Infrastructure Serveur Windows Server — Guide complet

Guide complet en 15 chapitres couvrant l'ensemble des services Windows Server : Active Directory, DHCP, DNS, DFS, GPO, WSUS, WDS, PowerShell, sécurité et surveillance. Procédures graphiques depuis les consoles Windows Server.

120 min de lecture **Niveau Avancé**

Document généré le 11/07/2026 à 20h42 · nouvy.fr/wiki/infrastructure-serveur-windows-server

Sommaire

107 section(s) · 120 min de lecture

Table des matières

Chapitre 1 : Services de domaine Active Directory

1. Présentation des services de l'Active Directory

Les **Services de domaine Active Directory (AD DS)** constituent le cœur de l'infrastructure d'identité Microsoft. Ils permettent de centraliser l'authentification, l'autorisation et la gestion des ressources dans un réseau d'entreprise.

Concepts fondamentaux :

- **Contrôleur de domaine (DC)** : serveur qui héberge une copie de la base de données AD DS (NTDS.dit) et répond aux demandes d'authentification Kerberos/NTLM.
- **Forêt** : niveau le plus élevé dans la hiérarchie AD. Ensemble d'arbres partageant un schéma commun, un catalogue global et des relations d'approbation implicites.
- **Arbre** : ensemble de domaines partageant un espace de noms DNS contigu (ex : nouvy.lan, paris.nouvy.lan, lyon.nouvy.lan).
- **Domaine** : unité administrative et de sécurité de base. Contient des utilisateurs, ordinateurs, groupes et stratégies.
- **Unité d'organisation (OU)** : conteneur logique dans un domaine, permettant de déléguer l'administration et d'appliquer des GPO de façon granulaire.
- **Schéma AD** : définit les classes d'objets (utilisateur, ordinateur, groupe...) et leurs attributs autorisés dans la forêt. Unique par forêt, extensible mais non réversible.
- **Catalogue global (CG)** : DC particulier qui stocke une copie partielle (attributs les plus utilisés) de tous les objets de la forêt. Indispensable pour la résolution UPN et les recherches inter-domaines.

Les 5 rôles FSMO (Flexible Single Master Operations) :

Rôle FSMO	Étendue	Rôle
Maître de schéma	Forêt (1 seul)	Seul DC autorisé à modifier le schéma AD
Maître de nommage de domaine	Forêt (1 seul)	Gère l'ajout/suppression de domaines dans la forêt
RID Master	Domaine	Attribue des blocs de RID aux DC pour créer des objets avec SID uniques
Émulateur PDC	Domaine	Synchronisation de l'heure, traitement des verrouillages, compatibilité NT4
Maître d'infrastructure	Domaine	Maintient les références inter-domaines (phantoms) à jour

> ***Bonne pratique :*** *les 5 rôles sont initialement sur le premier DC. En production, Maître de schéma et Maître de nommage restent ensemble, RID Master et Émulateur PDC restent ensemble, le Maître d'infrastructure va sur un DC qui n'est pas CG (sauf si tous les DC sont CG).*

2. Promotion d'un contrôleur de domaine

Depuis **Server Manager** sur le futur DC :

1. **Server Manager → Gérer → Ajouter des rôles et fonctionnalités**
2. Type d'installation : Installation basée sur un rôle ou une fonctionnalité → Suivant
3. Sélectionner le serveur cible → Suivant
4. Cocher **Services de domaine Active Directory (AD DS)** → ajouter les fonctionnalités requises → Suivant
5. Suivant jusqu'à **Installer** (ne pas fermer l'assistant)
6. Une fois l'installation terminée, cliquer sur le lien **"Promouvoir ce serveur en contrôleur de domaine"** (dans la notification jaune de Server Manager)

Assistant de configuration des services de domaine Active Directory :

7. Choisir l'opération de déploiement :
    - **Ajouter une nouvelle forêt** (premier DC) → saisir le nom de domaine racine (ex : `nouvy.lan`)
    - **Ajouter un contrôleur de domaine à un domaine existant** → saisir le nom du domaine et les identifiants d'un admin de domaine
    - **Ajouter un nouveau domaine à une forêt existante**
8. Options du contrôleur de domaine :
    - Niveau fonctionnel de la **forêt** → Windows Server 2016 (ou supérieur)
    - Niveau fonctionnel du **domaine** → Windows Server 2016 (ou supérieur)
    - Cocher **Serveur DNS** ✓
    - Cocher **Catalogue global (CG)** ✓ (recommandé)
    - Définir le **mot de passe DSRM** (Directory Services Restore Mode) — conserver précieusement
9. Options DNS : ignorer l'avertissement délégation DNS (normal pour première installation)
10. Nom NetBIOS : vérifié automatiquement (ex : NOUVY)
11. Chemins : laisser par défaut `C:WindowsNTDS` (base), `C:WindowsSYSVOL` (sysvol)
12. Vérification des prérequis → des avertissements sont normaux, les erreurs bloquantes doivent être corrigées
13. **Installer** → le serveur redémarre automatiquement et se configure comme DC

---

3. Redémarrage de l'Active Directory

Si le service AD DS doit être redémarré (maintenance, problème) :

Méthode 1 — Via services.msc :

1. `Windows + R` → `services.msc`
2. Localiser **"Services de domaine Active Directory"**
3. Clic droit → **Redémarrer**

Méthode 2 — Via Server Manager :

1. Server Manager → **Outils** → **Services**
2. Localiser et redémarrer le service AD DS

> ***Attention :*** *redémarrer AD DS sur le seul DC du domaine interrompra l'authentification. Prévoir une fenêtre de maintenance.*

Mode de restauration des services d'annuaire (DSRM) :

- Démarrer le serveur → F8 → "Mode de restauration des services d'annuaire"
- Connexion avec le compte Administrateur local et le **mot de passe DSRM**
- Utilisé pour la restauration de la base NTDS.dit

---

4. Suppression d'un contrôleur de domaine

Prérequis avant de rétrograder :

- Transférer tous les rôles FSMO vers un autre DC
- S'assurer qu'un autre DC est opérationnel et répliqué

Procédure depuis Server Manager :

1. **Gérer → Supprimer des rôles et fonctionnalités**
2. Décocher **Services de domaine Active Directory**
3. Une boîte de dialogue propose de **"Rétrograder ce contrôleur de domaine"** → Cliquer
4. Assistant de rétrogradation :
    - Si dernier DC du domaine : cocher "Procéder à la suppression"
    - Cocher **"Forcer la suppression de ce contrôleur de domaine"** si le DC est inaccessible ou hors ligne
    - Cocher "Supprimer ce serveur DNS" et "Supprimer les partitions d'application"
5. Saisir le nouveau mot de passe administrateur local
6. **Rétrograder** → redémarrage automatique

> ***Si un DC est définitivement perdu*** *sans rétrogradation propre : utiliser* `ntdsutil` → `metadata cleanup` *pour supprimer manuellement les métadonnées de l'ancien DC depuis la console AD.*

---

5. Clonage d'un contrôleur de domaine virtualisé

Le clonage de DC virtualisé (supporté depuis Windows Server 2012 avec des hyperviseurs compatibles VM-GenerationID comme Hyper-V) permet de déployer rapidement des DC supplémentaires.

Prérequis :

- L'émulateur PDC doit être sur Windows Server 2012 ou supérieur
- Le DC source doit être membre du groupe **"Contrôleurs de domaine clonables"** dans l'OU `Domain Controllers`
- Vérifier les applications incompatibles

Procédure :

1. **Vérifier la compatibilité :** depuis Server Manager → Outils → **Centre d'administration Active Directory** → cliquer sur le groupe "Contrôleurs de domaine clonables" → ajouter le compte du DC source
2. **Identifier les applications incompatibles :** sur le DC source, utiliser `Get-ADDCCloningExcludedApplicationList` depuis PowerShell (liste les services qui empêchent le clonage)
3. **Créer le fichier DCCloneConfig.xml** dans `C:\Windows\NTDS` avec le nom, l'adresse IP statique et le site du nouveau DC
4. **Arrêter le DC source** (ne pas le rétrograder)
5. **Exporter la VM** depuis la console Hyper-V Manager
6. **Importer la VM exportée** avec un nouveau nom
7. **Démarrer la VM importée** : le système détecte le clonage (VM-GenerationID différent) et lance automatiquement la configuration du nouveau DC

---

6. Sécurité du système d'information

AdminSDHolder et SD Propagator :

- `AdminSDHolder` est un objet spécial dans `CN=System` qui définit un ACL de référence pour les comptes privilegiés
- Le processus `SDProp` s'exécute toutes les 60 minutes et réapplique cet ACL sur tous les membres des groupes sensibles
- Conséquence : les permissions héritées sont ignorées sur ces comptes → vérifier les permissions effectives via l'onglet "Sécurité" → Avancé → Accès effectif

Groupes sensibles à surveiller :

Groupe	Niveau de risque	Remarque
Domain Admins	Très élevé	Admin de tout le domaine
Enterprise Admins	Très élevé	Admin de toute la forêt
Schema Admins	Très élevé	Peut modifier le schéma
Administrators (local DC)	Élevé	Admin local des DC
Account Operators	Moyen	Peut créer/modifier des comptes
Backup Operators	Moyen	Peut contourner les permissions fichiers

Bonnes pratiques de sécurité (Tiering Model) :

- **Tier 0** : comptes d'administration des DC, AD, infrastructure d'identité — jamais utilisés pour autre chose
- **Tier 1** : comptes d'administration des serveurs applicatifs
- **Tier 2** : comptes d'administration des postes de travail
- Chaque administrateur dispose d'un **compte courant non-privilégié** (emails, navigation) et d'un **compte admin dédié** par tier
- **PAW (Privileged Access Workstation)** : poste dédié pour les tâches d'administration Tier 0

---

7. Sécurisation du service DNS

Mises à jour dynamiques sécurisées :

1. Ouvrir **dnsmgmt.msc**
2. Déployer les Zones de recherche directe → clic droit sur la zone → **Propriétés**
3. Onglet **Général** → "Mises à jour dynamiques" → sélectionner **"Sécurisées uniquement"**
4. Cette option n'est disponible que si la zone est **intégrée à Active Directory**

Vieillissement et nettoyage des enregistrements obsolètes :

1. Dans **dnsmgmt.msc** → clic droit sur le serveur DNS → **"Définir le vieillissement/nettoyage pour toutes les zones"**
2. Cocher **"Nettoyer les enregistrements de ressources obsolètes"**
3. Configurer :
    - Période sans actualisation : 7 jours (les enregistrements récents ne sont pas nettoyés)
    - Période d'actualisation : 7 jours (après ce délai, l'enregistrement peut être supprimé)
4. Activer aussi sur chaque zone individuellement : clic droit zone → Propriétés → onglet Général → **Vieillissement**

---

8. Mise à niveau d'un contrôleur de domaine 2012 R2 vers 2022

Étape 1 — Préparer le schéma sur l'ancien DC :

1. Insérer le DVD / monter l'ISO Windows Server 2022 sur l'ancien DC
2. Dans une invite de commandes élevée sur le DC hébergeant le **Maître de schéma** :
    - `adprep /forestprep` → valide la mise à jour du schéma pour la forêt
    - `adprep /domainprep` → prépare chaque domaine (à exécuter sur le DC hébergeant l'Émulateur PDC de chaque domaine)

Étape 2 — Installer un nouveau DC Windows Server 2022 :

- Installer Windows Server 2022 sur un nouveau serveur
- Rejoindre le domaine existant

- Promouvoir comme DC supplémentaire (cf. §2 ci-dessus)
- Vérifier la réplication : **Outils → Sites et services Active Directory (ntdssite.msc)** → clic droit sur le lien de connexion → Répliquer maintenant

Étape 3 — Transférer les rôles FSMO vers le nouveau DC :

Rôle	Console	Procédure
Maître de schéma	Schéma Active Directory (schmmgmt.msc — à enregistrer)	Clic droit sur "Maître de schéma" → Modifier le maître de schéma
Maître de nommage	dsa.msc (AD Users & Computers)	Menu Action → Maîtres d'opérations → onglet UPN/DNS
RID Master	dsa.msc	Menu Action → Maîtres d'opérations → onglet RID
Émulateur PDC	dsa.msc	Menu Action → Maîtres d'opérations → onglet PDC
Maître d'infrastructure	dsa.msc	Menu Action → Maîtres d'opérations → onglet Infrastructure

Pour les rôles de site : **ntdssite.msc** → clic droit sur le serveur → Maître d'opérations

Étape 4 — Rétrograder l'ancien DC 2012 R2 :

- Cf. §4 — procédure de suppression d'un contrôleur de domaine

Étape 5 — Élever le niveau fonctionnel :

1. **dsa.msc** → clic droit sur le domaine → **Élever le niveau fonctionnel du domaine** → Windows Server 2016 (ou 2022 si supporté)
2. **dsa.msc** → clic droit sur "Active Directory - Utilisateurs et ordinateurs" → **Élever le niveau fonctionnel de la forêt**

> ***Attention :*** *l'élévation du niveau fonctionnel est irréversible.*

---

9. Utilisation d'Azure Active Directory (Entra ID)

Différences AD local vs Azure AD (Entra ID) :

Critère	AD DS (on-premise)	Azure AD / Entra ID
Protocole d'authentification	Kerberos, NTLM	OAuth 2.0, OpenID Connect, SAML
Protocole d'annuaire	LDAP	API REST (Microsoft Graph)
Objets gérés	Utilisateurs, ordinateurs, groupes, GPO, OU	Utilisateurs, groupes, applications, appareils
Jonction de domaine	Oui (classique)	Azure AD Join / Hybrid Join
GPO	Oui	Non (remplacé par Intune / Endpoint Manager)
MFA natif	Non (RADIUS/NPS nécessaire)	Oui (natif)
Accès conditionnel	Non	Oui (Conditional Access)

Azure AD Connect : Outil Microsoft permettant de synchroniser l'AD local vers Entra ID.

Types de synchronisation :

Méthode	Description	Cas d'usage
Synchronisation de hachage de mot de passe (PHS)	Le hash du mot de passe est synchronisé vers Azure AD	Recommandé, simple, résilient
Authentification directe (PTA)	L'authentification est renvoyée vers les DC on-premise	Pas de hash dans le cloud, conformité
Fédération ADFS	Serveur ADFS dédié gère l'authentification	Scénarios complexes, SSO avancé

Installation d'Azure AD Connect :

1. Télécharger **Azure AD Connect** depuis le Centre de téléchargement Microsoft
2. Installer sur un serveur membre (pas un DC — recommandation Microsoft)
3. Choisir la configuration : **Express** (PHS, domaine unique) ou **Personnalisée**
4. Saisir les identifiants Azure AD (compte Global Administrator)
5. Saisir les identifiants AD local (compte Enterprise Admin)
6. Configurer le filtrage (par OU ou domaine) si nécessaire
7. Lancer la synchronisation initiale

> ***Entra ID** est le nouveau nom commercial d'Azure Active Directory depuis juillet 2023. Les fonctionnalités restent identiques mais la terminologie évolue (ex : Entra ID P1/P2 remplace Azure AD Premium P1/P2).*

Chapitre 2 : Console Gestionnaire de serveur

1. Le Gestionnaire de serveur

Le **Gestionnaire de serveur (Server Manager)** est la console de gestion centrale de Windows Server, accessible depuis la barre des tâches ou via `servermanager.exe`.

Tableau de bord :

- Résumé des rôles installés avec indicateurs d'état (vert = OK, rouge = alerte)
- Compteurs d'événements récents (Erreur, Avertissement) par rôle
- Alertes de services et de performances
- Accès rapide aux tâches de configuration post-déploiement

Ajouter des serveurs distants pour administration centralisée :

1. Server Manager → **Gérer → Ajouter des serveurs**
2. Onglet **Active Directory** : rechercher par nom ou attribut AD
3. Onglet **DNS** : rechercher par nom DNS
4. Onglet **Importer** : importer une liste de noms depuis un fichier .txt

5. Les serveurs ajoutés apparaissent dans le panneau "Tous les serveurs"

Créer des groupes de serveurs personnalisés :

1. Gérer → **Créer un groupe de serveurs**
2. Nommer le groupe (ex : "Serveurs DNS Production")
3. Ajouter les serveurs membres depuis l'annuaire ou la liste

Vue par rôle :

- Le panneau gauche affiche chaque rôle installé (DNS, DHCP, AD DS, Services de fichiers...)
- Cliquer sur un rôle affiche tous les serveurs hébergeant ce rôle avec leurs événements spécifiques

> ***Prérequis pour gérer un serveur distant :*** *WinRM doit être activé sur le serveur cible (`winrm quickconfig`), le pare-feu doit autoriser la gestion à distance, et les identifiants d'admin doivent être disponibles.*

---

2. Serveur en mode installation minimale (Core)

Windows Server Core est une installation sans interface graphique complète (pas d'explorateur, pas de bureau), uniquement une invite de commandes (cmd) et PowerShell.

Comparatif Server Core vs Expérience utilisateur (Desktop Experience) :

Critère	Server Core	Avec interface graphique
Surface d'attaque	Réduite (moins de composants)	Plus large
Mémoire RAM utilisée	~1 Go de moins	Plus élevée
Fréquence des mises à jour	Moins nombreuses	Plus nombreuses (GUI components)
Redémarrages nécessaires	Moins fréquents	Plus fréquents
Administration locale	Ligne de commande uniquement	MMC, GUI possible
Administration distante	Obligatoire (RSAT, WAC, PSRemoting)	Possible localement et à distance
Recommandé pour	Production, sécurité maximale	Lab, développement, test
Empreinte disque	Réduite	Normale

Convertir entre Core et GUI (Windows Server 2019+) :

- L'interface graphique peut être ajoutée/retirée sans réinstallation via **fonctionnalités** (Expérience utilisateur du serveur)

---

3. Installation de rôles en mode Core

Outil sconfig : Taper `sconfig` dans l'invite de commandes → menu texte interactif numéroté :

Option	Action
1	Domaine/Groupe de travail
2	Nom de l'ordinateur
3	Ajouter un administrateur local
4	Configurer la mise à jour (Windows Update)
5	Paramètres de mise à jour
6	Télécharger et installer les mises à jour
7	Activer le Bureau à distance
8	Paramètres réseau (IP, DNS, passerelle)
9	Date et heure
10	Télémétrie
11	Activer la gestion à distance
12	Informations sur le serveur
13	Déconnexion
14	Redémarrer le serveur
15	Arrêter le serveur
16	Quitter (retour à l'invite)

Administration depuis Server Manager à distance :

1. Sur le serveur d'administration (avec GUI), ouvrir **Server Manager**
2. Gérer → Ajouter des serveurs → rechercher le serveur Core
3. Une fois ajouté, le serveur Core apparaît dans "Tous les serveurs"
4. Clic droit → Ajouter des rôles et fonctionnalités → exécuté à distance sur le Core
5. Les MMC (dnsmgmt.msc, dhcpmgmt.msc, dsa.msc...) pointent sur le serveur Core distant

Windows Admin Center :

- Alternative graphique web moderne pour gérer un serveur Core
- Connexion HTTPS depuis n'importe quel navigateur compatible
- Pas besoin d'installer RSAT sur chaque poste d'administration

---

4. Suppression du groupe de serveurs

1. Dans Server Manager → panneau gauche → clic droit sur le **groupe de serveurs personnalisé** à supprimer
2. Sélectionner **"Supprimer le groupe de serveurs"**
3. Confirmer la suppression

> ***Important :*** *cette action supprime uniquement le regroupement logique dans Server Manager. Les serveurs eux-mêmes ne sont pas affectés, ils restent dans "Tous les serveurs" et continuent de fonctionner normalement.*

Pour retirer un serveur de la liste "Tous les serveurs" : clic droit sur le serveur → **Supprimer le serveur**. Cela ne désinstalle rien sur le serveur distant.

---

5. Les conteneurs Windows

Les conteneurs permettent d'isoler des applications dans des environnements légers et reproductibles.

Deux modes d'isolation :

Mode	Isolation	Noyau partagé	Usage
Conteneurs de processus Windows (WC)	Par processus et espace de noms	Oui (noyau hôte)	Développement, microservices, CI/CD
Conteneurs Hyper-V	Par VM légère	Non (noyau isolé)	Production, multi-tenant, sécurité renforcée

Images de base Microsoft :

- **Windows Server Core** : image complète avec .NET Framework — plus lourde (~5 Go) mais compatible avec la plupart des apps Windows
- **Nano Server** : image ultra-légère — optimisée pour les microservices .NET Core, pas d'interface MMC
- **Windows** : image complète avec GUI components

Docker Desktop sur Windows Server :

1. Server Manager → Ajouter des fonctionnalités → **Conteneurs**
2. Installer Docker Engine (depuis PowerShell ou via le programme d'installation Docker Enterprise)
3. Commandes de base depuis l'invite : `docker pull`, `docker run`, `docker ps`, `docker build`
4. Orchestration : intégration avec **Kubernetes** ou **Docker Swarm**

---

6. Windows Admin Center (WAC)

Windows Admin Center est une interface web de gestion unifiée qui remplace ou complète les MMC traditionnelles.

Installation :

1. Télécharger **Windows Admin Center** depuis `aka.ms/WindowsAdminCenter`
2. Choisir le mode de déploiement :
    - **Mode passerelle (Gateway)** : installation sur un serveur Windows dédié, accès multi-utilisateurs via navigateur — recommandé en production
    - **Mode bureau (Desktop)** : installation sur un poste Windows 10/11, accès local uniquement — pour les administrateurs individuels
3. Lancer le MSI → suivre l'assistant → choisir le port HTTPS (443 pour gateway, 6516 pour desktop)
4. Configurer le certificat SSL (auto-signé par défaut, remplacer par un certificat d'entreprise en production)

Accès :

- Mode gateway : `https://nom-serveur-wac` ou `https://IP:443`
- Mode desktop : `https://localhost:6516`
- Navigateurs supportés : Microsoft Edge (recommandé), Chrome, Firefox

Fonctionnalités principales :

Module	Fonctionnalité
Vue d'ensemble	CPU, mémoire, réseau, disques en temps réel
Disques	Gestion des volumes, partitions, espaces de stockage
Réseau	Configuration des cartes, routes, pare-feu
Rôles et fonctionnalités	Ajouter/supprimer sans quitter le navigateur
Services	Démarrer, arrêter, redémarrer les services Windows
Registre	Naviguer et modifier les clés de registre
Planificateur de tâches	Voir et gérer les tâches planifiées
Hyper-V	Gérer les VM si le rôle est installé
PowerShell	Terminal PowerShell intégré dans le navigateur
Bureau à distance	Connexion RDP dans le navigateur (extension)
Mises à jour	Gérer Windows Update directement

> ***Avantage clé :*** *WAC fonctionne sans VPN ni RSAT sur le poste client — un simple navigateur suffit. Il supporte aussi la gestion des clusters Hyper-V et des clusters de basculement.*

Chapitre 3 : Gestion des objets Active Directory

1. Le compte utilisateur

Création d'un compte utilisateur depuis dsa.msc :

1. `Windows + R` → `dsa.msc` (Utilisateurs et ordinateurs Active Directory)
2. Déployer le domaine → naviguer jusqu'à l'**OU cible**
3. Clic droit sur l'OU → **Nouveau → Utilisateur**
4. Remplir le formulaire :
    - Prénom, Initiales, Nom
    - Nom complet (généré automatiquement)
    - **Nom d'ouverture de session (UPN)** : `prenom.nom@nouvy.lan`
    - Nom d'ouverture de session pré-Windows 2000 : `NOUVYprenom.nom`
5. Page suivante — définir le mot de passe et les options :

Option	Description
L'utilisateur doit changer le mot de passe à la prochaine ouverture	Bonne pratique pour les nouveaux comptes
L'utilisateur ne peut pas changer le mot de passe	Comptes de service
Le mot de passe n'expire jamais	Comptes de service (avec justification)
Le compte est désactivé	Création anticipée de comptes

Propriétés détaillées du compte :

Onglet	Contenu notable
Général	Nom, prénom, description, bureau, téléphone, email
Compte	UPN, options de mot de passe, expiration du compte, heures d'ouverture de session autorisées
Profil	Chemin du profil itinérant, script d'ouverture de session, dossier de base
Téléphones	Téléphone domicile, mobile, télécopie
Organisation	Intitulé du poste, service, société, nom du responsable
Membre de	Groupes de sécurité dont le compte est membre
Appel entrant	Permissions d'accès distant (VPN, RAS)
Environnement / Sessions / Contrôle à distance	Paramètres Services Bureau à distance

Modèle de compte (Template) :

- Créer un utilisateur "modèle" avec le préfixe `_` (ex : `_Modele_Comptable`)
- Le désactiver → configurer ses groupes, profil, paramètres de compte
- Pour créer un compte similaire : clic droit sur le modèle → **Copier**
- Les groupes, paramètres de compte, chemin de profil (partiellement) sont copiés
- Seuls le nom, prénom et mot de passe sont à saisir

Opérations courantes :

- **Désactivation** : clic droit sur le compte → **Désactiver le compte** (icône flèche vers le bas)
- **Réactivation** : clic droit → **Activer le compte**
- **Réinitialisation mot de passe** : clic droit → **Réinitialiser le mot de passe**
- **Déverrouillage** : ouvrir les propriétés → onglet **Compte** → décocher **"Le compte est verrouillé"**
- **Déplacement** : clic droit → **Déplacer** → sélectionner l'OU de destination

---

2. Les groupes dans Active Directory

Types de groupes :

- **Groupe de sécurité** : utilisé pour attribuer des permissions sur des ressources (dossiers partagés, imprimantes, GPO...) et comme liste de distribution
- **Groupe de distribution** : uniquement pour les listes de diffusion email (Exchange/Microsoft 365) — pas de permissions de sécurité

Étendues des groupes :

Étendue	Membres acceptés	Peut être utilisé dans
Local de domaine	Utilisateurs, ordinateurs, groupes globaux et universels de n'importe quel domaine, groupes locaux du même domaine	Ressources du domaine local uniquement
Globale	Utilisateurs, ordinateurs, groupes globaux du même domaine	N'importe quel domaine de la forêt
Universelle	Utilisateurs, ordinateurs, groupes globaux et universels de n'importe quel domaine	N'importe quel domaine de la forêt

Stratégie AGDLP (bonne pratique recommandée par Microsoft) :

- **A**ccount → **G**lobal group → **D**omain **L**ocal group → **P**ermission
- Les comptes utilisateurs sont membres de groupes globaux (par rôle ou département)
- Les groupes globaux sont membres de groupes locaux de domaine (par ressource)
- Les permissions sont attribuées aux groupes locaux de domaine

Groupes par défaut importants :

Groupe	Emplacement	Rôle
Domain Admins	CN=Users	Administrateurs complets du domaine
Enterprise Admins	CN=Users	Administrateurs de toute la forêt
Schema Admins	CN=Users	Modification du schéma AD
Domain Users	CN=Users	Groupe primaire de tous les utilisateurs
Domain Computers	CN=Users	Tous les ordinateurs membres du domaine
Domain Controllers	OU=Domain Controllers	Tous les contrôleurs de domaine
Group Policy Creator Owners	CN=Users	Peut créer et modifier des GPO
Protected Users	CN=Users	Protection renforcée contre vol de credentials

Créer un groupe depuis dsa.msc :

1. Clic droit sur l'OU → **Nouveau → Groupe**
2. Nom du groupe, nom pré-Windows 2000
3. Étendue : Domaine local / Globale / Universelle
4. Type : Sécurité / Distribution
5. Après création → onglet **Membres** → **Ajouter** pour ajouter des membres

---

3. Le compte ordinateur

Jonction d'un poste au domaine (Windows 10/11) :

1. Clic droit sur **"Ce PC"** → **Propriétés**
2. Cliquer sur **"Modifier les paramètres"** (ou "Domaine ou groupe de travail" selon la version)
3. Onglet **Nom de l'ordinateur** → **Modifier**
4. Sélectionner **"Membre d'un domaine"** → saisir le nom du domaine (ex : `nouvy.lan`)
5. Saisir les identifiants d'un compte ayant le droit de joindre des machines au domaine (par défaut : Domain Admins ou délégation spécifique)
6. Message de bienvenue dans le domaine → Redémarrer

> ***Bonne pratique :*** *déléguer le droit de joindre des machines à un groupe spécifique (ex : HelpDesk) plutôt que d'utiliser Domain Admins, et limiter le nombre de machines qu'un compte non-admin peut joindre (attribut `ms-DS-MachineAccountQuota`, défaut = 10).*

Pré-création d'un compte ordinateur dans dsa.msc :

1. Clic droit sur l'OU cible → **Nouveau → Ordinateur**
2. Saisir le nom de l'ordinateur (doit correspondre exactement au nom réseau)
3. Optionnel : spécifier qui peut joindre cet ordinateur au domaine

Réinitialisation du compte ordinateur (relation domaine brisée) :

- Symptôme : "La relation d'approbation entre ce poste de travail et le domaine principal a échoué"
- Solution sans rejoindre le domaine : clic droit sur le compte ordinateur dans dsa.msc → **Réinitialiser le compte**
- Puis sur le poste : se connecter avec un compte local admin → retirer du domaine → rejoindre le domaine

---

4. La corbeille Active Directory

La **Corbeille AD** permet de restaurer des objets supprimés sans restauration de sauvegarde, en conservant tous leurs attributs.

Activation de la Corbeille AD (opération irréversible) :

Prérequis : niveau fonctionnel du domaine et de la forêt ≥ Windows Server 2008 R2

1. Ouvrir **Outils → Centre d'administration Active Directory**
2. Dans le panneau de gauche, cliquer sur le **nom du domaine** (ex : nouvy (local))
3. Dans le volet **Tâches** à droite → cliquer sur **"Activer la corbeille..."**
4. Message d'avertissement → **OK** pour confirmer
5. Cliquer sur **Actualiser** (F5) dans le Centre d'administration AD

Restauration d'un objet supprimé :

1. Dans le Centre d'administration AD → déployer le domaine dans le panneau gauche
2. Cliquer sur le conteneur **"Deleted Objects"** (Objets supprimés)
3. Localiser l'objet (utiliser le champ de recherche si nécessaire)
4. Clic droit sur l'objet → **"Restaurer"** (restaure dans l'OU d'origine) ou **"Restaurer vers..."** (choisir une OU de destination)
5. Vérifier que l'objet est bien restauré avec tous ses attributs et groupes d'appartenance

Paramètres de conservation :

- Durée de conservation par défaut : **180 jours** (paramètre `msDS-deletedObjectLifetime`)
- Après cette période, l'objet passe en "recycled" puis est définitivement purgé
- Modifier la durée : via ADSI Edit → CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration

> ***Limitation :*** *si la Corbeille AD n'est pas activée, la restauration nécessite une sauvegarde (Windows Server Backup + restauration faisant autorité avec ntdsutil).*

Chapitre 4 : Implémentation d'un serveur DHCP

1. Rôle et fonctionnement du service DHCP

Le protocole **DHCP (Dynamic Host Configuration Protocol)** permet l'attribution automatique de configurations réseau aux clients (adresse IP, masque, passerelle, DNS, suffixe DNS...).

Processus DORA (négociation DHCP) :

Étape	Message	Type	Description
1	DISCOVER	Broadcast (255.255.255.255)	Le client diffuse sur tout le réseau pour trouver un serveur DHCP
2	OFFER	Broadcast/Unicast	Le serveur propose une adresse IP disponible avec les options
3	REQUEST	Broadcast	Le client accepte l'offre et demande officiellement cette adresse (informe les autres serveurs)
4	ACKNOWLEDGE	Broadcast/Unicast	Le serveur confirme, attribue l'adresse et envoie toutes les options DHCP

Bail DHCP (Lease) :

- Durée par défaut : **8 jours**
- Le client tente de renouveler à **T1 = 50%** de la durée (4 jours) en contactant directement son serveur DHCP
- Si échec, tente à **T2 = 87,5%** (7 jours) en broadcast
- Si toujours échec à l'expiration : le client arrête d'utiliser l'adresse

Options DHCP importantes :

Code	Option	Exemple
003	Routeur (passerelle par défaut)	192.168.1.1
006	Serveurs DNS	192.168.1.10, 192.168.1.11
015	Nom de domaine DNS	nouvy.lan
043	Options spécifiques fournisseur	Paramètres VoIP, PXE
066	Nom de l'hôte serveur de démarrage	Serveur WDS/PXE
067	Nom du fichier de démarrage	PXE boot file

---

2. Installation et configuration du rôle DHCP

Installation depuis Server Manager :

1. **Gérer → Ajouter des rôles et fonctionnalités**
2. Type d'installation → basée sur un rôle → sélectionner le serveur
3. Cocher **"Serveur DHCP"** → ajouter les fonctionnalités → Suivant → Installer
4. Après installation : cliquer sur **"Configuration post-déploiement DHCP"**

(notification jaune)

5. → **Autoriser le serveur DHCP dans Active Directory** (nécessite des identifiants d'admin de domaine)

> *Un serveur DHCP non autorisé dans AD est automatiquement arrêté si un DC est détecté sur le réseau.*

Configuration d'une étendue depuis dhcpmgmt.msc :

1. `Windows + R` → `dhcpmgmt.msc`
2. Clic droit sur le serveur → **"Nouvelle étendue"** → assistant
3. **Nom et description** : ex. "LAN-Bureau" / "Réseau bureau principal"
4. **Plage d'adresses IP** : ex. Début `192.168.1.100` → Fin `192.168.1.200`, Masque `255.255.255.0`
5. **Exclusions et délai** : exclure les adresses réservées pour les équipements fixes (ex : `.1` à `.99`)
6. **Durée du bail** : 8 jours (réseau filaire stable) — réduire à 2h-4h pour les réseaux Wi-Fi publics
7. **Configurer les options DHCP maintenant** :
   - Option 003 (Routeur) : `192.168.1.1`
   - Option 006 (Serveurs DNS) : `192.168.1.10`
   - Option 015 (Nom de domaine) : `nouvy.lan`
8. **Activer l'étendue** : Oui

Réservations DHCP (adresse fixe par MAC) :

1. Déployer l'étendue → clic droit **"Réservations" → Nouvelle réservation**
2. Nom, adresse IP à réserver, adresse MAC du client (sans tirets)
3. Type : DHCP uniquement / BOOTP uniquement / Les deux

---

3. Base de données du service DHCP

Emplacement et fichiers :

Fichier	Rôle
`C:WindowsSystem32dhcpdhcp.mdb`	Base de données principale (format JET/ESE)
`C:WindowsSystem32dhcpj50.log`	Journal des transactions actif
`C:WindowsSystem32dhcpj50*.log`	Journaux de transactions archivés
`C:WindowsSystem32dhcp mp.edb`	Fichier temporaire

Sauvegarde de la base DHCP :

- `dhcpmgmt.msc` → clic droit sur le serveur → **"Sauvegarder"**
- Choisir un dossier de destination (par défaut : `C:WindowsSystem32dhcp□ackup`)
- La sauvegarde inclut la base, les étendues, les réservations et les options
- Planifier la sauvegarde automatique : intervalle configurable dans le registre (défaut : toutes les 60 minutes)

Restauration :

- `dhcpmgmt.msc` → clic droit sur le serveur → **"Restaurer"**
- Le service DHCP est arrêté automatiquement pendant la restauration, puis redémarré

Conciliation des étendues :

- Clic droit sur l'étendue → **"Concilier"** (Reconcile)
- Vérifie la cohérence entre la base DHCP et le registre → corrige les incohérences
- Utile après une restauration ou en cas de comportement anormal

---

4. Haute disponibilité du service DHCP

Configuration du basculement DHCP (DHCP Failover) :

Depuis **dhcpmgmt.msc** sur le serveur DHCP primaire :

1. Clic droit sur l'étendue → **"Configurer le basculement"**
2. Cliquer sur **Ajouter un serveur** → saisir le nom ou l'IP du serveur partenaire
3. Choisir le **mode de basculement** :

Mode	Description	Cas d'usage
Équilibrage de charge (Hot Standby)	Les deux serveurs répondent aux requêtes DHCP (ratio configurable, défaut 50/50)	Haute disponibilité active-active
Secours (Failover)	Le serveur secondaire ne répond que si le primaire est indisponible	Sites distants, économie de ressources

4. **Paramètres avancés :**
   - **Délai MCLT** (Maximum Client Lead Time) : 1 heure par défaut — durée pendant laquelle le secondaire peut attribuer des baux sans contact avec le primaire
   - **Intervalle de basculement d'état** : délai avant que le partenaire soit déclaré hors ligne
   - **Nom du partenariat** : identifiant unique de la relation
   - **Secret partagé** : pour sécuriser la communication entre les deux serveurs DHCP

> ***Prérequis :*** *les deux serveurs DHCP doivent être autorisés dans AD et joignables l'un par l'autre. Le basculement réplique automatiquement les étendues, réservations et options vers le partenaire.*

---

5. Gestion du DHCP en PowerShell

Voir **Chapitre 15 — PowerShell** pour les commandes `Add-DhcpServerv4Scope`, `Get-DhcpServerv4Lease`, `Set-DhcpServerv4OptionValue`, etc.

---

6. IPAM (IP Address Management)

IPAM est une fonctionnalité Windows Server permettant la gestion centralisée de l'espace d'adressage IP, des serveurs DHCP et DNS de l'organisation.

Installation :

1. Server Manager → **Gérer → Ajouter des fonctionnalités**
2. Cocher **"Gestion des adresses IP (IPAM)"** → Installer

Configuration initiale :

1. Server Manager → **IPAM** → lancer l'**Assistant de provisionnement IPAM**
2. Méthode de provisionnement : **Stratégie de groupe** (recommandé) ou Manuelle
3. Préfixe GPO : saisir un préfixe (ex : `IPAM`) → des GPO sont créées automatiquement pour configurer les serveurs DHCP/DNS gérés
4. Découverte des serveurs : définir le périmètre (forêt/domaines) → lancer la découverte
5. Sélectionner les serveurs à gérer → les ajouter à la gestion IPAM

Fonctionnalités de la console IPAM :

- Vue de l'utilisation des plages IP (pourcentage d'utilisation, seuils d'alerte)
- Historique des baux DHCP (qui avait quelle IP et quand)
- Suivi des adresses IP (association IP ↔ nom d'hôte ↔ utilisateur ↔ MAC)
- Gestion unifiée de plusieurs serveurs DHCP/DNS depuis une seule console
- Rapports d'utilisation et d'audit

---

7. Attribution fondée sur une stratégie (Policy-Based Assignment)

Cette fonctionnalité permet d'attribuer des plages d'adresses et des options DHCP différentes selon des critères identifiant le client.

Configuration depuis dhcpmgmt.msc :

1. Déployer une étendue → clic droit sur **"Stratégies"** → **"Nouvelle stratégie"**
2. **Nom de la stratégie** : ex. "Imprimantes réseau", "Téléphones VoIP", "Serveurs"
3. **Conditions** (combinables avec ET/OU) :

Critère	Exemple
Adresse MAC	Commence par `00:11:22` (préfixe OUI du fabricant)
Classe d'utilisateur	DHCP User Class définie par le client
Classe fournisseur	Identifiant du type de matériel
Nom d'ordinateur	Contient "PRINT", commence par "SRV"
Identificateur client	Valeur personnalisée

4. **Plage d'adresses dédiée** à cette stratégie (doit être dans la plage de l'étendue parente)
5. **Options spécifiques** : passerelle différente, DNS différent, durée de bail différente

> ***Exemple typique :*** *attribuer les adresses `.200`–`.220` aux imprimantes identifiées par leur OUI MAC, avec une durée de bail de 30 jours et pas de passerelle.*

Chapitre 5 : Les services réseau sous Windows Server

1. Introduction à l'adressage IPv4

Configuration d'une carte réseau depuis le panneau de configuration :

Panneau de configuration → Centre Réseau et partage → **"Modifier les paramètres de la carte"** → clic droit sur la carte → **Propriétés** → double-clic sur **"Protocole Internet version 4 (TCP/IPv4)"**

Paramètre	Description	Exemple
Adresse IP	Identifiant unique de l'interface	192.168.1.10
Masque de sous-réseau	Délimite la partie réseau et hôte	255.255.255.0
Passerelle par défaut	Routeur pour les communications hors du sous-réseau	192.168.1.1
Serveur DNS préféré	Premier serveur DNS interrogé	192.168.1.10
Serveur DNS auxiliaire	Utilisé si le préféré est indisponible	192.168.1.11

Classes d'adresses privées (RFC 1918) :

Classe	Plage	Masque par défaut	Nombre d'hôtes	Utilisation
A	10.0.0.0 – 10.255.255.255	/8 (255.0.0.0)	~16 millions	Très grands réseaux d'entreprise
B	172.16.0.0 – 172.31.255.255	/16 (255.255.0.0)	~65 000	Réseaux de taille moyenne
C	192.168.0.0 – 192.168.255.255	/24 (255.255.255.0)	254	Petits réseaux, TPE, domicile

Adresses spéciales importantes :

- `127.0.0.1` : loopback (test de la pile TCP/IP locale)
- `169.254.x.x` : APIPA (Auto-configuration quand aucun DHCP n'est disponible)
- `255.255.255.255` : broadcast limité
- `0.0.0.0` : route par défaut

CIDR — Notation préfixe :

Notation CIDR	Masque	Hôtes disponibles
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14

---

2. Introduction à l'IPv6

L'IPv6 utilise des adresses de **128 bits** notées en hexadécimal séparés par des `:` (ex : `2001:0db8:85a3:0000:0000:8a2e:0370:7334`). Les groupes de zéros consécutifs peuvent être remplacés par `::` (une seule fois).

Types d'adresses IPv6 :

Type	Préfixe	Exemple	Caractéristique
Lien-local	fe80::/10	fe80::1	Non routable, automatiquement configurée, scope du lien uniquement
Globale unicast	2000::/3	2001:db8::1	Équivalent IPv4 public, routable sur Internet
Loopback	::1/128	::1	Équivalent de 127.0.0.1 en IPv4
Multicast	ff00::/8	ff02::1 (tous nœuds), ff02::2 (tous routeurs)	Remplace le broadcast IPv4
Unicast site-local	fec0::/10	Déprécié	Remplacé par les adresses locales uniques
Locale unique	fc00::/7	fd00::1	Équivalent RFC 1918, routage privé

Mécanismes de configuration IPv6 :

- **SLAAC** (Stateless Address Autoconfiguration) : le client génère automatiquement son adresse à partir du préfixe annoncé par le routeur (RA — Router Advertisement) et de son adresse MAC (EUI-64)
- **DHCPv6** : attribution stateful d'adresses IPv6 (comme DHCP pour IPv4)
- **Configuration manuelle** : Propriétés carte réseau → Protocole Internet version 6 (TCP/IPv6) → saisir l'adresse, préfixe, passerelle, DNS

---

3. Configuration du Centre Réseau et partage

Accès : Panneau de configuration → **Centre Réseau et partage**

Profils réseau et implications de sécurité :

Profil	Contexte d'application	Partage de fichiers	Découverte réseau	Pare-feu
Domaine	Réseau d'entreprise avec DC détecté	Configuré par GPO	Configuré par GPO	Règles GPO
Privé	Réseau de confiance choisi manuellement	Activé par défaut	Activé	Moins restrictif
Public	Réseau inconnu (Wi-Fi café, hôtel...)	Désactivé	Désactivé	Plus restrictif

Paramètres de partage avancés (lien dans le panneau gauche) :

- Activer/désactiver la découverte réseau par profil
- Activer/désactiver le partage de fichiers et d'imprimantes
- Configurer le partage de dossier public
- Partage protégé par mot de passe

Diagnostics réseau :

- Lien **"Résoudre les problèmes"** → lance l'utilitaire de diagnostic automatique
- Identifie les problèmes courants (carte désactivée, pas de passerelle, DNS non répondant...)

---

4. La norme 802.11 (Wi-Fi)

Standards Wi-Fi et leurs caractéristiques :

Standard	Bande de fréquence	Débit max théorique	Portée indicative	Certification Wi-Fi
802.11a	5 GHz uniquement	54 Mbps	~35 m intérieur	—
802.11b	2,4 GHz uniquement	11 Mbps	~38 m intérieur	—
802.11g	2,4 GHz uniquement	54 Mbps	~38 m intérieur	—
802.11n	2,4 GHz et 5 GHz	600 Mbps (MIMO 4x4)	~70 m intérieur	Wi-Fi 4
802.11ac	5 GHz uniquement	6,9 Gbps (MU-MIMO)	~35 m intérieur	Wi-Fi 5
802.11ax	2,4, 5 et 6 GHz	9,6 Gbps (OFDMA)	~30 m intérieur	Wi-Fi 6 / 6E
802.11be	2,4, 5 et 6 GHz	46 Gbps	—	Wi-Fi 7

Protocoles de sécurité Wi-Fi :

Protocole	Chiffrement	Authentification	Recommandation
WEP	RC4	Clé partagée	Obsolète — ne pas utiliser
WPA	TKIP	PSK ou 802.1X	Obsolète
WPA2-Personal	AES-CCMP	Clé pré-partagée (PSK)	Acceptable pour usage domestique
WPA2-Enterprise	AES-CCMP	802.1X (certificats/RADIUS)	Recommandé en entreprise
WPA3-Personal	SAE	—	Recommandé
WPA3-Enterprise	AES-256-GCMP	802.1X renforcé	Recommandé

---

5. Présentation des fonctionnalités de sécurité réseau

NPS (Network Policy Server) :

- Rôle Windows Server qui implémente un serveur **RADIUS** (Remote Authentication Dial-In User Service)
- Centralise l'authentification et l'autorisation pour les connexions VPN, Wi-Fi 802.1X, commutateurs managés
- Installation : Server Manager → Ajouter des rôles → **Stratégie réseau et services d'accès → Serveur NPS**
- Console `nps.msc` : configurer les clients RADIUS (commutateurs, bornes Wi-Fi), les stratégies réseau (conditions, contraintes, paramètres)

802.1X — Authentification réseau par port :

- Le commutateur managé ou la borne Wi-Fi joue le rôle de **NAS (Network Access Server) / Authentificateur**
- Le client (supplicant) présente ses identifiants via **EAP** (Extensible Authentication Protocol)
- Le NAS transmet au serveur **NPS (RADIUS)** qui valide contre AD
- En cas de succès : le port est autorisé ; en cas d'échec : redirection vers un VLAN de quarantaine
- Protocoles EAP courants : EAP-TLS (certificats mutuels — le plus sécurisé), PEAP-MSCHAPv2 (certificat serveur + mot de passe)

NAP (Network Access Protection) :

- Vérifie la conformité des postes clients avant de les autoriser sur le réseau (mises à jour, antivirus, pare-feu activé)
- Déprécié depuis Windows Server 2012 R2 — remplacé par des solutions MDM et Intune

---

6. Équilibrage de charge réseau (NLB)

Le **NLB (Network Load Balancing)** permet de répartir le trafic réseau entrant entre

plusieurs serveurs pour améliorer la disponibilité et les performances.

Depuis nlbmgr.exe (Gestionnaire NLB) :

1. **Cluster → Nouveau** → saisir le nom ou l'IP du premier hôte membre
2. Configurer les **paramètres du cluster** :
    - **Adresse IP virtuelle** (VIP) du cluster : adresse partagée accessible aux clients
    - **Masque de sous-réseau**
    - **Nom Internet complet** (FQDN du cluster)
    - **Mode d'opération** :
        - **Monodiffusion (Unicast)** : tous les hôtes partagent une MAC virtuelle — trafic interne entre hôtes via un switch recommandé (problème de communication hôte à hôte)
        - **Multidiffusion (Multicast)** : chaque hôte conserve sa MAC — évite les problèmes unicast
3. **Règles de port** : définir les ports gérés par le NLB (ex : 80, 443), le protocole (TCP/UDP), le mode de filtrage :
    - **Hôte unique** : un seul hôte gère ce port (failover)
    - **Hôtes multiples** : répartition entre les hôtes
    - **Désactivé** : le cluster ne gère pas ce port
4. **Affinité client** :
    - **Aucune** : les requêtes sont distribuées sans considération du client (sessions sans état)
    - **Unique** : même client → même hôte (sessions avec état, ex : applications non distribuées)
    - **Réseau** : même sous-réseau client → même hôte
5. **Ajouter les hôtes** : Cluster → Ajouter un hôte → répéter pour chaque serveur membre

> ***Cas d'usage NLB :*** *serveurs web IIS, serveurs de terminaux RDS, passerelles VPN — pour les applications sans état ou avec affinité de session. Pour les bases de données ou les applications avec état complexe, préférer un cluster de basculement (Failover Cluster).*

---

7. Utilisation d'Azure Arc avec Windows Server

Azure Arc permet d'étendre les services et la gestion Azure aux serveurs on-premise, dans d'autres clouds ou en edge.

Déploiement de l'agent Azure Arc :

1. Dans le **portail Azure** : naviguer vers **Azure Arc → Infrastructure → Serveurs → Ajouter**
2. Choisir la méthode d'ajout : **"Ajouter un seul serveur"** ou script pour plusieurs serveurs
3. Sélectionner l'abonnement, le groupe de ressources, la région, le système d'exploitation
4. **Générer le script d'installation** (PowerShell pour Windows)

5. Exécuter le script sur le serveur Windows cible (nécessite une connexion Internet sortante vers les endpoints Azure Arc)
6. Authentifier avec un compte Azure pendant l'installation

Après enregistrement — capacités disponibles depuis le portail Azure :

Fonctionnalité	Description
Azure Policy	Appliquer des stratégies de conformité (ex : antivirus installé, TLS 1.2 obligatoire)
Azure Update Manager	Gérer les mises à jour Windows depuis Azure
Microsoft Defender for Servers	Détection des menaces et évaluation des vulnérabilités
Azure Monitor	Collecter les journaux et métriques, créer des alertes
Microsoft Sentinel	SIEM cloud (analyse des événements de sécurité)
SSH/RDP via Azure	Connexion sécurisée sans VPN ni IP publique
Extensions VM	Déployer des agents (MMA, Dependency Agent...) comme sur une VM Azure

> ***Prérequis réseau :*** *l'agent Arc doit pouvoir contacter plusieurs endpoints Azure (management.azure.com, login.microsoftonline.com, etc.) en HTTPS sortant sur le port 443.*

Chapitre 6 : Implémentation d'un serveur DNS

1. Présentation du service DNS

Le **Domain Name System (DNS)** est le service qui résout les noms d'hôtes en adresses IP (et inversement). Il fonctionne selon une hiérarchie arborescente distribuée.

Hiérarchie DNS :

```
. (zone racine — gérée par l'ICANN, 13 serveurs racine)
│
├── .com / .fr / .org / .net (TLD — Top Level Domain)
│   │
│   ├── microsoft.com / nouvy.fr (domaines de second niveau)
│   │   │
│   │   ├── www.microsoft.com (hôtes)
│   │   ├── mail.microsoft.com
│   │   └── srv1.nouvy.fr
```

Copier

Principaux types d'enregistrements DNS :

Type	Rôle	Exemple
A	Nom d'hôte → adresse IPv4	`srv1.nouvy.lan → 192.168.1.10`
AAAA	Nom d'hôte → adresse IPv6	`srv1.nouvy.lan → 2001:db8::1`
CNAME	Alias pointant vers un autre nom	`www.nouvy.lan → srv1.nouvy.lan`
MX	Serveur de messagerie du domaine	`nouvy.lan → mail.nouvy.lan (priorité 10)`
PTR	Résolution inverse IPv4 → Nom	`10.1.168.192.in-addr.arpa → srv1.nouvy.lan`
NS	Serveur de noms autoritaire de la zone	`nouvy.lan → ns1.nouvy.lan`
SOA	Enregistrement d'autorité de zone (Serial, Refresh, Retry, Expire, TTL minimum)	Paramètres de la zone
SRV	Localisation de services	`_ldap._tcp.nouvy.lan → dc1.nouvy.lan:389`
TXT	Informations textuelles	SPF, DKIM, DMARC pour l'email

Résolution récursive vs Itérative :

Mode	Description	Qui effectue le travail
Récursive	Le client demande une réponse complète au serveur DNS — le serveur fait tout le travail	Le serveur DNS résolveur
Itérative	Le serveur répond avec la meilleure réponse qu'il a (référence vers un autre serveur) — le client ou le résolveur continue	Le client/résolveur

En pratique : le client fait une requête **récursive** à son DNS résolveur → le résolveur fait des requêtes **itératives** vers les serveurs racine, TLD, et autoritaires.

TTL (Time To Live) :

- Durée en secondes pendant laquelle un enregistrement peut être mis en cache
- TTL élevé (86400s = 1 jour) : moins de requêtes, mais propagation des changements plus lente
- TTL faible (300s = 5 min) : recommandé avant une migration, changements propagés rapidement

---

2. Installation du rôle Serveur DNS

Via Server Manager :

1. **Gérer → Ajouter des rôles et fonctionnalités**
2. Cocher **"Serveur DNS"** → ajouter les fonctionnalités → Installer
3. Vérification post-installation : Server Manager → **DNS** → le serveur doit apparaître en vert

> ***Note :*** *si AD DS est installé en premier, le DNS est automatiquement installé et configuré lors de la promotion du DC. La zone du domaine (ex : `nouvy.lan`) est créée automatiquement, intégrée à AD.*

Vérification du service DNS :

- `services.msc` → "DNS Server" → doit être démarré et en démarrage automatique
- `dnsmgmt.msc` → le serveur doit apparaître avec une icône verte

---

3. Gestion des zones DNS

Depuis dnsmgmt.msc :

Créer une zone de recherche directe :

1. Clic droit sur **"Zones de recherche directe"** → **"Nouvelle zone"**
2. **Type de zone :**

Type	Description	Usage
Principale	Zone maître, modifiable localement dans le fichier ou AD	Serveur DNS autoritaire principal
Secondaire	Copie en lecture seule d'une zone principale (transfert de zone)	Serveur DNS secondaire pour redondance
Stub	Contient uniquement SOA, NS et enregistrement A des serveurs NS	Résolution entre zones/forêts
Intégrée à Active Directory	Stockée dans AD, répliquée automatiquement entre DC, sécurisée par ACL AD	Recommandé pour DNS Active Directory

3. **Portée de réplication** (si intégrée à AD) :
    - Tous les serveurs DNS de la forêt
    - Tous les serveurs DNS du domaine (recommandé)
    - Tous les DC du domaine
    - Personnalisée
4. **Nom de la zone** : ex. `nouvy.lan`
5. **Mises à jour dynamiques** : Sécurisées uniquement (si intégrée à AD) — recommandé

Créer une zone de recherche inverse :

1. Clic droit sur **"Zones de recherche inverse"** → **"Nouvelle zone"**
2. Saisir l'identifiant réseau : ex. `192.168.1` → Windows crée automatiquement `1.168.192.in-addr.arpa`
3. Choisir le type (intégrée à AD recommandé)

Ajouter des enregistrements dans une zone :

- Clic droit dans la zone → **Nouvel hôte (A ou AAAA)** : saisir le nom et l'IP, cocher "Créer l'enregistrement PTR associé" si une zone inverse existe
- Clic droit → **Nouveau nom d'alias (CNAME)** : saisir l'alias et le FQDN cible
- Clic droit → **Nouvel échangeur de courrier (MX)** : saisir la priorité et le FQDN du serveur mail
- Clic droit → **Autres nouveaux enregistrements** : accès à tous les types (SRV, TXT, NS...)

---

4. Gestion du serveur DNS

Redirecteurs (résolution externe) :

1. Dans `dnsmgmt.msc` → clic droit sur le **serveur** → **Propriétés** → onglet **Redirecteurs**
2. Cliquer sur **Modifier** → ajouter les adresses des serveurs DNS publics :
   - `8.8.8.8` / `8.8.4.4` (Google)
   - `1.1.1.1` / `1.0.0.1` (Cloudflare)
   - `9.9.9.9` (Quad9)
3. Décocher "Utiliser les indications de racine si aucun redirecteur n'est disponible" si le serveur ne doit pas résoudre directement via les racines

Redirecteurs conditionnels :

1. Clic droit sur **"Redirecteurs conditionnels"** → **"Nouveau redirecteur conditionnel"**
2. **Domaine DNS** : ex. `partenaire.com`
3. **Adresses IP des serveurs DNS** de ce domaine
4. Optionnel : stocker dans AD pour réplication entre DC
5. Usage : résolution des domaines partenaires, DMZ, forêts multiples

Transfert de zone (zone secondaire) :

1. Clic droit sur la zone → **Propriétés** → onglet **Transferts de zone**
2. Cocher **"Autoriser les transferts de zone"**
3. Choisir : vers tout serveur / vers les serveurs listés dans l'onglet Serveurs de noms / vers les serveurs spécifiés
4. Configurer une notification : onglet **Notification** → ajouter l'adresse du serveur secondaire (pour notification push lors des changements)

Vieillissement et nettoyage :

- Clic droit sur le **serveur** → **"Définir le vieillissement/nettoyage pour toutes les zones"**
- Activer par zone : clic droit zone → Propriétés → onglet **Général** → **Vieillissement**
- Lancer un nettoyage manuel : clic droit serveur → **"Nettoyer les enregistrements de ressources obsolètes"**

Surveillance et test DNS :

1. Clic droit sur le serveur → Propriétés → onglet **Surveillance**

2. Cocher **"Test simple"** (vérifie la résolution locale)
3. Cocher **"Test récursif"** (vérifie la résolution complète vers les racines)
4. Cliquer **Tester maintenant** ou activer les tests automatiques périodiques

Déboguer avec la console DNS :

- Onglet **Journalisation de débogage** : activer les logs détaillés vers un fichier (impact performance — à utiliser temporairement)
- Onglet **Journal des événements** : lien vers l'Observateur d'événements filtré sur DNS

Chapitre 7 : Implémentation d'un serveur de fichiers

1. Le système de fichiers NTFS

NTFS (New Technology File System) est le système de fichiers standard de Windows Server, offrant des fonctionnalités avancées de sécurité, de compression, de chiffrement et de journalisation.

Permissions NTFS (configurées depuis l'onglet **Sécurité** des propriétés d'un dossier/fichier) :

Permission	Sur un dossier	Sur un fichier
Contrôle total	Toutes les opérations + modification des permissions et du propriétaire	Idem
Modification	Lire, écrire, supprimer, exécuter	Idem
Lecture et exécution	Parcourir le dossier, voir les attributs, lire, exécuter	Lire et exécuter
Liste du contenu du dossier	Voir la liste des fichiers et sous-dossiers	N/A
Lecture	Lire le contenu, voir les attributs et les permissions	Idem
Écriture	Créer des fichiers/sous-dossiers, modifier les attributs	Modifier le contenu

Règles d'application des permissions NTFS :

- **Cumul** : les permissions de plusieurs groupes s'accumulent (union)
- **Refus prioritaire** : une permission "Refuser" (Deny) l'emporte sur n'importe quel "Autoriser" (Allow)
- **Exception** : le propriétaire du fichier peut toujours modifier les permissions même si Deny est appliqué
- **Héritage** : par défaut, les sous-dossiers et fichiers héritent des permissions du dossier parent

Gestion de l'héritage :

1. Clic droit sur le dossier → **Propriétés → Sécurité → Avancé**
2. Cliquer sur **"Désactiver l'héritage"** → choisir :
    - **Convertir les autorisations héritées en autorisations explicites** (conserve les permissions actuelles)
    - **Supprimer toutes les autorisations héritées** (repart de zéro)

Vérifier les permissions effectives :

1. Propriétés du dossier → **Sécurité → Avancé → onglet Accès effectif**
2. Cliquer sur **"Sélectionner un utilisateur"** → choisir le compte
3. Cliquer sur **"Afficher l'accès effectif"** → liste les permissions réellement appliquées

Permissions de partage vs NTFS :

Aspect	Permissions de partage	Permissions NTFS
S'appliquent	Accès réseau uniquement	Réseau ET local
Granularité	Faible (Lecture, Modification, Contrôle total)	Élevée (6+ niveaux)
Bonne pratique	Mettre "Contrôle total" pour "Tout le monde"	Contrôler finement avec NTFS
Résultat combiné	La permission la plus restrictive des deux s'applique à distance	

---

2. Tolérance de panne — RAID

Niveaux RAID disponibles depuis diskmgmt.msc (volumes dynamiques) :

RAID	Disques min	Redondance	Performance lecture	Performance écriture	Capacité utile	Usage recommandé
RAID 0 (Agrégat par bandes)	2	Aucune	Très haute	Très haute	100% (n × disques)	Performances pures, pas de données critiques
RAID 1 (Miroir)	2	Oui (1 panne tolérée)	Haute (lecture parallèle)	Identique à 1 disque	50%	OS, logs, données critiques petite taille
RAID 5 (Parité distribuée)	3	Oui (1 panne tolérée)	Bonne	Réduite (calcul parité)	(n-1)/n	Données générales, bon compromis
RAID 6 (Double parité)	4	Oui (2 pannes tolérées)	Bonne	Plus réduite	(n-2)/n	Archives, tolérance maximale
RAID 10 (Miroir + bandes)	4	Oui (1 panne par paire)	Très haute	Haute	50%	Bases de données, haute performance + redondance

Depuis diskmgmt.msc (`Windows + R` → `diskmgmt.msc`) :

1. Les disques doivent être en mode **Dynamique** (clic droit disque → Convertir en disque dynamique)
2. Clic droit sur l'espace non alloué → choisir le type :
    - **Nouveau volume agrégé par bandes** → RAID 0
    - **Nouveau volume en miroir** → RAID 1
    - **Nouveau volume RAID-5** → RAID 5

> ***Note :*** *Windows Server ne supporte pas nativement RAID 6 et RAID 10 en logiciel via diskmgmt.msc. Ces niveaux sont généralement gérés par des contrôleurs RAID matériels ou via les Espaces de stockage.*

---

3. DAS, NAS et SAN

Critère	DAS	NAS	SAN
Connexion	Directe (SATA, SAS, USB, PCIe)	Réseau Ethernet standard	Réseau dédié (Fibre Channel, iSCSI, FCoE)
Protocole	SATA / SAS	SMB (Windows), NFS (Linux/Unix)	iSCSI, Fibre Channel, NVMe-oF
Type d'accès	Bloc	Fichier	Bloc
Partage	Non (un seul serveur)	Oui (partage de fichiers)	Oui (LUN partagé entre serveurs)
Performance	Très haute	Moyenne	Très haute
Latence	Très faible	Moyenne (réseau)	Faible (réseau dédié)
Coût	Faible	Moyen	Élevé
Complexité	Simple	Modérée	Élevée
Usage typique	Serveur standalone	Partage de fichiers bureautique	Virtualisation (Hyper-V, VMware), bases de données

---

4. Espaces de stockage (Storage Spaces)

Les **Espaces de stockage** permettent de regrouper des disques physiques en pools et de créer des disques virtuels avec redondance, gérés depuis Windows.

Depuis Server Manager → Services de fichiers et de stockage → Espaces de stockage :

1. **Créer un nouveau pool de stockage :**
    - Volet Pools de stockage → **Tâches → Nouveau pool de stockage**

    - Nommer le pool (ex : "Pool-Données")
    - Sélectionner le sous-système (serveur local)
    - Sélectionner les **disques physiques** à inclure (disques non formatés recommandés)

2. **Créer un disque virtuel dans le pool :**
    - Clic droit sur le pool → **Nouveau disque virtuel**
    - Nommer le disque virtuel
    - **Disposition de stockage (mise en miroir/parité) :**

Disposition	Redondance	Espace utilisé	Disques min
Simple	Aucune (comme RAID 0)	100%	1
Miroir à 2 voies	1 défaillance tolérée	50%	2
Miroir à 3 voies	2 défaillances tolérées	33%	5
Parité	1 défaillance tolérée	~67%	3

- **Type d'approvisionnement :** Fixe (espace réservé immédiatement) ou Dynamique (thin provisioning)
- Définir la **taille** du disque virtuel

3. **Créer un volume sur le disque virtuel :**
    - Formater en **NTFS** ou **ReFS** (Resilient File System — recommandé pour grandes données)
    - Attribuer une lettre de lecteur ou un point de montage

---

5. Les clichés instantanés (Volume Shadow Copy Service — VSS)

Les **clichés instantanés** permettent de conserver des versions antérieures de fichiers et dossiers, accessibles directement par les utilisateurs sans intervention des administrateurs.

Activation depuis l'Explorateur de fichiers :

1. Ouvrir l'**Explorateur de fichiers** → clic droit sur le volume (ex : `C:`) → **Propriétés**
2. Onglet **"Clichés instantanés"**
3. Sélectionner le volume dans la liste → cliquer **"Activer"**
4. Confirmer → un premier cliché est créé immédiatement

Planification des clichés :

1. Sélectionner le volume activé → bouton **"Paramètres"**
2. Configurer le volume de stockage des clichés (peut être un volume différent — recommandé)
3. Cliquer sur **"Planifier"** → configurer la fréquence :
    - Par défaut : **7h00 et 12h00** les jours de semaine
    - Recommandation : ajouter une heure en soirée (ex : 18h00)
4. Limite d'espace : configurer une taille maximale (les plus anciens clichés sont

supprimés quand la limite est atteinte)

Restauration d'une version précédente (côté utilisateur) :

1. Clic droit sur le fichier ou le dossier → **Propriétés** → onglet **"Versions précédentes"**
2. Sélectionner la version dans la liste (date et heure du cliché)
3. Options disponibles :
    - **Ouvrir** : ouvrir la version en lecture seule sans restaurer
    - **Copier** : copier la version vers un emplacement choisi
    - **Restaurer** : remplacer la version actuelle par la version sélectionnée (irréversible — faire une copie avant)

> ***Limitation VSS :*** *les clichés instantanés ne remplacent pas une sauvegarde complète. Ils sont stockés sur le même serveur et seront perdus en cas de défaillance matérielle.*

---

6. Le rôle Services d'impression

Installation depuis Server Manager :

1. Gérer → Ajouter des rôles → **"Services d'impression et de document"**
2. Sélectionner les services :
    - **Serveur d'impression** (obligatoire)
    - Impression Internet (optionnel, pour impression via HTTP)
    - Service LPD (optionnel, pour clients Unix/Linux)

Console Gestion de l'impression (printmanagement.msc) :

Ajouter un serveur d'impression :

1. Clic droit sur **"Serveurs d'impression"** → **"Ajouter/supprimer des serveurs"**
2. Saisir le nom ou l'IP du serveur → **Ajouter à la liste**

Ajouter une imprimante :

1. Clic droit sur le serveur d'impression → **"Ajouter une imprimante"**
2. Choisir la méthode de recherche :
    - **TCP/IP ou nom d'hôte** (imprimante réseau) → saisir l'IP
    - **Détection automatique** → scan du réseau
3. Installer le pilote approprié (ou le télécharger depuis Windows Update)
4. Configurer le partage : nom de partage, commentaire, emplacement

Déploiement d'imprimantes via GPO :

1. Clic droit sur l'imprimante dans `printmanagement.msc` → **"Déployer avec la stratégie de groupe"**
2. Parcourir → sélectionner la GPO cible (existante ou en créer une)
3. Choisir : déployer pour les **utilisateurs** ou pour les **ordinateurs**
4. L'imprimante est installée automatiquement à la prochaine connexion/démarrage

Pool d'impression :

1. Propriétés de l'imprimante → onglet **"Ports"**
2. Cocher **"Activer le pool d'impression"**
3. Cocher plusieurs ports/imprimantes identiques
4. Windows envoie chaque travail à la première imprimante disponible dans le pool

---

7. Rôle de serveur de fichiers et FSRM

Installation du rôle : Server Manager → Ajouter des rôles → **Services de fichiers et de stockage → Serveur de fichiers**

Ajouter aussi : **Gestionnaire de ressources du serveur de fichiers (FSRM)**

Création d'un partage depuis Server Manager :

1. Server Manager → **Services de fichiers et de stockage → Partages**
2. **Tâches → Nouveau partage**
3. Profil de partage :

Profil	Description
SMB Partage — Rapide	Partage simple sans options avancées
SMB Partage — Avancé	Avec quotas, filtrage de fichiers, rapports (nécessite FSRM)
SMB Partage — Applications	Optimisé pour Hyper-V, SQL Server, applications clustérisées
NFS Partage — Rapide	Pour clients Unix/Linux

4. Sélectionner le volume et le chemin local (ou créer un nouveau dossier)
5. Configurer les **permissions de partage** (simplifié : Tout le monde — Contrôle total puis affiner avec NTFS)
6. Configurer les **permissions NTFS** de façon granulaire
7. Activer les **quotas** si nécessaire
8. Finaliser → le partage est accessible via `\serveur om-du-partage`

FSRM — Gestionnaire de ressources du serveur de fichiers :

Ouvrir `fsrm.msc` ou depuis Server Manager → Outils → Gestionnaire de ressources du serveur de fichiers

Fonctionnalité	Description	Exemple
Quotas	Limiter l'espace disque par dossier	10 Go par dossier de département
Modèles de quota	Modèles réutilisables de quotas avec alertes	Alerte à 85%, blocage à 100%
Filtrage de fichiers	Bloquer certains types de fichiers	Bloquer .mp3, .avi, .exe
Groupes de fichiers	Définir des catégories de fichiers	Groupe "Médias" = *.mp3, *.mp4, *.avi
Rapports de stockage	Rapports planifiés ou à la demande	Gros fichiers, fichiers en double, utilisation par type
Classification	Classer automatiquement les fichiers par propriétés	Marquer les fichiers contenant "Confidentiel"
Gestion des tâches de fichiers	Appliquer des actions selon la classification	Chiffrer ou déplacer les fichiers confidentiels

Chapitre 8 : Gestion du système de fichiers DFS

1. Vue d'ensemble du système de fichiers DFS

DFS (Distributed File System) se compose de deux technologies complémentaires :

- **DFS Namespace (DFS-N)** : crée un chemin d'accès virtuel unifié (ex : `\nouvy.lanpartages`) qui masque l'architecture réelle des serveurs. L'utilisateur n'a pas besoin de connaître le nom du serveur physique.

- **DFS Replication (DFS-R)** : réplique le contenu des dossiers entre plusieurs serveurs à l'aide d'un algorithme différentiel (RDC — Remote Differential Compression) qui ne transfère que les blocs modifiés.

Avantages de DFS :

Avantage	Description
Accès transparent	L'utilisateur utilise toujours le même chemin UNC `\domainepartage` quel que soit le serveur
Haute disponibilité	Plusieurs cibles configurées pour un même dossier — si un serveur tombe, le client bascule automatiquement
Optimisation WAN	DFS-R n'envoie que les blocs modifiés (RDC) — économise la bande passante entre sites
Consolidation	Regrouper des partages de plusieurs serveurs sous un seul espace de noms
Équilibrage de charge	Le client est dirigé vers la cible la plus proche (site AD)

Installation du rôle DFS : Server Manager → Ajouter des rôles → Services de fichiers et de stockage → **Espaces de noms DFS** et **Réplication DFS**

---

2. L'espace de noms DFS (DFS Namespace)

Types d'espaces de noms :

Type	Chemin UNC	Haute disponibilité	Stockage des métadonnées
Basé sur un domaine (mode Windows 2008)	`\nouvy.lanpartages`	Oui (plusieurs serveurs d'espace de noms)	Active Directory
Basé sur un domaine (mode Windows 2000)	`\nouvy.lanpartages`	Limitée	Active Directory
Autonome	`\serveur1partages`	Non (un seul serveur)	Registre du serveur

Création d'un espace de noms depuis dfsmgmt.msc :

1. `Windows + R` → `dfsmgmt.msc` (Gestion DFS)
2. Clic droit sur **"Espaces de noms"** → **"Nouvel espace de noms"**
3. **Sélectionner le serveur** d'espace de noms (serveur hébergeant les métadonnées)
4. **Nom de l'espace de noms** : ex. `Partages` → le chemin complet sera `\nouvy.lanPartages`
5. **Type** : sélectionner **"Espace de noms basé sur un domaine"** → cocher **mode Windows Server 2008** pour les fonctionnalités complètes
6. Vérification → **Créer**

Ajouter des dossiers à l'espace de noms :

1. Clic droit sur l'espace de noms → **"Nouveau dossier"**
2. **Nom du dossier** : ex. `RH` → le chemin virtuel sera `\nouvy.lanPartagesRH`
3. Cliquer **"Ajouter"** pour ajouter des **cibles de dossier** (chemins UNC réels) :
    - ex. `\SRV-FIC1RH` et `\SRV-FIC2RH` (deux cibles pour la haute disponibilité)
4. L'ordre de référence peut être configuré (par coût de site, aléatoire...)

Ajouter un deuxième serveur d'espace de noms (haute disponibilité) :

1. Clic droit sur l'espace de noms → **"Ajouter un serveur d'espace de noms"**
2. Sélectionner le serveur supplémentaire
3. Les deux serveurs d'espace de noms répondent aux requêtes DFS des clients

---

3. La réplication DFS (DFS Replication)

Création d'un groupe de réplication depuis dfsmgmt.msc :

1. Clic droit sur **"Réplication"** → **"Nouveau groupe de réplication"**
2. **Type de groupe de réplication :**
    - **Réplication multisite** : usage général, entre plusieurs serveurs et sites
    - **Réplication de données de dossier public** : scénario spécifique dossier SYSVOL-like
3. **Nom du groupe** : ex. `GR-RH-Bilatéral`
4. **Membres du groupe** : ajouter tous les serveurs qui doivent répliquer (ex : SRV-FIC1, SRV-FIC2)

Topologies de réplication :

Topologie	Description	Usage
Maillée complète (Full Mesh)	Chaque serveur réplique directement avec tous les autres	Petit nombre de serveurs (≤ 10), LAN
Hub and Spoke	Un ou plusieurs serveurs hub centraux → répliquent vers des spoke	Nombreux sites distants, WAN
Personnalisée	Connexions définies manuellement	Topologies complexes

5. **Planification de réplication :**

        - **Réplication continue** : 24h/24, 7j/7 (recommandé si bande passante suffisante)
        - **Planifiée** : définir des plages horaires et la bande passante maximale (en Kbps) par plage
6. **Membre principal** : désigner le serveur dont le contenu initial sera répliqué vers les autres
7. **Dossier répliqué** :
        - Nom du dossier répliqué
        - Chemin local sur chaque membre (ex : `D:PartagesRH` sur SRV-FIC1, `E:DFS-RH` sur SRV-FIC2)

Conflit de réplication :

- Si deux utilisateurs modifient le même fichier simultanément sur deux serveurs différents
- DFS-R conserve la version la plus récente et place la version perdante dans le dossier `DfsrPrivateConflictAndDeleted`
- Consulter les conflits : `dfsmgmt.msc` → rapport de diagnostic

---

4. Utilisation des rapports DFS

Générer un rapport de diagnostic depuis dfsmgmt.msc :

1. Clic droit sur un **groupe de réplication** → **"Créer un rapport de diagnostic"**
2. **Types de rapports disponibles :**

Type de rapport	Informations fournies
État de la santé	Erreurs de réplication, membres en retard, conflits
Vecteur de version	État de convergence de chaque fichier sur chaque membre
Fichiers en attente de réplication	Liste des fichiers en file d'attente avec taille et ancienneté
Fichiers propagés	Statistiques des fichiers répliqués sur une période

3. **Membres** : sélectionner les membres à inclure dans le rapport
4. **Chemin et format** : choisir un chemin local et le format **HTML** (s'ouvre dans le navigateur)
5. Cliquer **Créer** → le rapport est généré et peut s'ouvrir automatiquement

Interpréter le rapport :

- **Vecteur de version identique sur tous les membres** = convergence complète (état sain)
- **Retard de réplication important** = problème de connectivité ou de bande passante entre membres
- **Erreurs 5002 / 9026** dans l'Observateur d'événements (journal DFS Replication) = problèmes courants à investiguer

Suivi de l'état de réplication :

1. `dfsmgmt.msc` → Réplication → sélectionner le groupe
2. Onglet **"Membres"** : état de chaque membre (Activé, Replication en cours, Erreur)
3. Onglet **"Connexions"** : état des connexions entrantes et sortantes entre membres

---

5. Création d'un espace de noms DFS avec PowerShell

Voir **Chapitre 15 — PowerShell** pour les commandes `New-DfsnRoot`, `New-DfsnFolder`, `New-DfsnFolderTarget`, `New-DfsReplicationGroup`, `New-DfsReplicatedFolder`, `Add-DfsrMember`.

Infrastructure Serveur Windows Server — Chapitres 9 à 15

> ***Règle absolue :** Toutes les procédures sont décrites depuis les **consoles graphiques** Windows. PowerShell est réservé au Chapitre 15.*

Table des matières

Chapitre 9 — Infrastructure de stratégies de groupe

1. Introduction aux stratégies de groupe

Une **GPO (Group Policy Object)** est un conteneur de paramètres de configuration appliqués à des utilisateurs et/ou des ordinateurs membres d'un domaine Active Directory.

Console principale : `gpmc.msc` — Gestion des stratégies de groupe

Ordre d'application LSDOU

Les GPO sont appliquées dans un ordre précis, chaque niveau pouvant écraser le précédent :

Ordre	Niveau	Description
1	**Local**	Politique locale de la machine (`gpedit.msc`)
2	**Site**	Politiques liées au site AD DS
3	**Domaine**	Politiques liées au domaine
4	**OU**	Politiques liées aux unités d'organisation (plus spécifiques)

> *La dernière GPO appliquée remporte en cas de conflit, **sauf** si une GPO est marquée **Appliqué (Enforced)**.*

Deux sections dans une GPO

Section	Moment d'application
Configuration ordinateur	Au démarrage de la machine
Configuration utilisateur	À l'ouverture de session

---

2. Traitement en boucle (Loopback Processing)

Cas d'usage

Le traitement en boucle est conçu pour les environnements où l'on souhaite que **les paramètres suivent l'ordinateur plutôt que l'utilisateur** :

- Salles de classe informatiques partagées
- Bornes interactives et kiosques publics
- Postes de travail partagés (accueil, production)
- Serveurs Terminal Services / RDS

Deux modes disponibles

Mode	Comportement
Fusion	GPO utilisateur normales + GPO liées à l'OU de l'ordinateur (les GPO ordinateur ont la priorité en cas de conflit)
Remplacement	Seules les GPO liées à l'OU de l'ordinateur s'appliquent (GPO utilisateur habituelles ignorées)

Activation dans l'éditeur GPO

`Éditeur GPO` → `Configuration ordinateur` → `Modèles d'administration` → `Système` → `Stratégie de groupe` → **Configurer le mode de traitement en boucle de la stratégie de groupe utilisateur** → Activé → choisir le mode (Fusion ou Remplacement)

---

3. Gestion des stratégies de groupe

Toutes les opérations ci-dessous s'effectuent depuis **`gpmc.msc`**.

Créer une GPO et la lier à une OU

1. Dans l'arbre de gauche, développer le domaine
2. Clic droit sur le domaine ou l'OU cible → **Créer un objet GPO dans ce domaine, et le lier ici...**
3. Nommer la GPO (convention recommandée : `[Cible]-[Objet]-[Action]`, ex : `PC-Bureau-Restrictions`)
4. Clic droit sur la GPO nouvellement créée → **Modifier** → l'Éditeur de gestion des stratégies de groupe s'ouvre

Lier une GPO existante à une OU

1. Clic droit sur l'OU cible → **Lier un objet de stratégie de groupe existant...**
2. Sélectionner la GPO dans la liste proposée → OK

Sauvegarder une GPO

- Clic droit sur la GPO → **Sauvegarder...**
- Choisir un dossier de destination (idéalement un partage réseau dédié)
- La sauvegarde contient tous les paramètres, les filtres WMI et les informations de liaison

Restaurer une GPO

- Clic droit sur **Objets de stratégie de groupe** → **Gérer les sauvegardes...**
- Sélectionner la sauvegarde dans la liste → **Restaurer**
- Possibilité de visualiser les paramètres avant restauration

Supprimer une GPO

- Clic droit sur la GPO → **Supprimer**
- Attention : distinguer **supprimer la liaison** (la GPO reste dans AD) de **supprimer la GPO** (définitivement)

---

4. Modèles d'administration

Fichiers ADMX / ADML

Fichier	Rôle	Emplacement par défaut
`.admx`	Définition des paramètres (structure XML)	`%SystemRoot%PolicyDefinitions`
`.adml`	Traduction dans une langue	`%SystemRoot%PolicyDefinitionsfr-FR`

Magasin central (Central Store)

Pour éviter que chaque DC utilise ses propres modèles, créer un **magasin central** sur SYSVOL :

1. Sur le contrôleur de domaine, copier le contenu de `C:WindowsPolicyDefinitions` vers `\nouvy.lanSYSVOL ouvy.lanPoliciesPolicyDefinitions`

2. Désormais, tous les administrateurs utilisent les mêmes modèles, quelle que soit leur machine

Ajouter des modèles tiers

Exemples : Google Chrome, Mozilla Firefox, Microsoft Office, Adobe Reader...

1. Télécharger les fichiers `.admx` et `.adml` depuis le site de l'éditeur
2. Copier les `.admx` dans `\domaineSYSVOLdomainePoliciesPolicyDefinitions`
3. Copier les `.adml` dans le sous-dossier de langue correspondant (ex: `fr-FR`)
4. Rouvrir l'éditeur GPO → les nouveaux paramètres apparaissent dans Modèles d'administration

Navigation dans l'éditeur

`Configuration ordinateur (ou utilisateur)` → `Modèles d'administration` → parcourir les catégories

Chaque paramètre a trois états :

- **Non configuré** : la GPO n'a aucun effet sur ce paramètre
- **Activé** : le paramètre est forcé à la valeur choisie
- **Désactivé** : le paramètre est explicitement désactivé

---

5. Gestion de l'héritage

Bloquer l'héritage

- Clic droit sur l'OU → **Bloquer l'héritage**
- Une icône bleue apparaît sur l'OU dans GPMC
- Les GPO des niveaux supérieurs (domaine, OU parentes) ne s'appliquent plus à cette OU
- Utile pour une OU de test ou une filiale avec une politique distincte

Appliquer (Enforced / Forcé)

- Clic droit sur **la liaison** de la GPO (pas la GPO elle-même) → **Appliqué**
- Une icône cadenas apparaît sur la liaison
- La GPO s'applique même si l'héritage est bloqué en dessous
- La GPO Enforced ne peut pas être remplacée par une GPO d'OU inférieure

> *Une GPO avec **Enforced** sur le domaine prime sur un **Bloquer l'héritage** sur une OU fille.*

Visualiser l'héritage effectif

Dans GPMC, sélectionner une OU → onglet **Héritage de stratégie de groupe** : liste toutes les GPO qui s'appliquent dans l'ordre de priorité (de bas en haut = de la plus haute priorité à la plus basse)

Ordre de liaison (Link Order)

Dans l'onglet **Objets de stratégie de groupe liés** d'une OU :

- **Chiffre le plus bas = priorité la plus haute** (traité en dernier, donc prime)
- Modifier l'ordre avec les flèches haut/bas dans GPMC

---

6. Préférences de stratégies de groupe

Les préférences complètent les stratégies en offrant plus de flexibilité.

Différences clés

Critère	Stratégies	Préférences
Tatouage (persistance)	Oui (supprimé avec la GPO)	Non (reste après suppression de la GPO)
Interface utilisateur	Grisée (l'utilisateur ne peut pas modifier)	Accessible (l'utilisateur peut modifier)
Flexibilité	Moins	Plus (ciblage au niveau élément)
Actions disponibles	Limité	Créer, Remplacer, Mettre à jour, Supprimer

Extensions disponibles

Dans l'éditeur GPO → `Configuration utilisateur/ordinateur` → **Préférences** :

Catégorie	Exemples d'utilisation
Lecteurs réseau	Mapper `Z:` vers `\SRV01Partages` selon le groupe AD
Imprimantes	Déployer des imprimantes réseau selon l'OU ou le site
Variables d'environnement	Définir `%APPDATA_CUSTOM%`
Raccourcis	Créer des raccourcis sur le bureau
Fichiers / Dossiers	Copier/créer/supprimer des fichiers selon conditions
Registre	Modifier des clés de registre avec ciblage
Services	Forcer l'état d'un service (démarré/arrêté/désactivé)
Planificateur de tâches	Créer des tâches planifiées sur les postes

Ciblage au niveau élément

Chaque préférence peut avoir des conditions d'application granulaires :

1. Dans la préférence → onglet **Commun** → cocher **Ciblage au niveau élément** → **Ciblage...**
2. Cliquer **Nouvel élément** → choisir une condition :
    - Appartenance à un groupe AD
    - Système d'exploitation (version, architecture)
    - Plage d'adresses IP
    - Nom de l'ordinateur (correspondance par motif)

    - Variable d'environnement
    - Heure de la journée ou jour de la semaine
    - Site Active Directory
3. Combiner les conditions avec ET / OU / PAS

---

7. Exécution de script PowerShell via une GPO

Depuis l'**Éditeur de gestion des stratégies de groupe** :

Scripts ordinateur (démarrage / arrêt)

1. `Configuration ordinateur` → `Paramètres Windows` → **Scripts**
2. Double-cliquer sur **Démarrage** (ou **Arrêt**)
3. Onglet **Scripts PowerShell** → **Ajouter...**
4. Cliquer **Parcourir** → copier le fichier `.ps1` dans le dossier SYSVOL de la GPO qui s'ouvre
5. Saisir le nom du script et les éventuels paramètres → OK

Scripts utilisateur (ouverture / fermeture de session)

1. `Configuration utilisateur` → `Paramètres Windows` → **Scripts**
2. Double-cliquer sur **Ouverture de session** (ou **Fermeture de session**)
3. Même procédure qu'au-dessus

Autoriser l'exécution de scripts PowerShell

`Configuration ordinateur` → `Modèles d'administration` → `Composants Windows` → `Windows PowerShell` → **Activer l'exécution des scripts** → Activé → choisir :

- **Tous les scripts signés** (recommandé en production)
- **Contourner** (pour les environnements de test)

> *Sans cette GPO, les postes clients peuvent bloquer l'exécution des scripts PS par défaut (politique `Restricted`).*

Chapitre 10 — Gestion de la politique de sécurité

1. Les stratégies par défaut

Deux GPO sont créées automatiquement lors de la promotion du premier DC :

GPO	Portée	Usage principal
Default Domain Policy	Tout le domaine	Politique de mot de passe, verrouillage de compte
Default Domain Controllers Policy	OU `Domain Controllers` uniquement	Droits d'utilisateurs, audit des connexions des DC

> ***Bonne pratique :*** *Ne **jamais** modifier directement ces deux GPO. Créer de nouvelles GPO liées au domaine (ou à l'OU DC) avec une priorité de liaison plus haute (numéro plus bas).*

Paramètres de mot de passe recommandés

Chemin : `Default Domain Policy` → `Configuration ordinateur` → `Paramètres Windows` → `Paramètres de sécurité` → `Stratégies de comptes` → **Stratégie de mot de passe**

Paramètre	Valeur recommandée
Longueur minimale du mot de passe	12 caractères minimum
Le mot de passe doit respecter des exigences de complexité	Activé
Durée de vie maximale du mot de passe	90 jours (ou illimitée avec MFA obligatoire)
Durée de vie minimale du mot de passe	1 jour (évite les changements en boucle)
Conserver l'historique des mots de passe	10 mots de passe mémorisés
Les mots de passe doivent être chiffrés de manière réversible	Désactivé

Stratégie de verrouillage de compte

Chemin : même emplacement → **Stratégie de verrouillage du compte**

Paramètre	Valeur recommandée
Seuil de verrouillage	5 tentatives échouées
Durée de verrouillage	15 minutes (ou 0 = déverrouillage admin uniquement)
Réinitialiser le compteur après	15 minutes

---

2. Les stratégies d'audit

Configuration via secpol.msc (local) ou GPO (domaine)

Chemin GPO : `Configuration ordinateur` → `Paramètres Windows` → `Paramètres de sécurité` → `Stratégies locales` → **Stratégie d'audit**

Catégorie d'audit	Événements générés
Auditer les connexions aux comptes	4768/4769 (Kerberos), 4776 (NTLM)
Auditer l'ouverture de session	4624 (succès), 4625 (échec), 4634/4647 (déconnexion)
Auditer la gestion des comptes	4720 (création), 4722 (activation), 4725 (désactivation), 4726 (suppression), 4723 (changement MDP)
Auditer l'accès aux objets	Accès fichiers/dossiers (requiert aussi un SACL sur l'objet)
Auditer l'utilisation des privilèges	Utilisation de droits sensibles (4672 : privilèges spéciaux)
Auditer les modifications de stratégie	Changements de GPO, de droits d'audit

Audit avancé (recommandé)

Chemin : `Paramètres de sécurité` → **Configuration avancée de la stratégie d'audit** (plus granulaire que l'audit de base, évite les conflits entre les deux)

Consultation des événements

`eventvwr.msc` → `Journaux Windows` → **Sécurité** → clic droit → **Filtrer le journal actuel** → saisir l'ID d'événement

---

3. Gestion de la sécurité

Security Configuration Wizard (scw.exe)

- Réduit la surface d'attaque en désactivant les services, ports et fonctionnalités inutiles
- Génère un fichier de politique `.xml` applicable à d'autres serveurs
- Accessible depuis Outils d'administration → **Assistant Configuration de la sécurité**

Modèles de sécurité

- Fichiers `.inf` prédéfinis contenant des configurations sécurisées
- Exemples : `Hisecws.inf` (poste haute sécurité), `Securedc.inf` (DC sécurisé)
- Analyser et appliquer via le snap-in MMC **Analyse et configuration de la sécurité** (`securityconfigurationanalysis`)

Microsoft Security Compliance Toolkit

- Baselines de sécurité officielles Microsoft pour Windows Server 2019/2022, Windows 10/11
- Téléchargeable sur le site Microsoft
- Importables directement comme GPO dans GPMC (`Import Settings...`)
- Contient également les outils **Policy Analyzer** (comparer des GPO) et **LGPO.exe**

---

4. Paramétrage de l'User Account Control (UAC)

Niveaux UAC

Accès : `Panneau de configuration` → `Comptes d'utilisateurs` → **Modifier les paramètres du contrôle de compte d'utilisateur**

Niveau	Description	Sécurité
Toujours notifier	Demande confirmation pour tout changement (apps et Windows)	Maximale
Notifier pour les changements d'application seulement	Par défaut — notifie pour les apps, pas pour les modifications Windows	Bonne
Notifier sans assombrir le bureau	Moins sécurisé (pas d'écran sécurisé)	Réduite
Ne jamais notifier	UAC désactivé	Déconseillé

Configuration via GPO

Chemin : `Configuration ordinateur` → `Paramètres Windows` → `Paramètres de sécurité` → `Stratégies locales` → `Options de sécurité` → paramètres **"Contrôle de compte d'utilisateur : ..."**

Paramètres notables :

- **Comportement de l'invite d'élévation pour les administrateurs** : demander les informations d'identification / consentement
- **Comportement de l'invite d'élévation pour les utilisateurs standard** : demander les informations d'identification
- **Exécuter tous les administrateurs en mode d'approbation administrateur** : doit rester activé

---

5. Le certificat numérique et la PKI

Hiérarchie PKI

```
AC Racine (Root CA) — hors ligne, hautement sécurisée
    └── AC Subordonnée (Subordinate CA) — en ligne, délivre les certificats
            ├── Certificats utilisateurs
            ├── Certificats machines
            └── Certificats serveurs (SSL/TLS)
```

Copier

Installation de l'Autorité de Certification

`Server Manager` → **Ajouter des rôles et des fonctionnalités** → `Services de certificats Active Directory` → choisir :

- **Autorité de certification** (obligatoire)
- **Inscription de l'autorité de certification via le Web** (pour les demandes navigateur)
- **Service de stratégie d'inscription de certificats réseau (NDES)** (pour les périphériques réseau)

Console de gestion : certsrv.msc

Action	Procédure
Délivrer un certificat en attente	`Demandes en attente` → clic droit → **Délivrer**
Révoquer un certificat	`Certificats délivrés` → clic droit → `Toutes les tâches` → **Révoquer le certificat**
Publier la CRL	`Certificats révoqués` → clic droit → `Toutes les tâches` → **Publier**
Modifier les modèles de certificat	`Modèles de certificats` → clic droit → **Gérer**

Demande de certificat depuis un client

`certmgr.msc` → `Certificats - Utilisateur actuel` → `Personnel` → clic droit → `Toutes les tâches` → **Demander un nouveau certificat**

Pour un ordinateur : `certlm.msc` (Gestionnaire de certificats machine locale)

Types de certificats courants

Type	Usage
SSL/TLS (Serveur Web)	Sécuriser un site web (HTTPS)
Authentification utilisateur	Connexion par carte à puce / smart card
Authentification ordinateur	802.1X (authentification réseau câblé/Wi-Fi)
Signature de code	Signer des scripts et applications
EFS	Chiffrement du système de fichiers (Encrypting File System)
OCSP	Répondeur d'état de certificat en ligne

---

6. Mise en place de la délégation de contrôle

La délégation permet d'accorder à des utilisateurs ou groupes des **droits d'administration limités** sur une OU, sans leur donner les droits Domain Admin.

Procédure depuis dsa.msc

1. Clic droit sur l'OU à déléguer → **Déléguer le contrôle...**
2. L'assistant démarre → **Suivant**
3. **Ajouter...** → sélectionner les utilisateurs ou groupes délégataires → **Suivant**
4. Choisir entre :
    - **Tâches courantes à déléguer** : liste prédéfinie des tâches fréquentes
    - **Créer une tâche personnalisée à déléguer** : contrôle granulaire sur les objets et permissions
5. Tâches courantes disponibles :
    - Créer, supprimer et gérer des comptes d'utilisateurs
    - Réinitialiser les mots de passe et forcer le changement au prochain connexion
    - Lire toutes les informations des utilisateurs
    - Créer, supprimer et gérer des groupes
    - Modifier l'appartenance à des groupes
    - Gérer les liens des stratégies de groupe
6. Finaliser l'assistant → les ACL sur l'OU AD sont modifiées automatiquement

Exemples de délégations courantes

Délégation	Groupe délégataire
Réinitialisation des mots de passe utilisateurs	Helpdesk Niveau 1
Gestion des comptes ordinateurs (jonction domaine)	Techniciens déploiement
Création/suppression de comptes utilisateurs	Helpdesk Niveau 2
Lecture des propriétés AD	Superviseurs / applications RH
Gestion des GPO sur une OU	Administrateurs locaux de site

> ***Vérification :*** *Les délégations sont visibles dans* `dsa.msc` *→ menu* ***Affichage*** *→* ***Fonctionnalités avancées*** *→ propriétés de l'OU → onglet* ***Sécurité****.*

---

7. Mise en place de LAPS

LAPS (Local Administrator Password Solution / Windows LAPS) gère automatiquement et de manière sécurisée le mot de passe du compte Administrateur local de chaque poste, en le stockant dans AD.

Versions

Version	Intégration	Notes
LAPS legacy (v6.x)	MSI à installer séparément	Attributs `ms-Mcs-AdmPwd` et `ms-Mcs-AdmPwdExpirationTime`
Windows LAPS (v3.0+)	Intégré nativement à Windows 11 23H2+ et Windows Server 2025	Attributs `msLAPS-Password`, chiffrement natif

Installation (LAPS legacy)

1. Télécharger `LAPS.x64.msi` depuis Microsoft
2. Sur le serveur AD : installer en choisissant **Outils de gestion** (extension GPMC + UI + cmdlets PowerShell)
3. Sur les postes clients : installer uniquement le composant **Agent** (via GPO Software Installation ou SCCM)

Extension du schéma AD (LAPS legacy)

> *Cette étape nécessite PowerShell (voir Chapitre 15) ou l'outil fourni :* `Update-AdmPwdADSchema`

Configuration GPO LAPS

1. Dans GPMC → créer une GPO dédiée LAPS (ex: `PC-LAPS-Config`)
2. `Configuration ordinateur` → `Modèles d'administration` → **LAPS**
3. Activer et configurer :
    - **Enable local admin password management** : Activé
    - **Password Settings** : longueur (min. 14 caractères recommandé), complexité, durée de vie (ex: 30 jours)
    - **Name of administrator account to manage** : préciser si le compte

n'est pas le compte par défaut

Consultation du mot de passe

- **LAPS UI** (interface graphique fournie avec LAPS) → saisir le nom de l'ordinateur → affiche le mot de passe actuel et sa date d'expiration
- Depuis `dsa.msc` → propriétés de l'ordinateur → onglet **Éditeur d'attributs** → attribut `ms-Mcs-AdmPwd`
- Depuis GPMC → rapport GPO pour LAPS

> *Seuls les utilisateurs/groupes ayant reçu la délégation de lecture de l'attribut `ms-Mcs-AdmPwd` peuvent voir le mot de passe.*

Chapitre 11 — Dépanner les stratégies de groupe

1. Composantes d'une GPO : GPC vs GPT

Une GPO est stockée en deux endroits distincts qui doivent rester synchronisés :

Composante	Emplacement	Contenu
GPC (Group Policy Container)	Active Directory : `CN=Policies,CN=System,DC=...` visible via `dsa.msc` → Affichage → Fonctionnalités avancées	Métadonnées, GUID, numéro de version GPC, état activé/désactivé
GPT (Group Policy Template)	SYSVOL : `\domaineSYSVOLdomainePolicies{GUID-de-la-GPO}`	Fichiers de configuration : `registry.pol`, scripts, modèles, paramètres de sécurité

Numéros de version

Chaque GPO possède un **numéro de version** qui s'incrémente à chaque modification. Ce numéro est stocké à la fois dans GPC (AD) et dans GPT (SYSVOL, fichier `GPT.INI`).

Si les numéros divergent entre le GPC et le GPT, ou entre différents DC → problème de réplication.

Structure du dossier GPT dans SYSVOL

```
\nouvy.lanSYSVOL
ouvy.lanPolicies{GUID}
├── GPT.INI               — version et flags
├── Machine              — paramètres Configuration ordinateur
│   ├── registry.pol      — paramètres de registre
│   ├── Scripts          — scripts de démarrage/arrêt
│   └── MicrosoftWindows NTSecEditGptTmpl.inf  — paramètres de sécurité
└── User                 — paramètres Configuration utilisateur
    ├── registry.pol
    └── Scripts          — scripts ouverture/fermeture de session
```

Copier

---

2. Utilisation de l'outil GpoTool

`gpotool.exe` est disponible dans les **Outils de support Windows Server** (Support Tools).

```
gpotool.exe /verbose
gpotool.exe /domain:nouvy.lan /verbose
gpotool.exe /gpo:"Nom de la GPO" /verbose
```

Copier

Cet outil :

- Interroge tous les contrôleurs de domaine
- Compare les numéros de version GPC (AD) et GPT (SYSVOL) sur chaque DC
- Signale les GPO avec des incohérences
- Vérifie l'intégrité des fichiers SYSVOL

---

3. Jeu de stratégie résultant (RSoP)

Depuis gpmc.msc

Dans GPMC → clic droit sur **Jeu de stratégie résultant** :

Mode Journalisation (réel) :

1. Suivant → sélectionner l'**ordinateur cible** (ou "ne pas afficher les paramètres ordinateur")
2. Sélectionner l'**utilisateur cible** → Suivant → Suivant → Terminer
3. GPMC affiche un rapport HTML avec les GPO appliquées, refusées, et les paramètres effectifs

Mode Planification (simulation) :

1. Choisir un utilisateur et un ordinateur cibles (pas forcément en ligne)
2. Simuler des changements : utilisateur dans d'autres groupes, ordinateur dans une autre OU...
3. Utile avant de déployer une nouvelle GPO pour vérifier son impact

Depuis rsop.msc

Lance directement le RSoP de l'ordinateur et de l'utilisateur **courants** (machine locale).

Rapport gpresult

Depuis l'invite de commandes ou PowerShell :

```
gpresult /h C:
apport-gpo.html   # Rapport HTML complet
gpresult /r                         # Résumé dans la console
gpresult /scope computer            # Uniquement les GPO ordinateur
gpresult /scope user                # Uniquement les GPO utilisateur
gpresult /s NOM-PC /h C:
apport-distant.html  # RSoP d'un poste distant
```

Copier

Le rapport HTML contient :

- **Onglet Résumé** : informations générales, GPO appliquées et refusées
- **Onglet Ordinateur** : liste des GPO ordinateur, paramètres en vigueur
- **Onglet Utilisateur** : liste des GPO utilisateur, paramètres en vigueur

---

4. Opérations de maintenance sur l'infrastructure GPO

Vérification de la réplication SYSVOL et AD

Outil	Commande	Usage
`repadmin`	`repadmin /showrepl`	Réplication AD entre DC
`repadmin`	`repadmin /replsummary`	Résumé de la santé de réplication
`dcdiag`	`dcdiag /test:sysvol`	Vérifier l'état SYSVOL
`dcdiag`	`dcdiag /v`	Diagnostic complet du DC

Journal Netlogon

Emplacement : `C:Windowsdebug etlogon.log`

Journalise les problèmes d'authentification, de découverte du DC et de traitement des GPO. Augmenter la verbosité : `nltest /dbflag:0x2080ffff`

Forcer la réplication AD entre DC

`ntdssite.msc` (Sites et services Active Directory) → développer `Sites` → développer le site → `NTDS Settings` du DC → clic droit sur la connexion de réplication → **Répliquer maintenant**

Forcer la mise à jour des GPO

- Localement : `gpupdate /force` depuis l'invite de commandes
- À distance depuis GPMC (Windows Server 2012 R2+) : clic droit sur une OU → **Mise à jour de la stratégie de groupe...** → sélectionner les ordinateurs cibles

Checklist de dépannage GPO

```
1. Vérifier que l'ordinateur/utilisateur est dans la bonne OU
2. Vérifier les filtres de sécurité (l'objet doit avoir "Lecture" et "Appliquer la stratégie de groupe")
3. Vérifier les filtres WMI éventuels
4. Vérifier l'héritage et les GPO bloquées
5. Lancer gpresult /h pour voir les GPO refusées et leur raison
6. Vérifier la réplication SYSVOL (gpotool.exe)
7. Consulter eventvwr.msc → Applications et services → Microsoft → Windows → Group Policy → Operational
```

Copier

Chapitre 12 — Implémentation du service de déploiement (WDS)

1. Présentation du boot PXE

PXE (Pre-boot eXecution Environment) permet à un ordinateur de démarrer depuis le réseau, sans OS ni média local.

Séquence de démarrage PXE détaillée

```
1. Le client s'allume → carte réseau diffuse une requête DHCP (broadcast)
   avec l'option 60 "PXEClient" pour signaler sa compatibilité PXE

2. Le serveur DHCP répond avec :
   - Une adresse IP (bail DHCP)
   - Option 66 : nom/IP du serveur TFTP (next-server)
   - Option 67 : nom du fichier de démarrage (ex: bootx64wdsnbp.com)

3. Le client télécharge le fichier de démarrage via TFTP (UDP 69)

4. Le NBP (Network Boot Program) s'exécute → affiche "Press F12 for network boot"

5. Si confirmé, WinPE se charge depuis le serveur WDS via TFTP

6. WinPE démarre → le client contacte le serveur WDS
   → affiche l'assistant de sélection d'image d'installation
```

Copier

> ***Cas particulier :*** *Si WDS est installé sur le même serveur que le DHCP, une configuration supplémentaire est nécessaire (options DHCP 60/66/67 ou listener PXE dédié sur WDS).*

---

2. Présentation et prérequis

Prérequis système

Prérequis	Détail
Active Directory DS	Domaine obligatoire, WDS doit être joint au domaine
Serveur DNS	Résolution des noms (requis par AD)
Serveur DHCP	Attribution des IP + options PXE 66/67
Volume NTFS	Dossier de stockage des images (hors volume système recommandé)
Compte administrateur	Droits d'administration locale et délégation AD
Bande passante réseau	Le transfert d'images (3-5 Go) peut saturer le réseau — prévoir la multidiffusion

Types d'images WDS

Type d'image	Description	Source
Image de démarrage	WinPE minimal pour démarrer depuis le réseau	`boot.wim` sur le DVD d'installation Windows
Image d'installation	OS complet à déployer	`install.wim` ou `install.esd` sur le DVD
Image de capture	WinPE spécialisé pour capturer un master Sysprep	Généré par WDS
Image découverte	Permet la découverte WDS depuis PXE sur un autre segment réseau	Généré par WDS

---

3. Mise en place de WDS

Installation du rôle

`Server Manager` → **Gérer** → **Ajouter des rôles et des fonctionnalités** → `Services de déploiement Windows` :

- Cocher **Serveur de déploiement** (moteur principal WDS)
- Cocher **Serveur Transport** (multidiffusion, transfert TFTP)

Configuration initiale

Après installation, dans la console `wdsmgmt.msc` (Services de déploiement Windows) :

1. Clic droit sur le serveur → **Configurer le serveur**
2. L'assistant démarre :
    - **Dossier de stockage** : ex. `D:RemoteInstall` (volume NTFS, espace suffisant pour les images)
    - **Paramètres du proxy DHCP** : si DHCP sur le même serveur → cocher "Ne pas écouter sur le port 67" et "Configurer les options DHCP"
    - **Réponse aux clients PXE** :
        - *Ne pas répondre* : WDS installé mais inactif
        - *Répondre uniquement aux clients connus* : seuls les ordinateurs

pré-enregistrés dans AD
    - *Répondre à tous les ordinateurs* : avec ou sans approbation administrateur

3. Ajouter une **image de démarrage** : clic droit sur `Images de démarrage` → **Ajouter une image de démarrage** → parcourir vers `boot.wim` sur le DVD → choisir l'architecture (x64) → nommer l'image

Configurer la multidiffusion (Multicast)

Pour les grands déploiements simultanés (économise la bande passante) :

1. Clic droit sur **Transmissions par multidiffusion** → **Créer une transmission par multidiffusion**
2. Nommer la transmission → sélectionner l'image d'installation concernée
3. Type de transmission :
    - **Démarrage automatique** : démarre quand N clients sont connectés ou après X minutes
    - **Planifié** : démarre à une heure précise

---

4. Déploiement d'un système d'exploitation

Ajouter des images d'installation

1. Clic droit sur **Images d'installation** → **Ajouter un groupe d'images** → nommer (ex: `Windows Server 2022`)
2. Dans le groupe créé → clic droit → **Ajouter une image d'installation**
3. Parcourir vers `install.wim` depuis le DVD Windows
4. Sélectionner les éditions à inclure (Standard, Datacenter, Desktop Experience...) → Suivant → Terminer

Démarrage d'un client via PXE

1. Configurer le BIOS/UEFI du poste client pour démarrer en **réseau (PXE)** en premier
2. Démarrer le poste → appuyer sur **F12** lorsque l'invite PXE s'affiche
3. WinPE se charge → l'assistant Windows Setup démarre
4. Choisir la langue, les paramètres régionaux → entrer les informations de connexion AD (compte autorisé à joindre des ordinateurs au domaine)
5. Sélectionner l'image d'installation souhaitée → choisir le disque → l'installation démarre

Pré-approuver un ordinateur

Pour les environnements avec "Répondre uniquement aux clients connus" :

`dsa.msc` → `Computers` → Nouveau ordinateur → renseigner le nom + l'adresse MAC ou UUID du BIOS

Ou dans `wdsmgmt.msc` → `Périphériques` → **Ajouter un périphérique**

---

5. Création d'un fichier de réponse (Unattend.xml)

Outil : Windows System Image Manager (WSIM)

Installé avec le **Windows ADK** (Assessment and Deployment Kit) téléchargeable sur le site Microsoft.

Procédure complète

1. Ouvrir **WSIM** (`Windows System Image Manager`)
2. `Fichier` → **Sélectionner une image Windows** → parcourir vers `install.wim` → choisir l'édition cible
3. WSIM génère le fichier `.clg` (catalogue des composants disponibles)
4. `Fichier` → **Nouveau fichier de réponse**
5. Dans le volet **Composants Windows**, ajouter les composants aux bonnes passes :

Passe	Moment	Composants typiques
windowsPE	Avant installation	Partitionnement, langue d'installation, clé de produit
offlineServicing	Offline, avant premier démarrage	Packages, pilotes
generalize	Pendant Sysprep	Paramètres de généralisation
specialize	Premier démarrage	Nom ordinateur, réseau, fuseau horaire
auditSystem	Mode audit	Outils de déploiement
auditUser	Mode audit	Configuration utilisateur
oobeSystem	Configuration initiale (OOBE)	Compte admin local, paramètres régionaux, suppression OOBE

6. Remplir les valeurs dans le volet **Propriétés** pour chaque composant ajouté
7. `Outils` → **Valider le fichier de réponse** → corriger les erreurs signalées
8. `Fichier` → **Enregistrer le fichier de réponse** → sauvegarder en `Unattend.xml`

Associer le fichier de réponse dans WDS

`wdsmgmt.msc` → clic droit sur l'image d'installation → **Propriétés** → onglet **Déploiement sans assistance** → **Activer le déploiement sans assistance pour cette image** → parcourir vers `Unattend.xml`

Exemple de paramètres courants dans Unattend.xml

Composant	Passe	Paramètre	Valeur exemple
`Microsoft-Windows-International-Core-WinPE`	windowsPE	UILanguage	`fr-FR`
`Microsoft-Windows-SetupDiskConfiguration`	windowsPE	Partitionnement automatique	Voir format GPT/MBR
`Microsoft-Windows-Shell-Setup`	specialize	ComputerName	`%MACHINENAME%` ou nom fixe
`Microsoft-Windows-Shell-Setup`	oobeSystem	HideEULAPage	`true`
`Microsoft-Windows-Shell-SetupUserAccountsLocalAccounts`	oobeSystem	Compte admin local	Nom + mot de passe

Chapitre 13 — Distribuer des mises à jour avec WSUS

1. Présentation de WSUS

WSUS (Windows Server Update Services) est un rôle Windows Server permettant de centraliser la gestion et la distribution des mises à jour Microsoft au sein du réseau d'entreprise.

Avantages

Avantage	Détail
Contrôle qualité	Tester les mises à jour sur un groupe pilote avant déploiement général
Économie de bande passante	Téléchargement unique depuis Internet, redistribution en LAN
Reporting	Tableau de bord de conformité par ordinateur, par groupe, par mise à jour
Déploiement ciblé	Groupes d'ordinateurs différenciés (serveurs, postes, filiales)
Planification	Déploiement hors heures de production

Architectures WSUS

Modèle	Description	Cas d'usage
WSUS autonome	Synchronise directement depuis Microsoft Update	Site unique
WSUS en cascade	Serveur aval synchronise depuis un serveur WSUS amont	Multi-sites
Réplica	Copie exacte de la configuration du serveur amont, sans autonomie de décision	Succursales

Ports utilisés par WSUS

Usage	Port	Protocole
Console d'administration	8530 (HTTP) / 8531 (HTTPS)	TCP
Clients vers serveur WSUS	8530 (HTTP) / 8531 (HTTPS)	TCP
Synchronisation amont	443	TCP (HTTPS)

---

2. Mise en place du serveur WSUS

Installation du rôle

`Server Manager` → **Ajouter des rôles et des fonctionnalités** → **Windows Server Update**

Services :

- **WSUS Services** : moteur principal
- **Base de données WID** : Windows Internal Database (recommandé pour < 30 000 clients), ou SQL Server existant
- **Interface utilisateur** : console de gestion

Configuration Post-déploiement

Après installation : bandeau d'avertissement dans Server Manager → **Lancer la configuration post-déploiement**

1. Dossier de stockage des mises à jour : `D:\WSUS` (prévoir **50 à 150 Go** selon les produits)
2. L'assistant configure WID et les répertoires nécessaires

Configuration initiale via la console Update Services

`Outils` → **Update Services** → clic droit sur le serveur → **Options** → **Assistant Configuration de WSUS** :

1. **Connexion en amont** : synchroniser depuis Microsoft Update (ou depuis un serveur WSUS amont)
2. **Proxy** : configurer si le serveur accède à Internet via un proxy
3. **Langues** : Français (fr), Anglais (en)
4. **Produits** (sélectionner selon l'infrastructure) :
    - Windows 11, Windows 10
    - Windows Server 2022, Windows Server 2019
    - Microsoft 365 Apps / Office
    - SQL Server (selon versions déployées)
5. **Classifications** :

Classification	Description
Mises à jour critiques	Correctifs pour des vulnérabilités critiques
Mises à jour de sécurité	Correctifs de sécurité importants
Service Packs	Packs de mises à jour cumulatifs
Mises à jour de définitions	Signatures antivirus/antimalware
Pilotes	Pilotes matériels (optionnel, déconseillé sur WSUS)
Outils	Outils Microsoft (MSRT...)

6. **Planification de la synchronisation** : quotidienne à 3h00 du matin (hors heures de bureau)
7. **Lancer la première synchronisation** : peut prendre plusieurs heures — vérifier la progression dans **État de la synchronisation**

---

3. Gestion de WSUS

Groupes d'ordinateurs

1. `Update Services` → `Ordinateurs` → **Tous les ordinateurs** → clic droit → **Ajouter un groupe d'ordinateurs**
2. Exemples de groupes recommandés :

Groupe	Usage
Postes Pilotes	Tester les mises à jour en premier
Postes Production	Après validation sur le groupe Pilotes
Serveurs Production	Mises à jour avec fenêtre de maintenance stricte
Contrôleurs de domaine	Traitement prioritaire et supervisé
Serveurs Backup	Déploiement différé

3. **Affecter les ordinateurs à un groupe** :
    - Méthode 1 — **Ciblage côté client via GPO** (recommandé) :
        - `Configuration ordinateur` → `Modèles d'administration` → `Composants Windows` → `Windows Update`
        - Activer **"Activer la mise à jour automatique côté client"**
        - Activer **"Spécifier l'emplacement intranet du service de mise à jour Microsoft"** → `http://wsus-srv:8530`
        - Activer **"Activer le ciblage côté client"** → saisir le nom du groupe WSUS
    - Méthode 2 — **Ciblage côté serveur** : dans la console WSUS → clic droit sur un ordinateur → **Modifier l'appartenance**

Approbation des mises à jour

1. `Mises à jour` → choisir la vue (ex: **Mises à jour critiques**, **Mises à jour de sécurité**)
2. Sélectionner une ou plusieurs mises à jour
3. Clic droit → **Approuver...**
4. Dans la fenêtre → choisir le groupe + l'action :
    - **Installer** : la mise à jour sera déployée
    - **Non approuvé** : état neutre (ni déployé, ni refusé)
    - **Refuser** : la mise à jour ne sera pas proposée
5. Pour les mises à jour urgentes : **Deadline** → forcer l'installation à une date/heure précise

Règles d'approbation automatique

`Options` → **Approbation automatique** → **Nouvelle règle** :

- Conditions : classification (ex: Mises à jour critiques ET Mises à jour de sécurité)
- Actions : approuver pour le groupe "Postes Pilotes"
- Utile pour automatiser l'approbation des patches de sécurité urgents

Nettoyage du serveur WSUS

À effectuer mensuellement : `Options` → **Nettoyage du serveur** → cocher toutes les options :

- Ordinateurs obsolètes non contactés depuis 30 jours
- Mises à jour inutiles (non approuvées depuis plus de 30 jours)
- Fichiers de mise à jour obsolètes (sur le disque)
- Révisions expirées de mises à jour → **Suivant** — le nettoyage peut prendre du temps sur un serveur vieillissant

---

4. Les rapports dans WSUS

Depuis `Update Services` → **Rapports**

> ***Prérequis :*** *Microsoft Report Viewer 2012 (ou version compatible) doit être installé sur la machine qui affiche les rapports.*

Rapport	Contenu	Usage
Récapitulatif des mises à jour	Nombre de mises à jour approuvées, refusées, en attente par groupe	Vue globale de la conformité
État détaillé des mises à jour	Par mise à jour : liste des ordinateurs conformes, non conformes, non applicables	Identifier les postes qui n'ont pas installé un patch critique
Récapitulatif des ordinateurs	Par ordinateur : état de conformité global, dernière synchronisation	Repérer les postes qui ne contactent plus WSUS
État de la synchronisation	Historique des synchronisations avec Microsoft Update	Détecter les échecs de synchronisation
Récapitulatif des paramètres	Configuration actuelle du serveur WSUS	Documentation et audit

Exporter un rapport

Dans la fenêtre de rapport → icône d'export → choisir le format (Excel, PDF, Word)

Chapitre 14 — Gestion et surveillance des serveurs

1. Gestionnaire des tâches (taskmgr)

Accès : `Ctrl + Shift + Échap` | clic droit sur la barre des tâches → **Gestionnaire des tâches** | `taskmgr` dans Exécuter

Onglets principaux

Onglet	Utilisation principale
Processus	Vue synthétique : applications + processus en arrière-plan avec CPU/RAM/Disque/Réseau en pourcentage
Performances	Graphiques en temps réel : CPU (par cœur), Mémoire, Disque, Réseau, GPU
Historique des applications	Consommation cumulée par application (applications Store)
Démarrage	Applications lancées au démarrage Windows → désactiver celles inutiles
Utilisateurs	Sessions actives (y compris RDP) et ressources consommées par utilisateur
Détails	Vue exhaustive des processus : PID, état, compte utilisateur, consommation, ligne de commande
Services	État de tous les services → démarrer/arrêter/redémarrer directement

Actions utiles

- Clic droit sur un processus → **Fin de tâche** (arrêt immédiat)
- Clic droit → **Définir la priorité** : Temps réel, Élevée, Au-dessus de la normale, Normale, En dessous de la normale, Basse
- Clic droit → **Affinité** : restreindre un processus à certains cœurs CPU
- Clic droit → **Créer un fichier de vidage** : générer un dump mémoire pour analyse

> *Dans l'onglet **Performances**, cliquer sur **Ouvrir le Moniteur de ressources** pour une vue plus détaillée.*

---

2. Moniteur de ressources (resmon.exe)

Accès : `resmon.exe` | Gestionnaire des tâches → Performances → **Ouvrir le Moniteur de ressources**

Outil plus détaillé que le Gestionnaire des tâches, utile pour diagnostiquer des lenteurs.

Onglets

Onglet	Métriques clés
Vue d'ensemble	Synthèse CPU, disque, réseau, mémoire sur une seule page avec sparklines
CPU	Processus avec utilisation CPU, threads actifs, handles ouverts, services associés
Mémoire	Répartition physique : En cours d'utilisation / En veille / Disponible / Modifiée — handles par processus
Disque	Activité I/O par processus : lecture/écriture en Ko/s, temps de réponse, files d'attente
Réseau	Connexions TCP actives par processus (IP locale, port, IP distante, état, latence)

Astuce diagnostic réseau

Onglet **Réseau** → développer **Connexions TCP** → identifier quel processus utilise une connexion réseau inhabituelle (détection de logiciels suspects, fuites de données)

---

3. Analyseur de performances (perfmon.exe)

Accès : `perfmon.exe` | `Server Manager` → Outils → **Analyseur de performances**

Analyse en temps réel

1. Dans le volet de gauche → **Analyseur de performances** → cliquer sur l'icône **+** (Ajouter des compteurs)
2. Sélectionner la catégorie (ex: Processeur, LogicalDisk, Memory, Network Interface, ASP.NET...)
3. Sélectionner les instances (ex: disque C:, interface Ethernet...)
4. Choisir le type d'affichage : **Graphe**, **Histogramme**, **Rapport**

Compteurs essentiels à surveiller

Compteur	Instance	Seuil d'alerte
`Processeur\% Temps processeur`	`_Total`	> 80% de manière prolongée
`MemoryMégaoctets disponibles`	—	< 200 Mo
`PhysicalDisk\% Temps disque`	Chaque disque	> 90%
`PhysicalDiskLongueur actuelle de la file d'attente`	Chaque disque	> 2 par disque
`Network InterfaceOctets total/s`	Carte réseau	> 80% de la capacité
`SystèmeLongueur de la file du processeur`	—	> 2 × nombre de cœurs
`ASP.NETRequêtes par seconde`	—	Selon baseline établie

Ensembles collecteurs de données (logging planifié)

1. `Ensembles collecteurs de données` → `Définis par l'utilisateur` → clic droit → **Nouveau** → **Ensemble collecteur de données**
2. Nom + type : **Créer manuellement (avancé)** → Créer des journaux de données → **Compteurs de performances**
3. Ajouter les compteurs → définir l'intervalle d'échantillonnage (ex: 15 secondes)
4. Onglet **Planification** : heure de début, heure d'arrêt, jours
5. Onglet **Condition d'arrêt** : durée maximale, taille maximale du fichier
6. Dossier de sortie : ex. `C:PerfLogsMon-Serveur`
7. Démarrer l'ensemble collecteur → les données sont enregistrées en fichier `.blg`
8. Double-cliquer sur le fichier `.blg` pour l'ouvrir dans perfmon et analyser les données historiques

Alertes de performance

1. Ensembles collecteurs → Nouveau → **Alerte**
2. Ajouter un compteur + seuil de déclenchement
3. Action : journaliser dans l'Observateur d'événements, envoyer un message réseau, démarrer un ensemble collecteur

---

4. L'environnement WinRE

Windows Recovery Environment — environnement de récupération basé sur WinPE, accessible avant le chargement de l'OS.

Accès à WinRE

Méthode	Procédure
Touche au démarrage	F8 ou F11 selon le BIOS/UEFI
Depuis Windows 10/11	`Paramètres` → `Mise à jour et sécurité` → `Récupération` → **Démarrage avancé** → Redémarrer maintenant
Depuis Windows Server	`Paramètres` → `Mise à jour et sécurité` → `Récupération`
Automatique	Windows déclenche WinRE automatiquement après 2 échecs de démarrage consécutifs
Depuis un support	Démarrer depuis le DVD/USB Windows → **Réparer l'ordinateur**

Options disponibles dans WinRE

Option	Description
Réparation automatique	Windows tente de corriger les problèmes de démarrage automatiquement (BCD, MBR, fichiers système)
Restauration du système	Revenir à un point de restauration créé par Windows ou manuellement
Récupération de l'image système	Restaurer depuis une image complète créée par Windows Server Backup (bare-metal restore)
Réinitialiser ce PC	Réinstallation de Windows avec conservation ou suppression des données personnelles
Invite de commandes	Accès en ligne de commande pour les corrections manuelles

Commandes clés depuis l'invite WinRE

Commande	Action
`bootrec /fixmbr`	Répare le Master Boot Record
`bootrec /fixboot`	Répare le secteur de démarrage de la partition active
`bootrec /rebuildbcd`	Reconstruit le magasin BCD (Boot Configuration Data)
`bootrec /scanos`	Recherche les installations Windows sur tous les disques
`sfc /scannow`	Vérifie et répare les fichiers système protégés
`dism /online /cleanup-image /restorehealth`	Répare l'image Windows via Windows Update
`diskpart`	Gestion des disques, partitions, volumes
`bcdedit`	Édition directe du Boot Configuration Data

---

5. L'Observateur d'événements (eventvwr.msc)

Accès : `eventvwr.msc` | `Server Manager` → Outils → **Observateur d'événements**

Structure des journaux

Journal	Contenu
Application	Événements des applications installées (SQL Server, IIS, Exchange...)
Sécurité	Connexions, audits, tentatives d'accès, gestion des comptes
Système	Événements du noyau Windows, pilotes, services système
Installation	Événements d'installation de rôles, fonctionnalités et mises à jour
Microsoft-Windows- (Applications et services)	Journaux spécifiques par rôle : DNS, DHCP, AD DS, Group Policy, WDS, WSUS...

Niveaux de sévérité

Icône	Niveau	Signification
Rouge (X)	**Critique**	Dysfonctionnement grave nécessitant une intervention immédiate
Rouge	**Erreur**	Problème significatif qui peut affecter les fonctionnalités
Jaune	**Avertissement**	Problème potentiel à surveiller
Blanc/Bleu	**Information**	Événement normal de fonctionnement
Bleu	**Audit de succès**	Opération auditée réussie (journal Sécurité)
Gris	**Audit d'échec**	Opération auditée échouée (journal Sécurité)

Filtrage des événements

Clic droit sur un journal → **Filtrer le journal actuel** :

- Par **niveau** : Critique, Erreur, Avertissement, Information
- Par **source** : nom du composant ou application
- Par **ID d'événement** : ex. `4625` pour les échecs de connexion
- Par **plage de dates**
- Par **utilisateur** ou **ordinateur**

IDs d'événements importants à surveiller

ID	Journal	Signification
4624	Sécurité	Ouverture de session réussie
4625	Sécurité	Échec d'ouverture de session
4648	Sécurité	Ouverture de session avec informations d'identification explicites
4720	Sécurité	Création d'un compte utilisateur
4726	Sécurité	Suppression d'un compte utilisateur
4732	Sécurité	Ajout d'un membre à un groupe local sécurisé
4740	Sécurité	Compte utilisateur verrouillé
6005	Système	Le service Journal des événements a démarré (démarrage de l'OS)
6006	Système	Le service Journal des événements va s'arrêter (arrêt propre de l'OS)
6008	Système	Arrêt inattendu du système
41	Système	Redémarrage sans arrêt propre (kernel power)
1074	Système	Arrêt/redémarrage initié par un utilisateur ou une application

Vues personnalisées

`Observateur d'événements` → **Vues personnalisées** → clic droit → **Créer une vue personnalisée** :

- Filtrer sur plusieurs journaux simultanément
- Sauvegarder pour une utilisation récurrente
- Partager la vue entre administrateurs (export XML)

Abonnements (centralisation des logs)

1. `Observateur d'événements` → **Abonnements** → **Créer un abonnement**
2. Nommer l'abonnement
3. Type :
    - **Lancé par le collecteur** : le serveur central interroge les serveurs sources (nécessite configuration WinRM sur les sources)
    - **Lancé par la source** : les serveurs sources envoient les événements au collecteur
4. Sélectionner les **ordinateurs sources** → `Sélectionner des ordinateurs...`

5. Sélectionner les **événements** → `Sélectionner des événements...` → filtrer par journal, ID, niveau
6. Les événements collectés apparaissent dans `Journaux Windows` → **Événements transférés**

> ***Prérequis côté source :*** *`winrm quickconfig` doit avoir été exécuté, et le service `Windows Remote Management` doit être actif et autorisé dans le pare-feu.*

---

6. Le pare-feu Windows Defender (wf.msc)

Accès : `wf.msc` | `Panneau de configuration` → `Pare-feu Windows Defender` → `Paramètres avancés`

Profils réseau

Profil	S'applique quand
Domaine	L'ordinateur est joint au domaine et le DC est accessible
Privé	Réseau identifié comme privé (confiance accordée manuellement)
Public	Réseau non identifié, Wi-Fi public — règles les plus restrictives

> *Pour chaque profil : activé/désactivé, comportement des connexions entrantes/sortantes (bloquer, autoriser), notifications.*

Créer une règle de trafic entrant

1. `Règles de trafic entrant` → **Nouvelle règle...** (volet Actions)
2. **Type de règle** :
   - *Programme* : bloquer/autoriser une application spécifique
   - *Port* : selon le numéro de port TCP/UDP
   - *Prédéfini* : règles préconfigurées Windows (Bureau à distance, DNS, DHCP...)
   - *Personnalisé* : combinaison de programme + port + adresse IP
3. **Protocole et ports** : TCP/UDP → numéro(s) de port
4. **Étendue** : limiter à certaines adresses IP sources/destinations
5. **Action** :
   - *Autoriser la connexion*
   - *Autoriser la connexion si elle est sécurisée* (IPsec)
   - *Bloquer la connexion*
6. **Profils** : cocher Domaine, Privé, Public selon le besoin
7. **Nom** : nommer la règle de manière descriptive (ex: `RDP-Helpdesk-Entrant-TCP3389`)

Exporter / Importer les règles de pare-feu

`wf.msc` → clic droit sur **Pare-feu Windows Defender avec sécurité avancée** → **Exporter la stratégie...** → fichier `.wfw`

Pour importer sur un autre serveur : **Importer la stratégie...**

Règles de sécurité de connexion (IPsec)

Permettent de chiffrer et/ou d'authentifier les communications entre machines spécifiques :

- **Isolation** : seuls les ordinateurs du domaine peuvent communiquer
- **Exemption d'authentification** : exclure certaines IPs de l'IPsec
- **Tunnel** : VPN site à site
- **Personnalisé** : règles granulaires

---

7. Sauvegarde avec Windows Server Backup

Installation : `Server Manager` → **Fonctionnalités** → **Sauvegarde Windows Server**

Console : `Server Manager` → section `Windows Server Backup` | ou snap-in MMC `wbadmin.msc`

Types de sauvegarde

Type	Description	Espace disque	Durée
Complète (Full)	Tous les volumes/fichiers sélectionnés	Important	Longue
Incrémentielle	Seulement les modifications depuis la dernière sauvegarde	Faible	Rapide
Différentielle	Modifications depuis la dernière sauvegarde complète	Moyen	Moyenne
État du système	Registre, AD DS, SYSVOL, BCD, fichiers système	~10-20 Go	Rapide

> *Windows Server Backup utilise le service VSS (Volume Shadow Copy Service) pour sauvegarder des fichiers ouverts sans interruption de service.*

Planifier une sauvegarde

1. `Actions` → **Planifier la sauvegarde...**
2. **Configuration de la sauvegarde** :
   - *Serveur complet* : sauvegarde tous les volumes (recommandé pour bare-metal restore)
   - *Personnalisé* : sélectionner des volumes ou dossiers spécifiques
3. **Heure de sauvegarde** : une ou plusieurs fois par jour → choisir l'heure(s)
4. **Type de destination** :
   - *Disque dédié* : un disque entier réservé à la sauvegarde (recommandé — gestion automatique de la rétention)
   - *Dossier partagé distant* : `\SRV-BACKUPsauvegardes` (une seule sauvegarde conservée)
   - *Volumes* : volume local spécifique
5. Confirmer et **Terminer**

Sauvegarde manuelle

`Actions` → **Sauvegarder une fois...** → mêmes options que la planification

Restauration

- `Actions` → **Récupérer...** → l'assistant propose de récupérer :
  - Fichiers et dossiers (niveau fichier)
  - Volumes complets
  - Applications (Exchange, SQL Server avec leurs plugins VSS)
  - État du système
- Depuis **WinRE** → **Récupération de l'image système** → restauration bare-metal complète

Surveillance et alertes

- Les événements de sauvegarde/restauration sont journalisés dans `eventvwr.msc` → `Applications et services` → `Microsoft` → `Windows` → `Backup`
- ID 4 : sauvegarde réussie
- ID 5 : sauvegarde échouée

Chapitre 15 — PowerShell

> ***Note :*** *Ce chapitre est le seul à utiliser PowerShell. Toutes les procédures des chapitres précédents s'effectuent via les consoles graphiques Windows.*

1. Introduction à PowerShell

Historique

Version	Année	Nouveautés clés
PowerShell 1.0	2006	Naissance de PS, cmdlets de base
PowerShell 2.0	2009	Remoting (WinRM), Modules, ISE, Background Jobs
PowerShell 3.0	2012	Workflows, Scheduled Jobs, CIM cmdlets
PowerShell 4.0	2013	DSC (Desired State Configuration)
PowerShell 5.0	2015	Classes, PSGallery, JEA, OneGet
PowerShell 5.1	2016	Intégré à Windows Server 2016/2019/2022
PowerShell 7+	2020+	Cross-platform (Windows/Linux/macOS), open-source, moteur .NET Core

PowerShell vs CMD

Critère	CMD	PowerShell
Type de sortie	Texte brut	Objets .NET (propriétés et méthodes)
Pipeline	Texte → texte	Objet → objet
Scripts	`.bat` / `.cmd`	`.ps1`
Modules	Non	Oui (`Import-Module`)
Gestion à distance	Limitée (`psexec`)	WinRM / `Enter-PSSession` / `Invoke-Command`
Complétude fonctionnelle	Partielle	Accès complet à .NET et WMI/CIM
Gestion des erreurs	`errorlevel`	`try/catch/finally`, `$Error`, `-ErrorAction`

Concepts fondamentaux

- **Cmdlet** : commande native PowerShell au format `Verbe-Nom` (ex: `Get-Process`, `Stop-Service`, `New-ADUser`)
- **Pipeline** : le symbole `|` transmet des **objets** (pas du texte) d'une cmdlet à la suivante
- **Objet** : toute valeur en PS est un objet avec des **propriétés** (données) et des **méthodes** (actions)
- **Module** : regroupement de cmdlets, fonctions, variables (ex: `ActiveDirectory`, `DHCPServer`, `DNSServer`, `NetTCPIP`)
- **Provider** : interface pour naviguer dans des datastores comme un système de fichiers (`FileSystem`, `Registry`, `Certificate`, `AD`)

Politique d'exécution

```
Get-ExecutionPolicy                          # Voir la politique actuelle
Get-ExecutionPolicy -List                    # Voir par portée (MachinePolicy, UserPolicy,
Process, CurrentUser, LocalMachine)
Set-ExecutionPolicy RemoteSigned             # Autoriser les scripts locaux + les scripts
distants signés
Set-ExecutionPolicy AllSigned                # Exiger la signature pour tous les scripts
(production)
Set-ExecutionPolicy Bypass -Scope Process    # Bypass uniquement pour la session en cours
(sans modifier le registre)
```

Copier

Politique	Scripts locaux	Scripts distants/téléchargés
`Restricted`	Interdit	Interdit (par défaut client)
`AllSigned`	Autorisé si signé	Autorisé si signé
`RemoteSigned`	Autorisé	Autorisé si signé
`Unrestricted`	Autorisé	Autorisé (avec avertissement)
`Bypass`	Tout autorisé	Tout autorisé

Interfaces disponibles

Interface	Description	Usage recommandé
Windows PowerShell ISE	Éditeur graphique avec débogueur, coloration syntaxique, panneau de commandes	Scripts simples, Windows uniquement
Terminal PowerShell	Console classique, démarrage rapide	Commandes interactives
VS Code + extension PowerShell	Éditeur complet, débogage avancé, IntelliSense	Scripts complexes et projets
Windows Terminal	Terminal moderne, onglets, profils	Usage quotidien recommandé

---

2. Aide avec PowerShell

```
# Mettre à jour l'aide (une fois, connexion Internet requise)
Update-Help -Force
Update-Help -UICulture fr-FR -Force          # En français

# Obtenir l'aide d'une cmdlet
Get-Help Get-Process                          # Aide de base
Get-Help Get-Process -Full                    # Aide complète avec tous les paramètres
Get-Help Get-Process -Examples                # Uniquement les exemples pratiques
Get-Help Get-Process -Online                  # Ouvrir la documentation en ligne dans le
navigateur
Get-Help Get-Process -ShowWindow              # Afficher dans une fenêtre séparée

# Rechercher des cmdlets par mot-clé
Get-Help *service*                            # Toutes les rubriques d'aide contenant
"service"
Get-Help about_*                              # Lister les rubriques conceptuelles

# Découvrir les cmdlets disponibles
Get-Command                                   # Toutes les cmdlets, fonctions, alias
Get-Command -Verb Get                         # Toutes les cmdlets Get-*
Get-Command -Noun Process                     # Toutes les cmdlets *-Process
Get-Command -Module ActiveDirectory           # Cmdlets du module AD
Get-Command -CommandType Function             # Uniquement les fonctions

# Découvrir les propriétés et méthodes d'un objet
Get-Process | Get-Member                      # Propriétés et méthodes d'un objet Process
Get-Service | Get-Member
"Bonjour" | Get-Member                        # Membres d'une chaîne de caractères

# Alias courants
Get-Alias                                     # Lister tous les alias
Get-Alias ls                                  # Voir quel alias correspond à ls
```

Copier

---

3. La syntaxe PowerShell

Variables

```
$nom = "Serveur01"                          # Chaîne (String)
$age = 5                                    # Entier (Int32)
$actif = $true                              # Booléen
$pi = 3.14                                  # Décimal (Double)
$liste = @("srv1", "srv2", "srv3")          # Tableau (Array)
$table = @{Nom = "Jean"; Age = 30}          # Table de hachage (Hashtable)
$null                                       # Valeur nulle

# Variables typées
[string]$texte = "Hello"
[int]$nombre = 42
[datetime]$date = Get-Date

# Variables spéciales
$_                                          # Élément courant dans un pipeline
$?                                          # $true si la dernière commande a réussi
$LASTEXITCODE                               # Code de retour de la dernière commande
externe
$PSVersionTable                             # Version de PowerShell
$env:COMPUTERNAME                           # Variables d'environnement
$env:USERNAME
$env:PATH
```

Copier

Opérateurs de comparaison

Opérateur	Signification	Exemple
`-eq`	Égal à	`$a -eq $b`
`-ne`	Différent de	`$a -ne $b`
`-gt`	Supérieur à	`$a -gt 5`
`-ge`	Supérieur ou égal	`$a -ge 5`
`-lt`	Inférieur à	`$a -lt 5`
`-le`	Inférieur ou égal	`$a -le 5`
`-like`	Correspond au motif (wildcards `*` et `?`)	`$nom -like "Srv*"`
`-notlike`	Ne correspond pas	`$nom -notlike "PC*"`
`-match`	Correspond à l'expression régulière	`$ip -match "^192.168."`
`-notmatch`	Ne correspond pas à la regex	`$email -notmatch "@test"`
`-contains`	Le tableau contient la valeur	`$liste -contains "srv1"`
`-notcontains`	Le tableau ne contient pas la valeur	`$liste -notcontains "srv4"`
`-in`	La valeur est dans le tableau	`"srv1" -in $liste`
`-notin`	La valeur n'est pas dans le tableau	`"srv4" -notin $liste`

Opérateurs logiques : `-and`, `-or`, `-not`, `-xor`

Conditions

```
if ($service.Status -eq "Running") {
    Write-Host "Service actif" -ForegroundColor Green
} elseif ($service.Status -eq "Stopped") {
    Write-Host "Service arrêté" -ForegroundColor Yellow
} else {
    Write-Host "État inconnu : $($service.Status)" -ForegroundColor Red
}

# Switch (pour de multiples cas)
switch ($code) {
    200 { Write-Host "OK" }
    404 { Write-Host "Non trouvé" }
    500 { Write-Host "Erreur serveur" }
    default { Write-Host "Code inconnu : $code" }
}
```

Copier

Gestion des erreurs

```
try {
    Get-Content "C:fichier-inexistant.txt" -ErrorAction Stop
}
catch [System.IO.FileNotFoundException] {
    Write-Host "Fichier introuvable : $_" -ForegroundColor Red
}
catch {
    Write-Host "Erreur inattendue : $($_.Exception.Message)" -ForegroundColor Red
}
finally {
    Write-Host "Bloc finally toujours exécuté"
}
```

Copier

Cmdlets essentielles

```
# --- SERVICES ---
Get-Service                                  # Lister tous les services
Get-Service -Name "wuauserv"                 # Détails d'un service spécifique
Get-Service | Where-Object {$_.Status -eq "Stopped"} | Select-Object Name, DisplayName
Start-Service -Name "Spooler"               # Démarrer un service
Stop-Service -Name "Spooler"                # Arrêter un service
Restart-Service -Name "Spooler" -Force      # Redémarrer un service
Set-Service -Name "Spooler" -StartupType Automatic  # Modifier le type de démarrage

# --- PROCESSUS ---
Get-Process                                  # Lister les processus
Get-Process -Name "explorer"                 # Processus par nom
Get-Process | Sort-Object CPU -Descending | Select-Object -First 10  # Top 10 CPU
Stop-Process -Name "notepad" -Force         # Forcer l'arrêt d'un processus
Stop-Process -Id 1234                        # Arrêt par PID

# --- FICHIERS ET DOSSIERS ---
Get-ChildItem C:Windows                     # Lister (alias : ls, dir, gci)
Get-ChildItem C:Logs -Recurse -Filter "*.log"  # Récursif avec filtre
New-Item -Path "C:Test" -ItemType Directory    # Créer un dossier
New-Item -Path "C:Testfichier.txt" -ItemType File -Value "Contenu"
Copy-Item "C:Source*" "D:Destination" -Recurse  # Copier récursivement
Move-Item "C:Sourcefichier.txt" "D:Destination"
Remove-Item "C:Temp*" -Recurse -Force     # Supprimer récursivement
Get-Content "C:Logsapp.log" -Tail 50      # Lire les 50 dernières lignes

# --- FILTRAGE, TRI, SÉLECTION ---
Get-Service | Where-Object {$_.Status -eq "Running" -and $_.StartType -eq "Automatic"}
Get-Process | Sort-Object CPU -Descending
Get-Process | Select-Object Name, CPU, WorkingSet -First 20
Get-ADUser -Filter * | Select-Object Name, SamAccountName, Enabled | Sort-Object Name

# --- MISE EN FORME ET EXPORT ---
Get-Service | Format-Table Name, Status, StartType -AutoSize
Get-Process | Format-List Name, Id, CPU, WorkingSet  # Format liste détaillée
Get-Process | Export-Csv C:processus.csv -NoTypeInformation -Encoding UTF8
Get-Process | ConvertTo-Json | Out-File C:processus.json
Import-Csv C:utilisateurs.csv              # Lire un fichier CSV
Get-Service | Out-GridView                  # Affichage dans une grille interactive
(filtrable)

# --- RÉSEAU ---
Test-Connection -ComputerName "SRV01" -Count 4   # Ping
Test-NetConnection -ComputerName "SRV01" -Port 443  # Test port TCP
Get-NetAdapter                               # Cartes réseau
Get-NetIPAddress                            # Adresses IP configurées
Resolve-DnsName -Name "www.google.com"      # Résolution DNS
```

Copier

Active Directory

```
Import-Module ActiveDirectory              # Charger le module AD (automatique sur DC)

# --- UTILISATEURS ---
# Créer un utilisateur
New-ADUser `
    -Name "Jean Dupont" `
    -GivenName "Jean" `
    -Surname "Dupont" `
    -SamAccountName "jdupont" `
    -UserPrincipalName "jdupont@nouvy.lan" `
    -Path "OU=Utilisateurs,DC=nouvy,DC=lan" `
    -AccountPassword (ConvertTo-SecureString "P@ssw0rd!" -AsPlainText -Force) `
    -ChangePasswordAtLogon $true `
    -Enabled $true `
    -Department "Informatique" `
    -Title "Technicien"

Get-ADUser -Identity "jdupont" -Properties *         # Tous les attributs
Get-ADUser -Filter {Name -like "Jean*"} -Properties Department, Title
Get-ADUser -Filter {Enabled -eq $false}              # Comptes désactivés
Get-ADUser -Filter {PasswordLastSet -lt (Get-Date).AddDays(-90)}  # MDP > 90 jours
Set-ADUser -Identity "jdupont" -Title "Chef de projet" -Department "DSI"
Disable-ADAccount -Identity "jdupont"
Enable-ADAccount -Identity "jdupont"
Set-ADAccountPassword -Identity "jdupont" -NewPassword (ConvertTo-SecureString
"NouveauP@ss!" -AsPlainText -Force) -Reset
Unlock-ADAccount -Identity "jdupont"               # Déverrouiller un compte
Remove-ADUser -Identity "jdupont" -Confirm:$false

# --- GROUPES ---
New-ADGroup `
    -Name "GRP-Compta" `
    -GroupScope Global `
    -GroupCategory Security `
    -Path "OU=Groupes,DC=nouvy,DC=lan" `
    -Description "Groupe sécurité comptabilité"

Add-ADGroupMember -Identity "GRP-Compta" -Members "jdupont", "mmartin"
Remove-ADGroupMember -Identity "GRP-Compta" -Members "mmartin" -Confirm:$false
Get-ADGroupMember -Identity "Domain Admins" -Recursive
Get-ADPrincipalGroupMembership -Identity "jdupont"  # Groupes d'un utilisateur

# --- ORDINATEURS ---
New-ADComputer -Name "PC-BUREAU01" -Path "OU=Postes,DC=nouvy,DC=lan"
Get-ADComputer -Filter {Name -like "PC-*"} -Properties LastLogonDate, OperatingSystem
Get-ADComputer -Filter {LastLogonDate -lt (Get-Date).AddDays(-60)}  # Postes inactifs

# --- OUs ---
New-ADOrganizationalUnit -Name "TestUsers" -Path "OU=Utilisateurs,DC=nouvy,DC=lan"
Get-ADOrganizationalUnit -Filter * | Select-Object Name, DistinguishedName
```

Copier

DHCP

```
Import-Module DHCPServer

# Étendues
Add-DhcpServerv4Scope `
    -Name "LAN-Bureau" `
    -StartRange 192.168.1.100 `
    -EndRange 192.168.1.200 `
    -SubnetMask 255.255.255.0 `
    -State Active `
    -LeaseDuration (New-TimeSpan -Days 8)

Get-DhcpServerv4Scope                          # Lister les étendues
Set-DhcpServerv4Scope -ScopeId 192.168.1.0 -State Inactive  # Désactiver une étendue

# Exclusions et réservations
Add-DhcpServerv4ExclusionRange -ScopeId 192.168.1.0 -StartRange 192.168.1.100 -EndRange
192.168.1.110
Add-DhcpServerv4Reservation -ScopeId 192.168.1.0 -IPAddress 192.168.1.50 -ClientId "AA-BB-
CC-DD-EE-FF" -Name "Imprimante-Hall"

# Baux actifs
Get-DhcpServerv4Lease -ScopeId 192.168.1.0
Get-DhcpServerv4Lease -ScopeId 192.168.1.0 | Where-Object {$_.AddressState -eq "Active"}
```

Copier

DNS

```
Import-Module DNSServer

# Zones
Add-DnsServerPrimaryZone -Name "nouvy.lan" -ZoneFile "nouvy.lan.dns" -DynamicUpdate Secure
Add-DnsServerSecondaryZone -Name "nouvy.lan" -ZoneFile "nouvy.lan.dns" -MasterServers
192.168.1.1
Get-DnsServerZone                               # Lister les zones

# Enregistrements
Add-DnsServerResourceRecordA -ZoneName "nouvy.lan" -Name "srv-web" -IPv4Address
"192.168.1.20" -TimeToLive (New-TimeSpan -Hours 1)
Add-DnsServerResourceRecordCName -ZoneName "nouvy.lan" -Name "www" -HostNameAlias "srv-
web.nouvy.lan"
Add-DnsServerResourceRecordMX -ZoneName "nouvy.lan" -Name "@" -MailExchange "mail.nouvy.lan"
-Preference 10
Get-DnsServerResourceRecord -ZoneName "nouvy.lan" -RRType "A"
Remove-DnsServerResourceRecord -ZoneName "nouvy.lan" -Name "srv-web" -RRType "A" -
Confirm:$false
```

Copier

DFS

```
# Espace de noms DFS
New-DfsnRoot -TargetPath "\SRV01DFS" -Type DomainV2 -Path "\nouvy.lanDFS"
New-DfsnFolder -Path "\nouvy.lanDFSPartages" -TargetPath "\SRV01Partages"
New-DfsnFolder -Path "\nouvy.lanDFSLogiciels" -TargetPath "\SRV01Logiciels"

# Réplication DFS (DFS-R)
New-DfsReplicationGroup -GroupName "Replication-Partages"
Add-DfsrMember -GroupName "Replication-Partages" -ComputerName "SRV01", "SRV02"
New-DfsReplicatedFolder -GroupName "Replication-Partages" -FolderName "Partages" -DfsnPath
"\nouvy.lanDFSPartages"
Add-DfsrConnection -GroupName "Replication-Partages" -SourceComputerName "SRV01" -
DestinationComputerName "SRV02"
Get-DfsrState -GroupName "Replication-Partages"   # État de la réplication
```

Copier

---

4. Les boucles avec PowerShell

foreach — itérer sur une collection

```
$serveurs = @("SRV01", "SRV02", "SRV03", "SRV04")
foreach ($serveur in $serveurs) {
    $ping = Test-Connection -ComputerName $serveur -Count 1 -Quiet
    $statut = if ($ping) { "En ligne" } else { "Hors ligne" }
    $couleur = if ($ping) { "Green" } else { "Red" }
    Write-Host "$serveur : $statut" -ForegroundColor $couleur
}
```

Copier

ForEach-Object — dans un pipeline

```
# $_ représente l'élément courant
Get-ADUser -Filter {Enabled -eq $false} | ForEach-Object {
    Write-Host "Compte désactivé : $($_.SamAccountName) — Dernier login :
$($_.LastLogonDate)"
}

# Avec bloc begin/process/end
Get-Service | ForEach-Object -Begin {
    $count = 0
} -Process {
    if ($_.Status -eq "Stopped") { $count++ }
} -End {
    Write-Host "Nombre de services arrêtés : $count"
}
```

Copier

for — boucle avec compteur

```
# Créer 10 comptes de test
for ($i = 1; $i -le 10; $i++) {
    $login = "user{0:D2}" -f $i        # user01, user02... user10
    New-ADUser `
        -Name "Utilisateur Test $i" `
        -SamAccountName $login `
        -UserPrincipalName "$login@nouvy.lan" `
        -Path "OU=TestUsers,DC=nouvy,DC=lan" `
        -AccountPassword (ConvertTo-SecureString "P@ssw0rd$i!" -AsPlainText -Force) `
        -Enabled $true
    Write-Host "Créé : $login" -ForegroundColor Green
}
```

Copier

while — tant que la condition est vraie

```
$tentative = 0
$maxTentatives = 5
while ($tentative -lt $maxTentatives) {
    $tentative++
    $ping = Test-Connection -ComputerName "SRV01" -Count 1 -Quiet
    if ($ping) {
        Write-Host "SRV01 est en ligne (tentative $tentative)" -ForegroundColor Green
        break
    }
    Write-Host "Tentative $tentative/$maxTentatives — Hors ligne, nouvel essai dans 10
secondes..."
    Start-Sleep -Seconds 10
}
if ($tentative -eq $maxTentatives -and -not $ping) {
    Write-Host "SRV01 inaccessible après $maxTentatives tentatives" -ForegroundColor Red
}
```

Copier

do-while — exécuter au moins une fois

```
do {
    $reponse = Read-Host "Continuer ? (o/n)"
} while ($reponse -ne "n" -and $reponse -ne "N")
Write-Host "Script terminé."
```

Copier

Exemple pratique — créer des comptes depuis un fichier CSV

Fichier `C:utilisateurs.csv` :

```
Prenom,Nom,Service,OU
Jean,Dupont,Informatique,"OU=DSI,OU=Utilisateurs,DC=nouvy,DC=lan"
Marie,Martin,Comptabilité,"OU=Compta,OU=Utilisateurs,DC=nouvy,DC=lan"
Pierre,Bernard,Direction,"OU=Direction,OU=Utilisateurs,DC=nouvy,DC=lan"
```

Copier

Script de création :

```
$mdpDefaut = ConvertTo-SecureString "Bienvenue1!" -AsPlainText -Force
$rapport = @()

Import-Csv "C:utilisateurs.csv" -Delimiter "," | ForEach-Object {
    # Construire le login : 1ère lettre prénom + nom (en minuscules, sans accents)
    $prenomSansAccent = $_.Prenom -replace '[éèêë]','e' -replace '[àâ]','a' -replace
'[ùû]','u' -replace '[îï]','i' -replace '[ôö]','o'
    $nomSansAccent    = $_.Nom    -replace '[éèêë]','e' -replace '[àâ]','a' -replace
'[ùû]','u' -replace '[îï]','i' -replace '[ôö]','o'
    $login = "$($prenomSansAccent.Substring(0,1).ToLower())$($nomSansAccent.ToLower())"

    try {
        New-ADUser `
            -GivenName $_.Prenom `
            -Surname $_.Nom `
            -Name "$($_.Prenom) $($_.Nom)" `
            -SamAccountName $login `
            -UserPrincipalName "$login@nouvy.lan" `
            -Department $_.Service `
            -Path $_.OU `
            -AccountPassword $mdpDefaut `
            -ChangePasswordAtLogon $true `
            -Enabled $true `
            -ErrorAction Stop

        Write-Host "OK : $login ($($_.Prenom) $($_.Nom))" -ForegroundColor Green
        $rapport += [PSCustomObject]@{Login=$login; Nom="$($_.Prenom) $($_.Nom)";
Statut="Créé"; Erreur=""}
    }
    catch {
        Write-Host "ERREUR : $login — $($_.Exception.Message)" -ForegroundColor Red
        $rapport += [PSCustomObject]@{Login=$login; Nom="$($_.Prenom) $($_.Nom)";
Statut="Erreur"; Erreur=$_.Exception.Message}
    }
}

# Exporter le rapport de création
$rapport | Export-Csv "C:
apport-creation-comptes.csv" -NoTypeInformation -Encoding UTF8
Write-Host "`nRapport exporté : C:
apport-creation-comptes.csv"
```

Copier

---

5. PowerShell V5

Classes PowerShell

PowerShell 5 introduit la définition de **classes orientées objet** :

```
class Serveur {
    [string]$Nom
    [string]$IP
    [string]$Role
    [bool]$Actif

    # Constructeur
    Serveur([string]$nom, [string]$ip, [string]$role) {
        $this.Nom    = $nom
        $this.IP     = $ip
        $this.Role   = $role
        $this.Actif  = $true
    }

    # Méthode
    [string] TestConnectivite() {
        $ok = Test-Connection -ComputerName $this.IP -Count 1 -Quiet
        return if ($ok) { "$($this.Nom) : En ligne" } else { "$($this.Nom) : Hors ligne" }
    }

    # Méthode statique
    static [string] FormatIP([string]$ip) {
        return "IP : $ip"
    }
}

# Utilisation
$dc  = [Serveur]::new("DC01", "192.168.1.1", "Contrôleur de domaine")
$web = [Serveur]::new("SRV-WEB", "192.168.1.20", "Serveur Web")

$dc.TestConnectivite()
$web.TestConnectivite()
[Serveur]::FormatIP("192.168.1.50")

# Tableau de serveurs
$serveurs = @($dc, $web)
$serveurs | ForEach-Object { $_.TestConnectivite() }
```

Copier

Héritage de classes

```
class ServeurDC : Serveur {
    [string]$NomDomaine

    ServeurDC([string]$nom, [string]$ip, [string]$domaine) : base($nom, $ip, "DC") {
        $this.NomDomaine = $domaine
    }

    [string] GetFQDN() {
        return "$($this.Nom).$($this.NomDomaine)"
    }
}

$dc1 = [ServeurDC]::new("DC01", "192.168.1.1", "nouvy.lan")
$dc1.GetFQDN()       # DC01.nouvy.lan
$dc1.TestConnectivite()   # Héritée de la classe Serveur
```

Copier

PowerShellGet et PSGallery

PowerShell Gallery (https://www.powershellgallery.com) est le dépôt officiel de modules PowerShell.

```
# Découvrir
Find-Module -Name "*AD*"                    # Rechercher par nom
Find-Module -Tag "Azure"                    # Rechercher par tag
Find-Module -Command "Get-DiskSpace"        # Rechercher par cmdlet incluse

# Installer
Install-Module -Name PSWindowsUpdate -Scope AllUsers  # Pour tous les utilisateurs
Install-Module -Name ImportExcel            # Manipuler des fichiers Excel sans Excel
Install-Module -Name Posh-SSH               # Connexions SSH depuis PS

# Gérer
Get-InstalledModule                         # Lister les modules installés
Update-Module -Name PSWindowsUpdate         # Mettre à jour un module
Uninstall-Module -Name PSWindowsUpdate      # Désinstaller

# Modules utiles en administration Windows
Install-Module -Name PSWindowsUpdate        # Gérer Windows Update par PS
Install-Module -Name ImportExcel            # Lire/écrire des fichiers Excel
Install-Module -Name Pester                 # Framework de tests unitaires pour PS
Install-Module -Name PSScriptAnalyzer       # Analyser et corriger le style de code PS
```

Copier

DSC — Desired State Configuration

DSC permet de déclarer l'**état souhaité** d'une machine et d'y veiller automatiquement.

```
# Installer le module de ressources DSC nécessaire
Install-Module -Name PSDesiredStateConfiguration -Force

# Définir la configuration
Configuration MonServeurWeb {
    param ([string[]]$ComputerName = "localhost")

    Import-DscResource -ModuleName PSDesiredStateConfiguration

    Node $ComputerName {

        # Installer IIS
        WindowsFeature IIS {
            Ensure = "Present"
            Name   = "Web-Server"
        }

        # Installer ASP.NET 4.8
        WindowsFeature ASPNET {
            Ensure    = "Present"
            Name      = "Web-Asp-Net45"
            DependsOn = "[WindowsFeature]IIS"
        }

        # Assurer que le service W3SVC est démarré
        Service W3SVC {
            Ensure    = "Present"
            State     = "Running"
            Name      = "W3SVC"
            DependsOn = "[WindowsFeature]IIS"
        }

        # Assurer la présence d'un fichier de configuration
        File ConfigIIS {
            Ensure          = "Present"
            Type            = "File"
            DestinationPath = "C:inetpubwwwrootweb.config"
            Contents        = "<configuration></configuration>"
            DependsOn       = "[WindowsFeature]IIS"
        }
    }
}

# Générer le fichier MOF (document de configuration)
MonServeurWeb -ComputerName "SRV-WEB01"   # Crée .MonServeurWebSRV-WEB01.mof

# Appliquer la configuration
Start-DscConfiguration -Path .MonServeurWeb -Wait -Verbose -Force

# Vérifier la conformité
Test-DscConfiguration -ComputerName "SRV-WEB01"   # Retourne $true si conforme

# Obtenir l'état actuel
Get-DscConfiguration -CimSession "SRV-WEB01"
```

Copier

JEA — Just Enough Administration

JEA permet de **limiter les droits PowerShell Remoting** à un périmètre précis, sans

accorder des droits d'administrateur complets.

Cas d'usage type : Le helpdesk peut réinitialiser les mots de passe AD via PowerShell, sans avoir les droits Domain Admin.

```
# 1. Créer un dossier pour les fichiers JEA
New-Item -Path "C:JEARoleCapabilities" -ItemType Directory -Force

# 2. Créer un fichier de capacités de rôle (.psrc)
New-PSRoleCapabilityFile -Path "C:JEARoleCapabilitiesHelpdesk.psrc"

# Éditer Helpdesk.psrc pour autoriser uniquement :
# VisibleCmdlets = @(
#     'Get-ADUser',
#     @{Name='Set-ADAccountPassword'; Parameters=@{Name='Identity'}, @{Name='NewPassword'},
@{Name='Reset'}}
#     'Unlock-ADAccount',
#     'Get-ADGroupMember'
# )
# VisibleFunctions = 'Get-Help', 'Exit-PSSession'

# 3. Créer le fichier de configuration de session (.pssc)
New-PSSessionConfigurationFile `
    -Path "C:JEAJEA-Helpdesk.pssc" `
    -SessionType RestrictedRemoteServer `
    -RunAsVirtualAccount `
    -RoleDefinitions @{
        "NOUVYHelpdesk" = @{RoleCapabilities = "Helpdesk"}
    } `
    -LanguageMode NoLanguage

# 4. Enregistrer la configuration de session JEA
Register-PSSessionConfiguration -Name "JEA-Helpdesk" -Path "C:JEAJEA-Helpdesk.pssc" -Force

# 5. Se connecter à la session JEA (depuis le poste helpdesk)
Enter-PSSession -ComputerName "DC01" -ConfigurationName "JEA-Helpdesk"
# Dans la session : seules les cmdlets autorisées sont disponibles
```

Copier

Journalisation et transcription

```
# Transcription manuelle — enregistre toute la session dans un fichier texte
Start-Transcript -Path "C:Logssession-$(Get-Date -Format 'yyyyMMdd-HHmm').txt" -Append
# ... exécuter des commandes ...
Stop-Transcript

# Journalisation des modules (enregistre dans l'Observateur d'événements)
$LogModulePref = @{ EnableModuleLogging = $true; ModuleNames = @("ActiveDirectory",
"DHCPServer") }
Set-ExecutionPolicy RemoteSigned
# Via GPO : Configuration ordinateur → Modèles d'administration → Windows PowerShell →
Activer la journalisation des modules

# Script Block Logging (enregistre le contenu des scripts exécutés)
# Via GPO : Configuration ordinateur → Modèles d'administration → Windows PowerShell →
Activer la journalisation de bloc de script

# Vérifier les événements PS dans l'observateur
Get-WinEvent -LogName "Microsoft-Windows-PowerShell/Operational" -MaxEvents 50 |
    Where-Object {$_.Id -eq 4104} |        # ID 4104 = Script Block Logging
    Select-Object TimeCreated, Message |
    Format-List
```

Copier

Scripts utilitaires courants

```
# Inventaire rapide des serveurs du domaine
Get-ADComputer -Filter {OperatingSystem -like "Windows Server*"} -Properties
OperatingSystem, LastLogonDate |
    Select-Object Name, OperatingSystem, LastLogonDate |
    Sort-Object OperatingSystem |
    Export-Csv "C:inventaire-serveurs.csv" -NoTypeInformation -Encoding UTF8

# Rapport des comptes AD inactifs depuis 90 jours
$dateRef = (Get-Date).AddDays(-90)
Get-ADUser -Filter {LastLogonDate -lt $dateRef -and Enabled -eq $true} `
    -Properties LastLogonDate, Department |
    Select-Object Name, SamAccountName, Department, LastLogonDate |
    Export-Csv "C:comptes-inactifs.csv" -NoTypeInformation -Encoding UTF8

# Vérifier la réplication AD sur tous les DC
Import-Module ActiveDirectory
$dcs = Get-ADDomainController -Filter *
foreach ($dc in $dcs) {
    Write-Host "`n=== $($dc.Name) ===" -ForegroundColor Cyan
    repadmin /showrepl $dc.Name
}

# LAPS — Étendre le schéma et configurer les permissions (étape serveur)
# Prérequis : LAPS installé avec les outils de gestion
Import-Module AdmPwd.PS
Update-AdmPwdADSchema                                # Étendre le schéma AD
Set-AdmPwdComputerSelfPermission -OrgUnit "OU=Postes,DC=nouvy,DC=lan"  # Les postes peuvent
mettre à jour leur propre MDP
Set-AdmPwdReadPasswordPermission -OrgUnit "OU=Postes,DC=nouvy,DC=lan" -AllowedPrincipals
"NOUVYHelpdesk"  # Helpdesk peut lire les MDP
```

Copier

Récapitulatif général

Chapitre	Sujet	Console principale	Commande de lancement
1	Active Directory DS	Utilisateurs et ordinateurs AD	`dsa.msc`
2	Gestionnaire de serveur	Server Manager	`servermanager.exe`
3	Objets AD	Utilisateurs et ordinateurs AD	`dsa.msc`
4	DHCP	Console DHCP	`dhcpmgmt.msc`
5	Services réseau	Centre Réseau et partage	`ncpa.cpl`
6	DNS	Console DNS	`dnsmgmt.msc`
7	Serveur de fichiers	Explorateur + Server Manager	`explorer.exe`
8	DFS	Console DFS	`dfsmgmt.msc`
9	**Stratégies de groupe**	**Gestion des GPO**	**`gpmc.msc`**
10	**Sécurité**	**Stratégie de sécurité locale**	**`secpol.msc`**
11	**Dépannage GPO**	**RSoP + GPMC**	**`rsop.msc` / `gpmc.msc`**
12	**WDS**	**Services de déploiement**	**`wdsmgmt.msc`**
13	**WSUS**	**Update Services**	**`wsus.msc`**
14	**Surveillance**	**Analyseur de performances**	**`perfmon.exe`**
15	**PowerShell**	**PowerShell ISE / Terminal**	**`powershell_ise.exe`**

Ports réseau importants à retenir

Service	Port(s)	Protocole
DNS	53	TCP/UDP
DHCP	67 (serveur), 68 (client)	UDP
Kerberos	88	TCP/UDP
LDAP	389	TCP/UDP
LDAPS	636	TCP
SMB / Partages de fichiers	445	TCP
RDP (Bureau à distance)	3389	TCP
HTTPS	443	TCP
WinRM (PowerShell Remoting)	5985 (HTTP), 5986 (HTTPS)	TCP
WSUS	8530 (HTTP), 8531 (HTTPS)	TCP
TFTP (WDS/PXE)	69	UDP

Commandes de diagnostic rapide

Problème	Commande à lancer
Quelle GPO s'applique ?	`gpresult /r` ou `gpresult /h C:
apport.html`	
Les GPO sont-elles bien répliquées ?	`gpotool.exe /verbose`
Le domaine est-il atteignable ?	`nltest /dsgetdc:nouvy.lan`
La réplication AD fonctionne-t-elle ?	`repadmin /replsummary`
Le DC est-il sain ?	`dcdiag /v`
SYSVOL est-il répliqué ?	`dcdiag /test:sysvol`
Forcer la mise à jour des GPO	`gpupdate /force`

Dernière mise à jour : avril 2026 — Windows Server 2022 / Windows 11