AP 9 : Fonctionnalités principales d'un NAS	HUYNH Michael SAKO Bah FRANÇAIS Benjamin 2B-SISR

ASSURMER

Version	Auteur	Date	Nombre de pages	À l'attention de	Mode de diffusion	Validateur
1.0	HUYNH Michael	01/03/2025	21	Assurmer-IT	Document PDF	Benjamin FRANCAIS

FONCTIONNALITÉS PRINCIPALES D'UN NAS

Table des matières

Introduction

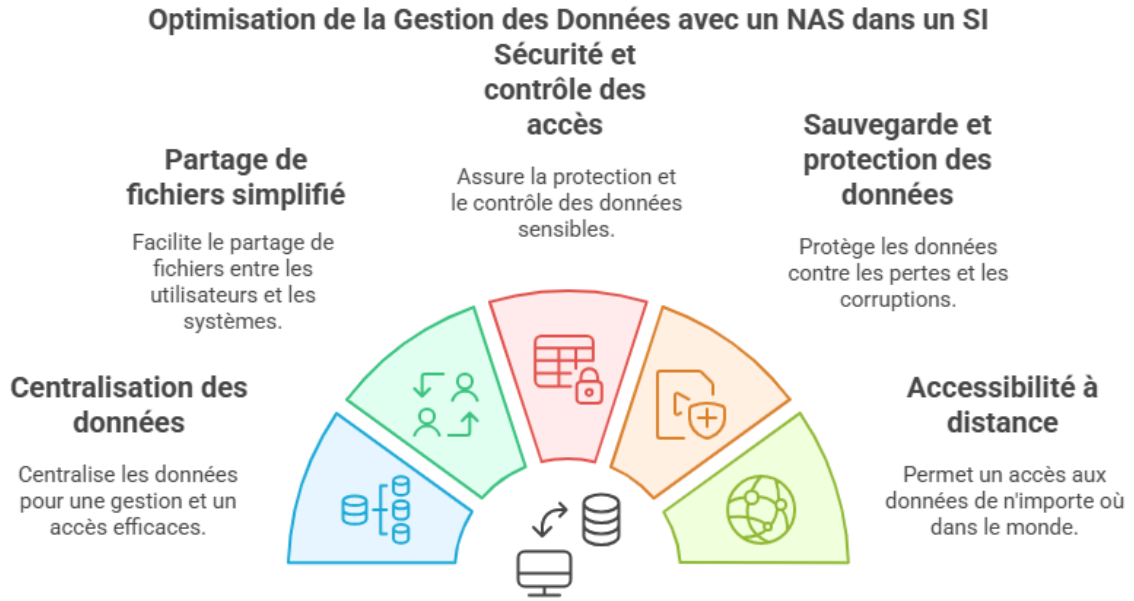
a. *Définition d'un NAS*

Un NAS (Network Attached Storage) est un périphérique de stockage connecté au réseau permettant à plusieurs utilisateurs et appareils d'accéder aux données centralisées. Contrairement aux disques durs externes classiques, un NAS est autonome et fonctionne comme un mini-serveur, offrant des services de stockage, de partage et de gestion des fichiers sur un réseau local (LAN) ou à distance.

Un NAS peut être utilisé à la fois dans des environnements personnels, pour stocker des fichiers multimédias et des sauvegardes, et dans des environnements professionnels, où il joue un rôle crucial dans la gestion des données, la collaboration et la protection des informations sensibles.

b. *Importance d'un NAS dans un Système d'Information (SI)*

L'intégration d'un NAS dans un Système d'Information (SI) est essentielle pour plusieurs raisons :

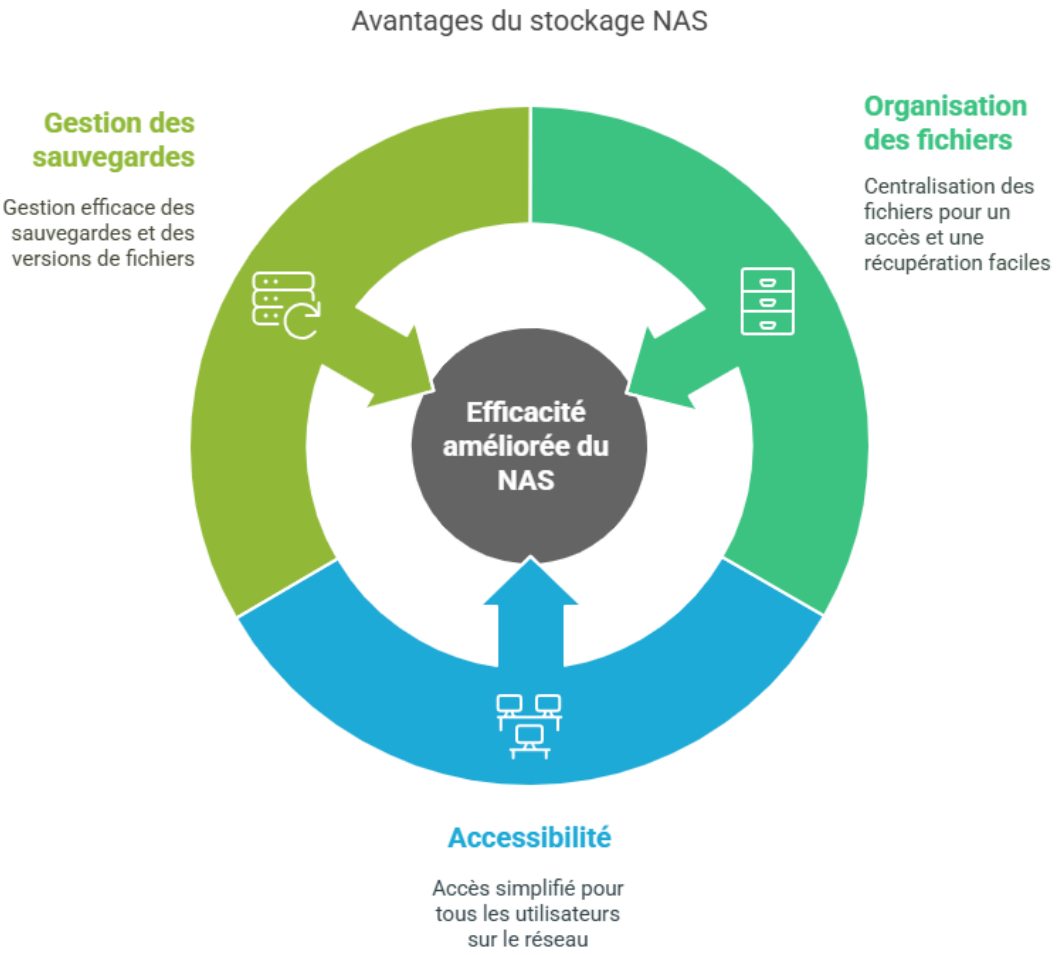


Présentation des fonctionnalités principales d'un NAS

Un NAS (Network Attached Storage) est bien plus qu'un simple espace de stockage en réseau. Il offre une multitude de fonctionnalités qui facilitent la gestion, le partage et la sécurisation des données. Dans cette section, nous allons détailler les principales caractéristiques qui font du NAS une solution incontournable pour les entreprises et les particuliers.

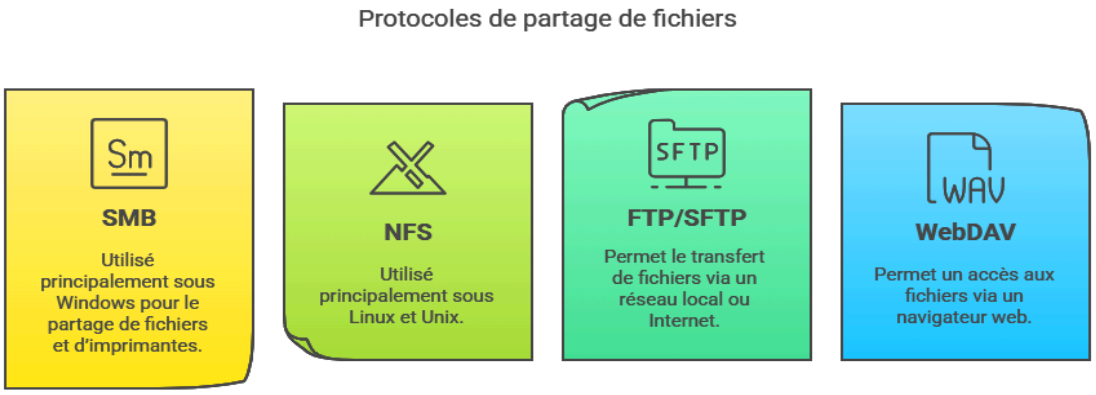
a. Stockage centralisé et accès aux fichiers

L'un des principaux avantages d'un NAS est de centraliser les données en un seul emplacement accessible par tous les utilisateurs autorisés. Cette centralisation permet :



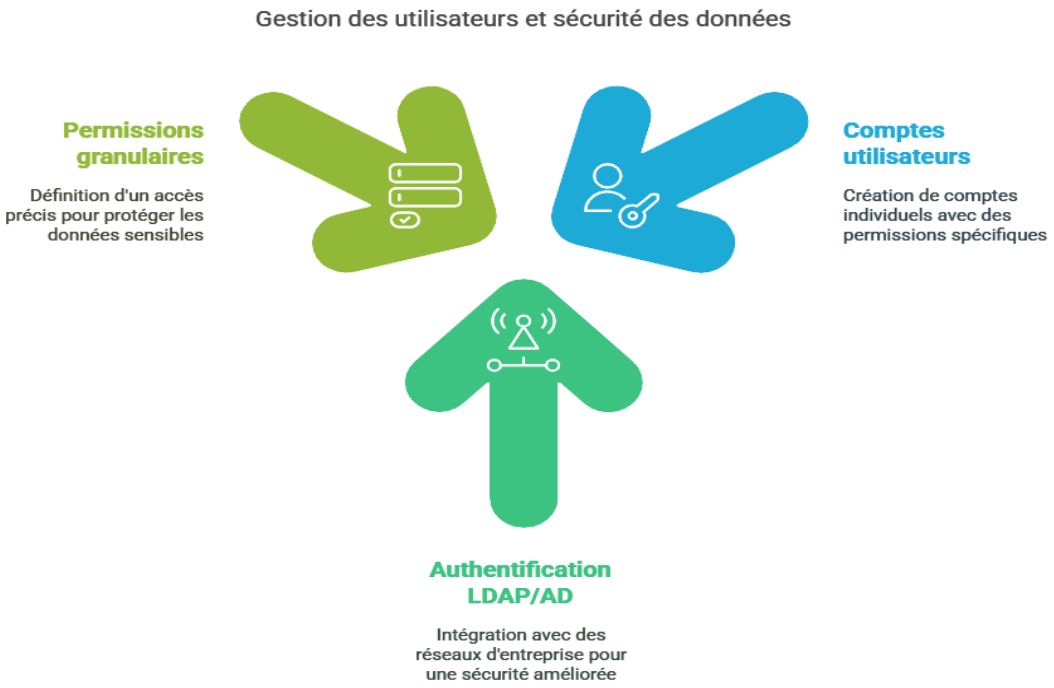
b. Partage de fichiers et protocoles pris en charge

Un NAS supporte plusieurs protocoles de communication pour assurer un partage efficace des fichiers entre différents systèmes d'exploitation (Windows, macOS, Linux) et appareils. Les protocoles les plus courants sont :



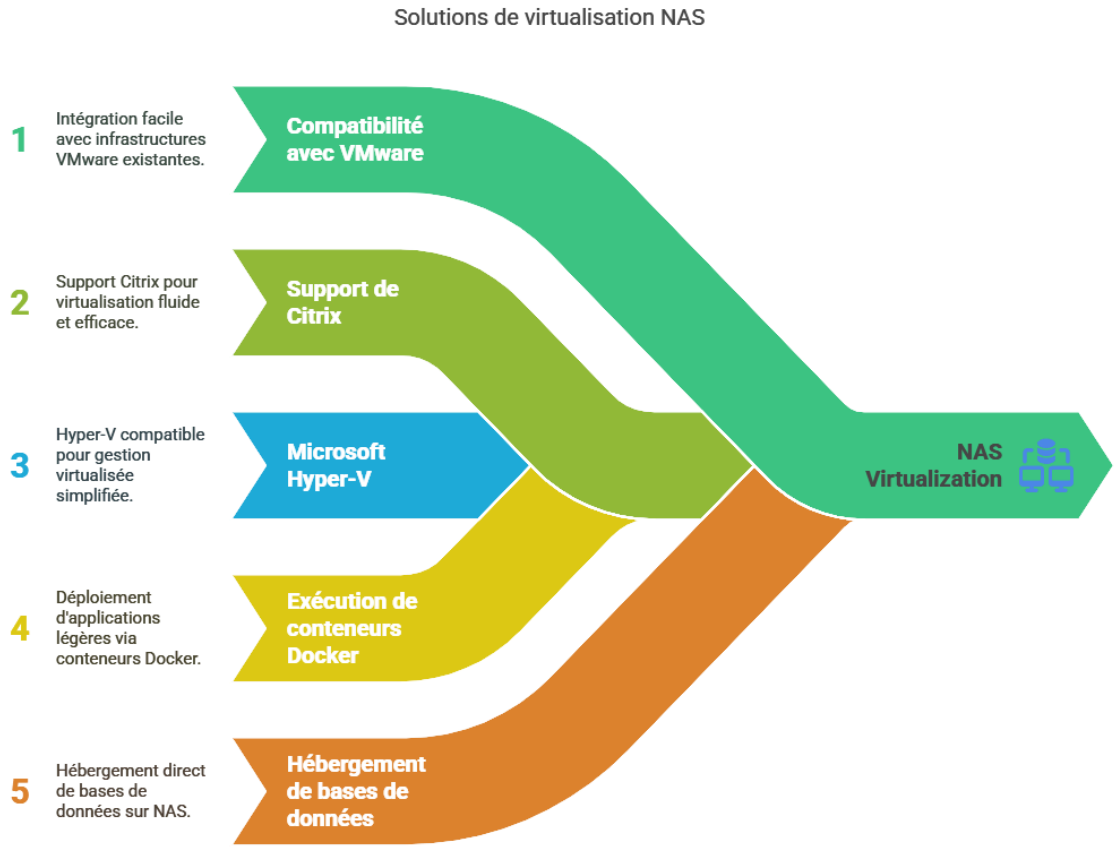
c. Gestion des utilisateurs et des droits d'accès

Un NAS permet une gestion avancée des utilisateurs et des permissions d'accès, ce qui est essentiel pour assurer la confidentialité et la sécurité des données. Les fonctionnalités incluent :



d. Virtualisation et compatibilité avec les environnements professionnels

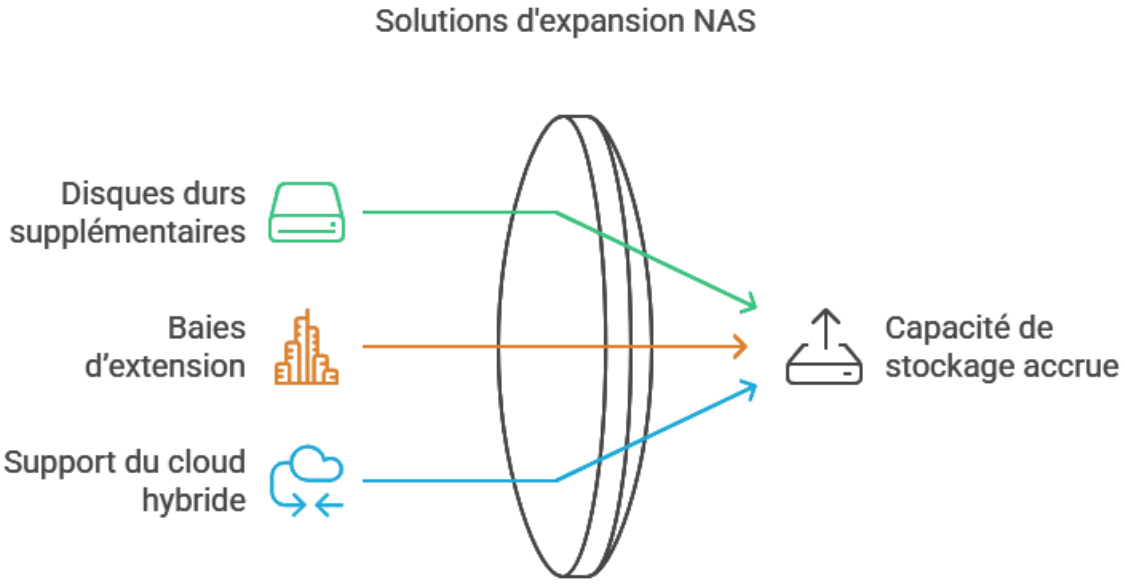
Certains NAS avancés offrent des fonctionnalités de virtualisation, permettant de créer et gérer des machines virtuelles (VM) directement sur l'appareil. Ces fonctionnalités incluent :



e. Extensibilité et évolutivité

Un NAS peut évoluer en fonction des besoins de l'utilisateur grâce à différentes options :

- Ajout de disques durs supplémentaires pour augmenter la capacité de stockage.
- Mise en place de baies d'extension pour accroître la capacité au-delà des limites initiales du NAS.
- Support du cloud hybride, permettant de combiner stockage local et solutions cloud comme Google Drive, Dropbox, ou Amazon S3.



Sécurité des données sur un NAS

La sécurité des données est un aspect fondamental de tout système de stockage en réseau. Un NAS contient souvent des informations sensibles, et il est donc essentiel de mettre en place des mesures de protection robustes pour éviter les accès non autorisés, les fuites de données et les cyberattaques.

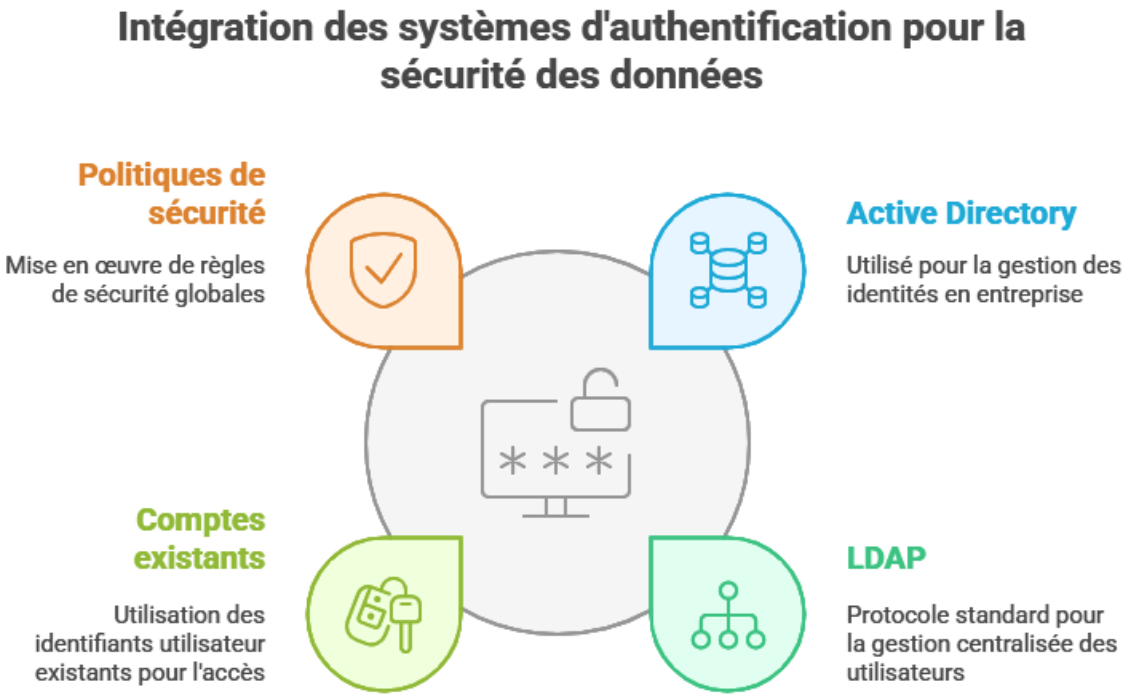
a. Gestion des permissions et des accès

Un NAS permet de définir des niveaux d'accès spécifiques pour chaque utilisateur ou groupe, garantissant que seules les personnes autorisées peuvent consulter ou modifier certains fichiers.

b. Authentification et intégration avec un annuaire LDAP/Active Directory

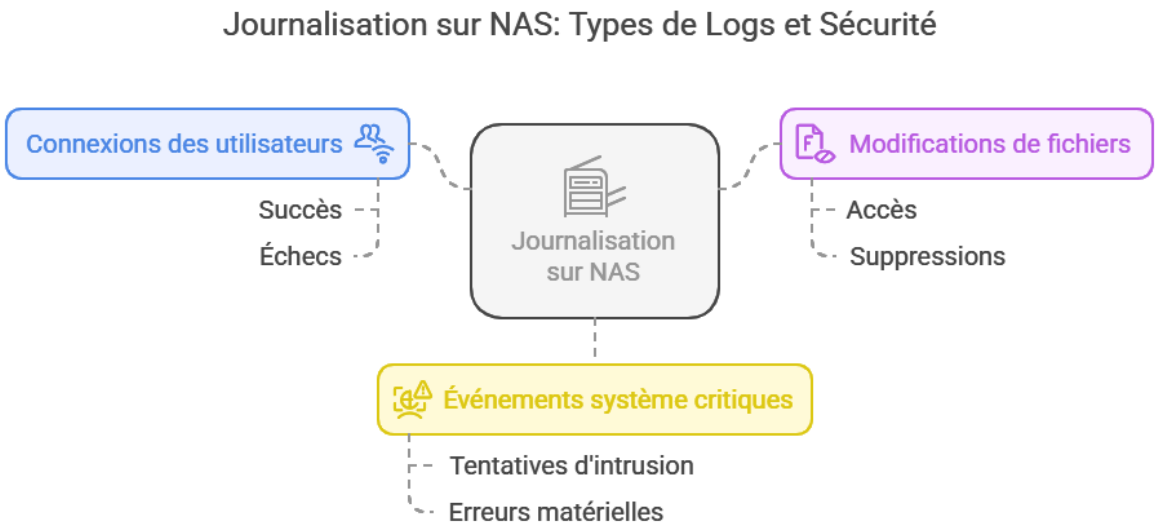
Pour une gestion centralisée des accès, les NAS modernes offrent une intégration avec des annuaires d'authentification tels que :

Active Directory (AD) de Microsoft, utilisé en entreprise pour la gestion des identités.
LDAP (Lightweight Directory Access Protocol), un protocole standard pour centraliser les utilisateurs et leurs droits.



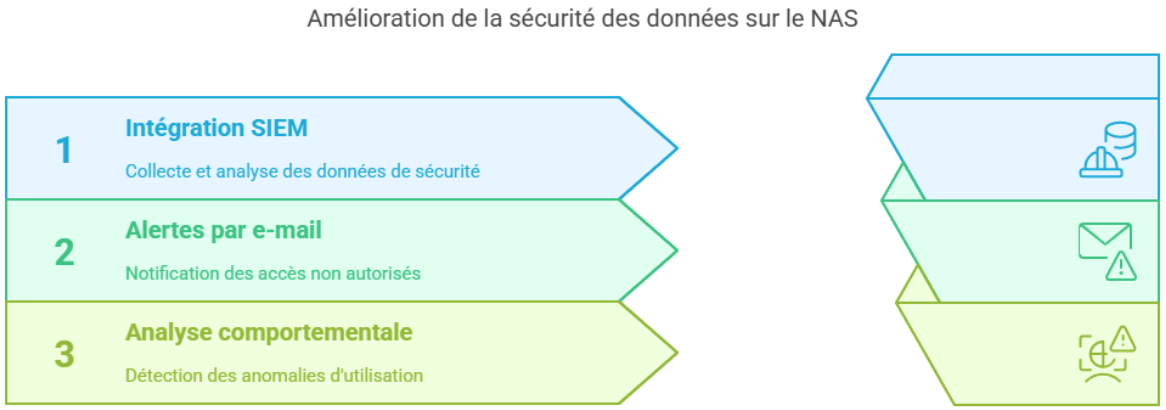
c. Surveillance et journalisation des accès

La mise en place d'un système de journalisation est cruciale pour suivre les activités sur un NAS et détecter d'éventuels comportements suspects.



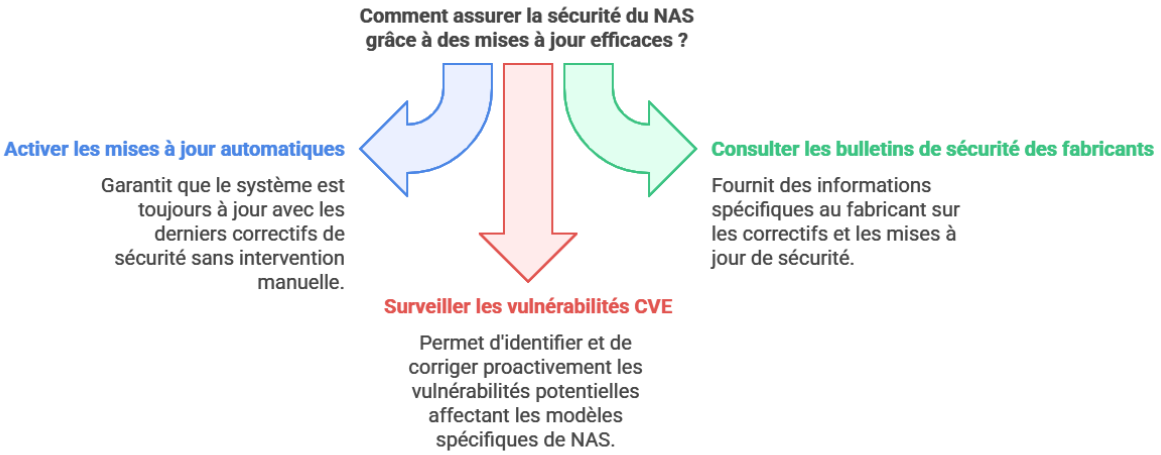
Certains NAS permettent même de générer des alertes en temps réel pour prévenir l'administrateur en cas d'activités anormales.

Exemple de fonctionnalités avancées :

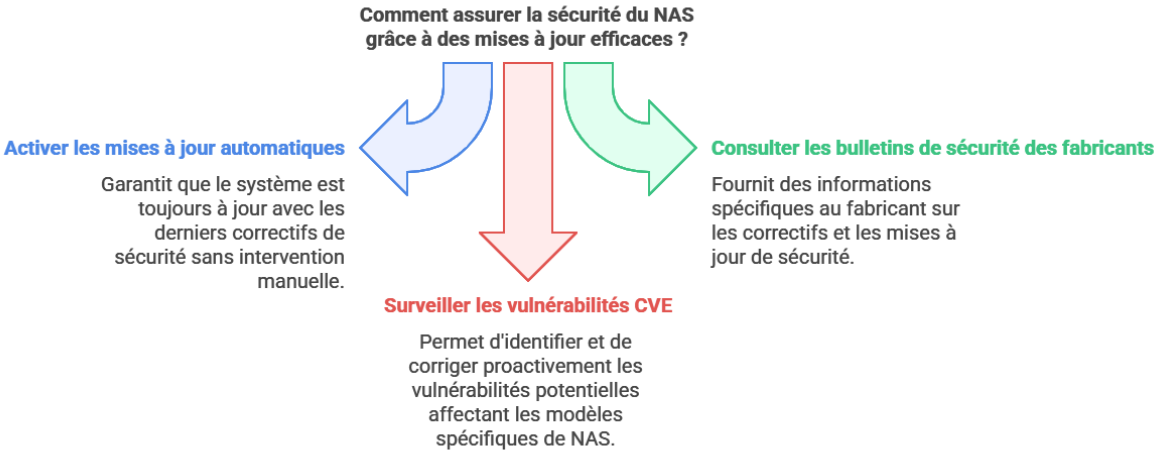


d. Mises à jour et gestion des vulnérabilités

Un NAS doit être régulièrement mis à jour pour corriger les failles de sécurité et éviter les attaques exploitant des vulnérabilités connues.



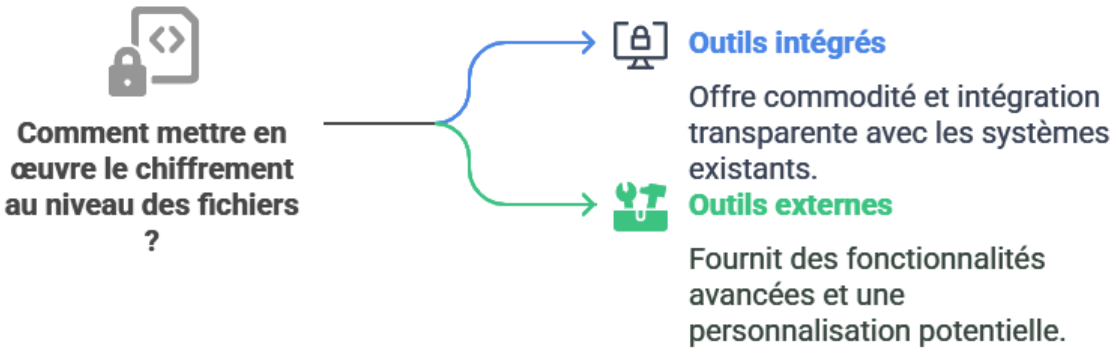
De plus, certaines solutions NAS offrent des outils de protection avancée, comme :



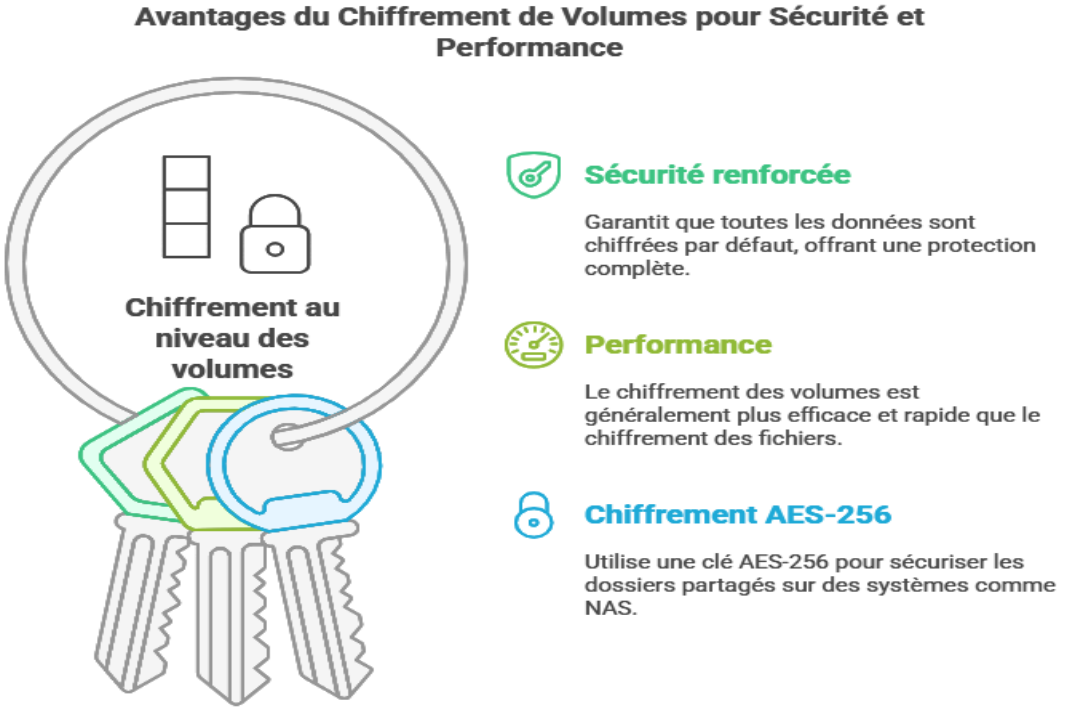
Chiffrement des données sur un NAS

Les solutions NAS offrent généralement deux types de chiffrement :

a. *Chiffrement au niveau des fichiers et des volumes*

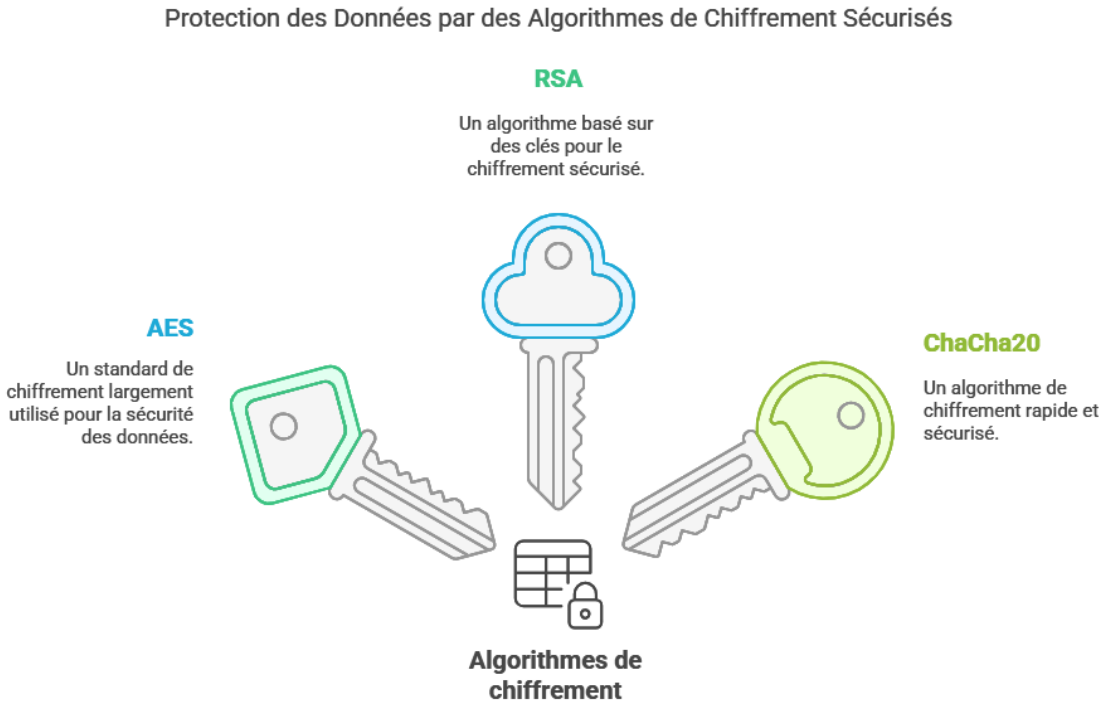


Volumes :



b. Algorithmes de chiffrement couramment utilisés

Le chiffrement repose sur des algorithmes cryptographiques qui garantissent la protection des données contre toute tentative de déchiffrement non autorisé. Les algorithmes les plus couramment utilisés dans les solutions NAS sont :



AES (Advanced Encryption Standard)

AES-128, AES-192 et AES-256 sont les standards les plus courants.
AES-256 est le plus sécurisé et recommandé pour les environnements professionnels.
Utilisé par de nombreuses solutions NAS (Synology, QNAP, TrueNAS, etc.).

RSA (Rivest-Shamir-Adleman)

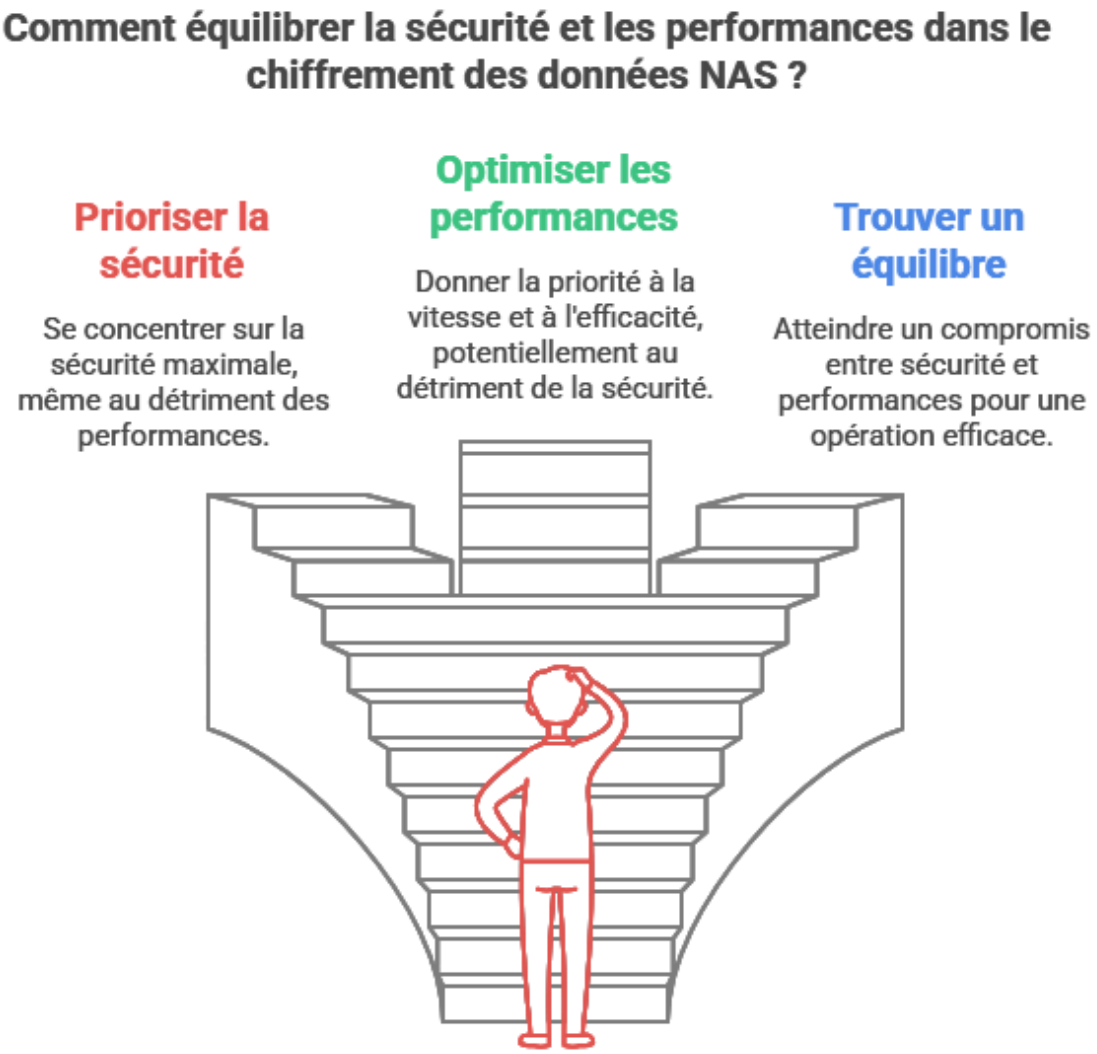
Principalement utilisé pour l'authentification et l'échange de clés.
Permet de sécuriser la transmission des clés de chiffrement.

ChaCha20

Un algorithme alternatif à AES, réputé pour sa rapidité et son efficacité sur des appareils avec peu de puissance de calcul.

c. Impact du chiffrement sur les performances

Le chiffrement apporte un haut niveau de sécurité, mais il peut aussi avoir un impact sur les performances du NAS. Voici quelques éléments à prendre en compte :



Consommation des ressources

Le chiffrement demande de la puissance de calcul, ce qui peut ralentir les transferts de fichiers et les accès aux données.
Un NAS avec un processeur compatible AES-NI (accélération matérielle du chiffrement) réduit cet impact.

Débit réseau réduit

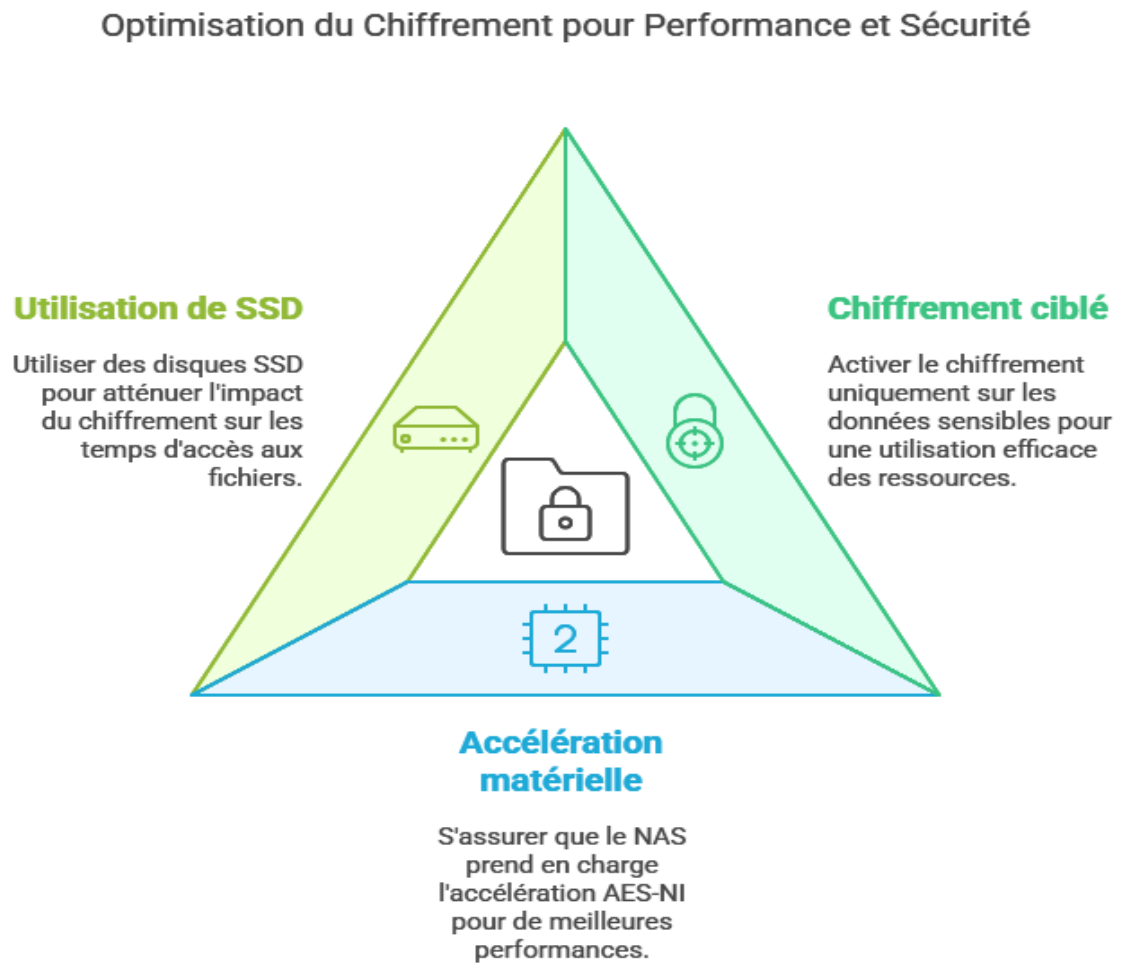
Les fichiers chiffrés peuvent prendre plus de temps à être transférés, en fonction du type de chiffrement utilisé.

Espace disque utilisé

Le chiffrement ne modifie pas la taille des fichiers, mais certains systèmes de chiffrement créent des métadonnées qui peuvent légèrement augmenter l'utilisation du stockage.

Bonnes pratiques pour minimiser l'impact :

Activer le chiffrement uniquement sur les données sensibles.
Vérifier que le NAS supporte l'accélération matérielle AES-NI.
Utiliser des disques SSD si le chiffrement ralentit l'accès aux fichiers.



d. Gestion des clés et récupération des données

La gestion des clés de chiffrement est un aspect critique du chiffrement des données. Sans la clé, les fichiers deviennent totalement inaccessibles.

Stockage des clés de chiffrement

Certaines solutions permettent de stocker la clé sur le NAS (moins sécurisé).
Il est recommandé d'utiliser un périphérique externe (clé USB, serveur distant) pour stocker la clé en dehors du NAS.

Récupération en cas de perte de la clé

Si la clé est perdue et qu'aucune sauvegarde n'a été faite, les données sont irrécupérables.
Il est important d'imprimer ou de stocker une copie de la clé de récupération dans un endroit sûr.

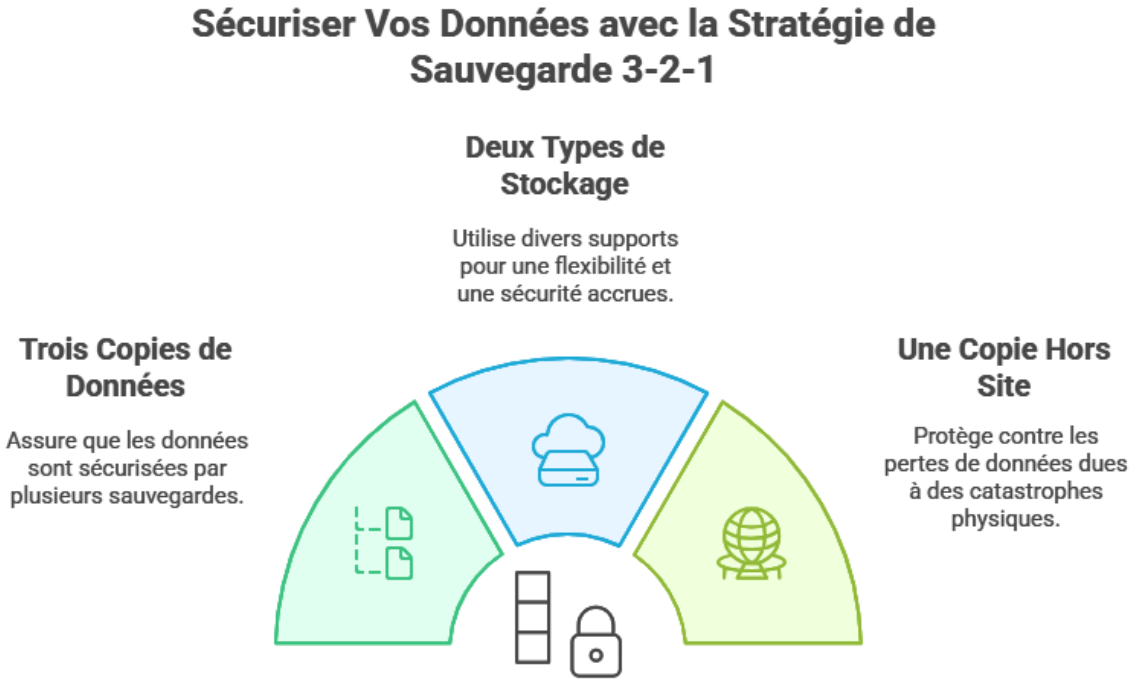
Bonnes pratiques pour la gestion des clés :

Sauvegarde et redondance des données

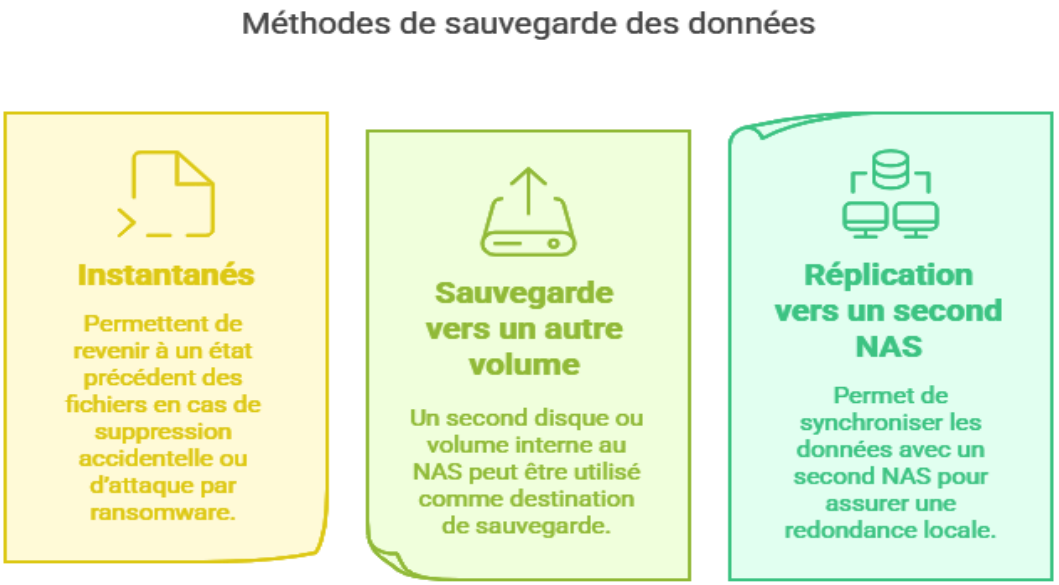
Un NAS est une solution efficace pour stocker et partager des données, mais il est essentiel de mettre en place des mécanismes de sauvegarde et de redondance afin de prévenir la perte de données en cas de panne matérielle, d'attaque informatique ou d'erreur humaine. Cette section explore les différentes stratégies permettant d'assurer la continuité et la sécurité des données stockées sur un NAS.

a. Stratégies de sauvegarde intégrées

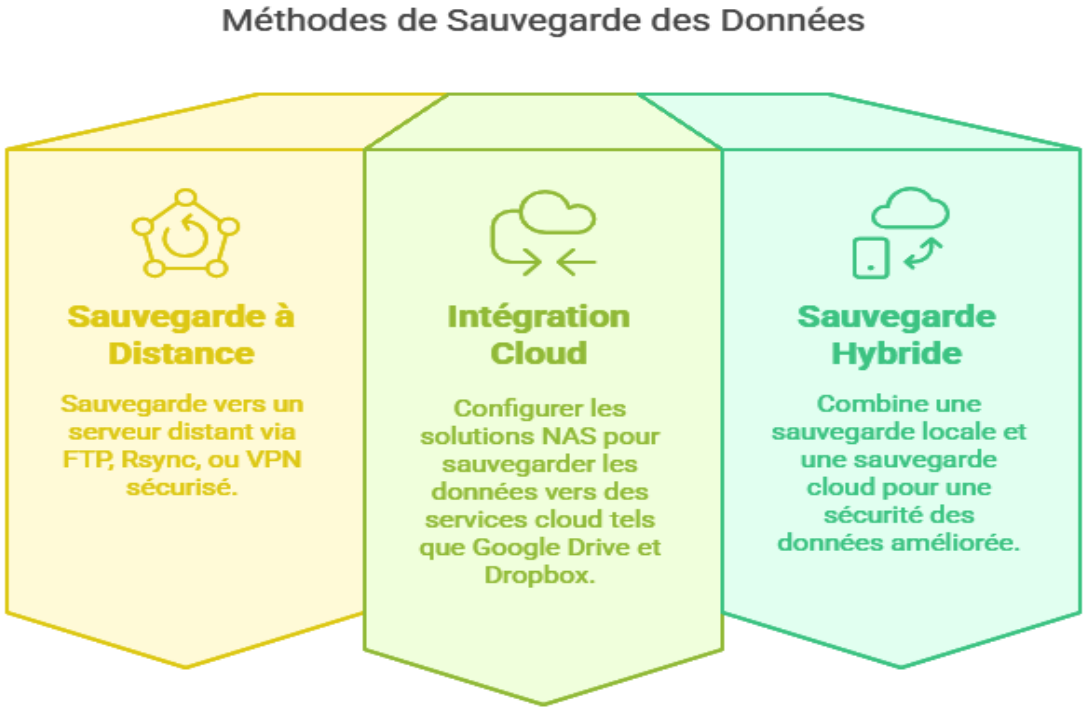
Une bonne stratégie de sauvegarde repose sur le principe du 3-2-1 :



Sauvegarde locale :

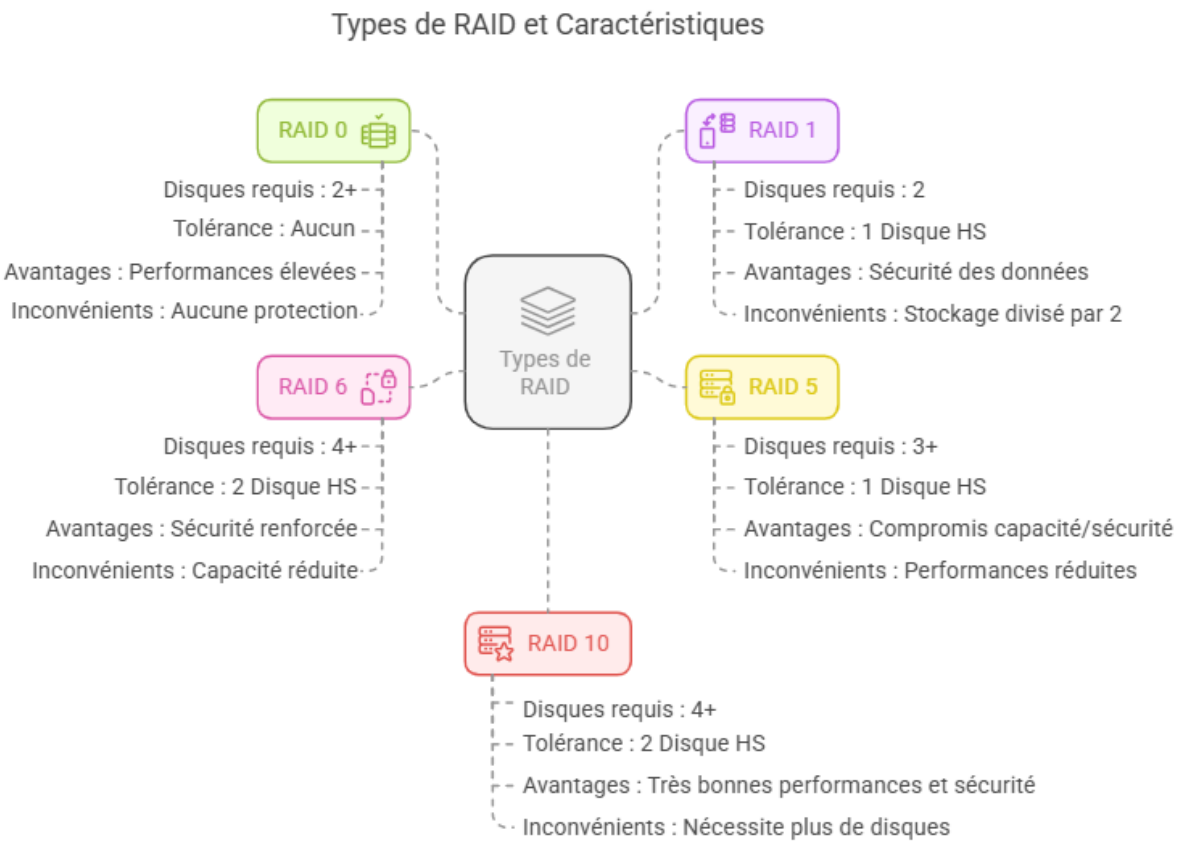


Sauvegarde distante et cloud :



b. Systèmes de redondance : RAID et snapshots

Le RAID (Redundant Array of Independent Disks) est une technologie qui assure une redondance des données sur plusieurs disques afin d'éviter la perte en cas de panne matérielle.

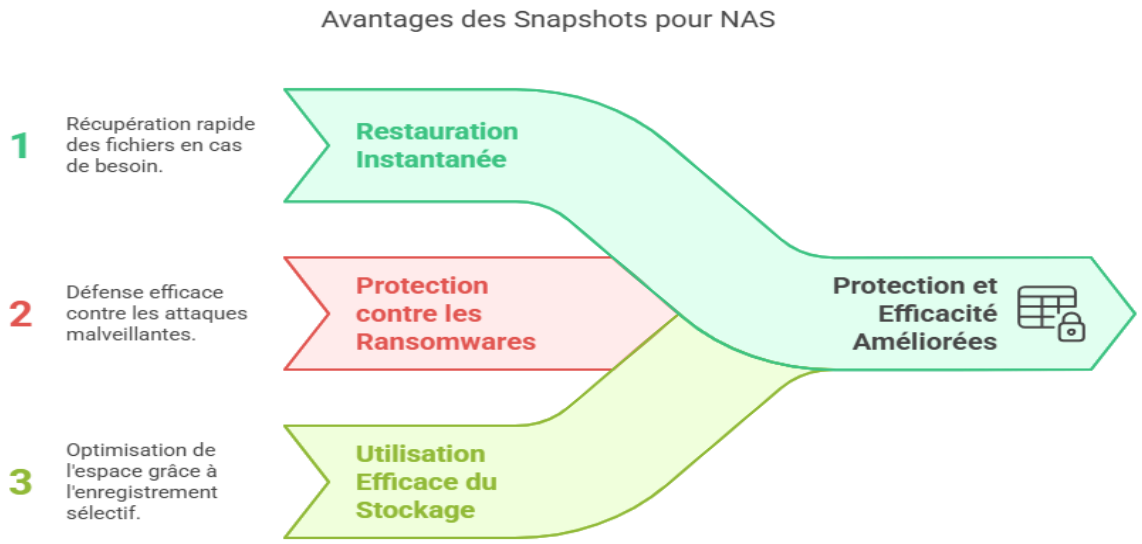


Exemple : Un NAS en RAID 1 avec deux disques permet de dupliquer les données en temps réel. Si un disque tombe en panne, l'autre prend immédiatement le relais.

<u>Snapshots et versioning</u>

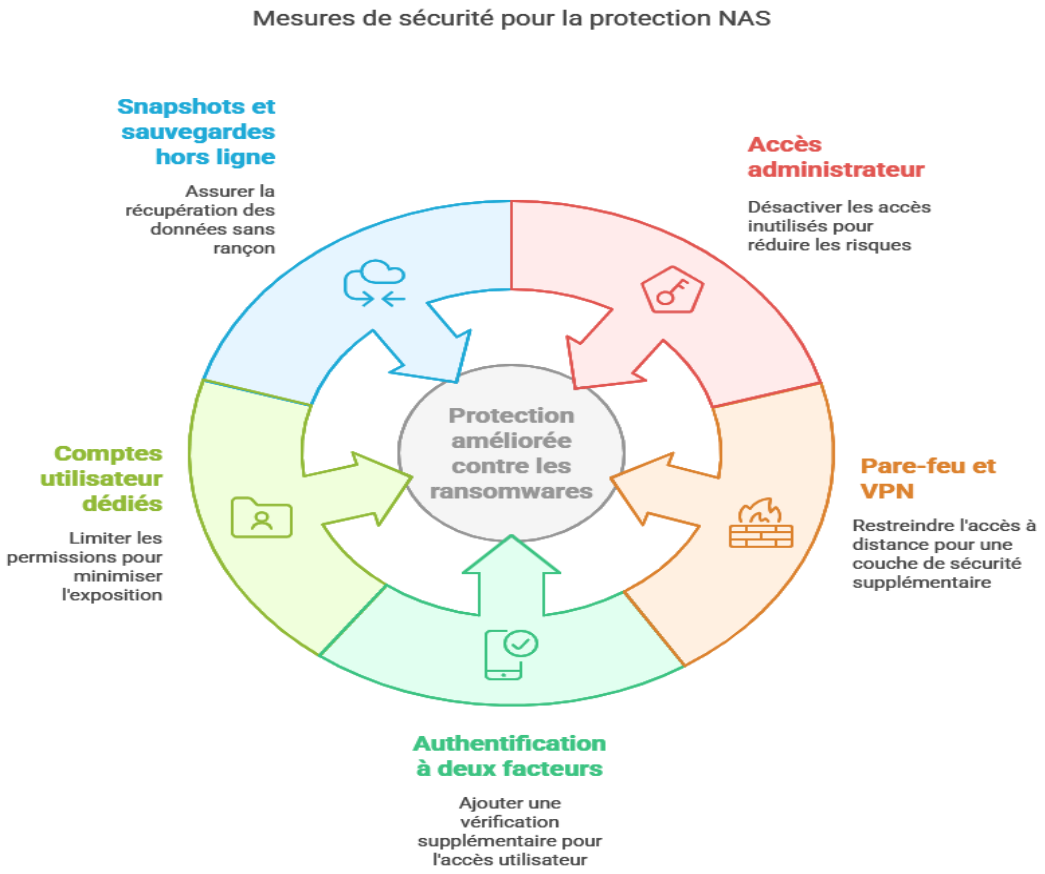
Les snapshots sont des copies instantanées des fichiers à un moment donné. En cas de suppression accidentelle ou d'attaque ransomware, les fichiers peuvent être restaurés rapidement sans perte majeure.

Avantages des snapshots :

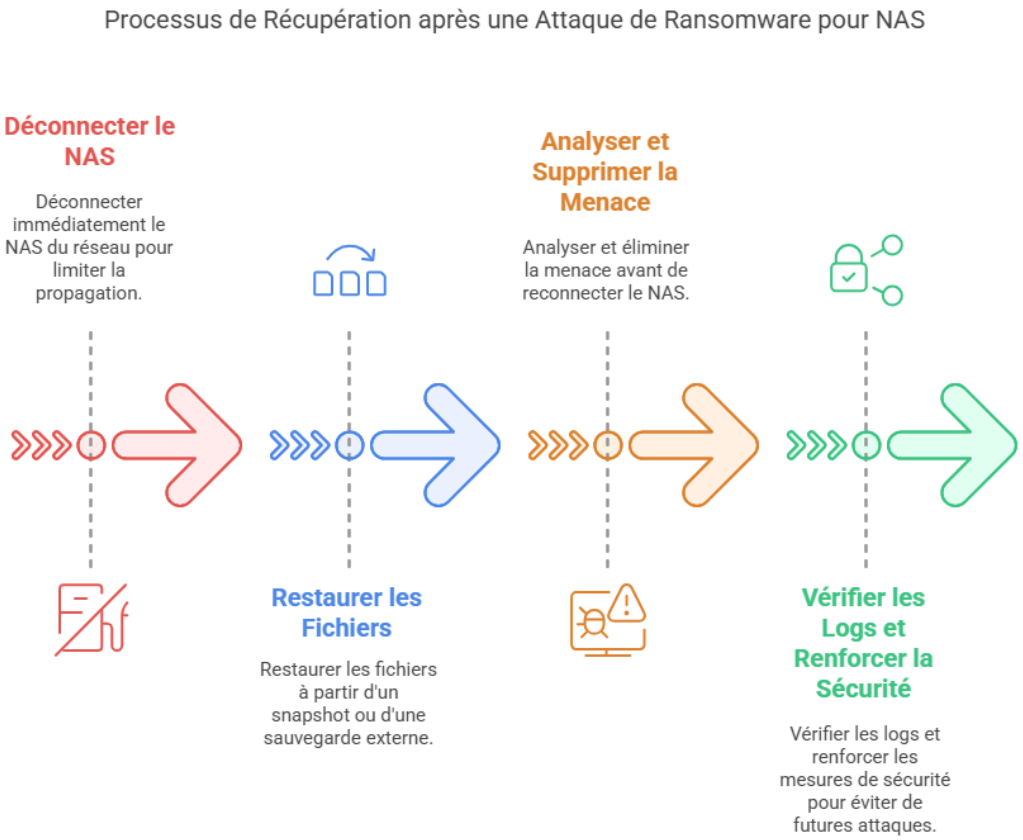


c. Protection contre les ransomwares et récupération après incident

Les ransomwares sont des logiciels malveillants qui chiffrent les fichiers et exigent une rançon pour les débloquer. Un NAS mal sécurisé peut être une cible de choix pour ce type d'attaque.



Que faire en cas d’attaque ?



Webographie

Synology – Documentation officielle

QNAP – Support technique et guides utilisateur

TrueNAS (anciennement FreeNAS) – Documentation et forums

Guide Synology sur la sécurité des NAS

Site officiel des CVE (Common Vulnerabilities and Exposures)

OWASP (Open Web Application Security Project)

RAID Explained – How to Choose the Right RAID for Your NAS

Guide Synology sur la sauvegarde et la restauration des données

Backup Strategy 3-2-1 Explained

Reddit – r/DataHoarder

Forum officiel TrueNAS

Documentation OpenMediaVault (alternative NAS open-source)