

Sécurisation basique de son Proxmox

Je vois sur Internet des serveurs Proxmox pas sécurisés voire pire, des conseils qui préconisent d'utiliser un firewall comme pfSense installé en machine virtuelle pour sécuriser l'hyperviseur, alors que ce dernier est hébergé chez un fournisseur dont on ne sait rien du réseau. Votre fournisseur peut proposer un firewall comme chez OVH avec son système anti-DDoS, mais cela ne vous protège que de l'extérieur, pas de l'intérieur du réseau, qui lui comporte une multitude de serveurs d'autres clients.

La logique pour un réseau en entreprise ou chez soi, pour un home lab ou de l'auto-hébergement sera la même.

Quel que soit l'hyperviseur, il faut que celui-ci soit sécurisé. S'il n'est pas sécurisé, toutes vos machines virtuelles ou vos conteneurs sont potentiellement compromis.

Pour citer Andy Grove, co-fondateur d'Intel, dans son livre autobiographique qui porte le même nom : « Seuls les paranoïaques survivent ».

[Wikipedia]: Il explique dans sa biographie *Seuls les paranoïaques survivent* que le moteur psychique qui lui a permis de mener son entreprise au sommet a été durant 38 ans

Ce concept est parfaitement adapté pour la sécurité.

1. Protection physique

Le ou les serveurs doivent être à minima protégés physiquement, comme une salle sécurisée, ou si dans un datacenter, dans une baie fermée à clefs. Mais il est aussi important de protéger l'accès au BIOS/UEFI par un mot de passe costaud et interdire le boot sur autre chose que l'hyperviseur.

Il serait dommage qu'une personne avec une clef usb boote sur un autre OS, et modifie le mot de passe root, formate le ou les disques où sont installés Proxmox, etc.

Les sociétés qui fournissent des serveurs comme OVH, Scaleway, etc. peuvent avoir dans leurs employés des personnes mal intentionnées, tout comme dans vos collègues de travail ou prestataires.

2. Firewall

Proxmox intègre un firewall agissant sur 3 parties distinctes :

- Datacenter
- Serveur Proxmox alias PVE
- Machines virtuelles et conteneurs LXC

La partie machine virtuelle et conteneurs est indépendante des deux autres. Elle n'a pas d'intérêt dans la sécurisation du serveur Proxmox.

Je me base seulement pour un seul hôte Proxmox, qui dans ce cas le fait de faire les règles au niveau du data center ou du node n'aura pas forcément d'impact.

2.1 Ports utilisés par Proxmox

Proxmox utilise par défaut ces ports pour fonctionner.

Si vous modifiez le port SSH, utilisez le même port sur tous les serveurs du cluster au risque d'avoir des surprises.

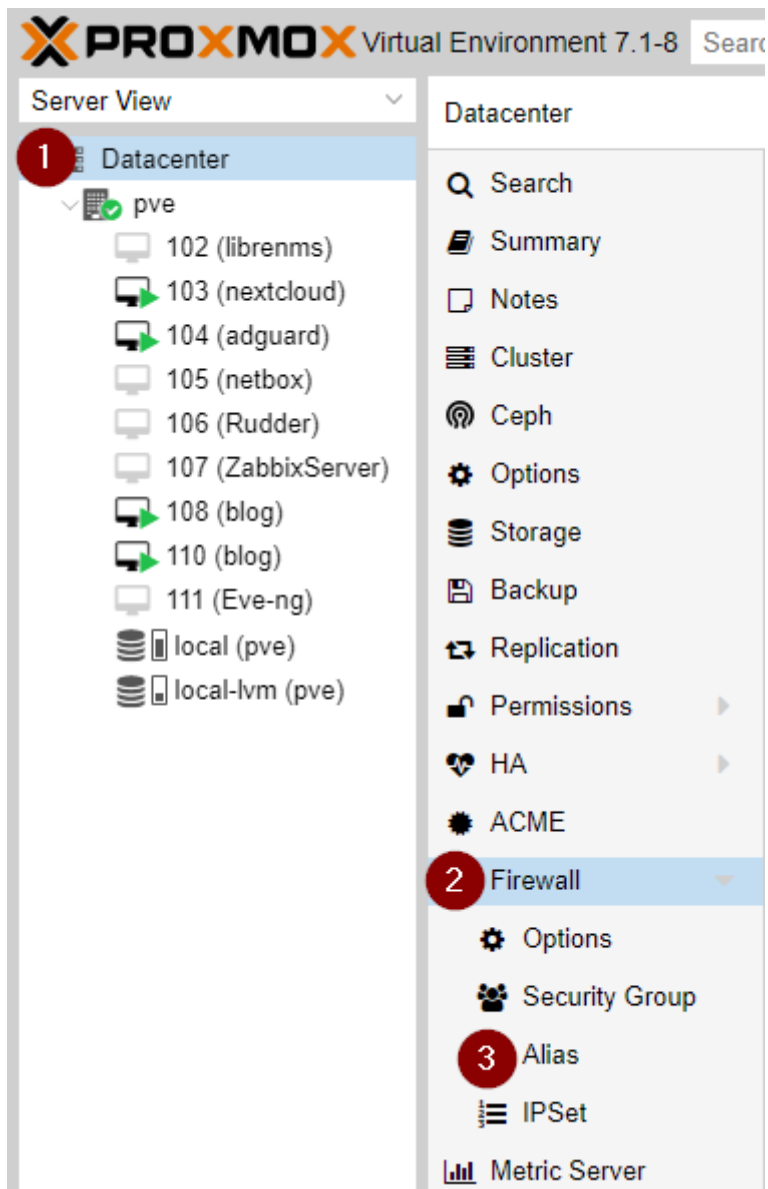
Services	Protocole	Ports
Web interface	TCP	8006
SSHD	SSH	22
pvedaemon (en écoute)	TCP	85
rpcbind	TCP	111
corosync multicast (pour les clusters)	UDP	5404, 5405
SPICE proxy	TCP	3128

[Source](#)

2.2 Alias

Alias se trouve dans la partie firewall du Datacenter et va permettre de nommer les IP ou les plages d'IP à utiliser dans le firewall.

C'est une habitude de travail de créer des alias, ça évite les oublis, ça permet aussi d'aller plus vite quand on a une correction à effectuer sur une grosse quantité de règles de filtrage.



2.2.1 Plage d'IP

Edit: Alias

Name:

IP/CIDR:

Comment:

OK Reset

2.2.2 Une IP

Add: Alias

Name:

IP_Administration_SSH

IP/CIDR:

192.168.1.76

Comment:

Add

2.3 Règles de firewall

Rien de compliqué, on autorise en entrée le port 8006, le SSH, le ping. Et comme ce n'est qu'un seul node, pas besoin de préciser la destination (pas idéal, mais cela simplifie les choses) ni l'interface sur laquelle le trafic doit passer, qui de toute façon pour un seul node sera vmbr0.

Direction	Action	Source	Protocol	Destination Port	Log Level	Comment
in	ALLOW		tcp	8006	nolog	web GUI
in	ALLOW		tcp	22	nolog	ssh
in	ALLOW		icmp		nolog	ping

2.3.1 Macro

Il est possible d'utiliser des macros de configuration pour certains protocoles comme le SSH ou le protocole SMB qui a besoin d'ouverture de plusieurs ports (TCP 445, TCP 139, UDP 138-139), cela facilite grandement la lecture des règles si vous devez l'utiliser.

Edit: Rule

Direction:

in

Enable:
☒

Action:

ACCEPT

Macro:

SSH

Interface:

Protocol:

Source:

ip_plage_administra

Source port:

Destination:

Dest. port:

Comment:

Log level:

nolog

Advanced ☒

OK

Reset

2.3.2 Protocole

Edit: Rule

Direction:

in

Enable:
☒

Action:

ACCEPT

Macro:

Interface:

Protocol:

tcp

Source:

ip_plage_administra

Source port:

Destination:

Dest. port:

8006

Comment:

Log level:

nolog

Advanced ☒

OK

Reset

2.4 Chef, je me suis coupé la main !

En console, il est possible de désactiver le firewall

Éditez le fichier `/etc/pve/firewall/cluster.fw` et remplacez la valeur **1** par **0**.

[OPTIONS]

enable: 1

2.5 Utilisation de pfsense pour les VM

Je vous oriente sur le site de [zwindler](#) qui a 3 articles sur le sujet :

- [Proxmox VE 6 + pfsense sur un serveur dédié \(1/2\)](#)
- [Proxmox VE 6 + pfsense sur un serveur dédié \(2/2\)](#)
- [Optimisation de PFsense dans Proxmox VE](#)

Et aussi le script bash de [Noa](#) disponible sur son GitHub :

- [Iptables Proxmox Forward pfsense](#)

3. Fail2Ban

3.1 Installation de Fail2Ban

```
apt install fail2ban
```

3.2 Configuration de fail2Ban

Editez le fichier `:/etc/fail2ban/jail.local`

```
[proxmox]
enabled = true
port = https,http,8006
filter = proxmox
backend = systemd
maxretry = 3
```

```
findtime = 2d
bantime = 1h

[sshd]
enabled = true
port = ssh
filter = sshd
logpath = journal
backend = systemd
maxretry = 2
findtime = 300
banaction = iptables-allports
bantime = 86400
ignoreip = 127.0.0.1
```

/etc/fail2ban/filter.d/proxmox.conf

```
[Definition]
failregex = pvedaemon\[.*authentication failure; rhost=<HOST> user=.* msg=.*
ignoreregex =
journalmatch = _SYSTEMD_UNIT=pvedaemon.service
```

Relancer le service de Fail2Ban

```
systemctl restart fail2ban.service
```

Sources : [wiki Proxmox](#)

3.3 Les commandes utiles de Fail2Ban

3.3.1 Bannir une IP

```
fail2ban-client set [nom du jail] banip [IP à bannir]
```

3.3.2 Enlever le ban d'une IP

```
fail2ban-client set [nom du jail] unbanip [IP concerné]
```

3.3.3 Lister les règles

```
fail2ban-client status
```

```
Status
```

```
| - Number of jail:    1
```

```
`- Jail list:  sshd
```

3.3.4 Détails d'une règle

```
fail2ban-client status sshd
```

```
Status for the jail: sshd
```

```
| - Filter
```

```
| | - Currently failed: 0
```

```
| | - Total failed:    5
```

```
| ` - File list:      /var/log/auth.log
```

```
` - Actions
```

```
  | - Currently banned: 1
```

```
  | - Total banned:    1
```

```
  ` - Banned IP list:  192.168.1.21
```

Et si l'on veut en savoir plus sur les tentatives de connexion, il faut regarder dans `/var/log/auth.log`

```
tail /var/log/auth.log
```

```
Dec  9 12:46:14 pve sshd[3769206]: Failed password for nidouille from 192.168.1.21 port 39516 ssh2
```

```
Dec  9 12:46:18 pve sshd[3769206]: Failed password for nidouille from 192.168.1.21 port 39516 ssh2
```

```
Dec  9 12:46:22 pve sshd[3769206]: Failed password for nidouille from 192.168.1.21 port 39516 ssh2
```

```
Dec  9 12:46:23 pve sshd[3769206]: Connection closed by authenticating user nidouille 192.168.1.21 port 39516 [preauth]
```

```
Dec  9 12:46:23 pve sshd[3769206]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.21 user=nidouille
```

4. SSH

Par défaut, Proxmox ne propose qu'un compte utilisateur : root. On va le sécuriser à minima pour les connexions SSH.

Voici les options activées après une installation d'un node dans `/etc/ssh/sshd_config`, et ce n'est pas fou.

```
PermitRootLogin yes

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

UsePAM yes
X11Forwarding yes
PrintMotd no

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem      sftp    /usr/lib/openssh/sftp-server
```

Fail2Ban amène une protection pour les attaques par brute force, mais si on garde l'utilisateur root pour l'accès distant en ssh, on va monter d'un cran la sécurité en obligeant la connexion via clefs. Je ne saurais que trop conseiller la désactivation de l'utilisateur SSH au profit d'un autre compte système.

Je pars du principe que vous avez vos clefs SSH privés et publique.

Dans `/root/.ssh/authorized_keys`, vous allez renseigner votre clef publique

Puis modifier `/etc/ssh/sshd_config` pour forcer l'authentification par clefs.

```
#PermitRootLogin yes
PermitRootLogin prohibit-password
PubkeyAuthentication yes
PasswordAuthentication no
PermitEmptyPassword no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

```
UsePAM yes
X11Forwarding no
PrintMotd no

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem      sftp    /usr/lib/openssh/sftp-server
```

5. Comptes utilisateurs

La gestion des comptes utilisateurs peut être précise et déroutante.

De base, on a deux types de comptes utilisateur :

- PAM (compte système)
- Proxmox

Auquel on peut rajouter d'autre source d'utilisateur via le menu Realms (non traité ici) :

- Active Directory
- LDAP
- OpenID Connect

Puis, on donne aux utilisateurs deux permissions :

- Path
- Role

Il est bien sûr possible de créer des groupes d'utilisateurs, de nouveaux rôles en associant les privilèges que l'on désire et de créer des pools regroupant des VM et des datastores pour encore affiner les droits si besoin.

5.1 Les rôles

Les rôles regroupent les privilèges.

Nom	Privilèges
Administrator	Tous les droits
NoAccess	Aucun droits donc aucun accès
PVEAdmin	Tout sauf les paramètres systèmes (Sys.PowerMgmt, Sys.Modify, Realm.Allocate)
PVEAuditor	Accès en lecture seule
PVEDatastoreAdmin	Administration des espaces de stockage et des templates (inclus le backup)
PVEDatastoreUser	Allocation des espaces de stockage et des templates (inclus le backup)
PVEPoolAdmin	Administration des pools
PVEPoolUser	Consultations des pools
PVESysAdmin	ACLs utilisateur, audit, console système et journaux système
PVETemplateUser	visualiser et cloner des templates
PVEUserAdmin	administration des utilisateurs
PVEVMAdmin	administrations des VM
PVEVMUser	visualisation, sauvegarde, CDROM de configuration, console VM, gestion de l'alimentation VM

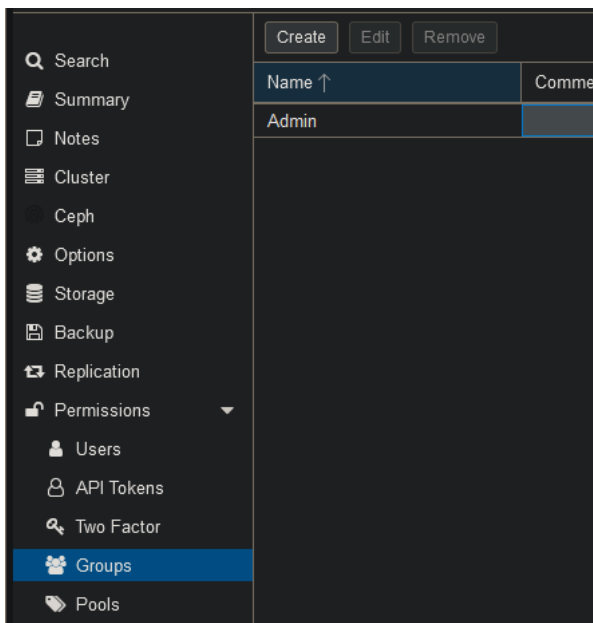
5.2 Comptes système (PAM)

Les comptes PAM sont des comptes systèmes. Les seuls à pouvoir se connecter en SSH ou console.

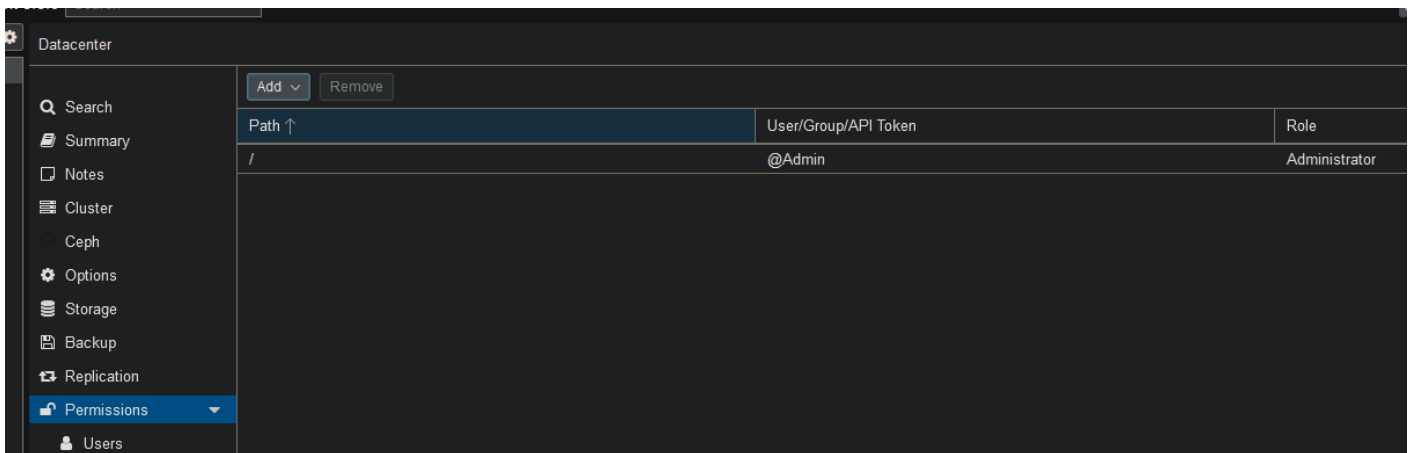
Pour la création de ce type de compte, en dehors du compte systèmes, le reste peut se faire en console ou via la GUI.

Configuration des permissions

Il faut en premier crée un groupe et configurer ses permission avant de crée l'utilisateur (cela peut aussi être faire après la création de compte)

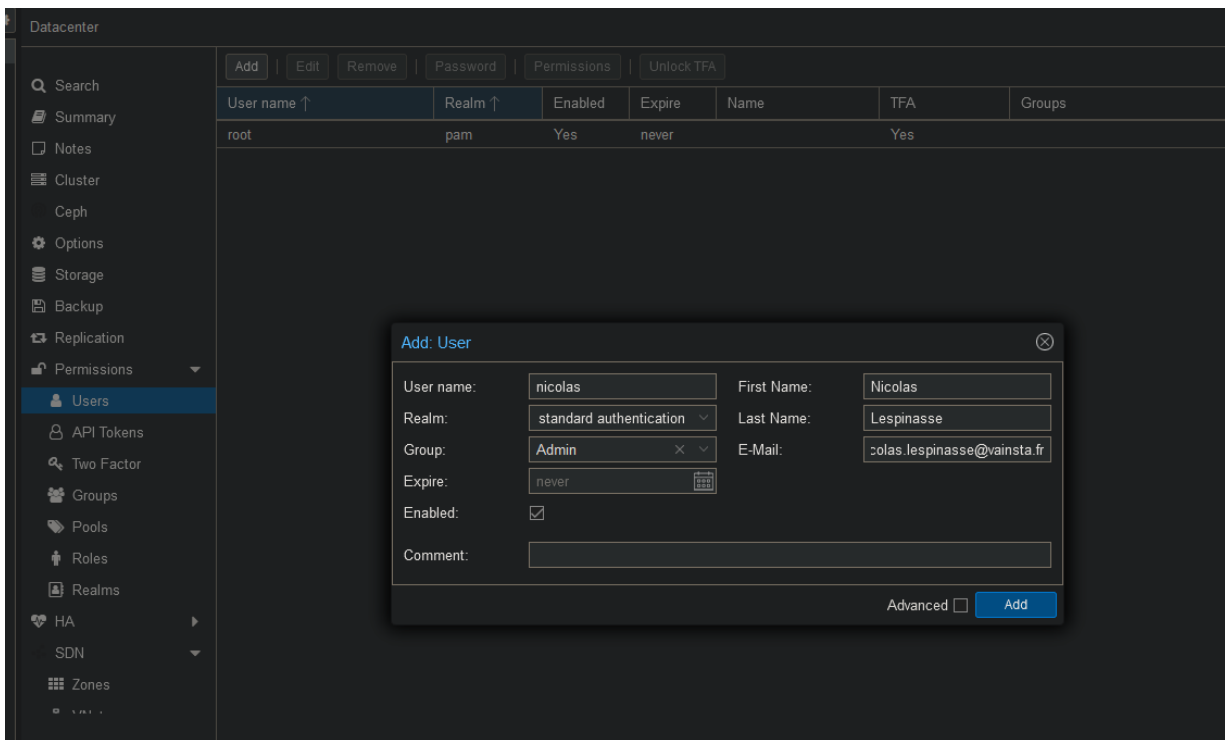


puis nous allons sur la page permission est ajouter les permission voulus a ce groupe



Création du compte système

On ajoute en premier le compte depuis Datacenter -> user

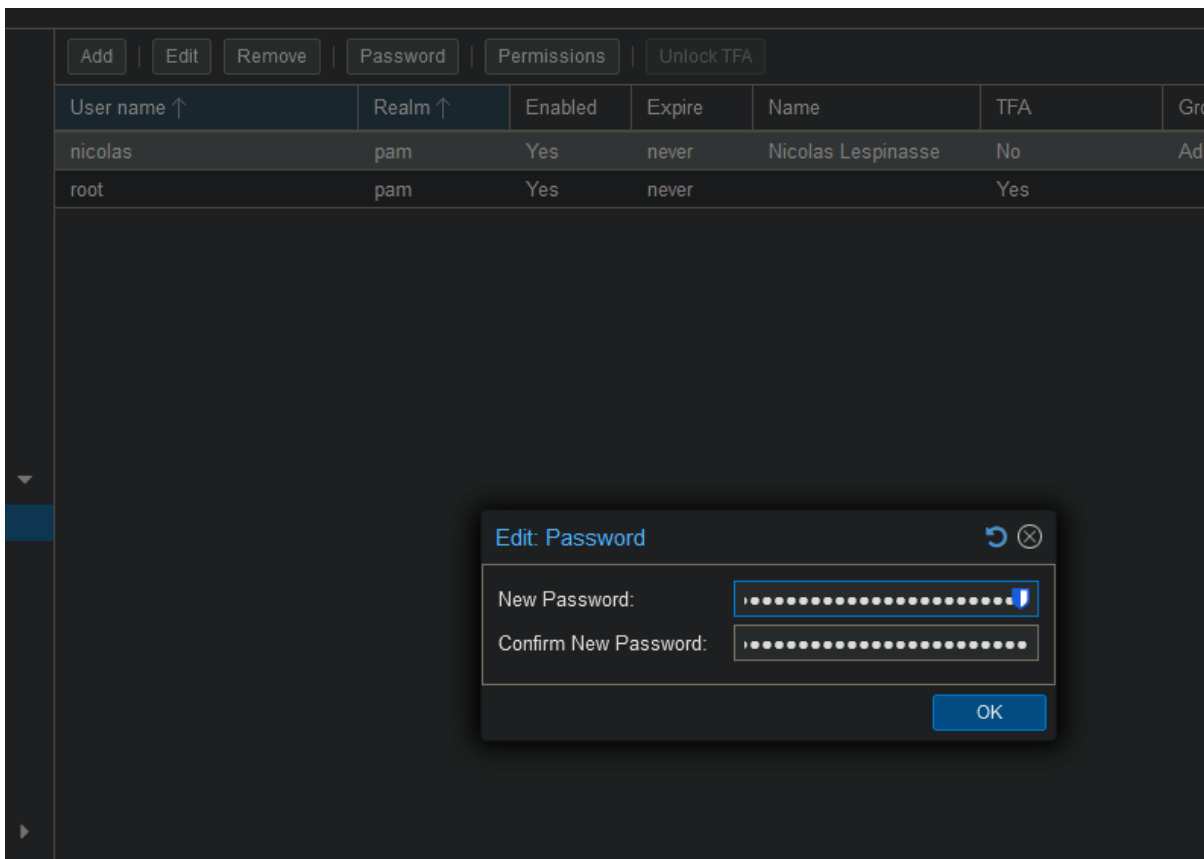


Il faut aussi l'ajouter manuellement sur la machine car il n'existe pas par défaut

```
root@pve:~# useradd nicolas
```

Configuration du mot de passe

Après avoir ajouter le compte sur la machine on peut retourner sur la page Utilisateur et editer le mot de passe



Configuration du Shell

Vu que l'utilisateur a été créé à la main par défaut il n'utilise pas bash il faut donc utiliser cette commande et se déconnecter et reconnecter

```
chsh -s /bin/bash USER
```

5.3 Authentification à double facteurs TOTP

Pour la mise en place rapide d'une double authentification, la solution du TOTP est idéal. Il faut juste un gestionnaire de mot de passe qui possède cette fonctionnalité comme Bitwarden, LastPass via son application dédiée Authenticator, NordPass, etc., ou des applications dédiées comme LastPass, Authenticator, etc.

Pour en savoir plus sur le TOTP:

- site de la société française Synestis spécialisé en cybersécurité : [lien](#)

- blog de l'hébergeur IONOS : [lien](#)

Pour le tutoriel, j'utilise Bitwarden (produit très utilisé) pour la génération du code aléatoire. Mais il n'est pas possible sur l'application d'effectuer des captures d'écran, les captures faites le sont sur mon client Bitwarden installé sur mon PC.

Add a TOTP login factor

User: admin1@pam

Description: admin1 TOTP

Secret: [Redacted] **Randomize**

Issuer Name: Proxmox VE - pve



Verify Code: Scan QR code in a TOTP app and enter an auth. code here

Help **Add**

Ouvrir Bitwarden sur votre téléphone

Créer un nouvel élément de type identifiant

- Nom pour Bitwarden
- Nom d'utilisateur
- Le mot de passe de l'utilisateur (facultatif)
- Clé authentification (TOTP) : prenez en photo le QR code généré et cela remplira la ligne

Nom

admin1 pve

Nom d'utilisateur

admin1

Mot de passe

[REDACTED]



Clé d'authentification (TOTP)

otpauth://totp/

[REDACTED]

Sauvegarder identifiant créé et ensuite, ouvrez-le. Vous verrez un code généré avec un temps avant la génération d'un nouveau code (30 secondes).

Nom

admin1 pve

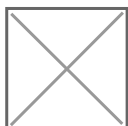
Nom d'utilisateur

admin1



Code de vérification (TOTP)

[REDACTED]



Rentrer le code dans la boîte de dialogue de création de compte TOTP de Proxmox pour activer le TOTP du compte.

User	Enabled	TFA Type	Created	Description
admin1@pam	Yes	totp	2021-12-10 12:00:21	admin1 TOTP

Proxmox VE Login

User name:

Password:

Realm:

Language:

Save User name: ☐

Login

Second login factor required

<

WebAuthn

TOTP App

Recovery Key

U2F

Y

>

Please enter your TOTP verification code:

Confirm Second Factor

Revision #11
Created 26 November 2024 14:11:40 by Nicolas
Updated 6 December 2024 01:01:52 by Nicolas