

# Failban

## Installer le plugin openmediavault-fail2ban 7.0.1

The screenshot shows the OpenMediaVault package manager interface. At the top, there are navigation links: 'Système' and 'Extensions'. Below that is a search bar with a magnifying glass icon, a download icon, and a trash bin icon. The main content area is titled 'Informations sur le paquet'. It displays the package name 'openmediavault-fail2ban 7.0.1' and its description 'OpenMediaVault Fail2ban plugin'. A green button labeled 'Installé' indicates it is already installed. Below the description, there is a brief summary: 'Protect OMV with Fail2ban. Fail2ban scans log files and bans IPs that show the malicious signs -- too many password failures, seeking for exploits, etc'. Further down, it lists the section as 'Network', the maintainer as 'OpenMediaVault Plugin Developers <plugins@omv-extras.org>', the repository as '/ ', and the size as '22.16 KiB'.

## Configuration de Failban

The screenshot shows the OpenMediaVault web interface. On the left is a sidebar menu with the following items: Tableau de bord, Système, Réseau, Stockage, Services (with BorgBackup, FTP, Fail2ban), Paramètres, and Prisons. The main content area has a blue header bar with the text 'Services | Fail2ban'. The main content area contains two tabs: 'Paramètres' (selected) and 'Prisons'. The 'Paramètres' tab is currently active.

## Il faut l'activer

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

Last update: 2025/01/19 12:56  
start:raspberry:nas:securite https://www.fablab37110.chanterie37.fr/doku.php?id=start:raspberry:nas:securite&rev=1737287799

The screenshot shows the openmediavault web interface with the sidebar menu expanded. The main content area is titled "Fail2ban" and displays a configuration form for a new rule named "nginx-404". The form includes fields for "Nom" (nginx-404), "Port" (http, https), "Max retry" (3), "Temps d'exclusion en secondes" (-1), and a "Filtre" section containing the regex pattern "/var/log/nginx/\*access\*.log". At the bottom right of the form are "Annuler" and "Enregistrer" buttons.

## Activer le blocage des différentes connexions

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

les paramètres : 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 répertoire du Log de l'exclusion : /var/log/nginx/\*access\*.log

The screenshot shows the openmediavault web interface with the sidebar menu expanded. The main content area is titled "Fail2ban" and displays a configuration form for an existing rule named "nginx-404". The form includes fields for "Nom" (nginx-404), "Port" (http, https), "Max retry" (3), "Temps d'exclusion en secondes" (-1), and a "Filtre" section containing the regex pattern "/var/log/nginx/\*access\*.log". At the bottom right of the form are "Annuler" and "Enregistrer" buttons.

From:  
<https://www.fablab37110.chanterie37.fr/> - Castel'Lab le Fablab MJC de Château-Renault

Permanent link:  
<https://www.fablab37110.chanterie37.fr/doku.php?id=start:raspberry:nas:securite&rev=1737287799>

Last update: 2025/01/19 12:56

