Mise en place d’un serveur de fichiers SMB sécurisé avec permissions NTFS et SMB

Années : 2025-2026

BTS SIO

Situation professionnelle numéro 4
Mise en place d’un serveur de fichiers SMB sécurisé avec permissions NTFS et SMB

Description :

Le serveur de fichiers est un composant essentiel des systèmes d’information. Il répond à des besoins de centralisation, de partage sécurisé et de gestion des accès aux données. Dans le cadre de mon homelab sous Proxmox VE 9, j’ai déployé un serveur de fichiers intégré à Active Directory afin de maîtriser les protocoles SMB, les permissions NTFS et SMB, et de reproduire une infrastructure professionnelle Windows.

Mots-clés :

Serveur de fichiers: Une machine qui stocke des dossiers et fichiers pour que plusieurs personnes du réseau puissent y accéder.
SMB: Un protocole Windows qui permet de partager des dossiers et accéder à des fichiers à distance sur un réseau.
Permissions NTFS: Les droits appliqués directement sur les fichiers/dossiers du disque (qui peut lire, modifier, supprimer…).
Permissions SMB: Les droits appliqués au partage réseau (qui peut accéder au dossier partagé depuis le réseau).
ABE(Access-Based Enumeration): Une fonction qui fait que les utilisateurs ne voient que les dossiers auxquels ils ont accès. Les autres restent invisibles.
Gestion des droits: Le fait d’attribuer ou retirer des permissions aux utilisateurs pour contrôler ce qu’ils peuvent faire sur le réseau ou les fichiers.

Plan de la situation

Le cahier des charges

L’expression des besoins

La société recherche un serveur de fichiers performant et stable. Elle souhaite centraliser les données partagées, gérer les accès en fonction des groupes Active Directory, et assurer la sécurité des flux. Un de nos besoins est de déployer un partage SMB avec des permissions NTFS et SMB complémentaires pour limiter les accès aux utilisateurs autorisés.

La description de l’existant

Le serveur existant utilise l’hyperviseur Proxmox VE 9.0.

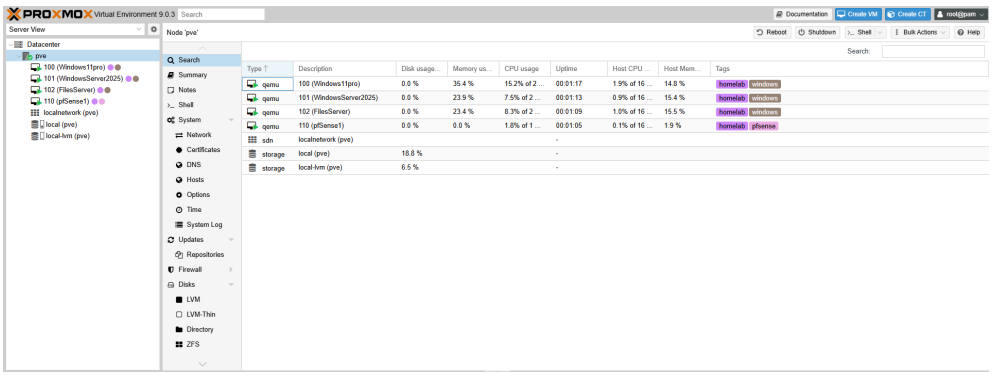
Le domaine Active Directory est opérationnel avec des utilisateurs et groupes.

La configuration du réseau est exprimée ci-dessous :

Réseau interne	**192.168.10.0/24**
Gateway	pfSense 192.168.10.254
DNS	DC 192.168.10.101
DHCP	Délivré par le serveur AD

Le homelab est capable de réaliser des partages, l’authentification AD est présente.

Voici une vue de notre infrastructure (Proxmox avec VMs AD et pfSense)



Les offres du marché :

Actuellement, énormément de solutions de serveurs de fichiers sont disponibles sur le marché et elles répondent à de nombreux problèmes posés dans le passé, pourtant elles ne sont pas toutes égales.

Voici un tableau comparatif des offres du marché existant en novembre 2025 :

	Windows File Server 2025	**Samba 4.3**	**Nextcloud 28**	**TrueNAS Scale 24**
Intégration AD	Native	Bonne	Via LDAP	Bonne
Permissions NTFS	Oui	Limitée	Non	ZFS ACL
Permissions SMB	Oui	Oui	Non (Web)	Oui
ABE	Oui	Oui	Non	Non
Quotas	Oui (FSRM)	Oui	Oui	Oui
Chiffrement	Oui	Oui	Oui	Oui
Interface	Explorer	CLI/Web	Web	Web
Licence	Évaluation 180 jours	Gratuit	Gratuit	Gratuit

L’analyse des choix

Windows File Server 2025 : Avec cette nouvelle version, Microsoft a amélioré son produit et propose un serveur de fichiers natif performant et complet. Il reste lié à l’écosystème Windows, ce qui est idéal pour notre domaine AD.

Samba 4.3 : Il ne domine plus ses concurrents directs comme c’était le cas auparavant. Même si les limites de la version gratuite ne devraient pas être gênantes pour un usage personnel.

Nextcloud 28 : Handicapé par une interface web uniquement, sans permissions NTFS natives.

TrueNAS Scale 24 : Procédure de configuration ZFS complexe et donc un système réservé à l’expert.

Le choix : Windows Server 2025 + rôle Serveur de fichiers

Nous avons opté pour Windows Server 2025 qui est une solution éprouvée car c’est un des standards en entreprise Windows. On utilise le protocole SMB pour les partages car il est natif à Windows, intégré à AD pour l’authentification, et permet une gestion fine des accès. Les permissions NTFS gèrent les droits au niveau fichier/dossier (lecture, écriture, exécution) tandis que les permissions SMB contrôlent l’accès au partage lui-même (contrôle total, lecture/écriture, lecture seule). Les deux sont complémentaires : les plus restrictives prévalent toujours, assurant une sécurité multicouche. Dans un environnement Windows, cela évite les failles et simplifie l’administration via AD.

Dans une autre mesure nous avons conscience que quelque soit la solution utilisée, elle n’est pas exemptée de problèmes de sécurité, et qu’elle amène un lot de nouveaux risques.

Les nouveaux risques du serveur de fichiers

- Compromission des données si permissions mal configurées
- Surcharge du stockage sans quotas
- Attaques ransomware via SMB si ports exposés
- Point unique de panne sur la VM

Complexification de la gestion des droits et des audits
Supervision des accès difficile sans outils avancés
Prolifération des données sensibles si pas de screening
Investigation post-incident plus difficile

Pour conclure, il nous faudra du temps pour maîtriser le fonctionnement global de notre serveur de fichiers.

Préparation de la mise en place du serveur de fichiers :

Le déploiement d'un serveur de fichiers est une étape critique. On doit créer une VM dédiée, joindre au domaine, puis configurer les partages et droits.

Étape 1 : Création de la VM FilesServer

Étape 2 : Rôles et fonctionnalités

Étape 3 : Création du partage SMB

Étape 4 : Configuration permissions et tests

Mise en œuvre

Préparation du serveur physique : Création de la VM FilesServer

Dans le but de favoriser une intégration AD, nous allons créer une VM dédiée pour le serveur de fichiers.

Création VM ID 102, nom FilesServer : 2 CPUs, 6Go RAM, stockage 256Go.

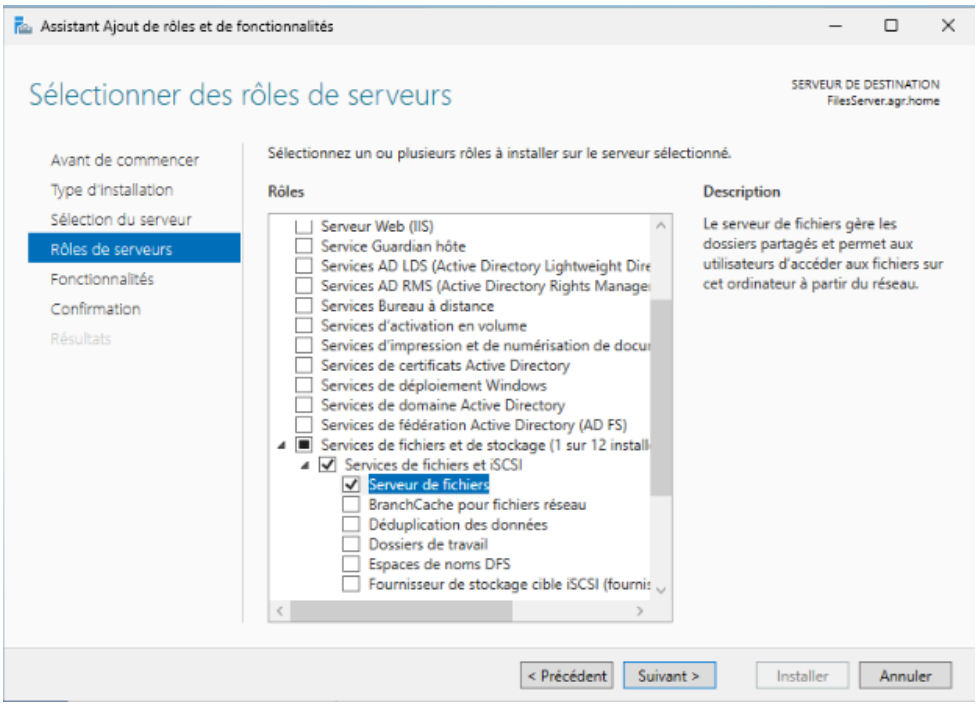
Image ISO Windows Server 2025, plus VirtIO pour pilotes.

Une fois installée, joindre directement au domaine agr.home via paramètres système.

Définir IP statique 192.168.10.110/24.

Préparation du serveur physique : Rôles et fonctionnalités

La VM FilesServer est en usage serveur depuis l'installation et utilise le rôle suivant :



Les fonctionnalités suivantes sont aussi disponibles : FSRM pour quotas.

Installation du rôle Serveur de fichiers et création du partage SMB

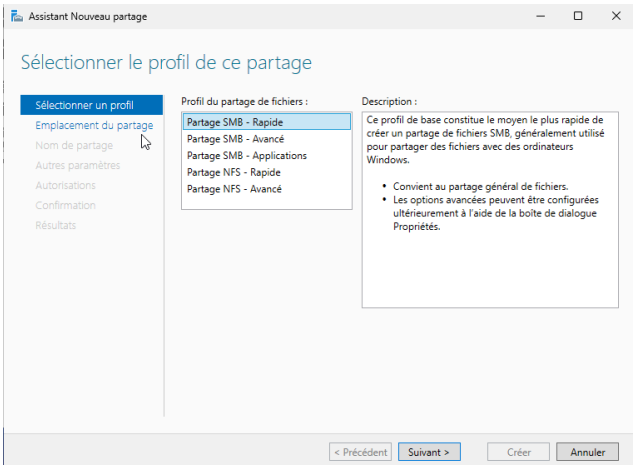
Pour commencer, nous allons ajouter le rôle Serveur de fichiers via Gestionnaire de serveur > Gérer > Ajouter des rôles et fonctionnalités.

Cela permet d'activer SMB, les outils de gestion et FSRM pour quotas.

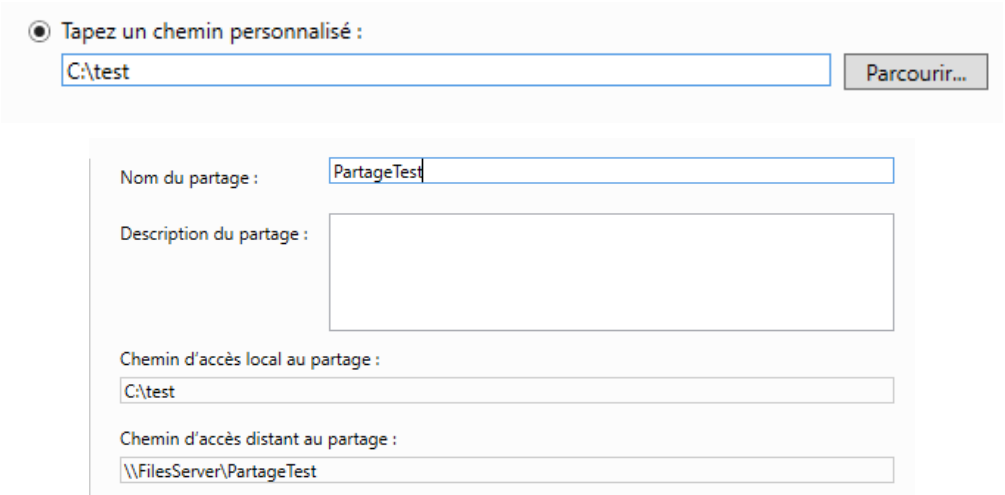
Pourquoi SMB : C'est le protocole standard Windows pour les partages réseau, sécurisé avec AD, et compatible avec les clients Windows pour un accès fluide.

Création du dossier C:\Test avec fichier .txt "Partage réussi" et sous-dossier vide.

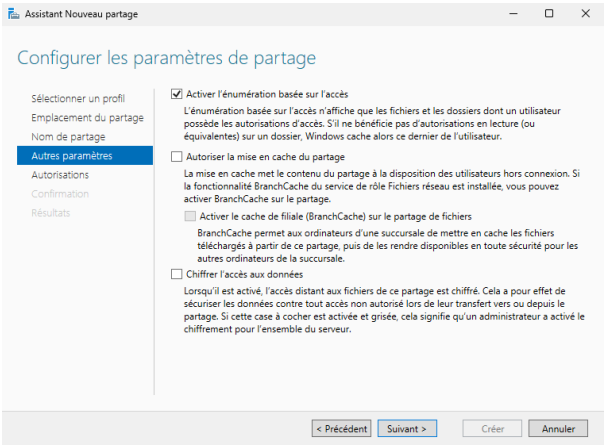
Création du partage SMB : Gestionnaire de serveur > Partages > Nouveau partage > SMB Rapide.



Nom : PartageTest, chemin \\FilesServer\PartageTest.



Options : Activer l'énumération basée sur l'accès (ABE) pour masquer les sous-dossiers non autorisés.



Configuration des permissions NTFS et SMB

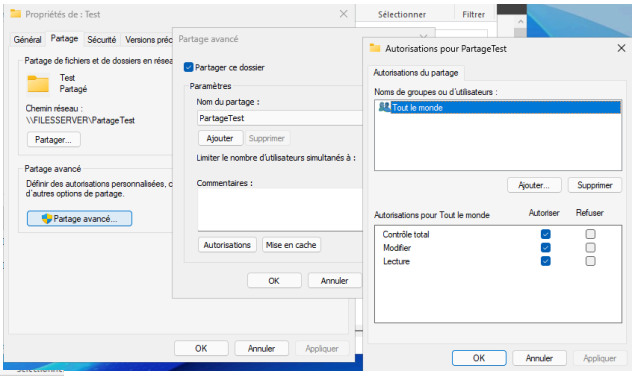
Nous allons séparer les permissions en deux : SMB au niveau partage et NTFS au niveau fichier.

Pourquoi permissions SMB : Elles contrôlent l'accès global au partage (Contrôle total, Lecture/Écriture, Lecture seule), simples et rapides à appliquer.

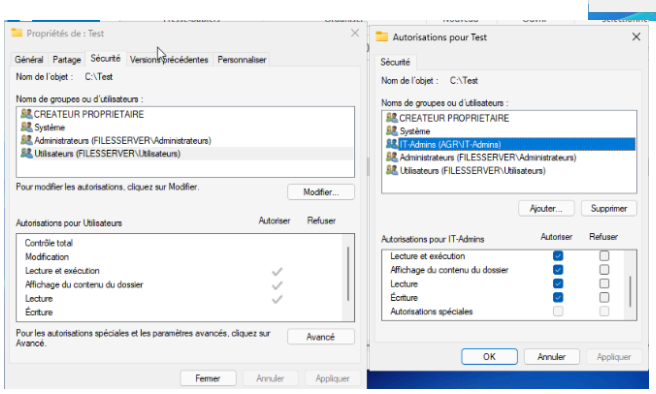
Pourquoi permissions NTFS : Elles gèrent les droits détaillés sur fichiers/dossiers (Lecture, Écriture, Modifier, etc.), persistants même si le disque est déplacé.

Les deux sont nécessaires et complémentaires : si conflit, les plus restrictives dominent.

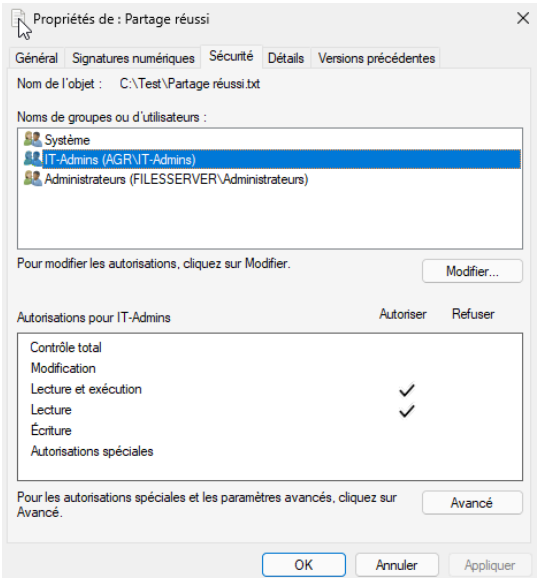
Permissions SMB : Explorateur > Propriétés > Partage avancé > Permissions > Groupe IT-Admins Lecture seule.



>

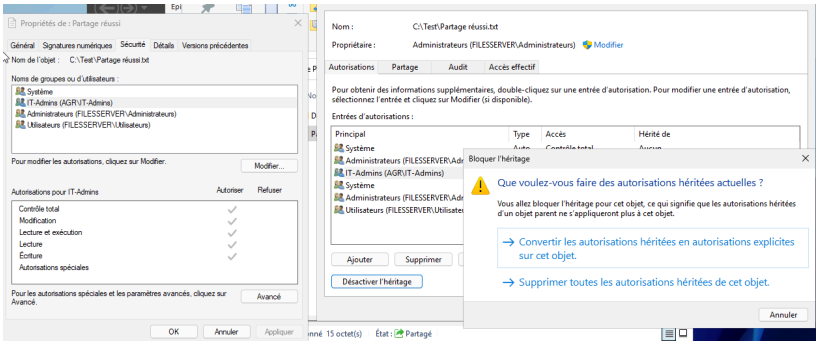


Permissions NTFS : Propriétés > Sécurité > Ajouter groupe IT-Admins > Lecture & exécution (fichier .txt visible, sous-dossier masqué pour autres).

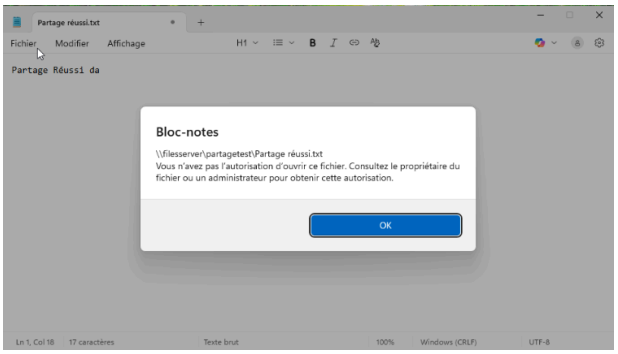


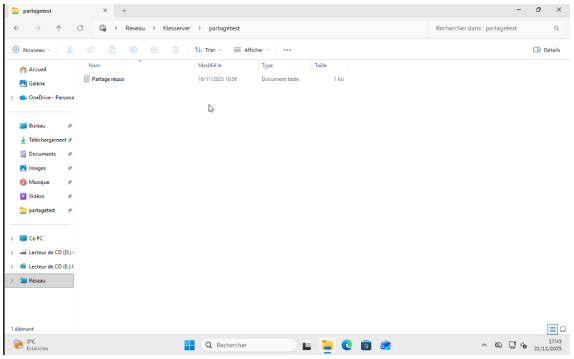
Tests d’accès et activation de l’ABE

Pourquoi ABE : Pour renforcer la sécurité en masquant les éléments non autorisés, évitant les fuites d’informations..



Test depuis VM Client avec utilisateur d.agricola (groupe IT-Admins) : \\FilesServer\PartageTest > fichier .txt visible en lecture seule, sous-dossier invisible grâce à ABE.





Bilan

Le serveur de fichiers est opérationnel avec partage SMB sécurisé, permissions NTFS/SMB complémentaires et ABE activée.

Les tests confirment un accès contrôlé en fonction des groupes AD.

Cette situation valide les compétences SISR en gestion des partages réseaux et sécurité des données.

Prochaines évolutions possibles :
– Migration du stockage partagé vers un NAS dédié (TrueNAS Scale ou Synology)
– Mise en place d’une DMZ
– Déploiement de Nextcloud ou Owncloud en parallèle pour un accès web/mobile sécurisé aux mêmes données