

Fail2Ban

- [How to add Filters in Fail2Ban on CloudPanzer?](#)
- [How to add Jails in Fail2Ban on CloudPanzer?](#)
- [How to Manage Fail2ban on CloudPanzer Servers?](#)

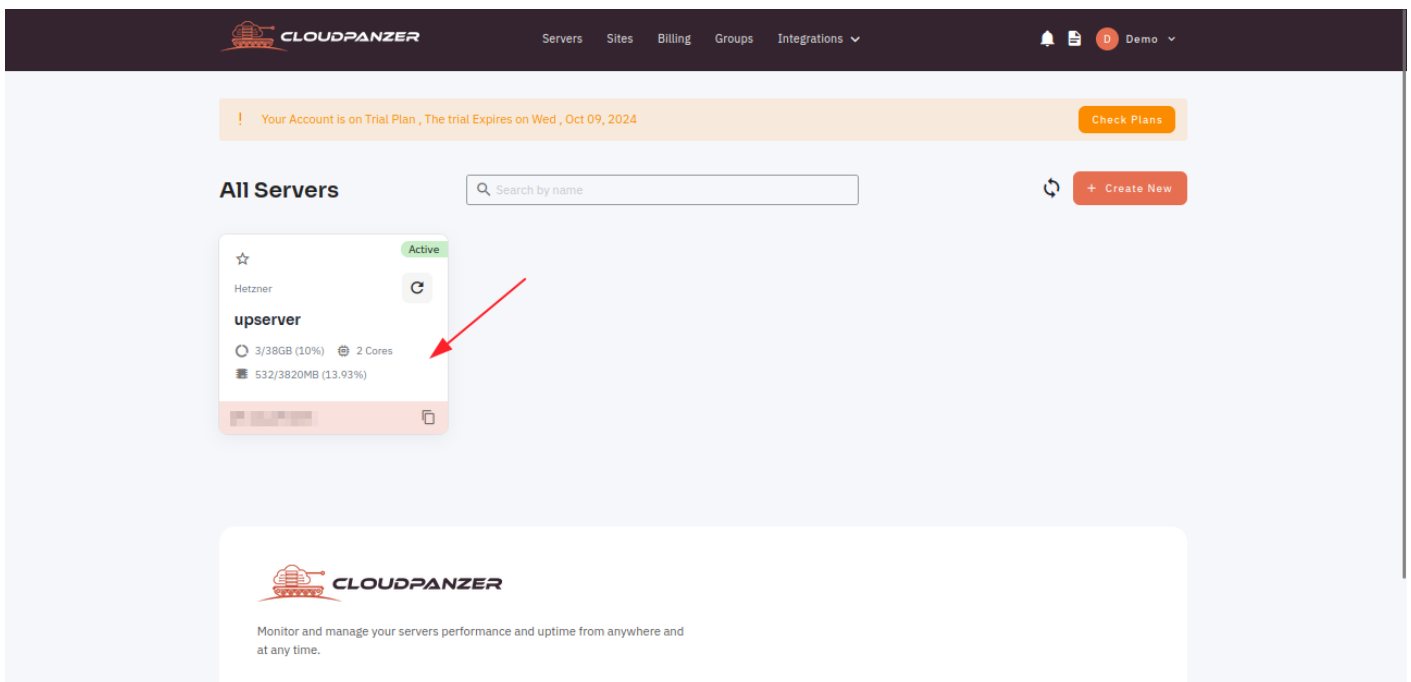
How to add Filters in Fail2Ban on CloudPanzer?

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.

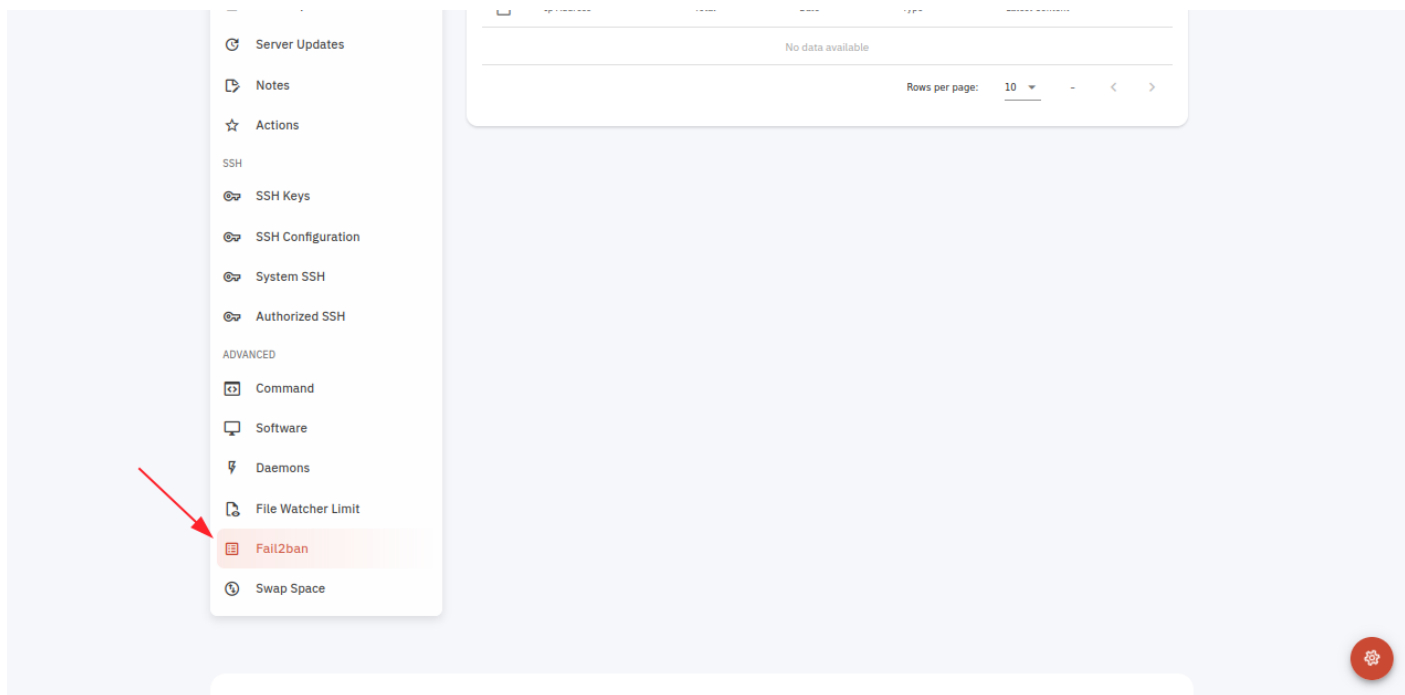
How to install a Server

Follow the steps below to add Filters in Fail2Ban.

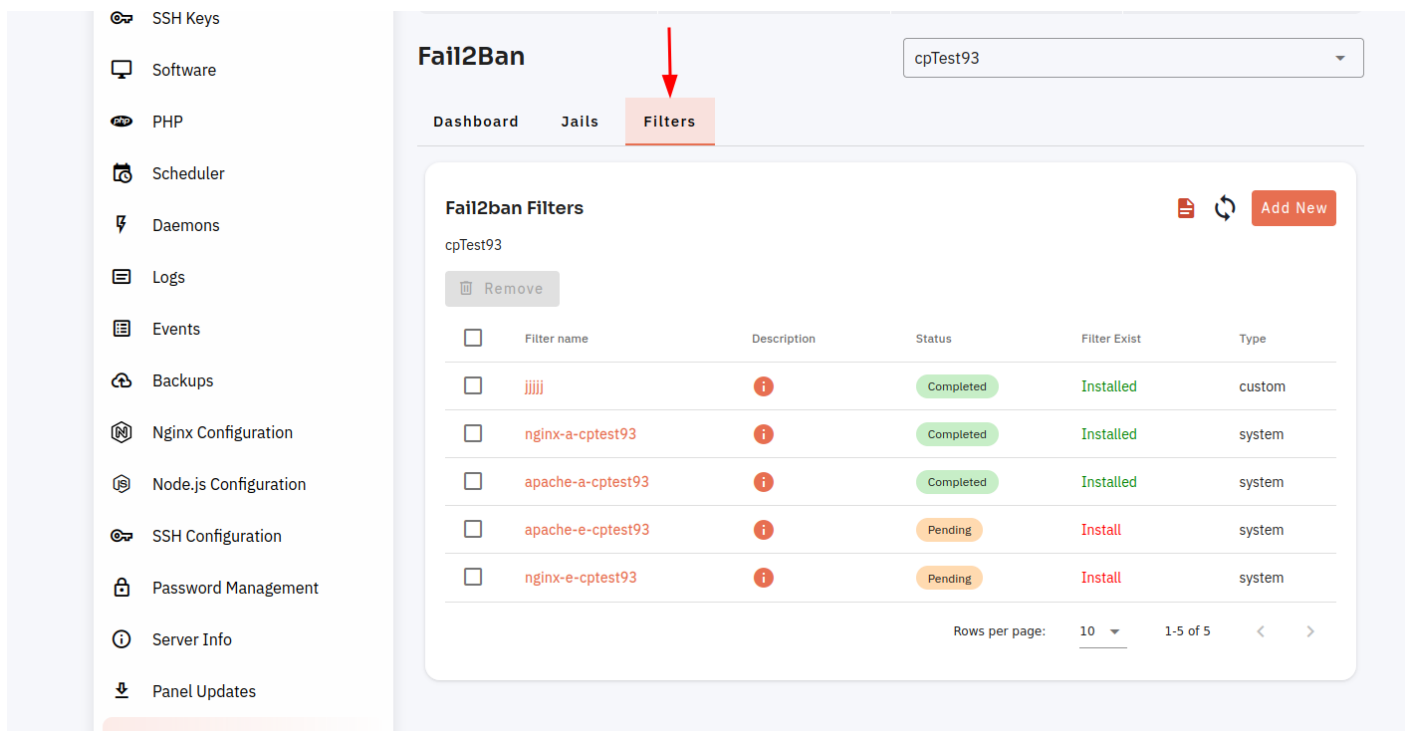
1: Once you are logged in, look for a "Server" and click on it.



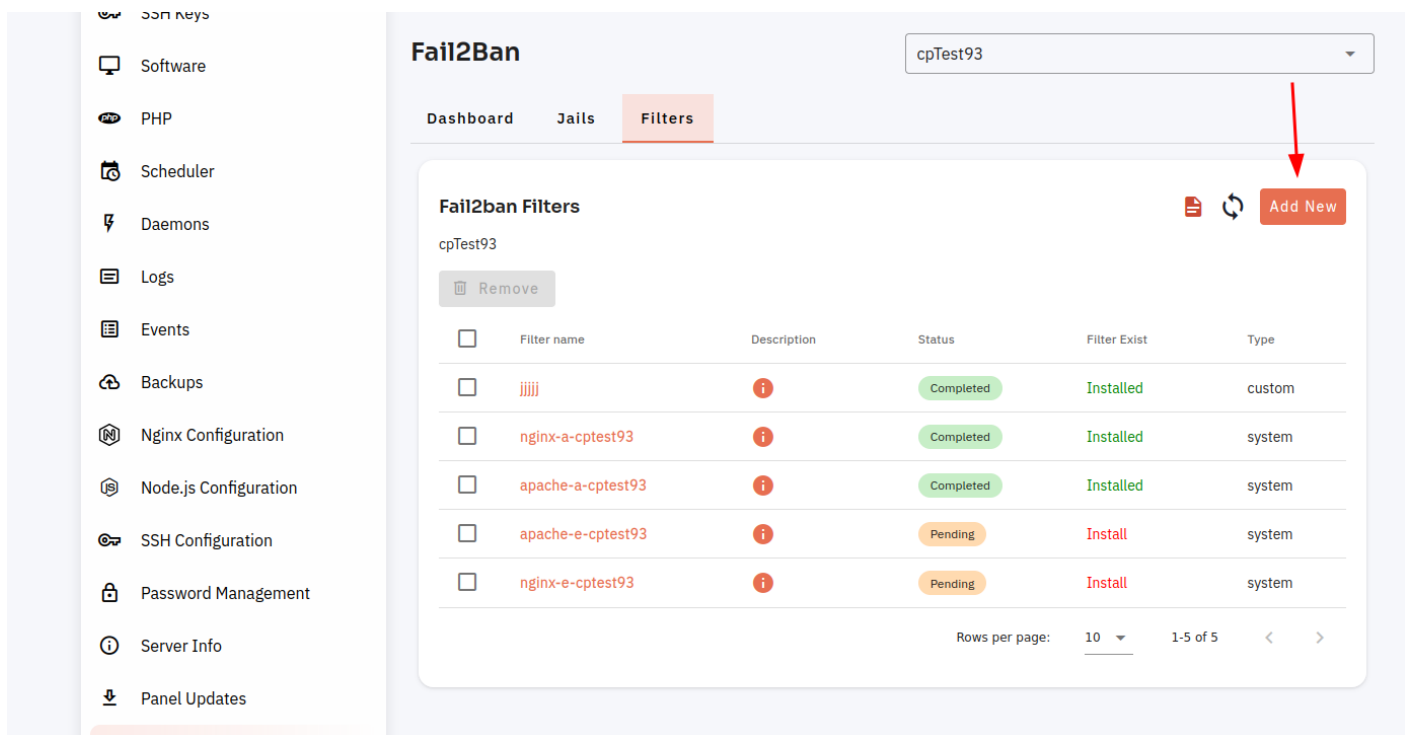
2. Select the Fail2ban option.



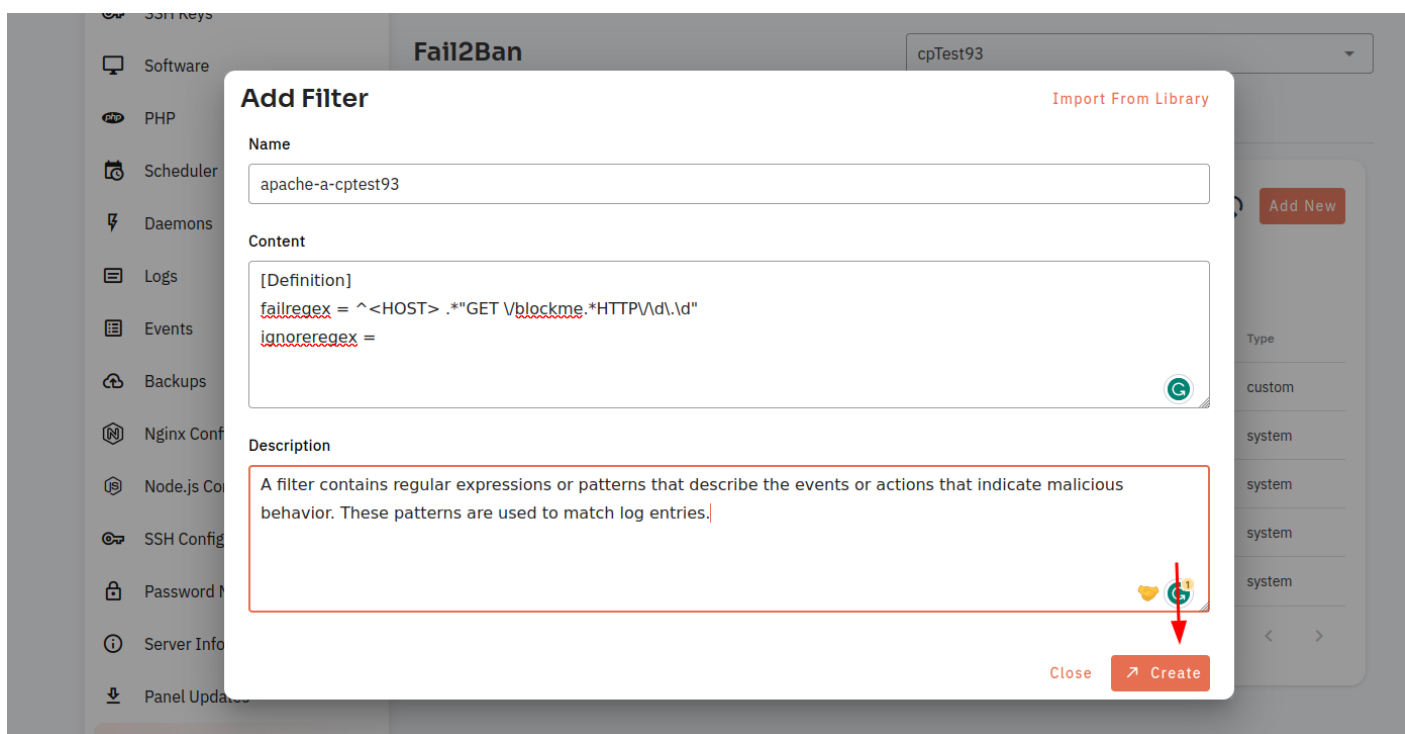
3. Click on the Filters button.



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

Ngix 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>

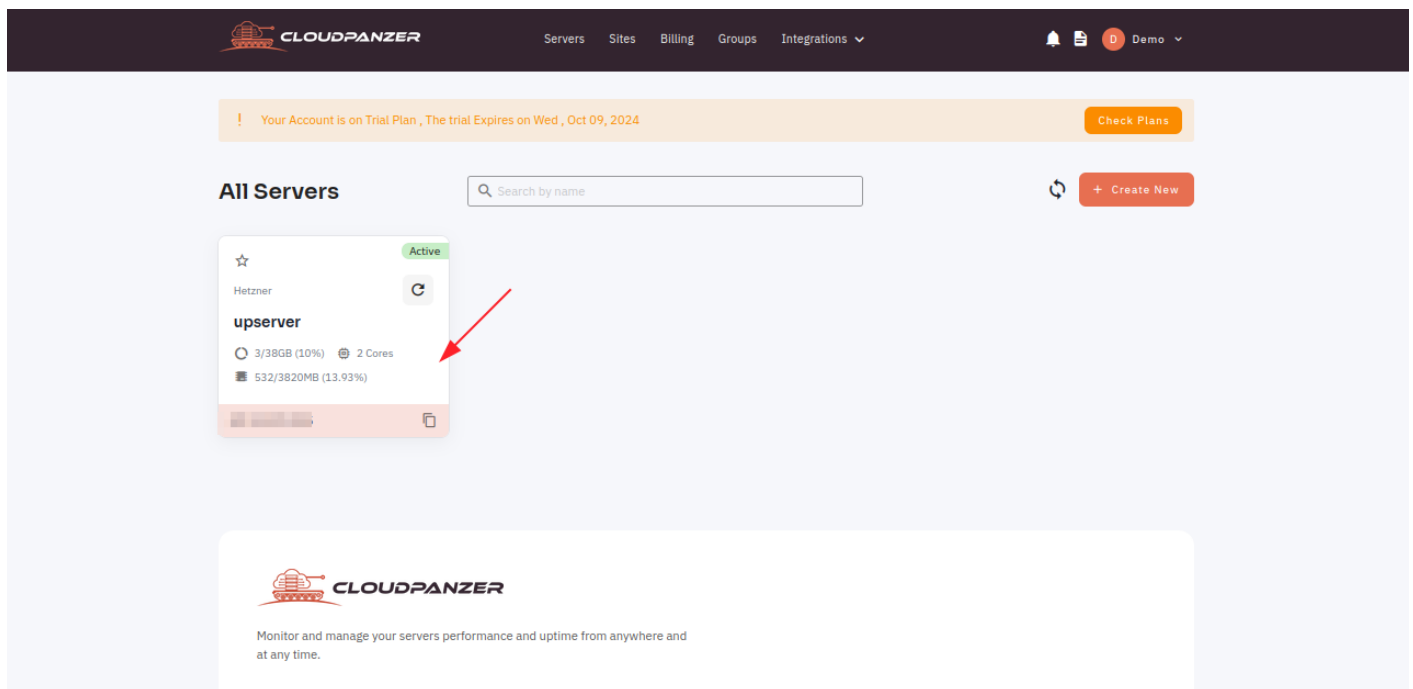
How to add Jails in Fail2Ban on CloudPanzer?

In Fail2Ban, a "jail" is a configuration section that specifies the rules, filters, actions, and settings for a particular service or application. Each jail is tailored to monitor a specific log file, detect certain patterns, and apply actions (such as banning an IP address) when those patterns are identified.

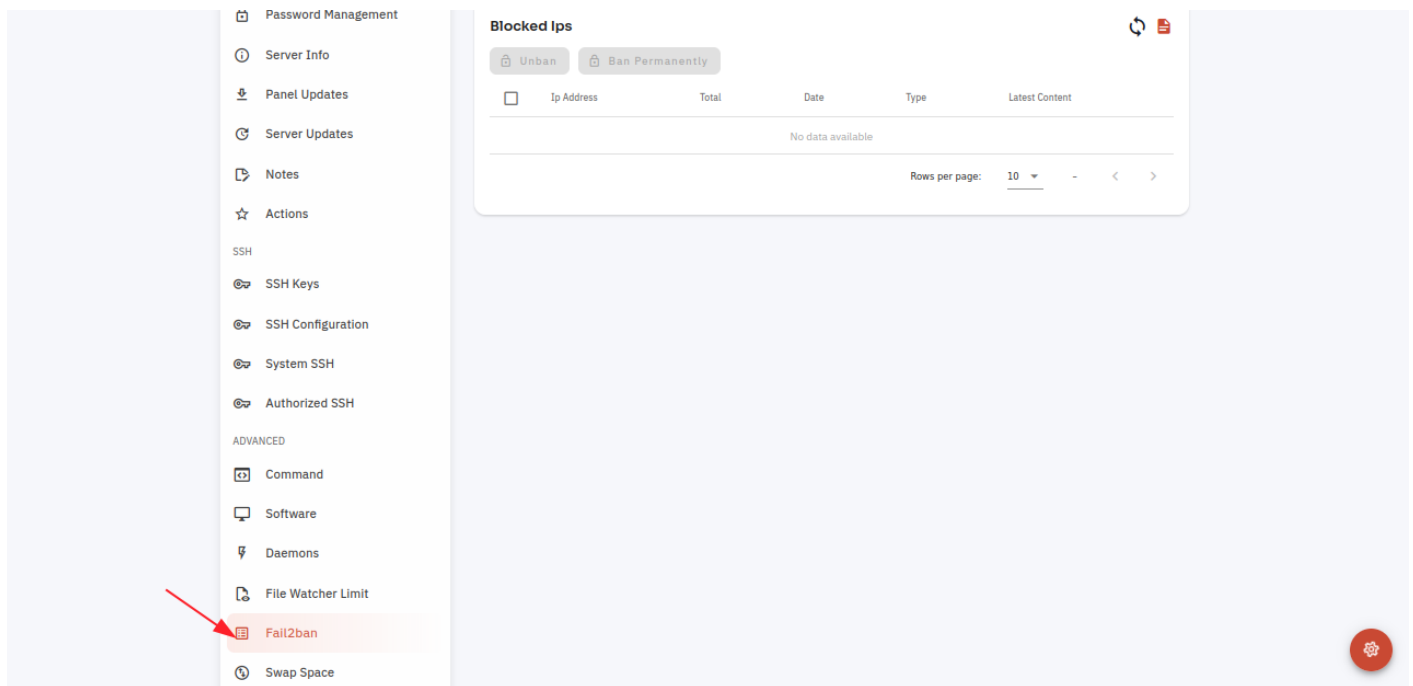
How to install a Server

Follow the steps below to add Jails in Fail2Ban.

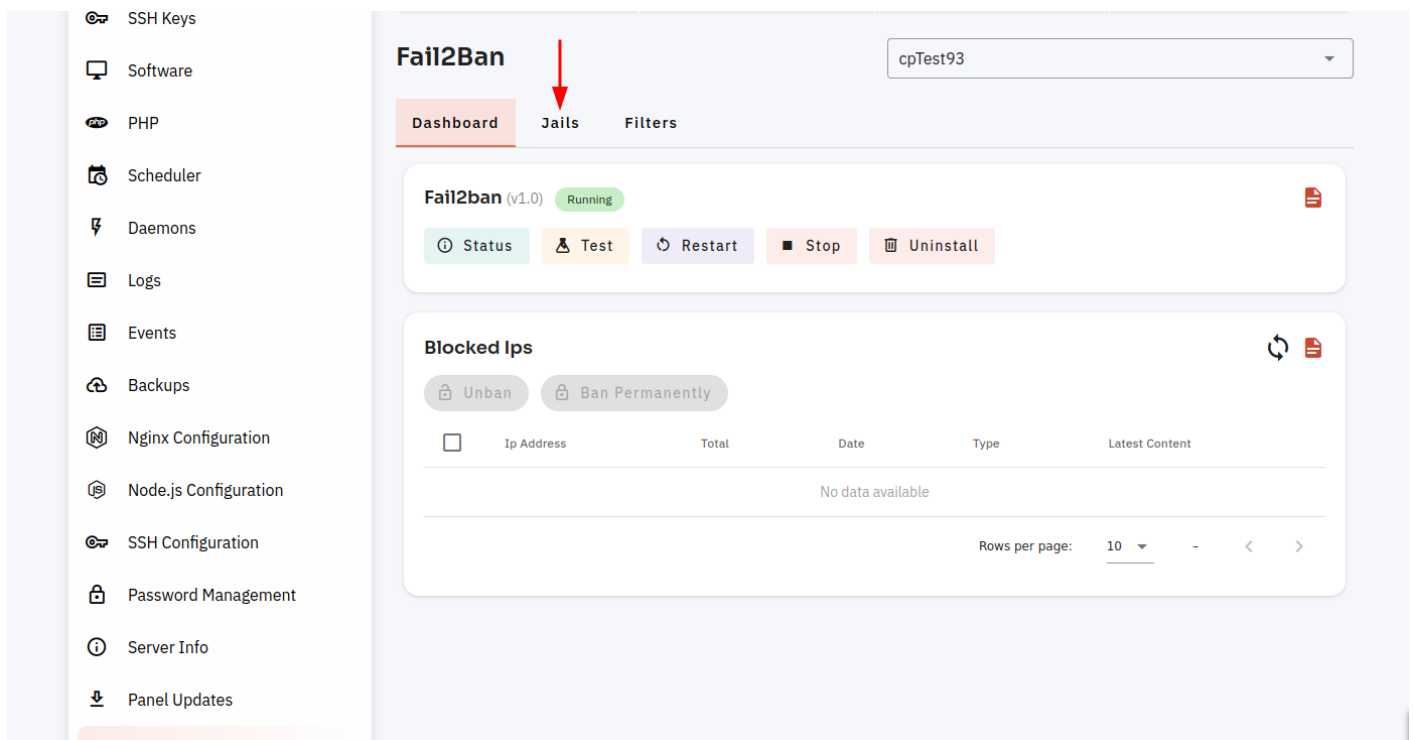
1: Once you are logged in, look for a "Server" and click on it.



2. Select the Fail2ban option.



3. Click on the jails button.



4. Click on the Add New Button.

Fail2Ban cpTest93

Dashboard **Jails** Filters

Fail2ban Jails cpTest93

Switch On Switch Off Remove

<input type="checkbox"/>	Jail name	Desc	Status	Jail Exist	Type	Active Status
<input type="checkbox"/>	testjail	i	Completed	Installed	custom	InActive
<input type="checkbox"/>	abc	i	Completed	Installed	custom	InActive
<input type="checkbox"/>	apache-e-cptest93	i	Pending	Install	system	InActive
<input type="checkbox"/>	nginx-e-cptest93	i	Pending	Install	system	InActive
<input type="checkbox"/>	apache-a-cptest93	i	Pending	Install	system	InActive
<input type="checkbox"/>	sshd	i	Pending	Install	system	InActive
<input type="checkbox"/>	nginx-a-cptest93	i	Pending	Install	system	InActive

Rows per page: 10 1-7 of 7

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

Add Jail

Name: apache-e-cptest94

Select Filter: apache-a-cptest93

Log Path: /var/log/apache2/error.log From Existing

IP address ban period (seconds): 50 The maximum number of failed login attempts: 5

Trusted Ips:

Description: The action can involve dynamically adding the offending IP address to a firewall rule, effectively blocking any further connections from that IP.

Close Create

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

Fail2Ban

cpTest93

Dashboard Jails Filters

Fail2ban Jails




cpTest93

Switch On Switch Off Remove

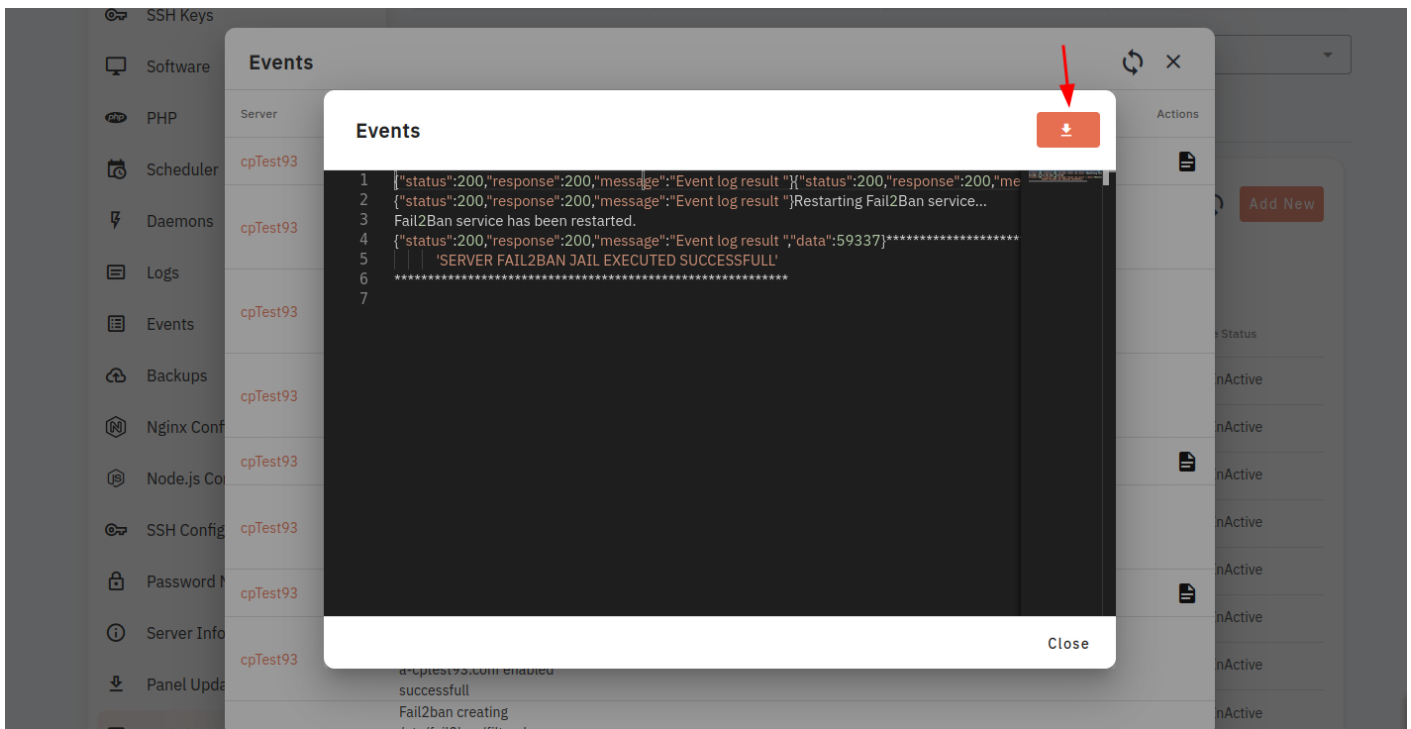
<input type="checkbox"/>	Jail name	Desc	Status	Jail Exist	Type	Active Status
<input type="checkbox"/>	apache-e-cptest94	i	Completed	Installed	custom	InActive
<input type="checkbox"/>	testjail	i	Completed	Installed	custom	InActive
<input type="checkbox"/>	abc	i	Completed	Installed	custom	InActive
<input type="checkbox"/>	apache-e-cptest93	i	Pending	Install	system	InActive
<input type="checkbox"/>	nginx-e-cptest93	i	Pending	Install	system	InActive
<input type="checkbox"/>	apache-a-cptest93	i	Pending	Install	system	InActive
<input type="checkbox"/>	sshd	i	Pending	Install	system	InActive
<input type="checkbox"/>	nginx-a-cptest93	i	Pending	Install	system	InActive

7. Here, a list of events has been displayed. You can check logs by clicking on the file icon.

Events

Server	Event	User	When	Actions
cpTest93	Setup Build successfully	John Doe	Mon , Aug 14, 2023 - 4:07 pm	
cpTest93	Fail2ban /etc/fail2ban /filter.d/apache-a-cptest93.conf enabled successfull	John Doe	Mon , Aug 14, 2023 - 4:07 pm	
cpTest93	Fail2ban creating /etc/fail2ban/filter.d /apache-a-cptest93.conf file	John Doe	Mon , Aug 14, 2023 - 4:07 pm	
cpTest93	Fail2ban /etc/fail2ban /filter.d/nginx-a-cptest93.conf enabled successfull	John Doe	Mon , Aug 14, 2023 - 3:19 pm	
cpTest93	Setup Build successfully	John Doe	Mon , Aug 14, 2023 - 3:19 pm	
cpTest93	Fail2ban creating /etc/fail2ban/filter.d /nginx-a-cptest93.conf file	John Doe	Mon , Aug 14, 2023 - 3:18 pm	
cpTest93	Setup Build successfully	John Doe	Mon , Aug 14, 2023 - 12:23 pm	
cpTest93	Fail2ban /etc/fail2ban /filter.d/apache-a-cptest93.conf enabled successfull	John Doe	Mon , Aug 14, 2023 - 12:23 pm	
cpTest93	Fail2ban creating			

8. Here, the event logs have been displayed. You can download it by clicking on the download button.



Looking for Web Instructions?

Available at <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-server-info-server-username>

How to Manage Fail2ban on CloudPanzer Servers?

Adding Fail2ban jails to your server helps enhance security by automatically blocking malicious IP addresses attempting to access your system. Fail2ban monitors logs and enforces bans or restrictions based on predefined rules called jails.

How to install a Server

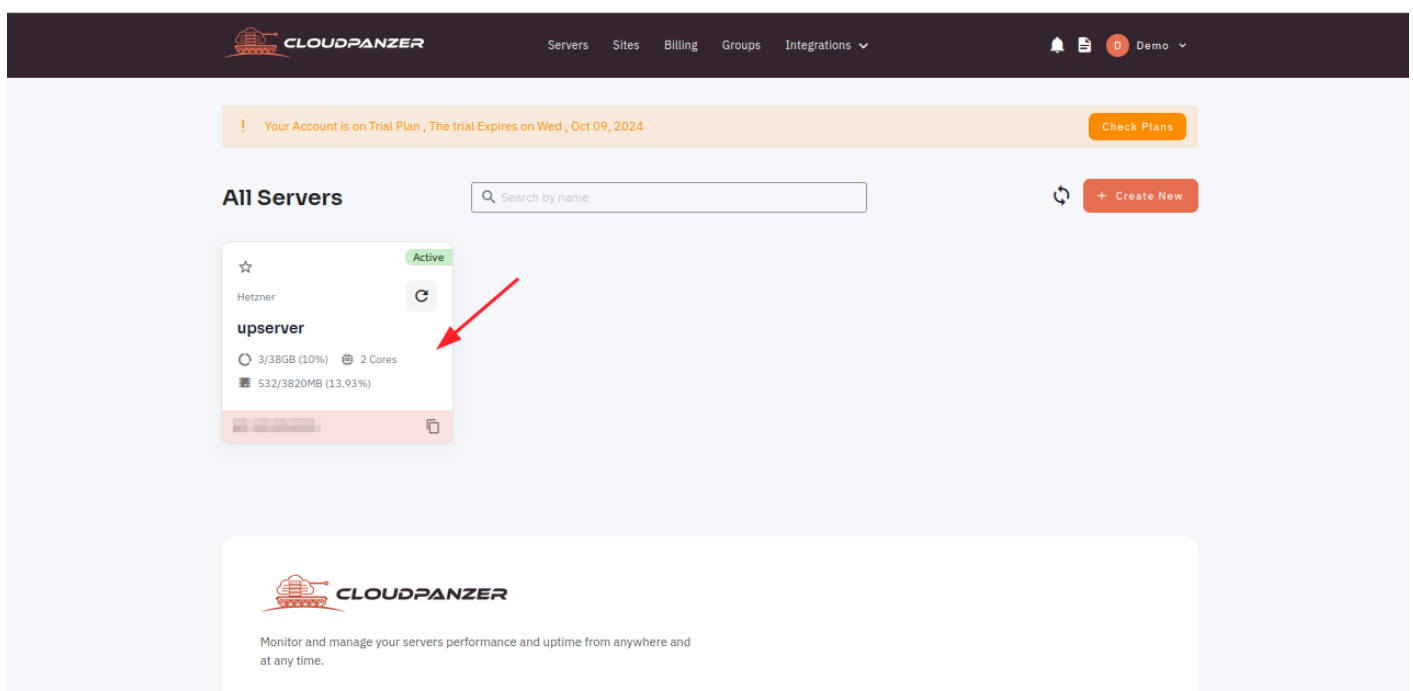
Tutorial :

You can watch the Video or Continue reading the post.

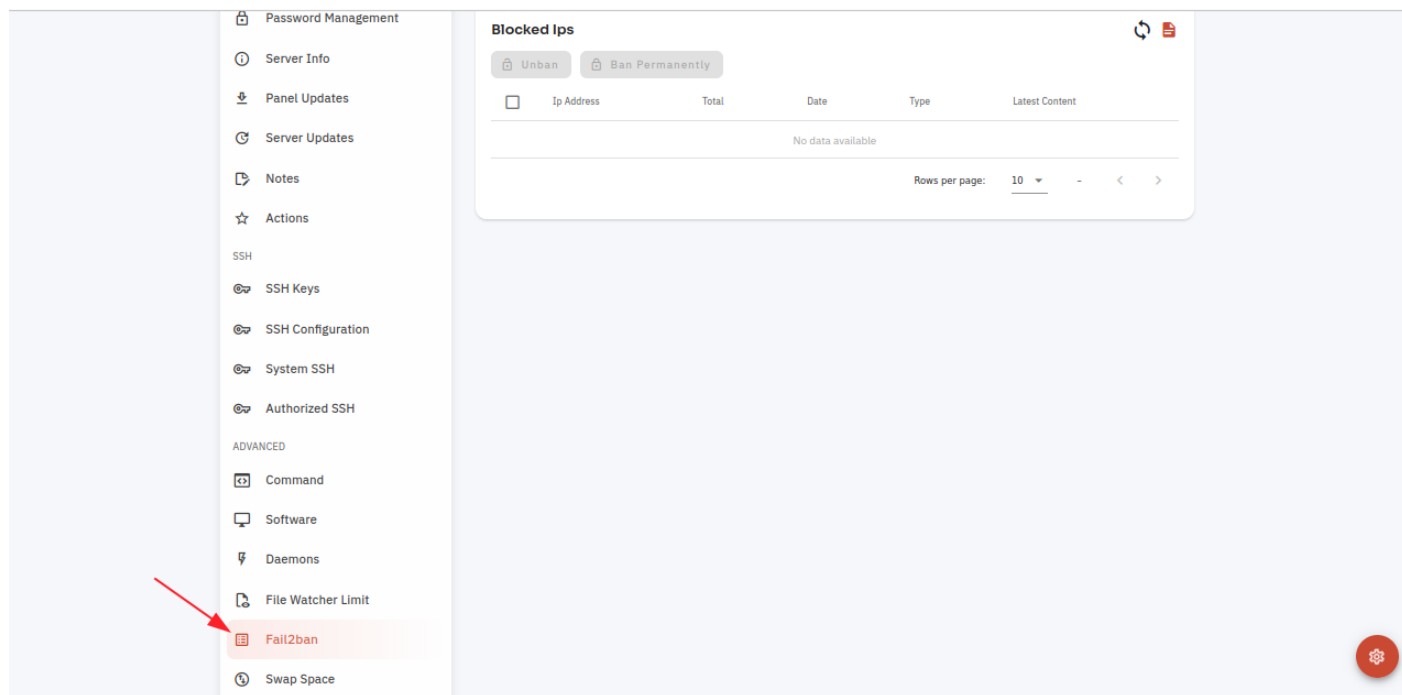
<https://www.youtube.com/embed/3pzI-vMFSMA>

Follow the steps below to add Fail2ban Jails to the server.

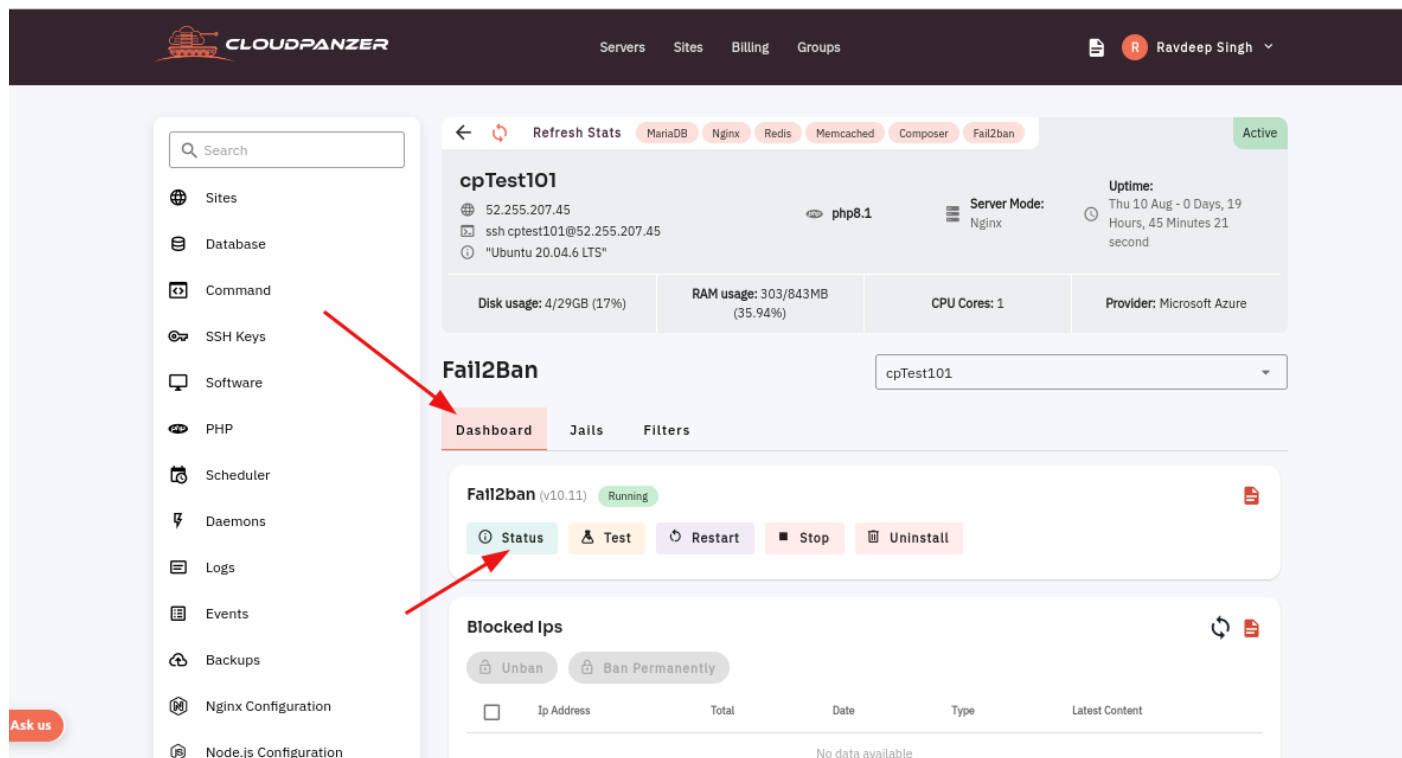
1: Once you are logged in, look for a "Server" and click on it.



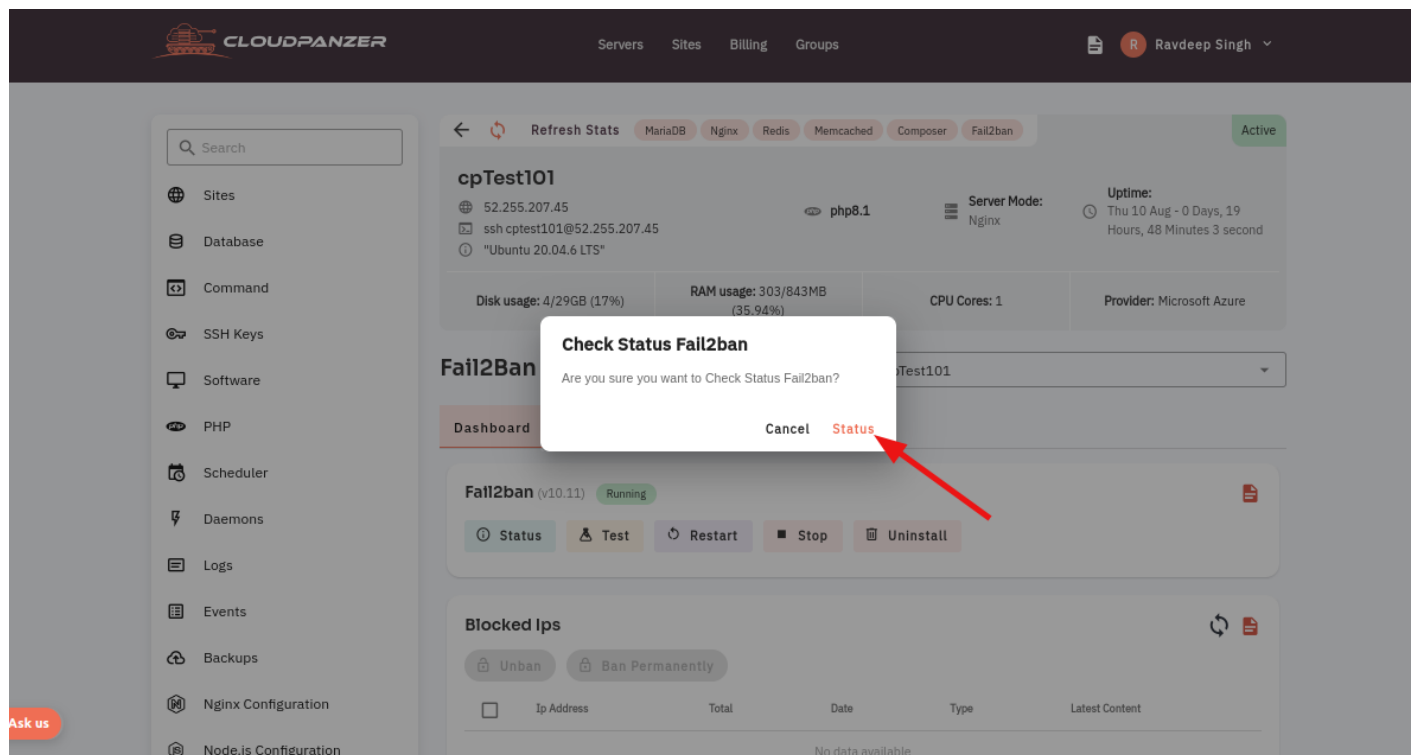
2. Select the Fail2ban option.



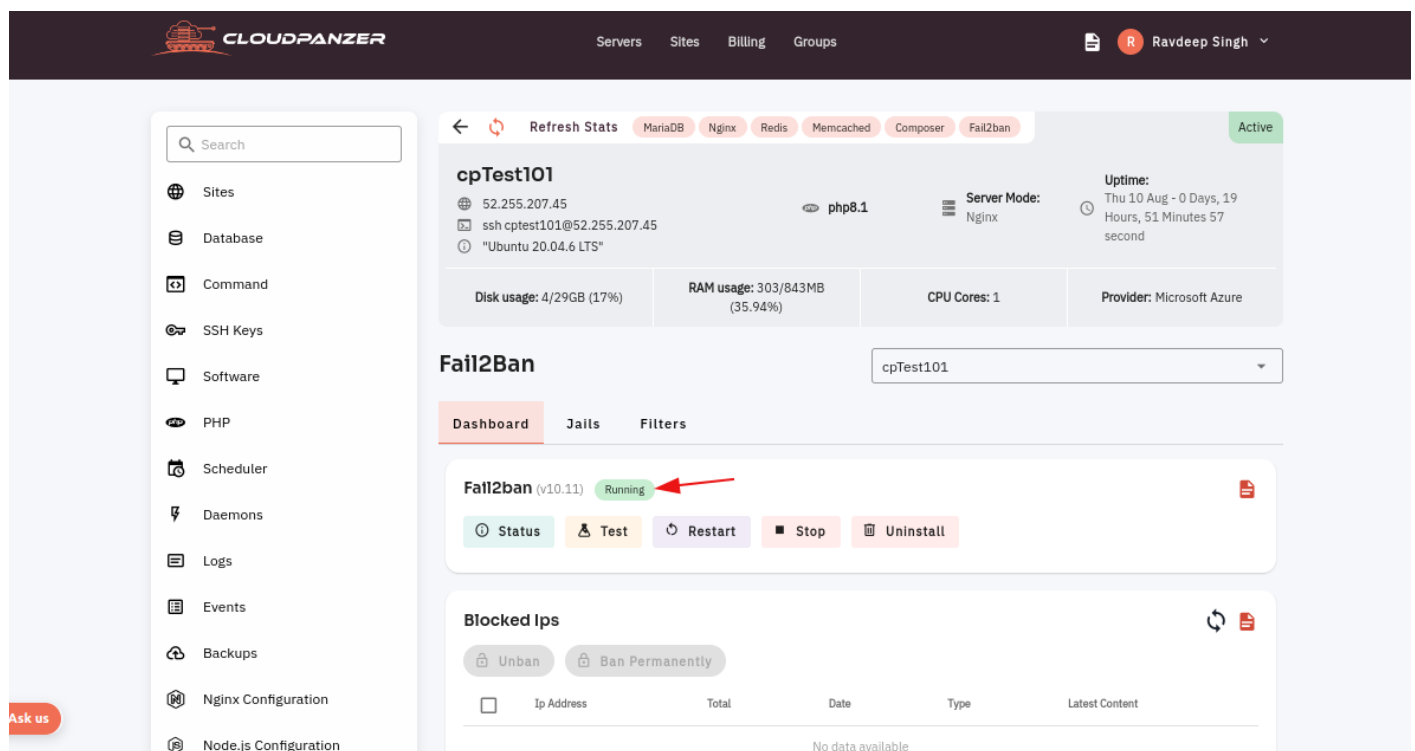
3. Select a Dashboard tab and click on the Status button.



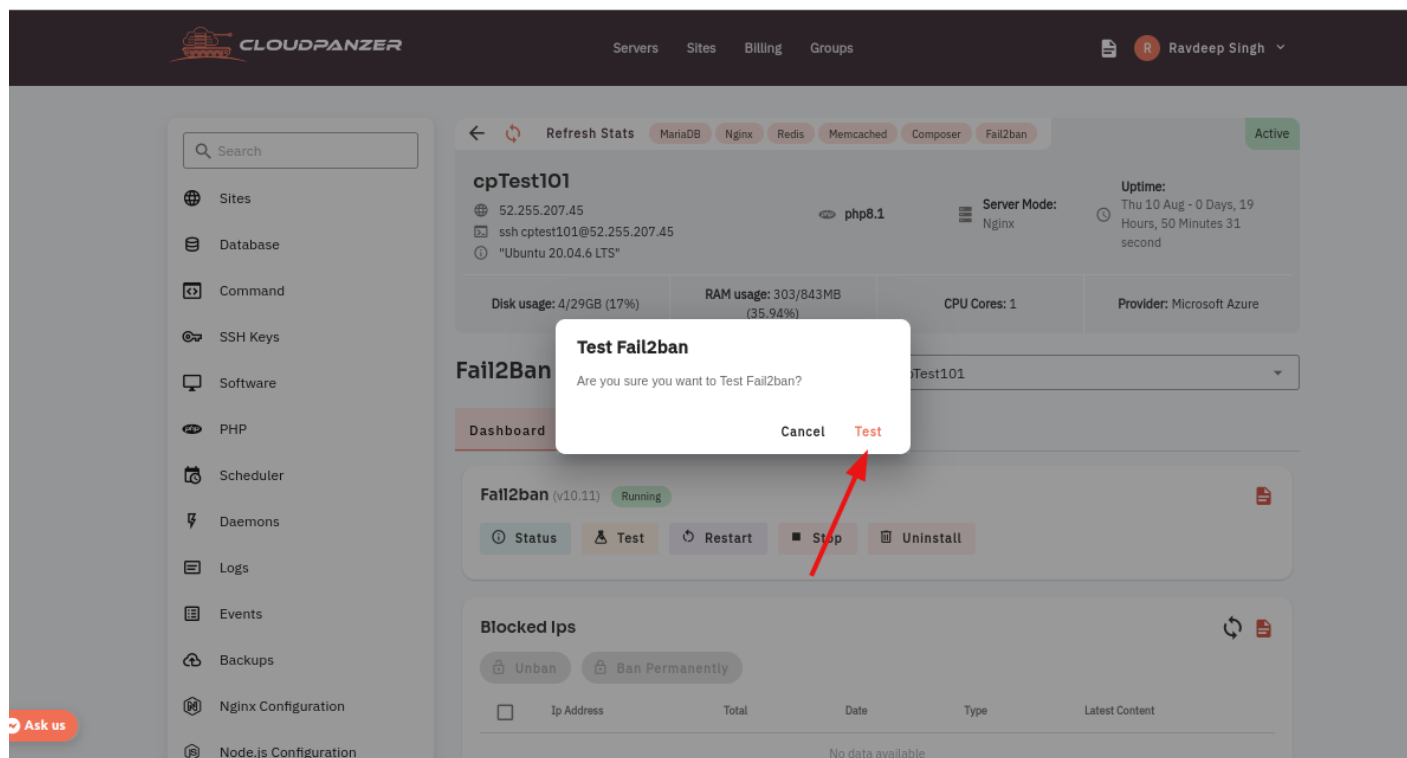
4. A dialog box will open and click on the Yes button to check the Status.



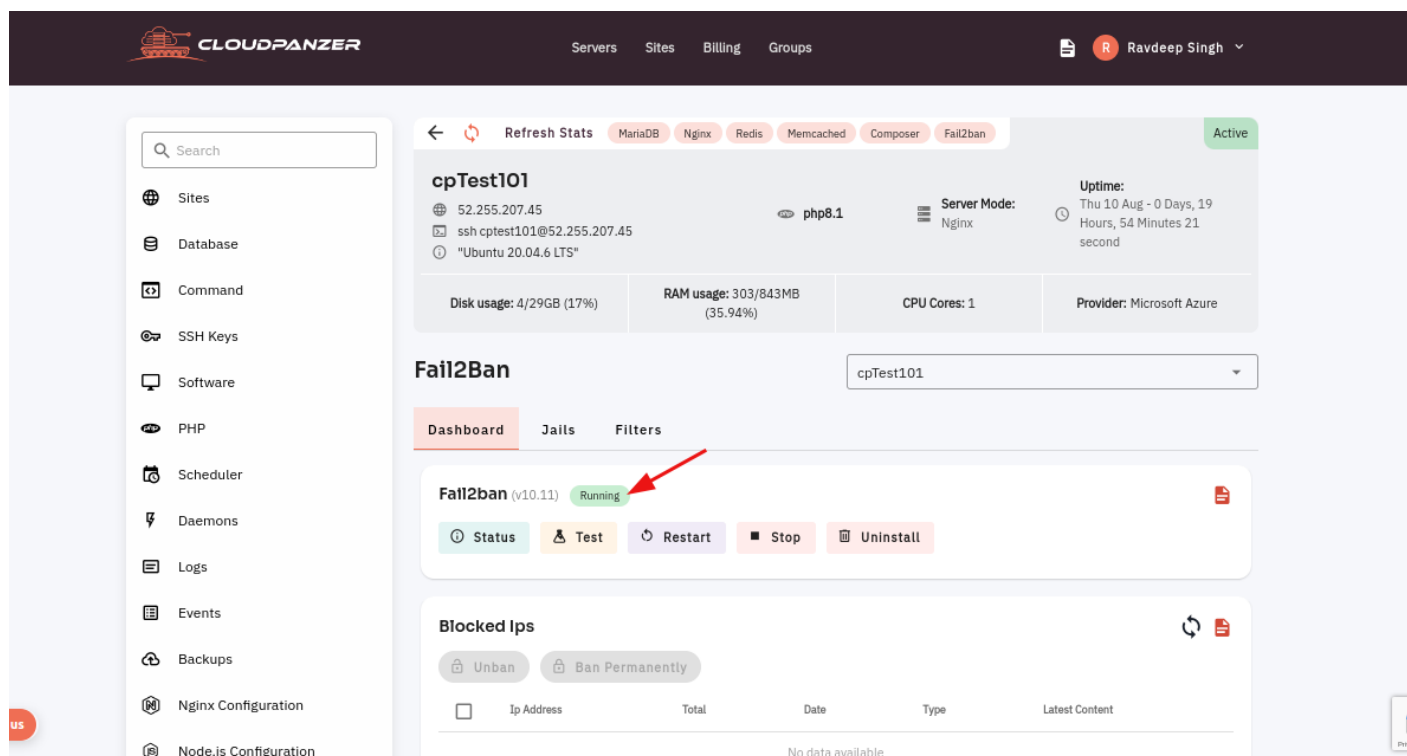
Here, you can see the Status checked successfully.



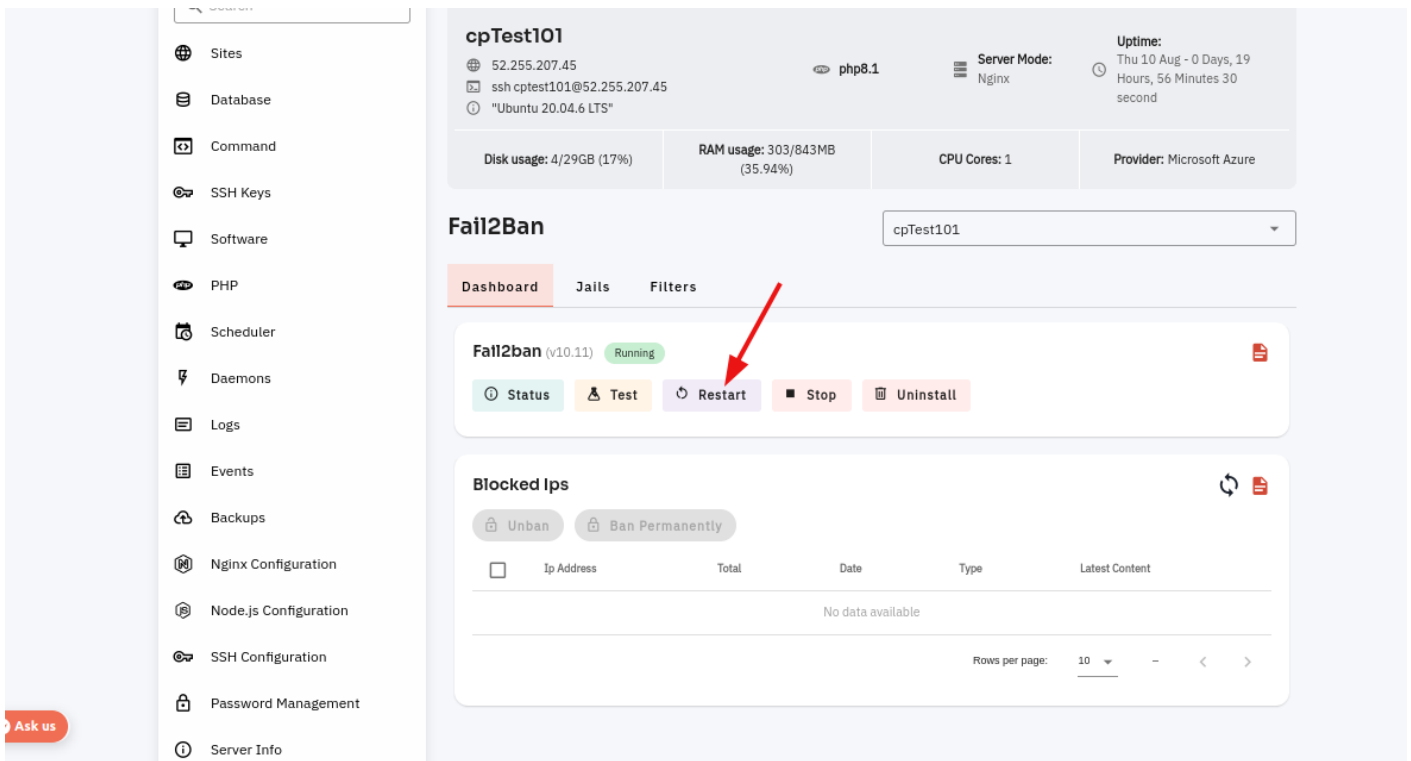
5. Click on the Test button to test a Fail2Ban.



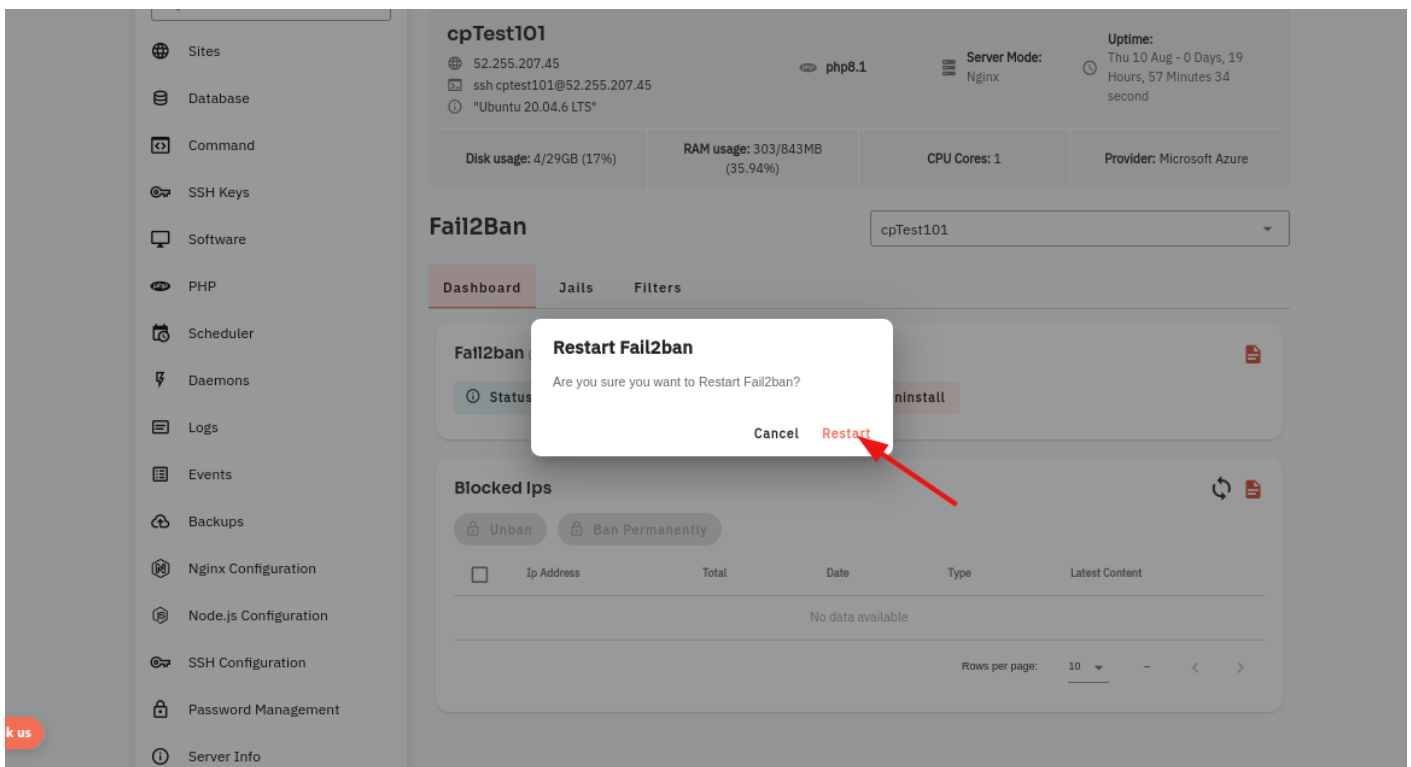
Here, you can see the server tested successfully.



6. Click on the Restart button.



7. A dialog will open, then click on the Restart button.



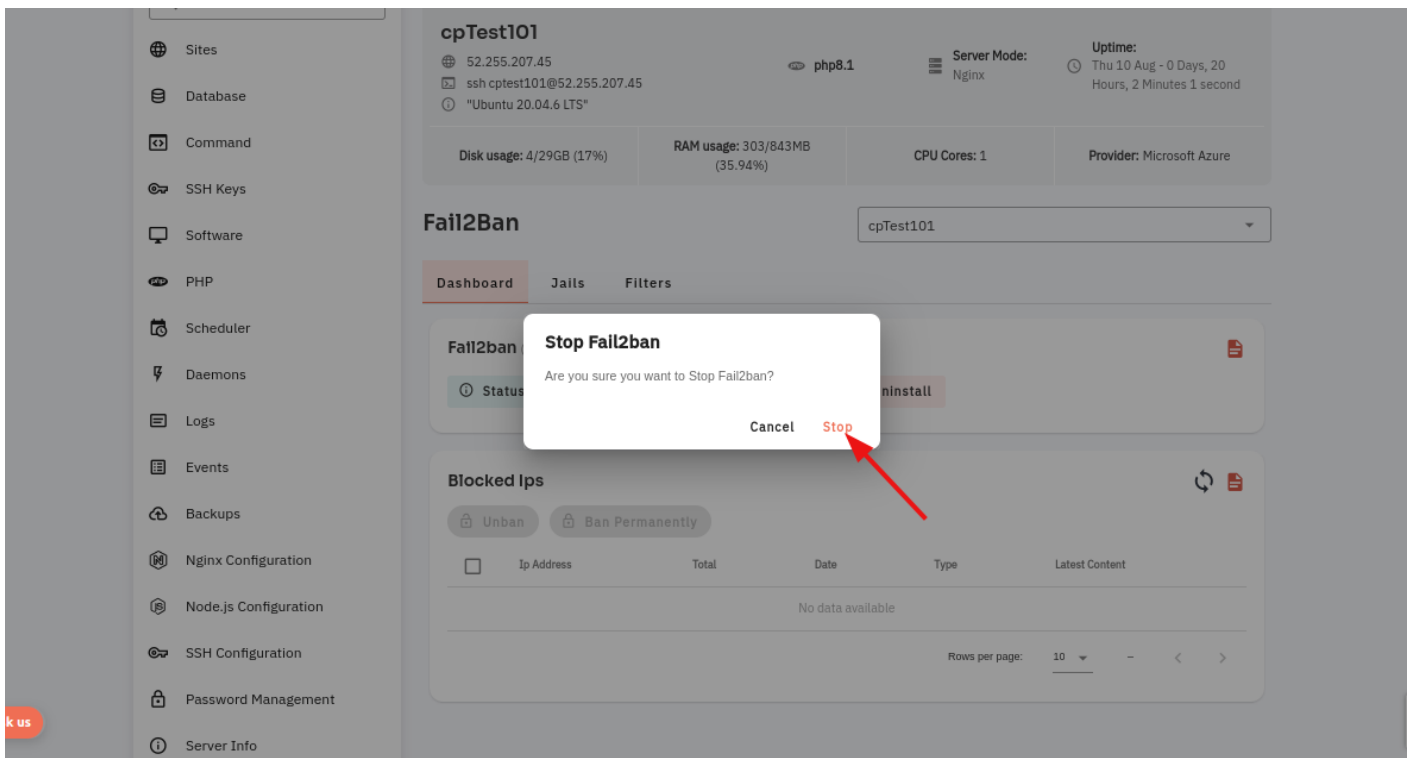
8. Here, you can see Fail2Ban restarted successfully.

The screenshot shows the Fail2Ban dashboard for a server named 'cpTest101'. The server details include IP 52.255.207.45, SSH access, and OS 'Ubuntu 20.04.6 LTS'. Resource usage is shown as Disk: 4/29GB (17%), RAM: 303/843MB (35.94%), and CPU: 1 core. The Fail2Ban service is currently 'Running', indicated by a green pill and a red arrow. Below the status bar are buttons for Status, Test, Restart, Stop, and Uninstall. The 'Blocked Ips' section is empty, showing 'No data available'.

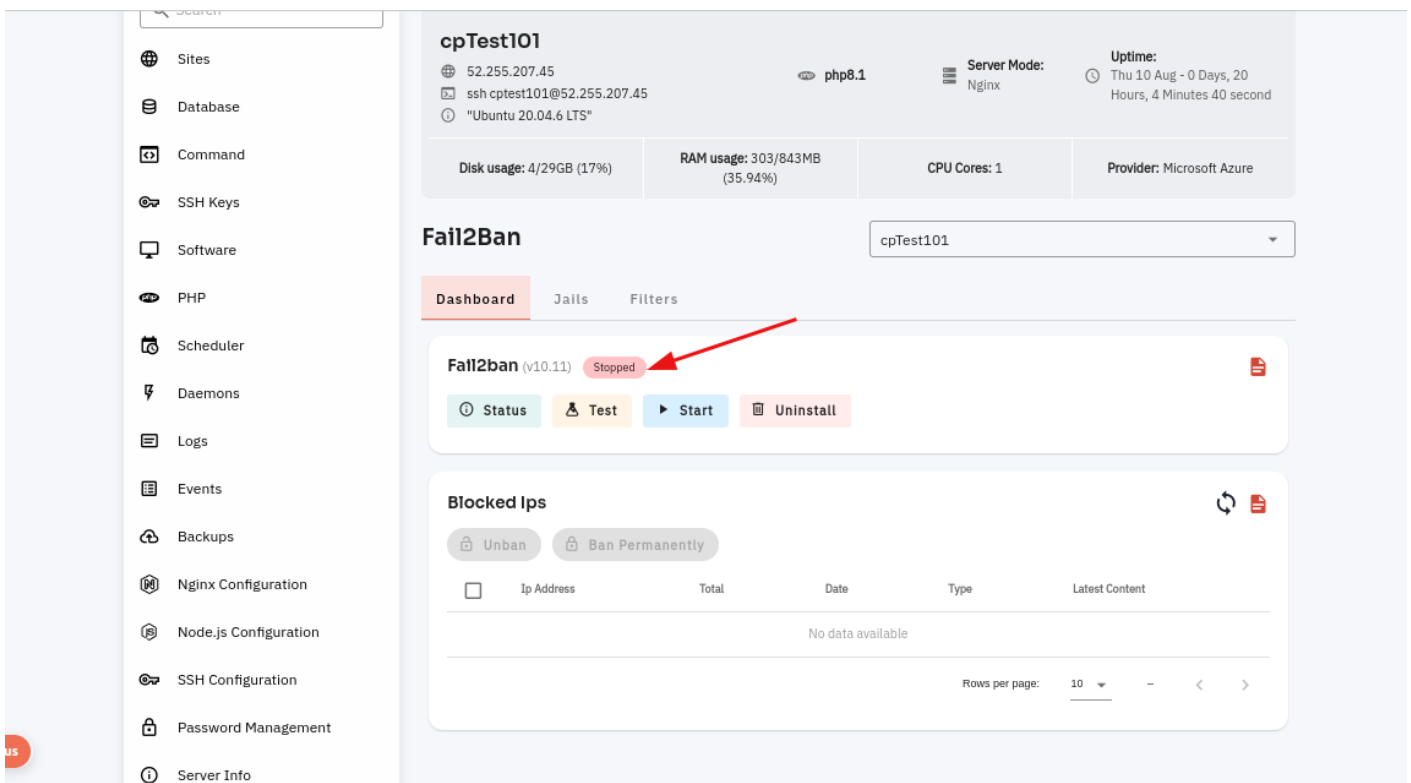
9. Click on the stop button.

This screenshot is identical to the previous one, but the red arrow now points to the 'Stop' button in the Fail2Ban status bar. The 'Running' status remains unchanged.

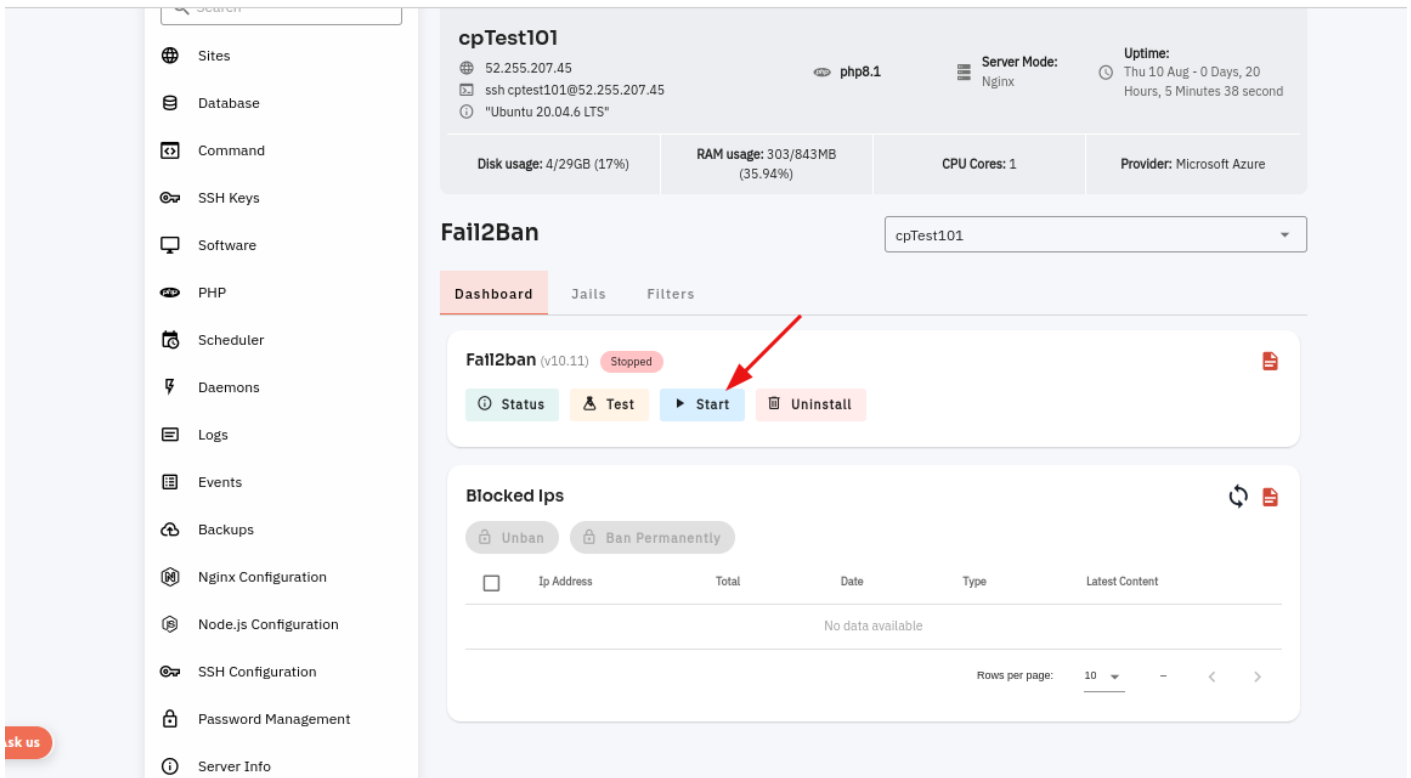
10. A dialog will open and click on the stop button.



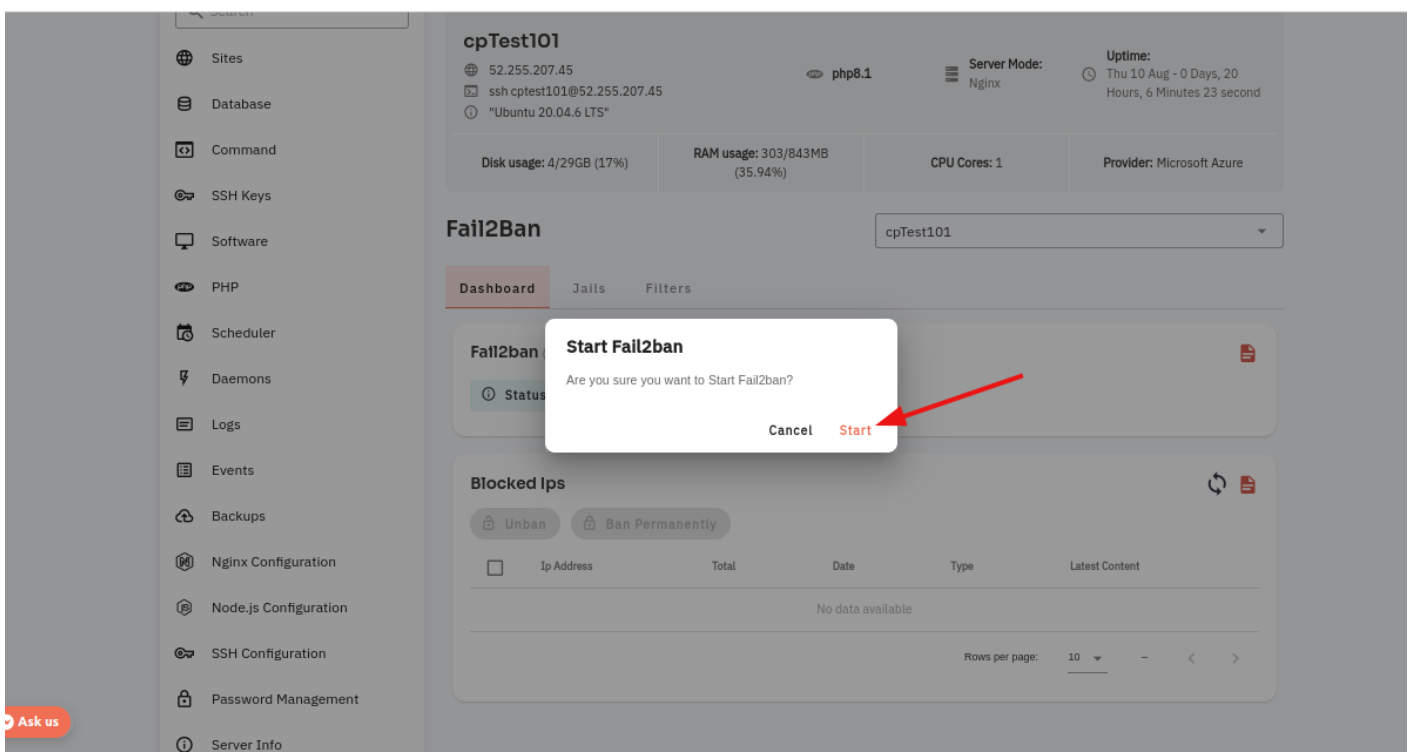
Here, you can see that Fail2Ban stopped successfully.



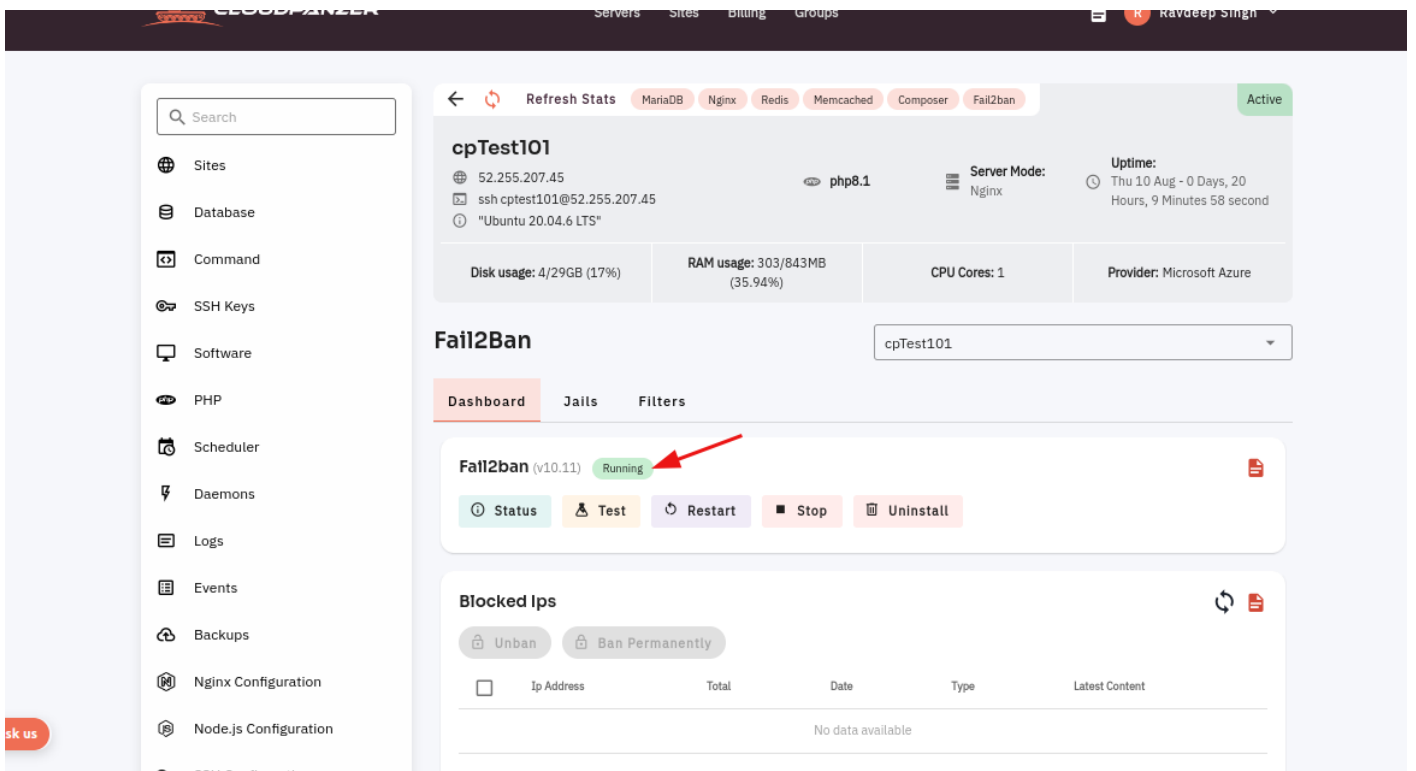
11. Click on the Start button.



12. A dialog box will open, then click on the start button.



13 . Here, you can see Fail2Ban Started Successfully.



Looking for mobile app Instructions?

Available at: <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-manage-the-fail2ban-configuration-of-cloudpanzer-through-the-mobile-application>