

COMPLÉMENT — SAUVEGARDE & VEEAM

11. Règle 3-2-1 et concepts clés Veeam

Règle 3-2-1 : 3 copies des données, sur 2 supports différents, dont 1 hors site (cloud ou site distant).

Concept	Définition
Backup Job	Tâche planifiée qui sauvegarde une ou plusieurs VM à intervalles définis.
Restore Point	Point de restauration créé à chaque exécution du job.
Repository	Emplacement de stockage où Veeam dépose les sauvegardes.
Retention Policy	Nombre de points de restauration conservés avant écrasement.

En environnement pro : sauvegarder, c'est le **quotidien** ; restaurer, c'est l'**exceptionnel**.

12. Le bit d'archive — mécanisme incrémentielle vs différentielle

L'incrémentielle et la différentielle lisent toutes les deux le **bit d'archive** (métadonnée NTFS marquant un fichier comme modifié). La différence est ce qu'elles en font après :

Incrémentielle : remet le bit à zéro après sauvegarde → fichier marqué "sauvegardé", ne sera repris que s'il est modifié à nouveau.

Différentielle : laisse le bit intact → revoit les mêmes fichiers à chaque passage depuis la dernière complète, d'où sa croissance.

Complète : remet le bit à zéro. **Copie** : ne touche pas au bit → ne perturbe pas la chaîne en cours.

Restauration — ce qu'il faut pour reconstruire : incrémentiel = la complète + **toutes les incrémentales dans l'ordre** (une seule manquante = chaîne bloquée) ; différentiel = la complète + **la dernière différentielle**, c'est tout.

13. Cibles de sauvegarde et précisions sur les repository

Support	Caractéristiques
Disque local / NAS / SAN	Disque interne, externe ou partage réseau.
Clé USB / disque amovible	Portable mais déconseillé en production.
Bande magnétique (cassette)	Archivage long terme, économique pour gros volumes (durée de vie 5 ans), mais écriture lente.
Cloud	Azure, AWS ou tout dépôt compatible S3 — copie hors site.

Précisions sur les 4 types de repository

- **DAS** : stockage branché directement sur le serveur Veeam. Pas de réseau entre Veeam et le stockage → **le plus rapide, choix labo**.
- **NAS** : partage SMB (`\\serveur\partage`) — plus lent qu'un DAS mais centralise les sauvegardes. **Recommandé en prod multi-hôtes**.
- **Deduplicating appliance** : matériel spécialisé (Dell EMC Data Domain, HPE StoreOnce, Quantum DXi...), déduplication/compression native, intégration via API. Coûteux, réservé à la grosse prod.
- **Object Storage (S3)** : AWS S3, Azure Blob ou on-prem (MinIO). Copie hors site/archivage dans une stratégie 3-2-1. **Pas fait pour restaurer vite**.

14. Les types de restauration Veeam — vue complète

Besoin	Option
VM up le plus vite possible (RTO minimal)	Instant Recovery
Restauration complète propre	Entire VM Restore
Récupérer un fichier constitutif de la VM (.vsv état sauvegardé, .bin mémoire, .xml configuration)	VM Files Restore
Extraire un disque virtuel (VHDX, VHD, VMDK) pour le rattacher à une autre VM ou l'analyser	Export Disk
Lire des données sans tout restaurer	Publish Disk
Migrer vers AWS / GCP / Azure	Restore to Public Cloud

Instant Recovery — finalisation et options

La VM démarre **directement depuis le repo de backup** : fonctionnel mais pas viable en prod (performances dégradées, repo mobilisé). **Migrate to production** déclenche une **Storage Live Migration à chaud** — données transférées en arrière-plan sans interruption. À 100 %, la VM est détachée du repo.

Option	Rôle
Migrate to production	Finalise l'IR — transfère les données vers le stockage de prod.
Retry	Relance si la migration a échoué.
Open VM console	Ouvre la console Hyper-V de la VM en cours de restauration.
Stop publishing	Arrête l'Instant Recovery sans migrer — la VM s'éteint.
Properties	Détails du job d'IR.

15. Checkpoint Hyper-V — le mécanisme .vhdx / .avhdx

À la prise du point de contrôle, Hyper-V **gèle l'écriture** sur le disque parent et crée un fichier différentiel :

```
SRVPA01.vhdx      ← disque parent (lecture seule dès la prise du checkpoint)
SRVPA01_snapshot.avhdx ← fichier différentiel (toutes les écritures vont là)
```

- Le **.avhdx** ne stocke que les **blocs modifiés après** le checkpoint — pas une copie complète.
- Plus le checkpoint vieillit, plus le **.avhdx** grossit. À la suppression, Hyper-V **fusionne (merge)** le différentiel dans le parent — opération longue qui sollicite le stockage.

Checkpoint ≠ sauvegarde. *Filet de sécurité court terme, pas un substitut à Veeam.*

16. Crash-consistent vs application-consistent + journaux AD

Sans application-aware processing : *snapshot crash-consistent = débrancher physiquement le serveur. NTDS.dit capturée dans un état potentiellement incohérent. Le backup d'un DC est alors techniquement inutilisable en conditions réelles. Veeam sauvegarde des octets, pas un Active Directory.*

Write-Ahead Logging (WAL) — pourquoi des journaux ?

Principe : toute modification est écrite **d'abord dans le log, ensuite dans la base**. Écriture directe dans NTDS.dit = accès aléatoire = goulot d'étranglement. Le log est en **écriture séquentielle** (on ajoute à la fin) — l'opération disque la plus rapide. AD confirme l'opération dès qu'elle est dans le log ; le commit dans la base se fait en arrière-plan.

Résilience : crash entre le log et le commit → AD relit les logs non commités au redémarrage, rejoue les opérations manquantes dans NTDS.dit. Le log, c'est la «to-do list» de la base.

Flux d'écriture : 1) écriture dans `EDB.log` → 2) commit dans `NTDS.dit` → 3) log archivé/tronqué (flush VSS ou sauvegarde propre).

Fichiers de C:\Windows\NTDS\

Fichier	Rôle	Note
NTDS.dit	Base AD principale	Toujours ouverte en écriture
EDB.log	Log de transaction actif (10 Mo fixe)	Reçoit toutes les écritures en premier
EDBtmp.log	Log en cours de création	Renommé en EDB.log quand celui-ci est plein
EDB00001.log...	Logs archivés (séquence hexadécimale)	Conservés jusqu'au flush VSS / sauvegarde
RES1.log / RES2.log	Fichiers réservés	Espace disque de secours garanti

17. Clichés instantanés — précisions importantes

Raison fondamentale du «≠ sauvegarde» : les clichés s'enregistrent sur le volume qu'ils protègent. Clichés activés sur D: → snapshots stockés sur D:. On perd D:, on perd tout, y compris les snapshots.

- C'est une fonctionnalité **Windows (service VSS)**, pas une fonctionnalité Hyper-V : fonctionne sur n'importe quel serveur Windows, virtualisé ou non.
- **Intérêt principal en prod : le self-service utilisateur.** L'utilisateur qui a écrasé/supprimé son fichier ouvre lui-même «Versions précédentes», choisit la version et clique Restaurer — **sans intervention admin.**
- Configurable : taille allouée aux clichés sur le volume + planification des prises.

18. Commandes à connaître

MAC Spoofing en PowerShell (à chaud, sans redémarrage, depuis le parent) :

```
Set-VMNetworkAdapter -VMName "SRVPA05" -MacAddressSpoofing On
```

Monter un partage administratif sur une lettre de lecteur :

```
net use Z: \\NomDuServeur\C$
```

Exposer les extensions de virtualisation (VM éteinte, sur l'hyperviseur parent) :

```
Set-VMProcessor -VMName "SRVPA04" -ExposeVirtualizationExtensions $true
```