Windows Server 2025 — Déploiement WDS/MDT & Gestion des logiciels par GPO

Lab complet Windows Server 2025 pour NOUVY.LAN : déploiement automatisé des postes Windows 11 via WDS/MDT (PXE, LiteTouchPE, images, Sysprep, fichier Unattend) et gestion des logiciels par stratégies de groupe (publication/attribution MSI, mises à niveau, AppLocker). AD NOUVY.LAN déjà en place.

45 min de lecture **Niveau Intermédiaire**

Document généré le 13/05/2026 à 11h14 · nouvy.fr/wiki/windows-server-2025-wds-mdt-gpo-logiciels

Sommaire

29 section(s) · 45 min de lecture

Environnement du lab

1. Installation des postes clients avec les services WDS

↳ Présentation du rôle WDS

↳ WDS et DHCP

↳ Installation du rôle WDS

↳ Image de démarrage WDS

2. Déploiement avec MDT (Microsoft Deployment Toolkit)

↳ Comparaison WDS seul vs WDS + MDT

↳ Installation de MDT sur SRV-WDS

↳ Créer un partage de déploiement MDT

↳ Ajouter Windows 11 dans MDT

↳ Ajouter des pilotes dans MDT

↳ Ajouter des applications dans MDT

↳ Créer une séquence de tâches

↳ Configurer Bootstrap.ini et CustomSettings.ini

↳ Générer le boot.wim MDT (LiteTouchPE)

↳ Intégrer MDT avec WDS

↳ Déployer un poste avec MDT

↳ Capturer une image de référence avec MDT

3. Gestion des logiciels avec les stratégies de groupe

↳ Publication et Attribution de logiciels

↳ Mise à niveau de logiciels

↳ Contrôle des logiciels avec AppLocker

↳ Création de packages MSI

Récapitulatif de l'infrastructure WDS, MDT & GPO

Points de vérification

↳ Vérifier WDS

↳ Vérifier les GPO logiciels

↳ Vérifier AppLocker

Environnement du lab

Ce lab s'appuie sur l'infrastructure **NOUVY.LAN** déjà opérationnelle (Active Directory, DHCP, DNS en place sur SRV-NOUVY). Deux grandes thématiques sont couvertes : le déploiement automatisé des postes Windows 11 via **WDS** (Windows Deployment Services) et la gestion centralisée des logiciels via les **stratégies de groupe (GPO)**.

Rôle	Nom machine	Adresse IP	Système
Contrôleur de domaine / DHCP / DNS	SRV-NOUVY	192.168.1.10	Windows Server 2025
Serveur WDS	SRV-WDS	192.168.1.20	Windows Server 2025
Domaine	NOUVY.LAN	—	—
Postes clients	PC-XXXX	192.168.1.x (DHCP)	Windows 11 Pro/Education/Enterprise

> ***Prérequis** : Active Directory DS, DHCP et DNS sont déjà configurés et opérationnels sur SRV-NOUVY. SRV-WDS est un nouveau serveur membre du domaine NOUVY.LAN, dédié au déploiement WDS.*

---

1. Installation des postes clients avec les services WDS

Présentation du rôle WDS

Windows Deployment Services (WDS) est un rôle Windows Server qui permet de déployer des systèmes d'exploitation Windows sur des ordinateurs en réseau, sans support physique (clé USB, DVD). Le déploiement se fait via le **PXE** (*Pre-boot eXecution Environment*), un standard réseau permettant à un poste de démarrer depuis le réseau avant même que son disque dur ne soit sollicité.

Comment fonctionne le boot PXE ?

```
1. Le poste client s'allume et son firmware (BIOS/UEFI) initie un boot réseau
2. Le poste envoie une requête DHCP sur le réseau
3. Le serveur DHCP répond avec une adresse IP + l'adresse du serveur WDS (option 66)
   et le nom du fichier de démarrage (option 67)
4. Le poste télécharge le fichier de démarrage via TFTP depuis WDS
5. L'environnement Windows PE (WinPE) se charge en mémoire
6. L'assistant de déploiement s'affiche : sélection de l'image à installer
7. L'image Windows 11 est transférée depuis WDS vers le poste
```

Copier

WDS vs MDT vs Windows Autopilot

Solution	Usage recommandé	Prérequis
WDS seul	Lab on-premise, déploiement simple	AD, DHCP, DNS
WDS + MDT	Déploiement avancé avec séquences de tâches, pilotes, applications	WDS + MDT installé
Windows Autopilot	Environnement cloud / hybride Azure AD	Azure AD, Intune

> ***Note Windows Server 2025*** *: WDS reste disponible et pleinement fonctionnel sur Windows Server 2025. Microsoft recommande Windows Autopilot pour les environnements modernes avec Azure AD / Intune. Pour un lab on-premise comme NOUVY.LAN, WDS est la solution standard et suffisante.*

Prérequis WDS (tous déjà en place sur NOUVY.LAN)

Prérequis	Statut	Remarque
Active Directory DS	Operationnel	Domaine NOUVY.LAN
DHCP	Operationnel	Sur SRV-NOUVY
DNS	Operationnel	Sur SRV-NOUVY
Partition NTFS pour les images	A creer	Ex : D:\RemoteInstall

WDS et DHCP

WDS utilise le protocole DHCP pour indiquer aux postes clients l'adresse du serveur de déploiement. Selon la configuration, deux cas se présentent :

Dans notre configuration, **DHCP est sur SRV-NOUVY** et **WDS est sur SRV-WDS** (serveurs séparés). Il n'y a pas de conflit de port 67. Il faut simplement indiquer aux postes l'adresse de SRV-WDS via les options DHCP.

Option DHCP	Numéro	Valeur	Rôle
Serveur de boot	066	`192.168.1.20`	Adresse IP de SRV-WDS
Fichier de boot	067	`boot\x64\wdsnbp.com`	Fichier de démarrage réseau (UEFI 64 bits)

> ***Note*** *: l'option 060 (PXEClient) n'est nécessaire que lorsque DHCP et WDS sont sur le même serveur. Ici elle n'est pas requise.*

Configuration via l'interface graphique sur SRV-NOUVY :

1. Ouvrir le **Gestionnaire de serveur** → **Outils** → **DHCP**
2. Déplier `SRV-NOUVY.NOUVY.LAN` → `IPv4` → **Options de serveur**
3. Clic droit sur **Options de serveur** → **Configurer les options**
4. Cocher l'option **066** → Adresse IP : `192.168.1.20` → **Appliquer**

5. Cocher l'option **067** → Valeur de la chaine : `boot\x64\wdsnbp.com` → **OK**

> ***Attention** : ces options s'appliquent à tous les clients DHCP du scope. Si vous souhaitez restreindre le PXE à certaines machines, utilisez des **réservations DHCP** avec des options spécifiques.*

Installation du rôle WDS

Ajout du rôle via le Gestionnaire de serveur

1. Ouvrir le **Gestionnaire de serveur** sur SRV-WDS
2. Cliquer sur **Gérer** (en haut à droite) → **Ajouter des rôles et fonctionnalités**
3. Type d'installation : **Installation basée sur un rôle ou une fonctionnalité** → Suivant
4. Serveur cible : sélectionner **SRV-WDS** → Suivant
5. Dans la liste des rôles, cocher **Windows Deployment Services**
6. Une fenetre apparait pour ajouter les outils de gestion → cliquer **Ajouter des fonctionnalités**
7. Cliquer **Suivant**
8. Dans la page des services de rôle WDS, cocher les deux options :
    - **Serveur de déploiement** (gère les images et les sessions PXE)
    - **Serveur de transport** (gère le transfert de données réseau, multicast)
9. Cliquer **Suivant** → **Installer**
10. Attendre la fin de l'installation → **Fermer**

Configuration initiale de WDS

Après l'installation, WDS doit etre configuré avant de pouvoir etre utilisé.

1. Dans le **Gestionnaire de serveur**, cliquer sur **Outils** → **Windows Deployment Services**
2. Dans la console WDS, déplier **Serveurs**
3. Clic droit sur **SRV-WDS** → **Configurer le serveur**
4. L'assistant de configuration s'ouvre :

Etape 1 — Emplacement du dossier RemoteInstall :

```
D:\RemoteInstall
```

Copier

> *Choisir un disque différent du disque système (C:) si possible. Ce dossier contiendra toutes les images de démarrage et d'installation. Prevoir suffisamment d'espace (au moins 20 Go par image Windows 11).*

Etape 2 — Paramètres du serveur DHCP/proxy DHCP :

Comme DHCP et WDS sont sur des serveurs distincts :

- Cocher **Ne pas écouter sur le port 67 (DHCP)** : non applicable ici (pas de DHCP

sur SRV-WDS)
- Ne pas cocher **Notifier DHCP (option 60)** : les options 66/67 ont déjà été configurées sur SRV-NOUVY

Etape 3 — Paramètres AD :

- Sélectionner **Intégrer ce serveur à Active Directory** → le serveur WDS sera publié dans NOUVY.LAN

Etape 4 — Réponse aux clients PXE :

Option	Usage
Ne pas répondre aux clients	WDS inactif (désactivé)
Répondre uniquement aux clients connus	Seuls les ordinateurs pré-enregistrés dans AD reçoivent une réponse
Répondre à tous les ordinateurs clients	Tous les postes (connus et inconnus) peuvent démarrer en PXE

Pour un lab, sélectionner **Répondre à tous les ordinateurs clients (connus et inconnus)**.

> ***En production**, il est recommandé de sélectionner "Répondre uniquement aux clients connus" et de pré-enregistrer les ordinateurs dans AD (via leur adresse MAC) pour éviter les déploiements non autorisés.*

5. Cliquer **Terminer** pour valider la configuration.

Image de démarrage WDS

> ***Important — Windows 11 + Windows Server 2025** : depuis Windows 11, le `boot.wim` issu de l'ISO d'installation **ne peut plus être utilisé directement** comme image de démarrage WDS. Microsoft a bloqué cette fonctionnalité. L'image de démarrage à utiliser dans WDS est le **LiteTouchPE généré par MDT** (voir section suivante).*

WDS joue uniquement le rôle de **serveur PXE** : il sert via le réseau l'image WinPE produite par MDT. C'est MDT qui gère l'intégralité du déploiement.

---

2. Déploiement avec MDT (Microsoft Deployment Toolkit)

MDT est un outil Microsoft gratuit qui s'intègre avec WDS pour automatiser entièrement le déploiement des postes : installation de Windows, injection de pilotes, installation d'applications, scripts de post-configuration. C'est la solution on-premise gratuite de référence en 2026 pour les environnements sans Azure.

> ***Note** : MDT n'est plus activement développé par Microsoft (dernière version : 8450, 2019) mais reste pleinement fonctionnel avec Windows 11 et Windows Server 2025. C'est la solution retenue pour NOUVY.LAN.*

Comparaison WDS seul vs WDS + MDT

Fonctionnalité	WDS seul	WDS + MDT
Déploiement OS via PXE	✅	✅
Boot image compatible Windows 11	⚠️ Bloqué	✅ LiteTouchPE
Séquence de tâches automatisée	❌	✅
Injection de pilotes automatique	Manuelle (DISM)	✅ Automatique selon le modèle
Installation d'applications pendant le déploiement	❌	✅
Scripts de post-installation PowerShell	❌	✅
Jonction au domaine automatique	Via Unattend.xml	✅ Natif
Monitoring du déploiement en temps réel	❌	✅

Installation de MDT sur SRV-WDS

Prérequis : Windows ADK + PE Add-on

MDT nécessite l'**ADK Windows 11** et le **Windows PE Add-on** pour générer les images de démarrage.

1. Télécharger **Windows ADK** (dernière version disponible) :

```
https://go.microsoft.com/fwlink/?linkid=2289980
```

Copier

Installer en cochant uniquement : **Outils de déploiement**

2. Télécharger **Windows PE Add-on pour ADK** :

```
https://go.microsoft.com/fwlink/?linkid=2289981
```

Copier

Installer **tout**

Installation de MDT 8450

1. Télécharger **Microsoft Deployment Toolkit 8450** :

```
https://www.microsoft.com/en-us/download/details.aspx?id=57917
```

Copier

2. Lancer `MicrosoftDeploymentToolkit_x64.msi` → installation par défaut
3. Après installation, ouvrir **Deployment Workbench** depuis le menu Démarrer

---

Créer un partage de déploiement MDT

Le **Deployment Share** est le dossier central de MDT. Il contient les OS, pilotes, applications et séquences de tâches.

1. Dans **Deployment Workbench** → clic droit sur **Deployment Shares** → **New Deployment Share**
2. Remplir l'assistant :

Champ	Valeur
Deployment share path	`D:\DeploymentShare`
Share name	`DeploymentShare$`
Deployment share description	`NOUVY – Déploiement Windows 11`

3. Dans les options, cocher selon les besoins :
   - **Ask if a computer backup should be performed** : non (lab)
   - **Ask user to set the local Administrator Password** : selon besoin
4. Cliquer **Finish**

> *Le partage est accessible via `\\SRV-WDS\DeploymentShare$` depuis le réseau.*

Ajouter Windows 11 dans MDT

1. Dans **Deployment Workbench** → déplier le Deployment Share → **Operating Systems**
2. Clic droit → **Import Operating System**
3. Choisir **Full set of source files** → **Next**
4. Source directory : naviguer vers le lecteur où l'ISO Windows 11 est montée (ex : `D:\`)
5. Destination directory name : `Windows 11 25H2` → **Next** → **Finish**

MDT importe tous les fichiers de l'ISO dans le Deployment Share.

Ajouter des pilotes dans MDT

MDT peut injecter automatiquement les pilotes selon le modèle du poste.

1. Dans **Deployment Workbench** → **Out-of-Box Drivers**
2. Créer des sous-dossiers par modèle (bonne pratique) :
    - Clic droit → **New Folder** → nommer par modèle (ex : `Dell OptiPlex 7090`)
3. Clic droit sur le dossier → **Import Drivers**
4. Driver source directory : naviguer vers le dossier contenant les fichiers `.inf` du pilote
5. MDT détecte et importe automatiquement tous les pilotes trouvés

---

Ajouter des applications dans MDT

1. Dans **Deployment Workbench** → **Applications**
2. Clic droit → **New Application**
3. Choisir **Application with source files** (si vous avez les fichiers d'installation) ou **No source files** (si l'application s'installe depuis un partage réseau)
4. Remplir :

Champ	Exemple
Application name	Google Chrome
Command line	`ChromeSetup.msi /quiet /norestart`
Working directory	`.`

5. Cliquer **Finish**

Créer une séquence de tâches

La **séquence de tâches** définit toutes les étapes du déploiement dans l'ordre.

1. Dans **Deployment Workbench** → **Task Sequences**
2. Clic droit → **New Task Sequence**
3. Remplir l'assistant :

Champ	Valeur
Task sequence ID	`WIN11-PRO-001`
Task sequence name	`Déploiement Windows 11 Pro NOUVY`
Template	**Standard Client Task Sequence**

4. Sélectionner l'OS importé : **Windows 11 Pro**
5. Specify Product Key : laisser vide (lab) ou entrer la clé MAK/KMS
6. Remplir les informations du compte admin local → **Finish**

Personnaliser la séquence de tâches

1. Clic droit sur la séquence → **Properties** → onglet **Task Sequence**
2. L'éditeur affiche toutes les étapes dans l'ordre :

```
State Restore
  ├── Preinstall
  │     └── Enable BitLocker (désactiver si non utilisé)
  ├── Install
  │     └── Install Operating System
  ├── PostInstall
  │     ├── Apply Network Settings (jonction domaine)
  │     └── Apply Windows Settings
  ├── State Restore
  │     ├── Install Applications  ← ajouter les apps ici
  │     └── Windows Update (optionnel)
```

Copier

3. Pour ajouter une application : cliquer sur **Install Applications** → **Add** → **General** → **Install Application**
4. Sélectionner l'application ajoutée précédemment

Configurer Bootstrap.ini et CustomSettings.ini

Ces deux fichiers pilotent l'automatisation complète du déploiement MDT.

Bootstrap.ini

Ce fichier est intégré dans le LiteTouchPE (WinPE). Il indique à MDT où se trouve le Deployment Share et les credentials pour s'y connecter **avant** même que Windows soit installé.

Sur SRV-WDS, ouvrir :

```
E:\DeploymentShare\Control\Bootstrap.ini
```

Copier

Remplacer le contenu par :

```
[Settings]
Priority=Default

[Default]
DeployRoot=\\SRV-WDS01\DeploymentShare$
UserID=jonction-wds
UserDomain=NOUVY
UserPassword=MotDePasseJonction
SkipBDDWelcome=YES
```

Copier

> *Après modification de `Bootstrap.ini`, il faut **régénérer le LiteTouchPE** (Update Deployment Share) car ce fichier est embarqué dans le WIM.*

CustomSettings.ini

Ce fichier pilote le comportement de MDT pendant le déploiement : paramètres régionaux,

jonction au domaine, écrans à ignorer.

Sur SRV-WDS, ouvrir :

```
E:\DeploymentShare\Control\CustomSettings.ini
```

Copier

Remplacer le contenu par :

```
[Settings]
Priority=Default

[Default]
OSInstall=Y

; Parametres regionaux
KeyboardLocale=fr-FR
UserLocale=fr-FR
UILanguage=fr-FR
TimeZoneName=Romance Standard Time

; Jonction automatique au domaine NOUVY.LAN
JoinDomain=NOUVY.LAN
DomainAdmin=jonction-wds
DomainAdminDomain=NOUVY
DomainAdminPassword=MotDePasseJonction
MachineObjectOU=OU=Postes_Services,OU=Ordinateurs,OU=NOUVY,DC=NOUVY,DC=LAN

; Ignorer tous les ecrans - deploiement 0 clic
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerBackup=YES
SkipBitLocker=YES
SkipLocaleSelection=YES
SkipDomainMembership=YES
SkipUserData=YES
SkipComputerName=YES
SkipTaskSequence=YES
TaskSequenceID=WIN11-PRO-01
SkipSummary=YES
SkipFinalSummary=YES
FinishAction=REBOOT
```

Copier

> ***SkipTaskSequence=YES + TaskSequenceID=WIN11-PRO-01*** *: le déploiement démarre entièrement sans intervention. Le poste boot en PXE, MDT se connecte au Deployment Share, lance la séquence automatiquement, installe Windows 11, joint le domaine et redémarre.*

> ***Sécurité*** *: le mot de passe est en clair. Protéger l'accès au partage* `DeploymentShare$` *en lecture seule pour les comptes de déploiement.*

Générer le boot.wim MDT (LiteTouchPE)

MDT génère sa propre image de démarrage WinPE appelée **LiteTouchPE**.

Prérequis — Corriger l'erreur "Unable to open the specified WIM file"

L'ADK récent ne contient plus les composants WinPE **x86**. MDT essaie d'en générer un par défaut et échoue. Deux actions à faire avant de générer :

Action 1 — Créer le dossier x86 manquant (PowerShell en administrateur) :

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

Copier

Action 2 — Désactiver la génération de l'image x86 dans MDT :

1. Dans **Deployment Workbench** → clic droit sur le **Deployment Share** → **Properties**
2. Onglet **Windows PE** → menu déroulant **Platform** → sélectionner **x86**
3. Décocher :
    - **Generate a Lite Touch bootable RAM disk ISO image**
    - **Generate a Lite Touch bootable RAM disk WIM file**
4. Repasser sur **x64** → vérifier que les deux cases sont bien **cochées**
5. Cliquer **OK**

Générer les images

1. Dans **Deployment Workbench** → clic droit sur le **Deployment Share** → **Update Deployment Share**
2. Choisir **Completely regenerate the boot images** → **Next** → **Finish**
3. MDT génère les fichiers dans :

```
D:\DeploymentShare\Boot\
  ├── LiteTouchPE_x64.iso
  └── LiteTouchPE_x64.wim
```

Copier

Intégrer MDT avec WDS

L'image LiteTouchPE générée par MDT remplace (ou complète) l'image de démarrage standard de WDS.

1. Dans la console **WDS** → **Images de démarrage**
2. Clic droit → **Ajouter une image de démarrage**
3. Naviguer vers `D:\DeploymentShare\Boot\LiteTouchPE_x64.wim`
4. Nommer : `MDT LiteTouch PE x64` → **Terminer**

> ***Note** : conserver l'ancienne image de démarrage WDS si nécessaire. Les deux images coexistent et le client PXE peut choisir laquelle utiliser.*

Déployer un poste avec MDT

1. Allumer le poste client → **F12** pour le boot PXE
2. Le menu WDS s'affiche → sélectionner **MDT LiteTouch PE x64**
3. L'assistant **LiteTouch** démarre :
    - Entrer les identifiants du domaine (si `SkipDomainMembership=NO`)
    - Saisir le nom du poste (si `SkipComputerName=NO`)
    - Sélectionner la séquence de tâches : **Déploiement Windows 11 Pro NOUVY**
4. L'installation se déroule entièrement sans intervention :
    - Partitionnement automatique
    - Installation de Windows 11
    - Injection des pilotes
    - Installation des applications
    - Jonction au domaine NOUVY.LAN
    - Redémarrage automatique

Suivre le déploiement en temps réel

MDT inclut un tableau de bord de monitoring.

1. Sur SRV-WDS, ouvrir **Deployment Workbench** → **Monitoring**
2. Le tableau affiche en temps réel l'état de chaque déploiement en cours :

Colonne	Information
Name	Nom du poste en cours de déploiement
Percent Complete	Avancement en %
Current Step	Etape en cours (ex : "Installing Applications")
Messages	Eventuelles erreurs
Start Time	Heure de début

Capturer une image de référence avec MDT

La capture permet de créer une image `.wim` personnalisée depuis un **poste de référence** configuré avec les logiciels souhaités.

Etape 1 — Sysprep le poste de référence

Sur le poste de référence (non joint au domaine) :

```
C:\Windows\System32\Sysprep\sysprep.exe /oobe /generalize /shutdown
```

Copier

Etape 2 — Créer une Task Sequence de capture dans MDT

1. **Deployment Workbench** → **Task Sequences** → **New Task Sequence**

2. Template : **Sysprep and Capture** → ID : `CAPTURE-WIN11-01` → Nom : `Capture Windows 11 NOUVY`
3. Créer le dossier de destination :

```
mkdir E:\DeploymentShare\Captures
```

Copier

Etape 3 — Boot PXE et capture

1. Boot PXE sur le poste de référence → sélectionner **MDT LiteTouch PE x64**
2. Sélectionner la séquence **Capture Windows 11 NOUVY**
3. MDT capture automatiquement l'image dans :

```
E:\DeploymentShare\Captures\REFPC_Win11_NOUVY.wim
```

Copier

Etape 4 — Importer et déployer l'image capturée

1. **Operating Systems** → **Import Operating System** → **Custom image file**
2. Pointer vers `E:\DeploymentShare\Captures\REFPC_Win11_NOUVY.wim`
3. Mettre à jour la Task Sequence de déploiement pour utiliser cette image

---

3. Gestion des logiciels avec les stratégies de groupe

Publication et Attribution de logiciels

Les **GPO Software Installation** permettent de déployer des logiciels sur les postes du domaine de manière centralisée. Deux modes de déploiement existent.

Différence entre Publication et Attribution

Mode	Cible	Comportement
Attribution (ordinateur)	Objet Ordinateur	Installation automatique au démarrage du poste, avant la connexion de l'utilisateur
Attribution (utilisateur)	Objet Utilisateur	Installation déclenchée à la première ouverture d'un fichier associé OU à la connexion
Publication (utilisateur)	Objet Utilisateur	Le logiciel apparait dans **Paramètres → Applications → Fonctionnalités facultatives** ou dans l'ancien Panneau de configuration → Ajouter/Supprimer des programmes. L'utilisateur l'installe à la demande.

> ***Prérequis important** : la GPO Software Installation fonctionne uniquement avec des packages **MSI** (Microsoft Installer). Les fichiers `.exe` ne sont pas supportés nativement.*

Préparer le partage réseau des sources logiciels

Les fichiers MSI doivent etre accessibles depuis tous les postes du domaine via un partage réseau.

Créer le partage sur SRV-NOUVY :

1. Ouvrir l'**Explorateur de fichiers** sur SRV-WDS
2. Créer le dossier : `D:\Logiciels`
3. Clic droit sur `D:\Logiciels` → **Propriétés** → onglet **Partage** → **Partage avancé**
4. Cocher **Partager ce dossier** → Nom du partage : `Logiciels$`
5. Cliquer **Autorisations** → ajouter :
    - `Utilisateurs du domaine` → **Lecture**
    - `Administrateurs` → **Contrôle total**
6. Supprimer `Tout le monde` si présent → **OK**
7. Onglet **Sécurité** → vérifier que `Utilisateurs du domaine` a au moins **Lecture et exécution** en NTFS

```
\\SRV-NOUVY\Logiciels$
```

Copier

Créer une GPO de déploiement logiciel

1. Ouvrir le **Gestionnaire de stratégies de groupe** : **Gestionnaire de serveur** → **Outils** → **Gestion des stratégies de groupe**
2. Déplier `Foret : NOUVY.LAN` → `Domaines` → `NOUVY.LAN`
3. Clic droit sur l'OU cible (ex : `OU=Postes_Services` pour Attribution ordinateur, ou `OU=Commercial` pour Attribution utilisateur) → **Créer un objet GPO dans ce domaine, et le lier ici**
4. Nommer la GPO : `GPO_Deploy_NomLogiciel` → **OK**
5. Clic droit sur la nouvelle GPO → **Modifier**

Dans l'éditeur de stratégie de groupe :

Pour une **Attribution ordinateur** :

```
Configuration ordinateur
  └── Stratégies
        └── Paramètres du logiciel
              └── Installation de logiciels   ← clic droit ici
```

Copier

Pour une **Attribution ou Publication utilisateur** :

```
Configuration utilisateur
  └── Stratégies
        └── Paramètres du logiciel
              └── Installation de logiciels   ← clic droit ici
```

Copier

6. Clic droit sur **Installation de logiciels** → **Nouveau** → **Package**

7. Dans la fenetre d'ouverture de fichier, taper le chemin UNC (obligatoire, pas un chemin local) :

```
\\SRV-NOUVY\Logiciels$\NomLogiciel.msi
```

Copier

8. Cliquer **Ouvrir**
9. Choisir la méthode de déploiement :
    - **Attribué** : installation automatique
    - **Publié** : disponible à la demande (uniquement pour Configuration utilisateur)
    - **Avancé** : permet de configurer des options supplémentaires (transformations, catégories)
10. Cliquer **OK**

Le logiciel sera déployé lors du prochain démarrage du poste (Attribution ordinateur) ou de la prochaine connexion de l'utilisateur (Attribution/Publication utilisateur).

> ***Forcer l'application des GPO** : sur le poste client, ouvrir **Paramètres** → **Comptes** → **Accéder professionnel ou scolaire** → cliquer sur la connexion NOUVY.LAN → **Informations** → **Synchroniser** (ou redémarrer le poste).*

Mise à niveau de logiciels

Lorsqu'une nouvelle version d'un logiciel est disponible, la GPO Software Installation permet de gérer la mise à niveau en remplacement de l'ancien package.

Procédure de mise à niveau

1. Copier le nouveau fichier MSI dans `\\SRV-NOUVY\Logiciels$\`
2. Ouvrir la GPO existante de déploiement → naviguer vers **Installation de logiciels**
3. Clic droit dans la zone blanche → **Nouveau** → **Package** → sélectionner le **nouveau MSI**
4. Choisir **Avancé** dans la fenetre de méthode de déploiement → **OK**
5. Dans les propriétés du nouveau package → onglet **Mises à niveau**
6. Cliquer **Ajouter**
7. Sélectionner l'**ancien package** (déjà présent dans la GPO)
8. Choisir le mode de mise à niveau :

Mode	Comportement
Désinstaller le package existant, puis installer le nouveau	Désinstallation propre avant réinstallation. Recommandé si les versions sont incompatibles.
Le package peut mettre à niveau le package existant	Mise à niveau en place, conserve les paramètres et données utilisateur

9. Cocher **La mise à niveau est obligatoire pour les utilisateurs existants** pour forcer la mise à niveau (sinon elle est optionnelle)

10. Cliquer **OK** → **Appliquer** → **OK**

> ***Ordre des GPO** : si l'ancien et le nouveau package sont dans des GPO différentes, s'assurer que les deux GPO sont liées à la meme OU et que l'ordre de traitement est correct (le nouveau package doit référencer l'ancien, peu importe leur GPO respective).*

Contrôle des logiciels avec AppLocker

AppLocker est la solution de confinement applicatif de Windows. Elle permet de définir des règles précises sur les programmes, scripts et packages autorisés à s'exécuter sur les postes du domaine.

> ***AppLocker est disponible sur Windows 11 Pro, Education et Enterprise. Il n'est pas disponible sur Windows 11 Home.***

Architecture d'AppLocker

AppLocker s'appuie sur le service **Application Identity** (`AppIDSvc`) qui doit etre actif sur les postes clients. Sans ce service, AppLocker ne peut pas appliquer ses règles.

Activer le service Application Identity via GPO :

1. Ouvrir (ou créer) une GPO liée à l'OU contenant les postes (ex : `OU=Postes_Services`)
2. Naviguer vers :

```
Configuration ordinateur
  └── Stratégies
        └── Paramètres Windows
              └── Paramètres de sécurité
                    └── Services système
```

Copier

3. Double-cliquer sur **Application Identity**
4. Cocher **Définir ce paramètre de stratégie**
5. Sélectionner **Automatique** → **OK**

Types de règles AppLocker

Type de règle	Extensions concernées	Usage
Règles d'exécutables	`.exe`, `.com`	Contrôle les programmes classiques
Règles Windows Installer	`.msi`, `.msp`, `.mst`	Contrôle les packages d'installation
Règles de scripts	`.ps1`, `.bat`, `.cmd`, `.vbs`, `.js`	Contrôle les scripts
Règles DLL	`.dll`, `.ocx`	Contr ôle avancé des bibliothèques
Règles d'applications empaquetées	Applications Store (APPX)	Contrôle les apps universelles Windows

Configurer AppLocker via GPO

1. Ouvrir la GPO liée aux postes → naviguer vers :

```
Configuration ordinateur
  └── Stratégies
        └── Paramètres Windows
              └── Paramètres de sécurité
                    └── Stratégies de contr ôle des applications
                          └── AppLocker
```

Copier

2. Clic droit sur **AppLocker** → **Propriétés**
3. Pour chaque catégorie à activer, cocher **Configuré** et choisir :
   - **Appliquer les règles** (mode actif — bloque les programmes non autorisés)
   - **Auditer uniquement** (mode audit — journalise sans bloquer, recommandé pour la phase de test)
4. Cliquer **OK**

Créer les règles par défaut

Les règles par défaut autorisent Windows, les applications de `Program Files` et les administrateurs à tout exécuter. Elles constituent la base minimale avant d'ajouter des règles personnalisées.

1. Clic droit sur **Règles d'exécutables** → **Créer des règles par défaut**
2. Les règles suivantes sont créées automatiquement :

Règle créée	Ce qu'elle autorise
Tout dans `%WINDIR%`	Tous les programmes Windows
Tout dans `%PROGRAMFILES%`	Tous les programmes installés dans Program Files
Tout pour le groupe Administrateurs	Les administrateurs ne sont pas bloqués

3. Répéter l'opération pour **Règles Windows Installer** et **Règles de scripts**.

Créer une règle personnalisée

Méthode recommandée : règle par éditeur (signature numérique)

Une règle par éditeur (ou règle de signature) est basée sur le certificat numérique de l'éditeur du logiciel. Elle reste valide meme si le logiciel est mis à jour (tant que l'éditeur ne change pas).

1. Clic droit sur **Règles d'exécutables** → **Créer une nouvelle règle**
2. **Avant de commencer** → Suivant
3. **Action** : choisir **Autoriser** ou **Refuser** → Suivant
4. **Conditions** : sélectionner **Editeur** → Suivant
5. Cliquer **Parcourir** → naviguer vers le fichier `.exe` concerné (ex : un installeur sur le partage réseau)
6. Le certificat de l'éditeur est détecté automatiquement

7. Affiner la règle avec le curseur :
    - **Quel que soit l'éditeur** (trop permissif)
    - **Nom de l'éditeur** (tout ce qui vient de cet éditeur)
    - **Nom du produit** (un produit spécifique de cet éditeur)
    - **Nom du fichier** (un fichier spécifique)
    - **Version du fichier** (une version exacte ou supérieure à)
8. Suivant → définir les **Exceptions** si nécessaire → Suivant
9. Nommer la règle → **Créer**

Méthode par chemin : autorise ou refuse tout ce qui se trouve dans un dossier spécifique. **Méthode par hachage** : autorise ou refuse un fichier précis identifié par son empreinte SHA-256. A utiliser en dernier recours car la règle doit etre mise à jour à chaque modification du fichier.

Mode audit — recommandation avant mise en production

Avant de passer AppLocker en mode "Appliquer les règles", activer le **mode audit** pour une période de test.

En mode audit, AppLocker journalise les blocages potentiels sans bloquer réellement les applications. Cela permet d'identifier les règles manquantes avant de les imposer.

Consulter les journaux AppLocker :

1. Sur un poste client, ouvrir l'**Observateur d'événements** : clic droit sur **Démarrer** → **Observateur d'événements**
2. Naviguer vers :

```
Journaux des applications et des services
  └── Microsoft
        └── Windows
              └── AppLocker
                    ├── EXE and DLL    (exécutables et DLL)
                    ├── MSI and Script (packages et scripts)
                    └── Packaged app-Execution (applications Store)
```

Copier

3. Les événements **8003** (Audit — aurait été bloqué) et **8004** (Audit — aurait été autorisé) apparaissent
4. Pour chaque événement 8003, créer une règle d'autorisation correspondante
5. Une fois toutes les règles créées, repasser la GPO AppLocker en mode **Appliquer les règles**

Création de packages MSI

Si l'application que vous souhaitez déployer n'existe qu'en format `.exe`, il faut la reconditionner en `.msi`. L'outil recommandé pour un lab est **Advanced Installer** (version Community — gratuite).

Installer Advanced Installer

1. Télécharger **Advanced Installer Community** depuis :

```
https://www.advancedinstaller.com/download.html
```

Copier

2. Lancer l'installeur → accepter les conditions → installer
3. Au premier lancement, choisir **Continuer avec la version gratuite (Community)**

Créer un package MSI avec Advanced Installer

1. Lancer **Advanced Installer** → **Nouveau projet**
2. Sélectionner le type de projet : **Simple** (sufficient pour un lab) → **Créer**
3. Remplir les **Informations du produit** :

Champ	Valeur
Nom de l'application	NomDeLApplication
Version	1.0.0
Editeur	NOUVY
GUID du produit	Généré automatiquement (ne pas modifier)
Dossier d'installation	`[ProgramFilesFolder]\NomDeLApplication`

4. Aller dans l'onglet **Fichiers et dossiers** :
    - Dans le volet de gauche, développer `[ProgramFilesFolder]` → cliquer sur le dossier de l'application
    - Clic droit dans le volet de droite → **Ajouter des fichiers** → sélectionner les fichiers de l'application
    - Pour ajouter un dossier entier : clic droit → **Ajouter un dossier**

5. Aller dans l'onglet **Raccourcis** :
    - Clic droit dans la section **Bureau** ou **Menu Démarrer** → **Nouveau raccourci vers un fichier existant**
    - Sélectionner l'exécutable principal de l'application

6. Aller dans l'onglet **Prérequis** (si l'application nécessite .NET ou Visual C++) :
    - Cliquer **Nouveau prérequis**
    - Sélectionner dans la liste : `.NET Framework`, `Visual C++ Redistributable`, etc.
    - Advanced Installer téléchargera et installera automatiquement le prérequis si absent

7. Aller dans **Construire** → **Construire** (ou Ctrl+B)

8. Le fichier `.msi` est généré dans le dossier `[ProjetAdvancedInstaller]\Output\`

Tester et déployer le MSI

1. **Tester localement** : sur SRV-NOUVY ou un poste de test, double-cliquer sur le `.msi` pour vérifier l'installation
2. **Copier le MSI dans le partage** :

```
\\SRV-NOUVY\Logiciels$\NomDeLApplication_1.0.0.msi
```

Copier

3. **Vérifier les permissions NTFS** sur `D:\Logiciels` :
   - Clic droit sur le dossier → **Propriétés** → onglet **Sécurité**
   - `Utilisateurs du domaine` doit avoir au minimum **Lecture et exécution**
4. **Créer la GPO** de déploiement comme décrit dans la section précédente

---

Récapitulatif de l'infrastructure WDS, MDT & GPO

Élément	Valeur
Domaine	NOUVY.LAN
Serveur WDS / DHCP / AD	SRV-NOUVY — 192.168.1.10 (Windows Server 2025)
Dossier RemoteInstall	D:\RemoteInstall
Partage logiciels	\SRV-NOUVY\Logiciels$
Postes clients	Windows 11 Pro / Education / Enterprise
Convention de nommage postes	PC-PRENOM ou PC-SERVICE (ex : PC-EMMA, PC-COMPTA01)
OU cible postes clients	OU=Postes_Services,OU=Ordinateurs,OU=NOUVY,DC=NOUVY,DC=LAN
Compte jonction domaine	jonction-wds (droits limités à la jonction)
AppLocker — mode initial	Audit uniquement (avant mise en production)

Points de vérification

Vérifier WDS

1. Dans la console **WDS** sur SRV-WDS : l'icone du serveur doit etre verte (service actif)
2. Vérifier la présence d'au moins une **image de démarrage** et une **image d'installation**

3. Depuis un poste de test, démarrer en PXE (F12) et vérifier que le menu WDS s'affiche

Vérifier les GPO logiciels

1. Sur un poste client joint au domaine, ouvrir un **Invite de commandes** en tant qu'administrateur
2. Taper :

```
gpresult /r
```

Copier

3. Vérifier que la GPO de déploiement apparait dans la section "Objets de stratégie de groupe appliqués"
4. Ouvrir **Paramètres** → **Applications** pour vérifier la présence des logiciels déployés

Vérifier AppLocker

1. Ouvrir l'**Observateur d'événements** sur un poste client
2. Naviguer vers `Journaux des applications et des services > Microsoft > Windows > AppLocker`
3. En mode audit : des événements 8003/8004 doivent apparaitre si des applications ont été exécutées
4. En mode actif : tenter d'exécuter un programme non autorisé → vérifier le blocage et l'événement 8004