FICHE DE RÉVISION — MAÎTRISE DU POSTE DE TRAVAIL

1. HISTORIQUE WINDOWS

Version	Date	Ligne	Points clés
MS-DOS	1981	Grand public	CLI 8 bits. Base de Windows jusqu'à 98.
Windows 95	1995	Grand public	Menu Démarrer, barre des tâches, PnP, 32 bits hybride. Révolution grand public.
Windows ME	2000	Grand public	Dernier OS basé sur DOS. Instable. Bureau = navigateur URL.
Windows NT 3.1	1993	Entreprise	1er noyau NT pur 32 bits, sans DOS. Fiable, stable, performant.
Windows NT 4.0	1996	Entreprise	Interface Win95. Pas d'USB ni PnP (technologies non stabilisées). Très fiable.
Windows 2000	2000	Entreprise	REVOLUTION : Active Directory. Stable, fiable. Fondation de tous les Windows modernes.
Windows XP	2001	Les deux	Noyau NT5. Schisme Famille / Pro (AD uniquement sur Pro). 32 bits pur.
Windows Vista	2007	Les deux	Lent et instable. Podium des mauvais OS.
Windows 10/11	2015/21	Les deux	64 bits. Win10 devait être le dernier. Win11 : verrouillage barre des tâches, TPM 2.0.
Server 2008	2008	Serveur	Hyper-V, Server Core, sécurité renforcée.
Server 2022/25	2022/25	Serveur	Azure hybrid, IA intégrée, sécurité avancée.

> *Depuis Windows 2000 Pro, aucune nouvelle fonctionnalité fondamentale n'a été ajoutée. Active Directory est la révolution clé de cette version.*
>
> *PnP (Plug and Play) = détection et installation automatique des périphériques dès branchement. Absent de NT 4.0 par choix de stabilité.*

2. STRUCTURE DE C:\WINDOWS

Dossier	Contenu	Remarque
System32	DLL 64 bits	Base du système. DLL manquante = panne fréquente.
SysWOW64	DLL 32 bits	Permet d'exécuter les applications 32 bits sur Windows 64 bits.
Program Files	Logiciels 64 bits	—
Program Files (x86)	Logiciels 32 bits	x86 = famille de puces Intel (8086, 8186, 8286…)
Users	Profils utilisateurs	Créé uniquement à la 1ère ouverture de session.

> *DLL = Dynamic Link Library : fragment de code réutilisable. Une panne est souvent causée par une DLL manquante dans System32. Résolution = remettre la DLL.*

Priorités processeur :

- Mode noyau : ticket priorité 5 (services système, drivers)
- Mode utilisateur : ticket priorité 15 (applications, logiciels)

3. COMPTES ET PROFILS UTILISATEURS

Compte utilisateur

Identifiant numérique stocké dans la SAM (Security Account Manager) ou BCUL (Base des Comptes Utilisateurs Locaux). Structure : Nom de compte + Mot de passe.

Deux rôles Windows : Administrateurs / Utilisateurs. L'appartenance à un groupe détermine le rôle.

Profil utilisateur

Dossier dans C:\Users\ contenant l'environnement de travail de l'utilisateur. N'est créé qu'à la 1ère ouverture de session avec ce compte.

Les dossiers de profils sont sécurisés : un utilisateur ne peut pas accéder au profil d'un autre (sauf admin).

UAC — User Account Control

Même en étant administrateur, les programmes ne se lancent pas en mode admin par défaut. L'UAC popup pour demander confirmation.

- Raccourci élévation de droits : Ctrl+Shift+Entrée
- Les boucliers (shield) sur les boutons = passage en mode administrateur requis

> *On ne travaille JAMAIS avec le compte Administrateur natif (désactivé par défaut). Toujours utiliser un compte admin personnel avec UAC actif.*

4 . GESTION DES DISQUES

MBR vs GPT

	MBR	GPT
Capacité max	2 To	Au-delà de 2 To
Partitions principales	4 maximum	Illimitées
BIOS requis	BIOS classique	UEFI obligatoire

> *Conversion MBR ↔ GPT : disque vide obligatoire, sans données. Les éviter lors de mises à niveau Windows (traîner les casseroles de l'ancien système).*

Types de partitions (MBR)

- Partition principale : bootable, maximum 4. Une seule peut être marquée active pour démarrer.
- Partition étendue : contient des lecteurs logiques non-bootables. Permet de dépasser la limite de 4 partitions.

Systèmes de fichiers

FS	Partition max	Fichier max	Fonctions clés
FAT	4 Go	2 Go	Compatibilité basique
FAT32	32 Go (Windows)	4 Go	Compatible large spectre d'appareils
NTFS	2 HexaOctets	Quasi illimité	Permissions, EFS (chiffrement par fichier), compression, journalisation
exFAT	Large	Large	Meilleure compatibilité multi-appareils (USB, SD)

Formatage

- Formatage rapide : efface la FAT (table d'allocation) + répertoire. Les données physiques restent sur les clusters et sont récupérables.
- Formatage complet : réécrit cluster par cluster. Définitif.
- Formatage bas niveau : outil constructeur, remise à zéro usine. Efface absolument tout.

> *On ne défragmente PLUS les SSD — cela use prématurément les transistors. Uniquement pertinent pour les disques mécaniques (HDD).*

Conversion FAT → NTFS (sans perte de données)

```
convert X: /fs:ntfs
```

> *L'inverse (NTFS → FAT32) est impossible sans formatage.*

Extension / Réduction de volume

- Extension via Gestionnaire de disques (GUI) ou diskpart (CMD admin).
- Réduction limitée par la fragmentation des fichiers dans les clusters.
- Extension de C: : doit passer par CMD en admin (diskpart).

5. RAID — VOLUMES DYNAMIQUES

Type	Disques min	Panne tolérée	Perte stockage	Principe
Volume fractionné	2	0	0%	Partition étalée sur plusieurs disques. Dépasse la limite d'1 disque. Perte totale si 1 disque tombe.
RAID 0 (bandes)	2	0	0%	Lecture/écriture parallèle = vitesse maximale. Pas de redondance. Usage éphémère.
RAID 1 (miroir)	2	1	50%	Duplication identique sur 2 disques. Résync possible après remplacement.
RAID 5 (bandes+parité)	3	1	1/n disques	RAID 0 + parité. A+B=P. Panne d'1 disque = recalcul par équation. Meilleur compromis.
RAID 6	4	2	2/n disques	RAID 5 + 2 parités. Tolère la perte simultanée de 2 disques.

> *RAID ≠ Sauvegarde. Le RAID ne protège pas contre la suppression accidentelle, les virus ou les sinistres.*

> *Mode dégradé RAID 5 (1 disque manquant) : 50% des performances. Pendant la resync/reconstruction : 25%. Risque total si 2e panne pendant cette phase.*

Ajout de disques en VM :

- VM éteinte → Contrôleur IDE
- VM en fonctionnement → Contrôleur SCSI (HotPlug)

6. SERVICES.MSC

Programmes lancés en tâche de fond, nécessaires au bon fonctionnement de Windows. Admin requis pour modification.

Type de démarrage	Comportement
Automatique	Démarre au boot Windows.
Automatique (différé)	Démarre après que Windows est complètement chargé.
Manuel	Démarre uniquement à la demande d'une application.
Désactivé	Ne démarre jamais.

- Si un service ne démarre pas : vérifier l'onglet Dépendances.
- RPC (Remote Procedure Call) = socle de fonctionnement Windows. Indispensable.

```
net start "Nom du service"
net stop "Nom du service"
```

7. REGISTRE WINDOWS (regedit)

Base de données centrale qui stocke tous les paramètres du système, des logiciels et du matériel. Ouverture : Win+R > regedit (admin requis).

> *Toujours suivre une procédure avant toute modification. Une erreur peut planter Windows.*

Ruches principales

Ruche	Périmètre
HKEY_LOCAL_MACHINE (HKLM)	Machine entière — matériel, logiciels installés. Cible principale des modifications système.
HKEY_CURRENT_USER (HKCU)	Utilisateur en session active.
HKEY_USERS\.DEFAULT	Profil par défaut appliqué avant toute session (ex: InitialKeyboardIndicators).

Types de valeurs

Type de valeur	Données	Usage typique
REG_SZ (chaîne)	Texte	DefaultUserName, chemins, noms de programmes
REG_BINARY (binaire)	0 / 1	Configuration matérielle bas niveau
REG_DWORD 32 bits	Nombre	AutoAdminLogon (0 ou 1), flags, codes
REG_QWORD 64 bits	Nombre large	Valeurs numériques 64 bits

Clés importantes à connaître

Clé	Usage
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Connexion automatique : AutoAdminLogon=1, DefaultUserName, DefaultPassword
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Lancement automatique au démarrage (toute la machine)
HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Lancement automatique au démarrage (utilisateur en cours uniquement)
HKEY_USERS\.DEFAULT\Control Panel\Keyboard	InitialKeyboardIndicators = 2 → Active le pavé numérique avant session

> *Ne JAMAIS double-cliquer sur un fichier .reg → applique immédiatement les modifications. Toujours ouvrir avec 'Modifier' pour inspecter d'abord.*

> *Les fichiers .reg sont bloqués par la plupart des clients mail (fichiers dangereux).*

8. GPEDIT.MSC — STRATÉGIES DE GROUPE LOCALES

Éditeur de stratégie de groupe. Permet de forcer des comportements, bloquer des menus, activer des options ou limiter des utilisateurs. Modifications en temps réel.

Nœud	Équivalent registre
Configuration ordinateur	= HKEY_LOCAL_MACHINE → s'applique à toute la machine
Configuration utilisateur	= HKEY_CURRENT_USER → s'applique à tous les utilisateurs
Non configuré	Remet l'état d'avant (contrairement à regedit qui garde la valeur)
Désactivé	Force la valeur inverse sans devoir connaître la clé regedit correspondante

> *MMC (Microsoft Management Console) : mmc via Win+R. Permet d'ajouter des snap-ins pour cibler un utilisateur spécifique (contourner gpedit qui s'applique à tous).*

9. INVITE DE COMMANDES — RÉFÉRENCE

Commande	Syntaxe exemple	Description
cd	cd C:\Windows	Changer de répertoire. cd.. = parent, cd \ = racine.
dir	dir /s / dir /a	/s = récursif dans sous-dossiers, /a = affiche fichiers cachés/système.
md	md "Mon Dossier"	Créer un dossier. Guillemets si nom avec espaces.
rd	rd /s C:\Dossier	Supprimer un dossier. /s = supprime même si non vide.
del	del *.* / del f.txt	Supprimer fichier(s). *.* = tous les fichiers du dossier.
copy	copy src.txt dst.txt	Copier un fichier.
ren	ren ancien.txt nvx.txt	Renommer un fichier ou dossier.
type	type fichier.txt	Afficher le contenu d'un fichier texte dans la console.
echo X > f	echo PSG > foot.txt	> redirige le texte vers un fichier (le crée si inexistant).
ipconfig /displaydns	—	Affiche le cache DNS local (historique ~1h). Utile pour détecter les backdoors.

ipconfig /flushdns	—	Vide le cache DNS (résolution de noms uniquement, pas le cache navigateur).
nslookup	nslookup	Teste la résolution de nom via le DNS configuré. Ne fonctionne pas sans DNS.
net start/stop	net start "Spooler"	Démarrer ou arrêter un service depuis la ligne de commande.
convert	convert X: /fs:ntfs	Convertir FAT/FAT32 → NTFS sans perte de données. L'inverse est impossible.
powercfg -h off	powercfg -h off	Désactiver la veille prolongée et supprimer hiberfil.sys.

Variables d'environnement

Raccourcis que Windows garde en mémoire pour les programmes. Syntaxe : %NOM_VARIABLE%

```
echo %username%       → Nom de l'utilisateur en session
echo %systemroot%     → Chemin du dossier Windows (C:\Windows)
echo %path%           → Liste des chemins de recherche des exécutables
```

10. OUTILS D'ADMINISTRATION — RÉCAPITULATIF

Outil	Accès	Usage
services.msc	Win+R	Gérer les services (démarrage, arrêt, récupération sur panne, dépendances).
regedit	Win+R (admin)	Modifier la base de registre Windows. PROCÉDURE OBLIGATOIRE avant toute modif.
gpedit.msc	Win+R	Stratégies de groupe locales. Config ordinateur = HKLM, Config utilisateur = HKCU.
mmc	Win+R	Console d'administration modulaire. Ajouter des snap-ins (stratégies, utilisateurs…).
sysdm.cpl	Win+R	Propriétés système, variables d'environnement, protection système.
msconfig	Win+R	Configuration démarrage (mode sans échec, services, programmes au démarrage).
taskmgr	Ctrl+Maj+Échap	Processus, performances CPU/RAM/disque/réseau, applications au démarrage.
sdclt.exe	Win+R	Sauvegarde et restauration. Création d'image système complète.
rstrui.exe	Win+R	Restauration système via points de restauration. Ne touche pas aux fichiers utilisateur.
Observateur d'événements	eventvwr.msc	Journaux : Application (erreurs logiciels), Système (noyau/pilotes), Sécurité (connexions/audits).

Fichiers système cachés

- pagefile.sys : mémoire virtuelle (pagination RAM). Suppression = limité à la RAM physique réelle.
- hiberfil.sys : sauvegarde RAM pour veille prolongée. Désactivation : powercfg -h off

11. RÉCUPÉRATION SYSTÈME ET SÉCURITÉ

Points de restauration

- Créés via sysdm.cpl → Protection système.
- Stockés dans System Volume Information (dossier caché à la racine de C:).
- Ne touche PAS aux fichiers utilisateur. Remet uniquement : fichiers système, registre, programmes.
- Créés automatiquement : installation de logiciels majeurs, mises à jour Windows, hebdomadairement.
- Suppression : désactiver puis réactiver la protection système (via sysdm.cpl).

Image système complète

- Copie de Windows + applications + fichiers. Via sdclt.exe.
- Restauration : boot USB Windows → Réparer → Image système.
- Meilleure option en cas de crash total.

Options de démarrage avancées

Accès : Menu Démarrer → Alimentation → maintenir Maj + cliquer Redémarrer

N°	Option	Description
3	Vidéo basse résolution	Démarre avec résolution minimale pour résoudre les problèmes de pilotes graphiques.
4	Mode sans échec	Pilotes et services essentiels uniquement. Diagnostic pannes, virus, conflits.
5	Sans échec + réseau	Idem mode sans échec + carte réseau active (accès internet possible).
6	Sans échec + CMD	Mode sans échec sans interface graphique. Tout en ligne de commande.
7	Désactiver signatures pilotes	Autorise pilotes non signés Microsoft (1 session uniquement).
8	**JAMAIS UTILISER**	Désactive Windows Defender. Ne jamais sélectionner.
9	Désactiver redémarrage auto	Empêche le redémarrage automatique après un BSOD. Permet de lire l'erreur.

Réinitialisation de mot de passe (boot USB)