Dylan CHAU
Axel BAUGÉ

2A-SISR

Comparaison de TrueNAS/XPEnology et veille informationnelle

Date de création : 22/11/2023
Version : 2.0
Pour validation : DSI
A destination : DSI
Mode de diffusion : Intranet
Nombre de pages : 14

Métadonnées

Diffusion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions		
Auteur	Version	Objet de la version et liste des modifications
Dylan Chau	1.0	Initialisation du document
Axel Baugé	1.5	Ajout de la veille et CVE
Dylan Chau	2.0	Finalisation

Validation			
Rédacteur		Validateur	
Nom	Date	Nom	Date
Dylan Chau	22/11/2023	DSI	20/12/2023
Date d'application : 20/12/2023			

Table des matières

I. Comparaison de TrueNAS et XPEnology

1. Présentation

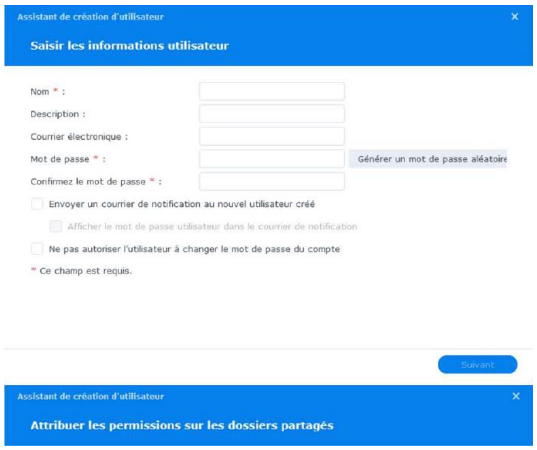
TrueNAS, anciennement connu sous le nom de FreeNAS, se divise en deux versions : TrueNAS Core et TrueNAS Scale. TrueNAS Core repose sur le système Unix FreeBSD, tandis que TrueNAS Scale fonctionne sur la distribution Linux Debian. TrueNAS Scale offre davantage de fonctionnalités, telles que la création de machines virtuelles directement sur le NAS et des conteneurs Docker, similaires à ce que propose XPenology. Cependant, TrueNAS Scale est basé sur le système de fichiers ZFS, ce qui le rend plus gourmand en ressources par rapport à TrueNAS Core.

XPEnology est un script de démarrage basé sur Linux permettant d'émuler un NAS Synology sur n'importe quelle configuration. XPEnology est open source et en développement continu, donnant la possibilité de l'installer sur du matériel x86. Grâce à la mise en open-source du code source de Synology (sous licence GNU), l'équipe XPEnology a récupéré et modifié le noyau DSM, pour fournir un "bootloader" (ou un "chargeur de système") au format ISO, appelé "XPEnoboot. Il permet alors d'installer l'OS Synology DiskStation Manager (DSM), reconnu pour son ergonomie et ses fonctionnalités.

2. La gestion des utilisateurs

TrueNAS propose une interface plus étendue pour la création d'utilisateurs, tout comme XPEnology. Il offre également la possibilité de gérer individuellement chaque personne sur le NAS. De plus, TrueNAS permet la gestion des accès SSH pour les utilisateurs sur le serveur, ainsi que l'utilisation de comptes Microsoft pour une connexion directe à l'Active Directory.

XPEnology permet de créer des utilisateurs avec des options similaires à TrueNAS. Une option intéressante qui n'existe que chez DSM est la possibilité de créer des utilisateurs en masse avec des fichiers CSV. L'import des informations Active Directory est également très simple, de même pour la création d'un dossier par utilisateur.



3. Les systèmes de fichiers et le stockage

TrueNAS et XPEnology utilisent des systèmes de fichiers différents.

TrueNAS s'appuie sur le système ZFS, plus exigeant en performances par rapport à XPEnology, qui avec DSM utilise les systèmes EXT4 ou BTRFS, moins gourmands en ressources.

Le ZFS offre des fonctionnalités telles que la compression directe des fichiers pour économiser de l'espace de stockage, une gestion efficace des gros fichiers et une capacité illimitée et optimisée de gestion des fichiers sans perte de performances grâce aux "nœuds d'index". De plus, le ZFS permet la sauvegarde à chaud des fichiers.

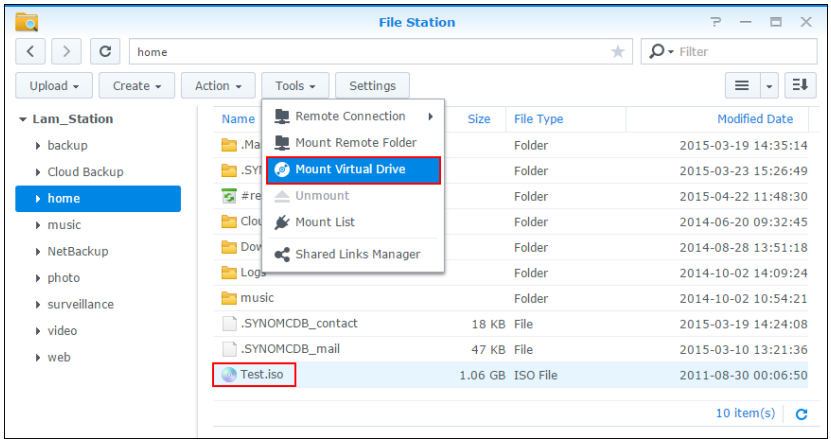
Le EXT4 et BTRFS sont efficaces pour traiter des gros fichiers, utilisent la mémoire RAM pour des performances élevées en lecture et en écriture, avec une optimisation particulière du BTRFS pour les SSD.

Les deux systèmes offrent des fonctionnalités similaires pour la création de volumes de stockage et proposent des options de RAID traditionnelles.

- TrueNAS utilise des termes différents des RAIDs classiques (Stripe pour RAID 0, Mirror pour RAID 1, RAID-Z pour RAID 5, RAID-Z2 pour RAID 6).
- DSM utilise le système RAID SHR et les noms de RAID classiques.

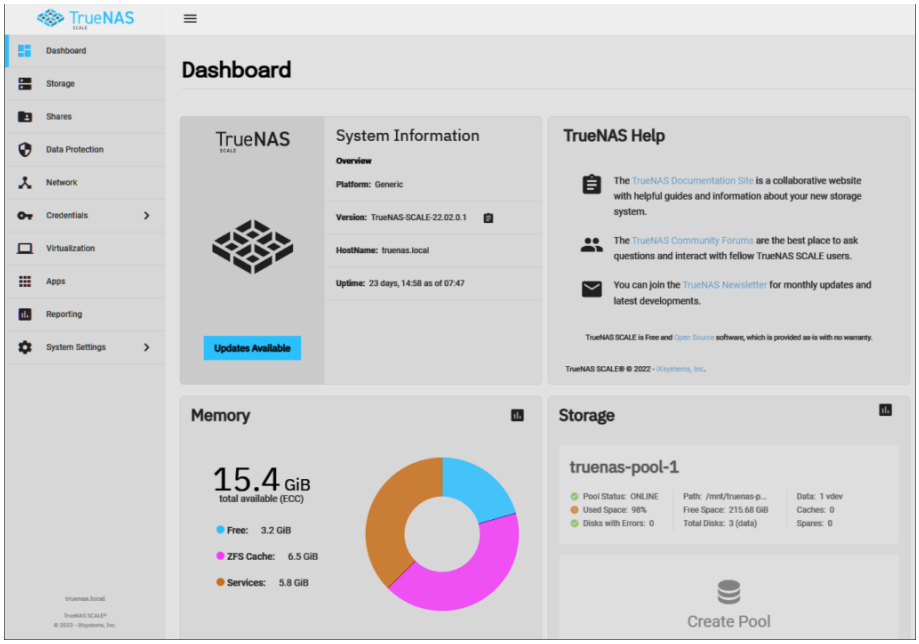
L'interface de gestion du stockage de DSM est plus conviviale que celle de TrueNAS, mais les deux restent tout de même similaires.

TrueNAS permet l'accès aux fichiers en permettant l'accès via les lecteurs réseaux et les protocoles comme SMB. XPEnology permet un accès de la même façon, mais également via son interface web avec File Station et les applications mobiles proposés.



4. L'interface Web

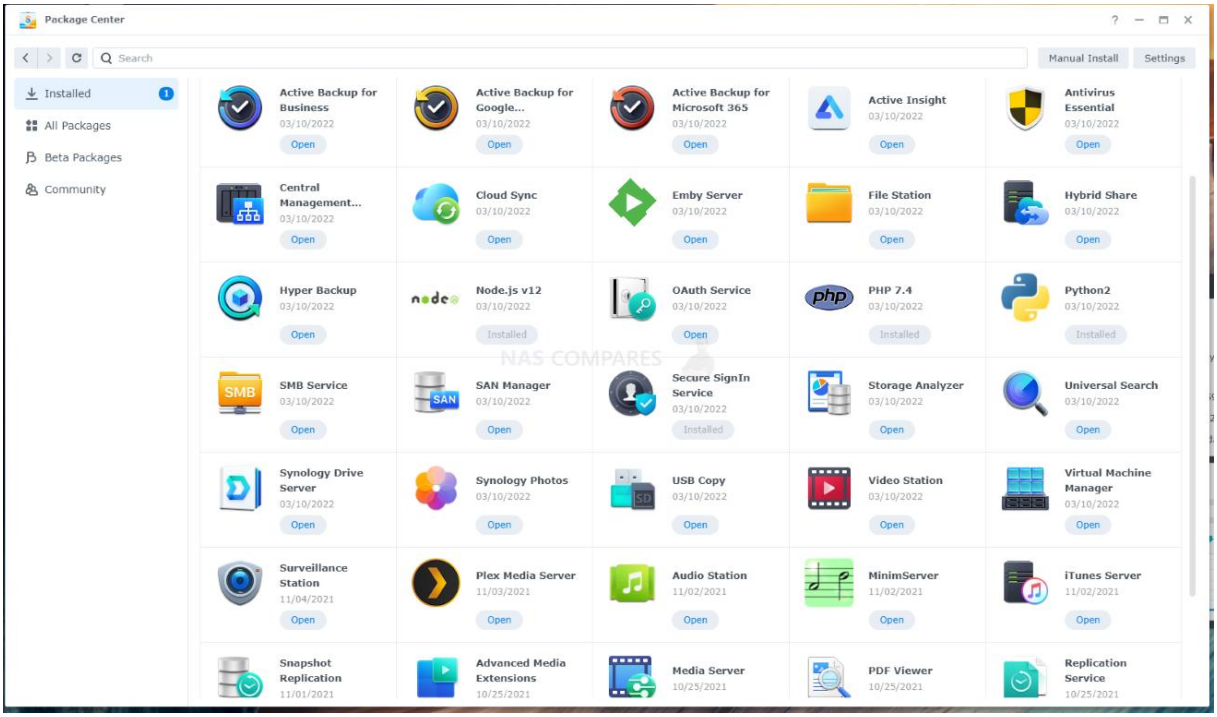
TrueNAS offre un tableau de bord en interface web qui contient une multitude de fonctionnalités et de données statistiques à surveiller. Bien que ce tableau de bord soit complètement adaptable, il peut sembler complexe pour les utilisateurs débutants. Néanmoins, il s'avère très performant pour les administrateurs expérimentés.



XPEnology propose une interface bien plus conviviale avec moins de personnalisation. Le système de bureau et d'applications à lancer rend l'outil plus simple à utiliser pour des utilisateurs débutants.

5. Fonctionnalités supplémentaires

Les 2 solutions proposent l'ajout de plugins ou de paquets gérés soit par l'entreprise ou par la communauté pour avoir des fonctionnalités supplémentaires.



Enfin, les 2 solutions proposent la mise en place d'un serveur VPN, des fonctionnalités d'intégration au domaine Active Directory, et LDAP ainsi que bien d'autres fonctionnalités.

6. Cybersécurité

TrueNAS et XPEnology offrent tous deux des niveaux élevés de sécurité, proposant des fonctionnalités diverses :

- **Chiffrement des données** :
  Les deux plateformes proposent du chiffrement AES 256 bits pour protéger les données stockées. Ils prennent en charge le chiffrement des disques, des volumes et des données réseau pour renforcer la confidentialité.
- **Contrôles d'accès** :
  Les systèmes proposent des mécanismes de contrôle d'accès avancés pour gérer les autorisations des utilisateurs et des groupes, assurant ainsi que seuls les utilisateurs autorisés puissent accéder aux données sensibles.
- **Authentification sécurisée** :
  Divers protocoles d'authentification sécurisée sont pris en charge telle que Kerberos, LDAP, Active Directory, etc, renforçant ainsi la sécurité des accès au système. De plus, l'authentification en deux étapes (2FA) est présente.
- **Protection contre les menaces** :
  Les deux solutions proposent des fonctionnalités de détection et de prévention des intrusions pour détecter les activités suspectes et potentiellement malveillantes comme Security Advisor chez Synology et TrueNAS.
- **Mises à jour et correctifs** :
  Les mises à jour sont régulières pour corriger les vulnérabilités connues et pour intégrer les dernières améliorations de sécurité.
- **Audit et journalisation** :
  Les deux systèmes offrent des fonctionnalités d'audit et de journalisation pour enregistrer les activités et les événements, permettant ainsi aux administrateurs de surveiller et d'analyser les accès et les opérations effectuées.
- **Sauvegardes sécurisées** :
  Des solutions de sauvegarde sécurisées sont proposées pour protéger les données en cas de sinistre ou de perte.

7. Solution retenue

L'usage de DSM étant restreint aux NAS Synology, Synology considère l'utilisation de XPEnology comme étant interdite, et même illégal. Il ne doit être utilisé que pour des tests ou des démonstrations.

De plus, XPEnology étant de l'émulation, si une mise à jour de DSM sort, l'équipe de XPEnology doit travailler pour déployer très rapidement un nouveau bootloader. L'équipe Synology propose très régulièrement des correctifs pour répondre aux failles de sécurité.

De plus, XPEnology ne fonctionne pas sur tous les appareils possibles comparés à TrueNAS et tous les périphériques ne sont pas compatibles.

TrueNAS est une solution open-source très performante et aussi complète que Synology avec de très nombreuses fonctionnalités. De plus, iXsystems propose régulièrement des mises à jour et assure un suivi de la solution. Si le budget nous le permettait, nous aurions pris comme solution le NAS Synology pour la facilité d'utilisation, l'interface conviviale, mais afin de rester dans la légalité, nous avons décidé de mettre en place **TrueNAS** au sein de notre infrastructure.

II. Etat des lieux CVE et veille informationnelle

1. Outils

a) TrueNAS

Le site officiel de TrueNAS offre une plateforme complète dédiée à la gestion des vulnérabilités, accessible via le lien suivant :

https://security.truenas.com/cves/

Cette base de données exhaustive recense l'ensemble des CVE (Common Vulnerabilities and Exposures), fournissant ainsi un historique détaillé des incidents ayant impacté le bon fonctionnement des divers produits TrueNAS.

La plateforme assure un suivi méticuleux des CVE répertoriées, permettant aux utilisateurs de rester informés sur les éventuelles menaces et vulnérabilités associées à TrueNAS CORE Enterprise, SCALE Enterprise, Command, ainsi que les Solutions Matérielles Entreprise. Ce dispositif de surveillance garantit une transparence totale quant à la sécurité des produits TrueNAS.

Par ailleurs, le site propose un mécanisme sophistiqué de signalement de vulnérabilités, permettant à la communauté des utilisateurs et aux experts en sécurité de contribuer à l'amélioration continue de la sécurité des solutions TrueNAS.

b) Synology

Synology propose à l'aide son site officiel une base de données mise à jour régulièrement sur les dernières vulnérabilités des produits Synology :

https://www.synology.com/fr-fr/security/advisory

Cette base de données est rendue public seulement au moment où les correctifs des vulnérabilités sont rendus publics afin de protéger les utilisateurs.

Afin de signaler une vulnérabilité Synology, il suffit de remplir un formulaire à l'aide d'une clé PGP. Cette clé permet de chiffrer vos informations sensibles à l'aide de la clé PGP de sécurité des produits Synology. Afin d'obtenir cette clé, il suffit de l'obtenir auprès d'Open PGP qui est un outil de chiffrement de mail.

c) CVEDetails

CVEDetails est un site offrant une documentation exhaustive sur une CVE, comprenant des informations détaillées sur la vulnérabilité telles que la date de découverte, le contexte et les catégories associées.

https://www.cvedetails.com/

Il présente également des prévisions quant à l'exploitation, exprimées en pourcentage d'utilisation probable de l'exploit.

Le site fournit des scores CVSS (Common Vulnerability Scoring System) pour évaluer la sévérité de la vulnérabilité. De plus, il référence diverses sources détaillant la CVE, offrant ainsi une perspective complète sur la nature de la vulnérabilité.

En outre, le site répertorie les infrastructures susceptibles d'être affectées par la vulnérabilité, offrant ainsi une vision claire de l'impact potentiel sur différentes plates-formes. En résumé, cette ressource centralisée offre une vue détaillée et holistique des aspects techniques et contextuels entourant la CVE en question.

d) CVSS

Le CVSS, est un score qui sert d'indicateur de la gravité de d'une faille, basé sur des critères objectifs et mesurables.

https://www.first.org/cvss/calculator/4.0

Il y a trois métriques permettant de définir cette gravité :

- Les métriques de base. Elles se regroupent en deux catégories, les métriques d'exploitation et les métriques d'impact :
  - Les métriques d'exploitation recouvrent :
    → Le vecteur d'accès (local, réseau local, réseau)
    → La complexité d'accès (basse, moyenne, haute)
    → L'authentification (multiple, simple, inexistante)
  - Les métriques d'impact incluent :
    → La confidentialité
    → L'intégrité
    → La disponibilité
- Les métriques temporelles.
- Les métriques environnementales.

Niveaux	Score
Aucun	0
Bas	0.1 - 3.9
Moyen	4.0 - 6.9
Haut	7.0 - 8.9
Critique	9.0 - 10.0

2. Résultats

a) Dernière CVE en date pour TrueNAS : CVE-2022-0194

Cette vulnérabilité permet à des attaquants distants d'exécuter du code arbitraire sur les installations affectées de Netatalk. L'authentification n'est pas nécessaire pour exploiter cette vulnérabilité. Le défaut spécifique existe dans la fonction ad_addcomment. Le problème résulte de l'absence de validation appropriée de la longueur des données fournies par l'utilisateur avant de les copier dans une mémoire tampon basée sur une pile de longueur fixe. Un attaquant peut exploiter cette vulnérabilité pour exécuter du code dans le contexte de root.

Netatalk est un logiciel open-source qui implémente le protocole Apple Filing Protocol (AFP) pour les systèmes Unix et Unix-like, permettant ainsi le partage de fichiers entre ordinateurs Macintosh et d'autres systèmes compatibles AFP sur un réseau.

Une mise à jour vers la version 3.1.13 de Netatalk a permis de corriger la faille.

Score CVSS :

Base score	9,8	Critique
Exploitabilité score	3,9	Bas
Score d'impact	5,9	Moyen

b) Dernière CVE en date pour Synology : CVE-2023-2729

Une vulnérabilité permet à des attaquants distants d'obtenir les informations d'identification de l'utilisateur via une version sensible de Synology DiskStation Manager (DSM).

Afin de corriger la vulnérabilité, une mise à jour pour DSM a été déployé pour passer en version 7.2-64561.

Score CVSS :

Base score	7.5	Haut
Exploitabilité score	3,9	Bas
Score d'impact	3,6	Bas