TrueNAS

Qu'est-ce que TrueNAS ?

TrueNAS Scale est un système d'exploitation de stockage en réseau (**NAS**) open source conçu pour fournir des capacités de stockage de niveau entreprise. Il est le successeur du système d'exploitation FreeNAS et est basé sur Debian Linux (la version Scale) et sur FreeBSD (la version Core). TrueNAS Scale est conçu pour fournir une solution de stockage **évolutive** et facile à utiliser qui peut être personnalisée pour répondre aux besoins d'un large éventail d'organisations.

TrueNAS comprend un certain nombre de fonctionnalités qui en font un choix attrayant pour les organisations qui ont besoin d'un stockage fiable et performant mais aussi pour une utilisation de type HomeLab*.

Certaines de ces fonctionnalités incluent :

- *Système de fichiers ZFS : TrueNAS Scale utilise le système de fichiers ZFS, qui fournit des fonctionnalités avancées de protection et de gestion des données, notamment le RAID intégré, la somme de contrôle et la création d'instantanés.*
- *GUI facile à utiliser (user-friendly) : TrueNAS Scale comprend une interface Web facile à utiliser et donne accès à toutes les fonctionnalités de gestion du stockage.*
- *Évolutivité : TrueNAS Scale est conçu pour évoluer des environnements de petits bureaux aux grands centres de données, avec prise en charge du clustering et de la réplication.*
- *Fonctionnalités de classe entreprise : TrueNAS Scale comprend une gamme de fonctionnalités de classe entreprise, telles que la prise en charge d'Active Directory et et LDAP, le chiffrement et la réplication d'instantanés.*
- *Open-Source : TrueNAS Scale est un projet open-source, ce qui signifie qu'il peut être librement utilisé, modifié et distribué par n'importe qui.*

Pourquoi avons-nous besoin de tout cela ?

Parce que est un système d'exploitation de stockage puissant et flexible conçu pour fournir des capacités de stockage de classe entreprise. C'est un bon choix pour les organisations qui ont besoin d'un stockage fiable et évolutif avec des capacités avancées de protection et de gestion des données. De plus, le fait qu'il soit open source en fait une option attrayante pour les organisations qui apprécient la flexibilité et la rentabilité.

SOMMAIRE

Dans les pages suivantes, la procédure étape par étape pour configurer les fonctions décrites ci dessus sera expliquée avec une explication d'accompagnement

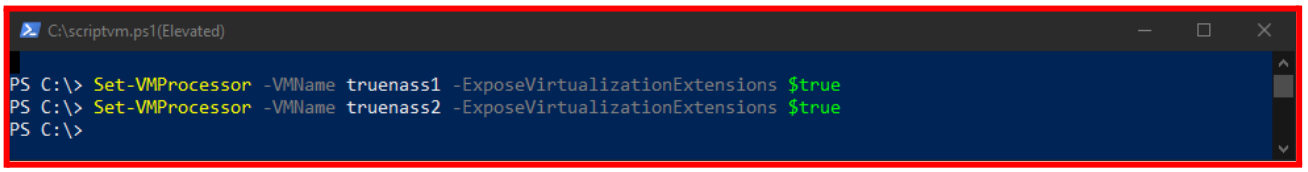
Dans ce tutoriel, nous utiliserons un systeme de test basée sur Proxmox:
• Une machine physique agirà come hyperviseur (Proxmox 7.3-6) (Thanks to Christophe)
• Une autre machine agira en tant que «VM» → TrueNAS CORE
• Une autre machine agira en tant que «VM» → TrueNAS SCALE

Toutes les captures d'écran de ce didacticiel seront disponibles sur ce lien sur Google Drive pour permettre la visualisation en HD de toutes les captures d'écran.

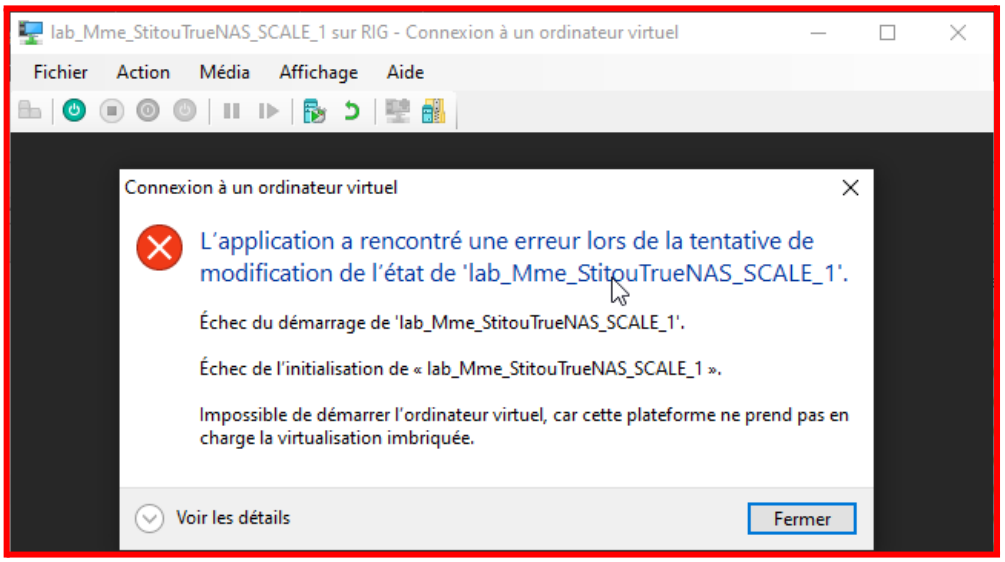
Raccourci	Explication
O.S.	Operating System, System d'exploitation
Machine	Ordinateur physique
AD, AD DS	Services de domaine Active Directory
DNS	Domain name system
Gateway	Passerelle
IP	Internet Protocol
Win srv	windows server
SMB	SAMBA
ZFS	système de fichiers avec des capacités de gestion de volume

Tests sur HyperV - Nested virtualization (virtualisation imbriquée)

La virtualisation imbriquée est une fonctionnalité qui permet d'exécuter Hyper-V à l'intérieur d'une machine virtuelle (VM) Hyper-V.
Malheureusement, la virtualisation de TrueNAS sur HyperV n'est pas entièrement fonctionnelle dans ce sens : Truenas fonctionnera, mais la fonctionnalité de conteneur sur TrueNAS Scale ne sera pas disponible. C'est parce que **KVM*** (Kernel-based Virtual Machine) n'est pas compatible avec HyperV.



En fait, essayez ces commandes comme suggéré par la communauté Microsoft.
https://learn.microsoft.com/fr-fr/virtualization/hyper-v-on-windows/user-guide/nested-virtualization
la vm avec TrueNAS retourne une erreur de ce type à chaque démarrage.



***KVM** : est une solution de virtualisation complète pour Linux sur du matériel x86 contenant des extensions de virtualisation (Intel VT ou AMD-V). Il se compose d'un module de noyau chargeable, kvm.ko, qui fournit l'infrastructure de virtualisation de base et d'un module spécifique au processeur, kvm-intel.ko ou kvm-amd.ko.

TrueNAS CORE *inclut la prise en charge de* **jails** (prisons en français) qui sont une fonctionnalité de qui vous permet de créer des environnements virtuels légers, ou "jails", au sein du système d'exploitation. Les jails offrent un moyen sécurisé d'exécuter des applications et des services isolés du reste du système, ce qui contribue à améliorer la sécurité et la stabilité.

Voici quelques-unes des fonctionnalités clés des prisons dans TrueNAS Core :

- **Isolation** : les prisons fournissent un environnement sécurisé et isolé dans lequel exécuter des applications et des services. Cela signifie que si une application ou un service dans une prison tombe en panne ou est compromis, cela n'affectera pas le reste du système.

- **Contrôle des ressources** : les jails vous permettent de définir des limites de ressources pour les applications et les services qui y sont exécutés. Cela garantit qu'ils ne consomment pas trop de CPU, de mémoire ou d'espace disque, ce qui peut aider à prévenir les problèmes de performances et à assurer la stabilité du système.

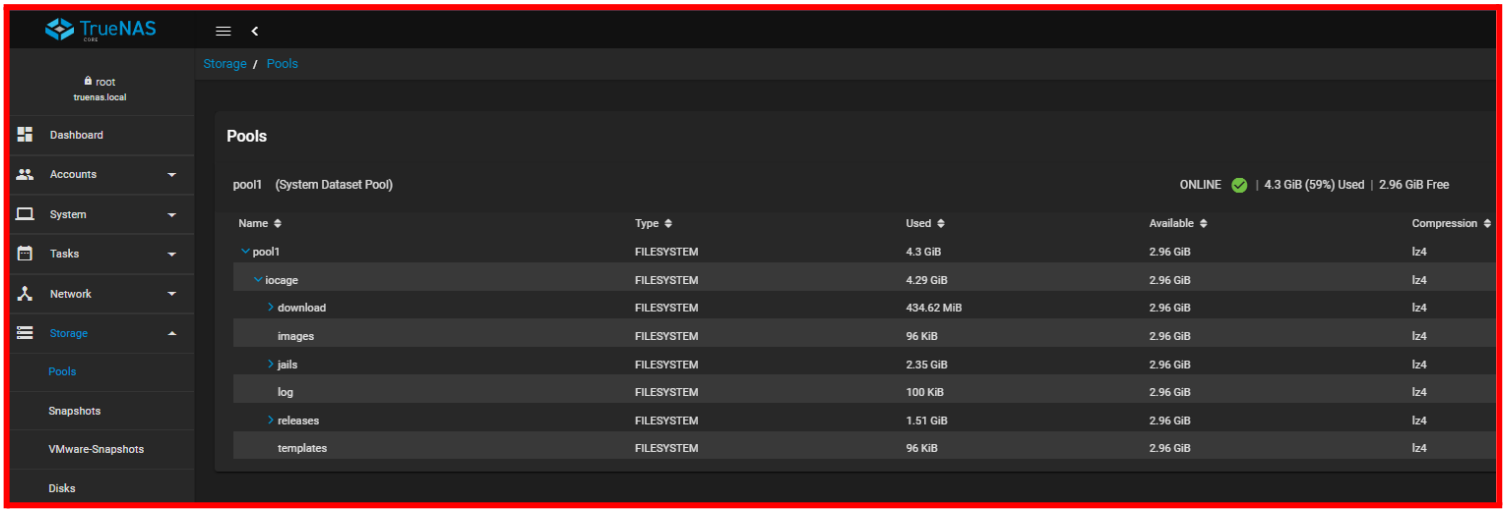
- **Portabilité** : les jails sont hautement portables et peuvent être facilement déplacés entre les systèmes ou sauvegardés à des fins de reprise après sinistre.

- **Gestion facile** : les prisons peuvent être facilement gérées via l'interface Web TrueNAS ou la ligne de commande. Cela vous permet de créer, modifier et supprimer des prisons selon vos besoins.

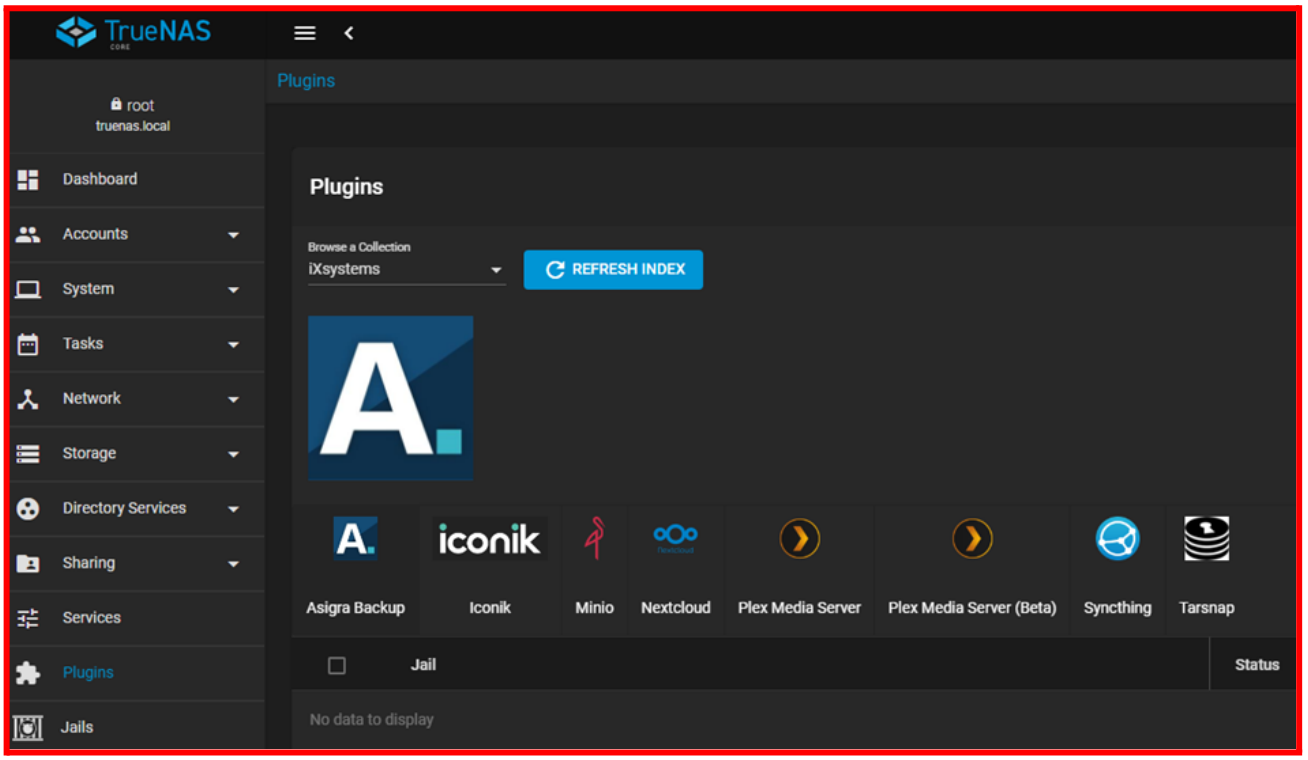
- **Compatibilité** : les jails sont compatibles avec une large gamme de logiciels et d'applications, ce qui en fait une solution flexible pour exécuter différents types de services et d'applications.

Dans l'ensemble, les jails sont une fonctionnalité puissante de TrueNAS Core qui offre un moyen sûr et flexible d'exécuter des applications et des services dans un environnement virtuel léger. Que vous utilisiez un serveur Web, une base de données ou un autre type d'application, les jails peuvent aider à améliorer la sécurité et la stabilité tout en offrant une gestion et une portabilité faciles.

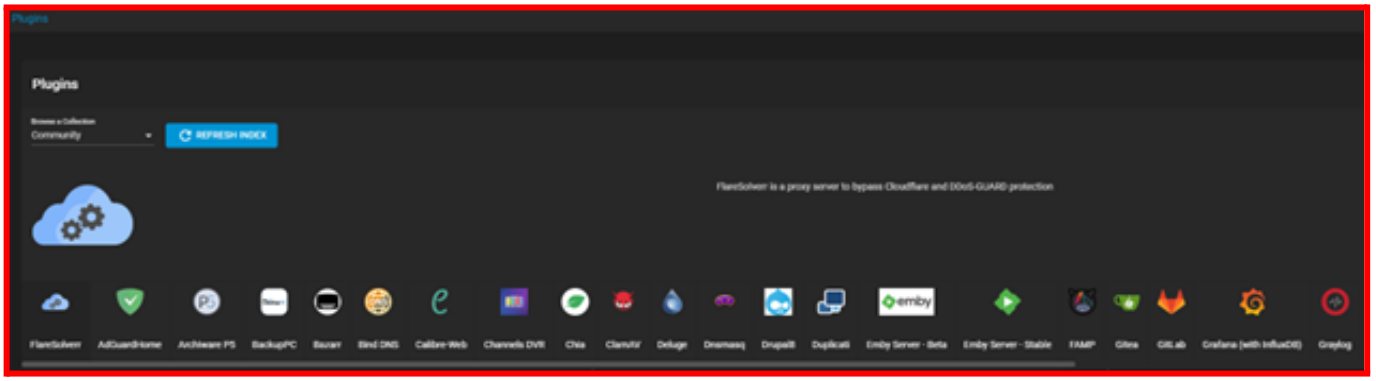
Tout d'abord il faut créer un pool dans storage pour permettre d'avoir un espace pour l'installation de jails.



Puis dans plugins nous avons quelques applications par default.

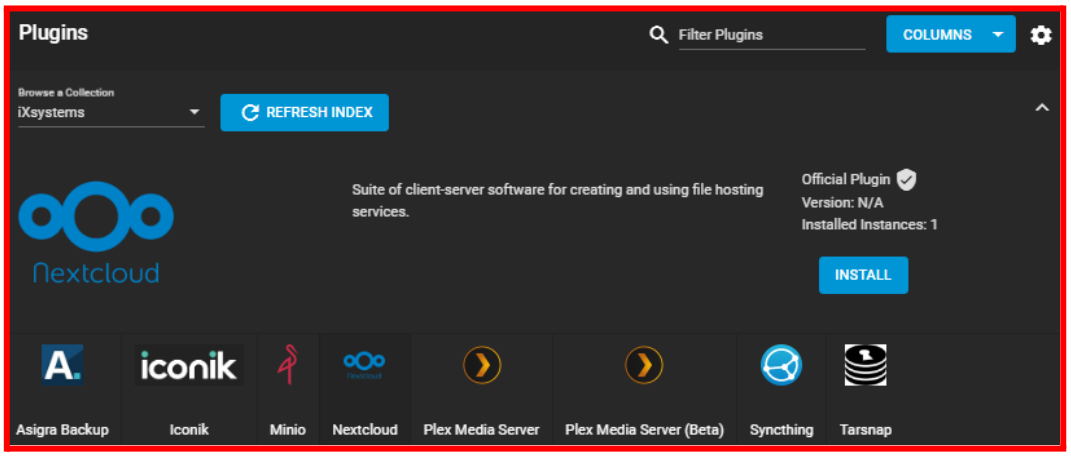


Dans "Browse a Collection", on peut choisir "Community" et avoir beaucoup plus de choix.

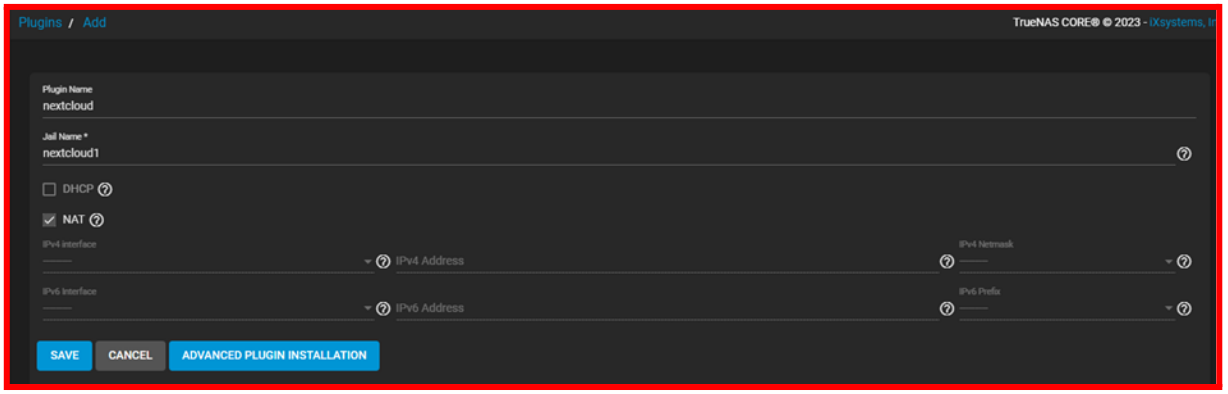


Nextcloud est un logiciel gratuit créé en tant que spin-off du populaire logiciel d'hébergement de fichiers open source ownCloud. Il permet d'avoir son propre cloud hébergé chez nous directement.

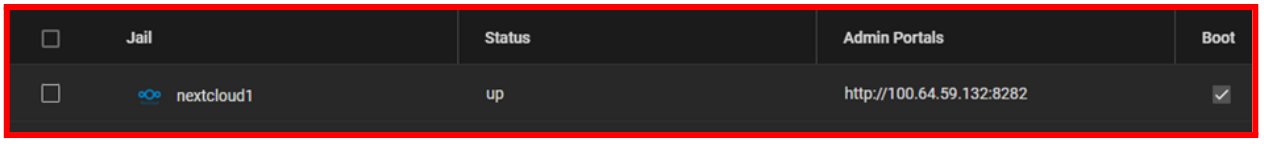
Exemple d'installation pour NextCloud sur TrueNas Core.



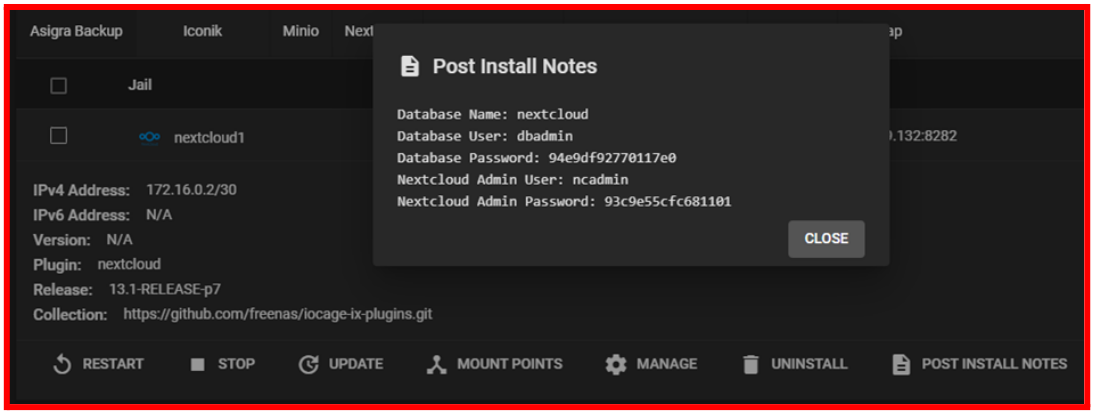
Cliquez sur "Install", puis choisissez un nom pour la Jails et cliquez sur "Save". Dans notre cas on peut laisser le NAT par défaut, nextcloud aura donc comme @IP la même que notre TrueNas.



L'installation prend plusieurs minutes, une fois installé l'@IP et le port du Nextcloud est affiché.



On peut récupérer les credentials dans "Post Install Notes".



TrueNAS SCALE *inclut la prise en charge de* ***Kubernetes*** *(**K8s**), qui est une plate-forme open source d'orchestration de conteneurs. Grâce à cette prise en charge, TrueNAS SCALE peut exécuter des applications conteneurisées à l'aide du moteur K8s. Cela permet aux utilisateurs de déployer, gérer et faire évoluer facilement des applications conteneurisées, sans avoir à se soucier de l'infrastructure sous-jacente.*

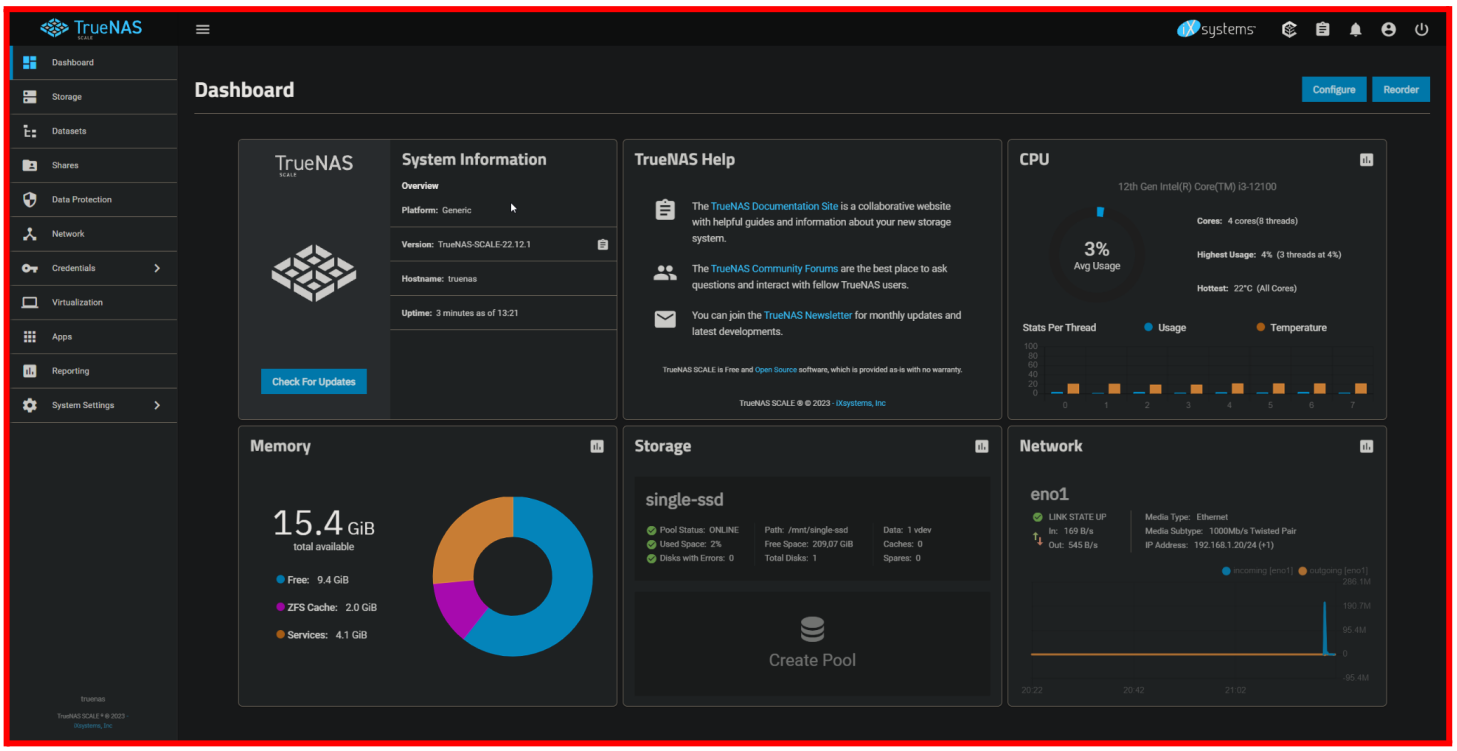
*L'un des principaux avantages de l'utilisation de TrueNAS SCALE avec K8s est la possibilité d'exécuter des applications conteneurisées en mode **HA** et tolérante aux pannes. K8s fournit des fonctionnalités telles que la mise à l'échelle automatique, les mises à jour progressives et l'auto-réparation, qui garantissent que les applications sont toujours disponibles et fonctionnent correctement.*

TrueNAS SCALE comprend également un certain nombre de fonctionnalités spécialement conçues pour prendre en charge les applications conteneurisées. Par exemple, il inclut la prise en charge du stockage persistant, qui permet aux conteneurs de stocker des données même lorsqu'ils sont déplacés entre des hôtes. Ceci est important pour les applications qui nécessitent la persistance des données, telles que les bases de données.

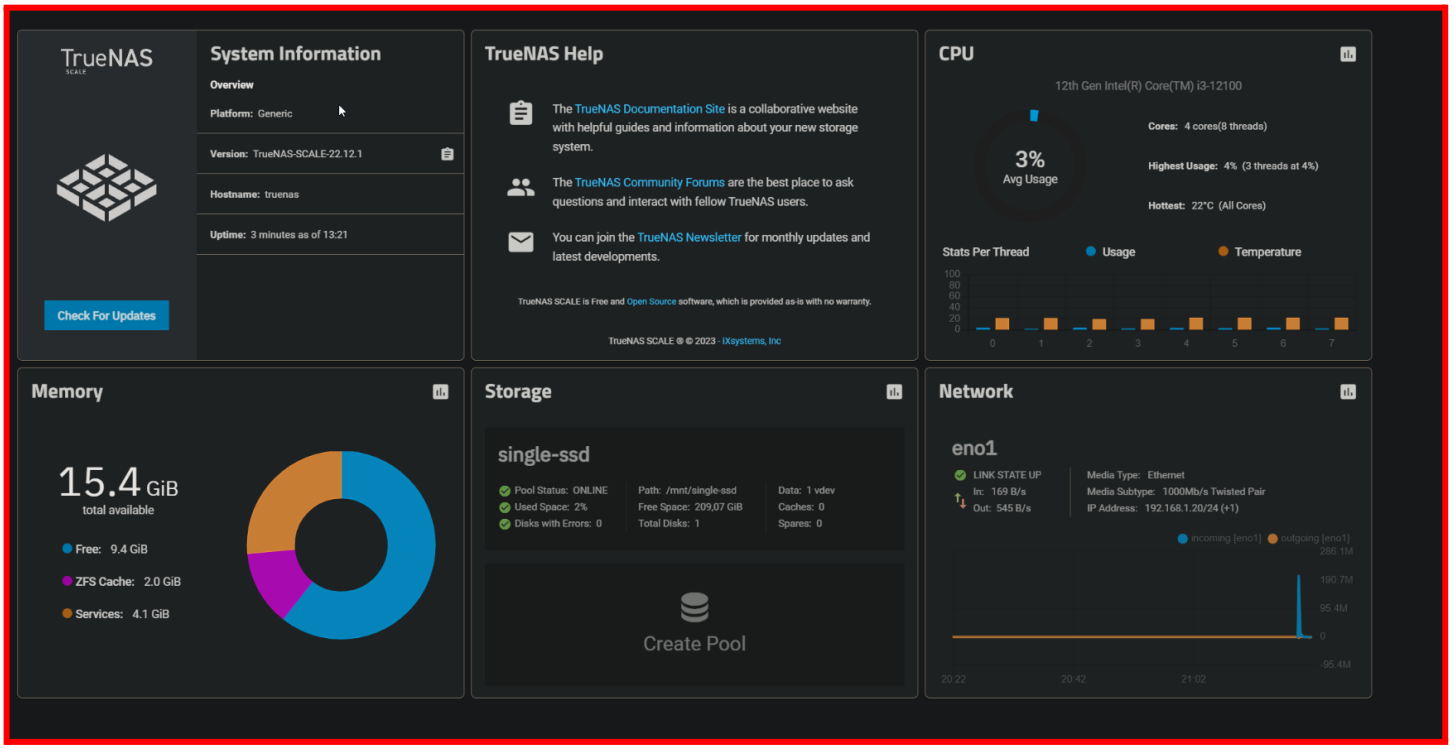
De plus, TrueNAS SCALE inclut la prise en charge de la mise en réseau des conteneurs, qui permet aux conteneurs de communiquer entre eux et avec le monde extérieur. Il inclut également la prise en charge de la sécurité des conteneurs, qui garantit que les conteneurs sont isolés les uns des autres et du système hôte.

*Dans l'ensemble, TrueNAS SCALE avec **K8s** fournit une plate-forme puissante et flexible pour le déploiement et la gestion d'applications conteneurisées. Que vous exécutiez un déploiement à petite échelle ou un environnement d'entreprise à grande échelle, TrueNAS SCALE possède les fonctionnalités et les capacités dont vous avez besoin pour faire le travail.*

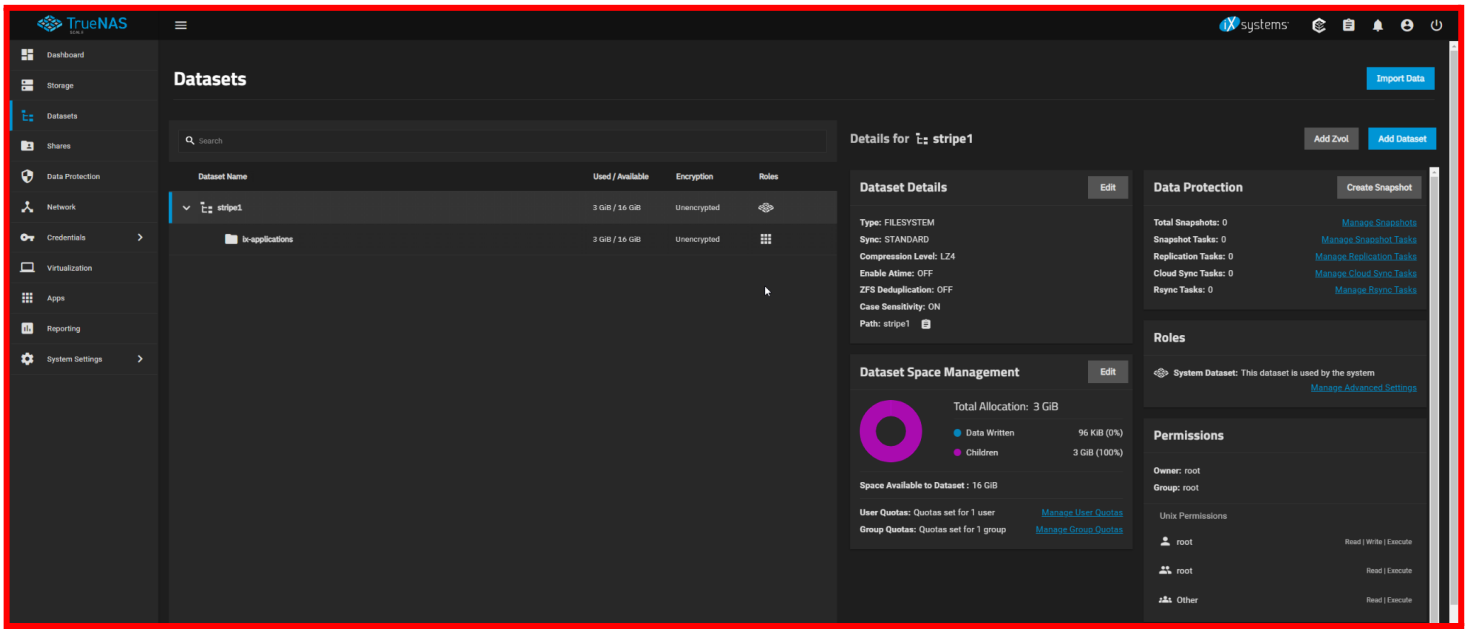
Quelques captures d'écran de l'interface principale concernant TrueNAS



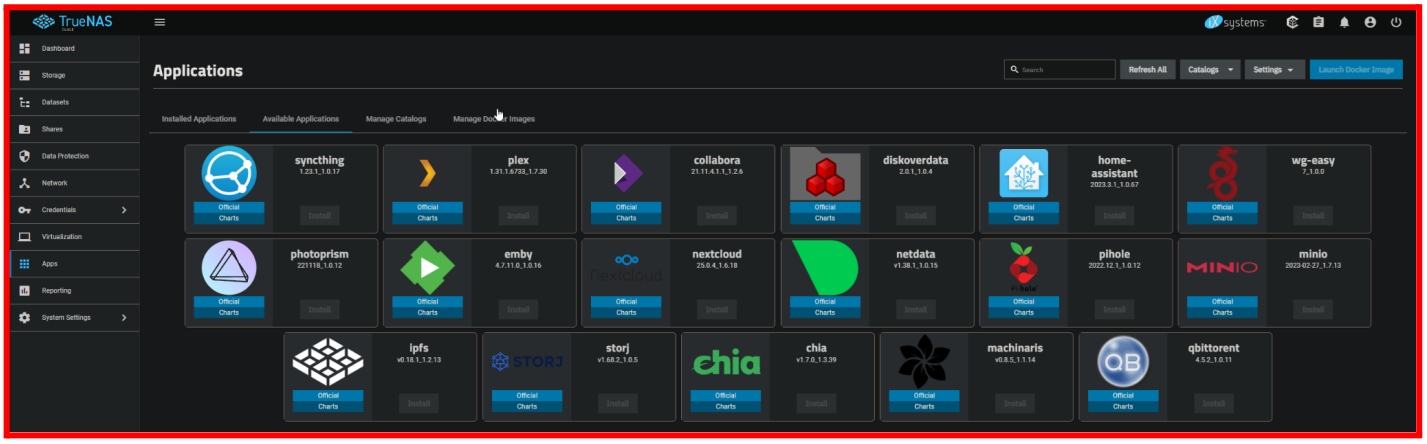
Le graphique relatif à la température et à l'utilisation des différents cœurs CPU est très agréable. A été implémenté dans les dernières versions.



Tout d'abord sur TrueNAS Scale (mais aussi sur la version CORE de la même manière) il vous faudra créer un DataSet. Dans notre cas il a été décidé de créer un raid1 sur Proxmox de deux disques virtuels de 20gb qui suffiront à installer à la fois les jails et les containers.



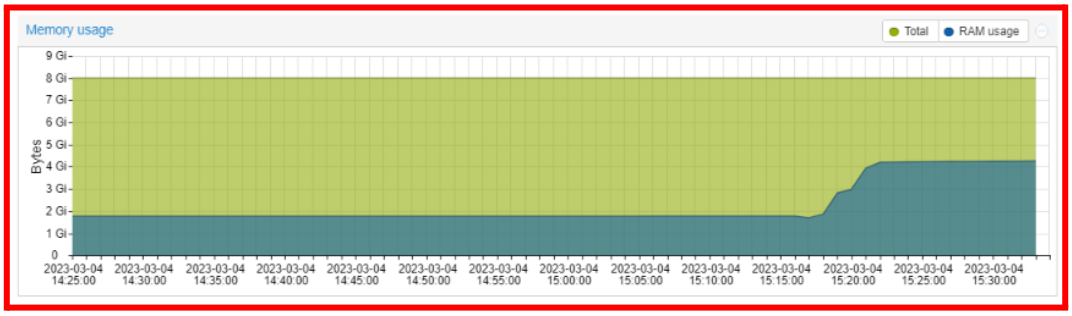
À la base, nous n'aurons que quelques applications disponibles avec les référentiels par défaut (catalogue). Mais il existe des référentiels fiables que nous pouvons ajouter pour allonger la liste.



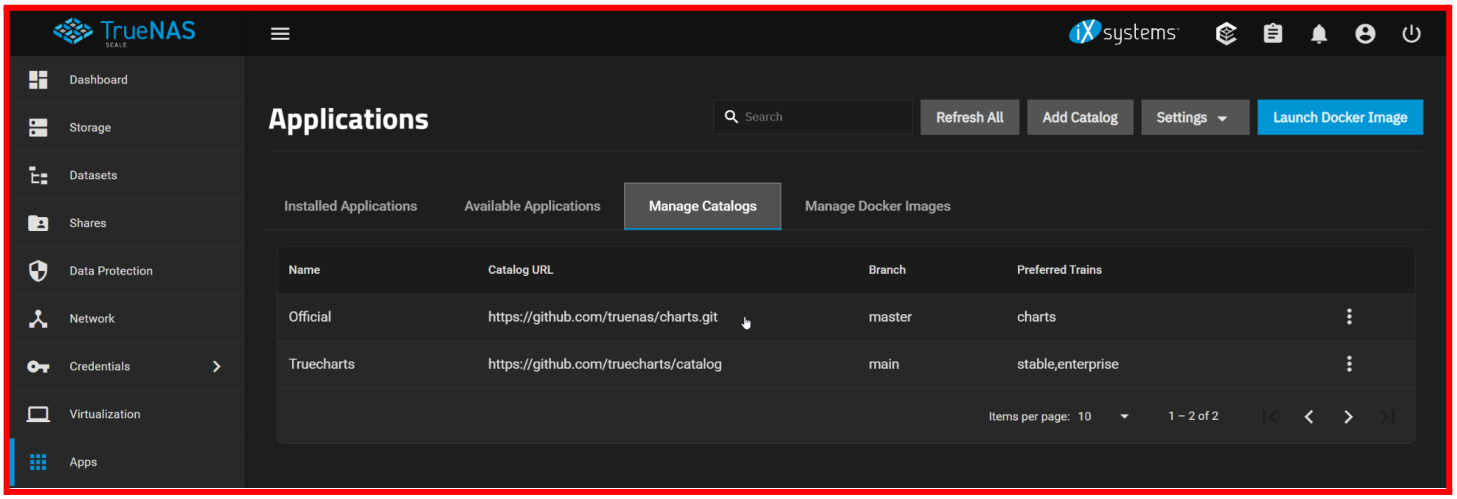
À la base, nous n'aurons que quelques applications disponibles avec les référentiels par défaut (catalogue). Mais il existe des référentiels fiables que nous pouvons ajouter pour allonger la liste. Il sera alors possible d'ajouter la liste TrueCharts à notre TrueNAS.

A partir de ce lien, il sera donc possible d'avoir toutes les informations pour ajouter les référentiels mentionnés ci-dessus. https://truecharts.org/manual/guides/Adding-TrueCharts/

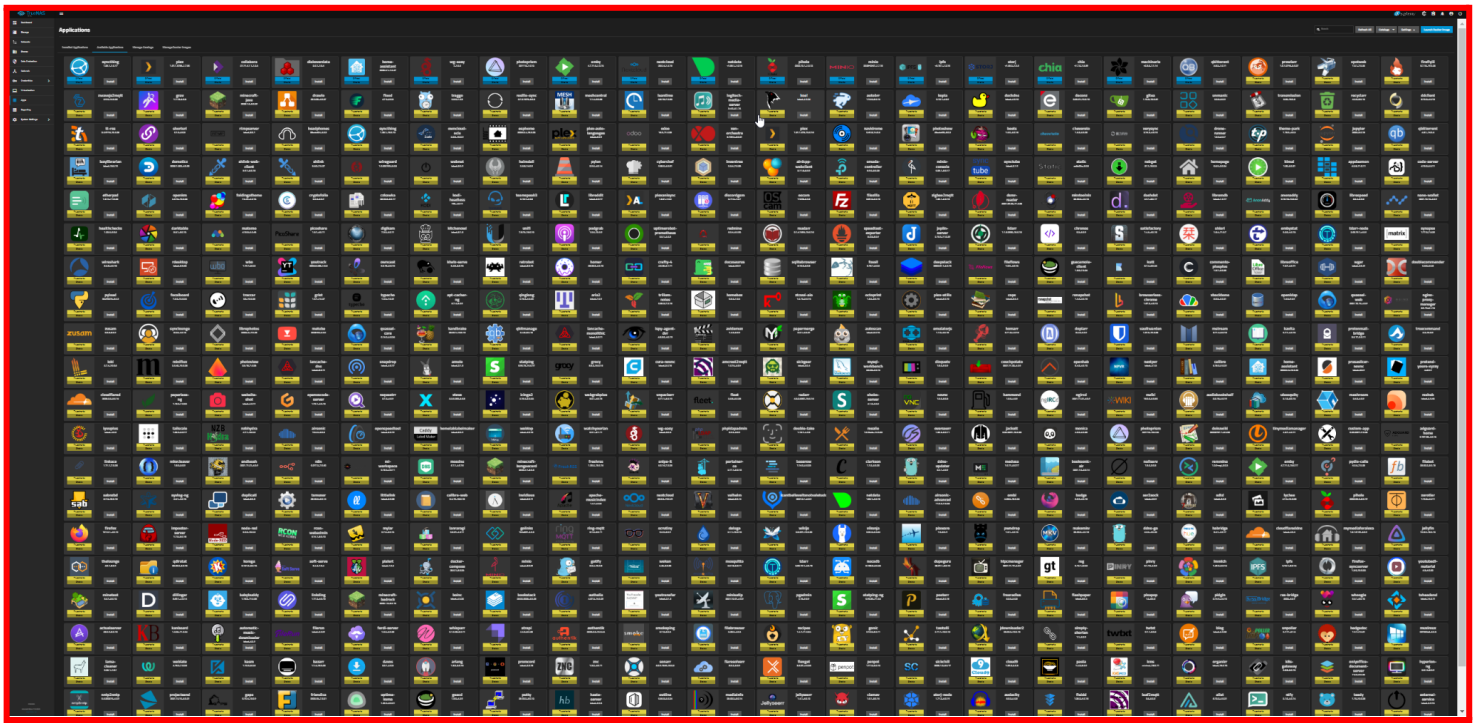
Après avoir démarré l'installation de n'importe quelle application, il sera possible de voir la différence de ressources prises en termes de RAM. K8s s'installe et démarre réellement, donc les ressources utilisées seront plus élevées.



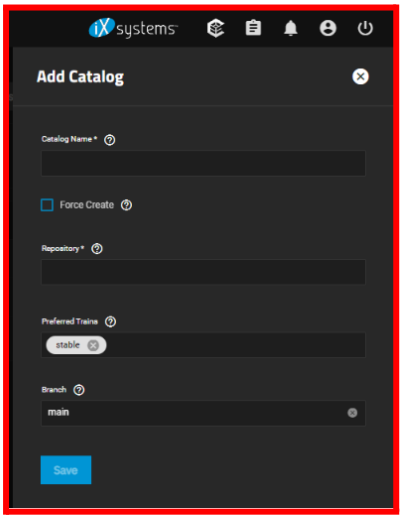
Après quelques minutes (le temps de chargement de l'ensemble du référentiel), toutes les applications sur TrueCharts seront disponibles et prêtes à être téléchargées.



La quantité d'applications disponibles est vraiment colossale par rapport à avant.



Évidemment il sera possible d'installer les dépôts de notre choix via le menu dédié à droite.



Pour des raisons de sécurité, il sera toujours recommandé de saisir des référentiels fiables. Le danger de "code malveillant" est toujours au coin de la rue, en particulier dans l'environnement business.

En fait, ce sont tous les risques que l'on peut avoir en installant des applications dont la source n'est pas fiable.

- Services interrompus sur l'hôte TrueNAS
- Interruption de service sur l'hôte TrueNAS
- Autorisations de système de fichiers brisées sur l'hôte
- Suppression inattendue des données utilisateur
- Configuration de service non sécurisée dans l'application
- Dégradation des performances et de la stabilité de l'hôte TrueNAS
- Logiciel malveillant

Pour ce TP nous allons installer trois services :

Wireguards (VPN)

WireGuard est un protocole de communication et un logiciel gratuit et open-source qui implémente des VPN (Virtual private network), et a été conçu avec les objectifs de facilité d'utilisation, de performances à haute vitesse et de faible surface d'attaque.

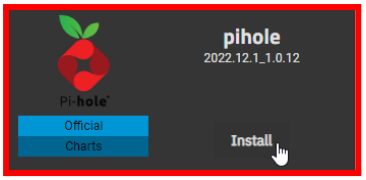
NextCloud (clouds privés)

Nextcloud est une suite de logiciels client-serveur permettant de créer et d'utiliser des services d'hébergement de fichiers. Nextcloud offre des fonctionnalités similaires à Dropbox, Office 365 ou Google Drive lorsqu'il est utilisé avec des solutions de suite bureautique intégrée comme Collabora Online ou OnlyOffice. Il peut être hébergé dans le cloud ou sur site

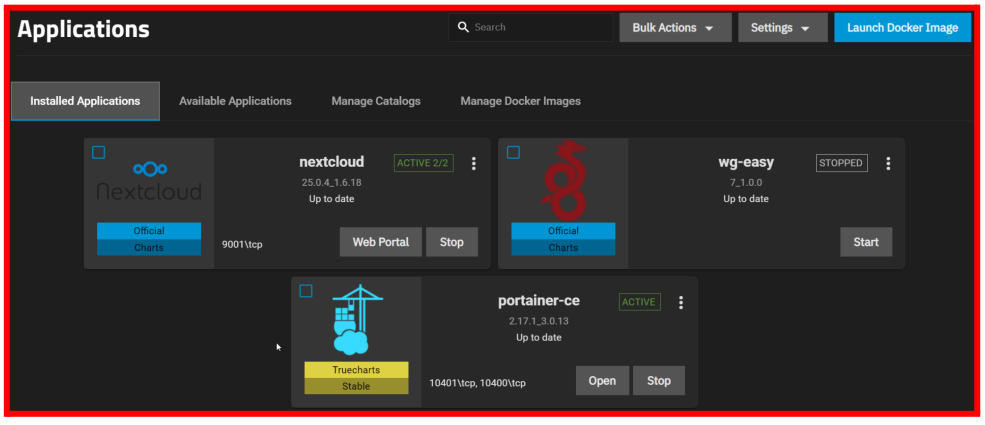
Portainer (gestion de conteneurs)

Portainer (la plate-forme de gestion de conteneurs hybride et multi-cloud de Portainer prend en charge Kubernetes, Docker, Swarm dans n'importe quel centre de données, cloud, réseau Edge ou appareil IIoT.)

Commençons donc par installer les applications cibles.
En effet, pour installer une application il suffira de cliquer sur installer une fois qu'on la trouvera présente dans le menu "applications disponibles".



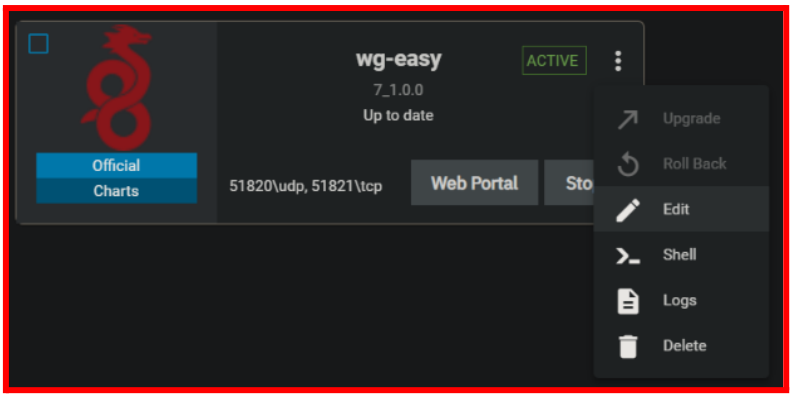
Une fois l'application installée, elle sera alors disponible sous l'onglet "Installed application"



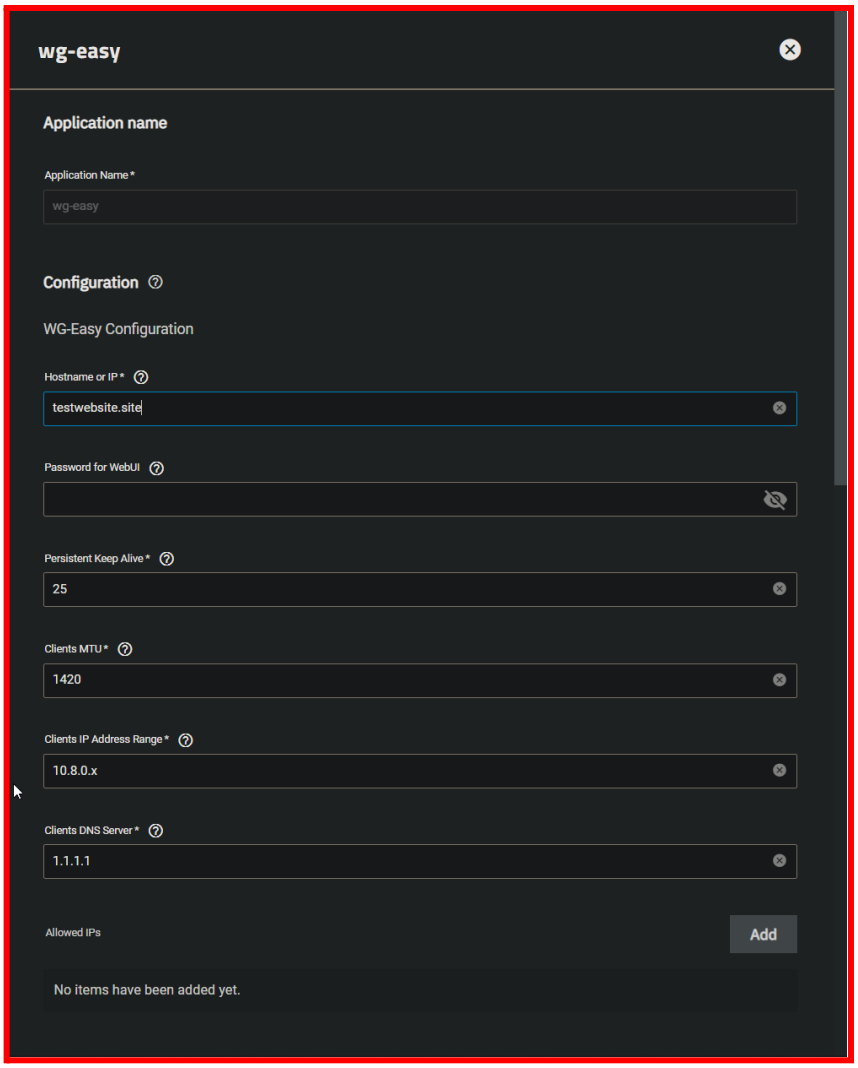
Configuration de mise en service des containers/services

Wireguard

Une fois l'application installée, il ne reste plus qu'à la configurer:La configuration est en effet très simple. tout ce qui doit être paramétré se trouve en fait dans le menu "édition" de l'application cible.



Il y a quelques paramètres essentiels e/ou importants qu'il faudra régler : Le **nom d'hôte** ou IP qui sera indispensable pour accéder à notre VPN, le mot de passe WebGui, pour protéger notre interface graphique d'où il sera possible d'avoir une vue d'ensemble de tous les clients connectés et d'où il sera possible de télécharger la configuration (via fichier ou code qr).



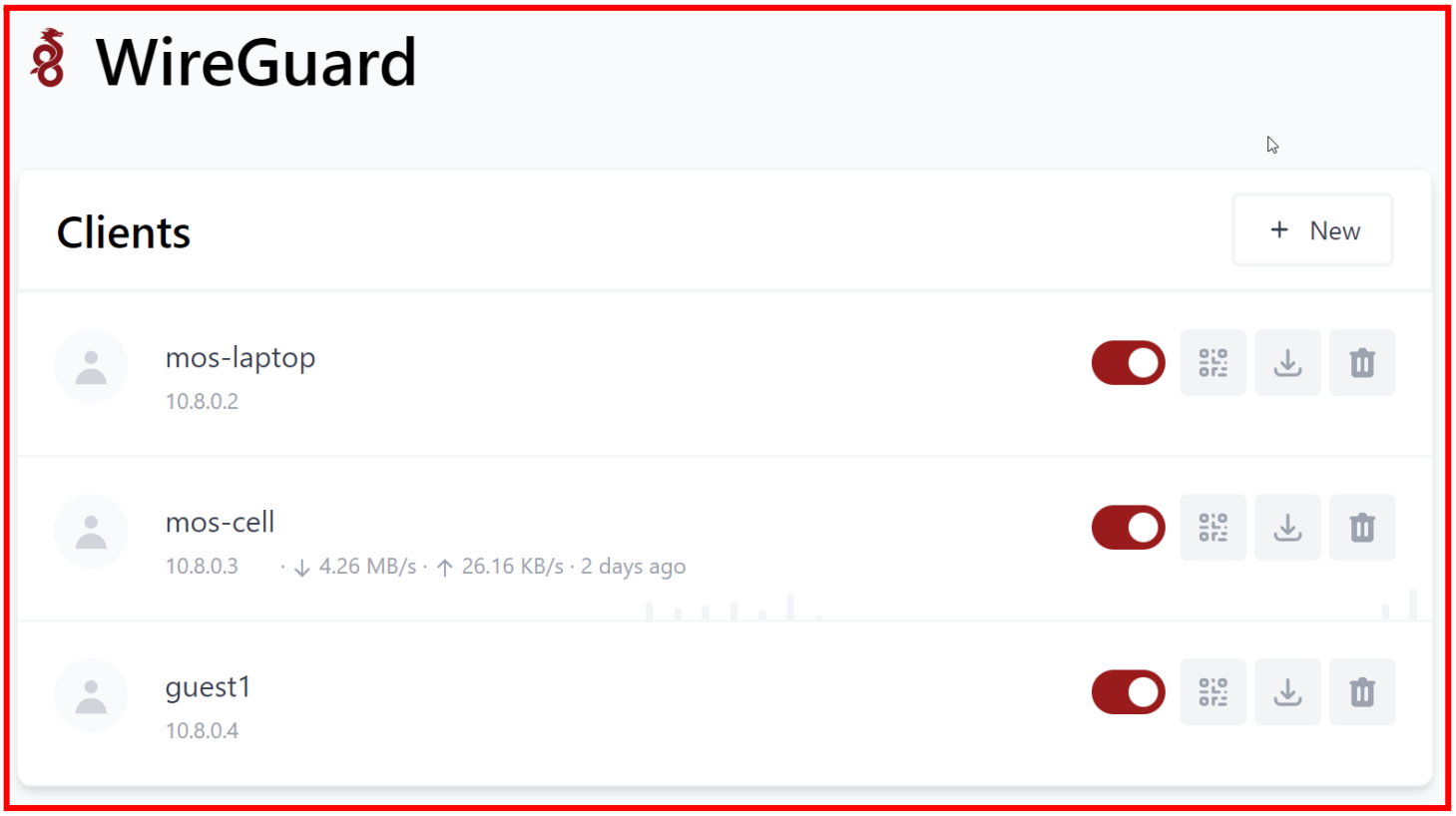
La fonction de “keep alive” est principalement destinée à la persistance de la traversée du NAT et du pare-feu. Si vous souhaitez en savoir plus sur ce paramètre et toutes les conséquences qui en découlent, je vous invite à lire ce paragraphe : https://www.wireguard.com/quickstart/

Le **MTU** (l'unité de transmission maximale) est la taille de la plus grande unité de données de protocole pouvant être communiquée dans une seule transaction de couche réseau. Le MTU n’est pas identique à la taille de trame maximale qui peut être transportée sur la couche de liaison de données.
Le réglage standard est correct dans la plupart des cas, mais dans certains cas il faudra le changer (par exemple si vous avez un réseau assez puissant avec des lignes de 2.5Gbit ou plus).

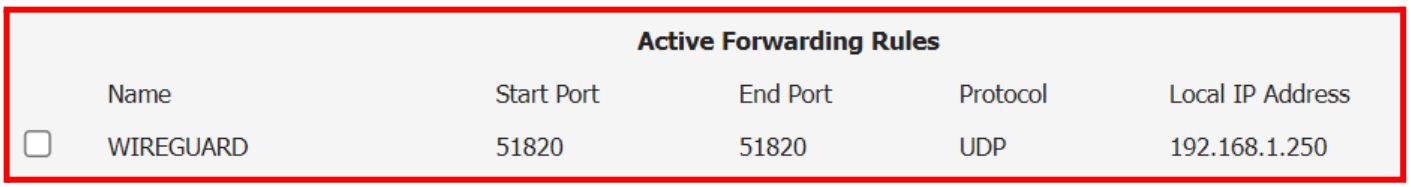
La **plage d'adresses IP** doit être définie en fonction du nombre de clients estimés s'être connectés. par exemple, un masque CIDR de /28 peut également être saisi pour une dizaine de clients connectés

Le **serveur DNS** peut également être défini sur une adresse locale s'il existe un serveur pi.hole local par exemple.

Une fois que nous sommes dans l'interface graphique, nous devons évidemment télécharger la configuration du client (qui pourra être téléchargée à la fois via le code qr et via le fichier de configuration)



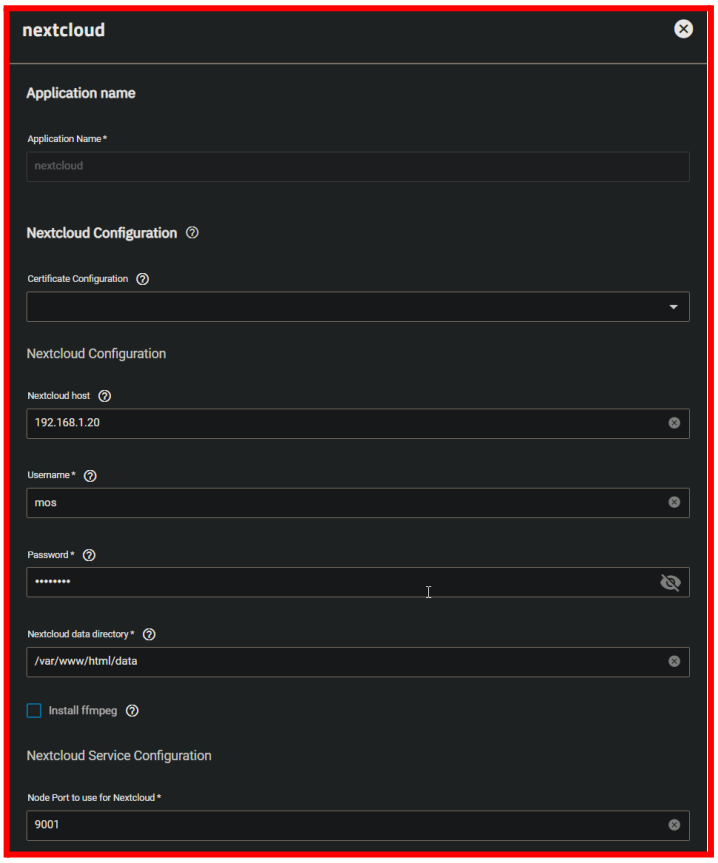
Le port (généralement 51820) doit être ouvert dans notre routeur/pare-feu.
L'adresse IP locale de notre appareil qui agit comme un serveur vpn et le port cible précédemment sélectionné doivent être sélectionnés.

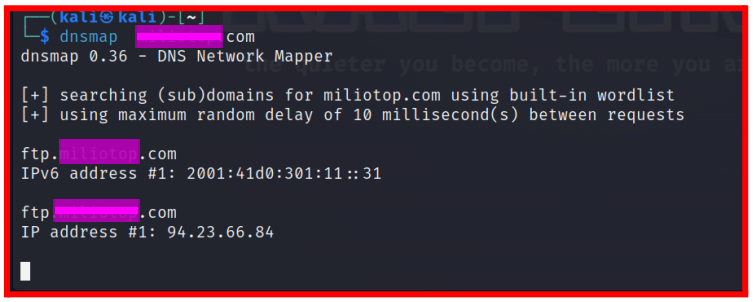


Active Forwarding Rules

Name	Start Port	End Port	Protocol	Local IP Address
WIREGUARD	51820	51820	UDP	192.168.1.250

NextCloud

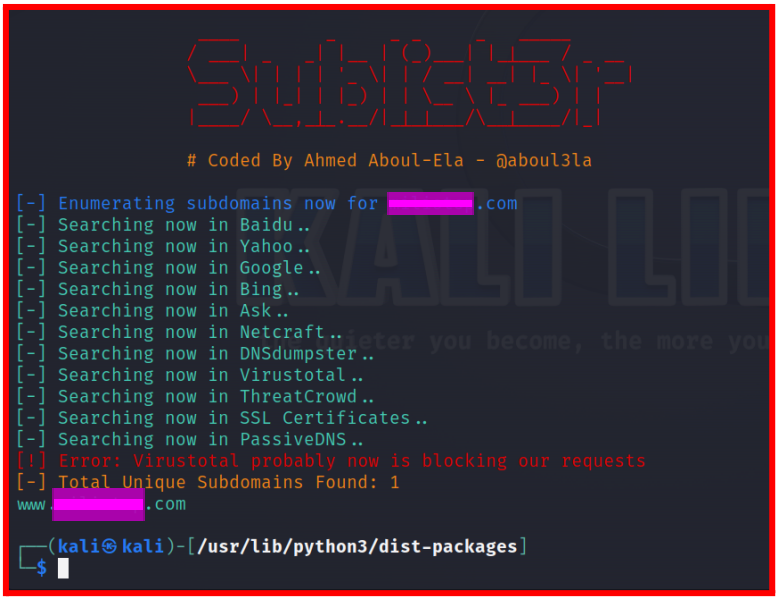




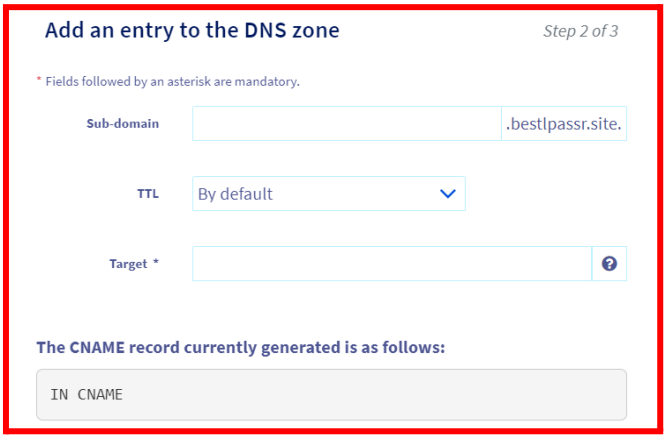
Quant à la configuration de **Nexcloud**, elle sera facile dans la même mesure que WireGuard a été installé. Il sera possible de "monter" d'autres dossiers qui sont par exemple stockés dans un autre appareil. Par exemple, il sera possible de créer un lien vers un dossier existant sur un NAS.

Quelques paramètres de base essentiels seront nécessaires.
L'adresse de l'hébergeur, le nom d'utilisateur et le mot de passe de l'interface graphique relatifs au premier login (il faudra ensuite le modifier), le répertoire relatif aux données et le port cible (9001 par défaut).

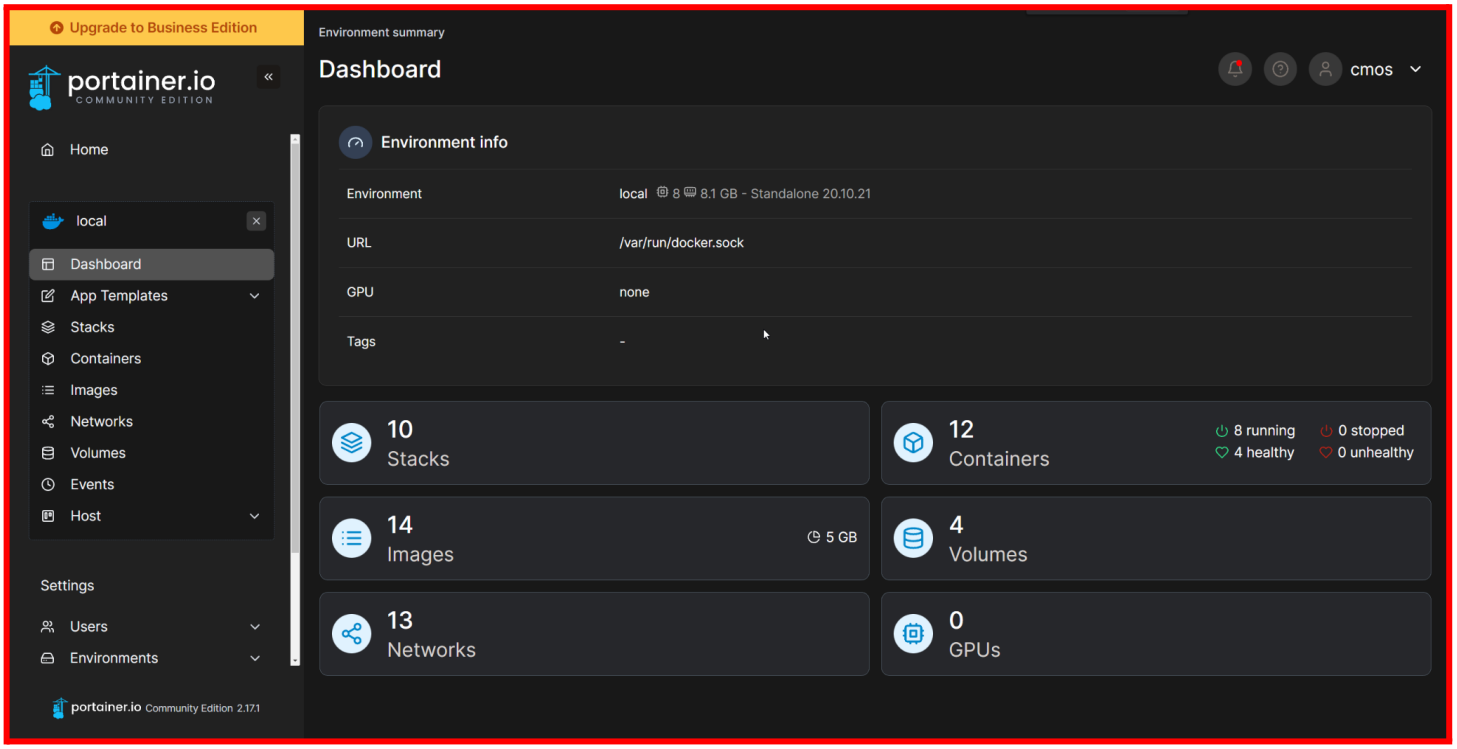
Une chose pratique à configurer avec Nextcloud sera un domaine personnalisé que nous pourrons contacter lorsque nous aurons besoin d'accéder à notre cloud à distance. À cet égard, mon collègue et moi étions préoccupés par la sécurité de cette opération. Eh bien, sur un **os kali linux**, nous avons testé comment les pirates peuvent trouver les sous-domaines d'un domaine existant. Apparemment, la seule façon de trouver un sous-domaine est de le forcer brutalement via un dictionnaire. Fondamentalement, si un sous-domaine complexe est saisi, tel que ***skfj1aonwofj9086na.subdomain.com***, il est peu probable que ce dernier soit découvert.



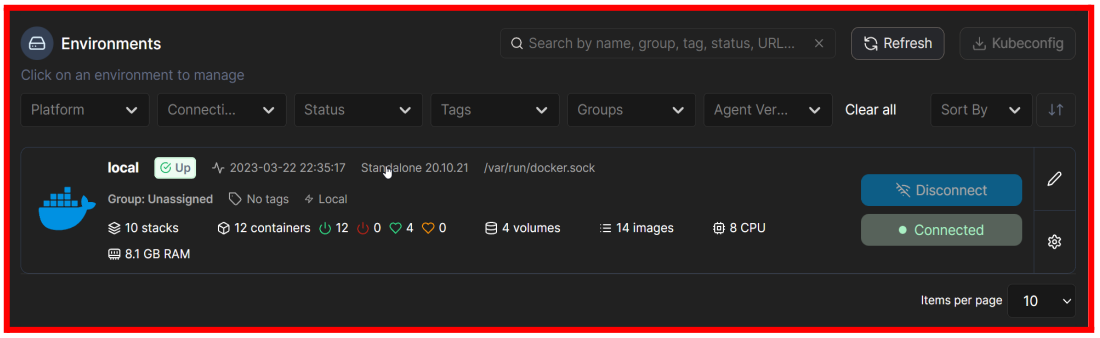
Ajouter un sous-domaine sera facile.
En fait, il faudra ajouter un enregistrement CNAME, l'adresse d'un serveur DNS qui servira d'ip cible si nous avons une adresse IP dynamique et le domaine cible que nous voulons créer.



Portainer



Portainer est une interface utilisateur de gestion “soft” qui permet de gérer facilement vos différents environnements Docker (host Docker ou clusters Swarm).



Portainer se veut aussi simple à déployer qu'à utiliser. Il se compose d'un conteneur unique qui peut s'exécuter sur n'importe quel moteur Docker (peut être déployé en tant que conteneur Linux ou conteneur natif Windows, prend également en charge d'autres plates-formes).

Portainer permet de gérer toutes les ressources Docker (conteneurs, images, volumes, réseaux et plus). Il est compatible avec le moteur Docker autonome et avec le mode Docker Swarm.

Est possibile de l’itiliser des cas qui fonctionnent tres bien tel que:

- lister les projets stack
- lister les conteneur/stacks
- afficher la configuration d’un conteneur
- faire un check de la console Web dans un conteneur spécifique
- afficher/filtrer les legs de conteneur

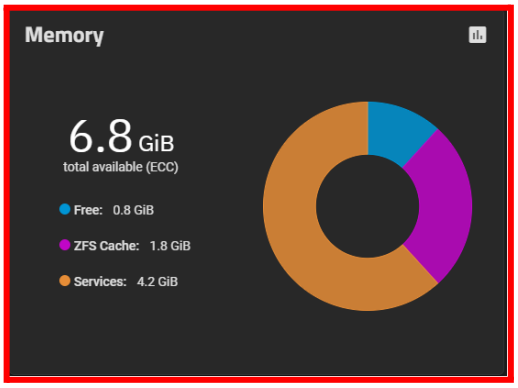
le site officiel : https://www.portainer.io/

Comparison

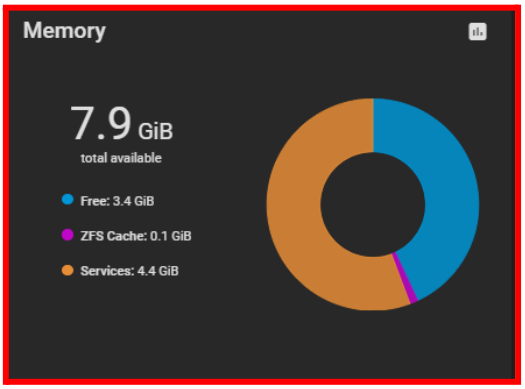
Comme on le voit sur deux machines avec plus ou moins les mêmes performances on a une utilisation des ressources très différente. En fait, sur la version de base, nous avons une utilisation des ressources beaucoup plus faible que sur la version SCALE. Ceci est en fait dû à deux facteurs. La version Scale de TrueNAS est en fait construite sur un système o.s. ***Debian*** qui est plus gourmande en ressources, contrairement à la version CORE qui est basée sur ***FreeBSD***. La version SCALE consommera également plus car c'est le système ***K8s*** qui sert de base aux conteneurs.

4,5 Gb de RAM *sont consommés par la version Core*
6,0 Gb de RAM *sont plutôt consommés par la version SCALE*

TrueNAS SCALE



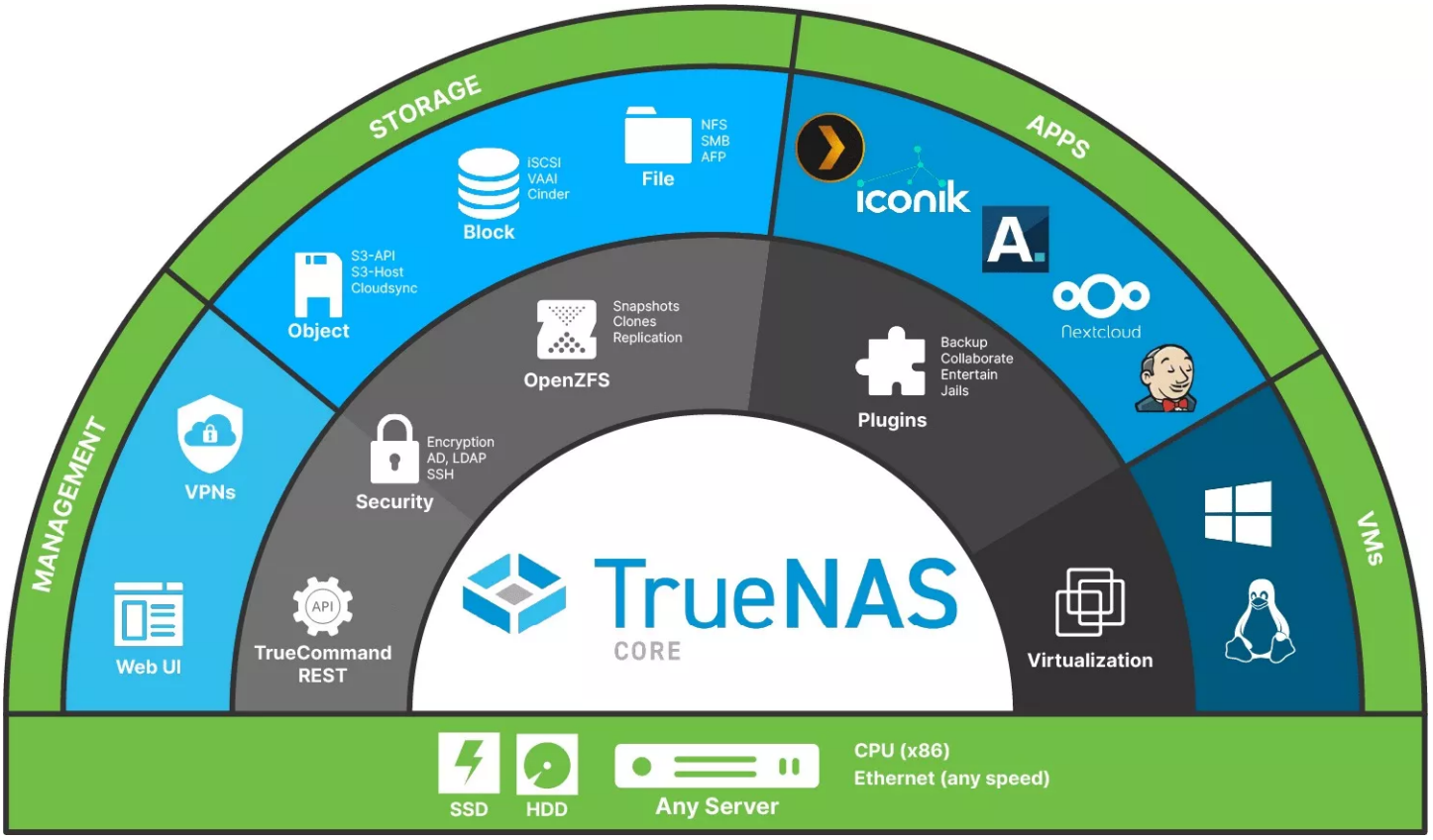
TrueNAS CORE



Le test de cette comparaison a été effectué avec une seule application utilisée dans le jail/conteneur. Donc uniquement avec nextcloud opérationnel.

On constate donc que les jails utilise moins de ressource que les conteneurs de sur la version Scale.

Comme mentionné précédemment, TrueNAS SCALE a de nombreuses autres applications dans le référentiel. S'il est possible dans la version TrueNAS CORE de charger plusieurs jails en externe, il est tout de même plus pratique sur TrueNAS SCALE de déployer des applications en quelques clics.

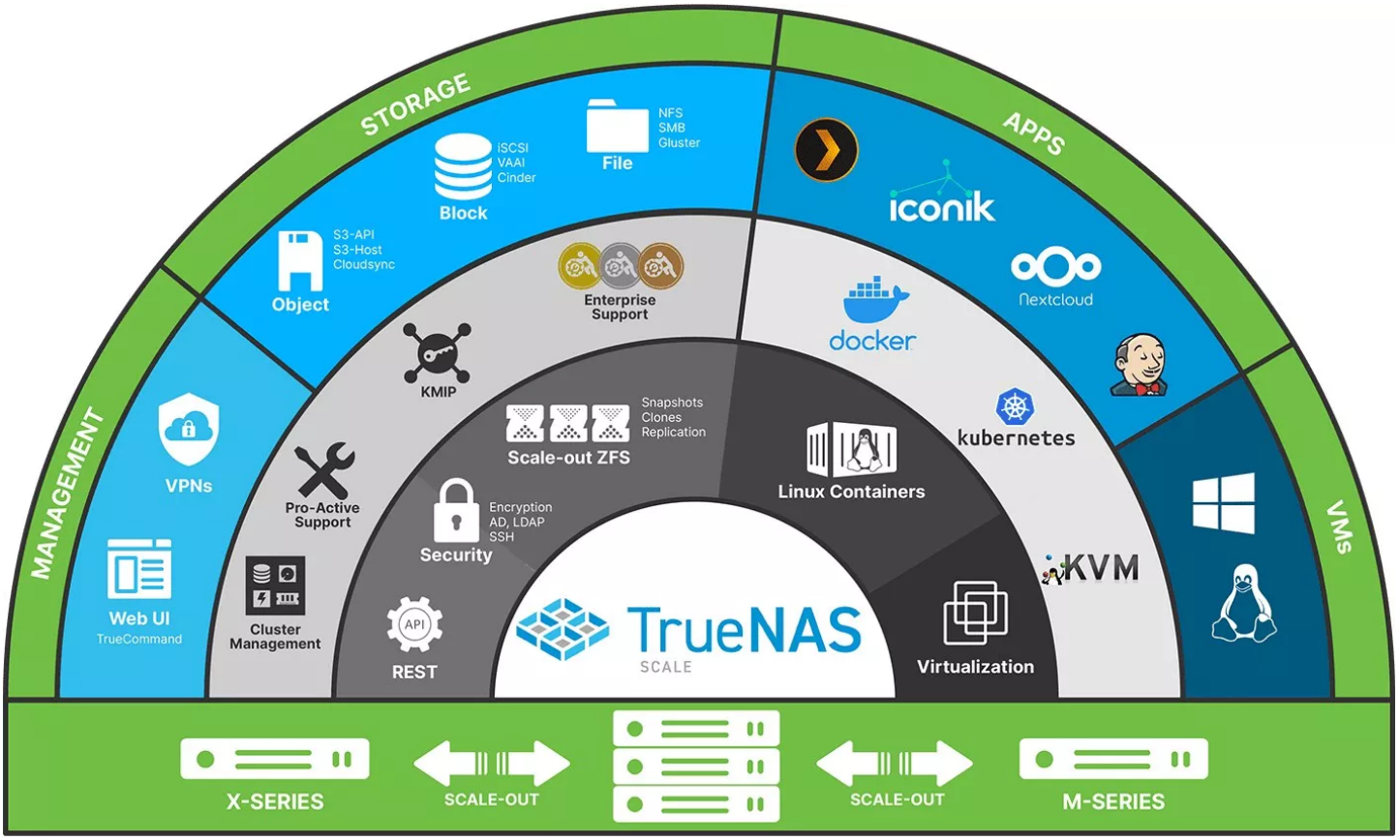


Comme déjà expliqué ci-dessus, TrueNAS Core est davantage destiné aux environnements HOME, aux utilisateurs passionnés, mais pas à un environnement **business**.

Néanmoins, le côté application (comme il est possible de le voir dans la partie bleue, reste largement inchangé sur les deux versions)

La différence réside dans le niveau de l'application au niveau du système. Sans oublier que la version SCALE de TrueNAS dispose d'un **support technique PRO** de son côté qui est l'une des caractéristiques clés de la version SCALE.

Jenkins, (oui l'icône de l'homme qui ressemble au gars du Monopoly) est un conteneur qui sert à créer des automatisations. En effet, il sera possible de créer de véritables "Jobs" liés à la cause/effet et programmables à volonté.



TrueNAS SCALE est en effet plus évolutif que son coté CORE. Il est plus adapté aux environnements professionnels, généralement dans les environnements de serveurs en rack.

Une autre des fonctionnalités clés de TrueNAS Scale est le protocole **KMIP** (Key Management Interoperability Protocol) que est un protocole de communication client/serveur extensible pour le stockage et la maintenance des clés, des certificats et des objets secrets. KMIP sur TrueNAS Enterprise intègre le système dans une infrastructure de gestion de clés centralisée existante et utilise une seule source fiable pour créer, utiliser et détruire les mots de passe SED et les clés de chiffrement ZFS.

Conclusion

Bien sûr, je serais heureux de vous aider à comprendre les différences entre TrueNAS SCALE et TrueNAS CORE et à quel environnement chacun est le plus adapté.

TrueNAS CORE est un système d'exploitation de stockage en réseau (NAS) gratuit et open source basé sur FreeBSD. Il est conçu pour les environnements domestiques et de petites entreprises, offrant aux utilisateurs une interface Web intuitive pour gérer et stocker leurs données. TrueNAS CORE prend en charge une large gamme de protocoles, notamment CIFS/SMB, NFS, AFP, iSCSI, FTP et WebDAV, ce qui en fait une option polyvalente pour une variété de cas d'utilisation.

D'autre part, TrueNAS SCALE est une solution de stockage open source de niveau entreprise conçue pour les grandes organisations et les centres de données. Il est basé sur Debian Linux et utilise le système de fichiers OpenZFS. TrueNAS SCALE est plus puissant et riche en fonctionnalités que TrueNAS CORE, offrant des fonctionnalités avancées telles que la conteneurisation avec Docker et Kubernetes, la virtualisation avec KVM et la prise en charge de fonctionnalités avancées de mise en réseau et de sécurité.

Donc, en résumé, si vous recherchez une solution NAS gratuite et open source pour votre maison ou votre petit bureau, TrueNAS CORE est un excellent choix. Il est facile à utiliser et prend en charge une large gamme de protocoles. D'autre part, si vous êtes une grande organisation ou un centre de données à la recherche d'une solution de stockage plus puissante et riche en fonctionnalités, TrueNAS SCALE serait le meilleur choix. Il offre des fonctionnalités avancées et la possibilité d'évoluer pour répondre aux besoins des environnements les plus vastes.