Fail2ban

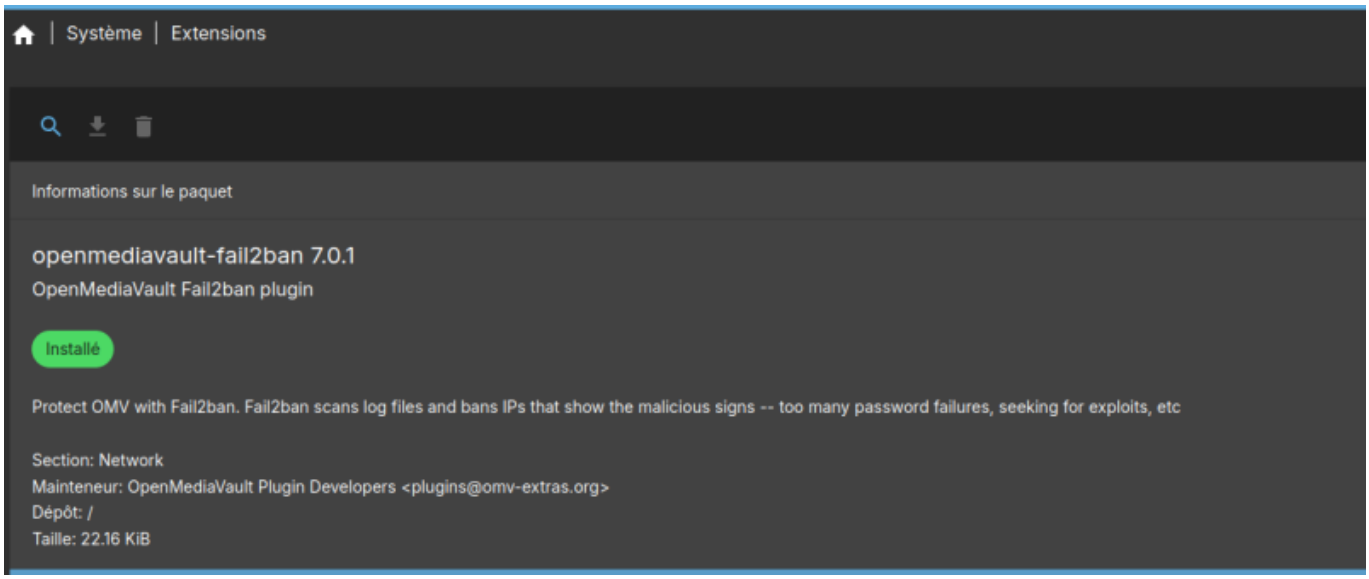
Definitions

Fail2ban est vraiment un outil puissant pour contrer des attaques par brutefoce et mitiger les attaques DoS.

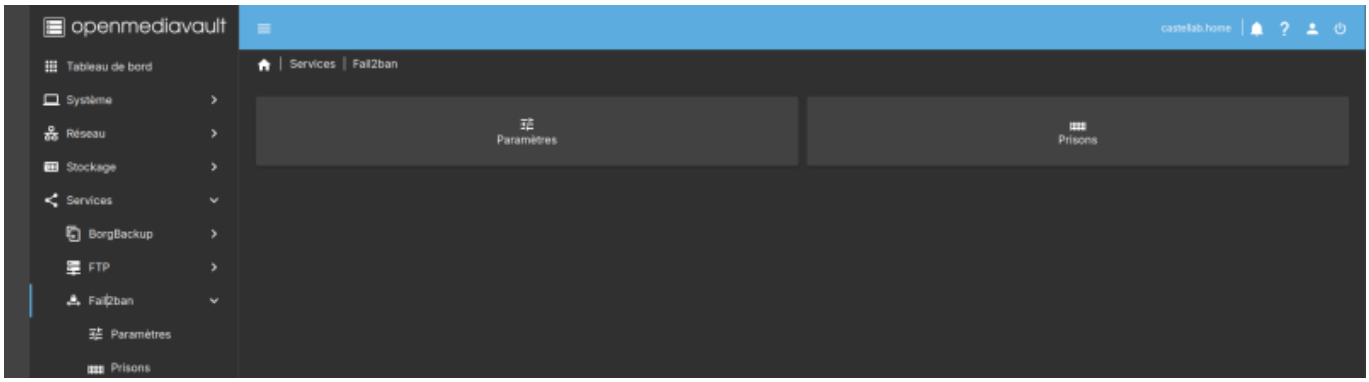
Fail2ban est donc un outil que l'on peut installer sur une machine UNIX ou LINUX, il va se charger de lire, parcourir les logs de différentes applications pour vérifier et détecter des comportements dis “suspects”. Il va par exemple savoir détecter un nombre X de tentatives d'authentification infructueuses sur une service SFTP, SSH, ou WEB ou détecter des requêtes anormales sur un services web tel qu'Apache2 ou Nginx.

Le fonctionnement de Fail2ban se fait avec des prisons. Globalement, une prison est un ou plusieurs services ou ports sur lesquels vont s'appliquer des règles et dans laquelle des IP ne respectant pas ces règles vont être mises. Une fois le comportement d'une IP détectée comme suspecte, une action est effectuée pour contrer cette IP. Par défaut il s'agit de bloquer l'IP en l'interdisant de communiquer avec le serveur pendant 600 secondes ou plus .... via des règles Iptables (pare-feu par défaut de beaucoup de distributions UNIX ou LINUX).

Installer le plugin openmediavault-fail2ban 7.0.1

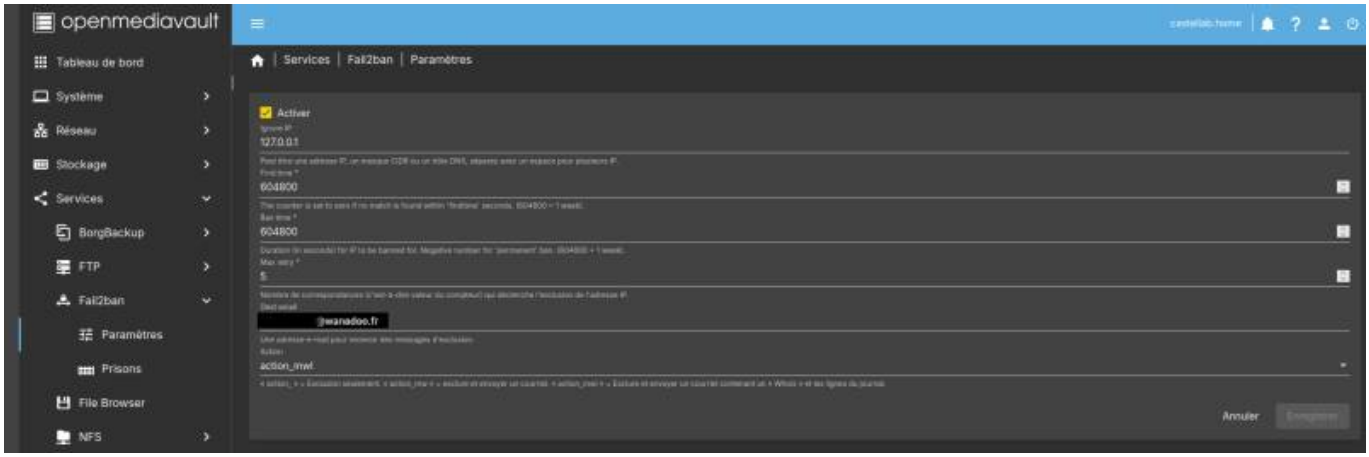


Configuration de Fail2ban



Il faut l'activer

Et bien sur remplir les parametres : les @IP non bloquées, le temps de blocage , etc ...



Activer le blocage des differentes connexions

Exemples : la connexion en ssh, **la connexion à OMV** , ...

les parametres : Nom :nginx-404, les ports : http,https, MAX d'essais : 3 (Nombre de correspondances (c'est-à-dire valeur du compteur) qui déclenche l'exclusion de l'adresse IP.) ,Temps d'exclusion en secondes : -1 (Toujours), le filtre d'exclusion :nginx-404, Le chemin du repertoire du Log de l'exclusion : /var/log/nginx*/*access*.log