Fonctionnalités principales d’un NAS : Chiffrement et Sécurité des Données

1. Introduction

Un Network Attached Storage (NAS) est un serveur de stockage centralisé permettant de partager des fichiers et de gérer les données des utilisateurs d’une entreprise. Il offre une gestion efficace des accès, une redondance des données et des fonctionnalités avancées de sécurité et de chiffrement. Pour Assurmer, l’implémentation d’un NAS vise à garantir l’intégrité et la disponibilité des données professionnelles tout en minimisant les risques de perte ou de vol.

2. Fonctionnalités principales d’un NAS

a) Stockage centralisé et gestion des accès

Un NAS permet à plusieurs utilisateurs d’accéder simultanément aux fichiers via un réseau local ou distant. Les droits d’accès sont gérés grâce à des permissions spécifiques définies par l’administrateur, avec des ACL (Access Control List) précises.

Configuration recommandée : - **Création des utilisateurs et groupes :** Utilisation d’un serveur LDAP ou Active Directory pour centraliser la gestion des accès. - **Permissions d’accès :** Application de la politique du moindre privilège en attribuant des droits en lecture, écriture ou exécution uniquement lorsque nécessaire.

b) Protocoles de partage de fichiers

Les NAS modernes supportent plusieurs protocoles pour le partage et l’accès aux fichiers :

Protocole	Description	Cas d’usage recommandé
SMB (Server Message Block)	Utilisé principalement dans les environnements Windows.	Partage de fichiers entre machines Windows, intégration avec Active Directory.

Protocole	Description	Cas d’usage recommandé
NFS (Network File System)	Adapté aux systèmes Linux/Unix.	Montage de volumes distants pour serveurs Linux et Unix.
FTP / SFTP	Permet un transfert sécurisé des fichiers.	Transferts ponctuels nécessitant une sécurité accrue.
iSCSI	Utilisé pour le stockage en bloc et les bases de données.	Stockage réseau pour serveurs nécessitant des disques en réseau.

c) Redondance et sauvegarde des données

Les NAS intègrent des systèmes de protection des données tels que :

Technologie	Description	Avantages
RAID 1	Mirroring des disques	Sécurité accrue contre la perte de disque.
RAID 5	Répartition des données avec parité	Bon compromis entre performance et sécurité.
RAID 6	Double parité	Meilleure protection contre les pannes multiples.
RAID 10	RAID 1 + RAID 0	Haute performance et redondance optimale.

3. Chiffrement des données

a) Chiffrement au repos

Le chiffrement des fichiers stockés sur le NAS protège contre les accès non autorisés, même en cas de vol des disques.

Algorithme	Description	Utilisation
AES-256	Chiffrement symétrique puissant adapté aux fichiers sensibles.	Protection des fichiers stockés sur le NAS.
RSA	Chiffrement asymétrique pour la protection des clés de chiffrement.	Sécurisation des échanges de clés.

b) Chiffrement en transit

Le chiffrement des données en transit empêche l'interception lors du transfert sur le réseau.

Protocole	Description	Utilisation recommandée
TLS 1.2 / 1.3	Assure une communication sécurisée entre le client et le serveur.	Accès distant sécurisé.
VPN (OpenVPN, WireGuard)	Création d'un tunnel sécurisé entre client et NAS.	Accès sécurisé pour les utilisateurs distants.

c) Impact sur la performance

Le chiffrement peut ralentir légèrement les performances du NAS en raison des calculs cryptographiques. Il est donc conseillé : - D'utiliser des processeurs prenant en charge l'accélération matérielle AES-NI. - D'optimiser les caches disque et la gestion des IOPS.

4. Sécurité des données

a) Gestion des accès et authentification

Sécurité	Description	Recommandation
Active Directory (AD) / LDAP		Intégration avec le SI de l'entreprise.

Sécurité	Description	Recommandation
	Gestion centralisée des utilisateurs et des permissions.	
Authentification multifacteur (MFA)	Protection renforcée des comptes utilisateurs.	Activation obligatoire pour les accès distants.

b) Protection contre les cyberattaques

Menace	Solution	Recommandation
Ransomware	Sauvegarde régulière et snapshots des données.	Automatisation des snapshots toutes les heures.
Intrusions réseau	Pare-feu et filtrage IP stricts.	Blocage des adresses IP suspectes.
Malware	Antivirus intégré et analyse des fichiers.	Vérification hebdomadaire des fichiers stockés.

c) Mises à jour et correctifs de sécurité

Un NAS doit être régulièrement mis à jour pour corriger les vulnérabilités connues (CVE). Il est recommandé d’activer :

Action	Objectif	Outil recommandé
Notifications de mises à jour automatiques	Maintien d’un environnement sécurisé.	TrueNAS Update Manager, Synology DSM Update.
Surveillance des vulnérabilités via CVE Tracker	Identification proactive des menaces.	CVE Tracker, RSS des éditeurs.

5. Conclusion

L’intégration d’un NAS chez Assurmer améliore la gestion et la sécurité des données tout en assurant une protection contre les menaces cybernétiques. Le chiffrement des données et la gestion des accès sont des éléments essentiels pour garantir l’intégrité et la confidentialité des fichiers professionnels. La mise en place d’un monitoring actif et d’une stratégie de sauvegarde adaptée renforce la robustesse du système face aux menaces modernes.