Administration GNU/Linux

Vous trouverez ici mes astuces d'administration GNU/Linux.

- Guide des commandes Linux et administration Debian
- Installez un serveur Debian 12 de façon sécurisée
- Méthode de sauvegarde
- Configuration d'un accès SFTP restreint au répertoire chroot
- Guide de validation des disques durs avant mise en production
- Chiffrer un serveur Debian et déverrouiller à distance
- Geekbench 6
- Flash Mellanox CX2
- Tmux

Guide des commandes Linux et administration Debian

Structure du système de fichiers Debian

Répertoires racine du système Debian

Répertoire	Description	Contenu principal
`/`	Racine du système	Point de montage principal
`/bin`	Binaires essentiels	Commandes de base (ls, cat, cp, mv, etc.)
`/boot`	Fichiers de démarrage	Noyau Linux, initramfs, GRUB
`/dev`	Périphériques	Fichiers spéciaux des périphériques
`/etc`	Configuration système	Fichiers de configuration globaux
`/home`	Répertoires utilisateurs	Dossiers personnels des utilisateurs
`/lib`	Bibliothèques partagées	Bibliothèques système essentielles
`/lib64`	Bibliothèques 64-bit	Bibliothèques pour architecture 64-bit
`/media`	Points de montage amovibles	CD/DVD, clés USB montés automatiquement
`/mnt`	Points de montage temporaires	Montages manuels temporaires
`/opt`	Logiciels optionnels	Applications tierces
`/proc`	Système de fichiers virtuel	Informations sur les processus
`/root`	Répertoire de l'administrateur	Dossier personnel du compte root
`/run`	Données d'exécution	Fichiers temporaires des services
`/sbin`	Binaires système	Commandes d'administration système
`/srv`	Données de service	Données servies par le système
`/sys`	Système de fichiers virtuel	Interface avec le noyau
`/tmp`	Fichiers temporaires	Fichiers temporaires effacés au redémarrage
`/usr`	Ressources utilisateur	Applications et bibliothèques utilisateur

Répertoire	Description	Contenu principal
`/var`	Données variables	Logs, caches, bases de données

Répertoires importants dans `/usr`

Répertoire	Description
`/usr/bin`	Binaires utilisateur non-essentiels
`/usr/lib`	Bibliothèques pour `/usr/bin`
`/usr/local`	Logiciels installés localement
`/usr/sbin`	Binaires système non-essentiels
`/usr/share`	Données partagées (documentation, man pages)

Répertoires importants dans `/var`

Répertoire	Description
`/var/log`	Fichiers journaux (logs)
`/var/cache`	Cache des applications
`/var/lib`	Données variables des applications
`/var/tmp`	Fichiers temporaires persistants
`/var/www`	Contenu web (Apache/Nginx)

Commandes de base Linux

Navigation et manipulation de fichiers

`ls` - Lister le contenu d'un répertoire

```
ls                # Liste les fichiers et dossiers du répertoire courant
ls -l             # Liste détaillée avec permissions, propriétaire, taille
ls -a             # Affiche les fichiers cachés (commençant par .)
ls -lh            # Liste détaillée avec tailles lisibles (Ko, Mo, Go)
ls /chemin/dossier  # Liste le contenu d'un dossier spécifique
```

`cd` - Changer de répertoire

```
cd /home/utilisateur   # Aller dans un répertoire spécifique
cd ..                   # Remonter d'un niveau dans l'arborescence
cd ~                   # Aller dans le répertoire personnel
cd -                   # Revenir au répertoire précédent
```

`pwd` - Afficher le répertoire courant

```
pwd                    # Affiche le chemin complet du répertoire actuel
```

`mkdir` - Créer un répertoire

```
mkdir nouveau_dossier           # Créer un dossier
mkdir -p dossier/sous_dossier   # Créer un dossier avec ses parents
```

`rmdir` - Supprimer un répertoire vide

```
rmdir dossier_vide    # Supprime uniquement un dossier sans contenu
```

`rm` - Supprimer des fichiers/répertoires

```
rm fichier.txt                # Supprimer un fichier
rm -r dossier                 # Supprimer un dossier et son contenu
rm -rf dossier                # Supprimer forcément sans confirmation
```

`cp` - Copier des fichiers/répertoires

```
cp fichier1 fichier2          # Copier un fichier
cp -r dossier1 dossier2       # Copier un dossier et son contenu
cp fichier /chemin/destination # Copier vers un autre emplacement
```

`mv` - Déplacer/renommer des fichiers/répertoires

```
mv fichier1 fichier2          # Renommer un fichier
mv fichier /nouveau/chemin     # Déplacer un fichier
mv dossier1 /nouveau/chemin    # Déplacer un dossier
```

`find` - Rechercher des fichiers

```
find /chemin -name "*.txt"     # Trouver tous les fichiers .txt - Cas sensible au majuscule et
minuscule
find /chemin -iname "*.txt"     # Trouver tous les fichiers .txt - Cas insensible au majuscule
```

```
et minuscule
find . -type f -size +10M      # Fichiers > 10 Mo dans le répertoire courant
find /home -user utilisateur    # Fichiers appartenant à un utilisateur
```

`locate` - Localiser des fichiers rapidement

```
locate nom_fichier             # Recherche rapide dans l'index système
sudo updatedb                  # Mettre à jour l'index de recherche
```

Gestion des permissions

`chmod` - Modifier les permissions

```
chmod 755 fichier.txt           # Définir des permissions (rwxr-xr-x)
chmod u+x script.sh             # Ajouter droit d'exécution au propriétaire
chmod g-w fichier               # Retirer droit d'écriture au groupe
chmod +t dossier                # Activer le sticky bit sur un dossier
chmod 1777 dossier_partage      # Sticky bit sur permissions rwxrwxrwt
```

- **Sticky bit** : Permet, sur un répertoire (comme `/tmp`), que seuls les propriétaires puissent supprimer ou renommer leurs propres fichiers, même si d'autres ont des droits d’écriture. Représenté par un `t` à la fin dans `ls -l` (`drwxrwxrwt`).

`chown` - Changer le propriétaire

```
chown utilisateur fichier.txt   # Changer le propriétaire
chown utilisateur:groupe fichier # Changer propriétaire et groupe
```

`chgrp` - Changer le groupe

```
chgrp groupe fichier.txt        # Changer le groupe d'un fichier
```

Surveillance système

`ps` - Afficher les processus

```
ps aux                      # Liste détaillée de tous les processus
ps -ef                      # Autre format de listing
```

`top` - Monitorer les processus en temps réel

```
top                          # Monitorer l'utilisation système
```

`htop` - Version améliorée de top

```
htop                         # Interface interactive de surveillance
```

`df` - Afficher l'espace disque

```
df -h                        # Affichage lisible des espaces disques
df -T                        # Afficher les types de systèmes de fichiers
```

`du` - Afficher l'utilisation de l'espace

```
du -sh /chemin               # Taille totale d'un dossier
du -h --max-depth=1          # Taille des sous-dossiers
```

`free` - Afficher la mémoire disponible

```
free -h                      # Mémoire utilisable en format lisible
free -m                      # Mémoire en MégaOctets
```

Informations Système

`uname` - Informations sur le système

```
uname -a                     # Afficher toutes les informations système
uname -s                     # Nom du système d'exploitation
uname -r                     # Version du noyau
uname -m                     # Architecture machine
```

`lsblk` - Lister les périphériques de bloc

```
lsblk                        # Liste des disques et partitions# Changer les permissions
chmod 755 fichier.txt
chmod u+x fichier.sh         # Ajouter exécution pour le propriétaire
chmod g-w fichier.txt        # Retirer écriture pour le groupe
chmod o=r fichier.txt        # Définir lecture seule pour les autres

# Changer le propriétaire
chown utilisateur:groupe fichier.txt
```

```
chown utilisateur fichier.txt
chgrp groupe fichier.txt
lsblk -f                        # Afficher les systèmes de fichiers
lsblk -a                        # Afficher tous les périphériques
```

`fdisk` - Gestion des partitions

```
sudo fdisk -l                   # Lister toutes les partitions
sudo fdisk /dev/sdX             # Gérer une partition spécifique
```

`lscpu` - Informations sur le processeur

```
lscpu                           # Détails complets du processeur
lscpu | grep "CPU(s)"           # Nombre de processeurs
```

`lspci` - Périphériques PCI

```
lspci                           # Liste des périphériques PCI
lspci -v                        # Informations détaillées
```

`lsusb` - Périphériques USB

```
lsusb                           # Liste des périphériques USB
lsusb -v                        # Informations détaillées
```

`cat` - Afficher des informations système

```
cat /etc/os-release             # Informations sur la distribution
cat /proc/cpuinfo               # Détails du processeur
cat /proc/meminfo               # Informations mémoire
```

`hostnamectl` - Informations système

```
hostnamectl                     # Afficher les informations système
hostnamectl status              # Statut du système
```

Tableau des droits des fichiers

Représentation numérique (octale)

Valeur	Binaire	Permissions	Description
0	000	---	Aucun droit
1	001	--x	Exécution seulement
2	010	-w-	Écriture seulement
3	011	-wx	Écriture + Exécution
4	100	r--	Lecture seulement
5	101	r-x	Lecture + Exécution
6	110	rw-	Lecture + Écriture
7	111	rwx	Tous les droits

Structure des permissions

Les permissions sont définies pour trois entités :

- **Propriétaire** (user) - Premier chiffre
- **Groupe** (group) - Deuxième chiffre
- **Autres** (others) - Troisième chiffre

Exemples courants

Permission	Signification
755	rwxr-xr-x (propriétaire: tous droits, groupe/autres: lecture+exécution)
644	rw-r--r-- (propriétaire: lecture+écriture, groupe/autres: lecture seule)
600	rw------- (propriétaire: lecture+écriture, groupe/autres: aucun droit)
777	rwxrwxrwx (tous droits pour tous)
700	rwx------ (propriétaire: tous droits, groupe/autres: aucun droit)

Commandes de gestion des permissions

```
# Changer les permissions d'un fichier
chmod 755 fichier.txt

# Changer les permissions d'un dossier de façon récursive
```

```
chmod -R 755 dossier

# Ajouter une permission d'exécution pour le propriétaire sur un fichier
chmod u+x fichier.sh

# Ajouter une permission d'exécution pour le propriétaire sur un dossier de façon récursive
chmod -R u+x dossier

# Retirer l'écriture pour le groupe sur un fichier
chmod g-w fichier.txt

# Retirer l'écriture pour le groupe sur un dossier de façon récursive
chmod -R g-w dossier

# Définir la lecture seule pour les autres sur un fichier
chmod o=r fichier.txt

# Définir la lecture seule pour les autres sur un dossier de façon récursive
chmod -R o=r dossier

# Changer le propriétaire d'un fichier
chown utilisateur:groupe fichier.txt

# Changer le propriétaire d'un dossier de façon récursive
chown -R utilisateur:groupe dossier

# Changer le groupe d'un fichier
chgrp groupe fichier.txt

# Changer le groupe d'un dossier de façon récursive
chgrp -R groupe dossier
```

Gestion des serveurs Debian

Services système

- `systemctl start service` - Démarrer un service
- `systemctl stop service` - Arrêter un service

- `systemctl restart service` - Redémarrer un service
- `systemctl enable service` - Activer un service au démarrage
- `systemctl status service` - Vérifier le statut d'un service

Gestion des paquets

- `apt update` - Mettre à jour la liste des paquets
- `apt upgrade` - Mettre à jour les paquets installés
- `apt install package` - Installer un paquet
- `apt remove package` - Supprimer un paquet

Réparation d'APT

Problèmes courants et solutions

1. Réparer les paquets cassés

Corriger les dépendances cassées :

```
sudo apt --fix-broken install
```

Forcer la configuration des paquets :

```
sudo dpkg --configure -a
```

Réparer les paquets partiellement installés :

```
sudo apt-get -f install
```

2. Nettoyer le cache APT

Nettoyer le cache des paquets :

```
sudo apt clean
```

```
sudo apt autoclean
```

Supprimer les paquets orphelins :

```
sudo apt autoremove
sudo apt autoremove --purge  # Supprimer aussi les fichiers de configuration
```

3. Reconfigurer APT

Reconstruire la base de données des paquets :

```
sudo apt update --fix-missing
```

Forcer la mise à jour des sources :

```
sudo apt update && sudo apt upgrade
```

4. Problèmes de verrouillage

Supprimer les verrous APT (si aucun processus APT n'est en cours) :

```
sudo rm /var/lib/dpkg/lock-frontend
```

```
sudo rm /var/lib/dpkg/lock
```

```
sudo rm /var/cache/apt/archives/lock
```

Reconfigurer dpkg :

```
sudo dpkg --configure -a
```

5. Réinitialiser les sources APT

Sauvegarder les sources actuelles :

```
sudo cp /etc/apt/sources.list /etc/apt/sources.list.backup
```

Éditer les sources si nécessaire :

```
sudo nano /etc/apt/sources.list
```

Mettre à jour après modification :

```
sudo apt update
```

6. Vérifier l'intégrité du système

Vérifier les paquets installés :

```
sudo apt check
```

Simuler les actions sans les exécuter :

```
sudo apt -s upgrade
```

Forcer la réinstallation d'un paquet :

```
sudo apt reinstall nom_du_paquet
```

Administration des utilisateurs

Création et gestion des comptes utilisateurs

```
# Créer un compte utilisateur
sudo adduser username

# Modifier le mot de passe
sudo passwd utilisateur

# Créer un nouveau groupe
sudo addgroup nom_groupe

# Ajouter un utilisateur à un groupe
sudo adduser utilisateur groupe

# Modifier le répertoire personnel
sudo usermod -m -d /newhome/username username

# Supprimer un utilisateur
sudo deluser username

# Supprimer un utilisateur et son répertoire personnel
sudo deluser --remove-home username

# Lister les utilisateurs
cat /etc/passwd

# Lister les groupes
cat /etc/group
```

```
# Voir les groupes d'un utilisateur
groups username
```

Gestion des identifiants système

```
# Modifier le GID (identifiant de groupe) d'un utilisateur
sudo groupmod -g 900 toto

# Modifier l'UID (identifiant utilisateur) et le GID simultanément
sudo usermod -u 800 -g 900 toto

# Changer le shell par défaut d'un utilisateur
sudo usermod -s /bin/bash username

# Verrouiller un compte utilisateur
sudo usermod -L username

# Déverrouiller un compte utilisateur
sudo usermod -U username
```

Suppression de mot de passe

Méthode sécurisée :

```
# Supprimer le mot de passe d'un utilisateur
sudo passwd -d username

# Forcer le changement de mot de passe à la prochaine connexion
sudo passwd -e username
```

Méthode manuelle (mode recovery) : Pour supprimer manuellement un mot de passe, démarrez en mode live et modifiez le fichier `/etc/shadow`. Localisez la ligne correspondant à l'utilisateur et supprimez les caractères situés entre les deux premiers séparateurs « `:` ».

Exemple pour l'utilisateur Michu :

```
michu:$6$68oL9D6yVVCMTVswSb.51oFHz/:17999:0:99999:7:::
```

Devient :

```
michu::17999:0:99999:7:::
```

Connexion par tunnel SSH (équivalent VPN)

Cette méthode permet d'utiliser la connexion du serveur via un tunnel SSH.

Tunnel SOCKS (Dynamic Port Forwarding)

```
# Créer un tunnel SOCKS sur le port local 8080
ssh user@serveur -p port -D 8080

# Exemple avec l'utilisateur Michu
ssh michu@158.136.345.678 -p 1234 -D 8080
```

Autres types de tunnels SSH

```
# Tunnel local (Local Port Forwarding)
ssh -L 8080:localhost:80 user@serveur

# Tunnel distant (Remote Port Forwarding)
ssh -R 8080:localhost:80 user@serveur

# Tunnel avec compression
ssh -C -D 8080 user@serveur

# Tunnel en arrière-plan
ssh -f -N -D 8080 user@serveur
```

Configuration du proxy : Configurez votre navigateur pour utiliser le proxy SOCKS avec l'adresse `127.0.0.1` et le port `8080`.

Note : L'option `-p` spécifie le port SSH s'il diffère du port par défaut (22).

Personnalisation et automatisation

Message d'accueil personnalisé (MOTD)

```
# Créer un message d'accueil personnalisé
sudo nano /etc/motd.d/01-custom
```

Maintenance et optimisation du système

Nettoyage APT [1]

Suppression complète du cache (supprime tous les paquets de /var/cache/apt/archives) :

```
sudo apt-get clean
```

Nettoyage intelligent (conserve les paquets ayant des équivalents dans les dépôts, supprime les versions obsolètes) :

```
sudo apt-get autoclean
```

Cette approche de nettoyage permet de récupérer de l'espace disque tout en préservant les paquets utiles pour de futures réinstallations.

Désactivation du compte root

Méthodes de désactivation du compte root

1. Verrouiller le compte root

```
sudo passwd -l root
```

2. Désactiver la connexion SSH pour root

Éditer le fichier de configuration SSH :

```
sudo nano /etc/ssh/sshd_config
```

Modifier ou ajouter la ligne :

```
PermitRootLogin no
```

Redémarrer le service SSH :

```
sudo systemctl restart ssh
```

3. Désactiver le compte root avec sudo

Éditer le fichier sudoers :

```
sudo visudo
```

Ajouter la ligne pour restreindre totalement l'accès root :

```
root ALL=(ALL) NOALL
```

4. Utiliser sudo à la place de root

Créer un utilisateur avec des privilèges sudo :

```
sudo adduser votreutilisateur
sudo usermod -aG sudo votreutilisateur
```

5. Vérifier les restrictions

Tester la connexion root :

```
sudo -i
```

Précautions supplémentaires

Vérifier les connexions root :

```
sudo grep root /var/log/auth.log
```

Surveiller les tentatives de connexion :

```
sudo last root
```

Bonnes pratiques

- Utilisez toujours `sudo` pour les actions administratives

- Créez un utilisateur distinct avec des privilèges sudo
- Utilisez des mots de passe forts
- Configurez l'authentification à deux facteurs
- Mettez à jour régulièrement le système

Installez un serveur Debian 12 de façon sécurisée

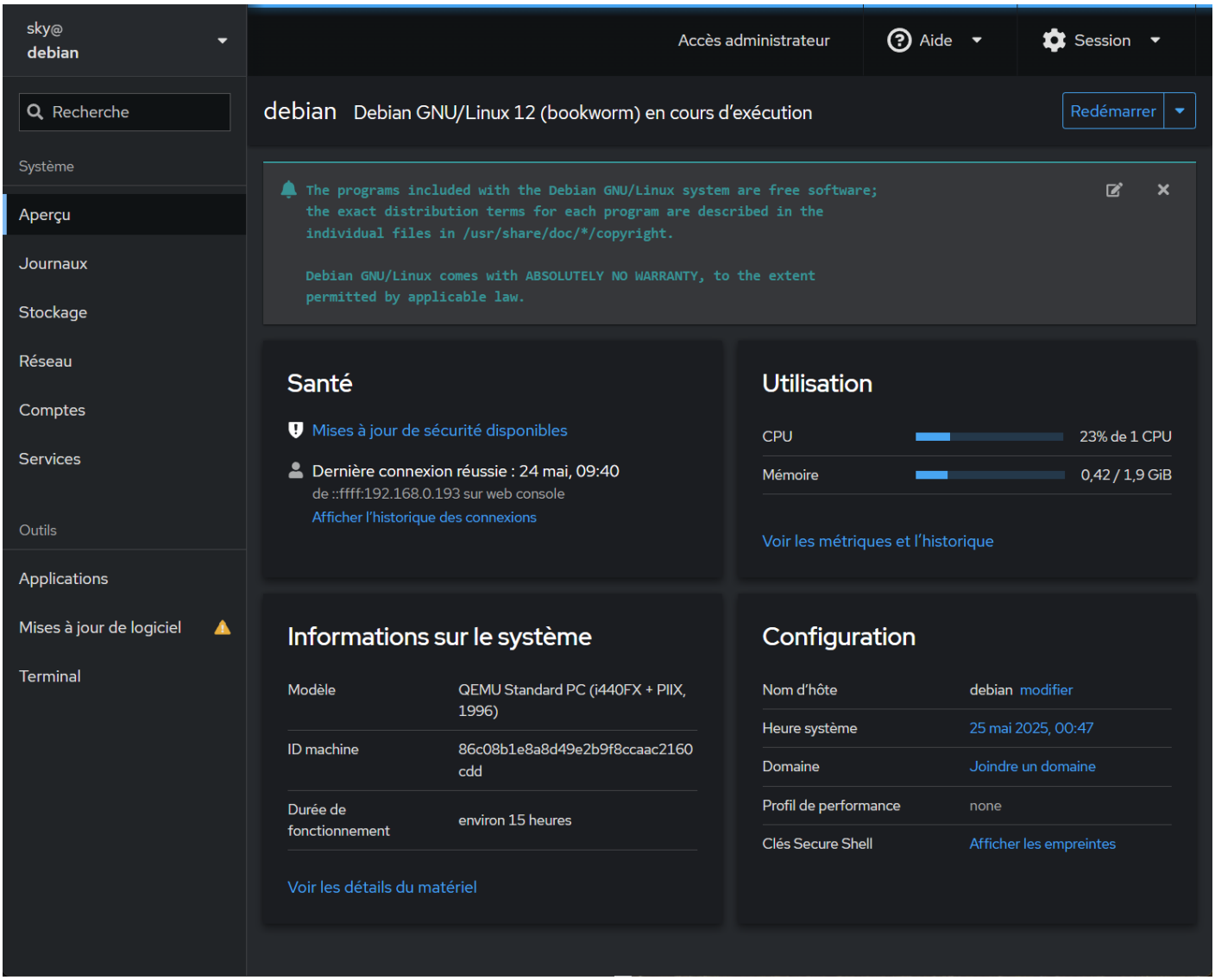
Nous allons installer Debian 12 de manière simple et sécurisée avec un mot de passe à usage unique (OTP) pour le serveur SSH et Cockpit, un pare-feu pour bloquer les IP malveillantes avec CrowdSec, et des mises à jour automatiques.

Prérequis :

- Debian 12 avec le compte root désactivé déjà installé
- Nom d'utilisateur qui ne contient pas de nom générique comme `Debian, Serveur, etc.`
- Compte avec un mot de passe fort
- Serveur SSH
- Installez l'application Android Google Authenticator ou un équivalent sur votre téléphone

Installation de Cockpit avec un mot de passe à usage unique (OTP)

Cockpit est une interface web de gestion de serveurs Linux. Il permet aux administrateurs de surveiller et de gérer facilement leurs serveurs via un navigateur web, offrant une vue d'ensemble des performances du système, des journaux, des utilisateurs, et des services en cours d'exécution. Cockpit simplifie la gestion des tâches administratives courantes sans nécessiter de compétences avancées en ligne de commande.



L'OTP (One-Time Password) est un mot de passe à usage unique qui change à chaque connexion, renforçant la sécurité en rendant difficile l'accès non autorisé. L'OTP est souvent utilisé dans le cadre de l'authentification à deux facteurs (2FA), où un code généré par une application comme Google Authenticator est requis en plus du mot de passe traditionnel. Cela ajoute une couche supplémentaire de sécurité en vérifiant non seulement ce que vous savez (le mot de passe), mais aussi ce que vous avez (le code OTP).

Installation de Cockpit et de libpam-google-authenticator :

```
sudo apt install -y cockpit libpam-google-authenticator
```

Flashez le QR code avec Google Authenticator après avoir exécuté cette commande :

```
google-authenticator -t -f -d -w 3 -e 10 -r 3 -R 30
```

Copiez vos paramètres 2FA dans un endroit sûr :

```
cat .google_authenticator
```

Explication des options :

- **-t** : Activer la vérification TOTP (Time-based One-Time Password).
- **-f** : Écrire la configuration dans le fichier `~/.google_authenticator`.
- **-d** : Interdire la réutilisation des jetons précédemment utilisés.
- **-w 3** : Définir la taille de la fenêtre des jetons autorisés. Par défaut, les jetons expirent toutes les 30 secondes. Une fenêtre de taille 3 permet l'authentification avec le jeton précédent et le jeton suivant pour compenser un éventuel décalage horaire.
- **-e 10** : Générer 10 codes de secours d'urgence.
- **-r 3 -R 30** : Limiter le taux de connexion. Autoriser 3 tentatives de connexion toutes les 30 secondes.

Ajoutez à la fin du fichier `/etc/pam.d/cockpit`. L'option `nullok` permet aux utilisateurs qui n'ont pas encore généré de code 2FA de se connecter, tandis que les codes sont requis si l'utilisateur a suivi l'étape 2 ci-dessus. Cette option est utile lors du déploiement. Une fois que tous les utilisateurs auront généré des codes, vous pourrez supprimer l'option `nullok` pour exiger la 2FA pour tous. :

```
echo 'auth required pam_google_authenticator.so nullok' | sudo tee -a /etc/pam.d/cockpit
```

Redémarrez le service cockpit :

```
sudo systemctl restart cockpit
```

Configurez SSH pour utiliser l'OTP

Modifiez le fichier de configuration PAM SSH :

```
sudo nano /etc/pam.d/sshd
```

Ajoutez la ligne suivante à la fin du fichier. L'option `nullok` permet aux utilisateurs qui n'ont pas encore généré de code 2FA de se connecter, tandis que les codes sont requis si l'utilisateur a suivi l'étape 2 ci-dessus. Cette option est utile lors du déploiement. Une fois que tous les utilisateurs auront généré des codes, vous pourrez supprimer l'option `nullok` pour exiger la 2FA pour tous.

```
auth required pam_google_authenticator.so nullok
```

Enregistrez et fermez le fichier.

Modifiez le fichier de configuration du démon SSH :

```
sudo nano /etc/ssh/sshd_config
```

Vérifiez que les options suivantes sont définies comme indiqué, ou ajoutez-les si elles n'existent pas :

```
KbdInteractiveAuthentication yes
ChallengeResponseAuthentication yes
X11Forwarding no
UsePAM yes
```

Enregistrez et fermez le fichier.

3. Redémarrez le service SSH.

```
sudo systemctl restart ssh
```

Accès

Accédez à la page d'administration via le navigateur web :

```
adresseipduserveur:9090
```

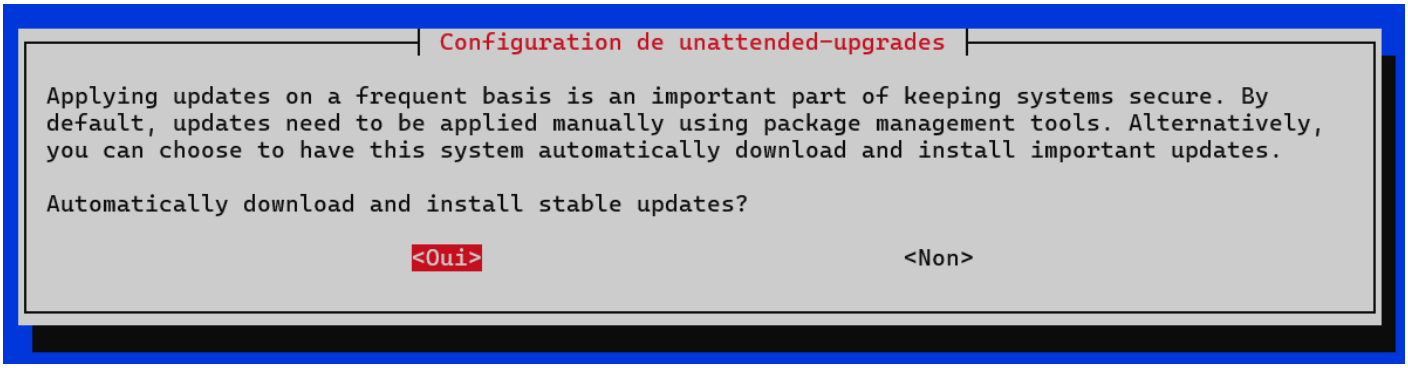
Désactivez le serveur SSH dans les services lorsque vous n'en avez pas besoin.

Mise à jour des paquets de sécurité

Activez les mises à jour automatiques à l'aide de la commande suivante, qui vous demandera si vous souhaitez activer les mises à jour automatiques. Sélectionnez Oui et appuyez sur Entrée, ce qui confirmera que le service unattended-upgrades est actif et prêt à gérer les mises à jour pour vous.

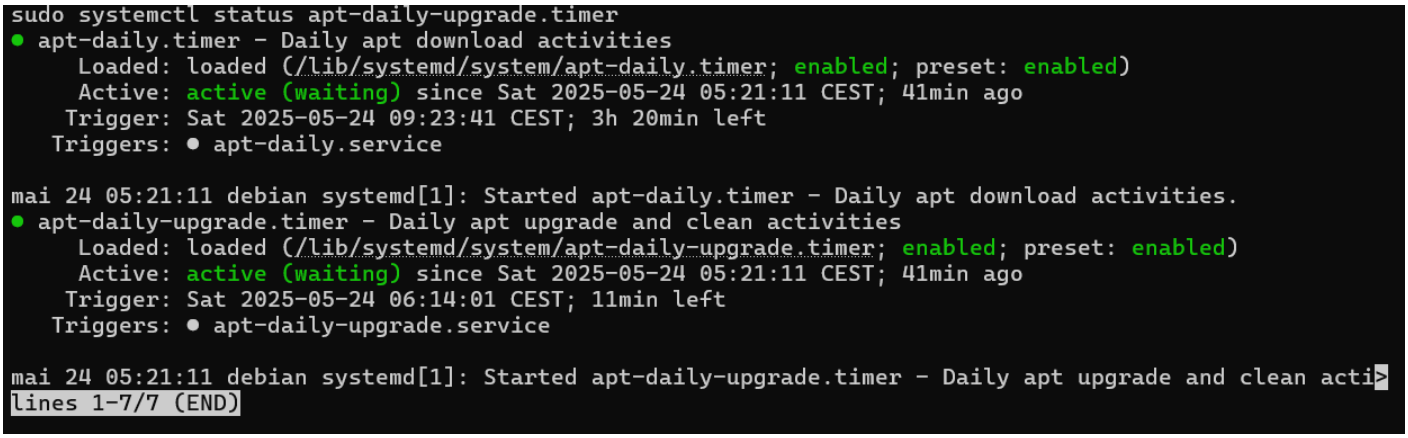
```
sudo apt install -y unattended-upgrades
```

```
sudo dpkg-reconfigure unattended-upgrades
```



Par défaut, unattended-upgrades fonctionne tous les jours, pour vérifier ou modifier l'horaire, vérifiez la minuterie systemd :

```
sudo systemctl status apt-daily.timer
sudo systemctl status apt-daily-upgrade.timer
```



Pour vous assurer que tout fonctionne, simulez une mise à niveau sans surveillance. Si vous venez de faire une nouvelle installation ou si vous aviez déjà mis à jour récemment le système, vous ne devriez pas avoir de réponse :


```
sudo unattended-upgrade --dry-run
```

Activez les redémarrages automatiques après les mises à jour du noyau en ajoutant cette ligne :

```
echo 'Unattended-Upgrade::Automatic-Reboot "true";' | sudo tee -a
/etc/apt/apt.conf.d/50unattended-upgrades
```

Vous pouvez également planifier des redémarrages à un moment précis :

```
echo 'Unattended-Upgrade::Automatic-Reboot-Time "02:00";' | sudo tee -a
/etc/apt/apt.conf.d/50unattended-upgrades
```

Vous pouvez surveiller les mises à jour automatiques en vérifiant les journaux :

```
sudo less /var/log/unattended-upgrades/unattended-upgrades.log
```

Planification des migrations vers Debian 13 et versions suivantes

Il est important de noter dans votre agenda la future migration vers Debian 13, ainsi que vers les versions suivantes, afin de toujours bénéficier des mises à jour de sécurité officielles. Debian maintient un cycle de support défini pour chaque version stable, généralement d'environ 5 ans, comprenant le support principal (security updates) et le support LTS (Long Term Support). Passé ces périodes, aucune mise à jour de sécurité n'est fournie, ce qui expose votre système à des risques importants.

Version Debian	Date de sortie	Fin du support standard	Fin du support LTS
Debian 11 (Bullseye)	14/08/2021	30/06/2024	30/06/2026
Debian 12 (Bookworm)	10/06/2023	10/06/2026	-
Debian 13 (Trixie) (prévue)	Mi-2026 (prévision)	Mi-2029 (prévision)	-

Conseils :

- Planifiez vos mises à jour majeures avant la fin du support standard pour éviter toute interruption de sécurité.
- Mettez un rappel périodique dans votre agenda pour suivre les annonces de Debian et les dates officielles.
- Faites systématiquement des sauvegardes complètes avant toute migration pour pouvoir revenir en arrière en cas de problème.
- Testez soigneusement vos systèmes avant la migration pour garantir la compatibilité des services critiques.

Installation du par-feu

Installez `iptables` :

```
sudo apt install iptables
```

Configuration des règles `iptables`

1. **Ouvrez les ports 22 et 9090 :**

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 9090 -j ACCEPT
```

2. **Enregistrez les règles pour qu'elles soient persistantes après un redémarrage :**

```
sudo apt install iptables-persistent
sudo netfilter-persistent save
```

Pour vérifier que les règles ont été appliquées correctement, utilisez la commande suivante :

```
sudo iptables -L -v
```

Pour ouvrir un port spécifique (par exemple, le port 8080) :

```
sudo iptables -A INPUT -p tcp --dport 8080 -j ACCEPT
sudo netfilter-persistent save
```

Pour fermer un port spécifique (par exemple, le port 8080) :

```
sudo iptables -D INPUT -p tcp --dport 8080 -j ACCEPT
sudo netfilter-persistent save
```

Explication des commandes

- `iptables -A INPUT -p tcp --dport <port> -j ACCEPT` : Ajoute une règle pour accepter les connexions entrantes sur le port spécifié.
- `iptables -D INPUT -p tcp --dport <port> -j ACCEPT` : Supprime la règle pour accepter les connexions entrantes sur le port spécifié.
- `netfilter-persistent save` : Enregistre les règles actuelles pour qu'elles soient appliquées automatiquement au démarrage.

Installation de CrowdSec pour bloquer les IP malveillantes

Prérequis :

- iptables

CrowdSec est une solution open-source de sécurité qui protège les serveurs et les applications contre les attaques malveillantes en analysant les journaux et en détectant les comportements

suspects. En utilisant des règles de détection et des listes de réputation, CrowdSec peut bloquer automatiquement les adresses IP malveillantes, partager ces informations avec une communauté mondiale, et ainsi améliorer collectivement la sécurité de tous les utilisateurs. Il s'intègre facilement avec divers services et plateformes, offrant une protection proactive et collaborative contre les cybermenaces.

```
sudo apt install -y curl && curl -s
https://packagecloud.io/install/repositories/crowdsec/crowdsec/script.deb.sh | sudo bash
```

```
sudo apt install -y crowdsec crowdsec-firewall-bouncer-iptables
```

Description des paquets :

- **crowdsec** : CrowdSec est une solution de sécurité open-source qui aide à détecter et à bloquer les comportements malveillants en temps réel. Elle fonctionne en analysant les journaux (logs) pour identifier les comportements suspects et en prenant des mesures appropriées.
- **crowdsec-firewall-bouncer-iptables** : Ce paquet est un "bouncer" pour CrowdSec qui utilise iptables (une interface pour Netfilter, le pare-feu Linux) pour bloquer les adresses IP identifiées comme malveillantes par CrowdSec. Un "bouncer" est un composant qui applique les règles de blocage définies par CrowdSec.

```
sudo systemctl reload crowdsec
```

Redémarrez le système :

```
sudo reboot
```

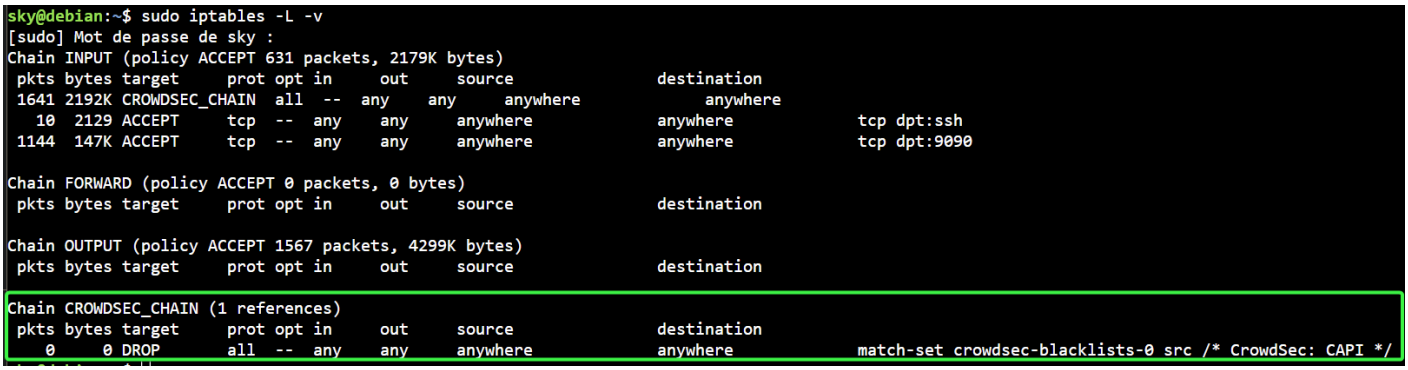
Vérifiez si le service et les règles de par-feu est lancez et fonctionne correctement :

```
sudo systemctl status crowdsec
```

```
sky@debian:~$ sudo systemctl status crowdsec
● crowdsec.service - Crowdsec agent
     Loaded: loaded (/lib/systemd/system/crowdsec.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-05-24 09:22:58 CEST; 2min 55s ago
   Main PID: 3043 (crowdsec)
      Tasks: 7 (limit: 2311)
     Memory: 43.5M
        CPU: 1.526s
     CGroup: /system.slice/crowdsec.service
             ├─3043 /usr/bin/crowdsec -c /etc/crowdsec/config.yaml
             └─3049 journalctl --follow -n 0 _SYSTEMD_UNIT=ssh.service

mai 24 09:22:54 debian systemd[1]: Starting crowdsec.service - Crowdsec agent...
mai 24 09:22:58 debian systemd[1]: Started crowdsec.service - Crowdsec agent.
```

```
sudo iptables -L -v
```



Documentation complémentaire

- Cockpit
- CrowdSec

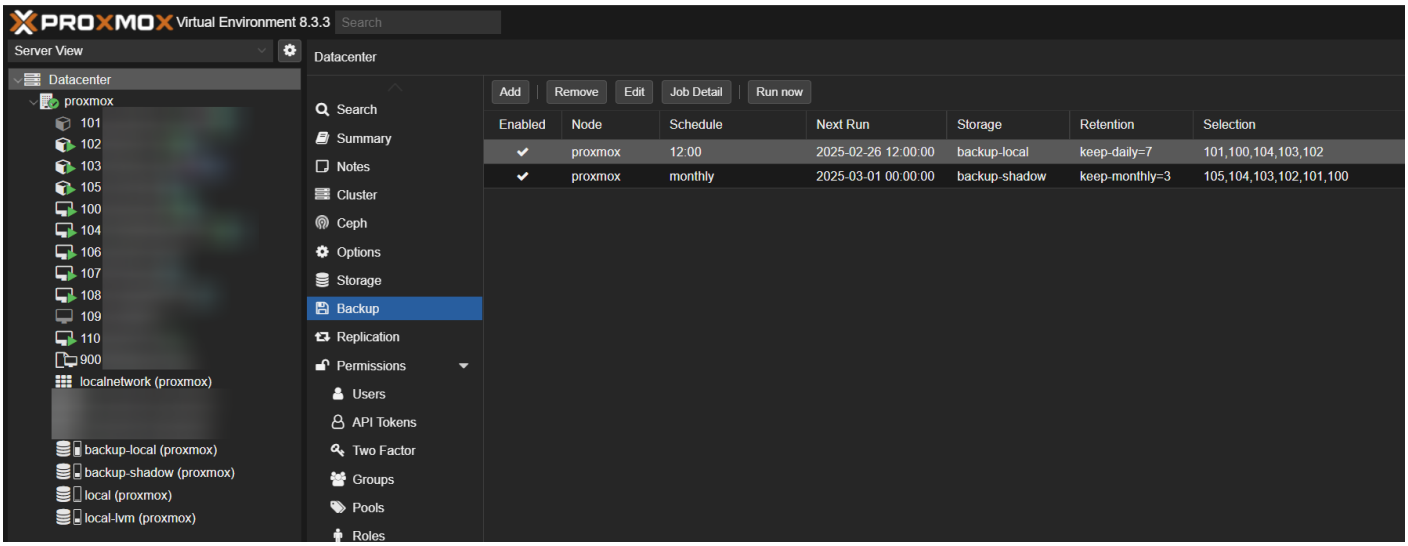
Méthode de sauvegarde

Méthode 3-2-1

La méthode de sauvegarde que j'utilise est basée sur le principe 3-2-1, qui est considéré comme une bonne pratique en matière de sauvegarde des données. J'ai 3 copies de mes données, stockées sur 2 types de supports différents, avec 1 copie hors site.

Ma méthode de sauvegarde :

1. **Sauvegardes quotidiennes :**
   - Les sauvegardes des serveurs, VM/VPS et configurations sont effectuées quotidiennement par l'utilisateur root.
   - Ces sauvegardes sont conservées pendant 7 jours.
   - Elles sont transférées sur le NAS et stockées à la fois sur la machine source et le NAS, puis synchronisées sur Scaleway.
2. **Sauvegardes mensuelles :**
   - Les sauvegardes des serveurs et VM/VPS sont effectuées le premier jour de chaque mois.
   - Ces sauvegardes sont conservées pendant 3 mois.
   - Elles sont directement stockées sur le NAS ou transférées après leur création, puis synchronisées sur Scaleway.
3. **Sauvegardes manuelles :**
   - Deux copies des sauvegardes des serveurs, des dossiers personnels (photos/vidéos) et des VM/VPS sont effectuées manuellement tous les trois ou six mois.
   - Ces sauvegardes sont stockées sur un ou deux disques durs externes, qui sont connectés uniquement pour le transfert.
4. **Sauvegarde Proxmox :**
   - Sur Proxmox, j'utilise l'interface graphique pour effectuer des sauvegardes quotidiennes des VMs et des conteneurs. Ces sauvegardes sont conservées pendant 7 jours sur le stockage local de Proxmox.
   - Les sauvegardes mensuelles sont ensuite transférées directement sur le NAS avec le point de montage NFS.



Vous pouvez trouver plus d'informations sur la [sauvegarde Proxmox dans la documentation officielle](#).

Synchronisation des fichiers personnels

Mes photos, vidéos, clés SSH, sauvegardes de jeux, documents personnels et gestionnaire de mots de passe sont synchronisés sur mon ordinateur portable, mon téléphone et mon PC fixe. Cela signifie que j'ai à tout moment ces fichiers synchronisés avec **Syncthing**. Sur Proxmox, j'ai un serveur Syncthing qui est lui-même sauvegardé selon les méthodes 1, 2 et 3 mentionnées précédemment.

Transfert des sauvegardes avec rclone

Pour le transfert des sauvegardes, j'utilise l'outil en ligne de commande **rclone**. Rclone est compatible avec de nombreux services de stockage tels que SFTP, Google Drive, Dropbox, Amazon S3, Scaleway, Proton Drive et bien d'autres. Cela me permet de gérer facilement les différents stockages et de synchroniser les données de manière efficace.

Chiffrement des sauvegardes avec rclone

Rclone offre une fonctionnalité de chiffrement intégrée appelée "crypt", qui me permet de chiffrer les fichiers uniquement sur le stockage distant (Scaleway, dans notre cas), sans avoir à les chiffrer localement. Ainsi, mes données sont sécurisées sur le service de stockage, mais restent lisibles sur mon système local. Lorsque je souhaite accéder à ces sauvegardes, je les déchiffre et les

télécharge en utilisant rclone avec ce fichier de configuration.

Tester les sauvegardes

Il est essentiel de tester régulièrement la restauration de vos sauvegardes pour vous assurer qu'elles sont fonctionnelles et que vous pouvez bien récupérer vos données en cas de besoin. Cela vous permettra d'identifier d'éventuels problèmes et de prendre les mesures correctives nécessaires.

Je recommande de tester la restauration de vos sauvegardes au moins une fois par trimestre. Choisissez des fichiers ou des données représentatifs, restaurez-les et vérifiez qu'ils sont bien récupérés et utilisables. Cette étape est cruciale pour garantir la fiabilité de votre système de sauvegarde.

Sécurité des transferts

Pour sécuriser les transferts de sauvegardes vers le NAS, il est important d'ouvrir les ports nécessaires sur le pare-feu et de mettre en place une liste blanche des adresses IP autorisées à se connecter. De plus, il est recommandé de créer un utilisateur dédié pour chaque machine qui a les droits d'accès spécifiques à son dossier de sauvegarde sur le NAS.

Cela permet de limiter les risques d'accès non autorisés et de garantir la confidentialité des données sauvegardées. Il est également important de s'assurer que les communications entre les machines et le NAS soient chiffrées (SSH, SFTP, etc.).

Stockage externe

Kdrive ou Swiss Backup

Il existe également la solution Kdrive ou Swiss Backup que vous pouvez utiliser. Il est possible de monter le disque sur votre ordinateur via le protocole WebDAV ou avec Rclone. Il faut découper les fichiers en blocs de moins de 50 gigaoctets avec Rclone, puis ces blocs seront automatiquement reconstitués lors du téléchargement.

Scaleway Cold Storage

Pour le stockage externe à long terme, j'utilise le service de stockage froid (Cold Storage) de Scaleway. Mes données sont stockées dans un abri sous-terrain sécurisé à un coût très abordable

de 0,002 € par gigaoctet et par mois. Cela me permet de conserver des copies de mes sauvegardes les plus importantes à un faible coût tout en bénéficiant d'un stockage sécurisé et durable.

Exemple de script Bash pour sauvegarder des dossiers

Voici un exemple de script Bash qui permet de sauvegarder des dossiers de manière automatique. Vous pouvez commenter avec `#` ce qui ne vous convient pas :

```
#!/bin/bash

# Description
# Ce script effectue une sauvegarde quotidienne des dossiers spécifiés.
# Les sauvegardes sont conservées pendant 7 jours et transférées sur le NAS.
# Le script est exécuté via une tâche cron tous les jours à 2h du matin.

# Dossiers à sauvegarder
BACKUP_DIRS=("/home/user/documents" "/home/user/photos" "/etc/config")

# Destination des sauvegardes
BACKUP_DEST="/mnt/nas/backups"

# Nombre de jours de conservation
RETENTION_DAYS=7

# Exécution de la sauvegarde
for dir in "${BACKUP_DIRS[@]}"; do
    filename="$(basename "$dir")_$(date +%Y-%m-%d).tar.gz"
    tar -czf "$BACKUP_DEST/$filename" "$dir"

    # Création du fichier de checksum SHA-256
    sha256sum "$BACKUP_DEST/$filename" > "$BACKUP_DEST/$filename.sha256"
done

# Suppression des sauvegardes obsolètes
find "$BACKUP_DEST" -type f -mtime +$RETENTION_DAYS -delete
```

```
# Synchronisation des sauvegardes sur Scaleway
rclone sync "$BACKUP_DEST" remote:backups

# Fin du script
echo "Sauvegarde terminée."

# Pour vérifier le checksum d'un fichier de sauvegarde, utilisez la commande suivante :
# sha256sum -c "$BACKUP_DEST/nom_du_fichier.tar.gz.sha256"
# Remplacez "nom_du_fichier" par le nom de votre fichier de sauvegarde.
```

Sans compression/suppression/syncronisation :

```
#!/bin/bash

# Description
# Ce script effectue une sauvegarde des dossiers spécifiés.

# Dossiers à sauvegarder
BACKUP_DIRS=("/home/user/documents" "/home/user/photos" "/etc/config")

# Destination des sauvegardes
BACKUP_DEST="/mnt/nas/backups"

# Exécution de la sauvegarde
for dir in "${BACKUP_DIRS[@]}"; do
    filename="$(basename "$dir")_$(date +%Y-%m-%d).tar"
    tar -cf "$BACKUP_DEST/$filename" "$dir"

    # Création du fichier de checksum SHA-256
    sha256sum "$BACKUP_DEST/$filename" > "$BACKUP_DEST/$filename.sha256"
done

# Fin du script
echo "Sauvegarde terminée."

# Pour vérifier le checksum d'un fichier de sauvegarde, utilisez la commande suivante :
# sha256sum -c "$BACKUP_DEST/nom_du_fichier.tar.sha256"
# Remplacez "nom_du_fichier" par le nom de votre fichier de sauvegarde.
```

Utilisation avec Crontab : Pour exécuter ce script automatiquement tous les jours à 2h du matin, ajoutez la ligne suivante à votre fichier Crontab (crontab -e) :

```
0 2 * * * /chemin/vers/votre/script.sh
```

Cela permettra d'effectuer les sauvegardes quotidiennes de manière régulière.

Exemple de crontab avec Rclone

Voici un exemple de script crontab qui permet de transférer les sauvegardes vers Scaleway de mes sauvegardes Proxmox :

```
0 2 * * * rclone sync /mnt/backupHDD/dump crypt_scaleway_sauvegarde_proxmox:/1semaines --verbose --log-file=/mnt/backupHDD/rclone_sauvegarde_proxmox.txt
0 3 1 * * rclone sync /mnt/pve/backup-shadow/dump crypt_scaleway_sauvegarde_proxmox:/3mois --verbose --log-file=/mnt/pve/backup-shadow//rclone_sauvegarde_proxmox.txt
```

Fichier de configuration rclone

Rclone offre une fonctionnalité de chiffrement intégrée appelée "crypt", qui me permet de chiffrer les fichiers uniquement sur le stockage distant (Scaleway, dans notre cas), sans avoir à les chiffrer localement. Ainsi, mes données sont sécurisées sur le service de stockage, mais restent lisibles sur mon système local. Lorsque je souhaite accéder à ces sauvegardes, je les déchiffre et les télécharge en utilisant rclone avec ce fichier de configuration.

Rclone se charge de générer les mots de passe nécessaires au chiffrement et au déchiffrement des données lors de la configuration du remote "crypt". Vous pouvez alors sauvegarder ce fichier de configuration rclone.conf et le transférer sur d'autres machines si nécessaire, afin d'accéder à vos sauvegardes chiffrées depuis différents endroits.

Le fichier de configuration rclone.conf est généralement placé dans l'un des emplacements suivants :

- Sur Linux/Unix : `~/.config/rclone/rclone.conf` (répertoire personnel de l'utilisateur)
- Sur Windows : `%USERPROFILE%\.config\rclone\rclone.conf` (répertoire personnel de l'utilisateur)
- Sur macOS : `~/Library/Application Support/rclone/rclone.conf` (répertoire personnel de l'utilisateur)

Vous pouvez également le placer à un emplacement de votre choix, mais vous devrez alors spécifier le chemin complet lors de l'utilisation de rclone.

Les principaux paramètres à configurer sont :

- `access_key_id` et `secret_access_key` : à remplacer par vos propres identifiants Scaleway.

- `region = fr-par` : région de stockage en France.
- `storage_class = GLACIER` : utilisation du stockage froid Glacier.
- `password` et `password2` : à remplacer par vos propres mots de passe forts pour le chiffrement.

Lorsque je souhaite accéder à ces sauvegardes, je les déchiffre et les télécharge en utilisant rclone avec ce fichier de configuration.

Exemple de commande pour télécharger les sauvegardes chiffrées

```
rclone ls crypt_scaleway:backups
rclone cat crypt_scaleway:backups/filename.tar.gz | tar xzf -
```

Explications :

1. `rclone ls crypt_scaleway:backups` : Cette commande liste le contenu du dossier "backups" sur le remote "crypt_scaleway". Cela vous permet de voir quels fichiers sont présents.
2. `rclone cat crypt_scaleway:backups/filename.tar.gz | tar xzf -` : Cette commande télécharge le fichier "filename.tar.gz" depuis le dossier "backups" du remote "crypt_scaleway", le déchiffre automatiquement, puis l'extrait dans le répertoire courant.

Le remote "crypt_scaleway" fait référence à la section `[crypt]` de votre fichier de configuration rclone. Il permet d'accéder aux fichiers chiffrés sur le stockage Scaleway.

Assurez-vous d'avoir correctement configuré les paramètres de chiffrement (mot de passe, etc.) dans votre fichier de configuration rclone.conf avant d'exécuter ces commandes.

Passage de la classe de stockage Glacier vers Standard

Lorsque vous avez des fichiers stockés dans la classe de stockage Glacier de Scaleway, vous pouvez changer leur classe de stockage individuellement via la console Scaleway. Cependant, si vous avez de nombreux fichiers à restaurer, cette méthode peut s'avérer fastidieuse.

Les scripts ci-dessous vous permettent de gérer de manière automatisée le passage de la classe Glacier vers la classe Standard pour l'ensemble des fichiers dans un ou plusieurs dossiers. Avant d'utiliser ces scripts, vous devez configurer l'AWS CLI pour accéder à votre compte Scaleway, en suivant la documentation officielle.

Vous pouvez télécharger les scripts ci-joint.

Liste des objets stockés en Glacier

Le script `list-glacier-objects.sh` vous permet de lister tous les objets stockés dans la classe Glacier d'un bucket Scaleway spécifique, avec la possibilité de filtrer par répertoire.

```
./list-glacier-objects.sh my-bucket my-directory
```

Cela générera un fichier texte contenant la liste des objets à restaurer.

Restauration des objets Glacier

Le script `update_class_standard.sh` lit la liste des objets générée précédemment et initie la restauration de ces objets depuis Glacier vers la classe de stockage Standard. Il vérifie au préalable que l'objet est bien encore en Glacier et qu'aucune restauration n'est en cours.

```
./update_class_standard.sh my-bucket object-list.txt 3
```

Cela restaurera les objets pendant 3 jours dans la classe Standard.

Liste des fichiers restaurés

Enfin, le script `list-file-bucket.sh` vous permet de lister tous les objets d'un bucket Scaleway, y compris ceux qui ont été restaurés depuis Glacier.

```
./list-file-bucket.sh my-bucket my-directory
```

Cela vous permet de vérifier que la restauration s'est bien déroulée.

Pour réaliser les scripts, je me suis basé sur la documentation officielle de Scaleway.

Configuration d'un accès SFTP restreint au répertoire chroot

Ce guide décrit comment configurer un environnement chroot avec un accès SFTP uniquement pour les utilisateurs, en utilisant des clés SSH.

Prérequis

- Un serveur exécutant GNU/Linux
- Un accès root au serveur
- OpenSSH installé et en cours d'exécution

Étapes

1. Créer un utilisateur chroot

```
adduser <nom_d'utilisateur>
```

2. Créer un groupe SFTP

```
groupadd sftpusers
```

3. Ajouter l'utilisateur au groupe SFTP

```
usermod -aG sftpusers <nom_d'utilisateur>
```

4. Configurer le répertoire chroot

Créer un répertoire pour les utilisateurs SFTP, en s'assurant que les droits de propriété et les autorisations sont configurés correctement.

```
mkdir -p /sftp/<nom_d'utilisateur>
chown root:root /sftp
chmod 755 /sftp
mkdir /sftp/<nom_d'utilisateur>
chown <nom_d'utilisateur>:<nom_d'utilisateur> /sftp/<nom_d'utilisateur>
chmod 700 /sftp/<nom_d'utilisateur>
```

5. Configurer SSH pour l'accès SFTP

Modifier le fichier `/etc/ssh/sshd_config` pour utiliser SFTP interne et définir les restrictions.

1. Mettre à jour la ligne `Subsystem` :

   ```
   Subsystem sftp internal-sftp
   ```

2. Ajouter un bloc `Match` à la fin :

   ```
   Match Group sftpusers
       ChrootDirectory /sftp/%u
       ForceCommand internal-sftp
       AllowTcpForwarding no
       X11Forwarding no
   ```

6. Configurer les clés SSH de l'utilisateur

Créer et configurer les répertoires SSH pour l'utilisateur :

```
mkdir /home/<nom_d'utilisateur>/.ssh
touch /home/<nom_d'utilisateur>/.ssh/authorized_keys
chmod 700 /home/<nom_d'utilisateur>/.ssh
chmod 600 /home/<nom_d'utilisateur>/.ssh/authorized_keys
chown <nom_d'utilisateur>:<nom_d'utilisateur> /home/<nom_d'utilisateur>/.ssh
chown <nom_d'utilisateur>:<nom_d'utilisateur> /home/<nom_d'utilisateur>/.ssh/authorized_keys
```

Copier la clé publique SSH dans `/home/<nom_d'utilisateur>/.ssh/authorized_keys`.

7. Redémarrer le service SSH

```
systemctl restart sshd
```

Vérification

- Essayez une connexion SFTP pour vérifier que l'accès est restreint.
- Assurez-vous que les utilisateurs ne peuvent pas accéder au shell.

Script qui automatise la configuration :

```
#!/bin/bash

# Ce script configure automatiquement un environnement chroot pour un utilisateur SFTP dans le répertoire /sftp.
# Il crée un utilisateur avec un accès SFTP restreint, met en place la structure de répertoires nécessaire,
# configure les autorisations et ajoute un fichier authorized_keys pour l'authentification par clé.

# Utilisation :
# Enregistrez ce script sous le nom "sftp_chroot.sh" et rendez-le exécutable en exécutant la commande : `chmod +x sftp_chroot.sh`.
# Ensuite, exécutez-le avec les privilèges root en utilisant : `sudo ./sftp_chroot.sh`.
# Le script vous demandera le nom d'utilisateur SFTP, configurera l'environnement chroot nécessaire, définira les autorisations,
# et appliquera les paramètres SSH pour restreindre l'utilisateur à l'accès SFTP uniquement. Enfin, il redémarrera le service SSH pour
# appliquer les modifications.

# Vérifier si le script est exécuté avec les privilèges root
if [[ $EUID -ne 0 ]]; then
    echo "Ce script doit être exécuté en tant que root."
    exit 1
fi

# Demander le nom d'utilisateur SFTP
read -p "Entrez le nom d'utilisateur SFTP : " USERNAME

# Créer l'utilisateur avec le shell /bin/false pour limiter l'accès
useradd -m -d /sftp/$USERNAME -s /bin/false $USERNAME
```

```
# Créer l'environnement chroot dans /sftp
mkdir -p /sftp/$USERNAME
mkdir -p /sftp/$USERNAME/upload
mkdir -p /sftp/$USERNAME/.ssh

# Définir les autorisations pour le répertoire chroot
chown root:root /sftp/$USERNAME
chmod 755 /sftp/$USERNAME
chown $USERNAME:$USERNAME /sftp/$USERNAME/upload

# Créer le fichier authorized_keys
touch /sftp/$USERNAME/.ssh/authorized_keys
chmod 700 /sftp/$USERNAME/.ssh
chmod 600 /sftp/$USERNAME/.ssh/authorized_keys
chown -R $USERNAME:$USERNAME /sftp/$USERNAME/.ssh

echo "L'utilisateur $USERNAME a été configuré avec succès dans un environnement chroot."

# Ajouter la configuration SFTP à sshd_config si nécessaire
if ! grep -q "Match User $USERNAME" /etc/ssh/sshd_config; then
    echo -e "\n# Configuration SFTP pour $USERNAME" >> /etc/ssh/sshd_config
    echo "Match User $USERNAME" >> /etc/ssh/sshd_config
    echo "    ChrootDirectory /sftp/$USERNAME" >> /etc/ssh/sshd_config
    echo "    ForceCommand internal-sftp" >> /etc/ssh/sshd_config
    echo "    AllowTcpForwarding no" >> /etc/ssh/sshd_config
    echo "    PermitTunnel no" >> /etc/ssh/sshd_config
fi

# Redémarrer le service SSH
systemctl restart ssh

echo "Le jail chroot pour $USERNAME a été configuré avec succès. Vous pouvez maintenant
ajouter les clés SSH dans /sftp/$USERNAME/.ssh/authorized_keys"
```

Guide de validation des disques durs avant mise en production

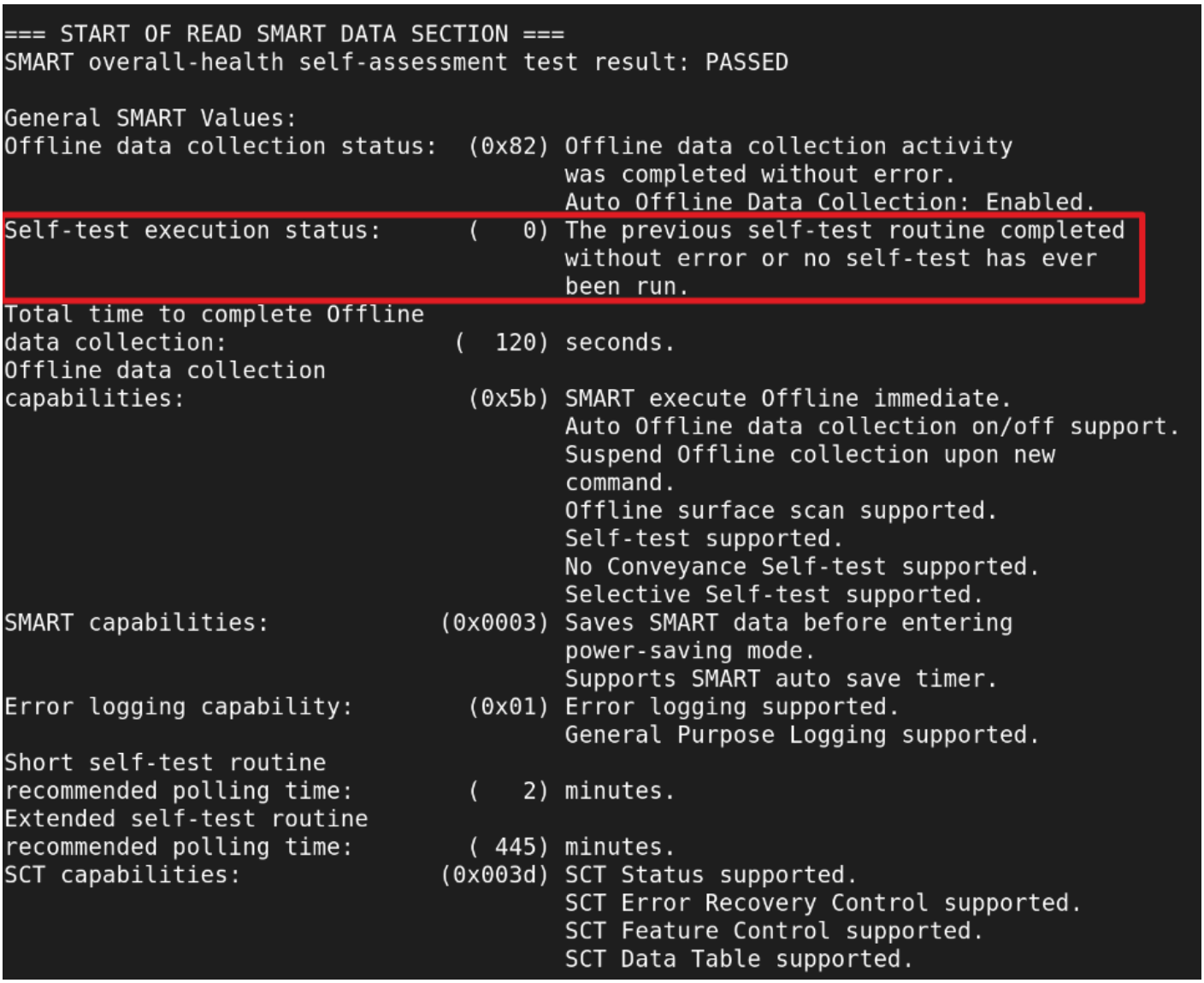
Première étape : Tests S.M.A.R.T.

S.M.A.R.T. (**Self-Monitoring, Analysis and Reporting Technology** / **Technologie d'auto-surveillance, d'analyse et de rapport**) est un système de surveillance intégré aux disques durs qui détecte et signale divers indicateurs de fiabilité dans le but de prévoir les défaillances matérielles.

Nous utiliserons `smartmontools` pour cette étape afin d'obtenir l'état du disque dur avant de le soumettre au test de stress. Le paquet dont vous aurez besoin d'installer s'appelle smartmontools :

Vous pouvez suivre la progression de n'importe lequel des tests suivants avec cette commande : `smartctl -a /dev/sdX`

La progression (en pourcentage) du test se trouve sur la ligne `Self-test execution status:`



La valeur zéro (`0`) signifie que notre test est terminé ou qu'aucun test n'est en cours d'exécution. Vous pouvez toujours interrompre un test avec `smartctl -X /dev/sdX`

> Remplacez X par la lettre de votre lecteur

Test court

Le test **court** effectue un diagnostic rapide des composants essentiels du disque (électronique, têtes de lecture, secteurs critiques).

`smartctl -t short /dev/sdX`

Environ 2 minutes pour un disque dur de 4 To.

Test de transport

Le test de **transport** détecte les dommages survenus pendant l'expédition (chocs, vibrations). Recommandé pour les disques neufs.

`smartctl -t conveyance /dev/sdX`

Environ 5 minutes pour un disque dur de 4 To.

Test long

Le test **long** analyse l'intégralité de la surface du disque, secteur par secteur. C'est le test le plus complet.

`smartctl -t long /dev/sdX`

Environ 500 minutes pour un disque dur de 4 To. Ce test peut prendre beaucoup de temps, selon la taille de votre disque dur.

Deuxième étape : Mise sous contrainte du disque dur

Préparation

Cette étape doit être effectuée via SSH, en utilisant `tmux`. Cela permettra de maintenir le test en cours même si la connexion est perdue. Activez le service `SSH` sur `TrueNAS` (Paramètres système -> Services -> SSH)

Test de stress

Cette commande vérifie l'intégrité physique d'un disque en écrivant et lisant des motifs de test sur tous ses secteurs pour détecter les blocs défectueux avant de l'utiliser ou après un doute sur sa fiabilité.

```
sudo badblocks -b 4096 -wvs /dev/sdX
```

`-b` définit la taille de bloc `-w` effectue un test destructif, ce qui signifie qu'il **SUPPRIMERA** toutes les données présentes sur ce disque `-v` affiche les informations détaillées `-s` affiche la progression

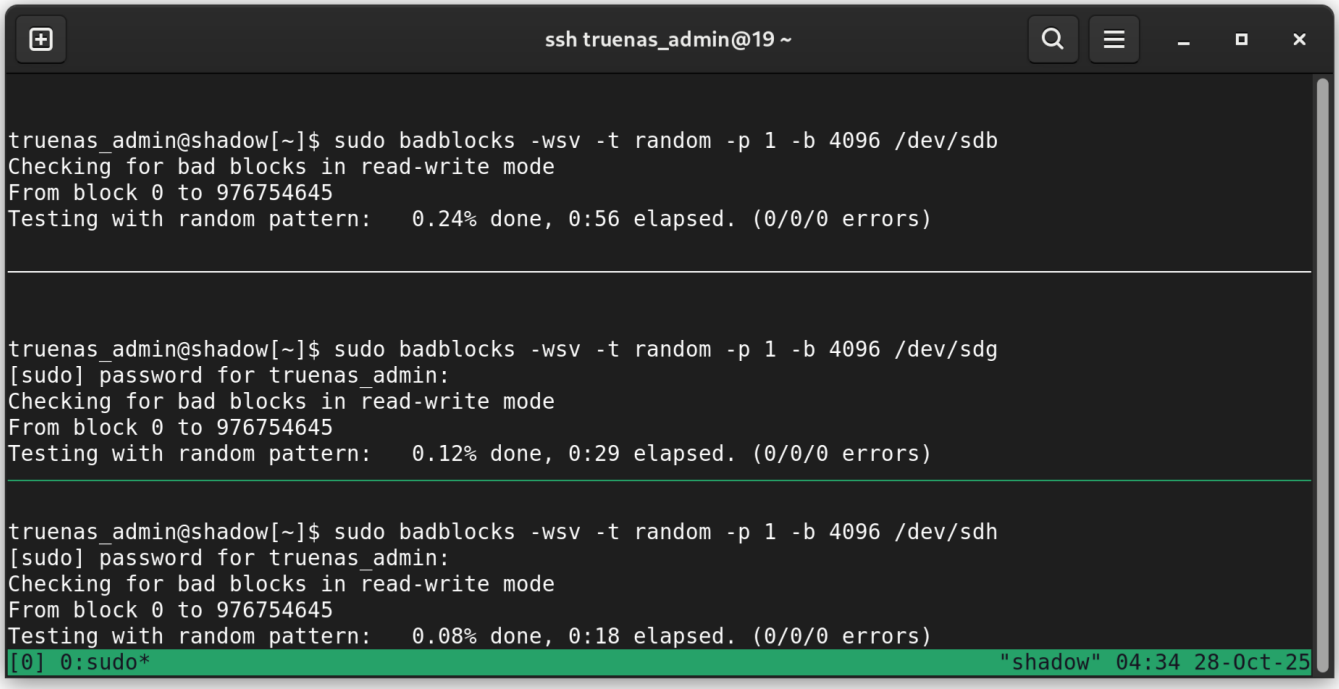
`badblocks` effectue `4` passes :

```
- Première passe : test avec le motif 0xaa (10101010)
- Puis lecture et comparaison
- Deuxième passe : test avec le motif 0x55 (01010101)
- Puis lecture et comparaison
- Troisième passe : test avec le motif 0xff (11111111)
- Puis lecture et comparaison
- Quatrième passe : test avec le motif 0x00 (00000000)
- Puis lecture et comparaison
```

Si vous voulez tester en une seule passe :

```
sudo badblocks -wsv -t random -p 1 /dev/sdX
```

Pour lancer le test sur d'autres disques durs, appuyez sur Ctrl + B puis sur ", cela divisera l'écran, vous pourrez alors exécuter `badblocks` sur le disque suivant. Vous pouvez diviser l'écran autant de fois que vous le souhaitez.



Après avoir lancé badblocks pour tous vos disques durs, vous pouvez laisser la connexion SSH ouverte ou la fermer. Pour vous reconnecter plus tard, reconnectez-vous en SSH à TrueNAS et exécutez `tmux attach`

Exemple de résultat de `badblocks` pour des disques durs en bon état :

```
truenas# badblocks -b 4096 -wvs /dev/sda
Checking for bad blocks in read-write mode
```

```
From block 0 to 976754645
Testing with pattern 0xaa: done
Reading and comparing: done
Testing with pattern 0x55: done
Reading and comparing: done
Testing with pattern 0xff: done
Reading and comparing: done
Testing with pattern 0x00: done
Reading and comparing: done
Pass completed, 0 bad blocks found. (0/0/0 errors)
```

Troisième étape : Résultats

Une fois le test de stress `badblocks` terminé, nous devons effectuer un autre test `long` sur chaque disque dur pour vérifier qu'aucun problème n'est apparu suite au stress intensif.

`smartctl -t long /dev/sdX`

Une fois le test `long` terminé, il est temps d'obtenir nos résultats. Nous les obtenons avec cette commande :

`smartctl -A /dev/sdX` (Notez le `A` majuscule)

Les champs importants sont les lignes `Reallocated_Sector_Ct`, `Current_Pending_Sector` et `Offline_Uncorrectable`. Toutes ces valeurs doivent avoir une `RAW_VALUE` de `0`, même si le champ `VALUE` affiche `200`. Tout résultat supérieur à `0` devrait être une raison de demander un RMA.

Résultat de `smartctl -A /dev/sdX` pour des disques durs en bon état :

```
truenas_admin@shadow[~]$ sudo smartctl -A /dev/sdb
smartctl 7.4 2023-08-01 r5530 [x86_64-linux-6.12.33-production+truenas] (local build)
Copyright (C) 2002-23, Bruce Allen, Christian Franke, www.smartmontools.org

=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 16
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000b   100   100   050    Pre-fail  Always       -       0
  2 Throughput_Performance  0x0005   100   100   050    Pre-fail  Offline      -       0
  3 Spin_Up_Time            0x0027   100   100   001    Pre-fail  Always       -       6910
  4 Start_Stop_Count        0x0032   100   100   000    Old_age   Always       -       11
  5 Reallocated_Sector_Ct   0x0033   100   100   050    Pre-fail  Always       -       0
  7 Seek_Error_Rate         0x000b   100   100   050    Pre-fail  Always       -       0
  8 Seek_Time_Performance   0x0005   100   100   050    Pre-fail  Offline      -       0
  9 Power_On_Hours          0x0032   100   100   000    Old_age   Always       -       111
 10 Spin_Retry_Count        0x0033   100   100   030    Pre-fail  Always       -       0
 12 Power_Cycle_Count       0x0032   100   100   000    Old_age   Always       -       11
191 G-Sense_Error_Rate      0x0032   100   100   000    Old_age   Always       -       0
192 Power-Off_Retract_Count 0x0032   100   100   000    Old_age   Always       -       6
193 Load_Cycle_Count        0x0032   100   100   000    Old_age   Always       -       212
194 Temperature_Celsius     0x0022   100   100   000    Old_age   Always       -       62 (Min/Max 23/63)
196 Reallocated_Event_Count 0x0032   100   100   000    Old_age   Always       -       0
197 Current_Pending_Sector  0x0032   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0030   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x0032   200   253   000    Old_age   Always       -       0
220 Disk_Shift              0x0002   100   100   000    Old_age   Always       -       0
222 Loaded_Hours            0x0032   100   100   000    Old_age   Always       -       63
223 Load_Retry_Count        0x0032   100   100   000    Old_age   Always       -       0
224 Load_Friction           0x0022   100   100   000    Old_age   Always       -       0
226 Load-in_Time            0x0026   100   100   000    Old_age   Always       -       588
240 Head_Flying_Hours       0x0001   100   100   001    Pre-fail  Offline      -       0
```

Chiffrer un serveur Debian et déverrouiller à distance

Documentation : https://www.cyberciti.biz/security/how-to-unlock-luks-using-dropbear-ssh-keys-remotely-in-linux/

Geekbench 6

Benchmark performances CPU "brutes" et permet de comparer rapidement le potentiel CPU entre machines/VM.

```
wget https://cdn.geekbench.com/Geekbench-6.4.0-Linux.tar.gz
tar xvf Geekbench-6.4.0-Linux.tar.gz
cd Geekbench-6.4.0-Linux
./geekbench6
```

Flash Mellanox CX2

Message de la carte si elle doit être flashée :

`root@shadow:/tmp # lspci -v | grep Mellanox 01:00.0 Non-VGA unclassified device: Mellanox Technologies MT25408 [ConnectX IB Flash Recovery]`

Solutions trouvées sur des forums/blog :

- https://forums.servethehome.com/index.php?threads/flashing-stock-mellanox-firmware-to-oem-emc-connectx-3-ib-ethernet-dual-port-qsfp-adapter.20525/#post-198015
- https://forums.developer.nvidia.com/t/connectx-ib-flash-recovery/208079
- https://nerdsniped.se/posts/switch-connectx-mode-from-infiniband-to-ethernet/

Configuration de la Mellanox MT25408 mono-port en mode Ethernet

Pour une carte **mono-port** (1 seul port), voici la procédure adaptée :

1. Préparation

Installer MFT (Mellanox Firmware Tools)

```
# Télécharger et installer MFT
wget http://www.mellanox.com/downloads/MFT/mft-4.xx.x-xxx-x86_64-deb.tgz
# ou pour RPM: mft-4.xx.x-xxx-x86_64-rpm.tgz

tar -xzf mft-4.xx.x-xxx-x86_64-*.tgz
cd mft-4.xx.x-xxx/
sudo ./install.sh
```

Démarrer MFT

```
sudo mst start
sudo mst status
```

2. Identifier la carte

```
# Voir les informations de la carte
sudo lspci | grep Mellanox
sudo flint -d /dev/mst/mt25408_pciconf0 query

# Noter le PSID (Part Number) - exemple: MT_0A10110009
```

3. Télécharger le firmware Ethernet

Pour une **MT25408 mono-port**, cherchez le firmware avec PartNumber:

- **MNPA19-XTR** (10GbE mono-port Ethernet)

Téléchargez depuis: https://network.nvidia.com/support/firmware/connectx/

4. Flash du firmware

```
# Backup du firmware actuel (IMPORTANT!)
sudo flint -d /dev/mst/mt25408_pciconf0 ri backup_original.bin

# Flash du nouveau firmware Ethernet
sudo flint -d /dev/mst/mt25408_pciconf0 -i fw-ConnectX-eth-mono.bin burn

# Taper "yes" pour confirmer
```

5. Configuration en mode Ethernet (mono-port)

```
# Configurer UNIQUEMENT le port 1 en Ethernet
sudo mlxconfig -d /dev/mst/mt25408_pciconf0 set LINK_TYPE_P1=1

# Valeurs: 1=Ethernet, 2=InfiniBand, 3=VPI
```

6. Réinitialisation

```
# Méthode 1: Redémarrage complet (recommandé)
sudo reboot

# Méthode 2: Reset de la carte uniquement
sudo mst restart
sudo mlxfwreset -d /dev/mst/mt25408_pciconf0 reset
```

7. Vérification

```
# Vérifier le mode configuré
sudo mst start
sudo mlxconfig -d /dev/mst/mt25408_pciconf0 query | grep LINK_TYPE

# Devrait afficher:
# LINK_TYPE_P1                        ETH(1)

# Vérifier l'interface réseau
ip link show
dmesg | grep mlx4
```

Résultat attendu

```
# L'interface devrait apparaître comme:
enp1s0 (ou eth0, selon votre système)
# Type: Ethernet
# Vitesse: 10000Mb/s
```

En cas de problème

```
# Restaurer le firmware original
sudo flint -d /dev/mst/mt25408_pciconf0 -i backup_original.bin burn

# Ou réinitialiser aux paramètres usine
sudo mlxconfig -d /dev/mst/mt25408_pciconf0 reset
```

Note : Pour une carte mono-port, configurez **uniquement LINK_TYPE_P1**, pas P2 !

Tmux

Tmux permet de gérer plusieurs terminaux dans une seule fenêtre et de garder vos sessions actives même après déconnexion.

Sessions

Commande	Description
`tmux`	Démarrer une nouvelle session
`tmux new -s nom`	Créer une session nommée
`tmux ls`	Lister les sessions
`tmux attach -t nom`	Se rattacher à une session
`tmux attach`	Se rattacher à la dernière session
`tmux kill-session -t nom`	Tuer une session
`tmux switch -t nom`	Changer de session
`tmux rename-session -t ancien nouveau`	Renommer une session

Raccourcis clavier (Préfixe par défaut : `Ctrl+b`)

Sessions

Raccourci	Description
`Préfixe + d`	Détacher de la session
`Préfixe + s`	Lister et changer de session
`Préfixe + $`	Renommer la session courante
`Préfixe + (`	Session précédente
`Préfixe + )`	Session suivante

Fenêtres (Windows)

Raccourci	Description
`Préfixe + c`	Créer une nouvelle fenêtre
`Préfixe + ,`	Renommer la fenêtre courante
`Préfixe + &`	Fermer la fenêtre courante
`Préfixe + w`	Lister les fenêtres
`Préfixe + n`	Fenêtre suivante
`Préfixe + p`	Fenêtre précédente
`Préfixe + numéro`	Aller à la fenêtre numéro X
`Préfixe + l`	Dernière fenêtre active

Panneaux (Panes)

Raccourci	Description
`Préfixe + %`	Diviser verticalement
`Préfixe + "`	Diviser horizontalement
`Préfixe + x`	Fermer le panneau courant
`Préfixe + o`	Passer au panneau suivant
`Préfixe + ;`	Basculer vers le dernier panneau
`Préfixe + flèches`	Naviguer entre les panneaux
`Préfixe + Ctrl+flèches`	Redimensionner le panneau
`Préfixe + Alt+flèches`	Redimensionner (par pas de 5)
`Préfixe + z`	Zoom/dézoom sur le panneau
`Préfixe + !`	Convertir le panneau en fenêtre
`Préfixe + {`	Déplacer le panneau à gauche
`Préfixe + }`	Déplacer le panneau à droite
`Préfixe + Espace`	Changer la disposition
`Préfixe + q`	Afficher les numéros de panneaux

Mode Copie

Raccourci	Description
`Préfixe + [`	Entrer en mode copie
`Espace`	Commencer la sélection

Raccourci	Description
`Entrée`	Copier la sélection
`Préfixe + ]`	Coller
`q`	Quitter le mode copie

Autres

Raccourci	Description
`Préfixe + ?`	Lister tous les raccourcis
`Préfixe + t`	Afficher l'heure
`Préfixe + :`	Entrer en mode commande

Configuration (~/.tmux.conf)

```
# Changer le préfixe
unbind C-b
set -g prefix C-a
bind C-a send-prefix

# Recharger la config
bind r source-file ~/.tmux.conf \; display "Config rechargée!"

# Navigation vim-style
bind h select-pane -L
bind j select-pane -D
bind k select-pane -U
bind l select-pane -R

# Splits plus intuitifs
bind | split-window -h
bind - split-window -v

# Activer la souris
set -g mouse on

# Historique
```

```
set -g history-limit 10000

# Numérotation à partir de 1
set -g base-index 1
setw -g pane-base-index 1

# Couleurs
set -g default-terminal "screen-256color"
```

Commandes utiles en mode commande

Commande	Description
`:new -s nom`	Nouvelle session
`:kill-session`	Tuer la session courante
`:resize-pane -D 5`	Redimensionner vers le bas
`:resize-pane -U 5`	Redimensionner vers le haut
`:resize-pane -L 5`	Redimensionner vers la gauche
`:resize-pane -R 5`	Redimensionner vers la droite
`:setw synchronize-panes on`	Synchroniser les panneaux
`:setw synchronize-panes off`	Désynchroniser les panneaux

Astuces

- **Copier vers le presse-papier système** : Installer `xclip` puis configurer
- **Session persistante** : tmux garde les sessions même après déconnexion
- **Workflow multiple serveurs** : Créer une session par serveur
- **Scripts de démarrage** : Automatiser la création de layouts complexes