BY+ — Intégration avec le serveur Samba existant

Oct 7, 2026 · @Rachid

Objet et contexte

BY+ ne remplace pas le partage Samba du client : il s'y branche. Samba reste le lieu de stockage des fichiers ; BY+ devient le registre des dossiers, des droits et de l'activité métier.

Ce document complète la proposition technique « Déploiement sur site ». Il précise comment BY+ s'intègre à l'existant.

Ce que le client a déjà :

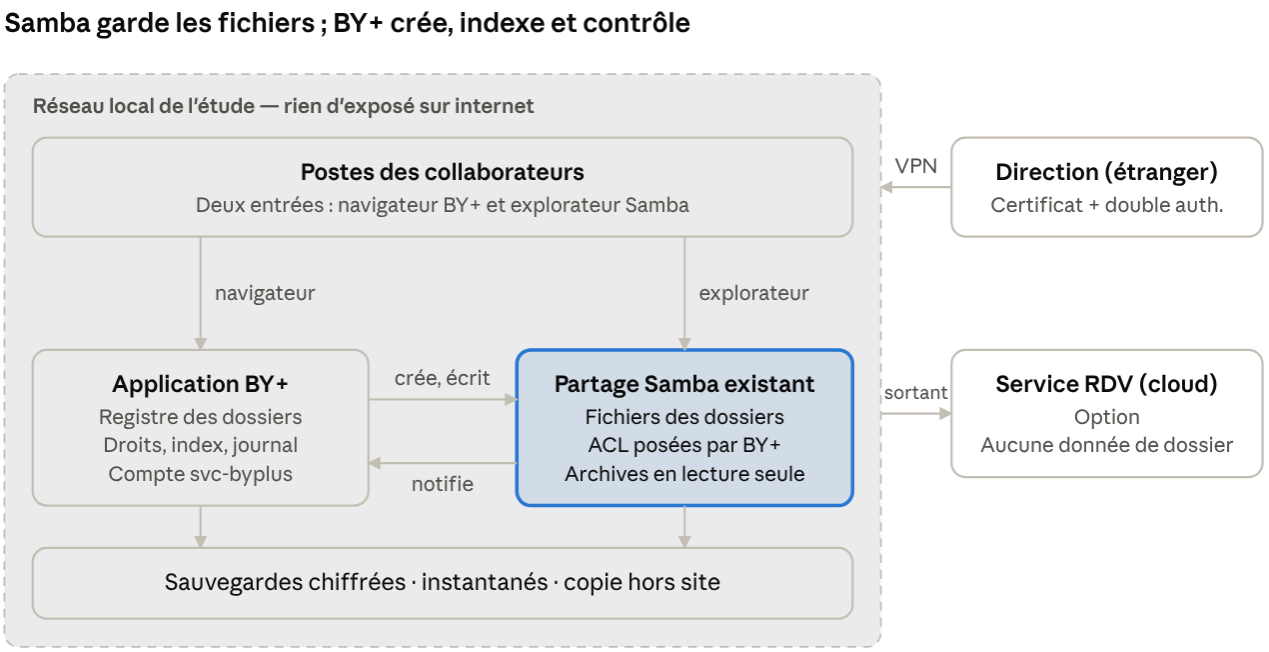
- un serveur local avec un partage Samba, exploré depuis l'explorateur de fichiers des postes ;
- une arborescence de dossiers déjà organisée ;
- une IP publique utilisée pour l'accès externe.

Ce que BY+ apporte :

- l'inscription d'un dossier dans l'application, qui crée automatiquement son dossier physique sous Samba ;
- deux entrées sur les mêmes fichiers : l'application BY+ et l'explorateur Samba, synchronisées ;
- des droits d'accès définis une fois dans BY+ et appliqués sur Samba ;
- l'accès distant sécurisé de la direction et, en option, la prise de rendez-vous en ligne.

Principe directeur : un fichier n'existe qu'une fois, sur Samba. BY+ ne stocke pas de copie ; il indexe, référence et contrôle.

Architecture cible



Architecture cible · BY+ branché sur le Samba existant

Les postes gardent leurs deux entrées sur les mêmes fichiers. BY+ crée et écrit sur Samba ; Samba lui notifie chaque changement fait dans l'explorateur. Le seul flux entrant depuis internet est le VPN de la direction ; le rendez-vous en ligne ne fonctionne qu'en sortant.

Principe de la double entrée

Toute création de dossier passe par BY+ ; ensuite, les fichiers se manipulent indifféremment depuis l'application ou depuis l'explorateur Samba.

Création d'un dossier (entrée unique : BY+)

1. L'utilisateur inscrit le dossier dans BY+ (client, nature, référence).
2. BY+ attribue un identifiant unique et calcule le chemin selon la convention de nommage du client, par exemple `\\SERVEUR\Dossiers\<Année>\<Référence> - <Client>`.
3. BY+ crée le dossier physique sur Samba, avec ses sous-dossiers types (ex. Actes, Pièces, Correspondance — à valider avec le client).
4. BY+ dépose un marqueur d'identité dans le dossier (attribut étendu ou fichier caché `.byplus`), qui lie le dossier physique à sa fiche, même après renommage.
5. BY+ pose les droits (ACL) correspondant aux personnes habilitées sur ce dossier.
6. Le dossier apparaît aussitôt dans l'explorateur des postes autorisés, et seulement d'eux.

Règle : la création d'un dossier racine directement dans l'explorateur est bloquée par les droits. Les utilisateurs créent librement des fichiers et sous-dossiers *à l'intérieur* d'un dossier.

Exploitation des fichiers (deux entrées)

Action	Depuis BY+	Depuis l'explorateur Samba
Ajouter un fichier	Téléversé et écrit directement dans le dossier Samba	Copié dans le dossier ; BY+ le détecte et l'indexe en quelques secondes
Modifier un fichier	Ouvert puis réenregistré sur Samba	Ouvert et enregistré normalement ; BY+ enregistre la nouvelle version
Renommer / déplacer un fichier	Mis à jour sur Samba	Détecté ; la référence dans BY+ suit
Supprimer un fichier	Placé en corbeille Samba, tracé	Placé en corbeille Samba ; BY+ trace l'événement
Renommer / supprimer le dossier racine	Réservé aux profils habilités	Bloqué par les droits
Clôturer / archiver	Le dossier passe dans le partage Archives, en lecture seule	Visible en lecture seule

Mécanisme de synchronisation

- **BY+ → Samba :** écriture directe sur le partage via un compte de service dédié (`svc-byplus`), sans copie intermédiaire.
- **Samba → BY+ :** surveillance des changements du système de fichiers (notifications noyau `inotify`) + un rapprochement complet planifié chaque nuit, pour rattraper tout événement manqué.
- **Accès simultanés :** les verrous Samba restent actifs ; un fichier ouvert par un collaborateur n'est pas écrasé par BY+. L'édition simultanée à plusieurs reste l'option « édition collaborative ».

Droits d'accès

Les droits se définissent dans BY+ et BY+ les applique sur Samba : une seule source de vérité, aucun réglage manuel des ACL.

Comptes : chaque collaborateur garde un compte Samba nominatif (local ou annuaire, selon l'existant). BY+ s'appuie sur ces mêmes comptes pour que l'identité soit la même dans l'application et dans l'explorateur.

Correspondance proposée :

Profil BY+	Droits sur les dossiers actifs	Droits sur Archives
Direction	Lecture / écriture sur tous les dossiers	Lecture
Collaborateur affecté au dossier	Lecture / écriture sur ce dossier, sans suppression du dossier racine	Lecture sur ses dossiers
Collaborateur non affecté	Aucun accès, dossier invisible	Aucun accès
Secrétariat / accueil	À définir avec le client	À définir
Compte de service `svc-byplus`	Contrôle total (création, ACL)	Contrôle total

Mise en œuvre côté Samba :

- un groupe par dossier (ou par équipe si le client travaille par pôles), alimenté par BY+ selon les affectations ;
- ACL étendues sur le système de fichiers (`vfs_acl_xattr`), lisibles depuis l'onglet Sécurité de Windows ;
- `access based share enumeration` activé : un utilisateur ne voit pas les dossiers auxquels il n'a pas droit ;
- contrôle automatique quotidien : BY+ compare les ACL réelles aux droits attendus et corrige tout écart, avec journal.

Reprise de l'existant

Les dossiers déjà présents sous Samba sont rattachés à BY+ sans être déplacés ni renommés de force : l'organisation actuelle du client est conservée.

1. **Inventaire :** analyse en lecture seule de l'arborescence (nombre de dossiers, volume, profondeur, nommage, droits actuels).
2. **Règles de correspondance :** déduites de la convention de nommage existante (année, référence, nom du client), validées avec le client.
3. **Rattachement automatique :** chaque dossier reconnu reçoit une fiche BY+ et son marqueur d'identité ; ses fichiers sont indexés.
4. **Rapport d'écarts :** les dossiers non reconnus, en doublon ou hors convention sont listés ; le client décide pour chacun (rattacher, archiver, laisser hors BY+).

5. **Alignement des droits :** les ACL actuelles sont comparées aux affectations BY+ ; les écarts sont validés avant d'être corrigés.

Cette étape remplace la « remédiation du stockage » de la proposition. Comme l'arborescence est déjà organisée, elle porte surtout sur la correspondance et les droits, pas sur un rangement complet.

Bascule : un gel court des créations de dossiers racine dans l'explorateur, le temps du rattachement. Les collaborateurs continuent de travailler sur leurs fichiers pendant toute l'opération.

Accès externe via l'IP publique

L'IP publique du client sert à un seul accès entrant : le tunnel chiffré de la direction. Samba et BY+ ne sont jamais exposés directement sur internet.

Flux	Sens	Exposé sur l'IP publique ?	Protection
Partage Samba (SMB, port 445)	—	**Jamais**	Réseau local uniquement
Interface web BY+	—	**Jamais**	Réseau local + tunnel direction
Accès direction	Entrant	Oui, un seul port (VPN, ex. WireGuard)	Certificat sur l'appareil + double authentification ; révocable instantanément
Rendez-vous en ligne (option)	Sortant	Non	BY+ interroge le service cloud ; aucun port ouvert
Sauvegardes hors site	Sortant	Non	Données chiffrées avant envoi
Maintenance NetByUs	Entrant via le même VPN	Pas de port supplémentaire	Compte nominatif, accès ponctuel, journalisé

À vérifier dans l'existant : quels ports sont déjà ouverts sur cette IP et pour quoi (bureau à distance, accès fichiers, autre application). Tout port exposant SMB ou un bureau à distance doit être fermé ou basculé derrière le VPN.

Une fois connectée au tunnel, la direction accède à BY+ comme au bureau. *À valider avec le client : la direction accède-t-elle aussi au lecteur Samba à distance, ou seulement à l'application ?*

Sauvegardes, chiffrement, journalisation

Les fichiers Samba et la base BY+ se sauvegardent ensemble, pour qu'une restauration ne crée jamais d'écart entre la fiche et le fichier.

- **Sauvegardes :** quotidiennes, hebdomadaires, mensuelles, chiffrées, avec une copie hors site. La sauvegarde existante du client est inventoriée à l'audit : elle est conservée, complétée ou remplacée.
- **Versions précédentes :** instantanés du système de fichiers exposés via Samba (`shadow_copy2`) ; un collaborateur restaure lui-même une version d'hier depuis l'onglet « Versions précédentes » de Windows.
- **Corbeille :** les suppressions passent par une corbeille Samba (`vfs_recycle`) avant purge.
- **Chiffrement au repos :** les données existantes ne sont probablement pas chiffrées aujourd'hui. Le chiffrement du volume suppose une migration vers un volume chiffré, planifiée à l'audit.
- **Journalisation :** BY+ trace qui a créé, ouvert, modifié ou supprimé quoi, quelle que soit l'entrée utilisée ; le module d'audit Samba (`vfs_full_audit`) complète ce journal côté explorateur.

Impacts sur la proposition et le planning

L'existence d'un Samba organisé ne change pas le service rendu, mais elle change où vivent les fichiers selon la variante.

Point	Variante A — serveur existant	Variante B — serveur dédié
Où tourne BY+	Machine virtuelle ou conteneur dédié sur le serveur Samba	Nouveau serveur dédié
Où restent les fichiers	Sur le Samba existant, accès local	Deux choix : (1) restent sur le Samba existant, BY+ y accède par le réseau ; (2) migrent sur le nouveau serveur, qui devient le serveur Samba
Qui administre Samba	Prestataire actuel + NetByUs (prérequis 3.1)	Choix (1) : partagé ; choix (2) : NetByUs seul
Garanties de la proposition	Limitées (cf. 3.1)	Pleines uniquement avec le choix (2)

Conséquence pour la recommandation : la variante B n'apporte ses garanties complètes que si le partage Samba migre sur le serveur dédié. Si les fichiers restent sur l'ancien serveur, on retombe sur une administration partagée.

Étapes du planning à renommer :

Étape de la proposition	Devient
3. Remédiation & fiabilisation du stockage	3. Reprise de l'existant : inventaire, rattachement, alignement des droits
4. Mise en place de l'accès réseau aux dossiers	4. Connexion BY+ ↔ Samba : compte de service, création automatique, synchronisation

Les durées de la proposition (2 semaines chacune) restent des plafonds ; elles seront confirmées après l'inventaire de l'audit. En variante B avec migration, prévoir la copie des données et une bascule hors heures ouvrées.

Prérequis et informations à collecter

Ces points complètent le questionnaire de l'annexe A ; ils sont à obtenir avant ou pendant l'audit.

Serveur et Samba

- [ ] Système d'exploitation et version de Samba
- [ ] Mode Samba : autonome, membre d'un domaine, ou contrôleur de domaine (Active Directory)
- [ ] Système de fichiers (ext4, XFS, ZFS, Btrfs) et support des attributs étendus / ACL
- [ ] Capacité disque, espace libre, processeur, mémoire, charge actuelle
- [ ] Virtualisation disponible (oui / non, laquelle)

Arborescence et droits

- [ ] Volume total, nombre de dossiers et de fichiers
- [ ] Convention de nommage actuelle, avec quelques exemples réels
- [ ] Sous-dossiers types utilisés dans chaque dossier
- [ ] Gestion actuelle des droits (par personne, par groupe, aucun)
- [ ] Liste des utilisateurs et de leurs rôles

Réseau et accès externe

- [ ] Pare-feu / routeur en place et qui l'administre
- [ ] Ports actuellement ouverts sur l'IP publique, et leur usage

- [ ] IP publique fixe ou dynamique

Exploitation

- [ ] Solution de sauvegarde actuelle et emplacement des copies
- [ ] Prestataire(s) intervenant aujourd'hui sur le serveur, et leurs accès
- [ ] Choix de la variante, et en variante B : fichiers conservés sur l'ancien serveur ou migrés

Risques et parades

Risque	Conséquence	Parade
Un utilisateur renomme ou déplace un dossier dans l'explorateur	Lien perdu entre fiche BY+ et dossier	Marqueur d'identité dans chaque dossier + droits bloquant le renommage du dossier racine
Dossier racine créé à la main sous Samba	Dossier hors BY+, sans droits contrôlés	Création racine interdite par ACL ; rapprochement nocturne qui signale tout dossier inconnu
Événements de fichiers manqués (gros volume, redémarrage)	Index BY+ en retard	Rapprochement complet chaque nuit + limites `inotify` dimensionnées à l'audit
Droits modifiés à la main par un tiers	Accès non autorisé à un dossier	Contrôle quotidien des ACL et correction automatique, journalisée
Fichier ouvert pendant une écriture BY+	Conflit de version	Respect des verrous Samba ; version conservée dans les instantanés
Mise à jour Samba ou système par un autre prestataire	Synchronisation interrompue	Prérequis 3.1 : préavis 72 h, instantané avant intervention
SMB ou bureau à distance exposé sur l'IP publique	Intrusion, rançongiciel	Fermeture des ports, accès externe uniquement par le VPN direction
Sauvegarde fichiers et base désynchronisées	Fiches sans fichiers ou l'inverse	Sauvegarde coordonnée base + partage, test de restauration à la recette