

SECURISER

Proxmox VE et Proxmox Backup Server



PROXMOX

ALERTE

SOMMAIRE

1. SECURISER PROXMOX 8.1

- a. Installation de Fail2ban
- b. Modification du port d'écoute SSH
- c. Désactivation de l'accès root SSH
- d. Création d'un compte utilisateur PVE
- e. Activation des notifications ("alerting")

2. SECURISER PROXMOX BACKUP SERVER 3.1

- a. Désactivation de l'accès root SSH
- b. Création d'un utilisateur PBS
- c. Installation de Fail2ban

© tutos-info.fr - 04/2024



DIFFICULTE



UTILISATION COMMERCIALE INTERDITE

Note :

De nos jours, la sécurisation des serveurs exposés au web est primordiale. Ce dossier présente quelques règles de base visant à sécuriser, à minima, votre hyperviseur Proxmox VE 8.1 et votre serveur de sauvegarde Proxmox Backup Server 3.1

Ce tutoriel suppose que vous avez installé l'hyperviseur et le serveur de sauvegarde (voir tutoriels précédents).

1 – SECURISER PROXMOX VE 8.1

1^{ère} ETAPE : INSTALLATION DE FAIL2BAN SUR L'HYPERVISEUR PROXMOX VE

a) Installer Fail2ban sur l'hyperviseur (depuis le shell de l'hyperviseur)

Dans l'interface de gestion de l'hyperviseur, cliquez sur le nom du nœud Proxmox et, dans le volet de droite, cliquez sur « **Shell** » et lancez les commandes suivantes :

```
apt update
apt upgrade -y
apt install fail2ban -y
```

b) Copier le fichier modèle "jail.conf" en "jail.local"

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

c) Éditer le fichier "jail.local" et ajouter les éléments donnés ci-dessous :

```
nano /etc/fail2ban/jail.local
```

Éléments à ajouter dans le fichier "jail.local", puis quitter en sauvegardant les modifications :

[proxmox]

```
enabled = true
port = https,http,8006
filter = proxmox
logpath = journal
backend = systemd
maxretry = 3
findtime = 2d
bantime = 1h
```

Bloc [PROXMOX]

Bloc à ajouter dans le fichier en respectant la forme ci-contre. Ce bloc peut être copié en fin de fichier par exemple.

[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
```

Bloc [SSHD]

Coller le contenu du bloc dans le fichier, en respectant la forme ci-contre. **Attention, ce bloc existe déjà** (voir en milieu de fichier) et **il n'est pas utile de copier [sshd]** car le bloc est déjà identifié.

d) Configurer le filtre en éditant le fichier "proxmox.conf" et en ajoutant les éléments donnés :

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

Éléments à ajouter au fichier :

[Definition]

```
failregex = pvedaemon\[.*authentication failure; rhost=<HOST> user=.* msg=.*
ignoreregex =
```

e) Désactivation de la gestion des adresses IPv6 (si elles ne sont pas gérées)

Si les adresses IPv6 ne sont pas gérées, la désactivation se fait au niveau du fichier « fail2ban.conf » dans le groupe [Définitions] :

```
nano /etc/fail2ban/fail2ban.conf
```

- Décommenter "allowipv6"
- Ajouter le paramètre "no"

```
# Option: allowipv6
# Notes.: Allows IPv6 interface:
#       Default: auto
# Values: [ auto yes (on, true, 1) no (off, false, 0) ] Default: auto
allowipv6 = no
```

f) Créer le fichier « auth.log » et lui attribuer les droits nécessaires

```
touch /var/log/auth.log
chmod 640 /var/log/auth.log
```

g) Redémarrer Fail2ban et vérifier le statut

```
systemctl restart fail2ban
systemctl status fail2ban
```

COMMANDES UTILES FAIL2BAN

Bannir une IP

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

Enlever le ban d'une IP

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

Lister les règles

```
fail2ban-client status
```

Afficher les détails d'une règle

```
fail2ban-client status sshd
```

Lister les tentatives de connexion

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

Lister les tentatives de connexion en temps réel

```
tail -f /var/log/auth.log
```

2^{ème} ETAPE : MODIFICATION DU PORT D'ECOUTE SSH

Une bonne alternative pourrait être la modification du port d'écoute SSH par défaut. En effet, les « bots » exécutent souvent des attaques de type « brute-force » sur le port « 22 » ultra connu.

La modification du port d'écoute SSH s'effectue en modifiant la ligne ci-dessous dans le fichier « sshd_config » :

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

- Décommentez la ligne « **#Port 22** » et saisissez le numéro du nouveau port d'écoute souhaité (**choisir un port au-dessus de 1024**) :

```
Port 22444
#AddressFamily any
#ListenAddress 0.0.0.0
```

La modification du port d'écoute peut être une parade aux attaques de type « brute-force » ; Pour cela, saisissez un n° de port non utilisé et supérieur à 1 024 parmi les 65 536 !

- Quittez en sauvegardant les modifications
- Relancez le service SSH avec la commande suivante :

```
systemctl restart ssh (relance du service SSH)
```

```
systemctl status ssh (pour vérifier le statut du service SSH)
```

3^{ème} ETAPE : DESACTIVATION DE L'ACCES SSH POUR LE ROOT

Attention, lors de l'installation de l'hyperviseur, **l'accès SSH pour le « root » a été laissé activé par défaut** ! Il convient de désactiver cet accès pour assurer un minimum de sécurité et combler cette faille (on pourra utiliser un utilisateur PVE pour se loguer en SSH à l'hyperviseur ; voir 4^{ème} étape, page suivante).

Proxmox VE 8.1 étant basé sur Debian 12, le fichier de configuration SSH se trouve à l'emplacement suivant :

« **/etc/ssh** »

Le nom du fichier est « **sshd_config** ».

- Depuis le « **shell** », éditez le fichier « **sshd_config** » avec la commande suivante :

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

- Assurez-vous que, dans le bloc « **Authentification** », la ligne « **PermitRootLogin** » est bien commentée (avec le # devant la ligne) :

```
# Authentication:
#LoginGraceTime 2
#PermitRootLogin
```

- Si la ligne n'est pas commentée, placez le signe « # » devant la ligne
- Quittez et sauvegardez les modifications (CTRL + X et « Y »)
- Relancez le service SSH avec la commande : `systemctl restart ssh`

a) Création d'un utilisateur PVE

Il est vivement recommandé de créer un utilisateur « PVE » afin d'éviter la connexion en « root » (PAM). Cet utilisateur pourra être utilisé pour se connecter en SSH par exemple. Un utilisateur PVE est un utilisateur Proxmox Virtual Environment. Pour le créer, effectuez les manipulations suivantes :

- Cliquez sur le « **Centre de données** » (datacenter)
- Dans le volet de droite, cliquez sur « **Utilisateurs** »
- Renseignez les champs d'identification et cliquez le bouton « Ok » pour valider :

Ajouter: Utilisateur

Nom d'utilisateur: toto Prénom: toto

Royaume: Proxmox VE authentical Nom: toto

Mot de passe: Courriel: toto.toto@gmail.com

Confirmer le mot de passe:

Groupe: [dropdown]

Date d'expiration: never [calendar icon]

Activé:

Ici, on sélectionne le « Royaume PVE » puisque l'utilisateur sera un utilisateur PVE et non Linux.

b) Gestion des permissions pour l'utilisateur PVE

Une fois l'utilisateur PVE créé, il est nécessaire de lui accorder des permissions afin qu'il puisse gérer l'hyperviseur. Pour cela, effectuez les manipulations suivantes :

- Cliquez sur le « **Centre de données** » (datacenter)
- Cliquez, dans le volet de droite, sur « **Permissions** »
- Cliquez le bouton « **Ajouter** » et « **Permissions de l'utilisateur** »
- Sélectionnez le chemin d'accès (ici, nous souhaitons que l'utilisateur accès à tous les dossiers)
- Sélectionnez l'utilisateur PVE et sélectionnez le rôle souhaité (voir description détaillée)
- Cliquez le bouton « **Ajouter** » :

Ajouter: Permissions de l'utilisateur

Chemin d'accès: /

Utilisateur: toto@pve

Rôle: PVEAdmin

Propager:

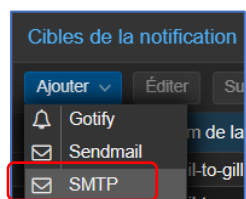
Aide [?] Ajouter

Ici, on sélectionne le chemin auquel on veut donner accès. En choisissant « / » on donne les droits sur tous les dossiers de l'hyperviseur (à adapter en fonction de votre stratégie de sécurité). On sélectionne, également, le rôle que l'on souhaite attribuer à l'utilisateur PVE (voir description des différents rôles possibles).

1^{ère} étape : configuration du compte mail SMTP (envoi des mails depuis Proxmox)

Il peut être judicieux d'activer les notifications afin de recevoir des alertes (alertes de dysfonctionnements, alertes de sauvegardes, etc.). Ici, nous allons configurer un compte SMTP qui permettra à l'hyperviseur d'envoyer des alertes depuis le compte de messagerie paramétré. Pour cela, effectuez les manipulations suivantes :

- Cliquez sur « **Centre de données** » (datacenter)
- Dans le volet de droite, cliquez sur « **Notifications** »
- Dans la rubrique « **Cibles de notification** », cliquez le bouton « **Ajouter** » et « **SMTP** » :



- Indiquez les identifiants nécessaires à la création du compte SMTP puis cliquez le bouton « **Ajouter** » :

Pour que la notification fonctionne, **assurez-vous que le compte utilisateur PVE sélectionné comme destinataire a bien une adresse mail configurée.**

Si ce n'est pas le cas, cliquez sur « **Centre de données** » et « **Utilisateurs** » et saisissez l'adresse mail dans le compte de l'utilisateur PVE concerné.

2^{ème} étape : configurer la "correspondance de notification"

Une fois le serveur SMTP configuré, il faut ajouter une "correspondance de notification".

Pour cela, sous la configuration du serveur SMTP figure une partie nommée "Correspondance de notification" ; ajoutez une correspondance en cliquant le bouton "**Ajouter**" et configurez-la ainsi :

- Dans l'onglet "**Général**", saisissez le nom de la correspondance :

Ajouter: Correspondance de notification ✕

Général Règles de correspondance Cibles à notifier

Nom de la correspondance:

Activer:

Commentaire:

? Aide Ajouter

- Dans l'onglet "**Cibles à notifier**", cliquez la cible qui doit être ajoutée (celle créée précédemment)
- Cliquez le bouton "**Ajouter**" :

Ajouter: Correspondance de notification ✕

Général Règles de correspondance **Cibles à notifier**

<input type="checkbox"/>	Nom de la cible ↑	Type	Commentaire
<input checked="" type="checkbox"/>	Mail-notifications...	smtp	Notifications_Backup_PVE Online
<input type="checkbox"/>	mail-to-root	sendmail	Send mails to root@pam's email address

? Aide Ajouter

3^{ème} étape : tester l'envoi d'une notification

- Cliquez à nouveau sur "**Notifications**" et cliquez le bouton "**Test**" pour vérifier vos paramètres
- Confirmez l'envoi de la notification de test en cliquant le bouton "**Oui**" :

Test de la cible de notification ✕

? Voulez-vous envoyer une notification de test à « Mail-notifications-Backups » ?

Oui Non

Si vos paramètres de messagerie ont été configurés correctement, vous recevrez un mail qui confirmera l'envoi de la notification. Si vous obtenez une erreur, revoyez vos paramètres de messagerie SMTP (numéro du port, mot de passe, etc.).

2 – SECURISER PROXMOX BACKUP SERVER 3.1

1ère ETAPE : DESACTIVATION DE L'ACCES SSH POUR LE ROOT

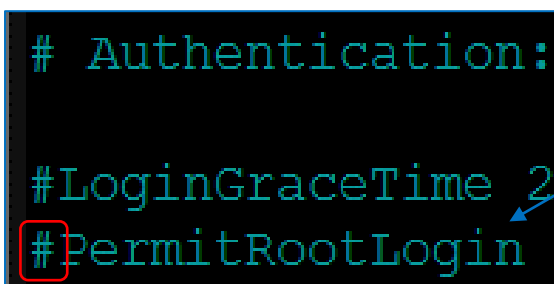
Tout comme Proxmox VE, le service SSH doit être désactivé pour le « root ». Le fichier « **sshd_config** » se trouve à l'emplacement « **/etc/ssh** ».

Pour cela, effectuez les manipulations suivantes :

- Depuis le « **shell** » de Proxmox Backup Server, éditez le fichier « **sshd_config** » avec la commande suivante :

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

- Assurez-vous que, dans le bloc « **Authentification** », la ligne « **PermitRootLogin** » est bien commentée (avec le # devant la ligne) :



```
# Authentification:  
  
#LoginGraceTime 2  
#PermitRootLogin
```

- Si la ligne n'est pas commentée, placez le signe « # » devant la ligne
- Quittez et sauvegardez les modifications (CTRL + X et « Y »)
- Relancez le service SSH avec la commande : **systemctl restart ssh**

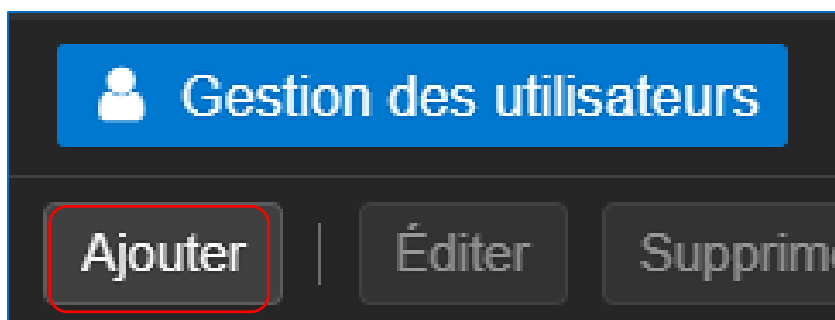
2ème ETAPE : CREATION D'UN UTILISATEUR ADMINISTRATEUR DU SERVEUR DE SAUVEGARDE

Il est vivement recommandé de créer un utilisateur au sein du « royaume PBA ».

Cet utilisateur aura les permissions nécessaires pour administrer Proxmox Backup Server et cela évitera la connexion depuis l'utilisateur « root ».

Dans l'interface d'administration de Proxmox Backup Server, effectuez les manipulations suivantes :

- Cliquez sur « **Contrôle d'accès** »
- Dans « **Gestion des utilisateurs** », cliquez le bouton « **Ajouter** » :



- Complétez la fenêtre (n'oubliez pas de renseigner l'adresse de courriel pour pouvoir recevoir des notifications), puis cliquez le bouton « **Ajouter** » :

Ajouter: Utilisateur

Nom d'utilisateur: totopbs Prénom: toto

Royaume: Proxmox Backup authen Nom: pbs

Mot de passe: Courriel: totopbs@gmail.com

Confirmer le mot de passe:

Date d'expiration: jamais

Activé:

Commentaire:

Aide **Ajouter**

Une fois l'utilisateur créé, on lui donne les permissions nécessaires sur le PBS, par exemple, l'administration du datastore (l'entrepôt de données) :

- Cliquez sur le nom de l'utilisateur PBS
- Cliquez le bouton "**Permissions**"
- Cliquez le bouton "**Ajouter**" et "**Permissions de l'utilisateur**"
- Complétez la fenêtre comme ceci :

Ajouter: Permissions de l'utilisateur

Chemin d'accès: /datastore

Utilisateur: adminpbs@pbs

Rôle: DatastoreAdmin

Propager:

Aide **Ajouter**

- Cliquez le bouton "**Ajouter**" pour valider vos paramètres

Désormais, l'utilisateur PBS aura la permission d'accès au datastore avec les droits d'admin sur le datastore (permissions à adapter en fonction de votre politique de sécurité).

a) Installer Fail2ban sur PBS (depuis le shell de PBS)

Dans l'interface de gestion de PBS, cliquez sur « **Administration** » et « **Shell** » et lancez les commandes suivantes :

```
apt update
apt upgrade -y
apt install fail2ban -y
```

b) Copier le fichier modèle "jail.conf" en "jail.local"

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

c) Éditer le fichier "jail.local" et ajouter les éléments donnés ci-dessous :

```
nano /etc/fail2ban/jail.local
```

Éléments à ajouter dans le fichier "jail.local", puis quitter en sauvegardant les modifications :

[pbs]

```
enabled = true
port = https,http,8007
filter = pbs
logpath = journal
backend = systemd
maxretry = 3
findtime = 2d
bantime = 1h
```

Bloc [PBS]

Bloc à ajouter dans le fichier en respectant la forme ci-contre. Ce bloc peut être copié en fin de fichier par exemple.

[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
```

Bloc [SSHD]

Coller le contenu du bloc dans le fichier, en respectant la forme ci-contre. **Attention, ce bloc existe déjà** (voir en milieu de fichier) et **il n'est pas utile de copier [sshd]** car le bloc est déjà identifié.

d) Configurer le filtre en créant le fichier "pbs.conf" et en ajoutant les éléments ci-dessous :

```
nano /etc/fail2ban/filter.d/pbs.conf
```

Éléments à ajouter au fichier :

[Definition]

```
failregex = pvedaemon\[.*authentication failure; rhost=<HOST> user=.* msg=.*
ignoreregex =
```

e) [Désactivation de la gestion des adresses IPv6 \(si elles ne sont pas gérées\)](#)

Si les adresses IPv6 ne sont pas gérées, la désactivation se fait au niveau du fichier « fail2ban.conf » dans le groupe **[Définitions]** :

```
nano /etc/fail2ban/fail2ban.conf
```

- Décommenter "allowipv6"
- Ajouter le paramètre "no"

```
# Option: allowipv6
# Notes.: Allows IPv6 interface:
#         Default: auto
# Values: [ auto yes (on, true, 1) no (off, false, 0) ] Default: auto
allowipv6 = no
```

f) [Créer le fichier « auth.log » et lui attribuer les droits nécessaires](#)

```
touch /var/log/auth.log
chmod 640 /var/log/auth.log
```

g) [Redémarrer Fail2ban et vérifier le statut](#)

```
systemctl restart fail2ban
systemctl status fail2ban
```

COMMANDES UTILES FAIL2BAN

Bannir une IP

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

Enlever le ban d'une IP

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

Lister les règles

```
fail2ban-client status
```

Status

```
| - Number of jail:  1
` - Jail list:  sshd
```

Afficher les détails d'une règle

```
fail2ban-client status sshd
```

Lister les tentatives de connexion

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

Lister les tentatives de connexion en temps réel

```
tail -f /var/log/auth.log
```

Toutes les étapes proposées dans ce tutoriel permettent de sécuriser, à minima, vos serveurs. Il ne s'agit, ici, que de recommandations de base et de nombreuses configurations supplémentaires peuvent être apportées.