Service Informatique

ASSURMER

2022

Fonctionnalités principales d'un NAS

Date	Rédacteur	Validateur
4 octobre 2022	LE DOHER Loïc ZAMBON Ronan POISSONNIER Mattéo KENNEDY John-Killian	

Table des matières

Définition du NAS

Le NAS est un serveur intelligent de stockage de données connecté au réseau. Composé d'un boîtier, d'un ou plusieurs processeurs, de mémoire RAM et de plusieurs disques durs de grande capacité, il centralise les données pour les mettre à disposition des utilisateurs de façon sécurisée, où qu'ils se trouvent. Très répandus en entreprise, les NAS sont également très largement adoptés par les particuliers qui détiennent des fichiers toujours plus lourds (photos, vidéos, films, séries, etc.).

Fonctionnalités d'un NAS

- Centraliser et stocker des données
- Sauvegarder des données
- Sauvegarder des postes de travail
- Partager des fichiers
- Collaborer à plusieurs sur des documents
- Synchroniser des fichiers entre ses appareils
- Faire de la surveillance vidéo
- Créer un media center
- Stocker & partager des vidéos, photos
- Héberger des sites et des adresses email
- Télécharger des fichiers torrent

Chiffrement et sécurité des données

Le chiffrement est l'un des moyens les plus efficaces pour protéger les données stockées sur des NAS. Il permet de rendre les données illisibles pour quiconque ne dispose pas de la clé de déchiffrement. De plus, le chiffrement fait partie de la mise en conformité RGPD.

1) <u>Chiffrez ce qui est nécessaire :</u>

   Ne chiffrez que les données qui ont besoin d'être protégées. Classez les données par ordre de priorité en fonction de leurs exigences en matière de confidentialité. Pour vous aider à les hiérarchiser, imaginez les répercussions que pourrait avoir la compromission de chaque type de données.

2) Chiffrez les données « au repos » :

Les données « au repos » font référence aux données stockées sur le NAS, par opposition aux données en cours de transmission entre deux appareils. Chiffrer ce qui est stocké sur les disques du NAS évite de devoir se soucier qu'un pirate parvienne à contourner les restrictions d'accès ou que quelqu'un dérobe le NAS lui-même.

3) Utilisation de protocole de transfert chiffrés :

Les données en transit sur les liens réseau sont exposées à des menaces comme l'écoute clandestine et le détournement des paquets TCP/IP. Si ces données ne sont pas chiffrées par le protocole de transmission, des cybercriminels peuvent y accéder avec plus de facilité. Le chiffrement des données lors de leur transmission est généralement recommandé lorsque ces données sont communiquées au-delà du pare-feu qui protège le réseau de l'entreprise. Chiffrer des données en mouvement revient à utiliser les bons protocoles au niveau de la couche de transport.

4) Utilisation de réseaux virtuel privés

Un VPN fournit une connexion chiffrée aux accès qui transitent par Internet. Il dissimule les détails de la session et ajoute une couche supplémentaire de protection pour les systèmes clients qui communiquent à distance avec les NAS. Comme un VPN déguise l'identité et l'activité en ligne d'un utilisateur, il est plus difficile pour les pirates de voler des données ou de compromettre des systèmes – ou même de déduire le contenu d'une session ou le type de données.