

# MISE EN PLACE D'UN SERVEUR DE FICHER AVEC SAMBA

# SAMBA

<b>I/</b>	<b>Cahier des charges .....</b>	<b>2</b>
1-	Descriptif de l'existant.....	2
2-	Besoins .....	2
3-	Contraintes.....	2
<b>II/</b>	<b>Ressources.....</b>	<b>3</b>
1-	Ressources mises à disposition .....	3
2-	Ressource nécessaire à la mise en place.....	3
3-	Gestion des ressources .....	4
<b>III/</b>	<b>Analyse.....</b>	<b>4</b>
1-	Descriptifs des solutions .....	4
2-	Comparaisons des solutions.....	5
3-	Choix d'une solution .....	6
4-	Cartographie du réseau.....	6
5-	Etude de l'impact sur le SI existant .....	7
6-	Phasage de l'intervention .....	8
7-	Prévision des tests de validation.....	9
8-	Déploiement .....	9
<b>IV/</b>	<b>Mise en place.....</b>	<b>10</b>
1-	Réalisation.....	10
2-	Rapport de tests.....	10
3-	Rapport de déploiement.....	11
<b>V/</b>	<b>Bilan .....</b>	<b>11</b>
1-	Conclusion.....	11
2-	Auto-évaluation.....	11

# I/ **Cahier des charges**

---

## 1- **Descriptif de l'existant**

L'infrastructure réseau actuellement en place a été conçue dans le cadre d'un environnement pédagogique destiné à l'épreuve E5 du BTS SIO option SISR. Elle repose sur une architecture segmentée en plusieurs VLAN permettant de structurer le trafic, d'améliorer la sécurité et de faciliter l'administration quotidienne.

Le réseau est organisé en quatre VLAN principaux.

- Le VLAN 10 regroupe l'ensemble des serveurs internes nécessaires au fonctionnement du système d'information (DHCP, AD / DNS, FOG, etc.).
- Le VLAN 20 est dédié aux services de sauvegarde et aux mécanismes de redondance, assurant la continuité des données et la résilience de l'infrastructure.
- Le VLAN 30 accueille les postes clients utilisés par les différents utilisateurs au sein du réseau.
- Le VLAN 99, réservé à l'administration, permet aux techniciens et administrateurs d'accéder aux outils de gestion et de supervision dans un espace isolé du trafic utilisateur (postes admins, serveur Zabbix, serveur Guacamole).

Une DMZ complète l'architecture en offrant un espace sécurisé destiné aux services nécessitant une exposition vers l'extérieur (serveur web). Elle limite ainsi les risques en cas de compromission de l'un de ces services.

L'accès aux réseaux externes et la connexion inter-VLAN est assurée par une solution pfSense configurée en haute disponibilité. Deux pare-feux pfSense fonctionnent conjointement grâce aux protocoles CARP, utilisé pour la gestion d'une adresse IP virtuelle partagée, et pfsync, permettant la synchronisation des états de connexion. Ce dispositif garantit une continuité de service en cas de défaillance d'un des deux équipements, tout en maintenant un niveau de sécurité constant.

## 2- **Besoins**

L'infrastructure doit être complétée par l'ajout d'un serveur de fichiers au sein du VLAN 10, dédié aux services internes. Ce serveur aura pour objectif principal de centraliser les ressources documentaires destinées aux différents services de l'organisation, tout en offrant aux utilisateurs un espace personnel accessible depuis leur poste de travail.

Les postes clients devront pouvoir accéder de manière sécurisée aux répertoires partagés ainsi qu'aux dossiers personnels, en fonction des autorisations définies. L'intégration du serveur dans l'environnement existant implique également qu'il puisse communiquer avec le contrôleur de domaine déjà en place. Celui-ci devra être en mesure de gérer les droits d'accès via les groupes Active Directory et d'appliquer certaines stratégies (GPO) nécessitant un accès direct aux partages.

L'ensemble doit s'intégrer naturellement au réseau actuel sans altérer la structure des VLAN ni les mécanismes de redondance déjà établis.

## 3- **Contraintes**

Le projet doit être mené dans un délai restreint, avec un rendu complet de l'infrastructure prévu pour le courant du mois d'avril. Cette contrainte impose une organisation rigoureuse, une planification

précise des interventions et une maîtrise des technologies utilisées afin d'éviter tout retard dans la mise en œuvre.

L'intégration du serveur de fichiers doit se faire sans perturber les services déjà opérationnels. La solution mise en place devra être compatible avec l'architecture réseau existante, notamment avec la segmentation par VLAN, la présence de la DMZ, ainsi qu'avec le système de haute disponibilité basé sur pfSense. Le serveur devra par ailleurs être pleinement interopérable avec le contrôleur de domaine afin de permettre la gestion centralisée des droits et des stratégies.

Enfin, la solution devra s'appuyer exclusivement sur des composants stables et éprouvés afin de garantir la fiabilité du service dans un contexte pédagogique simulant une production réelle.

## II/ Ressources

---

### 1- Ressources mises à disposition

L'infrastructure utilisée pour la réalisation du projet repose sur un environnement virtualisé mis à disposition dans le cadre de la formation. Cet environnement est hébergé sur une ferme de serveurs administrée par le GRETA, permettant aux étudiants de déployer et d'administrer différentes machines virtuelles pour leurs travaux pratiques et projets.

La virtualisation est assurée par l'hyperviseur open source Proxmox VE, qui permet de créer et de gérer plusieurs machines virtuelles au sein d'un même environnement physique. Cette plateforme facilite la mise en place d'une infrastructure réseau complète tout en offrant la possibilité de modifier ou de reconstruire rapidement les systèmes en cas de besoin.

L'environnement dispose également d'un accès à Internet, ce qui permet notamment de télécharger les différents systèmes d'exploitation, les logiciels nécessaires au déploiement des services ainsi que les mises à jour de sécurité. Cet accès est également indispensable pour tester les services destinés à être accessibles depuis l'extérieur du réseau, comme le futur service de cloud privé.

Les ressources matérielles allouées à l'infrastructure sont les suivantes :

- un espace de stockage total de 800 Go destiné à l'hébergement des machines virtuelles et de leurs données
- 64 Go de mémoire vive (RAM) permettant de faire fonctionner simultanément plusieurs serveurs et services
- 6 cœurs de processeur dédiés au fonctionnement de l'ensemble des machines virtuelles.

Ces ressources permettent de déployer l'ensemble des éléments de l'infrastructure nécessaires au projet, notamment les serveurs, les pare-feux, les services réseau ainsi que le futur serveur de fichiers.

### 2- Ressource nécessaire à la mise en place

La mise en place de l'infrastructure et des différents services associés nécessite l'utilisation de plusieurs systèmes d'exploitation déployés sous forme de machines virtuelles. Pour cela, différentes images ISO sont utilisées afin d'installer les systèmes nécessaires au fonctionnement du réseau et des services.

Tout d'abord, l'installation de pare-feu virtuels repose sur le système pfSense. Ce logiciel permet d'assurer plusieurs fonctions essentielles au sein de l'infrastructure, notamment le routage entre les

différents VLAN, le filtrage des flux réseau et la protection du système d'information. Deux instances sont déployées afin de garantir une redondance et d'améliorer la disponibilité du service.

Le système Windows Server 2025 est utilisé pour l'hébergement de plusieurs services d'infrastructure. Ce type de serveur peut notamment être utilisé pour la gestion de l'administration du réseau, l'hébergement de services internes ou encore la gestion des utilisateurs selon les besoins de l'infrastructure.

Les postes clients du réseau fonctionnent sous Windows 11. Ces machines permettent de tester l'accès aux différents services mis en place dans l'infrastructure, notamment l'accès aux ressources internes et aux services accessibles via le réseau.

Enfin, certaines machines virtuelles reposent sur le système d'exploitation libre Debian, notamment pour l'hébergement de services web ou applicatifs. Ce système est particulièrement adapté pour ce type d'usage en raison de sa stabilité et de sa large compatibilité avec de nombreux logiciels serveur. La version utilisée dans le cadre de ce projet est Debian 13, qui servira notamment de base pour le déploiement du service de cloud privé.

L'ensemble de ces systèmes constitue la base logicielle nécessaire à la création des différentes machines virtuelles de l'infrastructure et au déploiement des services attendus dans le cadre du projet.

### **3- Gestion des ressources**

Dans un environnement virtualisé, la gestion rigoureuse du processeur, de la mémoire vive et du stockage est indispensable pour garantir la stabilité des machines virtuelles. En utilisant la plateforme Proxmox VE, les ressources sont allouées sur mesure et ajustées selon l'importance de chaque service. Les éléments critiques, tels que les pare-feux pfSense et les serveurs applicatifs, bénéficient d'une priorité accrue pour assurer leur performance et la continuité du routage entre les VLAN. Parallèlement, les serveurs Windows Server 2025 et Debian 13 reçoivent des ressources adaptées à leurs rôles respectifs. Enfin, l'enveloppe globale de 800 Go de stockage est répartie stratégiquement afin de répondre aux besoins actuels tout en conservant une marge de manœuvre pour l'évolution future de l'infrastructure. Cette approche équilibrée permet d'allier performance système et flexibilité opérationnelle.

## **III/ Analyse**

---

### **1- Descriptifs des solutions**

Plusieurs approches peuvent être envisagées pour mettre en place un service de partage de fichiers dans l'infrastructure existante. Chaque solution présente des caractéristiques propres en termes de compatibilité, d'administration et de performances.

La première solution consiste à déployer un serveur de fichiers sous Windows Server. Cette approche repose sur le rôle "File and Storage Services", nativement intégré au système. Elle permet une gestion centralisée des partages, des permissions NTFS et une intégration complète à Active Directory. Cette solution offre également la possibilité d'appliquer des stratégies de groupe (GPO) pour automatiser la mise à disposition des lecteurs réseau sur les postes clients. Elle constitue un choix naturel dans les environnements majoritairement Windows.

La seconde solution consiste à utiliser un serveur de fichiers sous Linux, reposant sur le service Samba. Samba permet d'implémenter le protocole SMB, garantissant une compatibilité avec les postes Windows tout en conservant la flexibilité et la légèreté d'un système Linux. Cette alternative offre des performances solides, une grande stabilité et une administration adaptable selon les besoins de l'organisation. Elle peut être intégrée à Active Directory afin de gérer les permissions via les groupes de sécurité existants.

Une troisième option consiste à déployer un service de partage basé sur NFS (Network File System). Ce protocole, historiquement orienté vers les environnements Unix/Linux, offre de bonnes performances dans un contexte homogène. Toutefois, son intégration dans un parc majoritairement Windows nécessite des configurations supplémentaires et peut entraîner certaines limitations en matière de droits et d'authentification. Cette solution reste néanmoins envisageable dans des environnements mixtes ou pour des usages techniques spécifiques.

## 2- Comparaisons des solutions

Critère	Windows Server (Serveur de fichiers)	Linux + Samba	NFS
Compatibilité postes Windows	Excellente, native	Excellente via SMB	Moyenne, nécessite configurations spécifiques
Compatibilité postes Linux	Bonne mais moins naturelle	Très bonne	Excellente
Intégration Active Directory	Native et complète	Possible et stable	Limitée
Gestion des permissions	NTFS + ACL avancées	ACL POSIX + compatibilité AD	ACL possibles mais plus limitées
Gestion des GPO	Totale (lecteurs réseau, scripts, etc.)	Dépend d'AD (applicable indirectement)	Aucune
Performances	Très bonnes	Très bonnes selon configuration	Excellentes en environnement Linux
Sécurité	Avancée (NTFS, SMB signing, Kerberos)	Élevée (Kerberos, SMB3, chiffrement)	Bonne mais moins robuste pour Windows
Administration	Conviviale via GUI	Principalement en ligne de commande	Simple mais technique
Coût	Licence Windows Server obligatoire	Gratuit (open source)	Gratuit (open source)
Facilité de déploiement	Simple dans un environnement Windows	Demande une bonne maîtrise Linux	Simple dans un environnement Linux homogène
Adaptation aux environnements hétérogènes	Très bonne	Très bonne	Limité
Usage conseillé	Parcs Windows, intégration AD poussée	Environnements mixtes, besoin de flexibilité	Environnements Linux homogènes ou besoins techniques spécifiques

### 3- Choix d'une solution

Parmi les solutions étudiées, l'option retenue est l'installation d'un serveur de fichiers reposant sur Samba au sein d'un système Linux. Ce choix s'appuie sur plusieurs critères techniques et pédagogiques.

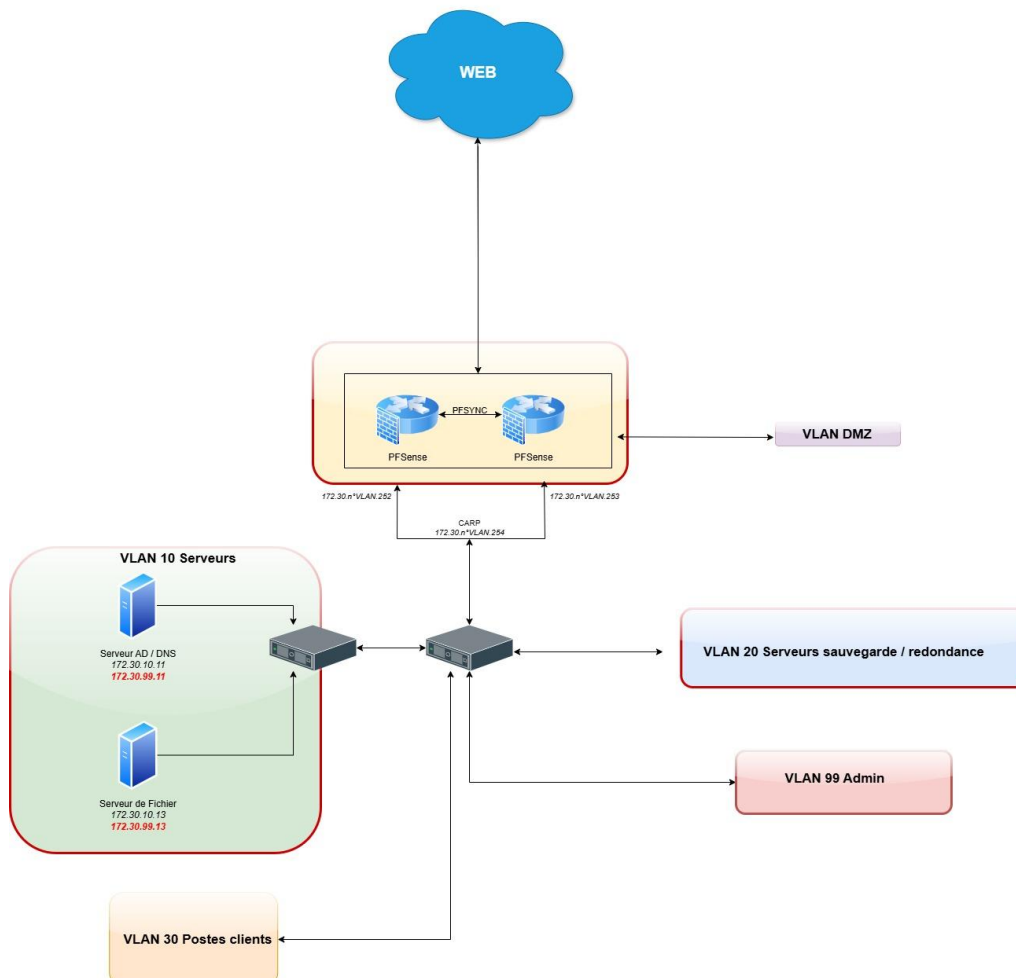
Linux offre une architecture légère et stable, particulièrement adaptée à un environnement virtualisé ou segmenté en VLAN comme celui de l'infrastructure existante. La consommation de ressources limitée et la fiabilité du système garantissent un fonctionnement efficace du service de partage de fichiers. Samba, de son côté, assure une compatibilité complète avec le protocole SMB, ce qui permet une intégration transparente avec les postes Windows et avec le contrôleur de domaine déjà en place.

Le choix d'une solution Linux/Samba présente également un intérêt pédagogique important. Il permet d'explorer en profondeur les mécanismes de gestion des permissions, les interactions entre Linux et Active Directory, ainsi que les aspects liés à la configuration réseau et à la sécurité. Cette approche favorise une compréhension plus large des environnements hétérogènes, dans lesquels Windows et Linux coexistent.

En combinant légèreté, interopérabilité et valeur pédagogique, la solution Samba constitue le choix le plus pertinent pour répondre aux besoins de l'infrastructure tout en offrant une occasion d'apprentissage complète et concrète.

### 4- Cartographie du réseau

#### a) Schéma



## b) Plan d'adressage

- VLAN 10 - Serveurs :

Réseau	172.30.10.0
Masque	255.255.255.0
1 <sup>ère</sup> Adresse	172.30.10.1
Dernière Adresse	172.30.10.254
Serveur AD / DNS	172.30.10.11
Serveur de fichiers	172.30.10.12
PFSense 1	172.30.10.252
PFSense 2	172.30.10.253
Passerelle CARP	172.30.10.254
Broadcast	172.30.10.255

- VLAN 99 - Admins :

Réseau	172.30.99.0
Masque	255.255.255.0
1 <sup>ère</sup> Adresse	172.30.99.1
Dernière Adresse	172.30.99.254
Serveur AD / DNS	172.30.99.11
Serveur de fichiers	172.30.99.12
PFSense 1	172.30.99.252
PFSense 2	172.30.99.253
Passerelle CARP	172.30.99.254
Broadcast	172.30.99.255

- VLAN 30 – Postes Clients :

Réseau	172.30.30.0
Masque	255.255.255.0
1 <sup>ère</sup> Adresse	172.30.30.1
Dernière Adresse	172.30.30.254
PFSense 1	172.30.30.252
PFSense 2	172.30.30.253
Passerelle CARP	172.30.30.254
Broadcast	172.30.30.255

## c) Tables de routage

- PFSense :

Réseau	Adresse	Masque	Passerelle	Interface
VLAN 10	172.30.10.0	255.255.255.0	172.30.10.254	172.30.10.254
VLAN 99	172.30.99.0	255.255.255.0	172.30.99.254	172.30.99.254
VLAN 30	172.30.30.0	255.255.255.0	172.30.30.254	172.30.30.254
Default	0.0.0.0	0.0.0.0	FAI	WAN

## 5- Etude de l'impact sur le SI existant

### a) Sécurité

L'ajout d'un serveur de fichiers Samba dans le VLAN 10 doit être réalisé en prenant en compte les aspects de sécurité afin de préserver l'intégrité et la confidentialité du système d'information existant.

Le serveur sera configuré pour restreindre l'accès aux partages selon les groupes Active Directory, garantissant que chaque utilisateur ou service ne puisse accéder qu'aux ressources qui lui sont autorisées. Les permissions seront définies de manière granulaire, en utilisant à la fois les ACL Samba et l'intégration AD, pour éviter tout accès non autorisé.

La communication entre le serveur et les postes clients, ainsi qu'avec le contrôleur de domaine, pourra être sécurisée via SMB3 avec chiffrement activé, réduisant le risque d'interception des données sur le réseau. L'accès au serveur depuis le VLAN 99 pourra également être limité pour renforcer la sécurité.

Enfin, le serveur sera intégré dans les mécanismes de sauvegarde existants (VLAN 20), permettant de sécuriser les données contre la perte ou la corruption, et les mises à jour du système et de Samba seront planifiées régulièrement pour corriger les vulnérabilités potentielles.

#### **b) Performance**

L'intégration d'un serveur Samba dans le VLAN 10 aura un impact sur les performances globales du réseau et du système d'information, qu'il est important d'anticiper.

Le serveur de fichiers sera dimensionné en fonction du nombre d'utilisateurs et de la charge attendue. La configuration du matériel (CPU, mémoire, stockage) sera adaptée pour permettre des transferts rapides et simultanés vers les postes clients.

Le placement du serveur dans le VLAN 10, déjà dédié aux services internes, permet de limiter l'exposition au trafic non nécessaire et de réduire la congestion réseau. Les mécanismes de redondance existants, notamment la haute disponibilité du pare-feu pfSense, contribuent également à maintenir des performances stables en cas de bascule d'un équipement.

Enfin, la mise en œuvre d'une surveillance des performances (Zabbix) permettra de détecter rapidement toute saturation ou ralentissement, et d'ajuster la configuration si nécessaire pour garantir une expérience utilisateur fluide et constante.

#### **c) Ergonomie**

L'intégration d'un serveur Samba sous Linux a été pensée pour que l'ergonomie reste optimale pour les utilisateurs finaux. Bien que le serveur fonctionne sans interface graphique, les postes clients accéderont aux fichiers via leur environnement Windows habituel, ce qui garantit une expérience familière et intuitive.

Les partages seront mappés en tant que lecteurs réseau sur les postes Windows, offrant un accès direct aux ressources des services et aux dossiers personnels sans nécessité de formation particulière. Les droits d'accès seront automatiquement gérés par Active Directory, assurant que chaque utilisateur ne voit que les fichiers qui lui sont autorisés.

Cette configuration permet de conserver un environnement familier pour les utilisateurs tout en profitant des avantages d'un serveur Linux léger et stable. L'expérience utilisateur reste cohérente avec leurs habitudes de travail, réduisant les erreurs et facilitant l'adoption du nouveau serveur de fichiers.

## **6- Phasage de l'intervention**

La mise en place du serveur Samba sera réalisée en plusieurs étapes afin de garantir une intégration progressive et maîtrisée dans l'infrastructure existante.

La première étape consistera à préparer le serveur Linux, avec l'installation de Debian 13 et l'application des mises à jour de sécurité. Les utilisateurs et groupes nécessaires seront créés conformément à l'Active Directory existant.

Ensuite, le serveur sera configuré pour se connecter au VLAN 10, assurant ainsi son intégration dans le réseau interne dédié aux services. Samba sera ensuite installé et configuré pour intégrer le serveur au domaine. Les partages de fichiers seront définis pour chaque service ainsi que pour les dossiers personnels des utilisateurs, avec création automatique de ces derniers afin qu'ils disposent d'un espace dédié dès leur première connexion.

La configuration des postes Windows permettra de rediriger le dossier Documents de chaque utilisateur vers son dossier personnel sur le serveur Samba. Cette redirection centralise les données, facilite les sauvegardes et garantit la cohérence des fichiers à travers les sessions.

Des tests de connectivité, d'accès aux partages et de fonctionnement de la redirection du dossier Documents seront réalisés pour valider la configuration avant la mise en production.

Enfin, une fois les tests concluants, le serveur sera mis en production et accessible aux utilisateurs. La surveillance des performances et de l'accès aux partages permettra d'assurer une exploitation optimale et continue.

## **7- Prévision des tests de validation**

Avant la mise en production du serveur Samba, plusieurs tests seront réalisés afin de s'assurer du bon fonctionnement du service et de son intégration dans le système d'information existant.

Il sera d'abord vérifié que le serveur est correctement connecté au VLAN 10 et qu'il communique avec le contrôleur de domaine. L'accès aux partages de fichiers pour chaque service sera testé, ainsi que la disponibilité des dossiers personnels pour tous les utilisateurs, conformément aux droits définis dans Active Directory.

La redirection du dossier Documents sur les postes Windows sera également vérifiée. Chaque utilisateur devra disposer d'un dossier personnel créé automatiquement lors de sa première connexion, et le contenu du dossier Documents devra se synchroniser correctement avec le serveur.

Des tests de performance permettront de s'assurer que le serveur peut supporter le nombre d'utilisateurs simultanés prévu et que les transferts de fichiers restent rapides et fiables. Enfin, la sécurité des données sera évaluée en vérifiant le chiffrement SMB, la restriction des accès selon les VLAN et les permissions définies, ainsi que la compatibilité avec les mécanismes de sauvegarde et de redondance existants.

Ces tests permettront de valider la configuration complète avant la mise en production, garantissant ainsi un service fiable et ergonomique pour l'ensemble des utilisateurs.

## **8- Déploiement**

Le déploiement du serveur Samba sera réalisé après validation complète des tests de pré-production. Le serveur sera intégré au VLAN 10 et rendu accessible aux postes clients.

Les partages de fichiers et les dossiers personnels seront configurés pour être automatiquement accessibles aux utilisateurs via les GPO du contrôleur de domaine. La redirection du dossier Documents

vers les dossiers personnels sera gérée directement par ces stratégies, garantissant une configuration uniforme et automatisée sur l'ensemble des postes Windows sans intervention manuelle.

Le déploiement inclura également l'intégration du serveur aux mécanismes de sauvegarde et de redondance existants, ainsi que la mise en place d'outils de surveillance des performances et des accès.

Un suivi post-déploiement sera assuré afin de vérifier que les utilisateurs accèdent correctement aux fichiers, que la redirection des documents fonctionne comme prévu et que l'infrastructure continue de respecter les exigences de sécurité et de performance.

## IV/ Mise en place

---

### 1- Réalisation

#### a) Installation des pare-feu PFSense

- [Installation et configuration de PFSense](#)
- Pour la configuration du CARP et de PFSync, se référer à la mise en situation professionnelle [Redondance de Pare-feu PFSense](#)

#### b) Mise en place du serveur de fichier

- [Installation de Debian 13](#)
  - Espace disque : 20 Go
  - Un disque supplémentaire de 100 Go pour stocker le dossier partagé.
  - Mémoire : 2 Go
  - Cœur : 1
- [Installation et configuration d'un serveur SAMBA](#)

### 2- Rapport de tests

Avant la mise en production, une série de tests a été réalisée pour valider le fonctionnement du serveur Samba et son intégration dans le réseau existant.

La connectivité du serveur au VLAN 10 a été vérifiée, assurant l'accès aux postes clients et au contrôleur de domaine. Les partages de fichiers ont été testés pour chaque service, confirmant que les dossiers étaient accessibles uniquement aux utilisateurs autorisés conformément aux groupes définis dans Active Directory.

La création automatique des dossiers personnels a été validée pour chaque utilisateur. La redirection du dossier Documents depuis les postes Windows vers les dossiers personnels sur le serveur a également été testée et fonctionne correctement, garantissant la centralisation des données et la continuité des fichiers entre les sessions.

Des tests de performance ont permis de vérifier que le serveur supporte le nombre d'utilisateurs simultanés prévu sans ralentissement significatif. La sécurité des échanges a été confirmée grâce au chiffrement SMB et à la limitation des accès selon les droits et le VLAN.

Ces tests ont permis de s'assurer que le serveur Samba est fonctionnel, sécurisé, performant et ergonomique pour les utilisateurs, avant son intégration finale dans le système d'information.

### **3- Rapport de déploiement**

Le serveur Samba a été déployé avec succès sur le VLAN 10 après validation des tests de pré-production. L'intégration au réseau interne a été réalisée sans interruption des services existants. Les partages de fichiers ont été mis à disposition des services, et les dossiers personnels ont été créés automatiquement pour tous les utilisateurs conformément aux configurations Active Directory.

La redirection du dossier Documents sur les postes Windows vers les dossiers personnels du serveur a été prise en charge par les GPO du domaine. Les utilisateurs ont ainsi pu accéder immédiatement à leurs ressources sans configuration manuelle sur leurs postes.

Le serveur a été intégré aux mécanismes de sauvegarde et de redondance existants, garantissant la sécurité et la continuité des données. Les outils de surveillance ont été activés pour suivre les performances et l'accès aux fichiers, permettant de détecter rapidement toute anomalie ou saturation.

Le déploiement s'est déroulé conformément au phasage prévu et aux exigences du cahier des charges. Les objectifs de performance, de sécurité et d'ergonomie ont été atteints, assurant une mise à disposition fiable et efficace des ressources aux utilisateurs.

## **v/ Bilan**

---

### **1- Conclusion**

La mise en place du serveur Samba sous Debian 13 a permis de répondre efficacement aux besoins identifiés dans le cahier des charges. L'infrastructure a été enrichie par un service de fichiers centralisé, accessible aux postes clients et intégré au contrôleur de domaine pour la gestion des droits et la redirection automatique des dossiers Documents.

Le choix d'une solution Linux/Samba s'est révélé pertinent, combinant légèreté, fiabilité et compatibilité avec les environnements Windows existants. L'intégration a été réalisée sans perturber les services existants, et les tests de connectivité, de sécurité et de performance ont confirmé le bon fonctionnement du serveur.

Ce projet a permis d'assurer une centralisation sécurisée des données, une gestion simplifiée des droits utilisateurs et une ergonomie adaptée pour les utilisateurs, tout en respectant les contraintes de délai et les standards de sécurité de l'infrastructure.

### **2- Auto-évaluation**

La réalisation de ce projet a permis de mobiliser et de développer plusieurs compétences essentielles pour un technicien réseau. La planification et le phasage de l'intervention ont renforcé la capacité à organiser et structurer un projet technique dans le respect des contraintes de temps et des standards professionnels.

La configuration d'un serveur Linux avec Samba, son intégration au domaine Active Directory et la mise en place de la redirection du dossier Documents ont permis d'acquérir des compétences concrètes en administration réseau, en gestion des droits et en interopérabilité entre systèmes Linux et Windows.

L'analyse de l'impact sur le système d'information, incluant les aspects de sécurité, de performance et d'ergonomie, a renforcé la compréhension des bonnes pratiques dans le déploiement d'un service critique pour les utilisateurs.

Enfin, la réalisation des tests de validation et le suivi du déploiement ont permis de mesurer l'importance de la vérification et de la documentation dans un projet professionnel. Ce projet constitue une expérience complète et formatrice, qui prépare efficacement à la gestion de services réseau dans un environnement réel.