Configuration du chiffrement côté serveur

Le chiffrement côté serveur sur Nextcloud repose sur un module intégré qui chiffre automatiquement tous les fichiers déposés sur le serveur dès qu'il est activé par l'administrateur. Ce chiffrement s'applique à l'ensemble du serveur, sans possibilité de sélectionner individuellement les fichiers à chiffrer.

Fonctionnement Lorsqu'il est activé, le module utilise les identifiants de chaque utilisateur comme clé privée de chiffrement. Après activation, il suffit de se déconnecter puis de se reconnecter pour générer les clés de chiffrement et chiffrer les fichiers existants

Transparence L'utilisation reste transparente pour l'utilisateur final : aucune manipulation particulière n'est requise pour gérer ou partager ses fichiers

Protection Ce système protège les fichiers contre l'accès non autorisé en cas de vol ou de réparation des disques, ou encore contre les regards indiscrets d'un administrateur système (qui ne pourra voir que les noms de fichiers)

Limites Seules les données des fichiers sont chiffrées : les noms de fichiers, l'arborescence des dossiers, les vignettes, les prévisualisations et certains fichiers système ne le sont pas

Récupération Il existe une option de clé de récupération, à activer pour éviter la perte d'accès aux fichiers en cas d'oubli du mot de passe

Consommation de ressources Le chiffrement augmente la consommation de ressources (CPU, mémoire, espace disque) et peut impacter les performances, notamment sur des machines peu puissantes