

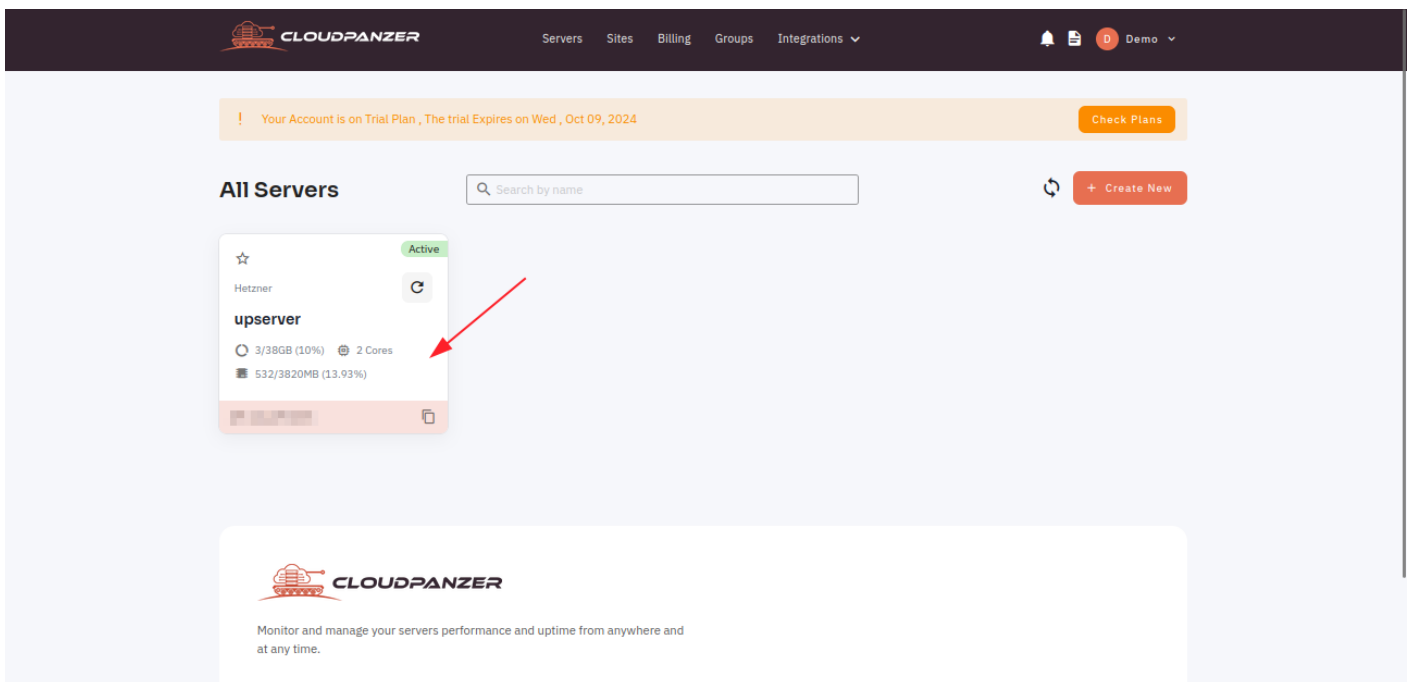
How to add Filters in Fail2Ban on CloudPanzer?

In Fail2Ban, filters are essential components used to define patterns and rules that detect malicious or suspicious behavior in log files. Filters enable Fail2Ban to identify specific events or actions within log entries and subsequently take actions, such as banning IP addresses, based on these patterns. Each service monitored by Fail2Ban typically has its own filter, which specifies what to look for in the logs.

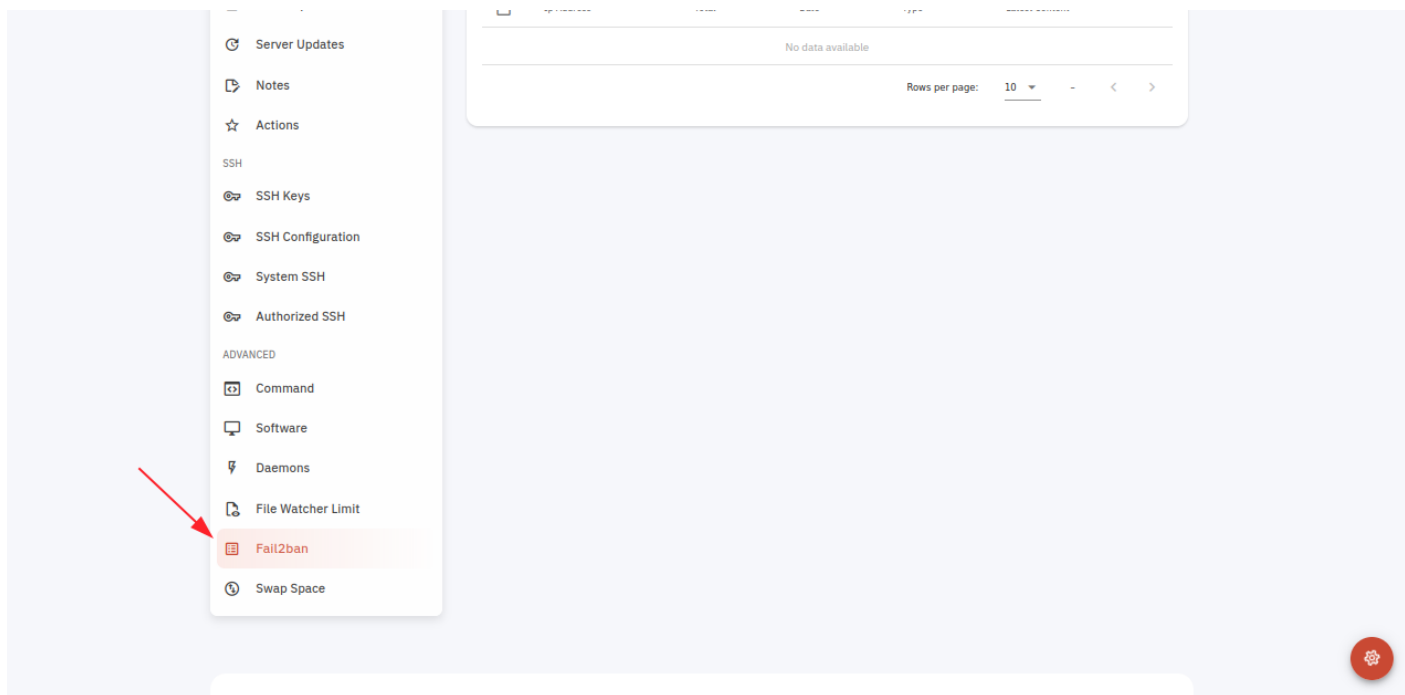
How to install a Server

Follow the steps below to add Filters in Fail2Ban.

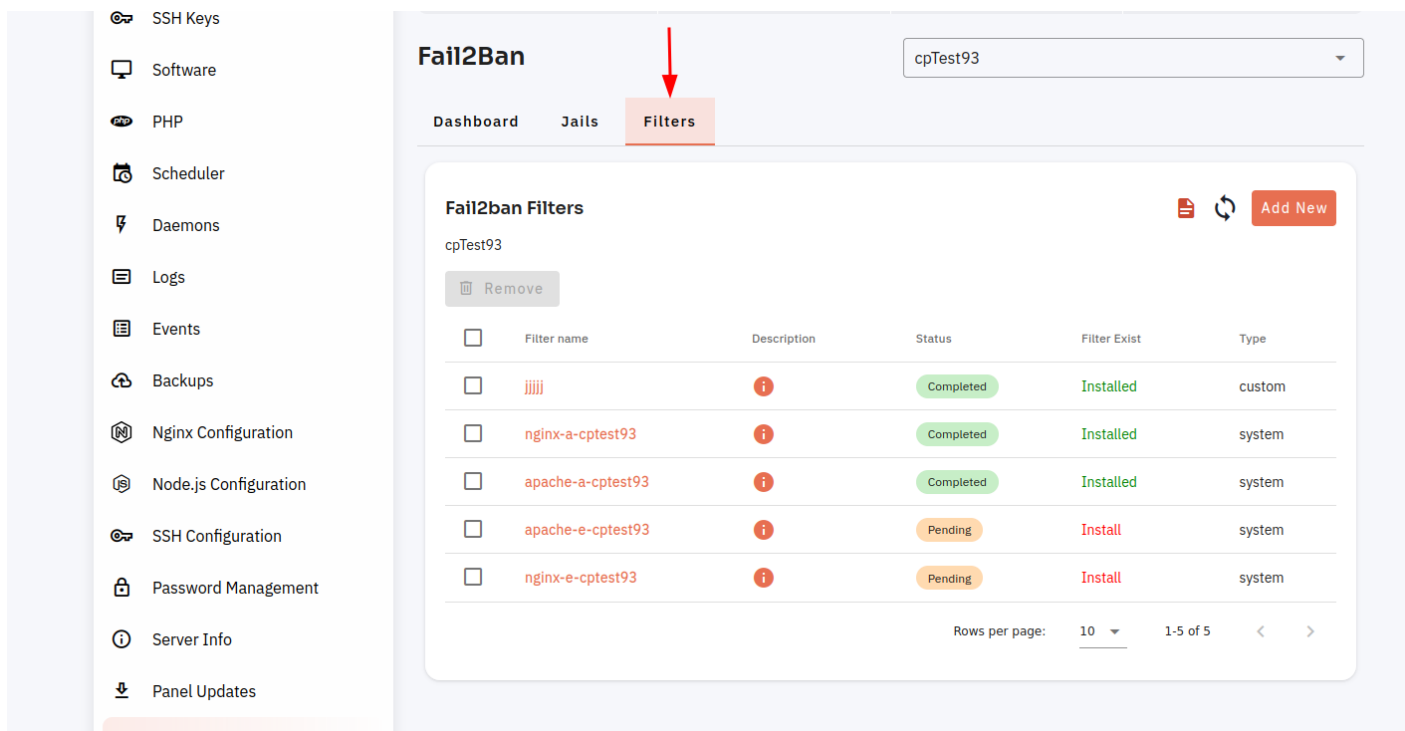
1: Once you are logged in, look for a "Server" and click on it.



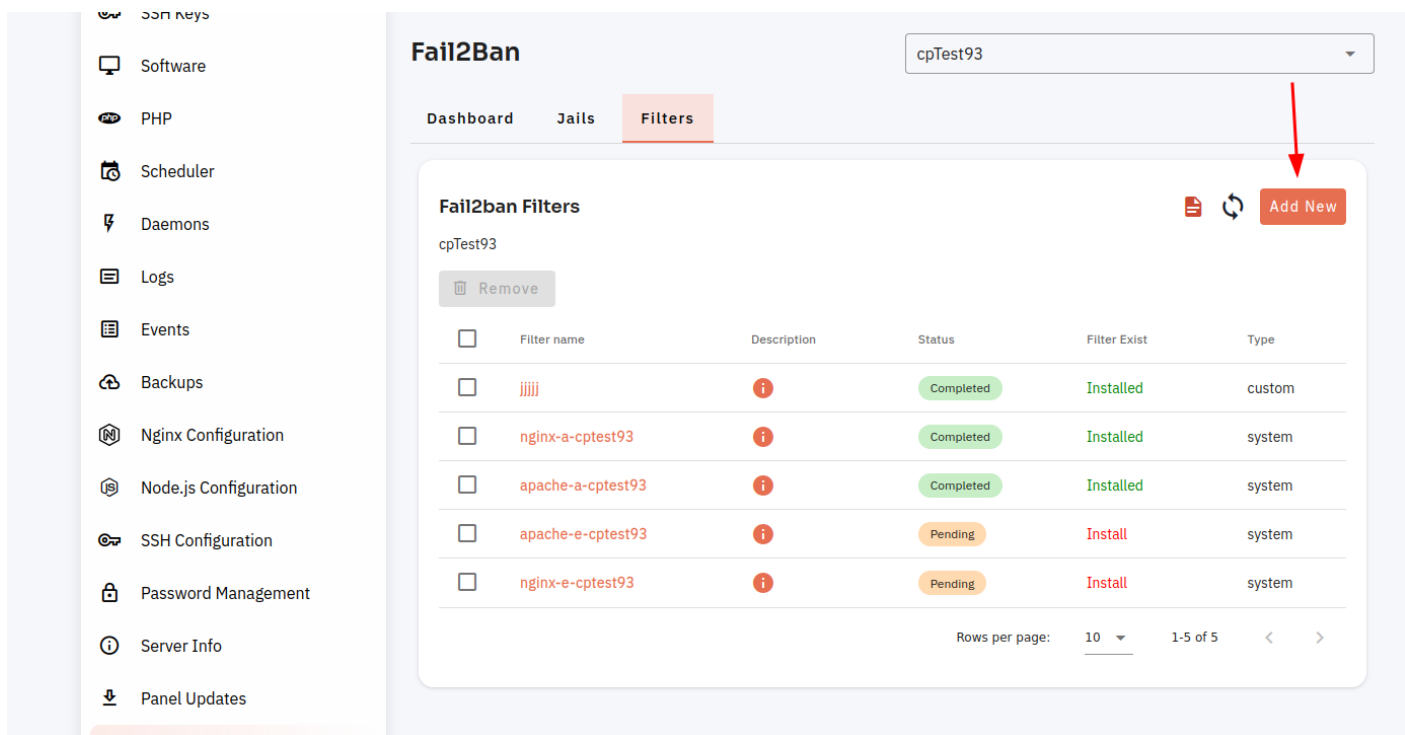
2. Select the Fail2ban option.



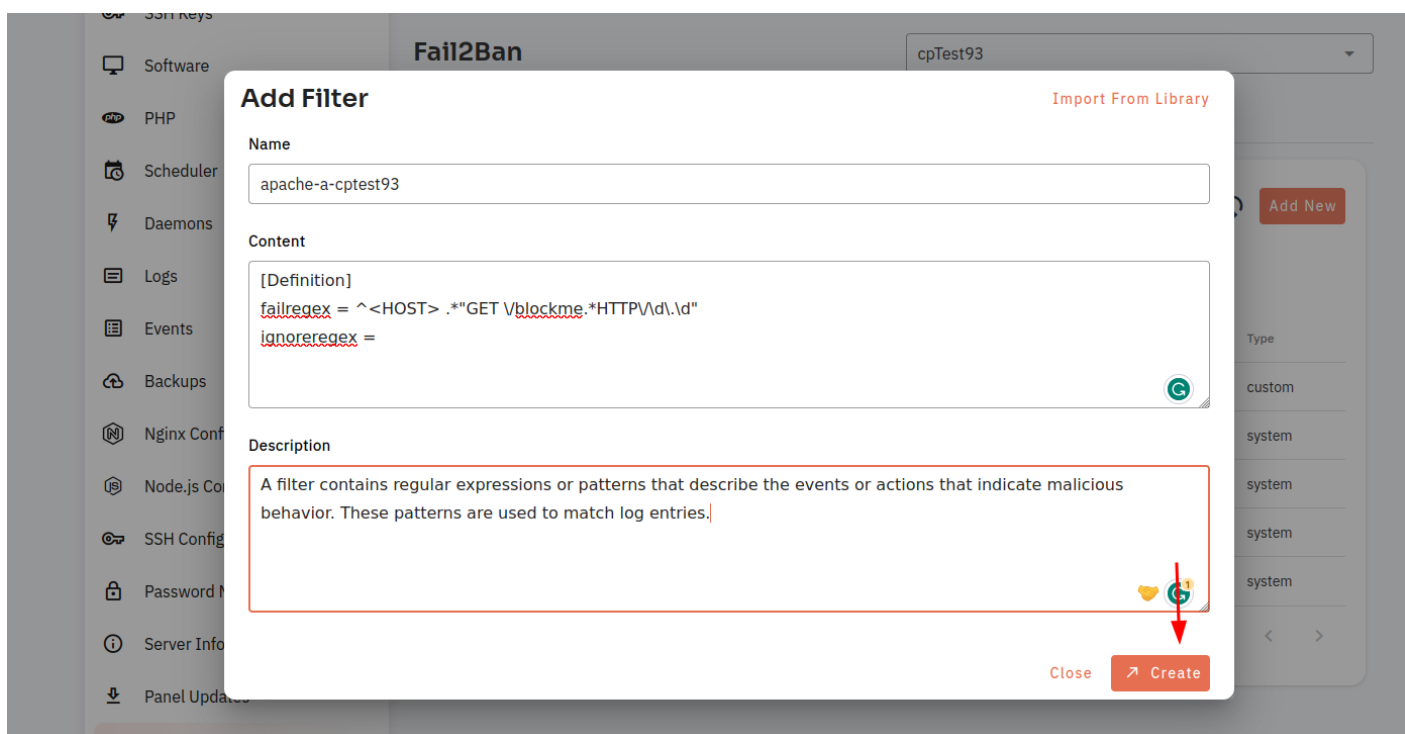
3. Click on the Filters button.



4. Click on the Add New button.



5. Fill in the details and click on the Create button. Then click on the Create button.



6. Here, a new filter has been created. You can also check events by clicking on the file icon.

SSH Keys

Software

PHP

Scheduler

Daemons

Logs

Events

Backups

Nginx Configuration

Node.js Configuration

SSH Configuration

Password Management

Server Info

Panel Updates

Fail2Ban

cpTest93

DashboardJailsFilters

Fail2ban Filters

cpTest93

Remove

Filter name

Description

Status

Filter Exist

Type

apache-a-cptest93

Completed

Installed

custom

jijiji

Completed

Installed

custom

nginx-a-cptest93

Completed

Installed

system

apache-a-cptest93

Completed

Installed

system

apache-e-cptest93

Pending

Install

system

nginx-e-cptest93

Pending

Install

system

Rows per page:

10

1-6 of 6

<

>

Add New

Looking for mobile App Instructions?

Available at: <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-create-filter-in-fail2ban-through-the-cloudpanzer-website>

Revision #7

Created 14 August 2023 10:59:24 by Admin

Updated 12 September 2024 08:33:05 by Admin