

WordPress : prouver sa restauration

Laboratoire sur serveur · Chemins et identifiants distincts de la production

Définir

- RPO : durée de données perdues acceptable. RTO : durée visée de retour du service.
- Prépare des témoins : article, média, PDF, rubrique et compte test.
- Chronomètre depuis la recherche de l'archive jusqu'aux vérifications finales.

Sauvegarder

- Lot = base + fichiers + versions + informations d'exploitation.
- Répertoire privé hors HTTP ; chiffrement et clé récupérable séparément.
- Assure la cohérence base/fichiers ; transaction SQL seule ≠ snapshot global.
- Copies séparées, générations protégées et empreintes de référence fiables.

Isoler avant démarrage

- VM serveur dédiée sans route vers Internet ni production, y compris IPv6.
- Pas de volume prod, compte DB prod, clé SSH prod ni socket Docker.
- Teste le filtrage avec des cibles témoins autorisées ; vérifie ses journaux.

Neutraliser la copie

- Configuration et secrets de laboratoire ; tâches serveur et cron vérifiés.
- MU-plugin : bloque wp_mail et l'API HTTP WordPress.
- Ces filtres ne bloquent pas SMTP/cURL directs : garde l'isolation réseau.
- Client navigateur isolé, pour éviter les requêtes vers des médias externes.

Restaurer

- Vérifie empreintes, chemins et liens avant extraction dans une arborescence neuve.
- Avant db import : contrôle DB_HOST, DB_NAME et chemin /srv/lab/wp.
- search-replace : dry-run, périmètre de tables défini, données sérialisées préservées.
- Applique uniquement au labo après lecture du rapport ; pas de DNS public modifié.

Prouver et améliorer

- Contenus, médias, liens, connexion et fonctions utiles vérifiés.
- Aucun mail réel ni appel externe ; collecteur de test uniquement interne.
- Mesure perte constatée et temps total, compare aux RPO/RTO.
- Corrige puis refais le test ; l'existence d'une archive ne prouve pas la récupération.

Article complet, exercices et sources : blog.gringao.fr/cyber-sauvegarde-restauration-wordpress-isolee/