Installer et préparer un poste Windows 11 Pro pour le domaine

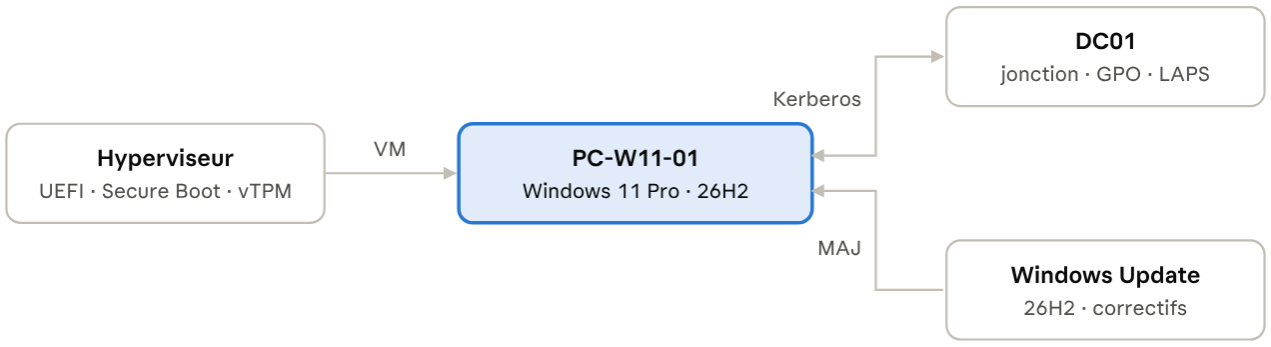
Nov 27, 2026 · @Serge Martins

Objectif

Installer **Windows 11 Pro** (version 25H2, mise à jour ensuite en 26H2) sur une machine virtuelle ou un poste physique, puis le préparer pour le domaine **martinscie.lan** : nom, mises à jour, sécurité et jonction à l'AD.

Élément	Valeur
Nom	PC-W11-01
Réseau	VLAN 20 · DHCP (192.168.20.0/24) · DNS 192.168.10.10
Édition	Windows 11 Pro (la jonction AD est impossible en édition Famille)
Prérequis matériels	CPU 64 bits compatible, 4 Go RAM, 64 Go disque, UEFI + Secure Boot, TPM 2.0

Un poste Windows 11 prêt : TPM, domaine et mises à jour



PC-W11-01 · Windows 11 Pro dans martinscie.lan

L'hyperviseur doit fournir UEFI, Secure Boot et un TPM virtuel ; une fois installé, le poste rejoint DC01 et reçoit ses mises à jour par Windows Update.

Étape 1 – Préparer la machine virtuelle

Hyperviseur	Réglages indispensables
Hyper-V	VM génération 2, démarrage sécurisé *Microsoft Windows*, **TPM virtuel activé**
VMware Workstation Pro	Firmware UEFI + Secure Boot, chiffrement de la VM puis ajout d'un **TPM**
VirtualBox 7	Système → EFI, Secure Boot, **TPM 2.0**
Proxmox VE	BIOS OVMF (UEFI) avec disque EFI, **TPM state v2.0**, contrôleur VirtIO SCSI (pilotes virtio-win)

Allouer 2 vCPU, 4 à 8 Go de RAM, 64 Go de disque et une carte réseau dans le VLAN 20.

Étape 2 – Installation

1. Démarrer sur l'ISO Windows 11 (français, x64), choisir **Windows 11 Pro**.
2. Installation personnalisée sur le disque vierge (Windows crée les partitions EFI, MSR, système et récupération).
3. Au premier démarrage (OOBE) : région France, clavier Français.
4. Choisir **Configurer pour le travail ou l'école → Options de connexion → Joindre un domaine à la place** : cela crée un compte administrateur local (par exemple `admlocal`) sans compte Microsoft.
5. Refuser les options de diagnostic facultatives, de localisation et de publicité.

> Pour un déploiement en série, préférer un fichier de réponse `autounattend.xml` (créé avec Windows System Image Manager de l'ADK) ou un outil de déploiement (Configuration Manager, WDS).

Étape 3 – Post-installation

```
# PowerShell en administrateur
Rename-Computer -NewName PC-W11-01
Get-NetIPConfiguration                    # vérifier l'adresse DHCP et le
DNS 192.168.10.10
Set-TimeZone -Id "Romance Standard Time"
winget upgrade --all --accept-source-agreements
```

Puis **Paramètres → Windows Update** : installer toutes les mises à jour (dont la mise à jour vers **26H2**, livrée en petit paquet d'activation) et redémarrer. Dans une VM, installer les outils invités de l'hyperviseur.

Étape 4 – Joindre le domaine

```
Add-Computer -DomainName martinscie.lan -OUPath
"OU=Postes,DC=martinscie,DC=lan" -Credential MARTINSCIE\Administrateur -
Restart
```

Au redémarrage, ouvrir une session avec un compte du domaine (`MARTINSCIE\adurand`). Le détail de la jonction et du dépannage est dans le guide « Joindre un poste Windows 11 et un poste Debian 13 au domaine Active Directory ».

Étape 5 – Sécuriser le poste

- **BitLocker** sur le lecteur système, clé de récupération sauvegardée dans l'AD (par GPO) :

```
Enable-BitLocker -MountPoint C: -EncryptionMethod XtsAes256 -TpmProtector
Add-BitLockerKeyProtector -MountPoint C: -RecoveryPasswordProtector
```

- **Windows LAPS** : activer par GPO la gestion du mot de passe administrateur local, stocké dans l'AD.
- **Microsoft Defender** et **pare-feu** actifs sur les trois profils ; **Smart App Control** si le poste est neuf.
- Bureau à distance uniquement si nécessaire, avec authentification au niveau du réseau (NLA) et restreint au groupe d'administrateurs.
- Inventaire : installer **GLPI Agent** (voir le guide dédié) pour remonter le poste dans GLPI.

Étape 6 – Vérifications finales

```
winver                                  # version 26H2
Get-Tpm                                 # TpmPresent et TpmReady = True
Confirm-SecureBootUEFI                  # True
manage-bde -status C:
gpresult /r                             # GPO appliquées
```

Dépannage

Symptôme	Piste
« Ce PC ne peut pas exécuter Windows 11 »	TPM 2.0, Secure Boot ou UEFI non activés dans la VM
Pas d'option de jonction à un domaine	Édition Famille : passer en Pro
Mise à jour 26H2 non proposée	Poste en 24H2/25H2 requis ; vérifier les blocages de compatibilité (release health)
Disque introuvable sous Proxmox	Charger le pilote VirtIO SCSI depuis l'ISO virtio-win