FICHE DE RÉVISION — ACTIVE DIRECTORY & GPO

1. Active Directory — Fondamentaux

L'Active Directory (AD) est un annuaire d'objets (comptes utilisateurs, ordinateurs, groupes, DNS…) basé sur le protocole LDAP (norme X.500 — ouverte et interopérable). Il fonctionne en couche 7 (Application) du modèle OSI.

Objectif principal : sécurité centralisée

DOMAINE AD : Ensemble d'ordinateurs qui partagent la même politique de sécurité. On choisit quels ordinateurs en font partie.

- Domaine AD = ensemble de machines qui partagent la même politique de sécurité
- Le DC (Domain Controller) héberge la Base des comptes AD — une super SAM valable sur tout le domaine
- L'AD dépend du DNS — sans DNS, l'AD ne fonctionne pas. Les erreurs AD viennent souvent du DNS.

	Workgroup	Domaine AD
Gestion sécurité	Locale — via SAM de chaque PC	Centralisée — via Base des comptes AD sur le DC
Connexion	Uniquement sur la machine locale	Sur n'importe quel PC du domaine
Politique commune	Non — chaque PC pour soi	Oui — même politique sur tout le parc

SÉCURITÉ AD — QUI / QUOI / COMMENT (QQC)

QUI = Identifier quelle personne / quel utilisateur. Ce sont les identités, les logins.
QUOI = Ce sont les ressources. Qui peut accéder à quoi.
COMMENT = Avec quelles autorisations on accède à la ressource et on peut interagir avec elle. C'est le droit qu'on donne sur la ressource.

Kerberos — mécanique d'authentification

Acteur	Rôle
DC	Contrôleur de Domaine — délivre les jetons Kerberos
Client Kerberos	Ordinateurs membres du domaine AD
Jeton Kerberos	Photo des droits d'accès de l'utilisateur au moment de la connexion. Durée de vie : 10 heures.

Le jeton est une photo des droits au moment de la connexion. Si les droits sont modifiés en cours de session, l'utilisateur doit se déconnecter/reconnecter pour obtenir un nouveau jeton.

DNS et Active Directory

L'enregistrement SRV est crucial : c'est lui qui permet aux clients de localiser les DC sur le réseau. Sans SRV, pas d'authentification possible.

Enregistrement	Nom	Rôle
A	Hôte	Nom → IP
CNAME	Alias	Nom → un autre nom
SRV	Service	Permet aux clients de trouver un service sur le réseau — crucial pour l'AD (les clients trouvent les DC via SRV).

Forêt et relations d'approbation

FORÊT AD : Ensemble de domaines AD reliés entre eux par des relations d'approbation bidirectionnelles et transitives.

- Bidirectionnelle : si A fait confiance à B, B fait confiance à A
- Transitive : si A↔B et B↔C, alors A fait confiance à C (même sans lien direct)
- Traverser le pont d'approbation nécessite quand même une autorisation de l'admin

Réplication des DC

- Réplication automatique toutes les 15 minutes entre DC
- Horodatage pour arbitrer les conflits (MAJ la plus récente gagne)
- Intérêt : redondance du service + équilibrage de charge
- Catalogue Global (GC) : DC qui contient l'intégralité des objets de la forêt et garantit l'unicité

Ne jamais déplacer les contrôleurs de domaine hors de leur conteneur Domain Controllers.

2. Structure AD — Unités d'Organisation (OU)

Les OU sont les "dossiers" de l'AD. Elles permettent d'organiser les objets hiérarchiquement. Supprimer une OU supprime TOUT son contenu. Par défaut elles sont protégées contre la suppression accidentelle.

Raison de créer une OU	Explication
1. Organiser	Structurer les objets AD : utilisateurs, ordinateurs, groupes. Comme des dossiers Windows.
2. Délégation de contrôle	Donner des droits d'administration partiels sur une OU à un utilisateur ou groupe, sans en faire un Domain Admin.
3. Lier des GPO	Appliquer des stratégies de groupe (GPO) ciblées sur un ensemble précis d'objets.

Activation des fonctionnalités avancées

Affichage → Fonctionnalités avancées → fait apparaître les conteneurs système cachés et l'onglet Objet dans les propriétés de chaque OU.

- Pour supprimer une OU protégée : propriétés → onglet Objet → décocher "Protéger l'objet des suppressions accidentelles"
- Attention aux conteneurs système qui apparaissent — ne jamais les supprimer

Exemple de structure OU

```
Domaine
  └── Bordeaux
        ├── Utilisateurs
        ├── Ordinateurs
        ├── Groupes
        ├── RH
        └── Informatique
```

> *Déplacer un objet d'une OU vers une autre change les GPO qui s'appliquent à lui. Les déplacements ont un réel impact — ne pas le faire sans réflexion.*

Comptes utilisateurs — paramètres importants

Paramètre	Usage
Contraintes horaires	Restreindre les heures de connexion autorisées
Connexion sur ordinateurs précis	Limiter la connexion à certaines machines uniquement
Date de péremption du compte	Idéal pour les stagiaires ou CDD — le compte s'expire automatiquement
Script d'ouverture de session	Script .bat exécuté à l'ouverture de session (ex : net use pour lecteur réseau)
Chemin du profil itinérant	\\serveur\profils\%username% — le profil suit l'utilisateur sur n'importe quel PC

Modèles utilisateurs

- Créer un compte modèle par type de profil (_MODELE_Comptabilité, _MODELE_RH…)
- Pré-configuré avec : script d'ouverture de session, chemin profil itinérant, groupes AGDLP
- Le modèle doit être DÉSACTIVÉ pour éviter son utilisation comme vrai compte
- Nommer avec underscore → remonte en haut de la liste et immédiatement identifiable
- Créer un nouvel utilisateur = copier le modèle → tous les paramètres et groupes remontent automatiquement

3. Permissions NTFS — ACL (Access Control List)

Les ACL contrôlent qui peut faire quoi sur les ressources (fichiers, dossiers, objets). Un fichier hérite des permissions de son dossier parent, qui hérite de son parent, jusqu'à la racine (C:\).

N°	Droit	Ce qu'il permet
1	Affichage du contenu	Voir la liste des fichiers/dossiers d'un répertoire
2	Lecture	Lire le contenu des fichiers
3	**Lecture + Exécution (RX)**	Lire et exécuter les fichiers (programmes, scripts). Usage quotidien le plus courant.
4	Écriture	Créer des fichiers et dossiers
5	**Modification (RXWD)**	Lire + Exécuter + Écrire + Supprimer. Modifier, renommer, déplacer. Usage quotidien le plus courant.
6	**Contrôle total**	Tous les droits + modifier les ACL elles-mêmes. Réservé aux admins. Utilisateurs = JAMAIS.
7	Autorisation spéciale	Granularité maximale — quand les droits standards ne suffisent pas ou sont trop génériques.

> *Les utilisateurs ne doivent JAMAIS avoir le Contrôle total. En quotidien : Lecture+Exécution (RX) ou Modification (RXWD).*

Identités spéciales

Identité	Description
SYSTEM	Compte utilisé par les services Windows (dont antivirus). Ne jamais toucher.
Administrateurs locaux	Groupe local sur chaque machine. Les Admins du Domaine y sont ajoutés automatiquement.
Utilisateurs authentifiés	Tout utilisateur avec compte valide dans un domaine approuvé. Exclut les anonymes.
Utilisateurs interactifs	Utilisateurs qui ont ouvert une session physique sur la machine.
Créateur Propriétaire	Celui qui a créé l'objet. A des autorisations spéciales sur sa propre création. Peut modifier ses permissions → masquer l'onglet Sécurité via GPO pour contrer.

Règles de gestion des ACL

Refus explicite (DENY) écrase toujours un Autoriser, quelle que soit la source.

- Éviter les refus explicites — mieux vaut ne pas donner le droit que le refuser explicitement
- Le refus sert uniquement à gérer des exceptions, pas la gestion courante des droits
- On n'ajoute JAMAIS des utilisateurs en direct sur les ACL — on passe TOUJOURS par des groupes
- Héritage : un objet hérite des permissions de son parent. Peut être coupé manuellement.

Appropriation

Un administrateur peut prendre possession (s'approprier) d'un objet dont il n'a pas accès, même sans permissions. Mécanisme de dernier recours si l'ancien propriétaire a modifié les autorisations.

> *Si un admin s'approprie le profil itinérant d'un utilisateur pour le dépanner, cela coupe la relation d'itinérance. Il faut remettre l'utilisateur en propriétaire après.*

4. AGDLP — Méthode Microsoft de gestion des permissions

La méthode recommandée par Microsoft pour gérer proprement les droits dans un domaine AD. Sépare QUI sont les gens (Global) de CE à quoi ils ont accès (Domaine Local).

Lettre	Signification	Rôle
A	Account (Compte)	L'utilisateur qu'on ajoute
G	Groupe Global	Regroupe les utilisateurs par métier/rôle. On gère LES PERSONNES ici. Ne peut contenir que des users/groupes du même domaine.
DL	Domaine Local	Regroupe les accès par ressource. On gère LES DROITS ici. Peut contenir des groupes globaux de n'importe quel domaine approuvé.
P	Permission	Les droits NTFS appliqués sur la ressource (RX, RXWD…). On applique les permissions AU GROUPE DOMAINE LOCAL, jamais à un user directement.

Exemple concret

```
Pierre (Account)
  └── GG_Comptabilité (Groupe Global → les PERSONNES)
        └── DL_Accès_Factures_RX (Domaine Local → les DROITS)
              └── Lecture sur \\SRV-Fichiers\Factures (Permission)
```

Pour chaque ressource, on crée 2 groupes Domaine Local : un RX (lecture) et un RXWD (écriture). On met ensuite les bons Groupes Globaux dedans.

> *Quand Pierre change de service : on le retire du Groupe Global → aucune permission à toucher, tout se met à jour automatiquement.*

Étendues de groupe

Étendue	Portée	Peut contenir
Domaine Local	Ressources du domaine local uniquement (Mono-domaine)	Users locaux, groupes globaux, groupes universels, groupes de domaines approuvés
Global	N'importe quel domaine approuvé (Multi-domaine)	Uniquement users et groupes globaux du MÊME domaine
Universel	Toute la forêt	Users, groupes globaux et universels de n'importe quel domaine de la forêt

> *En mono-domaine, l'étendue n'a pas d'incidence. C'est en multi-domaine qu'il faut choisir soigneusement.*

5. Partage de ressources — NTFS + Partage réseau

En cas de conflit entre autorisations NTFS et autorisations de Partage, c'est la PLUS RESTRICTIVE des deux qui s'applique.

Identités dans les ACL de partage

Identité	Ce qu'elle inclut	Usage recommandé
Tout le monde	Utilisateurs domaine + anonymes + autres forêts + comptes locaux. Aucun contrôle.	**SUPPRIMER. Trop permissif.**
Utilisateurs authentifiés	Tout utilisateur avec un compte valide dans un domaine approuvé. Exclut les anonymes.	Compromis rapide. Tout le domaine peut accéder.
Groupes métier (AGDLP)	Uniquement les membres du groupe concerné.	Bonne pratique optimale. Contrôle précis par service.
Créateur Propriétaire	Celui qui a créé le fichier/dossier. Autorisations spéciales sur sa propre création.	Conserver. L'utilisateur contrôle ses propres créations.

- En pratique : la sécurité est gérée au niveau NTFS. Le RSSI demande de sécuriser les deux couches (partage + ACL) — si erreur dans l'une, l'autre compense.

Chemin UNC

Pour accéder à une ressource partagée en réseau :

```
\\nom_machine_ou_IP\nom_du_partage
```

C'est un nom NetBIOS. Exemple : \\SRVPA03\travail

Énumération basée sur l'accès

Paramètre du partage réseau : l'utilisateur ne voit dans le partage QUE les dossiers auxquels il a accès. Les autres sont invisibles, pas juste inaccessibles.

```
Partage → Paramètres → Activer l'énumération basée sur l'accès
```

Lecteur réseau via script SYSVOL

Pour éviter que l'utilisateur tape l'UNC manuellement → créer un fichier .bat dans SYSVOL : \nom_domaine\SYSVOL\scripts

```
net use t: \\srvpa03\travail
```

Puis ajouter ce script dans le profil utilisateur (onglet Profil → Script d'ouverture de session).

Imprimantes

- Périphérique d'impression = le matériel physique avec une IP réseau (TCP/IP : IP, masque, GW, DNS)
- Imprimante = l'objet logique Windows (file d'attente, pilote, configuration partagée)
- Serveur d'impression = centralise tout. Si l'imprimante change, seul le serveur est reconfiguré, les postes clients ne voient rien.
- Droits sur imprimante : Imprimer (base) | Gestion documents (file d'attente) | Gérer l'imprimante (admin uniquement)

Renommage d'un dossier partagé

> *Renommer un dossier partagé casse le partage et réinitialise les autorisations. Procédure : 1) Vérifier si partagé 2) Renommer 3) Refaire le partage 4) Refaire TOUTES les autorisations.*

6. Profils itinérants

Le profil (bureau, documents, registre NTUser.DAT…) suit l'utilisateur sur n'importe quel PC du domaine. Utile pour les bureaux partagés, call centers, etc.

Action	Ce qui se passe
Ouverture de session	Téléchargement (download) du profil depuis le serveur de fichiers vers le poste
Fermeture de session	Téléversement (upload) du profil vers le serveur de fichiers

- Chemin générique : \\srvpa03\profils\%username% (le .V6 = version Windows, ajouté automatiquement)
- TOUJOURS fermer la session — éteindre sans fermer = profil non téléversé = modifications perdues
- Dernier fermé = référence. En cas de sessions simultanées, le dernier à fermer écrase tous les autres.

> *Configurer la GPO profils itinérants sur Configuration ORDINATEUR (pas utilisateur) → lier à l'OU contenant les PC clients. Ne pas lier au domaine entier (les serveurs n'ont pas besoin de profils itinérants).*

7. Délégation de contrôle & RSAT

Permet de donner des droits d'administration partiels sur une OU, sans en faire un Domain Admin.

Option	Description
Option 1 — Accès au DC ❌	Laisser l'utilisateur se connecter au DC. TRÈS MAUVAISE IDÉE. Un DC ne doit être accessible qu'aux admins.
Option 2 — RSAT + Délégation ☑	Installer les outils RSAT sur le poste de l'utilisateur + déléguer uniquement les droits nécessaires sur son OU. Il administre depuis son poste sans jamais toucher au DC.

Droits délégables courants : réinitialiser les MDP, créer/supprimer des utilisateurs, gérer les membres d'un groupe, modifier les attributs utilisateurs.

RSAT — Remote Server Administration Tools

Outils d'administration Windows (dsa.msc, DNS, DHCP, GPO…) installés sur un poste client pour administrer le serveur à distance.

```
Paramètres → Applications → Fonctionnalités facultatives → Ajouter → RSAT
```

8. Requêtes LDAP

Les requêtes LDAP dans "Requêtes enregistrées" de dsa.msc permettent de filtrer rapidement les objets AD sans naviguer manuellement OU par OU.

Exemples de requêtes

```
Tous les utilisateurs actifs :
  (&(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

```
Membres d'un groupe (distinguishedName obligatoire — le nom simple ne fonctionne pas) :
  (&(objectClass=user)(memberOf=CN=Service Compta,OU=GROUPES,OU=PSG,DC=DOMPA,DC=LAN))
```

> *Le distinguishedName d'un groupe se récupère via : dsa.msc → Affichage → Fonctionnalités avancées → propriétés du groupe → onglet Éditeur d'attributs → attribut distinguishedName.*

Les requêtes peuvent être sauvegardées dans la MMC pour réutilisation. La MMC permet de centraliser plusieurs snap-ins (AD, DNS, DHCP, GPO…) en un seul tableau de bord.

9. GPO — Group Policy Objects

Ensemble de paramètres de configuration appliqués à des utilisateurs ou ordinateurs dans un domaine AD. GPO = niveau domaine. gpedit.msc = niveau local uniquement.

À quoi ça sert

- Verrouillage de l'environnement utilisateur (masquer onglet Sécurité, restreindre panneau de configuration…)
- Remplacer les scripts de connexion (lecteurs réseau, imprimantes mappées)
- Installer des logiciels (format MSI obligatoire — setup.exe ne fonctionne pas)
- Modifier la sécurité locale (politique de MDP, pare-feu, arrêt/redémarrage, audit)
- Modifier la SAM locale des machines du domaine

Ordre d'application — LSDOU

Ordre	Niveau	Remarque
1	**L — Local**	gpedit.msc sur la machine locale. Appliqué en premier donc écrasé par tout le reste.
2	**S — Site**	GPO liée au site AD (géographique). Peu utilisé.
3	**D — Domaine**	GPO liée au domaine. S'applique à tous les objets du domaine.
4	**OU — Unité d'Organisation**	GPO liée à l'OU. Appliqué EN DERNIER donc prioritaire en cas de conflit. Plus proche de l'objet = prioritaire.

> *LSDOU à retenir absolument. En cas de conflit, le dernier appliqué gagne (le plus proche de l'objet = l'OU). GPO asynchrone : délai jusqu'à 90 min. Forcer : gpupdate*

Héritage, Blocage et Appliquer (Enforced)

Mécanisme	Description
Héritage	Par défaut, les GPO s'appliquent en cascade de parent en enfant dans l'arborescence des OU.
Bloquer l'héritage	L'OU n'hérite plus des GPO parentes. Limite : un GPO lié directement à cette OU s'applique quand même.
Appliquer (Enforced)	Force l'application du GPO même si l'héritage est bloqué. Priorité absolue — ne peut pas être contourné.
Désactiver le lien	Alternative à la suppression du lien — moins d'effets de bord. Le GPO existe toujours, il ne s'applique plus à cette OU.

> *On ne supprime JAMAIS un GPO lui-même depuis une OU — on supprime le LIEN. Le GPO continue d'exister et s'applique ailleurs. Vérifier toujours les autres liaisons avant de modifier un GPO.*

Ordre des liens (Link Order)

En cas de GPO contradictoires sur une même OU, l'ordre des liens détermine la priorité. Plus le numéro est bas, plus la priorité est haute. Ordre 1 bat ordre 3.

Filtrage de sécurité

- Pour cibler à qui s'applique un GPO au sein d'une même OU
- 1. Retirer 'Utilisateurs Authentifiés' (trop générique)
- 2. Remettre 'Ordinateurs du domaine' — si l'ordinateur ne peut pas lire le GPO, il ne peut pas le télécharger
- 3. Ajouter le groupe de filtrage : GF - [Ce que fait le GPO]

> *Convention de nommage : GF = Groupe de Filtrage. Le GPO ne s'applique qu'aux membres du groupe. Être dans l'OU + être dans le groupe de filtrage = les deux conditions sont nécessaires.*

Ciblage (Item-level Targeting)

Dans les Préférences GPO, on peut cibler un élément précis (ex : un mappage de lecteur) indépendamment du filtrage de sécurité. Plus fin que le filtrage — au niveau de l'élément lui-même.

Nommage des GPO

Le nom doit être explicite et descriptif. Exemples : MASQUER ONGLET SECURITE / INSTALLER FIREFOX / DESACTIVER MISE EN VEILLE ECRAN

10. GPO — Fonctionnalités détaillées

Mapper lecteurs réseau via GPO

Configuration utilisateur → Préférences → Paramètres Windows → Mappages de lecteurs → Nouveau → Lecteur mappé

- Définir la lettre et le chemin réseau (ex : \\serveur\partage)
- Remplace les scripts .bat dans SYSVOL — méthode moderne
- Possible d'ajouter un ciblage pour restreindre à certains groupes

Redirection de dossier

Configuration utilisateur → Stratégies → Paramètres Windows → Redirection de dossiers → Documents → Propriétés

- Redirige un dossier local (Documents) vers un partage réseau sur le serveur de fichiers
- Attention : 'Accorder droits exclusifs' → admin ne peut plus accéder sans appropriation
- Attention : 'Déplacer le contenu' → Cut/Paste vers le serveur, anticiper la volumétrie (quotas !)

Disponible hors connexion (Offline Files)

Les données du partage réseau sont copiées en local. En cas de réseau indisponible, l'utilisateur travaille sur la copie locale. Synchronisation à la reconnexion.

> *Limite volumétrie : la copie locale = taille du partage réseau. Un partage de 500 Go = 500 Go sur le disque local. Les quotas sont essentiels.*

Installation de logiciels via GPO

Méthode	Description
Configuration ordinateur	Logiciel installé au DÉMARRAGE de la machine. Redémarrage nécessaire. Méthode préférée — on cible des machines précises.
Configuration utilisateur	Logiciel installé à l'OUVERTURE DE SESSION. Attention : s'installe sur TOUTES les machines où l'utilisateur se connecte.

- Prérequis : dossier partagé sur le réseau + fichier MSI (setup.exe ne fonctionne pas)
- Dans le filtrage : ne pas laisser 'Ordinateurs du domaine' — créer un groupe GF dédié avec les postes cibles

Arrêt automatique des postes via GPO

Configuration utilisateur → Préférences → Paramètres du Panneau de configuration → Tâches planifiées → Nouveau → Tâche planifiée (min. Windows 7)

- Compte : System (saisir manuellement — ne pas utiliser le bouton Modifier)
- Action : Démarrer un programme → C:\Windows\System32\shutdown.exe
- Arguments : /s /t 0 (arrêt) ou /r /t 0 (redémarrage)
- Utiliser des filtres WMI pour éviter que le GPO s'applique aux serveurs

Modification de la SAM locale via GPO

Configuration ordinateur → Préférences → Paramètres du Panneau de configuration → Utilisateurs et groupes locaux → Groupe local

- Ajouter un groupe domaine dans les Administrateurs locaux des postes : Action 'Mettre à jour' (pas Remplacer)
- 'Remplacer' écrase tous les membres existants — risque de supprimer des accès critiques

Empêcher la mise en veille de l'écran

Configuration ordinateur → Stratégies → Modèles d'administration → Système → Gestion de l'alimentation → Paramètres de l'affichage et de la vidéo

```
Paramètre : Désactiver l'affichage (sur secteur) → Activé → valeur : 0 (jamais)
```

Déployer une adresse DNS auxiliaire

Configuration ordinateur → Stratégies → Paramètres Windows → Scripts (démarrage) → Démarrage

```
netsh interface ip add dns name="Ethernet" addr=X.X.X.X index=2
```

> *Le nom de l'interface (Ethernet, Ethernet0...) peut varier selon les machines — à vérifier sur les postes clients.*

11. Stratégies de mot de passe & verrouillage

Stratégie de mot de passe

Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies de comptes → Stratégie de mot de passe

Paramètre	Description / Valeur recommandée
Longueur minimale	Nombre de caractères minimum. Recommandé : 8 à 12 caractères.
Complexité	Force majuscules + minuscules + chiffres + caractères spéciaux. Activé = obligatoire.
Durée de vie maximale	Expiration obligatoire après X jours. Ex : 42 jours. Doit fonctionner avec historique.
Durée de vie minimale	Empêche de changer trop vite pour contourner l'historique. Ex : 1 jour.
Historique des mots de passe	Nombre de mots de passe mémorisés. Ex : 24. Sans historique, l'expiration ne sert à rien.
Chiffrement réversible	= stocker en clair. TOUJOURS DÉSACTIVÉ sauf besoin applicatif très spécifique.

> *La stratégie de mot de passe définie dans la Default Domain Policy s'applique à TOUS les comptes du domaine. C'est le seul endroit efficace pour les comptes de domaine — une GPO liée à une OU n'a pas d'effet.*

> *Les 3 paramètres interdépendants : durée max + durée min + historique. Sans les 3 configurés ensemble, la politique est contournable.*

Stratégie de verrouillage du compte

Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies de comptes → Stratégie de verrouillage

Paramètre	Description
Seuil de verrouillage	Nombre de tentatives échouées avant verrouillage. 0 = jamais verrouillé (dangereux).
Durée de verrouillage	Durée avant déverrouillage automatique. 0 = intervention manuelle d'un admin obligatoire.
Réinitialiser le compteur après	Délai en minutes après lequel le compteur de tentatives est remis à zéro.

> *Seuil à 0 = verrouillage désactivé. N'importe qui peut tenter un nombre illimité de mots de passe sans conséquence.*

Fine-Grained Password Policy (stratégie affinée)

Permet d'avoir des politiques de mot de passe différentes selon les groupes (ex : politique plus stricte pour les admins).

- Configuration : Centre d'administration AD → DOMPA (local) → System → Password Settings Container → Nouveau
- En cas de conflit entre deux stratégies affinées sur un même utilisateur → priorité la plus basse gagne
- S'applique directement à un groupe (pas à une OU)

12. Corbeille AD & Réplication DNS intégrée

Corbeille Active Directory

Par défaut, un objet supprimé dans l'AD est définitivement perdu. La Corbeille AD permet de restaurer des objets supprimés avec tous leurs attributs intacts.

- Activation : Centre d'administration AD → DOMPA (local) → clic droit → Activer la Corbeille
- L'activation est IRRÉVERSIBLE
- Restaurer → remet dans l'OU d'origine | Restaurer sur... → OU au choix

> *La Corbeille ne fonctionnera pas fiablement tant que tous les DC de la forêt n'ont pas répliqué le changement de configuration.*

Réplication DNS intégrée à AD

Méthode	Description
Sans AD (classique)	Zone principale (écriture) + zones secondaires (lecture seule). Transferts de zone à configurer manuellement.
Avec AD (intégrée)	Les données DNS sont dans la base AD. Le second DC avec rôle DNS réplique automatiquement via la réplication AD. Pas besoin de zones secondaires ni de transferts manuels. Les deux DC ont chacun une copie en écriture.

```
repadmin /syncall  → forcer la réplication des DC
```

13. Commandes et outils AD — référence

Commande	Usage
dsa.msc	Utilisateurs et ordinateurs Active Directory
gpmc.msc	Console de gestion des stratégies de groupe (GPO)
gpupdate	Applique uniquement les GPO modifiées ou nouvelles depuis la dernière mise à jour
gpupdate /force	Force la réapplication de TOUTES les GPO. Attention sur grand nombre de machines simultanément → surcharge le DC.
gpresult -r	Affiche les GPO appliquées sur la machine/l'utilisateur courant
whoami	Affiche le compte connecté. Permet de savoir si on est sur un compte local (SAM) ou domaine (AD).
sysdm.cpl	Propriétés système → pour joindre/quitter un domaine
.\nom_utilisateur	Forcer la connexion avec un compte local (SAM) quand on ne connaît pas le nom de la machine
repadmin /syncall	Forcer la réplication des DC (DNS intégré AD)
net use t: \\srv\partage	Connecter un lecteur réseau en lettre depuis un script .bat dans SYSVOL

> *Règle de sécurité N°1 : Le compte Administrateur ne s'appelle pas Administrateur. Utiliser un nom courant (Martin, Dupont…) ou un HoneyPot pour piéger les tentatives d'intrusion.*