Windows Server 2025 — Gestion des mises à jour avec WSUS

Mise en place complète de WSUS sur NOUVY.LAN : installation, configuration, synchronisation avec Microsoft Update, groupes d'ordinateurs, déploiement des mises à jour par GPO et règles d'approbation automatiques.

25 min de lecture **Niveau Intermédiaire**

Document généré le 25/06/2026 à 21h31 · nouvy.fr/wiki/windows-server-2025-wsus

Sommaire

33 section(s) · 25 min de lecture

↳ Vérifier les GPO appliquées sur un poste

↳ Vérifier que les clients contactent WSUS

↳ Vérifier la conformité des postes

↳ Ouvrir le port WSUS dans le pare-feu

Présentation de WSUS

WSUS (Windows Server Update Services) est un rôle Windows Server qui centralise la gestion des mises à jour Microsoft pour tous les postes et serveurs du domaine. Au lieu que chaque machine télécharge ses mises à jour directement depuis Internet, WSUS les télécharge une seule fois depuis Microsoft Update et les distribue en interne.

Avantages de WSUS pour NOUVY.LAN

Avantage	Description
Économie de bande passante	Les mises à jour sont téléchargées une seule fois pour tout le parc
Contrôle des déploiements	Tester les mises à jour avant de les déployer sur tous les postes
Groupes de déploiement	Déployer progressivement (pilotes → utilisateurs → serveurs)
Rapports de conformité	Savoir quels postes sont à jour ou en erreur
Approbation manuelle ou automatique	Choisir quelles mises à jour sont installées

Architecture WSUS pour NOUVY.LAN

Rôle	Machine	IP
Contrôleur de domaine / DNS / DHCP	SRV-NOUVY	192.168.1.10
Serveur WSUS	SRV-WSUS	192.168.1.30
Postes clients	PC-XXXX	192.168.1.x

> *SRV-WSUS est un serveur dédié membre du domaine NOUVY.LAN. Séparer WSUS de l'AD garantit de meilleures performances et facilite la maintenance.*

---

1. Installation et configuration de WSUS

Installation du rôle WSUS

1. Ouvrir le **Gestionnaire de serveur** sur **SRV-WSUS**
2. **Gérer** → **Ajouter des rôles et fonctionnalités**
3. Type d'installation : **Installation basée sur un rôle** → Suivant
4. Serveur cible : **SRV-WSUS** → Suivant
5. Dans la liste des rôles, cocher **Windows Server Update Services**
6. Une fenêtre propose d'ajouter les fonctionnalités requises → **Ajouter des fonctionnalités**

7. Suivant → dans la page des services de rôle, laisser cochés :
    - **WID Connectivity** (base de données interne Windows — suffisant pour un lab)
    - **WSUS Services**
8. Choisir le dossier de stockage des mises à jour :

```
D:\WSUS
```

Copier

> *Prévoir au minimum **20 à 50 Go** selon les produits synchronisés. Utiliser un disque séparé du système si possible.*

9. Cliquer **Suivant** → **Installer** → attendre la fin → **Fermer**
10. Une notification apparaît dans le Gestionnaire de serveur : **"Lancer les tâches de post-installation"** → cliquer dessus et attendre la fin

Configuration initiale via l'assistant WSUS

1. Ouvrir **Gestionnaire de serveur** → **Outils** → **Windows Server Update Services** sur SRV-WSUS
2. L'assistant de configuration s'ouvre automatiquement → **Suivant**

Etape 1 — Programme d'amélioration :

- Décocher la participation au programme → **Suivant**

Etape 2 — Choisir le serveur amont :

Option	Usage
Synchroniser depuis Microsoft Update	WSUS télécharge directement depuis Internet
Synchroniser depuis un autre serveur WSUS	Hiérarchie WSUS (environnements complexes)

Sélectionner **Synchroniser depuis Microsoft Update** → **Suivant**

Etape 3 — Paramètres du proxy :

- Si le réseau utilise un proxy : cocher et renseigner l'adresse
- Sinon : laisser vide → **Suivant**

Etape 4 — Se connecter au serveur amont :

- Cliquer **Démarrer la connexion** → attendre → **Suivant**

Etape 5 — Choisir les langues :

- Décocher **Télécharger les mises à jour dans toutes les langues**
- Cocher uniquement **Français** (et **Anglais** si nécessaire) → **Suivant**

Etape 6 — Choisir les produits :

Cocher uniquement les produits présents dans le parc :

Produit	Cocher si
Windows 11	Postes clients Windows 11
Windows Server 2025	Serveurs Windows Server 2025
Microsoft Edge	Si Edge est utilisé
Microsoft 365 Apps	Si Office 365 est déployé

> *Ne pas cocher tous les produits — cela évite de télécharger des Go inutiles.*

Etape 7 — Choisir les classifications :

Classification	Description	Recommandation
Mises à jour critiques	Correctifs urgents de sécurité	☑ Toujours
Mises à jour de sécurité	Correctifs CVE	☑ Toujours
Mises à jour de définitions	Antivirus / Defender	☑ Toujours
Service Packs	Grands packs cumulatifs	☐ Recommandé
Mises à jour	Améliorations fonctionnelles	☐ Recommandé
Feature Packs	Nouvelles fonctionnalités	Optionnel
Outils	Utilitaires Microsoft	Optionnel

Etape 8 — Planifier la synchronisation :

Option	Usage
Synchroniser manuellement	Pour le premier démarrage (lab)
Synchroniser automatiquement	Production — choisir 1 fois par jour

Pour la production, configurer : **Synchroniser automatiquement** → **1 fois par jour** → heure : `02:00` (nuit)

Etape 9 — Première synchronisation :

- Cocher **Commencer la synchronisation initiale** → **Terminer**

> *La première synchronisation peut prendre **30 minutes à plusieurs heures** selon la connexion et les produits sélectionnés.*

---

2. Synchronisation

Lancer une synchronisation manuelle

1. Dans la console **WSUS** → déplier **SRV-WSUS** → cliquer sur **Synchronisations**

2. Dans le volet Actions → **Synchroniser maintenant**
3. La progression s'affiche dans le volet central

Vérifier l'état de la synchronisation

1. Dans la console WSUS → **Rapport de synchronisation**
2. Les informations affichées :

Information	Description
Dernière synchronisation	Date et heure de la dernière sync réussie
Nouvelles mises à jour	Nombre de mises à jour récupérées
Mises à jour révisées	Mises à jour modifiées par Microsoft
Erreurs	Eventuelles erreurs de téléchargement

Configurer la synchronisation automatique

1. Dans la console WSUS → **Options** → **Planification de la synchronisation**
2. Sélectionner **Synchroniser automatiquement**
3. Configurer :
    - **Première synchronisation** : `02:00`
    - **Synchronisations par jour** : `1`
4. Cliquer **OK**

Nettoyage du serveur WSUS

Après quelques mois, WSUS accumule des données inutiles. Lancer régulièrement le nettoyage :

1. Dans la console WSUS → **Options** → **Assistant de nettoyage du serveur**
2. Cocher toutes les options :
    - Ordinateurs inutilisés
    - Mises à jour expirées inutilisées
    - Mises à jour expirées
    - Révisions de mises à jour inutiles
    - Fichiers de mise à jour inutilisés
3. Cliquer **Suivant** → attendre → **Terminer**

> *Planifier ce nettoyage une fois par mois via une tâche planifiée Windows.*

---

3. Groupes d'ordinateurs WSUS

Les groupes permettent de contrôler **quels postes reçoivent quelles mises à jour** et **quand**. La bonne pratique est de déployer progressivement : d'abord un groupe pilote, puis les utilisateurs, enfin les serveurs.

Architecture des groupes recommandée pour NOUVY.LAN

```
Tous les ordinateurs (groupe par défaut)
  ├── Serveurs
  │     └── SRV-NOUVY, SRV-WDS
  ├── Pilotes
  │     └── 2-3 postes de test
  └── Postes-Services
        └── Tous les postes utilisateurs
```

Copier

Créer les groupes

1. Dans la console **WSUS** → **Ordinateurs** → **Tous les ordinateurs**
2. Clic droit sur **Tous les ordinateurs** → **Ajouter un groupe d'ordinateurs**
3. Créer les groupes suivants :

Groupe	Contenu	Délai de déploiement
Pilotes	2-3 postes de test	Immédiat après approbation
Postes-Services	Tous les postes utilisateurs	7 jours après Pilotes
Serveurs	SRV-NOUVY, SRV-WDS	14 jours après Pilotes

Affecter les ordinateurs aux groupes

Les ordinateurs apparaissent dans WSUS une fois qu'ils ont contacté le serveur (après configuration GPO). Deux méthodes d'affectation :

Méthode 1 — Manuelle (côté serveur) :

1. Dans **Tous les ordinateurs** → clic droit sur un ordinateur → **Modifier l'appartenance**
2. Cocher le groupe souhaité → **OK**

Méthode 2 — Automatique par GPO (recommandée) : Configurer `Ciblage côté client` dans les GPO pour affecter automatiquement les postes aux groupes selon leur OU AD. Voir section **Configuration des clients**.

---

4. Configuration des clients par GPO

La GPO permet de pointer tous les postes vers le serveur WSUS et de les affecter automatiquement au bon groupe.

Créer la GPO WSUS

1. Ouvrir le **Gestionnaire de stratégies de groupe** sur SRV-NOUVY (le DC)
2. Déplier `NOUVY.LAN` → clic droit sur l'OU `Postes_Services` → **Créer un objet GPO et le lier ici**

3. Nommer : `GPO_WSUS_Postes` → **OK**
4. Clic droit sur la GPO → **Modifier**

Paramètres WSUS dans l'éditeur GPO

> ***Windows Server 2025*** *: les paramètres WSUS sont répartis dans* ***deux sous-dossiers*** *distincts sous* `Windows Update`*.*

Sous-dossier 1 — "Gérer les mises à jour proposées de Windows Server Update Service"

```
Configuration ordinateur
  └── Stratégies
        └── Modèles d'administration
              └── Composants Windows
                    └── Windows Update
                          └── Gérer les mises à jour proposées de Windows Server Update
Service
```

Copier

Spécifier l'emplacement intranet du service de mise à jour Microsoft

- Double-cliquer → **Activé**
- **Définir le service intranet de mise à jour pour la détection des mises à jour** :

```
http://SRV-WSUS:8530
```

Copier

- **Définir le serveur intranet de statistiques** :

```
http://SRV-WSUS:8530
```

Copier

- Cliquer **OK**

> *Le port par défaut de WSUS est* ***8530*** *(HTTP) ou* ***8531*** *(HTTPS). Ne pas oublier d'ouvrir ce port dans le pare-feu de* ***SRV-WSUS****.*

Autoriser le ciblage côté client

- Double-cliquer → **Activé**
- **Nom du groupe cible** : `Postes-Services`
- Cliquer **OK**

> *Créer une GPO séparée* `GPO_WSUS_Serveurs` *liée à l'OU des serveurs avec le nom de groupe* `Serveurs`*.*

Sous-dossier 2 — "Stratégies héritées"

> ***Windows Server 2025 / Windows 11 24H2** : le paramètre "**Configurer les mises à jour automatiques**" a été **supprimé** des templates ADMX par Microsoft. Il n'existe plus dans les GPO natives de Windows Server 2025.*

Le dossier **Stratégies héritées** contient uniquement des paramètres de comportement de redémarrage (notifications, délais, fenêtres de maintenance).

Pas de redémarrage automatique avec des utilisateurs connectés

- Double-cliquer → **Activé** → **OK**

> *Empêche Windows de redémarrer automatiquement si un utilisateur est connecté. Recommandé en production pour ne pas interrompre le travail.*

Replanifier les installations planifiées des mises à jour automatiques

- Double-cliquer → **Activé**
- Délai : `1` minute
- Cliquer **OK**

> *Si une installation planifiée a été manquée (poste éteint), Windows la relance 1 minute après le prochain démarrage.*

Comment planifier les mises à jour sans "Configurer les mises à jour automatiques" ?

Avec Windows 11 + WSUS, le téléchargement et l'installation des mises à jour approuvées se font **automatiquement** dès que le poste contacte WSUS. Le comportement par défaut de Windows Update suffit : les mises à jour approuvées sont téléchargées en arrière-plan et installées lors du prochain redémarrage.

Créer une GPO dédiée pour le groupe Pilotes

1. Créer `GPO_WSUS_Pilotes` liée à une OU `OU=Pilotes` (ou via filtre de sécurité sur des postes spécifiques)
2. Mêmes paramètres mais **Nom du groupe cible** : `Pilotes`
3. Ordre de priorité GPO : `GPO_WSUS_Pilotes` doit avoir une priorité **plus haute** que `GPO_WSUS_Postes`

Forcer l'application de la GPO

Sur un poste client (ou via script de déploiement) :

```
gpupdate /force
wuauclt /detectnow
wuauclt /reportnow
```

Copier

Ou en PowerShell :

```
gpupdate /force
Start-Sleep -Seconds 10
(New-Object -ComObject Microsoft.Update.AutoUpdate).DetectNow()
```

Copier

Le poste apparaît dans la console WSUS sous **Tous les ordinateurs** dans les minutes suivantes.

---

5. Règles d'approbation automatiques

Les règles d'approbation automatiques permettent d'approuver certaines catégories de mises à jour sans intervention manuelle.

Configurer les règles d'approbation

1. Dans la console **WSUS** → **Options** → **Approbations automatiques**
2. Onglet **Règles de mise à jour**

Règle 1 — Mises à jour critiques et de sécurité (groupe Pilotes)

Cette règle approuve automatiquement les mises à jour critiques et de sécurité uniquement pour le groupe Pilotes.

1. Cliquer **Nouvelle règle**
2. Cocher **Quand une mise à jour est dans une classification spécifique**
3. Cliquer sur le lien **toute classification** → sélectionner :
    - Mises à jour critiques
    - Mises à jour de sécurité
4. Cocher **Quand une mise à jour est pour un produit spécifique**
5. Cliquer sur **tout produit** → sélectionner **Windows 11**, **Windows Server 2025**
6. Cocher **Approuver la mise à jour pour un groupe spécifique**
7. Cliquer sur **tout groupe d'ordinateurs** → sélectionner **Pilotes**
8. Nommer la règle : `Auto - Critiques et Sécurité - Pilotes`
9. Cliquer **OK**

Règle 2 — Mises à jour de définitions (tous les groupes)

Les mises à jour de définitions (antivirus, Defender) doivent être déployées immédiatement sur tous les postes.

1. Cliquer **Nouvelle règle**
2. Classification : **Mises à jour de définitions**
3. Produit : **Windows 11**, **Windows Server 2025**
4. Groupe : **Tous les ordinateurs**
5. Nommer : `Auto - Définitions - Tous`
6. Cliquer **OK**

Règle 3 — Approbation manuelle pour Postes-Services et Serveurs

Les mises à jour vers les postes utilisateurs et serveurs restent en **approbation manuelle** pour valider d'abord sur les Pilotes.

> *Ne pas créer de règle automatique pour ces groupes. L'administrateur approuve manuellement après validation sur les Pilotes.*

Activer les règles

1. Dans l'onglet **Règles de mise à jour**, cocher les règles à activer
2. Cliquer **Exécuter la règle** pour appliquer immédiatement
3. Cliquer **OK**

Procédure d'approbation manuelle

Après validation sur les Pilotes (généralement 7 jours sans problème) :

1. Dans la console WSUS → **Mises à jour** → **Toutes les mises à jour**
2. Filtrer : **Approbation** = `Non approuvé` — **Etat** = `Echec ou Nécessaire`
3. Sélectionner les mises à jour à déployer
4. Clic droit → **Approuver**
5. Pour chaque groupe, choisir **Approuvé pour l'installation**
6. Cliquer **OK**

Récapitulatif WSUS NOUVY.LAN

Paramètre	Valeur
Serveur WSUS	SRV-WSUS — 192.168.1.30
Port WSUS	8530 (HTTP)
Dossier de stockage	D:\WSUS
Synchronisation	Automatique — 1x/jour à 02:00
Produits synchronisés	Windows 11, Windows Server 2025
Classifications	Critiques, Sécurité, Définitions, Mises à jour
Groupes	Pilotes, Postes-Services, Serveurs
GPO postes	GPO_WSUS_Postes → OU=Postes_Services
GPO serveurs	GPO_WSUS_Serveurs → OU=Serveurs
Approbation auto	Définitions (tous) + Critiques/Sécurité (Pilotes)
Approbation manuelle	Postes-Services et Serveurs

Points de vérification

Vérifier les GPO appliquées sur un poste

Commande rapide

> ***Important** : ouvrir l'invite de commandes **en tant qu'administrateur** (clic droit → Exécuter en tant qu'administrateur). Sans élévation, seule la section utilisateur s'affiche — les GPO ordinateur (dont WSUS) n'apparaissent pas.*

Sur le poste client, ouvrir un **CMD en administrateur** :

```
gpresult /r /scope computer
```

Copier

Affiche uniquement les GPO appliquées à l'**ordinateur**. C'est la commande à utiliser pour vérifier WSUS car la GPO est en **Configuration ordinateur**.

La GPO WSUS doit apparaître dans **"Objets de stratégie de groupe appliqués"**. Si elle est dans **"refusés"**, la raison est indiquée. Si elle n'apparaît nulle part, le poste ne voit pas la GPO (problème de liaison ou d'OU).

Rapport HTML détaillé

```
gpresult /h C:\rapport_gpo.html
```

Copier

Puis ouvrir `C:\rapport_gpo.html` dans un navigateur → rapport complet avec toutes les GPO, les paramètres appliqués et les GPO refusées (avec la raison).

GPO utilisateur uniquement

```
gpresult /r /scope user
```

Copier

Affiche uniquement les GPO appliquées à l'**utilisateur** connecté (non nécessaire pour WSUS).

Forcer la mise à jour des GPO

Si une GPO vient d'être modifiée et n'est pas encore appliquée :

```
gpupdate /force
```

Copier

Résultat attendu pour WSUS

Dans la section **"Objets de stratégie de groupe appliqués"** (ordinateur), les GPO suivantes doivent apparaître :

```
GPO_WSUS_Postes
GPO_WSUS_Pilotes  (si le poste est dans le groupe Pilotes)
```

Copier

Vérifier que les clients contactent WSUS

Sur un poste client, vérifier dans le registre :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
```

Copier

Les clés suivantes doivent être présentes :

- `WUServer` = `http://SRV-WSUS:8530`
- `WUStatusServer` = `http://SRV-WSUS:8530`
- `TargetGroup` = `Postes-Services`

Ou via PowerShell :

```
Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate"
```

Copier

Vérifier la conformité des postes

1. Dans la console WSUS → **Rapports** → **Résumé de la conformité des mises à jour**
2. Sélectionner le groupe à vérifier
3. Le rapport affiche pour chaque poste :

Statut	Description
Installé	Mise à jour installée avec succès
Nécessaire	Mise à jour approuvée mais pas encore installée
Echec	Erreur lors de l'installation
Non applicable	La mise à jour ne concerne pas ce poste
Inconnu	Le poste n'a pas encore contacté WSUS

Ouvrir le port WSUS dans le pare-feu

Sur SRV-WSUS (PowerShell en administrateur) :

```
New-NetFirewallRule -DisplayName "WSUS HTTP" -Direction Inbound -Protocol TCP -LocalPort
8530 -Action Allow
New-NetFirewallRule -DisplayName "WSUS HTTPS" -Direction Inbound -Protocol TCP -LocalPort
8531 -Action Allow
```

Copier