# MDT : déployer Windows 11 24H2 en entreprise sans frais de licence

MDT (Microsoft Deployment Toolkit) 8456 permet de déployer Windows 11 24H2 en entreprise gratuitement, avec injection automatique de drivers, installation silencieuse des applications, configuration post-déploiement via GPO et suivi dans le Deployment Share. Ce guide couvre l'installation complète MDT + ADK, la création d'une Task Sequence LTI, la personnalisation de CustomSettings.ini et Bootstrap.ini, et le déploiement via WDS ou clé USB bootable.

MDT pour déployer Windows 11 24H2 en entreprise est la solution gratuite de référence Microsoft pour automatiser les installations Windows à grande échelle, sans frais de licence supplémentaires au-delà de la licence Windows elle-même. MDT 8456, combiné à l'ADK (Assessment and Deployment Kit) Windows 11 et l'ADK PE add-on, permet d'automatiser complètement le déploiement : partitionnement du disque, installation de Windows 11 24H2, injection automatique des drivers selon le modèle de machine, installation silencieuse des applications (Microsoft 365, agents antivirus, etc.), jonction au domaine Active Directory et configuration post-installation via GPO. Selon les équipes IT interrogées dans les forums TechNet, un déploiement MDT bien configuré réduit le temps d'installation manuelle d'un poste de 3 à 4 heures à 45 à 90 minutes entièrement sans intervention. Ce guide pratique couvre toutes les étapes de A à Z : installation MDT et ADK sur Windows Server 2022, création du Deployment Share, import des sources Windows 11 24H2, création de la Task Sequence LTI (Lite Touch Installation), gestion des drivers par modèle, déploiement d'applications, personnalisation de CustomSettings.ini et Bootstrap.ini, et démarrage via WDS (Windows Deployment Services) ou clé USB bootable.

À RETENIR

## À retenir

**MDT 8456 + ADK 11 + ADK PE add-on** : trois composants doivent être installés dans cet ordre précis — ADK d'abord, ADK PE add-on ensuite, MDT en dernier — pour éviter les erreurs de génération WinPE.

**LTI vs ZTI** : MDT propose deux modes — LTI (Lite Touch Installation, une intervention minimale au démarrage) et ZTI (Zero Touch Installation, 100 % automatique mais nécessite Microsoft Endpoint Configuration Manager / SCCM). Ce guide couvre LTI, accessible sans SCCM.

**Drivers par modèle dans la sélection profile** : organiser les drivers dans des sous-dossiers par modèle (Dell Latitude 5540, HP EliteBook 845) et utiliser les Selection Profiles pour éviter les conflits de drivers entre modèles.

**CustomSettings.ini pilote tout** : ce fichier unique contrôle les réponses automatiques au Wizard MDT — jointure domaine, nom d'ordinateur, clé produit, timezone — sa bonne configuration est la clé d'un déploiement sans interaction.

**Gratuit mais limité à 150 déploiements simultanés** : MDT n'a pas de limite de licences mais le serveur WDS supporte un maximum pratique d'environ 150 déploiements PXE simultanés — au-delà, préférer SCCM/Intune ou un serveur WDS dédié.

## Prérequis et architecture — Qu'est-ce qu'on va déployer ?

MDT (Microsoft Deployment Toolkit) est un outil gratuit disponible sur le site Microsoft Learn. L'architecture de déploiement MDT repose sur un **Deployment Server** (le serveur MDT) qui

stocke les sources Windows, les drivers, les applications et les Task Sequences dans un **Deployment Share** (partage réseau CIFS). Les postes clients démarrent depuis le réseau (PXE via WDS) ou depuis une clé USB bootable contenant l'environnement WinPE, se connectent au Deployment Share et exécutent la Task Sequence automatiquement.

| Composant | Version | Lien téléchargement | Ordre installation |
|---|---|---|---|
| Windows ADK | Windows 11 24H2 (10.1.26100) | learn.microsoft.com/windows-hardware/get-started/adk-install | 1er |
| ADK PE Add-on | Windows 11 24H2 (10.1.26100) | Même page que ADK | 2ème |
| MDT | 8456 (dernière version) | microsoft.com/download/details.aspx?id=54259 | 3ème |
| Serveur MDT | Windows Server 2019 ou 2022 | N/A | Prérequis |
| WDS (optionnel PXE) | Rôle Windows Server | Rôle ADDS ou autonome | Après MDT |

Le serveur MDT doit être un membre du domaine Active Directory (pour la jonction automatique des postes au domaine) avec au moins 4 Go de RAM, 4 cœurs et un espace de stockage adapté : compter 20 Go pour Windows 11 24H2 (ISO), 5 à 10 Go par profil de drivers, et 500 Mo à plusieurs Go par application. Un Deployment Share typique occupe entre 50 et 200 Go selon le nombre de modèles de machines et d'applications incluses.

## Étape 1 — Installation ADK, ADK PE et MDT

L'ordre d'installation est strict : ADK en premier, ADK PE add-on en second, MDT en dernier. Installer MDT avant l'ADK génère des erreurs lors de la génération des images WinPE.

**Étape 1 — Installer Windows ADK 11 24H2** : télécharger l'installeur adksetup.exe depuis le site Microsoft et sélectionner uniquement les composants nécessaires.

```
 # Installation silencieuse Windows ADK (Deployment Tools uniquement pour MDT)
# Télécharger adksetup.exe depuis Microsoft
Start-Process "adksetup.exe" -ArgumentList `
  "/quiet /norestart /features OptionId.DeploymentTools" `
  -Wait -NoNewWindow

# Vérifier l'installation
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows Kits\Installed Roots" |
  Select-Object -ExpandProperty "KitsRoot10"
# Résultat attendu : C:\Program Files (x86)\Windows Kits\
```

**Étape 2 — Installer ADK PE Add-on** : le composant PE (Preinstallation Environment) est un téléchargement séparé depuis la même page Microsoft.

```
 # Installation silencieuse ADK PE Add-on
Start-Process "adkwinpesetup.exe" -ArgumentList `
  "/quiet /norestart /features OptionId.WindowsPreinstallationEnvironment" `
  -Wait -NoNewWindow
```

**Étape 3 — Installer MDT 8456** : l'installeur MDT est un MSI standard.

```
 # Installation MDT 8456 (MSI)
msiexec /i MicrosoftDeploymentToolkit_x64.msi /quiet /norestart
# Résultat : MDT installé dans C:\Program Files\Microsoft Deployment Toolkit
# Ouvrir la console MDT
# Démarrer -> Microsoft Deployment Toolkit -> Deployment Workbench
```

## Étape 2 — Création du Deployment Share et import de Windows 11

Le Deployment Share est le répertoire central qui contient toutes les ressources MDT. Il est partagé sur le réseau pour que les postes en cours de déploiement puissent y accéder. La création du share et l'import de Windows 11 24H2 sont les deux opérations fondatrices.

```
 # Via la console Deployment Workbench :
# Clic droit "Deployment Shares" -> "New Deployment Share"
# Path : D:\DeploymentShare  (disque avec suffisamment d'espace)
# Share name : DeploymentShare$  (le $ cache le partage aux utilisateurs)
# Description : MDT Deployment Share Production

# Équivalent PowerShell (MDT PowerShell Module)
Import-Module "C:\Program Files\Microsoft Deployment Toolkit□in\MicrosoftDeploymentToolkit.psd1"
New-PSDrive -Name "DS001" -PSProvider MDTProvider `
  -Root "D:\DeploymentShare" -Description "Production DS" `
  -NetworkPath "\MDT-SERVER\DeploymentShare$" | Add-MDTPersistentDrive

# Monter le Deployment Share
Restore-MDTPersistentDrive
```

```
 # Importer Windows 11 24H2 (depuis un ISO ou un dossier extrait)
# Monter l'ISO Windows 11 24H2
$iso = Mount-DiskImage -ImagePath "D:\Sources\Windows11_24H2.iso" -PassThru
$driveLetter = ($iso | Get-Volume).DriveLetter

# Importer le système d'exploitation dans MDT
Import-MDTOperatingSystem -Path "DS001:\Operating Systems" `
  -SourcePath "${driveLetter}:" `
  -DestinationFolder "Windows 11 24H2 Entreprise x64" `
  -Move:$false

# Démonter l'ISO
Dismount-DiskImage -ImagePath "D:\Sources\Windows11_24H2.iso"

# Vérifier l'import
Get-MDTOperatingSystem -Path "DS001:\Operating Systems"
```

## Comment créer une Task Sequence LTI pour Windows 11 24H2 ?

La Task Sequence est le script d'installation qui orchestre toutes les étapes du déploiement. MDT propose des templates de Task Sequence prédéfinis — utiliser *Standard Client Task Sequence* pour les déploiements LTI classiques. La Task Sequence peut être personnalisée en ajoutant des

étapes (scripts PowerShell, commandes, installations d'applications) à n'importe quel point de la séquence.

**Étape 1 — Créer la Task Sequence** : dans Deployment Workbench, clic droit sur Task Sequences → New Task Sequence.

```
 # Création de la Task Sequence via PowerShell MDT
Import-MDTTaskSequence -Path "DS001:\Task Sequences" `
  -Name "Windows 11 24H2 Enterprise LTI" `
  -Template "Client.xml" `
  -Comments "Déploiement standard postes bureautiques" `
  -ID "WIN11-24H2-LTI" `
  -Version "1.0" `
  -OperatingSystemPath "DS001:\Operating Systems\Windows 11 24H2 Enterprise x64\Windows 11 LTSC x
  -FullName "Utilisateur" `
  -OrgName "MonEntreprise" `
  -HomePage "about:blank"
```

**Étape 2 — Personnaliser les étapes de la Task Sequence** : dans l'interface graphique, double-cliquer sur la Task Sequence pour accéder à l'éditeur et ajouter les étapes personnalisées.

Les étapes clés d'une Task Sequence LTI Windows 11 type sont les suivantes, dans l'ordre :

Validate (vérification des prérequis matériels)

Gather (collecte des informations machine)

Format and Partition Disk (partitionnement UEFI avec partition EFI, MSR, Windows, Recovery)

Apply Operating System (application de l'image WIM)

Apply Windows Settings (timezone, organisation, nom)

Apply Network Settings (configuration réseau)

Apply Drivers (injection automatique des drivers)

Windows Update (optionnel — très long, préférer post-déploiement)

Applications — Install Applications (installation des logiciels)

Join Domain (jonction au domaine AD)

Execute Sysprep and Capture (si création d'image Gold)

## CustomSettings.ini et Bootstrap.ini — le cerveau du déploiement

Les fichiers `CustomSettings.ini` et `Bootstrap.ini` contrôlent le comportement du Deployment Wizard MDT. `Bootstrap.ini` est inclus dans l'image WinPE et définit comment se connecter au Deployment Share. `CustomSettings.ini` est lu depuis le Deployment Share et contrôle toutes les options du déploiement : identification du poste, jonction domaine, nom de la machine, timezone, applications à installer. Ces deux fichiers utilisent des sections dynamiques basées sur le modèle de machine, le BIOS UUID ou le préfixe MAC pour personnaliser le déploiement par poste ou par groupe de machines.

```
 # Bootstrap.ini (inclus dans l'image WinPE - D:\DeploymentShare\Control\Bootstrap.ini)
[Settings]
Priority=Default

[Default]
DeployRoot=\MDT-SERVER\DeploymentShare$
UserDomain=MONDOMAINE
UserID=mdt-service
UserPassword=Mdt_S3rvice_2026!
SkipBDDWelcome=YES
```

```
 # CustomSettings.ini (D:\DeploymentShare\Control\CustomSettings.ini)
[Settings]
Priority=MACAddress, Model, Default
Properties=MyCustomProperty

# Règle spécifique par adresse MAC (override nom d'ordinateur pour une machine connue)
[00:50:56:AA:BB:CC]
OSDComputerName=PC-DIRECTION-01
OSDComputerDescription=PC Direction Générale

# Règle par modèle de machine (pour appliquer des drivers ou apps spécifiques)
[Dell Latitude 5540]
DriverGroup001=Laptop\Dell\Latitude 5540
TaskSequenceID=WIN11-24H2-LAPTOP

[HP EliteBook 845 G10]
DriverGroup001=Laptop\HP\EliteBook845G10
TaskSequenceID=WIN11-24H2-LAPTOP

[Default]
OSInstall=Y
SkipCapture=YES
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerBackup=YES
SkipBitLocker=YES
SkipSummary=YES
SkipFinalSummary=NO

# Timezone
TimeZoneName=Romance Standard Time

# Jonction domaine Active Directory
JoinDomain=mondomaine.lan
DomainAdmin=mdt-service
DomainAdminDomain=MONDOMAINE
DomainAdminPassword=Mdt_S3rvice_2026!
MachineObjectOU=OU=Nouveaux_Postes,OU=Informatique,DC=mondomaine,DC=lan

# Applications à installer (références aux IDs des apps dans MDT)
Applications001={GUID-Microsoft365-Apps}
Applications002={GUID-AgentAntivirus}
Applications003={GUID-ZabbixAgent2}
```

```
# Nom automatique basé sur le numéro de série
OSDComputerName=PC-%SerialNumber%
```

## Import et gestion des drivers par modèle

La gestion des drivers est souvent la partie la plus chronophage d'un déploiement MDT. La bonne pratique est d'organiser les drivers dans une arborescence par constructeur et par modèle, puis d'utiliser les Selection Profiles pour que chaque Task Sequence n'injecte que les drivers du modèle en cours de déploiement, évitant ainsi les conflits entre drivers de machines différentes.

```
 # Créer une structure de dossiers drivers organisée par modèle
New-Item -Path "DS001:\Out-of-Box Drivers\Laptop\Dell\Latitude 5540" -ItemType Directory
New-Item -Path "DS001:\Out-of-Box Drivers\Laptop\HP\EliteBook845G10" -ItemType Directory
New-Item -Path "DS001:\Out-of-Box Drivers\Desktop\Dell\OptiPlex 7020" -ItemType Directory

# Télécharger les drivers depuis les sites constructeurs (exemple Dell)
# Dell : https://www.dell.com/support -> Drivers & Downloads -> Enterprise
# Extraire le pack drivers dans D:\Temp\Dell-Latitude-5540-Drivers
# Importer les drivers Dell Latitude 5540
Import-MDTDriver -Path "DS001:\Out-of-Box Drivers\Laptop\Dell\Latitude 5540" `
  -SourcePath "D:\Temp\Dell-Latitude-5540-Drivers" `
  -ImportDuplicates:$false

# Créer un Selection Profile pour Dell Latitude 5540
New-MDTSelectionProfile -Path "DS001:\Selection Profiles" `
  -Name "Dell Latitude 5540 Drivers" `
  -Comments "Drivers Dell Latitude 5540 Windows 11 24H2"

# Dans l'interface Deployment Workbench :
# Selection Profiles -> Dell Latitude 5540 Drivers -> Properties -> General
# Cocher uniquement "Out-of-Box Drivers\Laptop\Dell\Latitude 5540"

# Dans la Task Sequence, étape "Apply Drivers" :
# Inject drivers : From a selection profile
# Selection Profile : Dell Latitude 5540 Drivers
```

## Déploiement via WDS (PXE) ou clé USB bootable

MDT supporte deux méthodes de démarrage : via le réseau (PXE/WDS) pour les déploiements en masse, et via une clé USB bootable (LiteTouch ISO) pour les machines sans carte réseau compatible PXE ou les sites sans WDS. Les deux méthodes utilisent la même image WinPE générée par MDT.

```
 # Générer l'image WinPE LiteTouch (met à jour l'image après chaque modification MDT)
Update-MDTDeploymentShare -Path "DS001:" -Force -Verbose
# Durée : 5 à 15 minutes selon les drivers inclus dans WinPE
# Résultat : D:\DeploymentShare\Boot\LiteTouchPE_x64.iso

# Créer une clé USB bootable depuis l'ISO LiteTouch (PowerShell - remplacer E: par votre clé USB)
# Attention : formatage total de la clé USB !
$DriveLetter = "E:"
Format-Volume -DriveLetter "E" -FileSystem FAT32 -NewFileSystemLabel "MDT-BOOT" -Confirm:$false

# Copier l'ISO WinPE sur la clé (via DISM ou 7-Zip pour extraire le contenu)
# Méthode alternative avec Rufus (outil gratuit) :
# Sélectionner l'ISO LiteTouchPE_x64.iso, type MBR/GPT selon BIOS/UEFI du parc
```

```
 # Configuration WDS pour PXE (si WDS installé)
# Installer le rôle WDS
Install-WindowsFeature WDS -IncludeManagementTools

# Configurer WDS en mode mixte (standalone + AD intégré)
wdsutil /initialize-server /remoteinstall:"D:\RemoteInstall"
wdsutil /set-server /answerclients:all

# Lier MDT à WDS - Ajouter l'image de boot MDT dans WDS
# Deployment Workbench -> Deployment Share -> Configure -> Windows Deployment Services
# Ou via PowerShell :
Import-WdsBootImage -Path "D:\DeploymentShare\Boot\LiteTouchPE_x64.wim" -NewImageName "MDT LiteTo

# Vérifier que WDS reçoit les requêtes PXE
Get-WdsBootImage | Select-Object ImageName, Description, Architecture
```

> Lors d'un projet de renouvellement de parc pour une collectivité territoriale (450 postes, modèles mixtes Dell et HP), MDT 8456 avec des Selection Profiles par modèle a réduit le

> temps de déploiement moyen de 3h30 à 55 minutes par poste. La clé de réussite a été l'organisation rigoureuse des drivers et la politique de nommage automatique basée sur le numéro de série (format `PC-COLLECTIVITE-%SerialNumber%`). Les 450 postes ont été déployés en 3 semaines avec une équipe de 2 techniciens grâce au déploiement PXE simultané sur 20 postes maximum.
>
> *— Retour de projet déploiement MDT, mai 2026*

## Applications et post-configuration — automatiser le reste

MDT permet d'installer des applications de façon silencieuse pendant le déploiement. Chaque application est importée dans le Deployment Share avec sa ligne de commande d'installation silencieuse, et peut être conditionnée à un modèle de machine ou un groupe d'utilisateurs via les propriétés de la Task Sequence.

```
 # Importer Microsoft 365 Apps dans MDT
Import-MDTApplication -Path "DS001:\Applications" `
  -Name "Microsoft 365 Apps for Enterprise" `
  -ShortName "M365" `
  -Version "2024" `
  -Publisher "Microsoft" `
  -Language "fr-FR" `
  -CommandLine "setup.exe /configure configuration.xml" `
  -WorkingDirectory ".\Applications\Microsoft 365 Apps" `
  -ApplicationSourcePath "D:\Sources\M365" `
  -DestinationFolder "Microsoft 365 Apps"

# Importer Zabbix Agent 2 en déploiement silencieux
Import-MDTApplication -Path "DS001:\Applications" `
  -Name "Zabbix Agent 2 7.0" `
  -CommandLine "msiexec /i zabbix_agent2-7.0.0-windows-amd64.msi /quiet SERVER=192.168.1.100 SERV
  -ApplicationSourcePath "D:\Sources\Zabbix" `
  -DestinationFolder "Zabbix Agent 2"
```

Pour la gestion des postes après le déploiement MDT, Microsoft Intune prend naturellement le relais via l'Auto-enrollment Azure AD Hybrid Join. Notre guide sur Microsoft Intune : Politiques

de Conformité et Zero Trust détaille comment continuer à gérer les postes déployés via MDT dans un contexte Hybrid Join. Pour les GPO de sécurité appliquées immédiatement après la jonction domaine, notre guide GPO Sécurisation Active Directory : Hardening fournit les modèles de base à appliquer sur la nouvelle OU de staging.

## Questions fréquentes

### MDT supporte-t-il Windows 11 24H2 nativement ?

Oui, MDT 8456 supporte Windows 11 24H2 (build 26100) à condition d'utiliser l'ADK correspondant (version 10.1.26100 ou ultérieure). La version MDT 8456 est la dernière version stable et ne reçoit plus de mises à jour fonctionnelles depuis 2019, mais reste entièrement compatible avec Windows 11 24H2. Microsoft a annoncé qu'Intune et Windows Autopilot sont les successeurs stratégiques de MDT pour les nouvelles organisations — MDT reste cependant la seule option gratuite pour les déploiements on-premise sans accès Azure.

### Quelle est la différence entre MDT LTI et ZTI ?

LTI (Lite Touch Installation) nécessite une interaction minimale au démarrage : l'utilisateur ou le technicien choisit la Task Sequence dans un wizard simple. ZTI (Zero Touch Installation) est 100 % automatique sans aucune interaction, mais requiert Microsoft Configuration Manager (SCCM/ Intune On-Premises) qui est une solution payante distincte. MDT peut fonctionner seul en LTI ou en intégration avec SCCM pour le mode ZTI. Pour les petites et moyennes entreprises, LTI avec un CustomSettings.ini bien configuré permet d'obtenir un déploiement quasi-automatique avec une seule validation initiale.

### Comment gérer les mises à jour Windows pendant le déploiement MDT ?

La meilleure pratique est de ne pas installer les mises à jour Windows pendant la Task Sequence MDT (l'étape Windows Update allonge le déploiement de 30 à 90 minutes). Préférer une image

Windows 11 24H2 à jour (mise à jour mensuelle de l'ISO sources ou utilisation d'un WSUS) et laisser Windows Update s'exécuter après la jonction domaine, géré par GPO. Si la mise à jour pendant le déploiement est indispensable, utiliser l'étape *Windows Update (Pre-Application Installation)* de la Task Sequence avec les paramètres *Query for all applicable updates*.

### MDT peut-il déployer sur des machines UEFI avec Secure Boot activé ?

Oui, MDT 8456 avec l'ADK Windows 11 génère des images WinPE signées compatibles Secure Boot. La Task Sequence crée automatiquement une partition UEFI (EFI System Partition de 260 Mo) lors du partitionnement du disque. Si une machine refuse de démarrer sur le WinPE MDT en PXE avec Secure Boot activé, vérifier que WDS est configuré pour servir des images UEFI signées et que le firmware de la machine accepte les certificats Microsoft dans son Store Secure Boot.

Le CIS Benchmark for Windows 11 liste les 200+ contrôles de durcissement à appliquer après le déploiement MDT — intégrez-les directement dans votre Task Sequence pour une image de référence sécurisée.

### Comment tracer les déploiements et diagnostiquer les échecs ?

MDT génère des logs détaillés dans `X:\MININT\SMSOSD\OSDLOGS\` (sur le poste en cours de déploiement) et dans `D:\DeploymentShare\Logs\` (copié après un déploiement réussi, si la variable `SLShare` est configurée dans CustomSettings.ini). Le fichier `BDD.log` est le log principal — il est compatible avec l'outil CMTrace (fourni avec MDT) qui affiche les erreurs en rouge pour un diagnostic rapide. En cas d'échec, le code d'erreur SCCM visible dans BDD.log permet d'identifier précisément l'étape échouée.

## Comparaison MDT vs Intune Autopilot vs SCCM — quelle solution pour votre taille d'entreprise ?

En 2026, Microsoft propose trois solutions de déploiement Windows en entreprise avec des modèles économiques très différents. Le choix dépend principalement de la taille du parc, de la présence ou non d'Azure AD, et du budget disponible pour la gestion des postes de travail.

| Critère | MDT 8456 | Windows Autopilot + Intune | SCCM (Config Manager) |
|---|---|---|---|
| Coût | Gratuit | Inclus dans Microsoft 365 Business Premium / E3 | Licence System Center séparée (~120 €/poste/an) |
| Infrastructure requise | Serveur Windows + WDS/réseau | Azure AD + Intune (cloud) | Serveur SCCM + SQL Server + réseau |
| Niveau d'automatisation | LTI (quasi-auto) / ZTI avec SCCM | Zero Touch (100 % automatique) | Zero Touch (100 % automatique) |
| Déploiement hors site | Non (réseau local ou VPN) | Oui (Internet natif) | Partiel (Distribution Points) |
| Gestion post-déploiement | GPO uniquement | Intune policies, Conditional Access | Complète (patches, inventaire, remote) |
| Idéal pour | PME, administrations sans Azure | Entreprises Azure AD hybrides ou cloud | Grandes entreprises, on-premise fort |

Pour les entreprises ayant déjà Microsoft 365 E3 ou Business Premium, Autopilot + Intune est la solution moderne recommandée par Microsoft — le déploiement se fait en expédiant les machines directement chez les utilisateurs sans passer par le service informatique. MDT reste la solution de référence pour les environnements sans Azure AD, les collectivités et les administrations françaises contraintes à des hébergements souverains, et les PME souhaitant éviter les coûts supplémentaires de licences cloud.

## Sécurisation du serveur MDT et du Deployment Share

Le Deployment Share MDT contient des informations sensibles : le mot de passe de jonction domaine dans CustomSettings.ini, le compte de service MDT avec des droits d'écriture dans l'AD, et potentiellement des clés de produit Windows. Un accès non autorisé à ces données permettrait à un attaquant de joindre des machines malveillantes au domaine ou de récupérer les credentials de service.

```
 # Sécuriser l'accès au Deployment Share
# 1. Changer les permissions du partage réseau DeploymentShare$
# Retirer "Everyone" et n'accorder l'accès qu'aux comptes nécessaires
$Share = "DeploymentShare$"
$MDTServiceAccount = "MONDOMAINE\svc-mdt"

# Configurer les droits NTFS sur D:\DeploymentShare
$ACL = Get-Acl "D:\DeploymentShare"
$AccessRule = New-Object System.Security.AccessControl.FileSystemAccessRule(
    $MDTServiceAccount, "ReadAndExecute", "ContainerInherit,ObjectInherit", "None", "Allow")
$ACL.SetAccessRule($AccessRule)
Set-Acl "D:\DeploymentShare" $ACL

# 2. Chiffrer CustomSettings.ini pour protéger le mot de passe de jonction domaine
# MDT supporte le chiffrement des mots de passe avec la fonction ConvertFrom-MDTPassword
# Alternativement, utiliser un compte de service MDT avec droits minimaux :
# - Droit "Add workstations to domain" uniquement
# - Aucun droit administrateur
# - Mot de passe complexe 20+ caractères, rotation annuelle

# 3. Restreindre le WDS aux seuls sous-réseaux autorisés
# Dans WDS -> Servers -> Properties -> Network -> DHCP
# Configurer un DHCP scope helper ou des IP helper addresses pour limiter
# les requêtes PXE aux VLANs bureautiques uniquement

# 4. Audit des déploiements via logs centralisés
# SLShare=\LOG-SERVER\MDT-Logs$  (à ajouter dans CustomSettings.ini)
# Chaque déploiement copie ses logs sur le serveur de logs
```

Pour intégrer les postes déployés dans une politique de sécurité complète dès leur premier démarrage, consulter notre guide Guide Complet du Tiering Model Active Directory pour placer les nouveaux postes dans la bonne OU du modèle à niveaux, et notre guide GPO Sécurisation

Active Directory : Hardening pour les GPO de durcissement à appliquer automatiquement lors de la jonction domaine.

---

## Troubleshooting MDT — erreurs courantes et solutions

Les déploiements MDT échouent le plus souvent lors de quatre étapes : le démarrage PXE (problèmes WDS/DHCP), la connexion au Deployment Share (permissions ou réseau), l'injection de drivers (driver incompatible ou manquant), et la jonction au domaine (compte de service ou OU incorrects). Le log `BDD.log` est la référence première pour tout diagnostic.

```
 # Commandes de diagnostic courantes

# 1. Vérifier que WDS répond aux requêtes PXE
Get-WdsServer -ComputerName MDT-SERVER
wdsutil /get-server /show:All

# 2. Tester la connexion au Deployment Share depuis un poste
# Dans WinPE (F8 pour ouvrir un invite de commandes) :
# net use Z: \MDT-SERVER\DeploymentShare$ /user:MONDOMAINE\svc-mdt Mot_de_passe
# Si échec : vérifier le pare-feu (port TCP 445) et les permissions NTFS

# 3. Vérifier les drivers injectés
# Dans BDD.log, chercher "Applying driver packages to the image"
# Si erreur 0x00000077 (HAL.dll) : drivers chipset ou stockage manquants
# Solution : ajouter les drivers Intel VMD ou AMD RAID dans le Selection Profile

# 4. Diagnostiquer un échec de jonction domaine
# Dans BDD.log, chercher "ZTIWindowsUpdate" ou "Join Domain"
# Codes d'erreur courants :
# 0x00000035 : Serveur DC injoignable depuis WinPE (DNS ou réseau)
# 0x00000534 : Nom du compte de service incorrect
# 0x00000056 : Mot de passe du compte de service incorrect
# 0x80070005 : Permissions insuffisantes pour joindre le domaine

# 5. Forcer un déploiement de test depuis la ligne de commande WinPE
# X:\Deploy\Scripts\LiteTouch.wsf /debug:true
```