
6.6.2 Veille sur les bulletins de sécurité	50
6.7 Formation et sensibilisation des utilisateurs	50
6.7.1 Programme de sensibilisation	50
6.7.2 Documentation utilisateur	51
6.8 Tests et validation	51
6.8.1 Tests de pénétration	51
6.8.2 Audit de conformité	51
VII. Conclusion	51
7.1 Récapitulatif des méthodes de déploiement	52
7.2 Importance de la sécurisation	52
7.3 Recommandations	52
7.4 Perspectives d'avenir	53

I. Introduction

Dans le cadre du renouvellement intégral du parc informatique de l'entreprise EXPERTY, ce mémoire présente une étude approfondie des différentes méthodes de déploiement d'images Windows 11 sur 80 postes clients. L'objectif principal est d'automatiser au maximum ce processus tout en respectant les meilleures pratiques de sécurité.

Ce document détaille les procédures complètes pour la création et le déploiement d'images Windows 11 à l'aide de différents outils : NTLITE, FOG Project, et Windows Deployment Services (WDS). Chaque méthode sera expliquée en détail, accompagnée de captures d'écran illustratives et d'explications sur son fonctionnement.

Une attention particulière sera portée à la configuration de sécurité des machines, en suivant les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et de Microsoft.

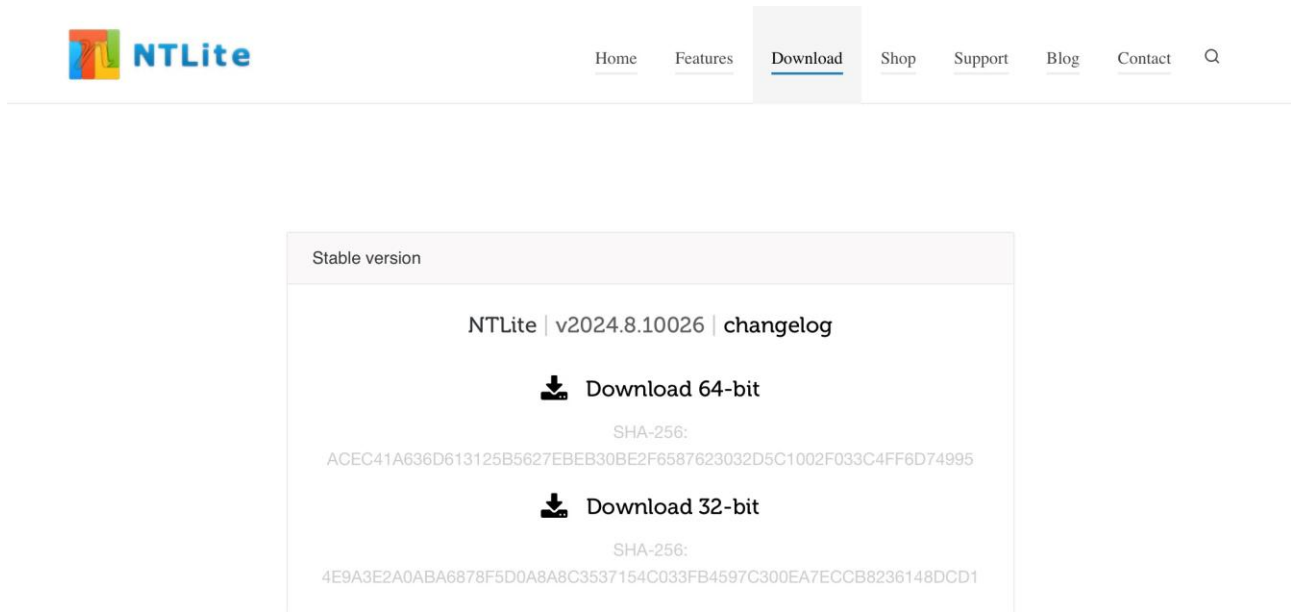
II. Création de l'image de déploiement avec NTLITE

2.1 Présentation de NTLITE

NTLITE est un outil puissant permettant de personnaliser et d'optimiser les images Windows. Il offre la possibilité de modifier les installations Windows existantes, de supprimer des composants inutiles, d'intégrer des mises à jour et des pilotes, et de créer des images de déploiement personnalisées.

2.2 Téléchargement et installation de NTLITE

Pour commencer, téléchargez NTLITE depuis le site officiel : <https://www.ntlite.com/>



Une fois le fichier d'installation téléchargé, suivez ces étapes pour l'installer :

1. Double-cliquez sur le fichier d'installation.
2. Acceptez les termes du contrat de licence.
3. Choisissez le dossier d'installation (laissez le dossier par défaut si vous n'avez pas de préférence particulière).
4. Cliquez sur "Installer" pour lancer l'installation.
5. Une fois l'installation terminée, lancez NTLITE.

2.3 Préparation de l'image Windows 11

Avant de commencer la personnalisation avec NTLITE, nous devons obtenir une image Windows 11 de base. Vous pouvez la télécharger depuis le site officiel de Microsoft ou utiliser une image fournie par votre entreprise.

1. Créez un dossier sur votre disque dur pour y placer les fichiers de l'image

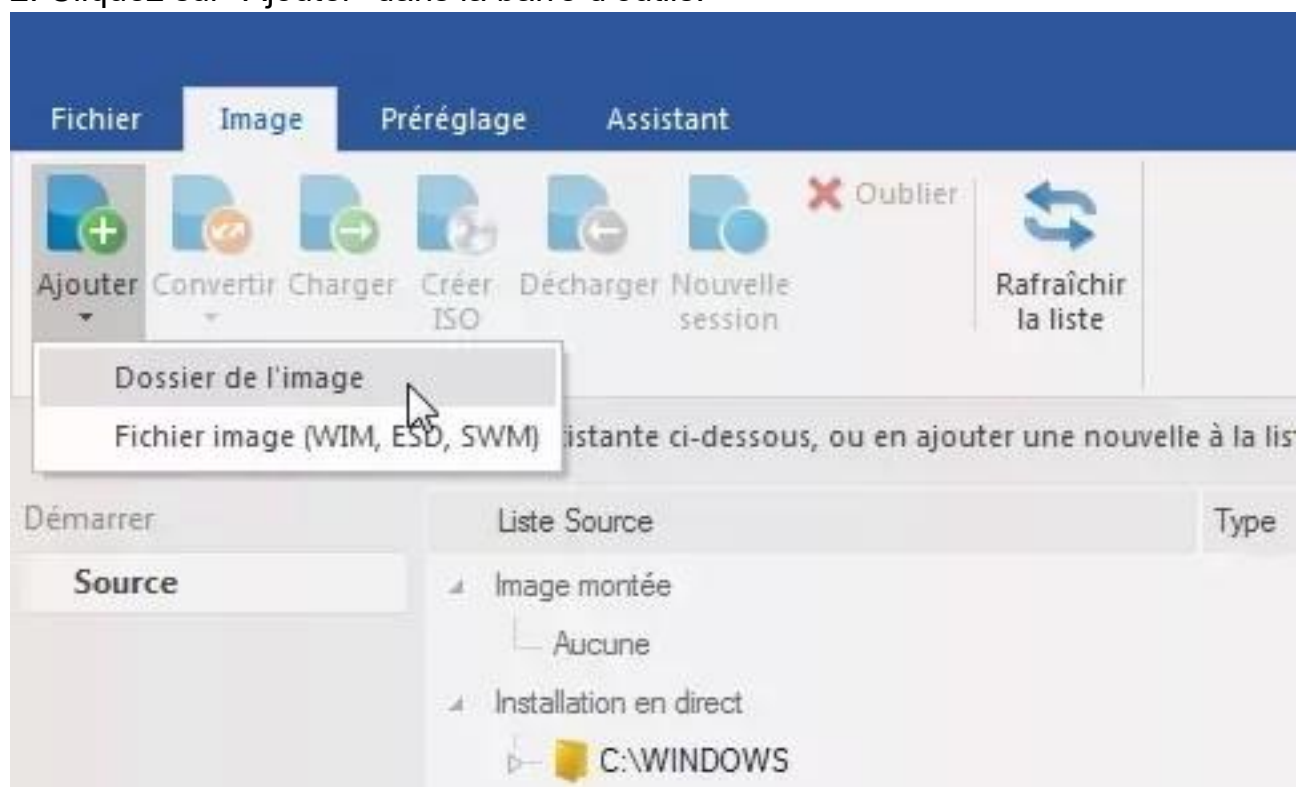
Windows 11.

2. Montez l'image ISO Windows 11 ou extrayez son contenu dans le dossier créé.

2.4 Chargement de l'image dans NTLITE

1. Lancez NTLITE.

2. Cliquez sur "Ajouter" dans la barre d'outils.



3. Naviguez jusqu'au dossier contenant les fichiers de l'image Windows 11 et sélectionnez-le.

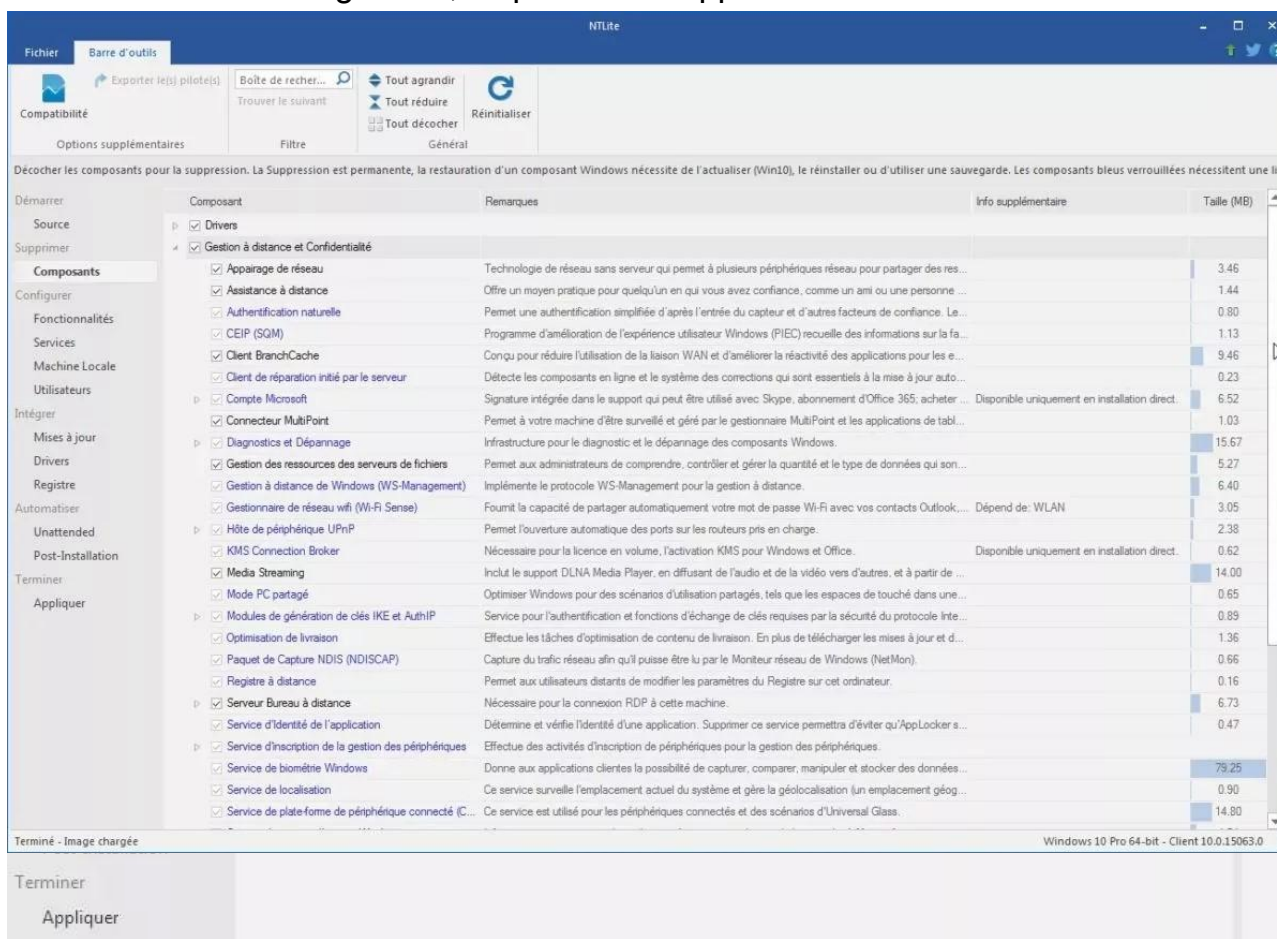
4. NTLITE va analyser l'image et afficher ses détails.

2.5 Personnalisation de l'image

Maintenant que l'image est chargée, nous allons la personnaliser pour répondre aux besoins de l'entreprise EXPERTY.

2.5.1 Suppression des composants inutiles

1. Dans le menu de gauche, cliquez sur "Supprimer".



2. Parcourez la liste des composants et décochez ceux qui ne sont pas nécessaires pour l'entreprise. Par exemple :

- Applications de démonstration Windows
- Jeux Windows
- Certaines fonctionnalités multimédia non essentielles

2.5.2 Intégration des applications requises

Pour intégrer les applications demandées (OpenOffice, Adobe Reader, 7zip, Google Chrome version entreprise), suivez ces étapes pour chaque application :

1. Dans le menu de gauche, cliquez sur "Integration".
2. Cliquez sur "Add" et sélectionnez "Package".
3. Naviguez jusqu'au fichier d'installation de l'application et sélectionnez-le.
4. Configurez les options d'installation silencieuse pour chaque application.

2.5.3 Configuration de Google Chrome

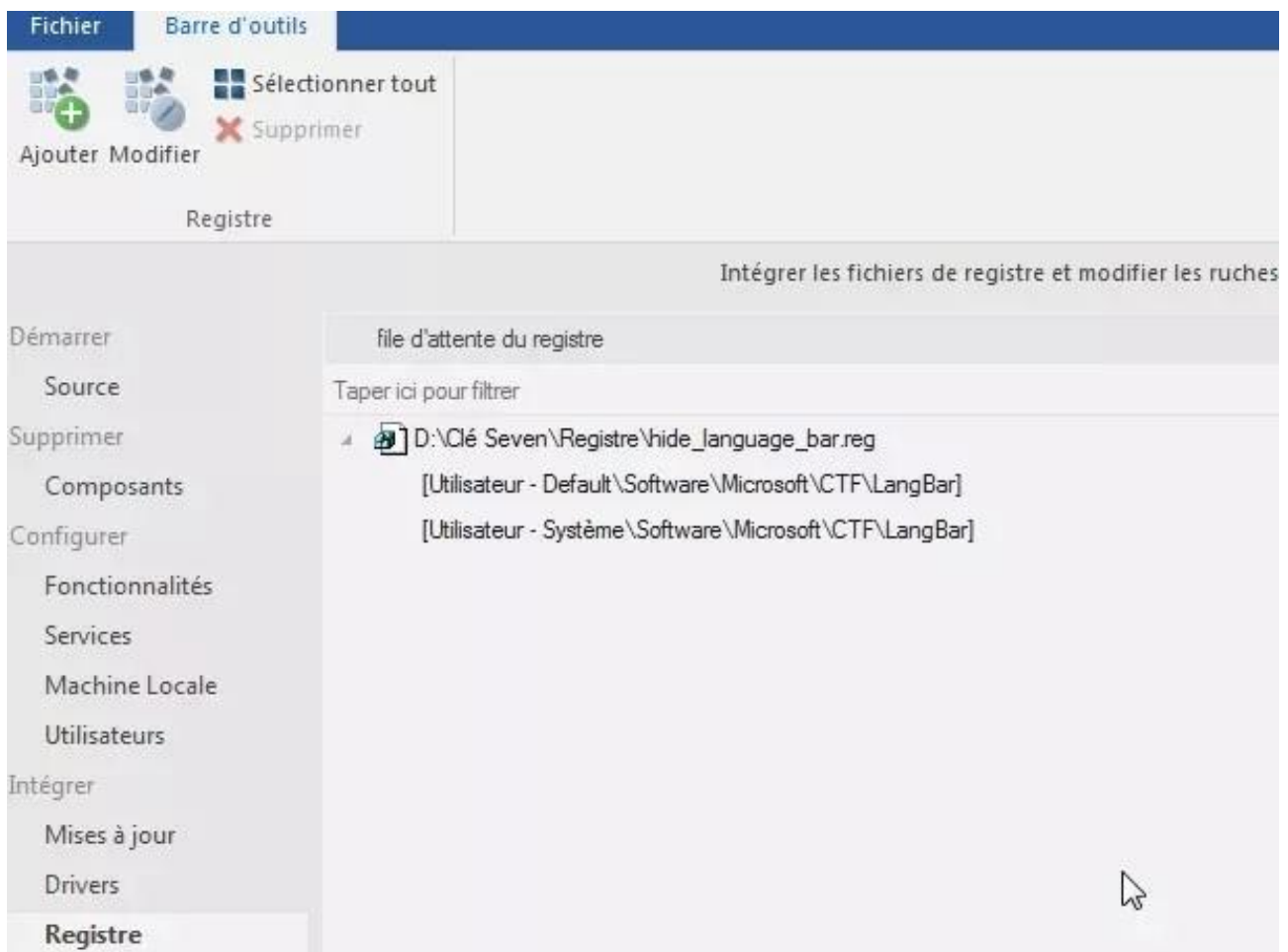
Pour configurer Google Chrome afin qu'il s'ouvre automatiquement à l'ouverture d'une session utilisateur et affiche la page `www.intranet.local` :

1. Dans la section "Registre", ajoutez une nouvelle clé :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

2. Créez une nouvelle valeur de chaîne nommée "Google Chrome" avec la valeur :

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" -  
start-maximized --homepage "http://www.intranet.local"
```



2.6 Application des paramètres de sécurité

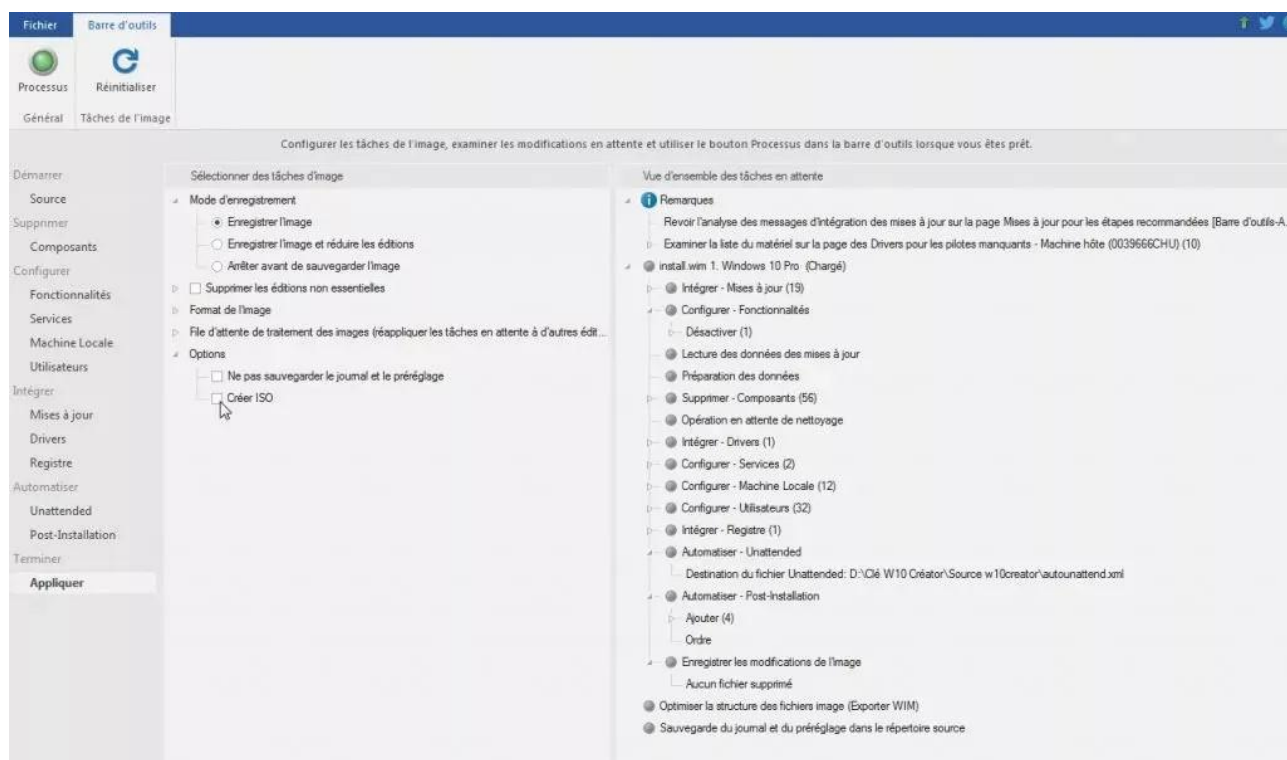
Dans cette section, nous allons appliquer les paramètres de sécurité recommandés par l'ANSSI et Microsoft. Nous détaillerons ces paramètres plus en profondeur dans la section 6 de ce document.

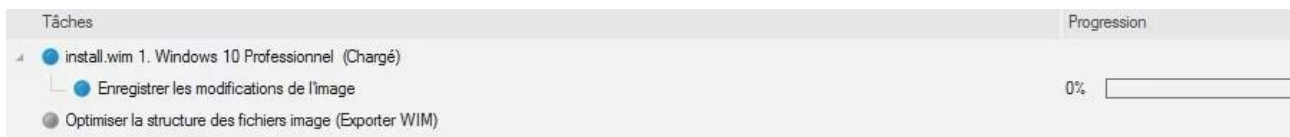
1. Dans le menu de gauche, cliquez sur "Registre".
2. Importez un fichier .reg contenant les paramètres de sécurité recommandés.
3. Vérifiez que tous les paramètres sont correctement appliqués.

2.7 Création de l'image finale

Une fois toutes les personnalisations effectuées, nous allons créer l'image finale :

1. Dans le menu de gauche, cliquez sur "Appliquer".
2. Sélectionnez "Créer ISO" comme type de sortie.
3. Choisissez un emplacement pour sauvegarder l'image ISO.



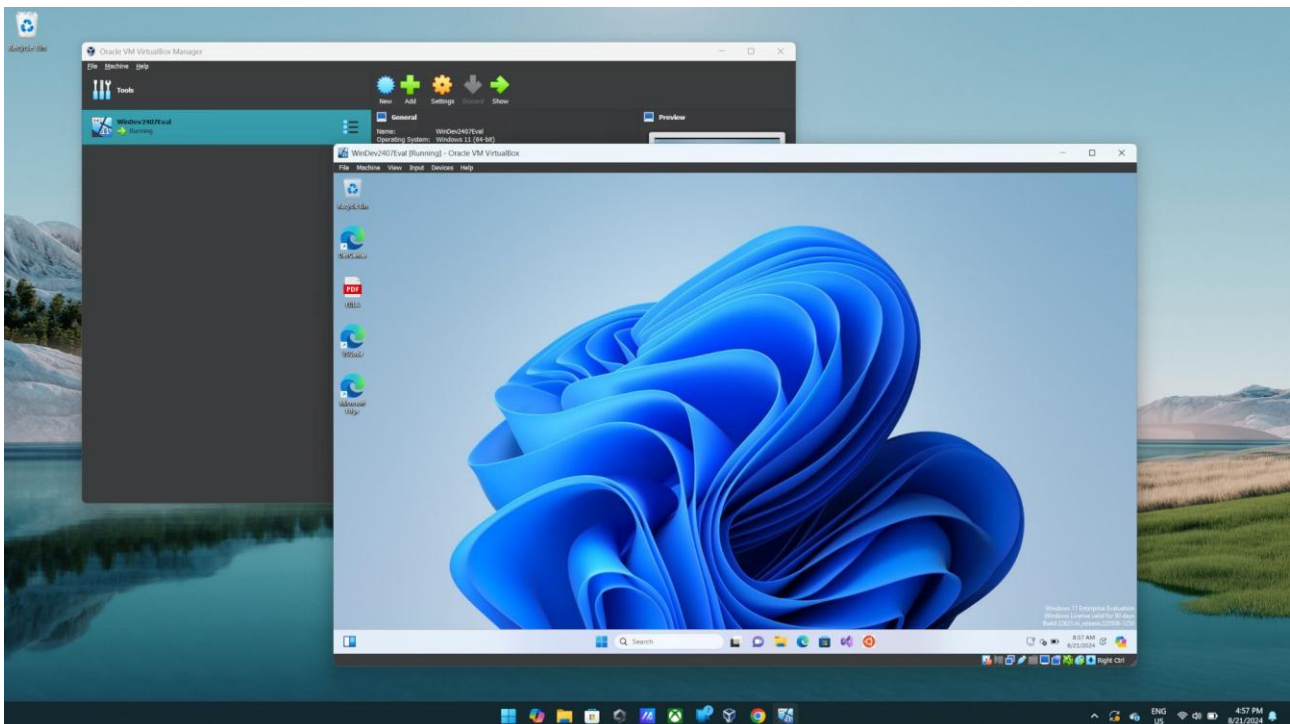


4. Cliquez sur "Processus" pour lancer la création de l'image.

2.8 Vérification de l'image

Une fois l'image créée, il est crucial de la tester dans un environnement virtuel pour s'assurer que toutes les personnalisations ont été correctement appliquées et que le système fonctionne comme prévu.

1. Utilisez un logiciel de virtualisation comme VirtualBox ou VMware pour créer une nouvelle machine virtuelle.
2. Installez l'image ISO créée sur cette machine virtuelle.
3. Vérifiez que toutes les applications sont présentes et fonctionnent correctement.
4. Assurez-vous que Google Chrome s'ouvre automatiquement au démarrage et affiche la page www.intranet.local.



5. Vérifiez que les paramètres de sécurité sont correctement appliqués.

Conclusion de la section

Dans cette section, nous avons détaillé le processus de création d'une image de déploiement personnalisée pour Windows 11 à l'aide de NTLITE. Cette image inclut toutes les applications requises, les configurations spécifiques demandées, et les paramètres de sécurité recommandés. Cette image servira de base pour les méthodes de déploiement que nous explorerons dans les sections suivantes.

III. Déploiement par clé USB de l'image NTLITE

3.1 Introduction au déploiement par clé USB

Le déploiement par clé USB est une méthode pratique et flexible pour installer une image Windows personnalisée sur des machines individuelles. Cette méthode est particulièrement utile lorsque l'accès au réseau est limité ou lorsqu'on travaille sur un petit nombre de machines à la fois.

3.2 Préparation de la clé USB

Pour créer une clé USB bootable avec notre image personnalisée, nous allons utiliser l'outil Rufus, qui est gratuit et facile à utiliser.

3.2.1 Téléchargement et installation de Rufus

1. Téléchargez Rufus depuis le site officiel : <https://rufus.ie/> ou le GitHub officiel : <https://github.com/pbatard/rufus>
2. L'application ne nécessite pas d'installation, il suffit de l'exécuter.

May 22

👤 pbatard

📁 v4.5

🔗 9551655

Compare

Rufus 4.5 Latest

- Add new advanced option to perform [runtime UEFI media validation](#) of suitable images (Windows, most Linux)
- Move the *Use Rufus MBR* advanced option to a cheat mode (`Alt-A`)
- Fix truncation of VHDX images, as well as a benign error message when writing VHD/VHDX ([#2468](#))
- Fix support for Linux persistence in some configurations (Mint, Ubuntu 24.04)
- Fix multiple potential vulnerabilities (with thanks to [Mansour Gashasbi](#))
- Update internal GRUB to version 2.12
- Update UEFI:NTFS to latest (now always uses the ntfs-3g driver, rather than the [buggy AMI NTFS one](#))
- Increase buffer size when copying ISO files, in an attempt to minimize the [AMI NTFS UEFI driver bug](#)
- Improve partition creation handling
- Don't display the WUE dialog when a conflicting `unattend.xml` already exists ([#2451](#))

▼ Assets 11

📄 rufus-4.5.exe	1.44 MB	May 22
📄 rufus-4.5.exe.sig	256 Bytes	May 22
📄 rufus-4.5p.exe	1.44 MB	May 22
📄 rufus-4.5_arm.exe	4.31 MB	May 22
📄 rufus-4.5_arm.exe.sig	256 Bytes	May 22
📄 rufus-4.5_arm64.exe	4.84 MB	May 22
📄 rufus-4.5_arm64.exe.sig	256 Bytes	May 22
📄 rufus-4.5_x86.exe	1.46 MB	May 22
📄 rufus-4.5_x86.exe.sig	256 Bytes	May 22
📄 Source code (zip)		May 22
📄 Source code (tar.gz)		May 22

👍 75
👎 9
🔥 26
❤️ 24
🔗 17
👁️ 10
104 people reacted

3.2.2 Création de la clé USB bootable

1. Insérez une clé USB d'au moins 8 Go dans votre ordinateur.
2. Lancez Rufus.
3. Dans Rufus, sélectionnez votre clé USB dans la liste des périphériques.
4. Sous "Type de démarrage", sélectionnez "Image ISO" et cliquez sur "Sélection" pour choisir l'image ISO créée avec NTLITE.
5. Laissez les autres options par défaut et cliquez sur "Démarrer".

Rufus 3.9.1624 (Portable)

Options de Périphérique

Périphérique
SAMSUNG (D:) [128 Go]

Type de démarrage
Image disque ou ISO (Veuillez sélectionner) ☒ SÉLECTION

Schéma de partition
MBR

Système de destination
BIOS (ou UEFI-CSM) ?

▼ Afficher les options de périphérique avancées

Options de Formatage

Nom de volume
SAMSUNG





Système de fichiers
Large FAT32 (Défaut)

Taille d'unité d'allocation
32 kilo-octets (Défaut)

▼ Afficher les options de formatage avancées

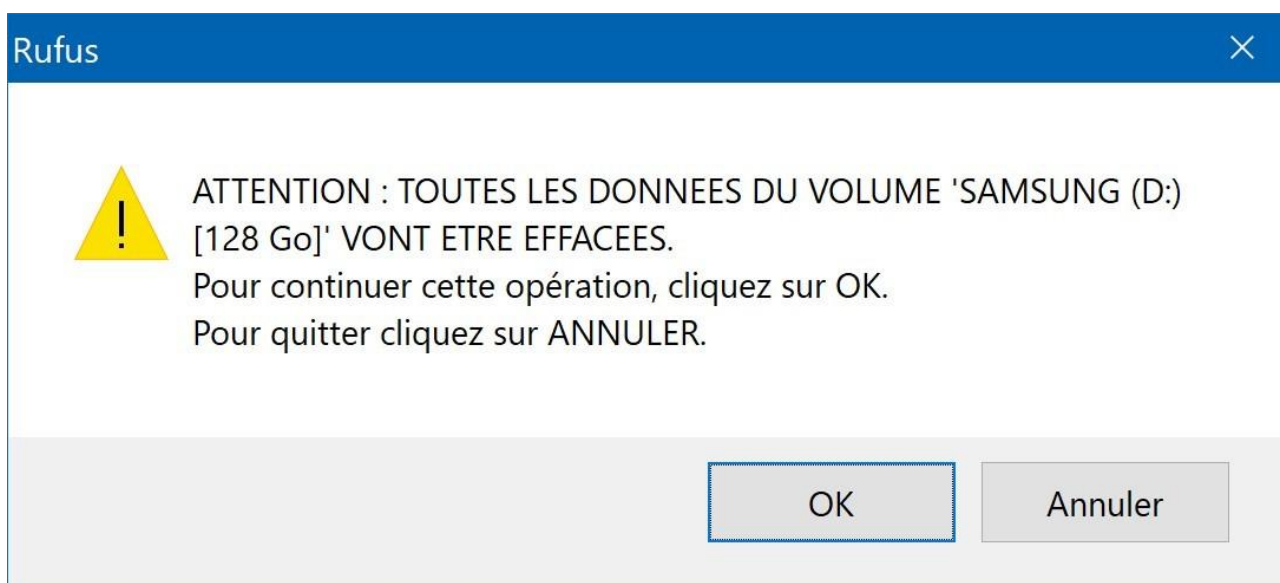
Statut

PRÊT

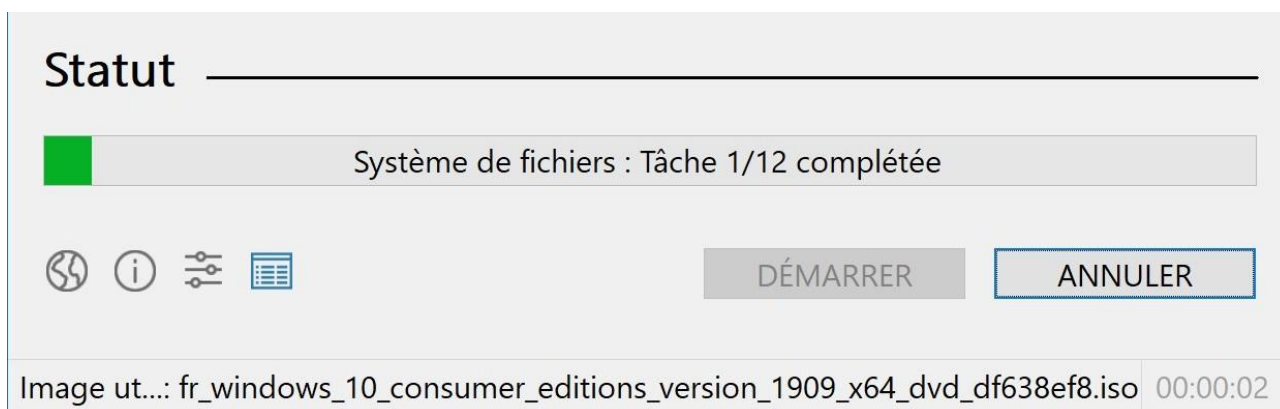





DÉMARRER FERMER

1 périphérique détecté



6. Confirmez que vous acceptez de formater la clé USB.



7. Attendez que le processus soit terminé. Cela peut prendre plusieurs minutes.

3.3 Procédure de déploiement

Une fois la clé USB préparée, suivez ces étapes pour déployer l'image sur chaque poste client :

3.3.1 Configuration du BIOS/UEFI

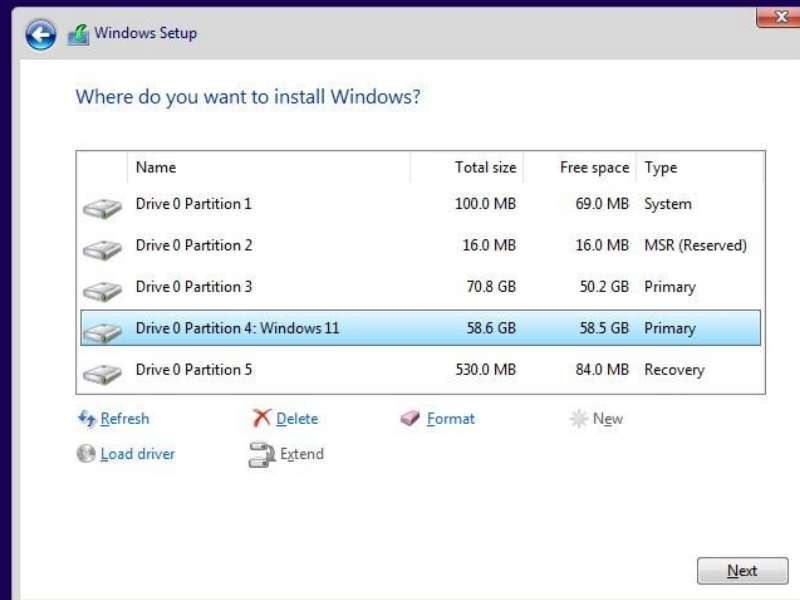
1. Démarrez ou redémarrez l'ordinateur cible.
2. Pendant le démarrage, appuyez sur la touche appropriée pour accéder au BIOS/UEFI (généralement F2, F12, ou Suppr).

3. Dans les paramètres de démarrage, modifiez l'ordre de boot pour placer le périphérique USB en premier.
4. Sauvegardez les changements et quittez le BIOS/UEFI.

PhoenixBIOS Setup Utility				
Main	Advanced	Security	Boot	Exit
CD-ROM Drive +Hard Drive +Removable Devices Network boot from Intel E1000				Item Specific Help Keys used to view or configure devices: <Enter> expands or collapses devices with a + or - <Ctrl+Enter> expands all <+> and <-> moves the device up or down. <n> May move removable device between Hard Disk or Removable Disk <d> Remove a device that is not installed.
F1	Help	↑↓	Select Item	-/+
Esc	Exit	↔	Select Menu	Enter
Change Values				F9
Select ► Sub-Menu				Setup Defaults
				F10
				Save and Exit

3.3.2 Installation de l'image

1. Insérez la clé USB préparée dans le port USB de l'ordinateur cible.
2. Redémarrez l'ordinateur. Il devrait démarrer à partir de la clé USB.
3. Suivez les instructions à l'écran pour lancer l'installation de Windows 11.
4. Lorsque vous y êtes invité, sélectionnez la partition sur laquelle vous souhaitez installer Windows.



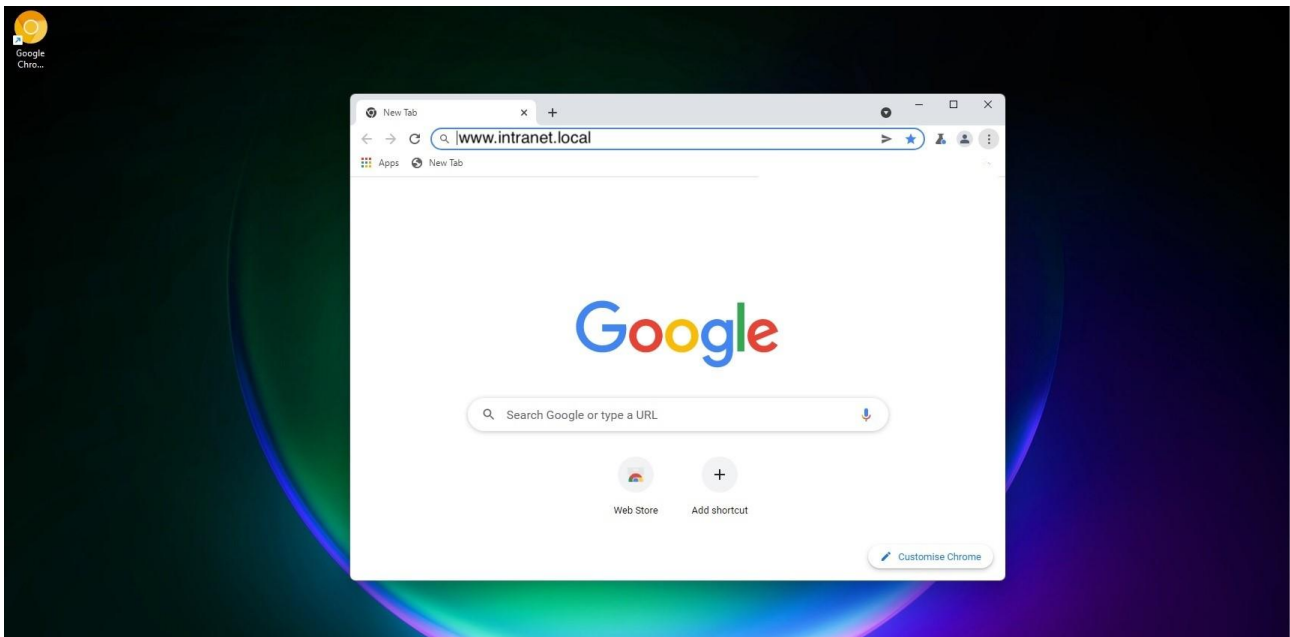
1 Collecting information 2 Installing Windows

5. L'installation se déroulera automatiquement, en appliquant toutes les personnalisations que nous avons configurées dans l'image NTLITE.
6. Une fois l'installation terminée, l'ordinateur redémarrera automatiquement.

3.3.3 Configuration post-installation

Après le redémarrage, quelques étapes de configuration finale peuvent être nécessaires :

1. Connectez-vous avec un compte administrateur local.
2. Vérifiez que toutes les applications prévues sont installées et fonctionnent correctement.
3. Assurez-vous que Google Chrome s'ouvre automatiquement et affiche la page www.intranet.local.
4. Vérifiez que les paramètres de sécurité sont correctement appliqués (nous détaillerons cette vérification dans la section 6).



3.4 Avantages et inconvénients du déploiement par clé USB

Avantages :

- Méthode simple et directe
- Ne nécessite pas d'infrastructure réseau complexe
- Idéal pour les petits déploiements ou les mises à jour ponctuelles

Inconvénients :

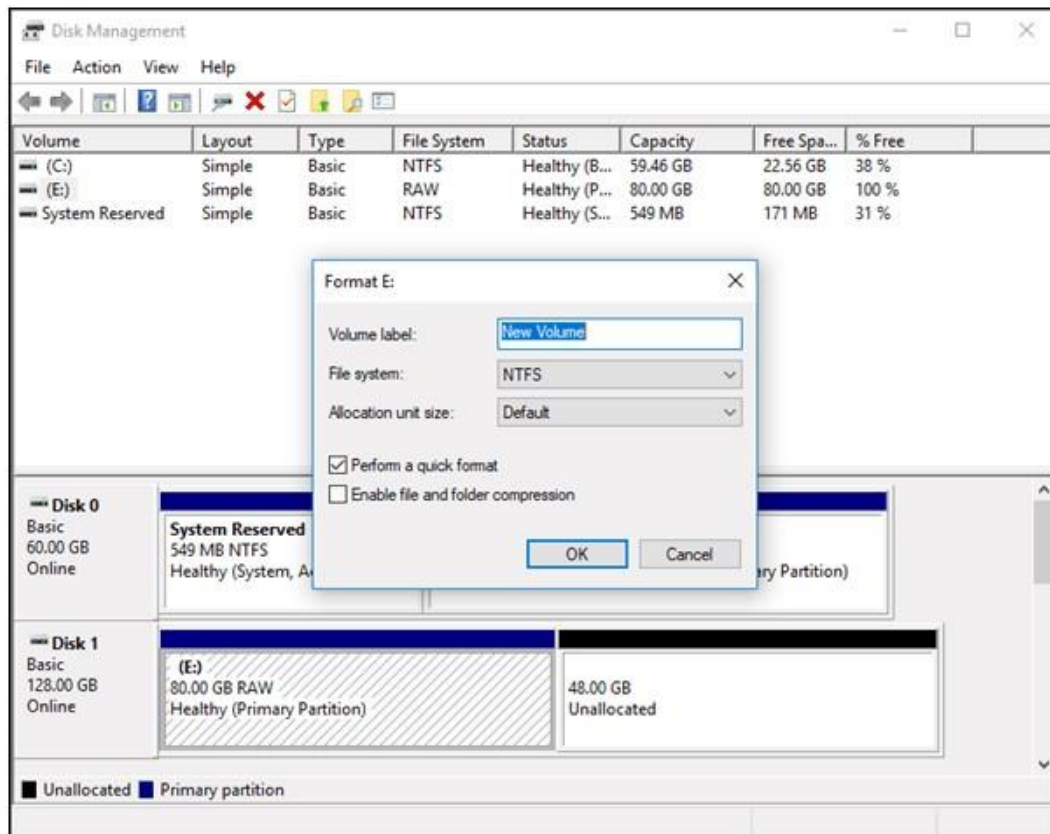
- Peut être chronophage pour un grand nombre de machines
- Nécessite une intervention manuelle sur chaque poste
- Risque d'erreurs humaines plus élevé que les méthodes automatisées

3.5 Considérations de sécurité

Lors de l'utilisation de clés USB pour le déploiement, il est important de prendre en compte certains aspects de sécurité :

1. Stockage sécurisé : Conservez les clés USB contenant l'image dans un endroit sécurisé lorsqu'elles ne sont pas utilisées.
2. Chiffrement : Envisagez de chiffrer le contenu de la clé USB pour protéger l'image en cas de perte ou de vol.

3. Destruction des données : Après le déploiement, effacez de manière sécurisée le contenu des clés USB si elles ne seront plus utilisées pour ce projet.



Conclusion de la section

Le déploiement par clé USB de l'image NTLITE offre une méthode flexible et directe pour installer Windows 11 sur les postes clients de l'entreprise EXPERTY. Bien que cette méthode puisse être chronophage pour un grand nombre de machines, elle reste une option viable, en particulier pour les petits déploiements ou les mises à jour ponctuelles. Dans la prochaine section, nous explorerons une méthode de déploiement plus automatisée utilisant le réseau.

IV. Déploiement par le réseau avec un serveur FOG

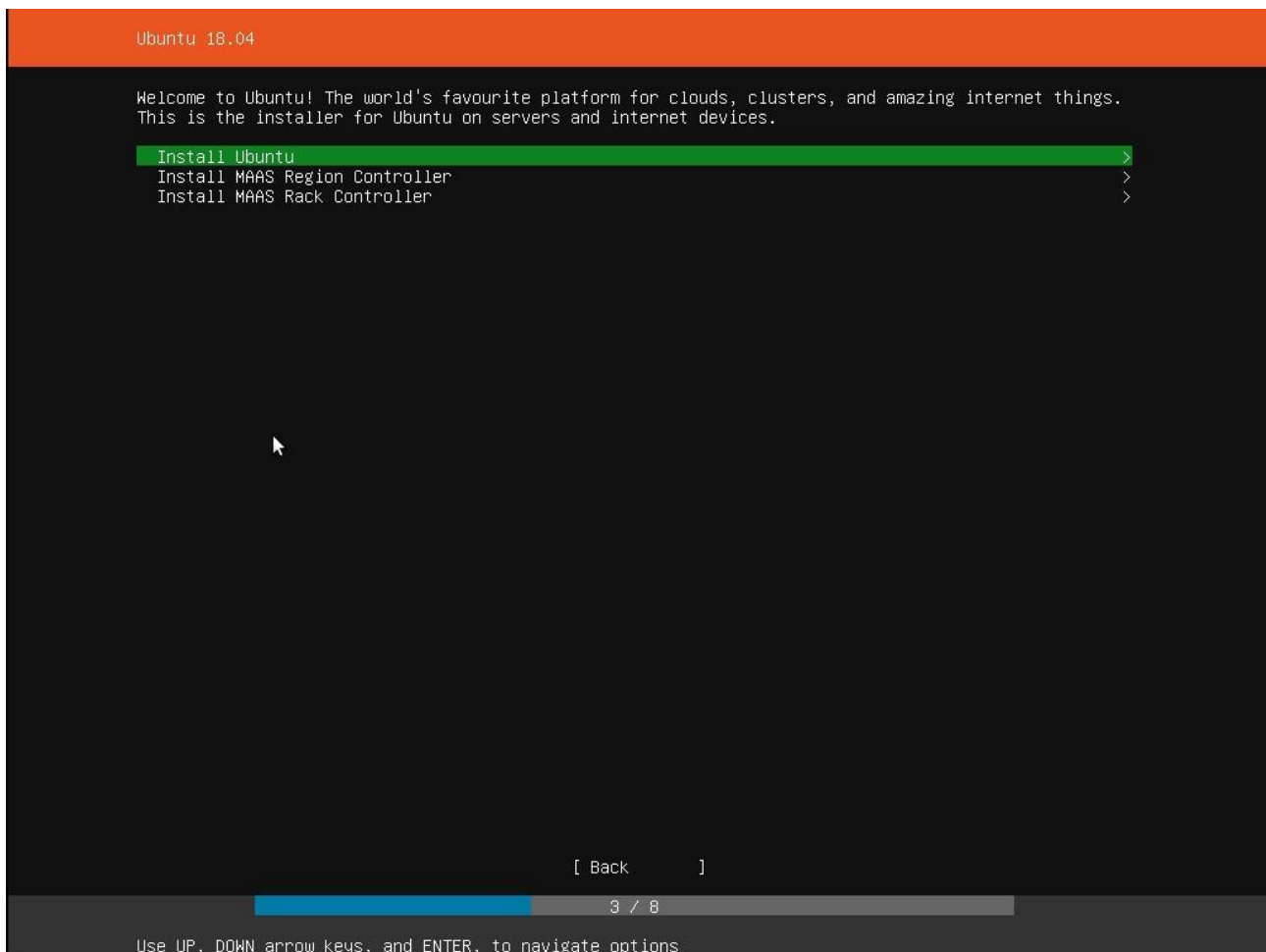
4.1 Introduction à FOG Project

FOG (Free Open-Source Ghost) est une solution de déploiement d'images système open-source basée sur Linux. Elle permet de déployer, gérer et dépanner des postes de travail et des serveurs sur un réseau. FOG offre une interface web conviviale pour gérer le processus de déploiement.

4.2 Installation du serveur FOG

4.2.1 Prérequis

- Un serveur dédié ou une machine virtuelle avec au moins 4 Go de RAM et 100 Go d'espace disque
- Une distribution Linux (nous utiliserons Ubuntu Server 22.04 LTS pour cet exemple)
- Une connexion réseau stable



4.2.2 Installation d'Ubuntu Server

1. Téléchargez l'image ISO d'Ubuntu Server 22.04 LTS depuis le site officiel d'Ubuntu.
2. Créez une clé USB bootable avec cette image.
3. Démarrez le serveur sur la clé USB et suivez les instructions d'installation d'Ubuntu Server.

4.2.3 Installation de FOG

Une fois Ubuntu Server installé et configuré, suivez ces étapes pour installer FOG :

1. Mettez à jour le système : `sudo apt update && sudo apt upgrade -y`

2. Téléchargez FOG :

```
wget  
https://github.com/FOGProject/fogproject/archive/devbranch.  
tar.gz
```

3. Extrayez l'archive :

```
tar -xzf dev-branch.tar.gz
```

4. Accédez au dossier d'installation :

```
cd fogproject-dev-branch/bin
```

5. Lancez le script d'installation :

```
sudo ./installfog.sh
```



```
root@root:~# tar -xzf dev-branch.tar.gz
root@root:~# cd fogproject-dev-branch/bin
root@root:~/fogproject-dev-branch/bin# sudo ./installfog.sh
Installing LSB_Release as needed
* Attempting to get release information.....Done
```

```
+-----+
| ..#####:.. ..,#,.. .:##:.. |
|.:##### .:;####:.....;#;.. |
|...##... ..##;;##:.....##... |
| ,# ..##.....##:## ..: |
| ## .:###,##. . ##.:#.:#####:.. |
|...##:##:##:.....#. .. .#...#. #...#::: |
|..:#####:.. ..##.....##:## .. # |
| # . ...##:,##;:::#: ... ##.. |
| .# . .:;####;:::..##:~;#:... |
| # ..:;###.. |
|+-----+
| Free Computer Imaging Solution |
|+-----+
| Credits: http://fogproject.org/Credits |
| http://fogproject.org/Credits |
| Released under GPL Version 3 |
|+-----+
```

Version: 1.5.10.1598 Installer/Updater

What version of Linux would you like to run the installation for?

- 1) Redhat Based Linux (Redhat, Alma, Rocky, CentOS, Mageia)
- 2) Debian Based Linux (Debian, Ubuntu, Kubuntu, Edubuntu)
- 3) Arch Linux

Choice: [2] █

6. Suivez les instructions à l'écran pour configurer FOG. Acceptez les valeurs par défaut sauf si vous avez des besoins spécifiques.

```
#####
#   FOG now has everything it needs for this setup, but please   #
#   understand that this script will overwrite any setting you may #
#   have setup for services like DHCP, apache, pxe, tftp, and NFS. #
#####
# It is not recommended that you install this on a production system #
#   as this script modifies many of your system settings.         #
#####
#   This script should be run by the root user.                   #
#   It will prepend the running with sudo if root is not set      #
#####
#   Please see our wiki for more information at:                   #
#####
#   https://wiki.fogproject.org/wiki/index.php                     #
#####
```

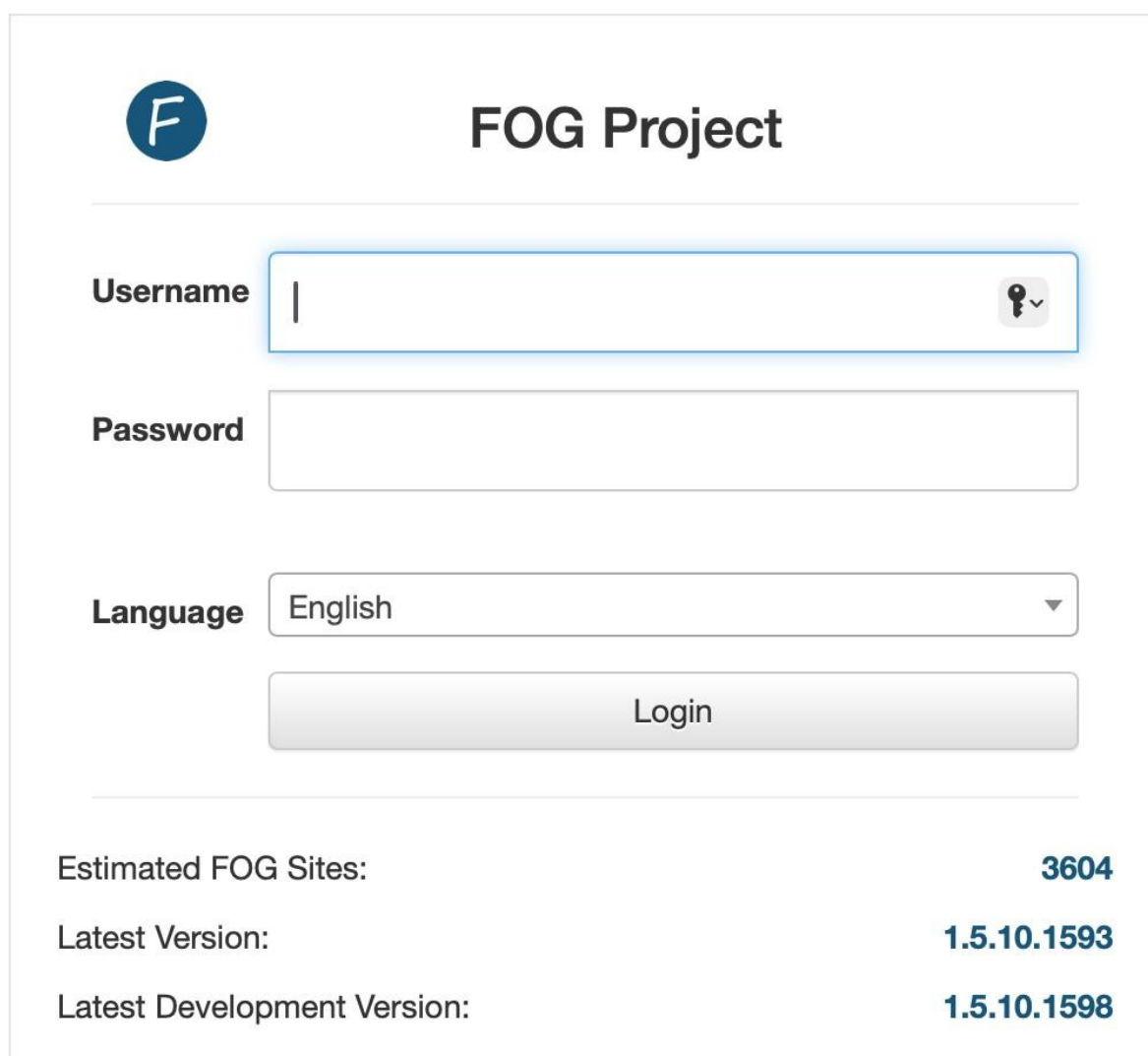
- * Here are the settings FOG will use:
- * Base Linux: Debian
- * Detected Linux Distribution: Ubuntu
- * Interface: ens160
- * Server IP Address: 192.168.188.133
- * Server Subnet Mask: 255.255.255.0
- * Hostname: root
- * Installation Type: Normal Server
- * Internationalization: No
- * Image Storage Location: /images
- * Using FOG DHCP: No
- * DHCP will NOT be setup but you must setup your
| current DHCP server to use FOG for PXE services.
- * On a Linux DHCP server you must set: next-server and filename
- * On a Windows DHCP server you must set options 066 and 067
- * Option 066/next-server is the IP of the FOG Server: (e.g. 192.168.188.133)
- * Option 067/filename is the bootfile: (e.g. undionly.kkpxe or snponly.efi)
- * Send OS Name, OS Version, and FOG Version: Yes
- * Are you sure you wish to continue (Y/N) ☐

4.3 Configuration du serveur FOG

4.3.1 Accès à l'interface web

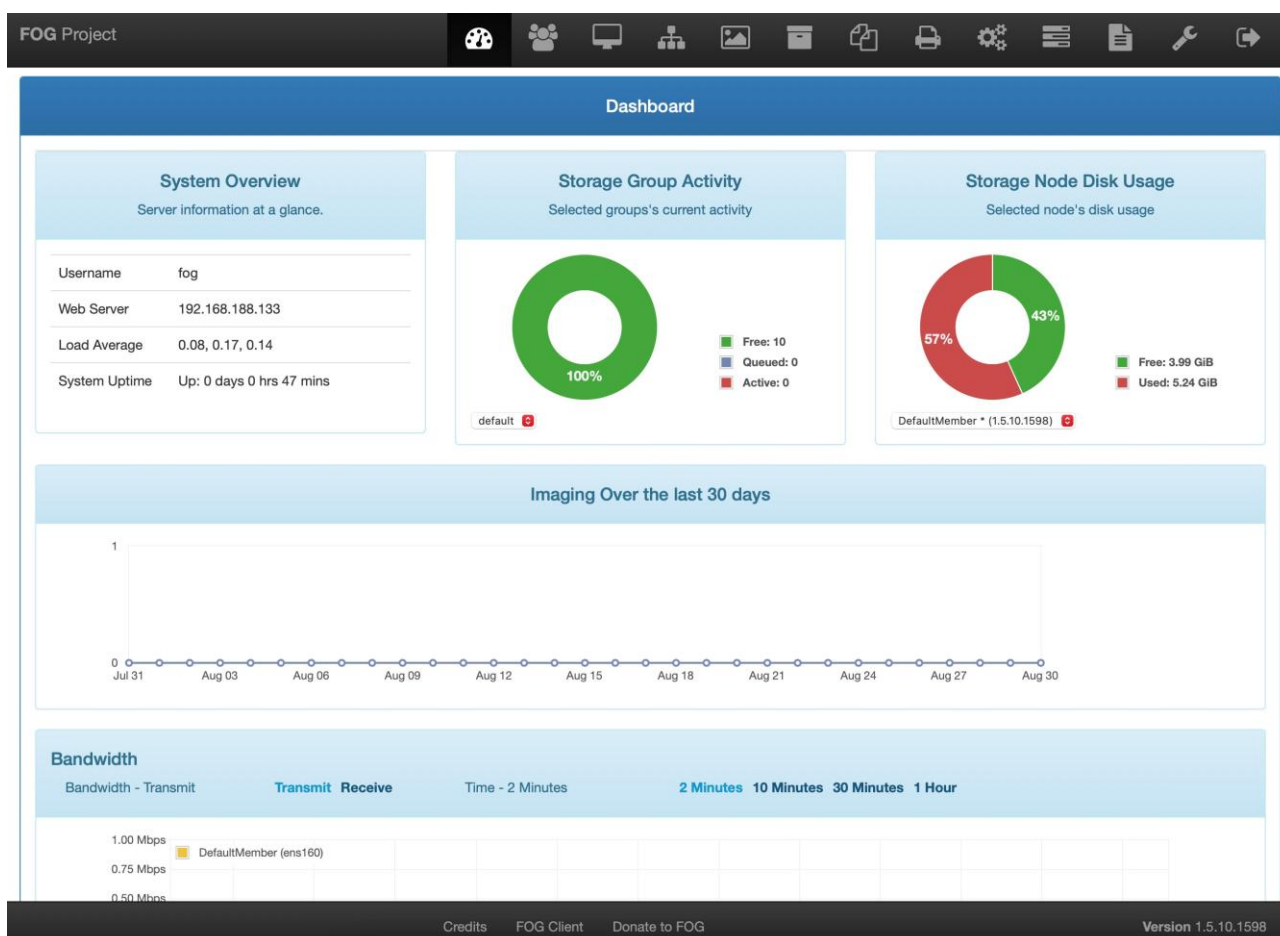
Une fois l'installation terminée, accédez à l'interface web de FOG :

1. Ouvrez un navigateur sur un autre ordinateur du réseau.
2. Entrez l'adresse IP du serveur FOG suivi de "/fog/management". Exemple : `http://192.168.188.133/fog/management`
3. Connectez-vous avec les identifiants par défaut (généralement "fog" pour l'utilisateur et "password" pour le mot de passe).



The screenshot shows the FOG Project web interface. At the top left is a blue circular logo with a white 'F'. To its right is the text 'FOG Project'. Below this is a login form with three fields: 'Username' (with a key icon and a dropdown arrow), 'Password', and 'Language' (with a dropdown menu showing 'English'). A 'Login' button is positioned below the 'Language' field. At the bottom of the page, there is a status section with three rows: 'Estimated FOG Sites: 3604', 'Latest Version: 1.5.10.1593', and 'Latest Development Version: 1.5.10.1598'.

Estimated FOG Sites:	3604
Latest Version:	1.5.10.1593
Latest Development Version:	1.5.10.1598



4.3.2 Configuration initiale

1. Changez immédiatement le mot de passe par défaut dans "User Management".
2. Configurez les paramètres réseau dans "FOG Configuration" pour correspondre à votre environnement.

4.4 Création et upload de l'image

4.4.1 Préparation de l'image de référence

1. Utilisez un ordinateur de référence avec l'image Windows 11 personnalisée que nous avons créée avec NTLITE.
2. Assurez-vous que toutes les applications et configurations sont correctes.

4.4.2 Création de l'image dans FOG

1. Dans l'interface web FOG, allez dans "Images" > "Create New Image".
2. Donnez un nom à l'image (par exemple, "Win11_EXPERTY").
3. Choisissez le type d'image "Single Disk - Resizable".

The screenshot displays the FOG Project web interface. At the top, there's a navigation bar with 'FOG Project' and a search bar. Below this is a 'Main Menu' sidebar with links: 'List All Images', 'Create New Image', 'Export Images', 'Import Images', and 'Multicast Image'. The main content area is titled 'Image Management' and contains a 'New Image' form. The form fields are as follows:

- Image Name:** A text input field.
- Image Description:** A text area.
- Storage Group:** A dropdown menu showing 'default - (1)'.
- Operating System:** A dropdown menu showing 'Windows 10 - (9)'.
- Image Path:** A text input field with a default value of '/images/'.
- Image Type:** A dropdown menu showing 'Single Disk - Resizable - (1)'.
- Partition:** A dropdown menu showing 'Everything - (1)'.
- Image Enabled:** A checkbox that is checked.
- Replicate?:** A checkbox that is checked.
- Compression:** A slider bar with a value of 6.
- Image Manager:** A dropdown menu showing 'Partclone Zstd'.
- Create Image:** A blue button labeled 'Add'.

At the bottom of the interface, there's a footer bar with links for 'Credits', 'FOG Client', and 'Donate to FOG', along with the version number 'Version 1.5.10.1598'.


4.4.3 Upload de l'image


1. Redémarrez l'ordinateur de référence et démarrez-le en mode PXE.
2. Sélectionnez "Quick Image" dans le menu FOG.
3. Choisissez l'image que vous venez de créer.
4. Laissez FOG capturer l'image. Ce processus peut prendre un certain temps selon la taille de l'image.


```

Partclone
Partclone v0.2.89 http://partclone.org
Starting to clone device (/dev/sda2) to image (/tmp/pigz1)
note: Storage Location 192.168.210.201:/images/dev/, Image
ame o790
Reading Super Block
Calculating bitmap... Please wait... done!
File system: NTFS
Device size: 250.0 GB = 61023743 Blocks
Space in use: 25.6 GB = 6241066 Blocks
Free Space: 224.4 GB = 54782677 Blocks
Block size: 4096 Byte

Elapsed: 00:03:47 Remaining: 00:19:55 Rate: 1.08GB/min
Current Block: 1060901 Total Block: 61023743

Data Block Process:
 15.96%

Total Block Process:
 1.74%

```

4.5 Déploiement de l'image

4.5.1 Enregistrement des postes clients

1. Dans l'interface web FOG, allez dans "Hosts" > "New Host".
2. Entrez les informations pour chaque poste client (nom, adresse MAC, etc.).

FOG Project Search...

Host Management

Main Menu

- List All Hosts
- Create New Host
- Export Hosts
- Import Hosts

New Host

Host Name

Primary MAC [Load MAC Vendors](#)

Host Description

Host Product Key

Host Image No items found

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 -

Active Directory

Credits FOG Client Donate to FOG Version 1.5.10.1598

4.5.2 Création d'une tâche de déploiement

1. Allez dans "Tasks" > "List All Hosts".
2. Sélectionnez le type de tâche "Deploy".
3. Choisissez l'image à déployer et les hôtes cibles.

FOG Project Search...

Task Management

Main Menu

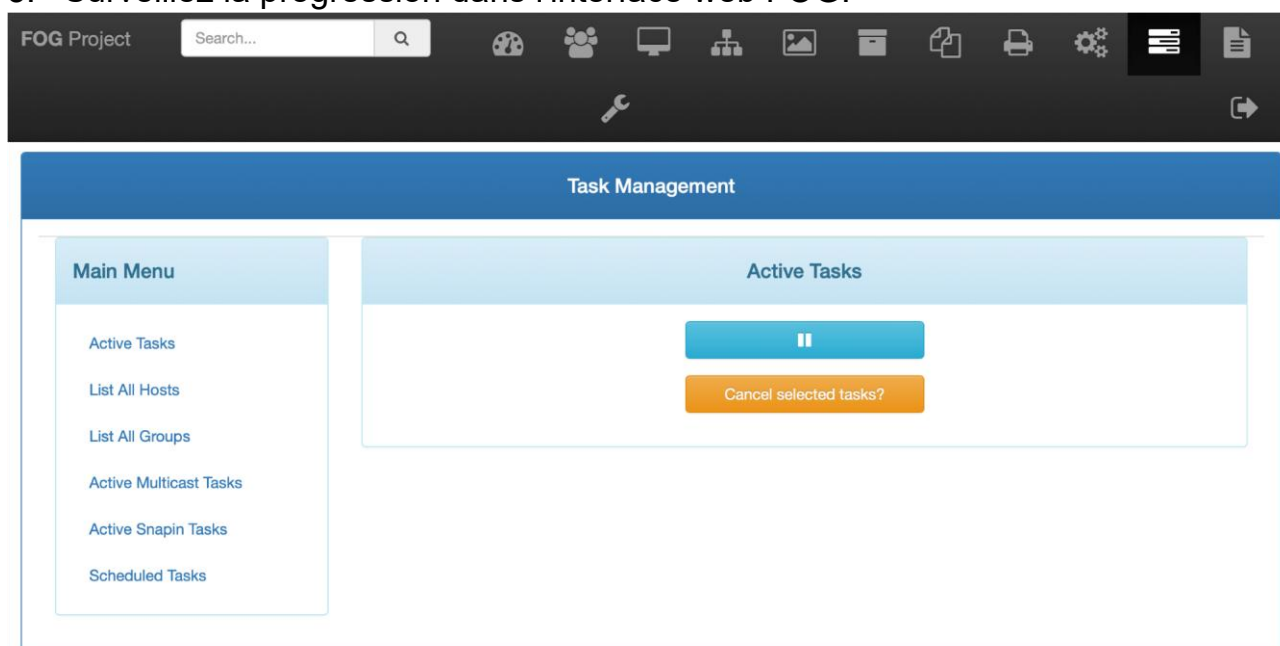
- Active Tasks
- List All Hosts
- List All Groups
- Active Multicast Tasks
- Active Snapin Tasks
- Scheduled Tasks

All Hosts

Host Name	Assigned Image	Tasking
Search...	Search...	
dsi 00:b0:d0:63:c2:26		

4.5.3 Lancement du déploiement

1. Démarrez les postes clients en mode PXE.
2. FOG détectera automatiquement les tâches en attente et commencera le déploiement.
3. Surveillez la progression dans l'interface web FOG.



4.6 Post-déploiement

4.6.1 Vérification

Après le déploiement, vérifiez sur chaque poste client :

1. Que toutes les applications sont correctement installées.
2. Que Google Chrome s'ouvre automatiquement sur www.intranet.local.
3. Que les paramètres de sécurité sont appliqués (détaillé dans la section 6).

4.6.2 Mise à jour de l'inventaire

Utilisez les fonctionnalités d'inventaire de FOG pour garder une trace de tous les postes déployés.

4.7 Avantages et inconvénients du déploiement avec FOG

Avantages :

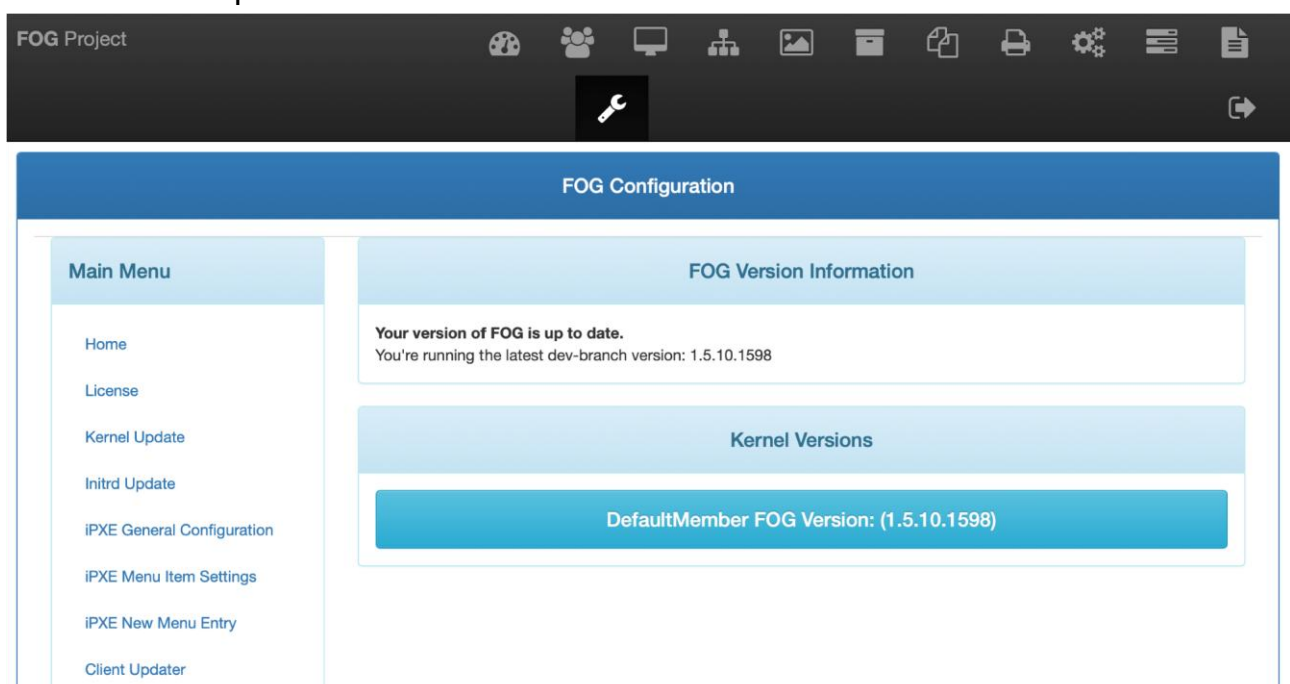
- Déploiement automatisé sur plusieurs machines simultanément
- Gestion centralisée des images et des déploiements
- Fonctionnalités additionnelles comme l'inventaire et la gestion des tâches

Inconvénients :

- Nécessite une configuration initiale plus complexe
- Dépend d'une infrastructure réseau robuste
- Peut nécessiter des ajustements pour les environnements de sécurité très stricts

4.8 Considérations de sécurité

1. Sécurisation du serveur FOG : Appliquez les meilleures pratiques de sécurité pour Ubuntu Server.
2. Chiffrement des communications : Configurez HTTPS pour l'interface web FOG.
3. Contrôle d'accès : Limitez l'accès au serveur FOG aux seuls administrateurs autorisés.
4. Surveillance : Mettez en place une surveillance des logs pour détecter toute activité suspecte.



Conclusion de la section

Le déploiement par le réseau avec FOG offre une solution puissante et flexible pour le déploiement à grande échelle de l'image Windows 11 personnalisée dans l'entreprise EXPERTY. Bien que sa mise en place initiale soit plus complexe que le déploiement par clé USB, FOG permet un déploiement plus rapide et plus efficace sur un grand nombre de machines, tout en offrant des fonctionnalités supplémentaires de gestion et d'inventaire.

V. Déploiement par le réseau avec un serveur WDS

5.1 Introduction à Windows Deployment Services (WDS)

Windows Deployment Services (WDS) est une technologie de Microsoft qui permet de déployer des systèmes d'exploitation Windows via le réseau. WDS utilise le protocole PXE (Preboot Execution Environment) pour démarrer les ordinateurs clients et déployer les images système.

5.2 Installation et configuration de WDS

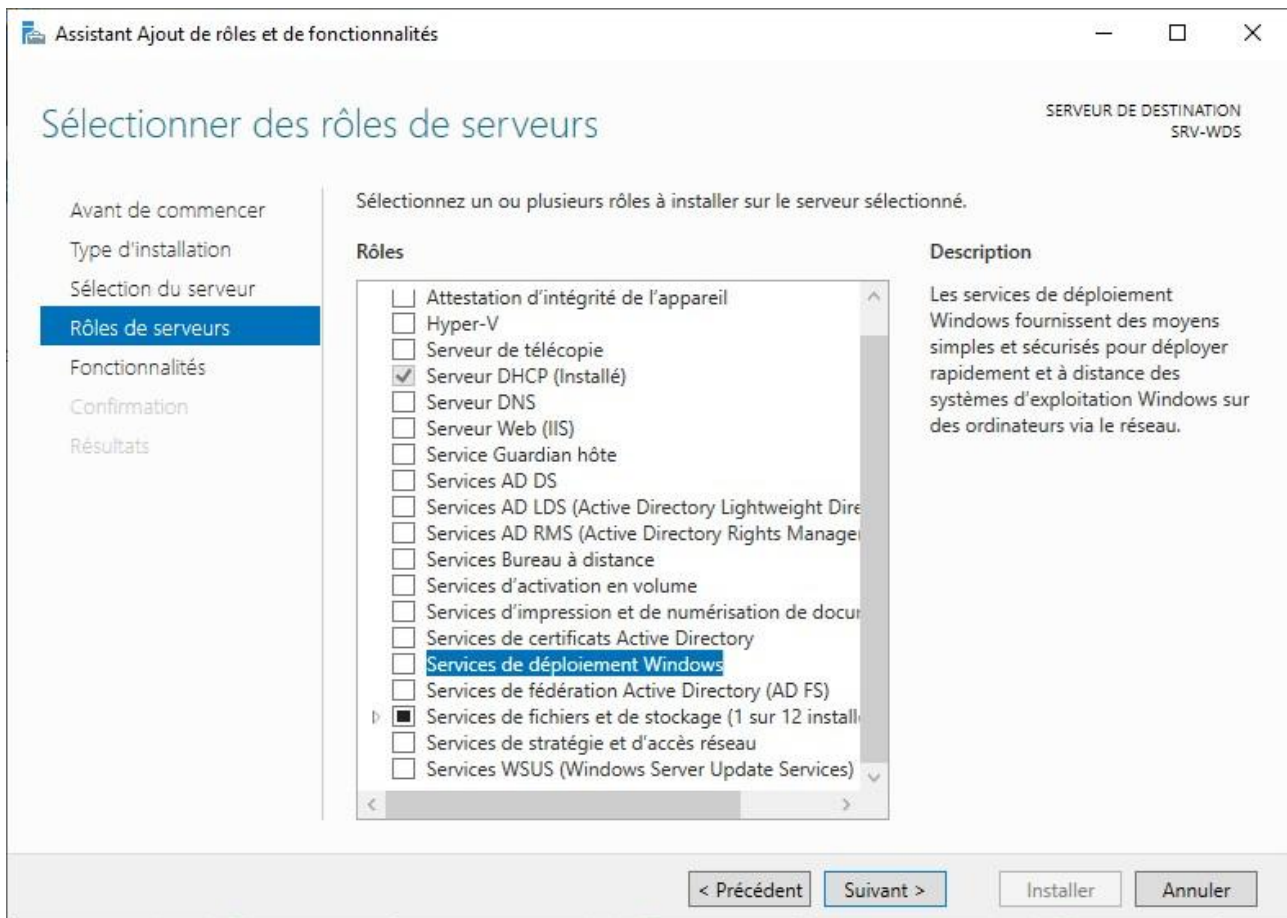
5.2.1 Prérequis

- Un serveur Windows Server (nous utiliserons Windows Server 2022 pour cet exemple)
- Un domaine Active Directory configuré
- Des droits d'administrateur sur le serveur et le domaine
- Une image Windows 11 personnalisée (créée avec NTLITE dans notre cas)

5.2.2 Installation du rôle WDS

1. Ouvrez le Gestionnaire de serveur sur votre serveur Windows.

2. Cliquez sur "Gérer" puis "Ajouter des rôles et fonctionnalités".
3. Suivez l'assistant jusqu'à la page "Rôles de serveurs".
4. Cochez la case "Services de déploiement Windows".
5. Ajoutez les fonctionnalités requises si demandé.
6. Terminez l'installation et redémarrez le serveur si nécessaire.



5.2.3 Configuration initiale de WDS

1. Ouvrez la console "Services de déploiement Windows" depuis les outils d'administration.
2. Cliquez droit sur le serveur et sélectionnez "Configurer le serveur".
3. Choisissez "Serveur intégré à Active Directory" et suivez l'assistant.
4. Spécifiez le chemin de stockage des images.
5. Configurez les options de réponse aux clients (PXE).

5.3 Préparation des images pour WDS

5.3.1 Conversion de l'image NTLITE en format WIM

1. Utilisez l'outil DISM (Deployment Image Servicing and Management) pour convertir l'image ISO en WIM :

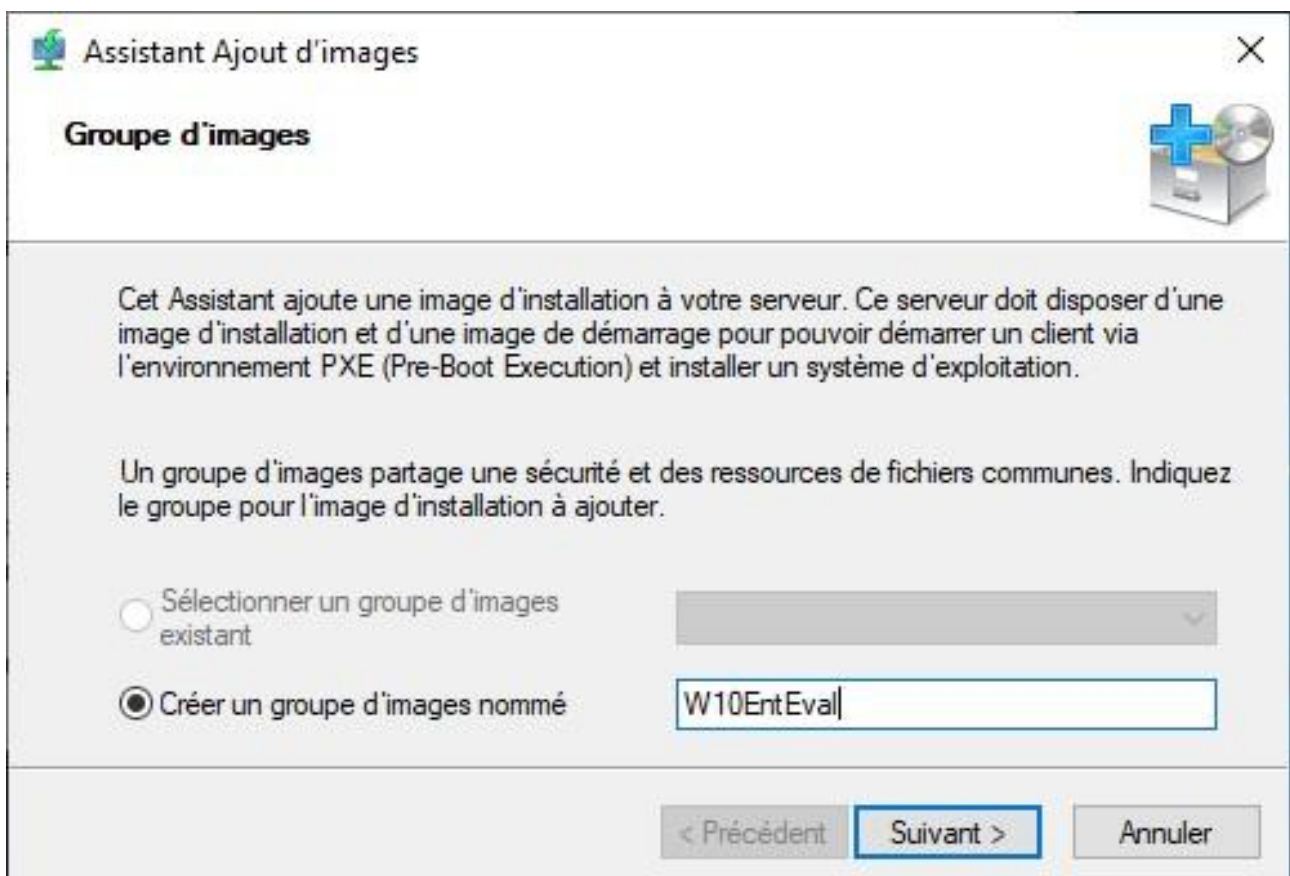
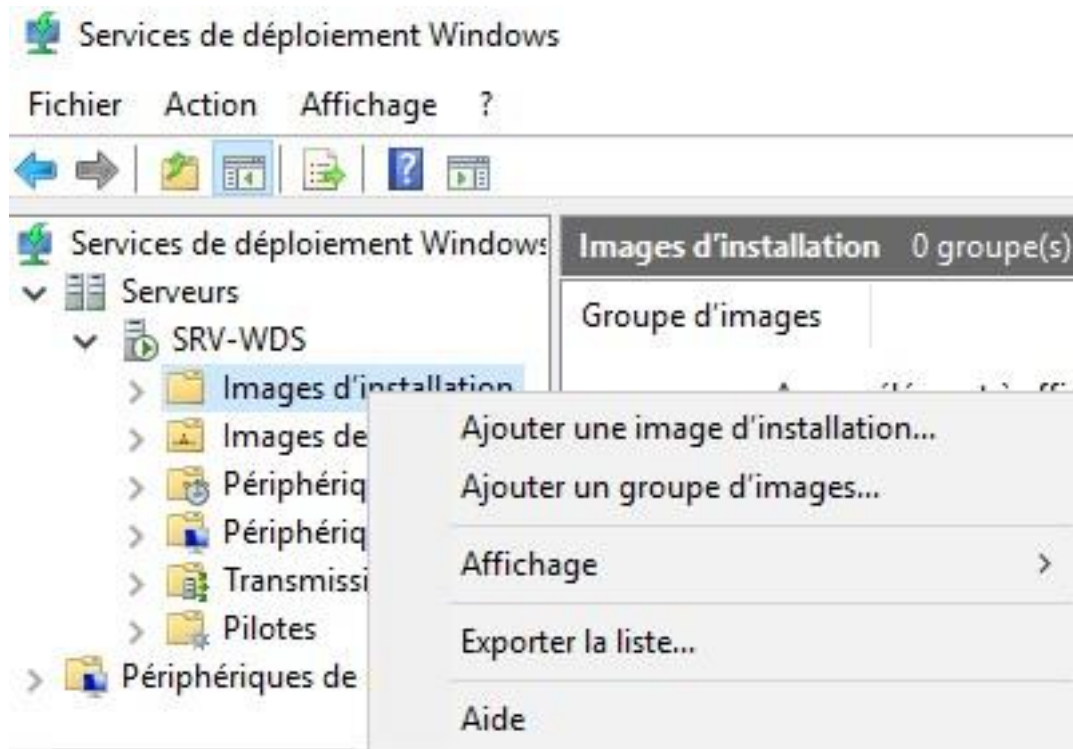
```
dism /Get-WimInfo /WimFile:C:\chemin\vers\image.iso
```


```
dism /Export-Image /SourceImageFile:C:\chemin\vers\image.iso /SourceIndex:1 /  
DestinationImageFile:C:\chemin\vers\image.wim /Compress:max  
/CheckIntegrity
```


```
Deployment Image Servicing and Management tool  
Version: 10.0.17134.1  
  
Exporting image  
[=====100.0%=====]  
The operation completed successfully.  
  
C:\temp>
```

5.3.2 Ajout de l'image à WDS

1. Dans la console WDS, cliquez droit sur "Images d'installation" et choisissez "Ajouter une image d'installation".
2. Créez un nouveau groupe d'images (par exemple, "Windows 11 EXPERTY").
3. Sélectionnez le fichier WIM créé précédemment.
4. Donnez un nom et une description à l'image.




Assistant Ajout d'images


Fichier image



Entrez l'emplacement du fichier image Windows contenant les images à ajouter.

Emplacement du fichier :

Remarque : les images d'installation et de démarrage par défaut (Boot.wim et Install.wim) sont présentes sur le DVD d'installation dans le dossier \Sources.

[Informations complémentaires sur les images et les types d'images](#)


Assistant Ajout d'images

Progression de la tâche


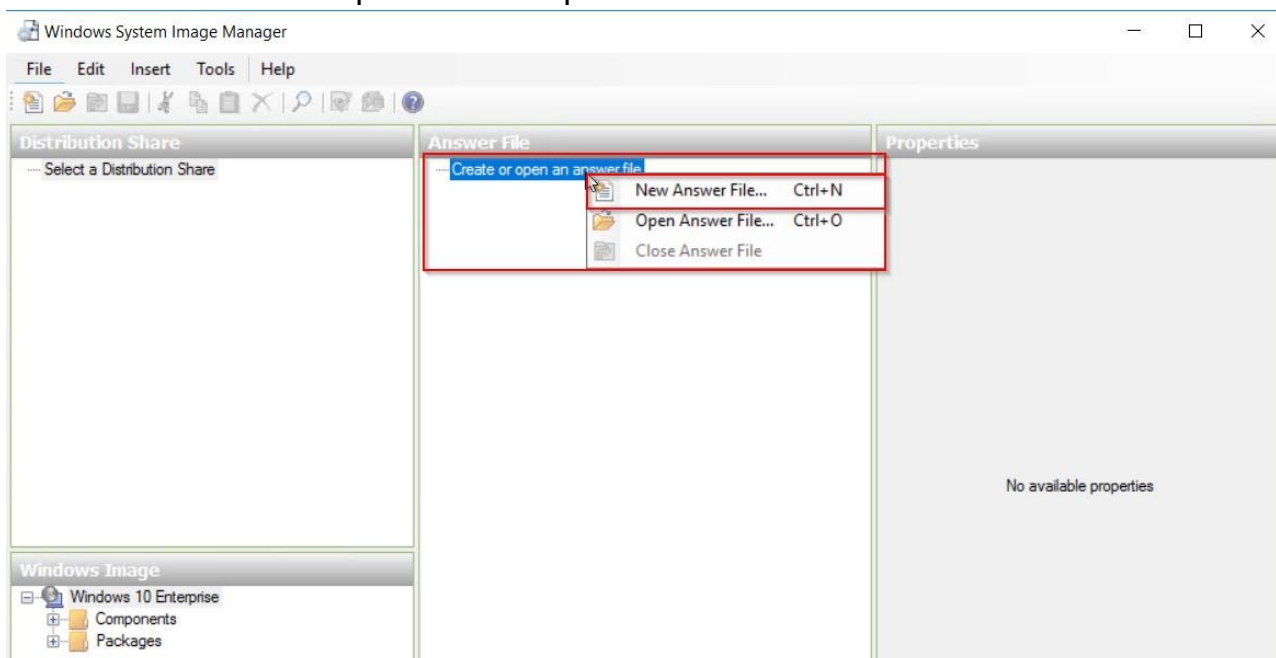
Ajout d'images Windows...

Ajout de l'image 1 de 1 (W10Ent20.04)

5.4 Configuration des options de déploiement

5.4.1 Création d'un fichier de réponse

1. Utilisez l'outil Windows System Image Manager (WSIM) pour créer un fichier de réponse (unattend.xml).
2. Configurez les paramètres tels que le nom de l'ordinateur, le fuseau horaire, et les paramètres réseau.
3. Incluez les clés de produit et les paramètres de domaine si nécessaire.



5.4.2 Association du fichier de réponse à l'image

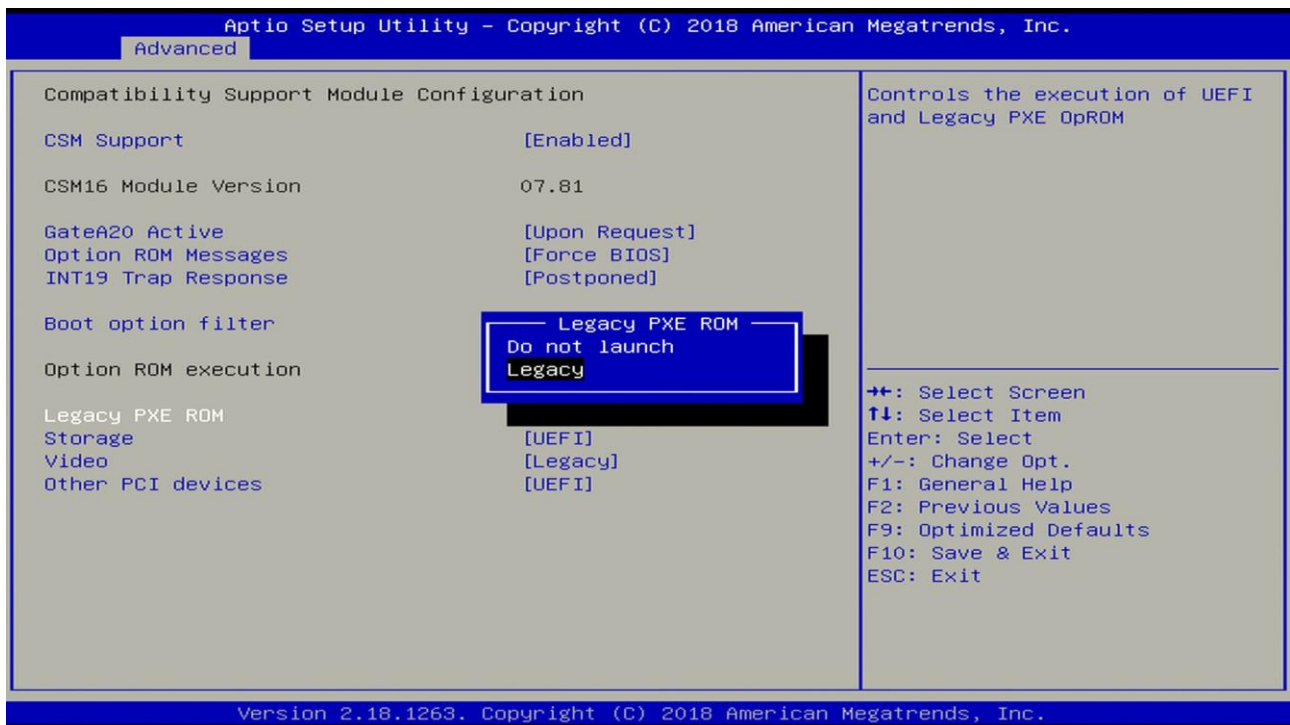
1. Dans la console WDS, cliquez droit sur l'image et choisissez "Propriétés".
2. Dans l'onglet "Général", associez le fichier de réponse créé.

5.5 Préparation des postes clients

5.5.1 Configuration du BIOS/UEFI

Sur chaque poste client :

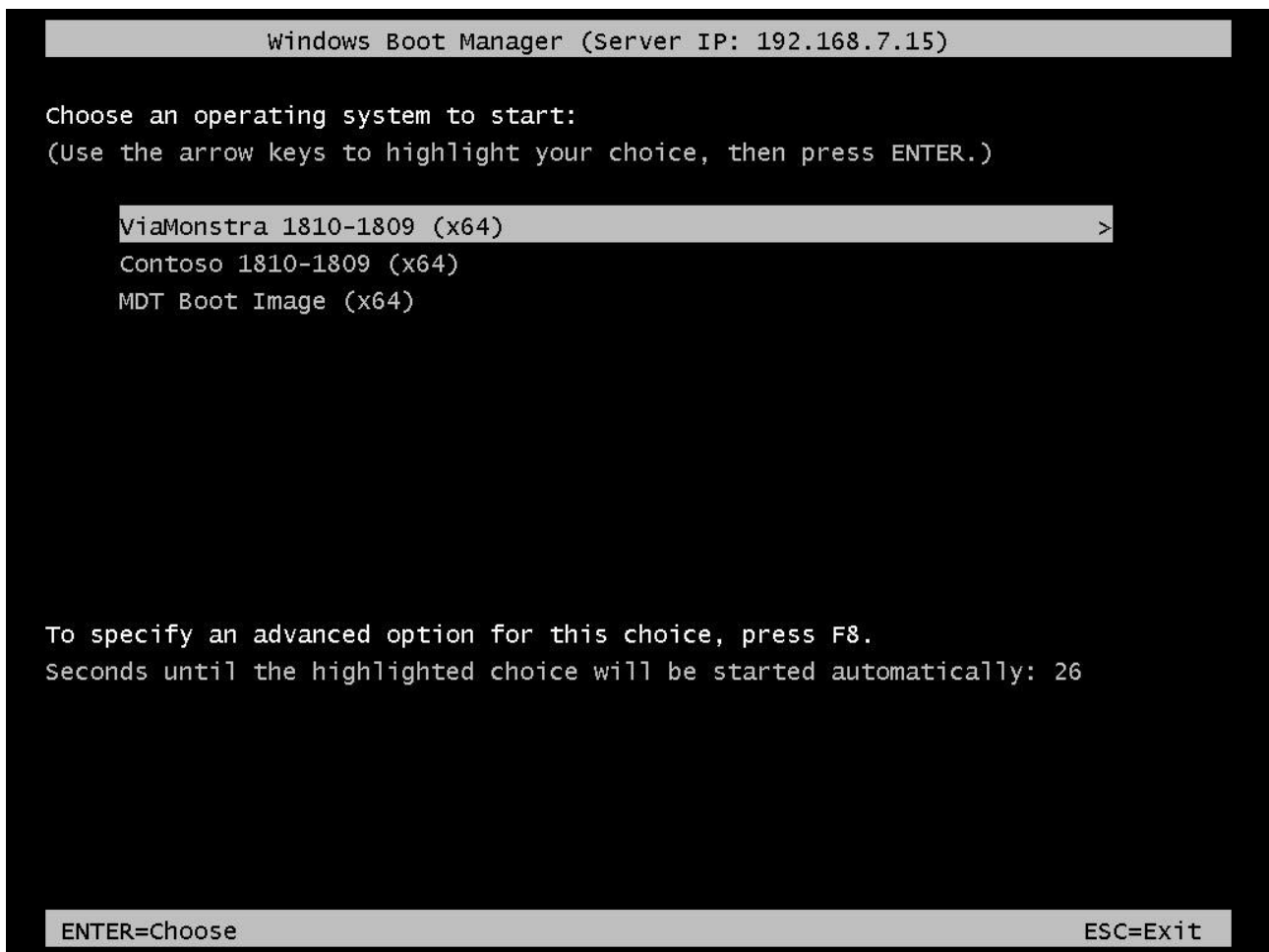
1. Accédez au BIOS/UEFI au démarrage.
2. Activez le démarrage PXE.
3. Placez le démarrage réseau en première position dans l'ordre de démarrage.



5.6 Processus de déploiement

5.6.1 Démarrage PXE et sélection de l'image

1. Démarrez le poste client. Il devrait se connecter au serveur WDS via PXE.
2. Sélectionnez l'image Windows 11 personnalisée dans le menu de démarrage.



5.6.2 Installation automatisée

1. L'installation de Windows 11 démarre automatiquement.
2. Le fichier de réponse applique les configurations prédéfinies.
3. Les applications incluses dans l'image sont installées.

5.6.3 Finalisation et vérification

1. Une fois l'installation terminée, vérifiez que toutes les applications sont présentes.
2. Assurez-vous que Google Chrome s'ouvre automatiquement sur www.intranet.local.
3. Vérifiez l'application des paramètres de sécurité (détaillé dans la section 6).

5.7 Gestion post-déploiement

5.7.1 Mise à jour de l'image

1. Mettez à jour l'image de référence avec NTLITE si nécessaire.
2. Reconvertissez l'image en WIM et remplacez-la dans WDS.

5.7.2 Surveillance et maintenance

1. Utilisez les journaux WDS pour surveiller les déploiements.
2. Nettoyez régulièrement les anciennes images non utilisées.

5.8 Avantages et inconvénients du déploiement avec WDS

Avantages :

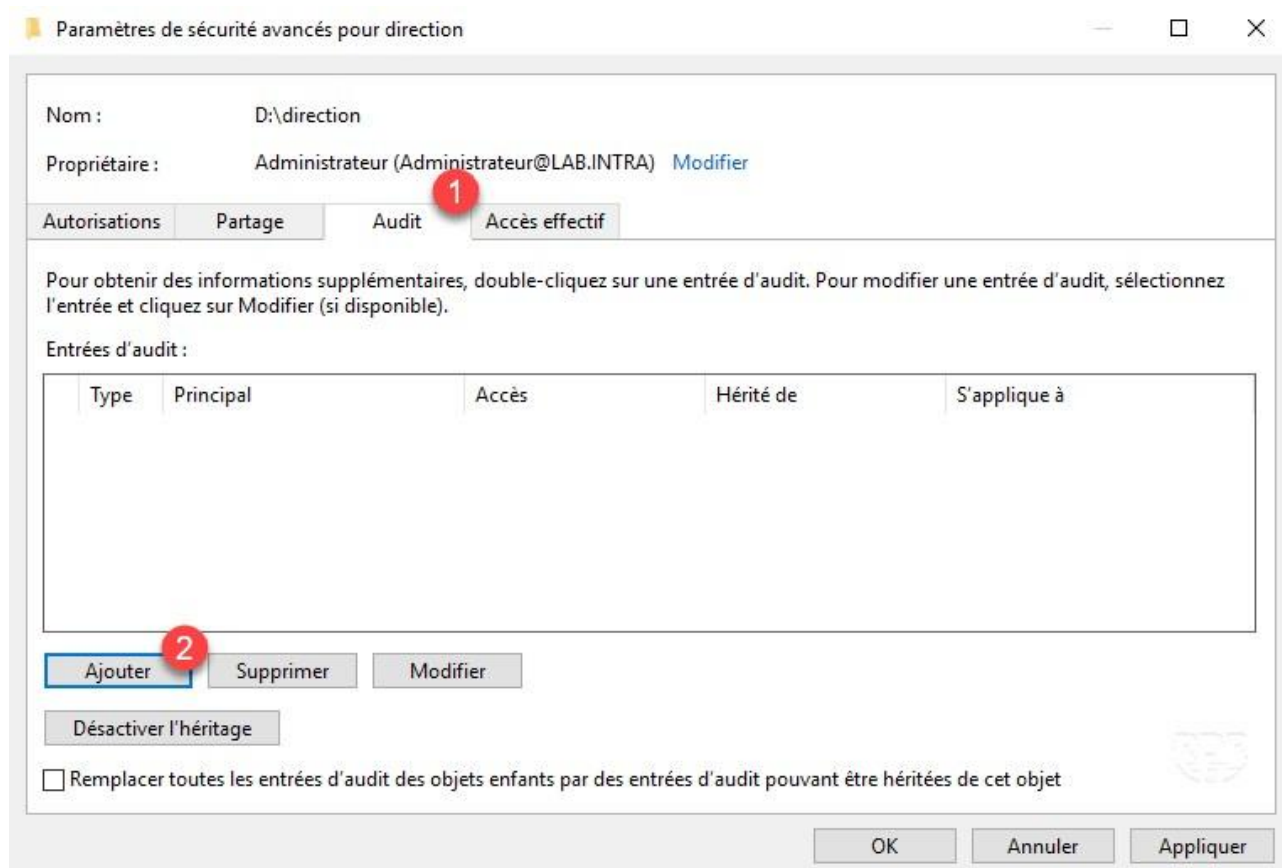
- Intégration native avec l'environnement Windows et Active Directory
- Déploiement simultané sur plusieurs machines
- Possibilité d'automatisation poussée avec les fichiers de réponse

Inconvénients :

- Nécessite une infrastructure Windows Server et Active Directory
- Peut être complexe à configurer initialement
- Moins flexible que certaines solutions tierces pour les environnements hétérogènes

5.9 Considérations de sécurité

1. Sécurisation du serveur WDS : Appliquez les dernières mises à jour et les meilleures pratiques de sécurité Windows Server.
2. Contrôle d'accès : Limitez l'accès au serveur WDS aux seuls administrateurs autorisés.
3. Chiffrement des transmissions : Configurez WDS pour utiliser le chiffrement lors des transmissions d'images.
4. Audits : Activez l'audit des accès et des actions sur le serveur WDS.



Conclusion de la section

Le déploiement par le réseau avec Windows Deployment Services offre une solution robuste et intégrée pour le déploiement à grande échelle de l'image Windows 11 personnalisée dans l'entreprise EXPERTY. Bien que sa configuration initiale puisse être complexe, WDS permet un déploiement efficace et automatisé, particulièrement adapté aux environnements Windows. Sa forte intégration avec Active Directory en fait un choix pertinent pour les entreprises déjà investies dans l'écosystème Microsoft.

VI. Configuration de sécurité selon les recommandations de l'ANSSI et Microsoft

6.1 Introduction à la sécurisation des postes clients

La sécurisation des postes clients est un aspect crucial du déploiement d'un parc informatique. Dans cette section, nous allons nous concentrer sur l'application des recommandations de sécurité de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et de Microsoft pour Windows 11.

6.2 Guides de référence

Pour cette configuration, nous nous baserons principalement sur les guides suivants :

1. Guide de l'ANSSI : "Recommandations de sécurité relatives à un système Windows 10" (applicable en grande partie à Windows 11)

Lien : <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-aun-systeme-windows-10/>

2. Guide de Microsoft : "Windows security baselines" pour Windows 11 Lien : <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines>

6.3 Configuration des paramètres de sécurité

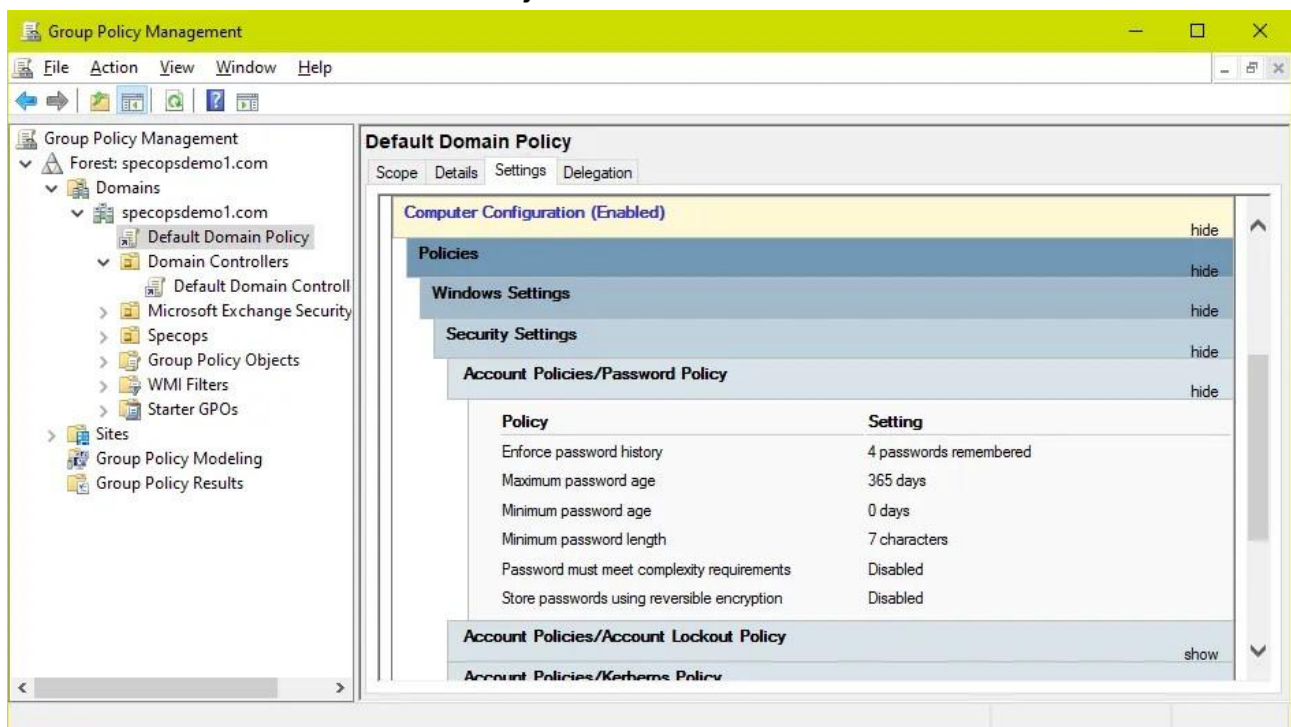
6.3.1 Gestion des comptes utilisateurs

1. Désactivation du compte Administrateur intégré : Net user administrateur /active:no

Justification : Le compte Administrateur intégré est une cible privilégiée pour les attaquants car son nom est connu. Sa désactivation réduit la surface d'attaque.

2. Renforcement de la politique de mot de passe :

- Longueur minimale : 14 caractères
- Complexité : activée (majuscules, minuscules, chiffres, caractères spéciaux) -
- Durée de validité maximale : 90 jours

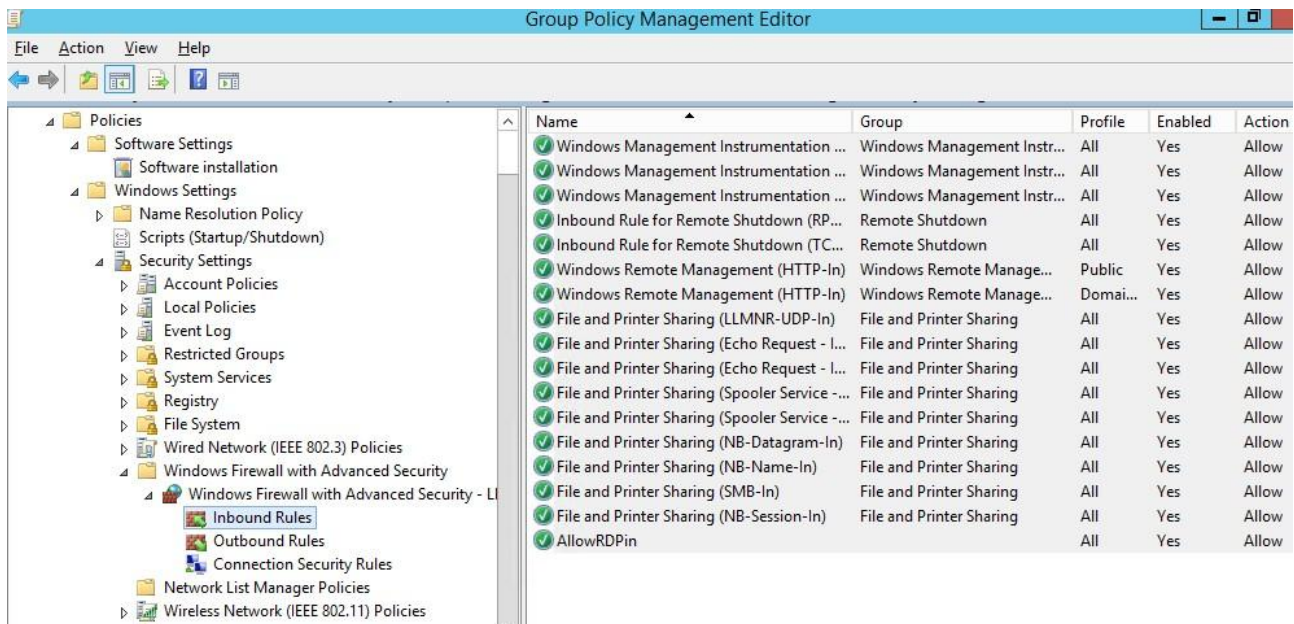


6.3.2 Restriction des droits d'administration

1. Création d'un groupe "Administrateurs locaux restreints"
2. Attribution des droits minimaux nécessaires à ce groupe

6.3.3 Configuration du pare-feu Windows

1. Activation du pare-feu sur tous les profils (Domaine, Privé, Public)
2. Blocage du trafic entrant par défaut
3. Autorisation du trafic sortant par défaut

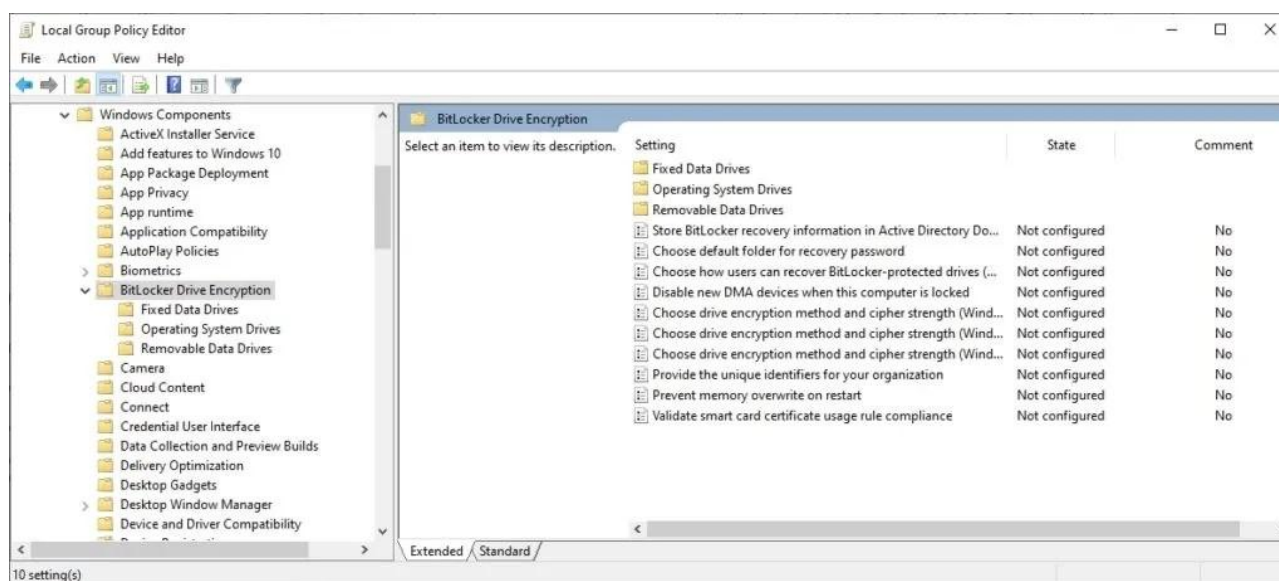


6.3.4 Mise à jour automatique

1. Activation des mises à jour automatiques
2. Configuration pour télécharger et installer automatiquement les mises à jour

6.3.5 BitLocker

1. Activation du chiffrement BitLocker sur tous les disques
2. Utilisation d'un PIN au démarrage pour les ordinateurs équipés d'une puce TPM



6.3.6 Désactivation des services inutiles

Selon les recommandations de l'ANSSI, désactivez les services suivants : -

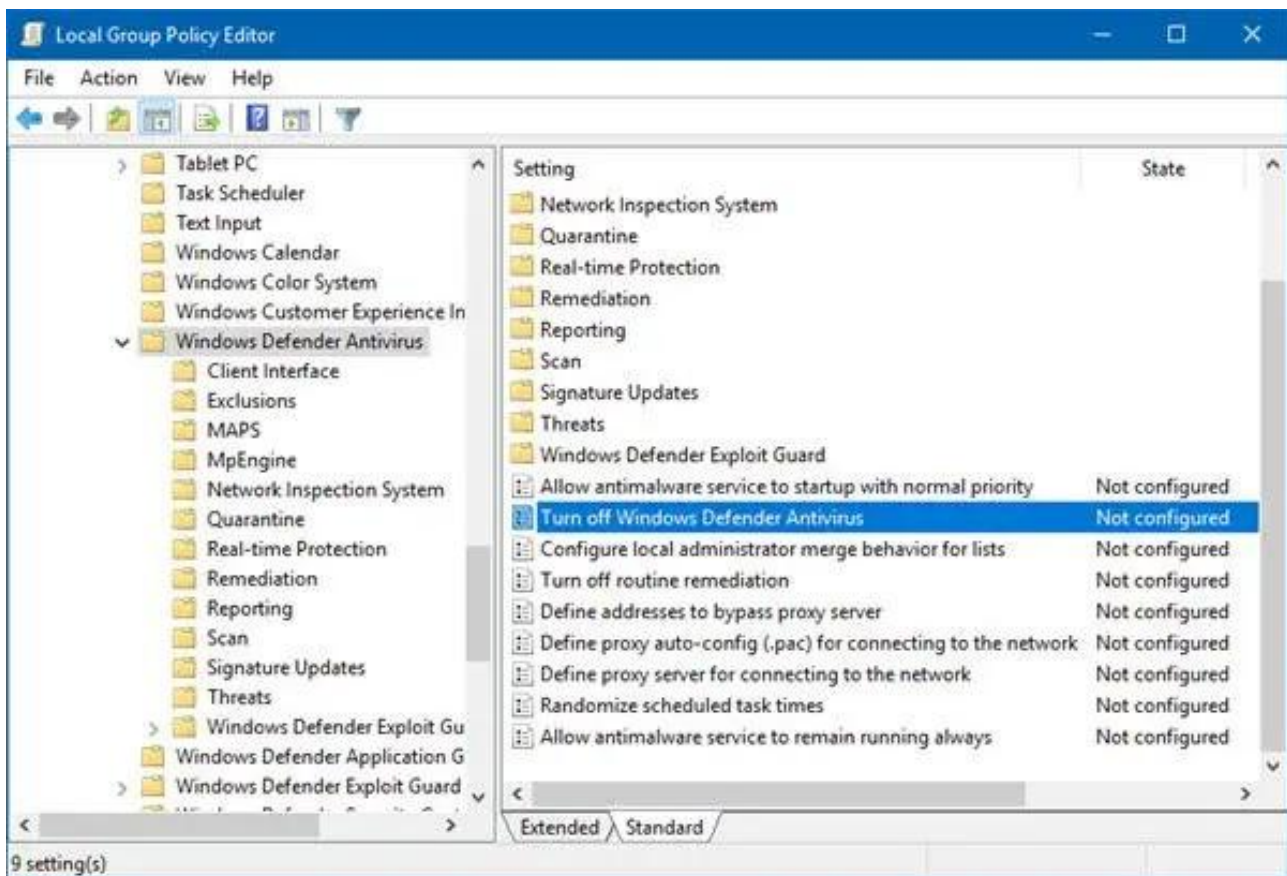
- Fax : Ce service n'est généralement plus utilisé dans les environnements modernes et peut présenter des vulnérabilités.

- Xbox Live Auth Manager et Xbox Live Game Save : Ces services sont inutiles dans un environnement professionnel et peuvent potentiellement être exploités. -

- AllJoyn Router Service : Ce service de découverte de périphériques sur le réseau peut être désactivé s'il n'est pas utilisé, réduisant ainsi les risques liés à la découverte non autorisée d'appareils.

6.3.7 Configuration de Microsoft Defender

1. Activation de la protection en temps réel
2. Activation de la protection basée sur le cloud
3. Activation de l'analyse des archives et des téléchargements



6.3.8 Désactivation des protocoles obsolètes

1. Désactivation de SMBv1

Justification : SMBv1 est un protocole ancien avec de nombreuses vulnérabilités connues. Sa désactivation protège contre des attaques comme WannaCry.

2. Désactivation de TLS 1.0 et 1.1, utilisation exclusive de TLS 1.2 et supérieur

Justification : Les versions antérieures de TLS présentent des failles de sécurité connues. TLS 1.2 et supérieur offrent un meilleur niveau de sécurité pour les communications chiffrées.

6.3.9 Restriction des autorisations PowerShell

1. Activation de la journalisation des scripts PowerShell

Justification : Permet de tracer l'exécution des scripts PowerShell, facilitant la détection d'activités malveillantes.

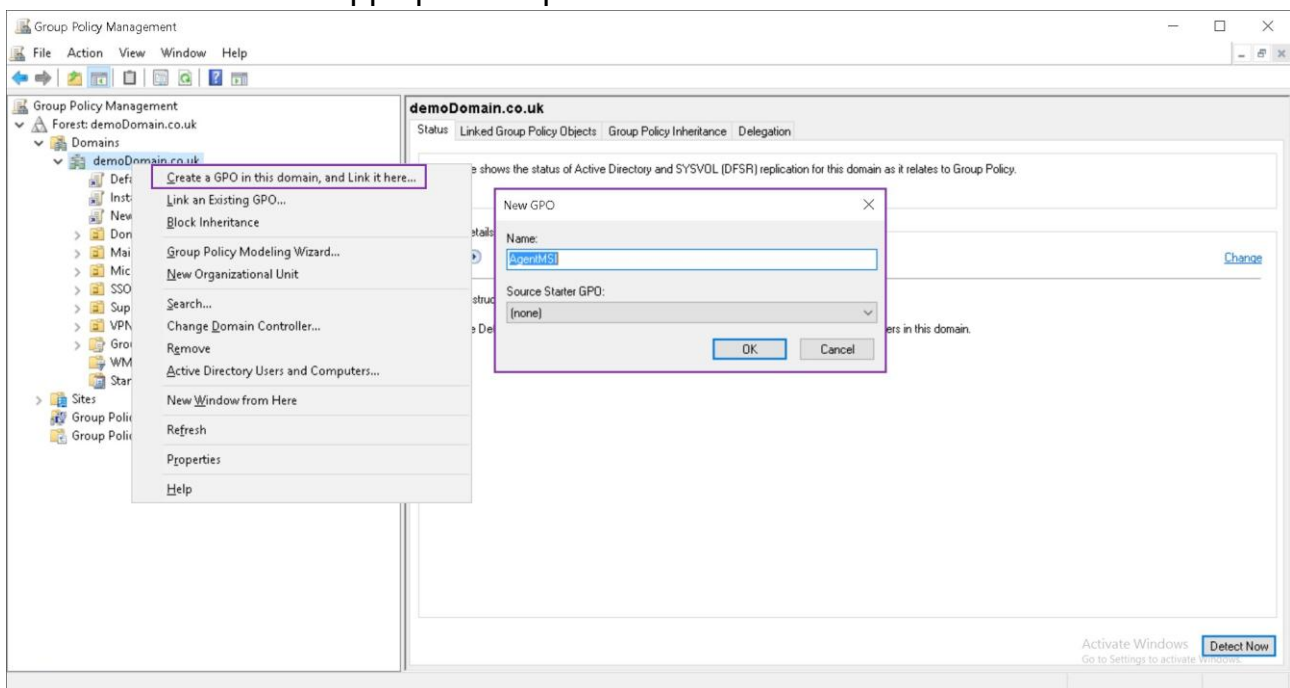
2. Restriction de l'exécution des scripts non signés

Justification : Limite l'exécution aux scripts approuvés, réduisant le risque d'exécution de code malveillant.

6.4 Application des paramètres via les stratégies de groupe (GPO)

Pour déployer ces configurations de manière centralisée, nous utiliserons les stratégies de groupe (GPO) :

1. Ouvrez la console de gestion des stratégies de groupe (gpmc.msc)
2. Créez une nouvelle GPO nommée "EXPERTY - Sécurité Windows 11"
3. Éditez la GPO et appliquez les paramètres décrits ci-dessus



6.5 Audit et surveillance

6.5.1 Configuration de l'audit

1. Activation de l'audit des événements de sécurité
2. Configuration de la taille maximale des journaux d'événements
3. Activation de l'audit des accès aux objets

6.5.2 Centralisation des journaux

Mise en place d'un serveur de collecte centralisée des journaux pour faciliter l'analyse et la détection d'incidents.

Justification : La centralisation des journaux permet une vue d'ensemble de l'activité du système, facilitant la détection rapide d'anomalies et d'incidents de sécurité potentiels.

6.6 Gestion des vulnérabilités

6.6.1 Analyse régulière des vulnérabilités

Utilisation d'outils comme Microsoft Baseline Security Analyzer (MBSA) pour effectuer des analyses régulières.

6.6.2 Veille sur les bulletins de sécurité

Mise en place d'un processus de veille sur les bulletins de sécurité Microsoft et application rapide des correctifs critiques.

6.7 Formation et sensibilisation des utilisateurs

6.7.1 Programme de sensibilisation

Mise en place d'un programme de sensibilisation à la sécurité pour les utilisateurs, couvrant des sujets tels que :

- La gestion des mots de passe
- La reconnaissance des tentatives de phishing
- L'importance des mises à jour

Justification : Les utilisateurs sont souvent le maillon faible de la sécurité informatique. Une formation régulière et une sensibilisation continue sont essentielles pour maintenir un niveau de vigilance élevé et réduire les risques d'erreurs humaines pouvant compromettre la sécurité.

6.7.2 Documentation utilisateur

Création d'un guide de bonnes pratiques de sécurité à destination des utilisateurs finaux.

6.8 Tests et validation

6.8.1 Tests de pénétration

Réalisation de tests de pénétration réguliers pour évaluer l'efficacité des mesures de sécurité mises en place.

6.8.2 Audit de conformité

Réalisation d'audits réguliers pour s'assurer que les configurations de sécurité sont toujours en place et efficaces.

Conclusion de la section

L'application des recommandations de sécurité de l'ANSSI et de Microsoft permet de mettre en place un socle solide pour la protection des postes clients de l'entreprise EXPERTY. Ces mesures, combinées à une vigilance constante et à la sensibilisation des utilisateurs, contribuent à réduire significativement les risques de sécurité. Il est important de noter que la sécurité est un processus continu qui nécessite des mises à jour et des ajustements réguliers pour rester efficace face aux nouvelles menaces.

VII. Conclusion

Ce mémoire de stage a présenté une étude approfondie des différentes méthodes de déploiement d'une image Windows 11 personnalisée pour le renouvellement du parc informatique de l'entreprise EXPERTY. Nous avons exploré trois approches principales : le déploiement par clé USB, le déploiement par le réseau avec FOG

Project, et le déploiement par le réseau avec Windows Deployment Services (WDS).

7.1 Récapitulatif des méthodes de déploiement

1. Déploiement par clé USB :

- Avantages : simplicité, flexibilité pour les petits déploiements
- Inconvénients : chronophage pour un grand nombre de machines, risque d'erreurs humaines

2. Déploiement avec FOG Project :

- Avantages : automatisation, gestion centralisée, open-source
- Inconvénients : nécessite une configuration initiale complexe, dépend d'une infrastructure réseau robuste

3. Déploiement avec WDS :

- Avantages : intégration native avec l'environnement Windows, automatisation poussée
- Inconvénients : nécessite une infrastructure Windows Server, peut être complexe à configurer initialement

7.2 Importance de la sécurisation

La sécurisation des postes clients, basée sur les recommandations de l'ANSSI et de Microsoft, constitue un aspect crucial de ce projet. Les mesures mises en place, telles que le renforcement des politiques de mot de passe, l'activation du chiffrement BitLocker, et la configuration avancée de Microsoft Defender, forment un socle solide pour la protection du parc informatique d'EXPERTY.

7.3 Recommandations

Pour le déploiement des 80 PC Windows 11 d'EXPERTY, nous recommandons l'utilisation de Windows Deployment Services (WDS) pour les raisons suivantes :

1. Intégration optimale avec l'infrastructure Windows existante
2. Capacité de déploiement simultané sur plusieurs machines
3. Possibilité d'automatisation poussée avec les fichiers de réponse
4. Facilité de maintenance et de mise à jour des images à long terme

Cependant, il est important de noter que la méthode de déploiement par clé USB reste pertinente pour les mises à jour ponctuelles ou les déploiements dans des zones avec une connectivité réseau limitée.

7.4 Perspectives d'avenir

À l'avenir, EXPERTY pourrait envisager les améliorations suivantes :

1. Mise en place d'une solution de gestion de parc informatique (ITAM) pour un meilleur suivi des actifs
2. Implémentation d'une solution de gestion des mises à jour tierces pour maintenir à jour les applications déployées
3. Exploration de solutions de virtualisation des postes de travail pour une flexibilité accrue

7.5 Mot de la fin

Ce projet de renouvellement du parc informatique représente une étape importante pour EXPERTY. En combinant des méthodes de déploiement efficaces avec une configuration de sécurité robuste, l'entreprise se dote d'une infrastructure informatique moderne, performante et sécurisée.

La réussite à long terme de ce projet dépendra de la formation continue des utilisateurs, de la veille technologique et sécuritaire, et de l'adaptation constante aux nouvelles menaces et aux évolutions technologiques.

En fin de compte, ce déploiement ne marque pas la fin d'un processus, mais plutôt le début d'une nouvelle ère de gestion informatique plus efficace et sécurisée pour EXPERTY.