

# Fail2Ban

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

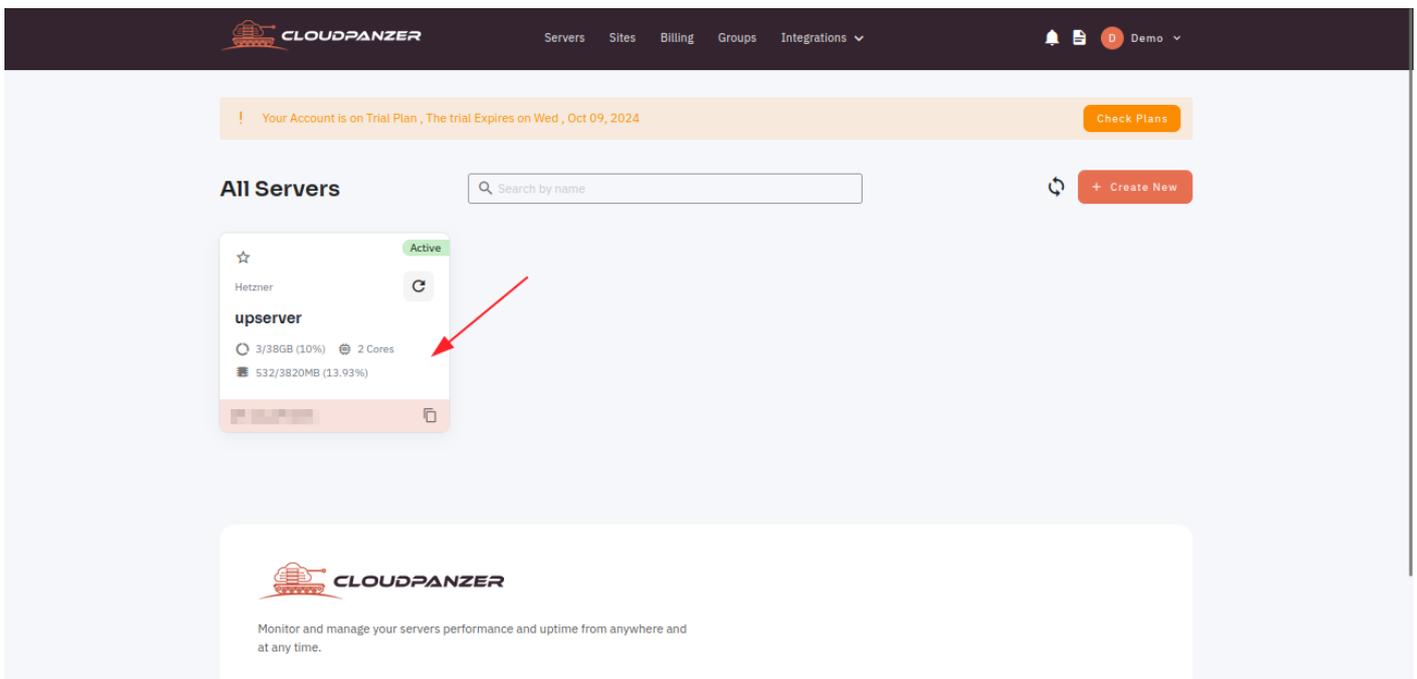
# How to add Filters in Fail2Ban on CloudPanzer?

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.

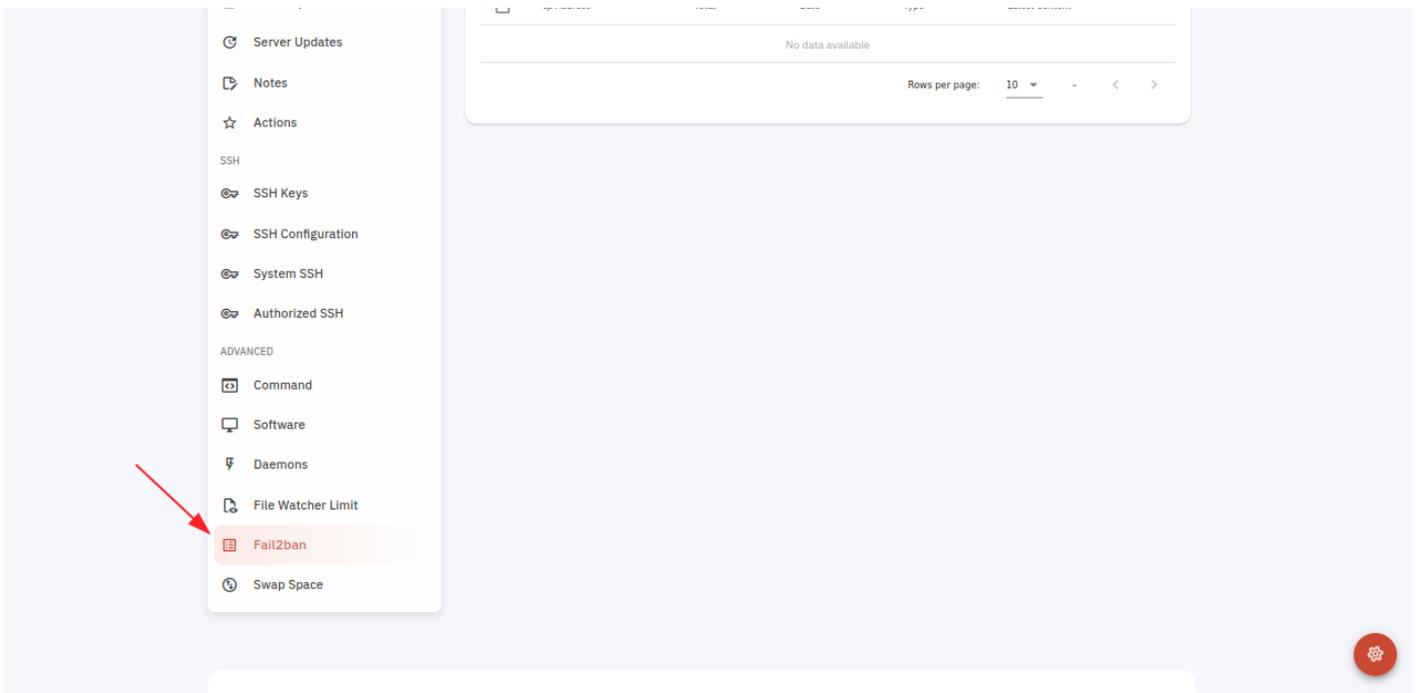
## How to install a Server

Follow the steps below to add Filters in Fail2Ban.

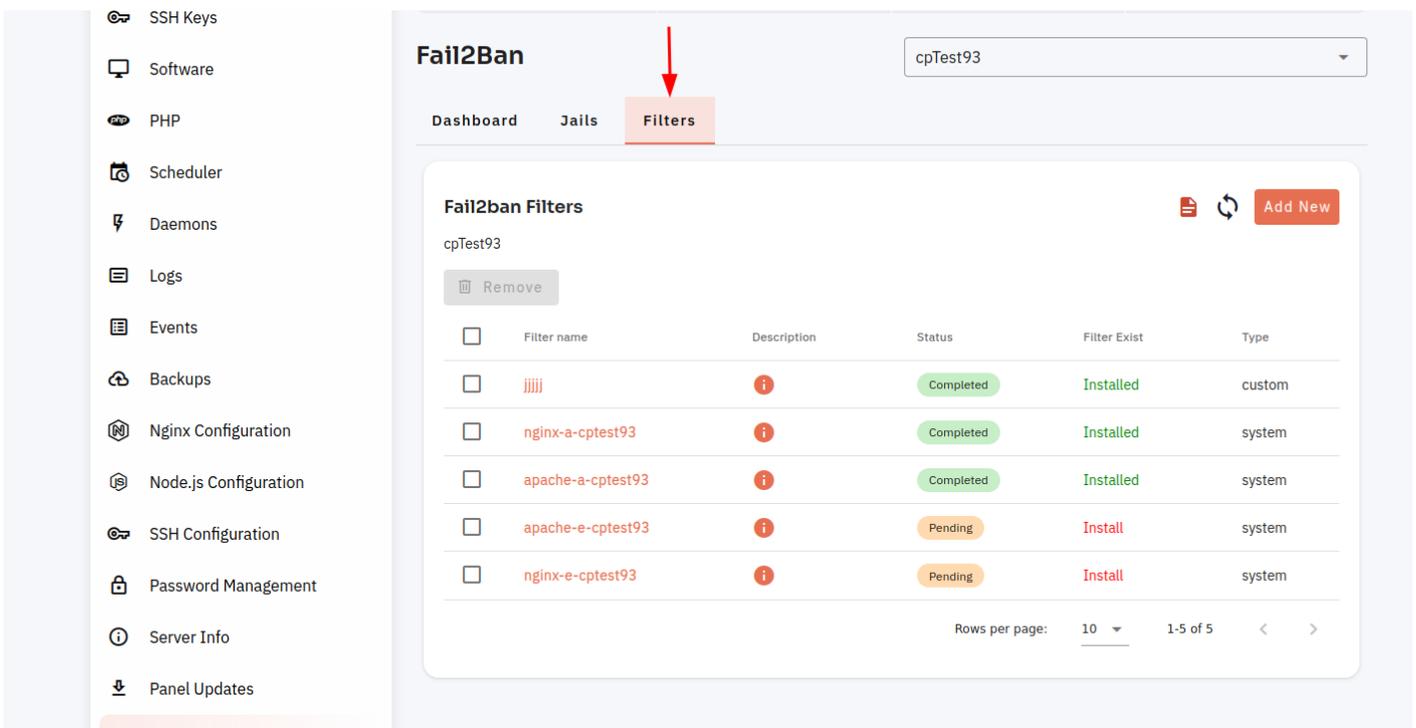
1: Once you are logged in, look for a "Server" and click on it.



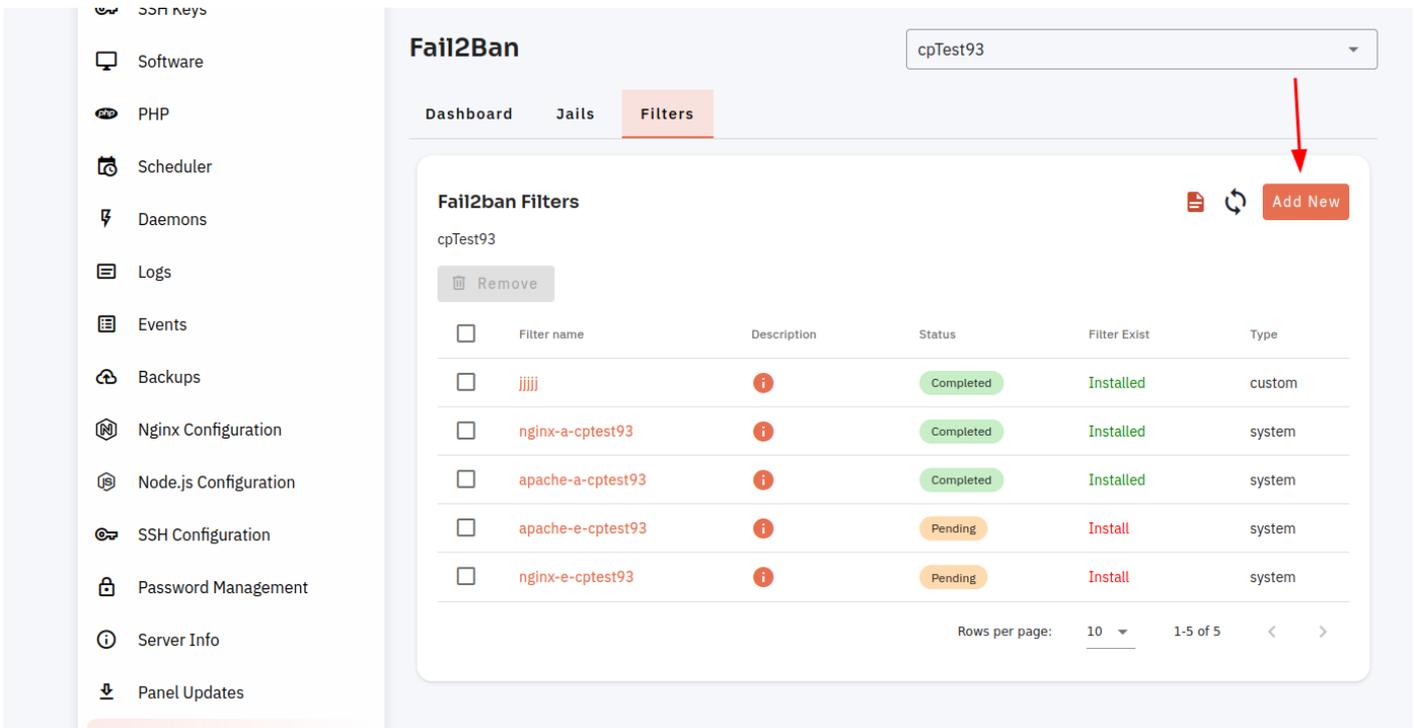
2. Select the Fail2ban option.



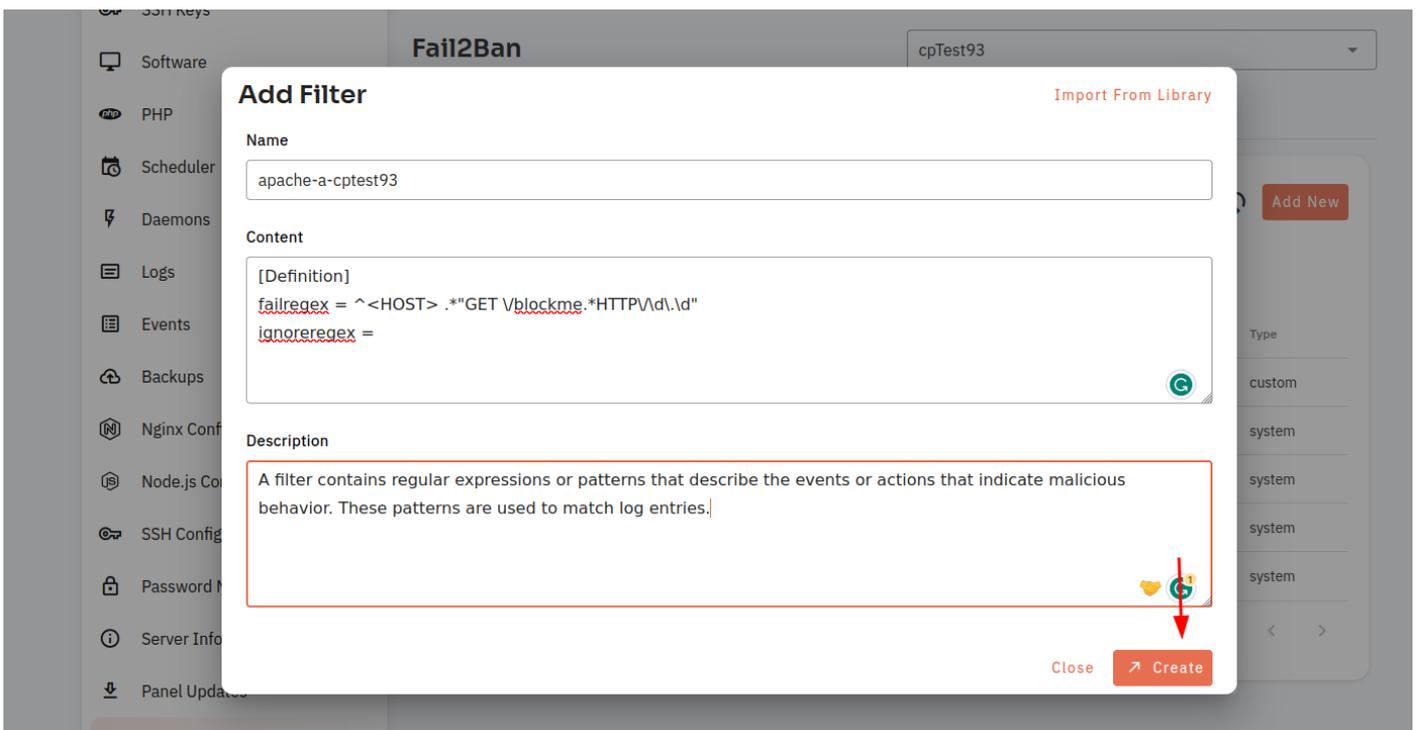
3. Click on the Filters button.



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.

The screenshot displays the Fail2Ban configuration interface. On the left is a sidebar with navigation options: SSH keys, Software, PHP, Scheduler, Daemons, Logs, Events, Backups, Nginx Configuration, Node.js Configuration, SSH Configuration, Password Management, Server Info, and Panel Updates. The main content area is titled 'Fail2Ban' and includes a dropdown menu for the jail 'cpTest93'. Below this are tabs for 'Dashboard', 'Jails', and 'Filters'. The 'Filters' tab is active, showing a 'Fail2ban Filters' section for 'cpTest93' with a 'Remove' button. A table lists the filters with columns for Filter name, Description, Status, Filter Exist, and Type. A red arrow points to the 'Add New' button in the top right corner of the table area.

<input type="checkbox"/>	Filter name	Description	Status	Filter Exist	Type
<input type="checkbox"/>	apache-a-cptest93		Completed	Installed	custom
<input type="checkbox"/>	jjjjj		Completed	Installed	custom
<input type="checkbox"/>	nginx-a-cptest93		Completed	Installed	system
<input type="checkbox"/>	apache-a-cptest93		Completed	Installed	system
<input type="checkbox"/>	apache-e-cptest93		Pending	Install	system
<input type="checkbox"/>	nginx-e-cptest93		Pending	Install	system

Rows per page: 10 1-6 of 6 < >

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>

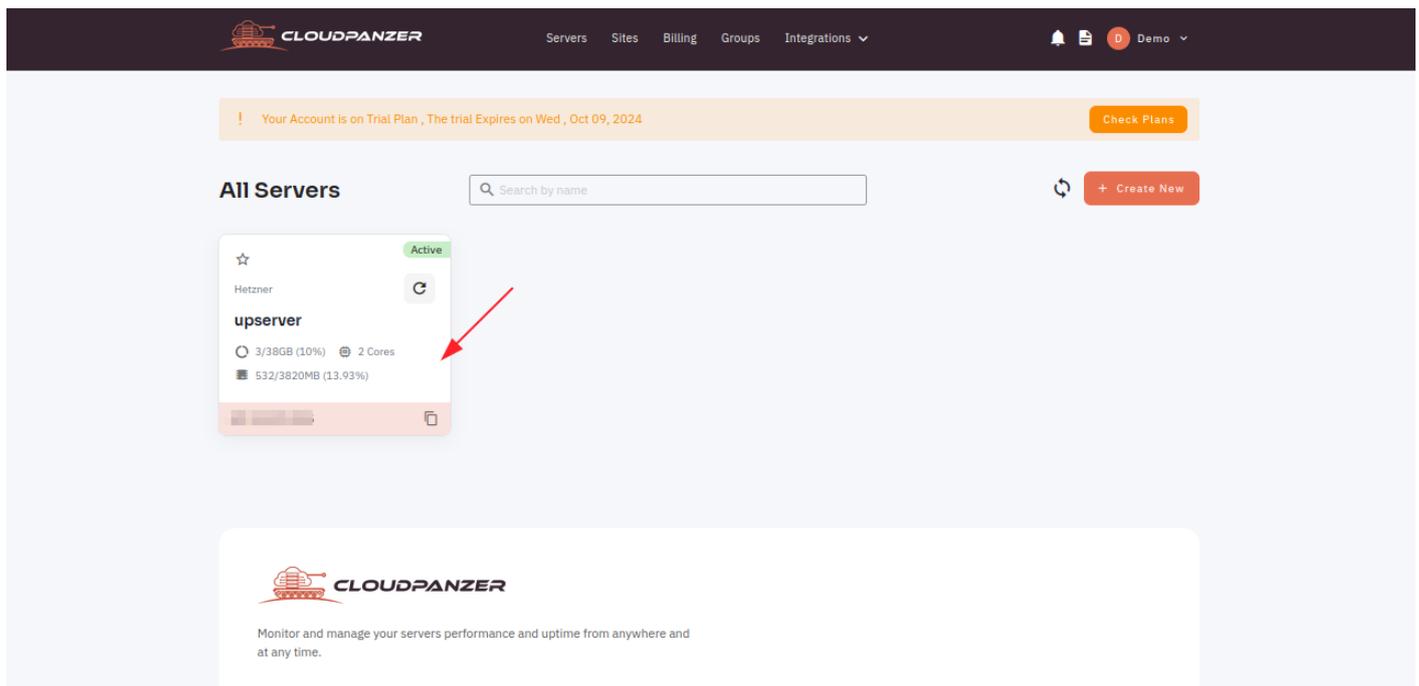
# How to add Jails in Fail2Ban on CloudPanzer?

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.

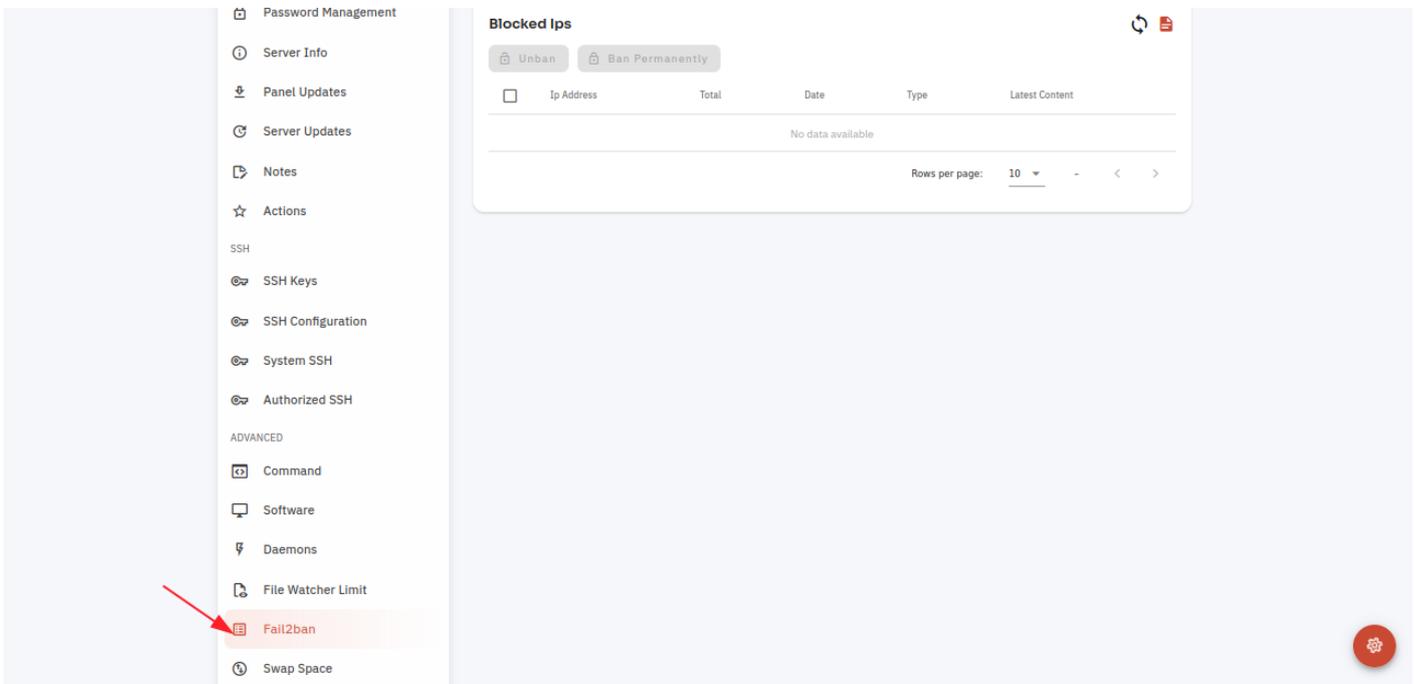
## How to install a Server

Follow the steps below to add Jails in Fail2Ban.

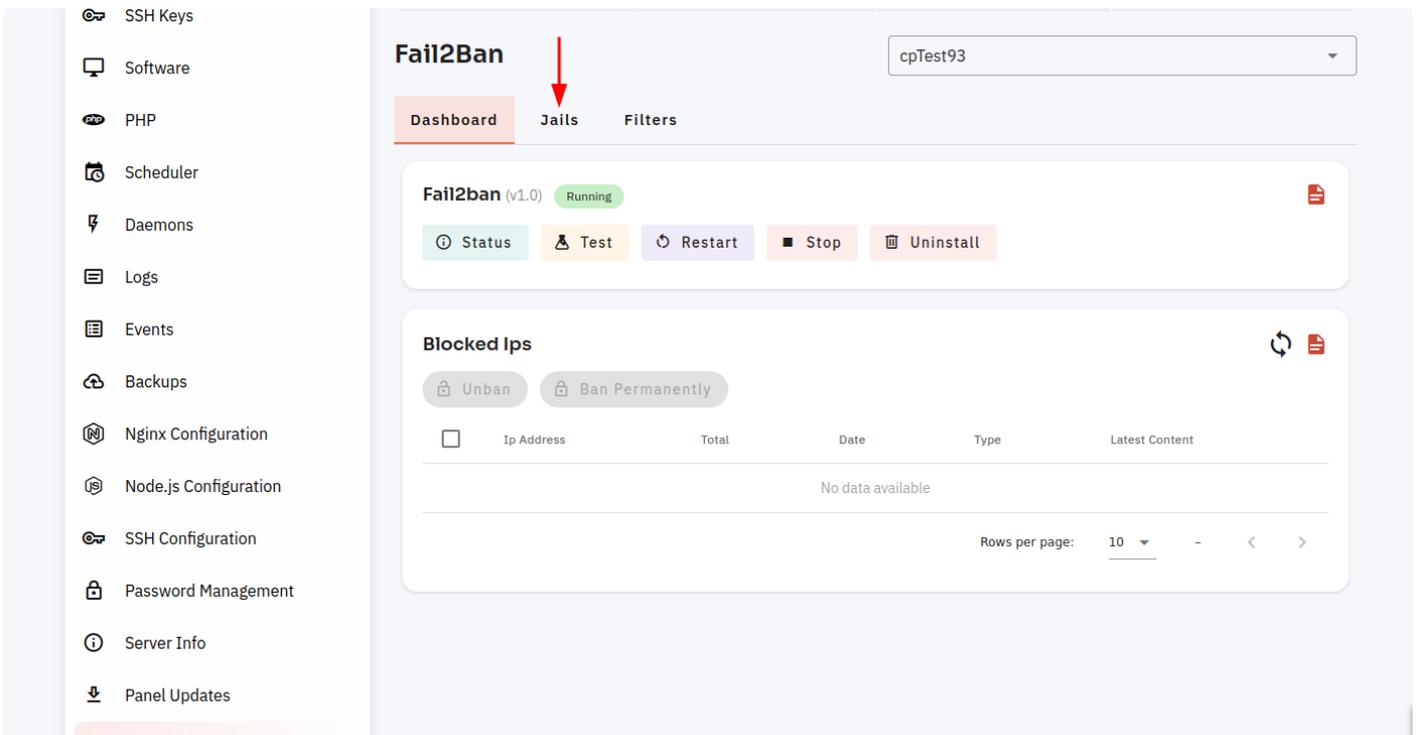
1: Once you are logged in, look for a "Server" and click on it.



2. Select the Fail2ban option.



3. Click on the Jails button.



4. Click on the Add New Button.

The screenshot shows the Fail2Ban Jails management interface. The left sidebar contains navigation options: SSH Keys, Software, PHP, Scheduler, Daemons, Logs, Events, Backups, Nginx Configuration, Node.js Configuration, SSH Configuration, Password Management, Server Info, and Panel Updates. The main content area is titled 'Fail2Ban' and shows the 'Jails' tab selected. A dropdown menu at the top right is set to 'cpTest93'. Below the tabs, there are buttons for 'Switch On', 'Switch Off', and 'Remove'. The 'Add New' button is highlighted with a red arrow. The main table lists existing jails with columns for Jail name, Desc, Status, Jail Exist, Type, and Active Status.

Jail name	Desc	Status	Jail Exist	Type	Active Status
testjail		Completed	Installed	custom	InActive
abc		Completed	Installed	custom	InActive
apache-e-cptest93		Pending	Install	system	InActive
nginx-e-cptest93		Pending	Install	system	InActive
apache-a-cptest93		Pending	Install	system	InActive
sshd		Pending	Install	system	InActive
nginx-a-cptest93		Pending	Install	system	InActive

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

The screenshot shows the 'Add Jail' form. The form fields are: Name (apache-e-cptest94), Select Filter (apache-a-cptest93), Log Path (/var/log/apache2/error.log), IP address ban period (seconds) (50), The maximum number of failed login attempts (5), Trusted Ips (empty), and Description (The action can involve dynamically adding the offending IP address to a firewall rule, effectively blocking any further communication from that IP). The 'From Existing' toggle is turned on. The 'Create' button is highlighted with a red arrow.

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

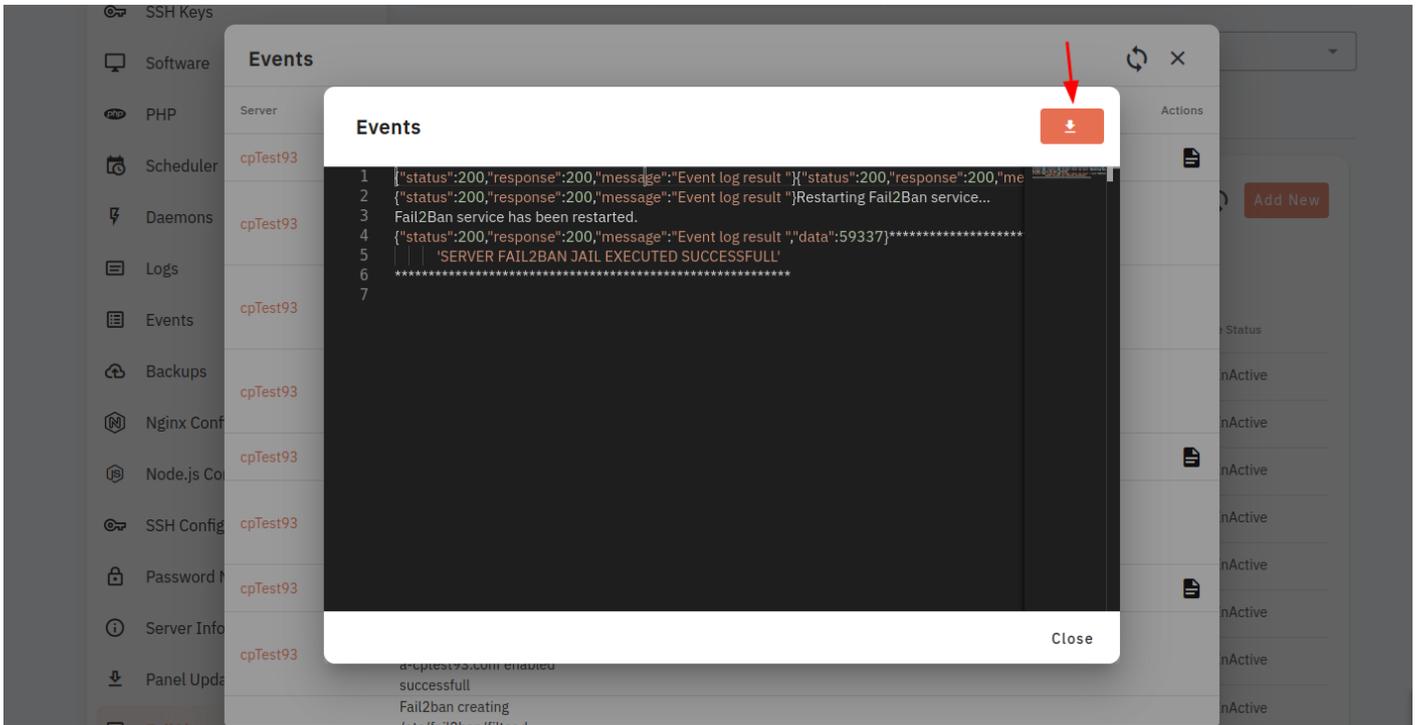
<input type="checkbox"/>	Jail name	Desc	Status	Jail Exist	Type	Active Status
<input type="checkbox"/>	apache-e-cptest94	i	Completed	Installed	custom	InActive
<input type="checkbox"/>	testjail	i	Completed	Installed	custom	InActive
<input type="checkbox"/>	abc	i	Completed	Installed	custom	InActive
<input 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

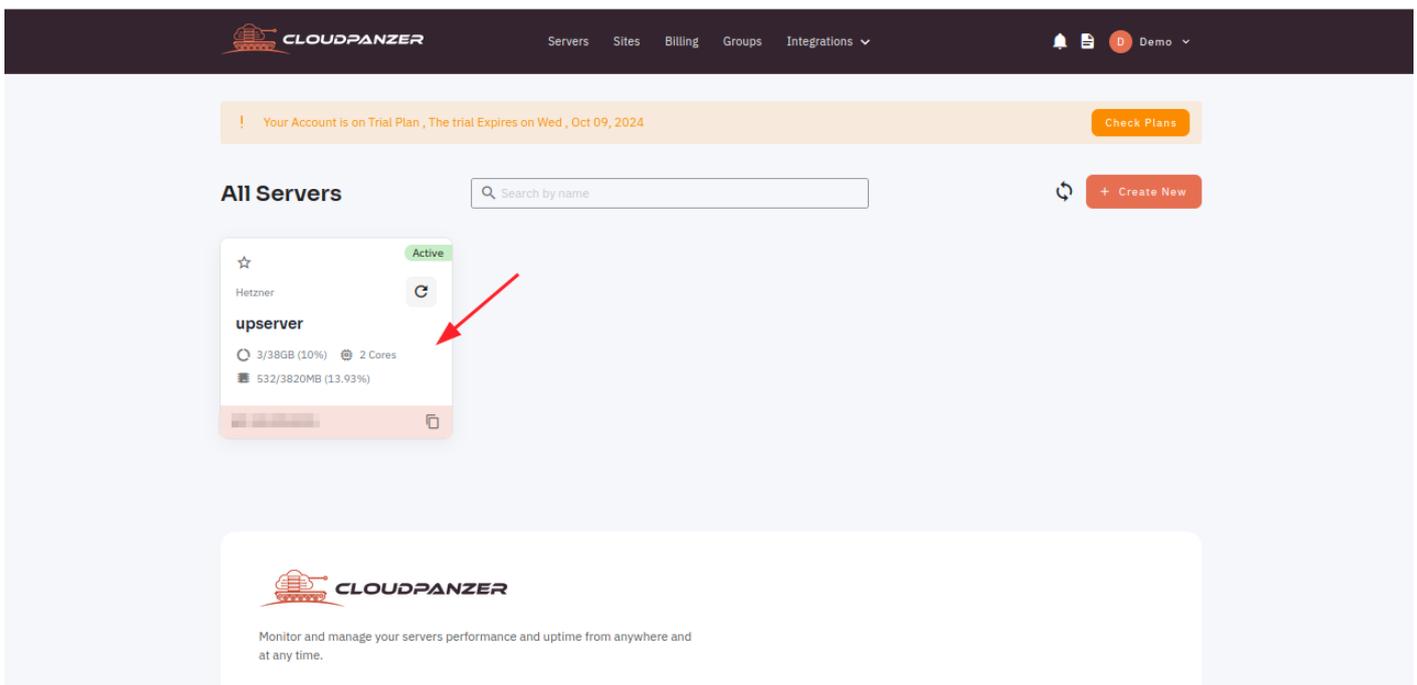
### Tutorial :

You can watch the Video or Continue reading the post.

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

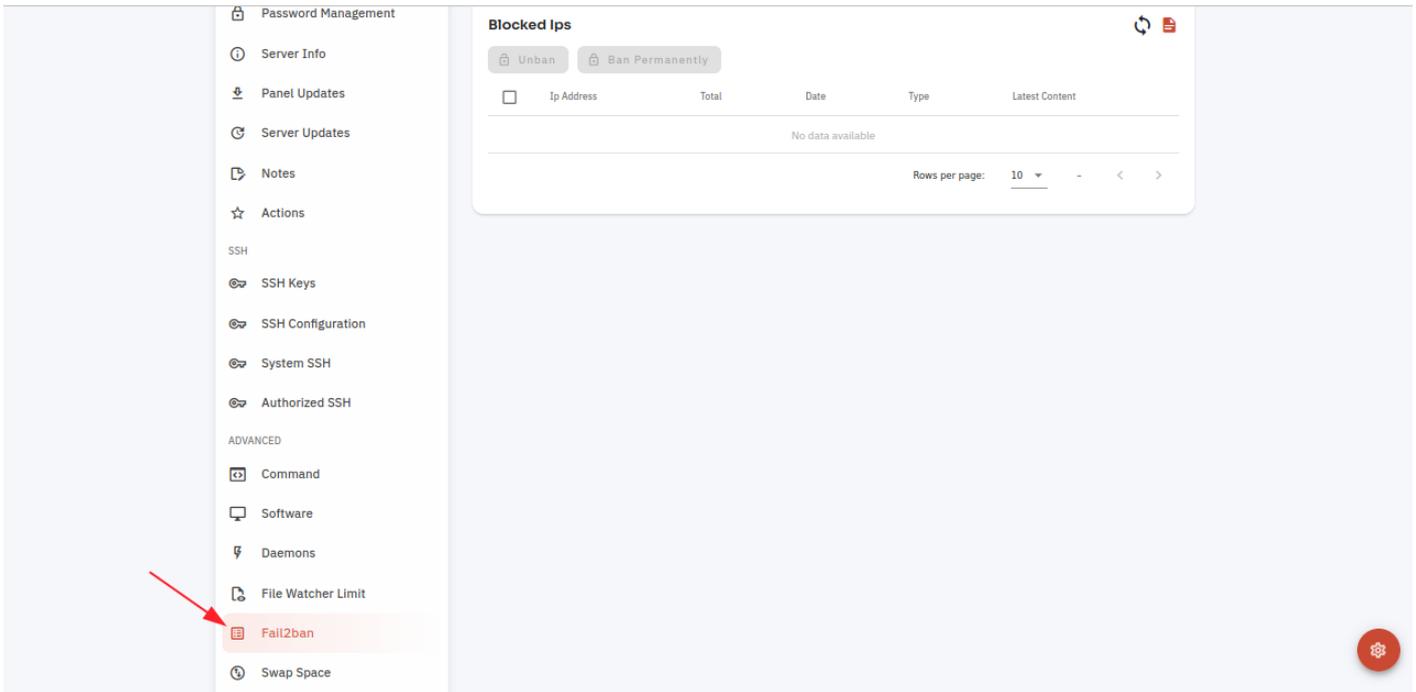
Follow the steps below to add Fail2ban Jails to the server.

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

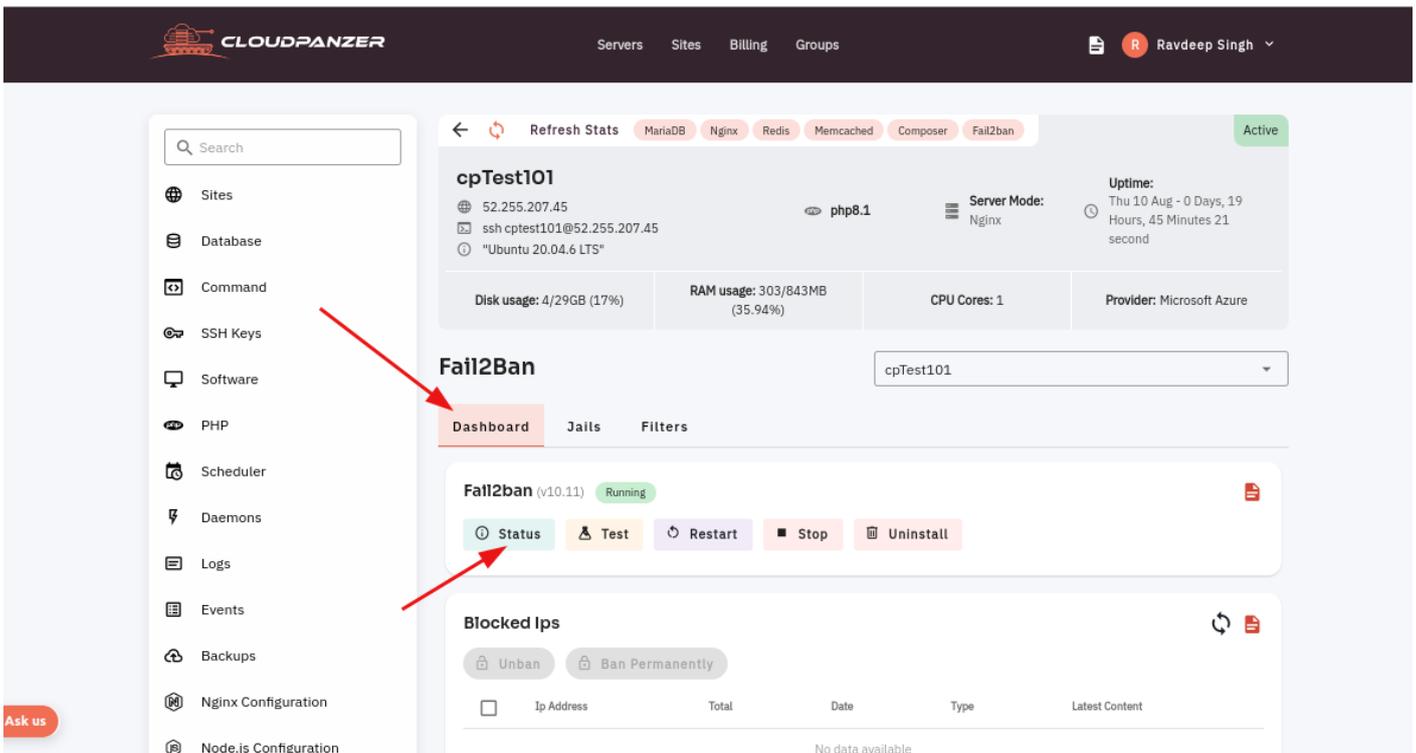


The screenshot shows the CloudPanzer dashboard interface. At the top, there is a navigation bar with the CloudPanzer logo and menu items: Servers, Sites, Billing, Groups, and Integrations. A notification banner at the top center states: "Your Account is on Trial Plan, The trial Expires on Wed, Oct 09, 2024" with a "Check Plans" button. Below the navigation, the main content area is titled "All Servers" and includes a search bar labeled "Search by name" and a "+ Create New" button. A server card is displayed, showing the name "upserver" and the provider "Hetzner". The card also displays resource usage: "3/38GB (10%)", "2 Cores", and "532/3820MB (13.93%)". A red arrow points to the "upserver" text on the card. At the bottom of the dashboard, there is a footer with the CloudPanzer logo and the text: "Monitor and manage your servers performance and uptime from anywhere and at any time."

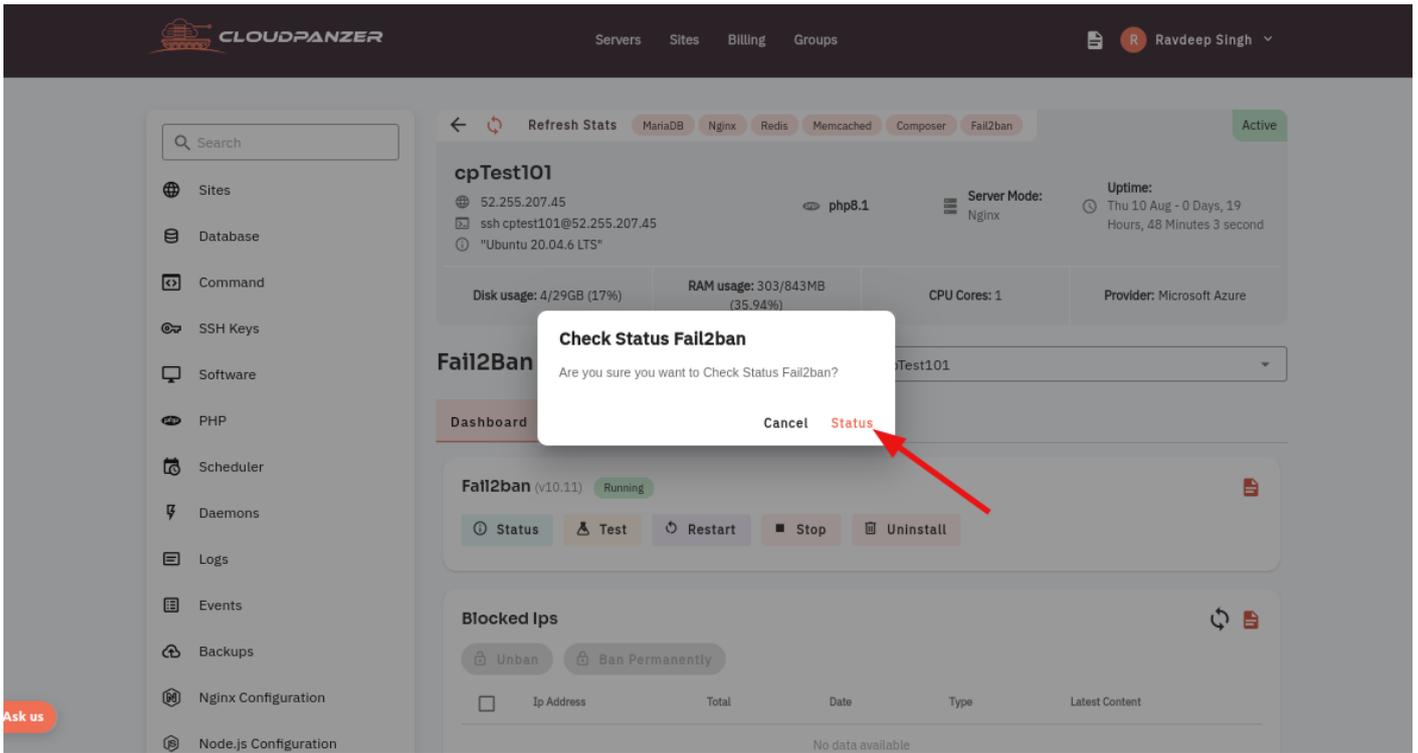
2. Select the Fail2ban option.



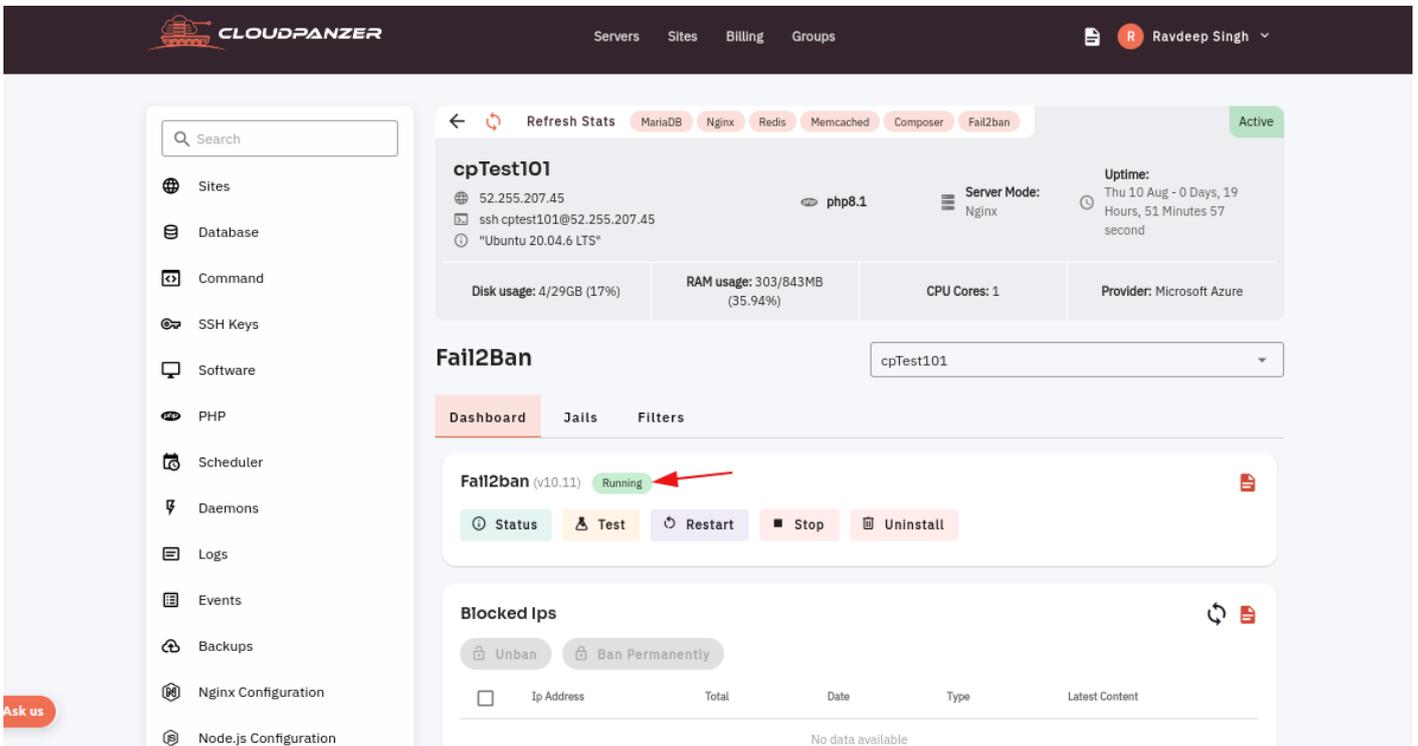
3. Select a Dashboard tab and click on the Status button.



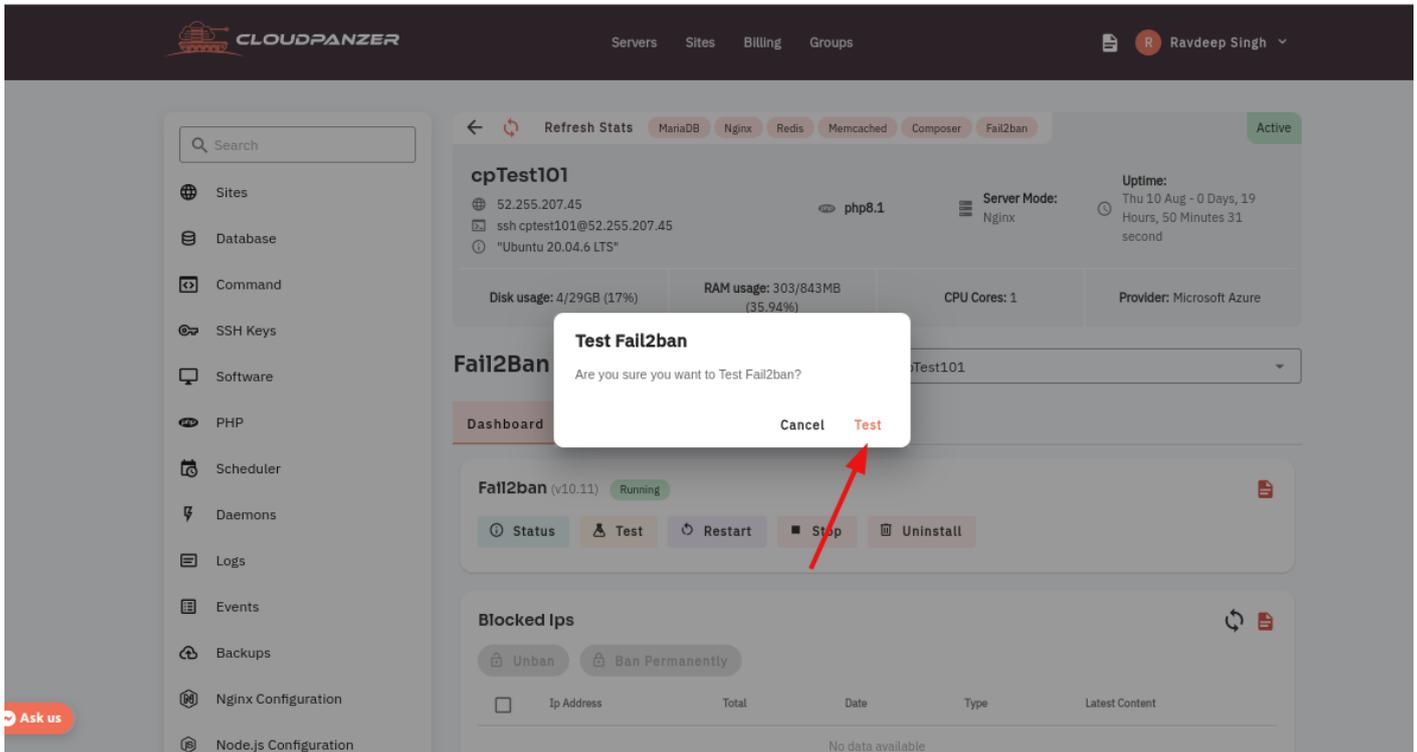
4. A dialog box will open and click on the Yes button to check the Status.



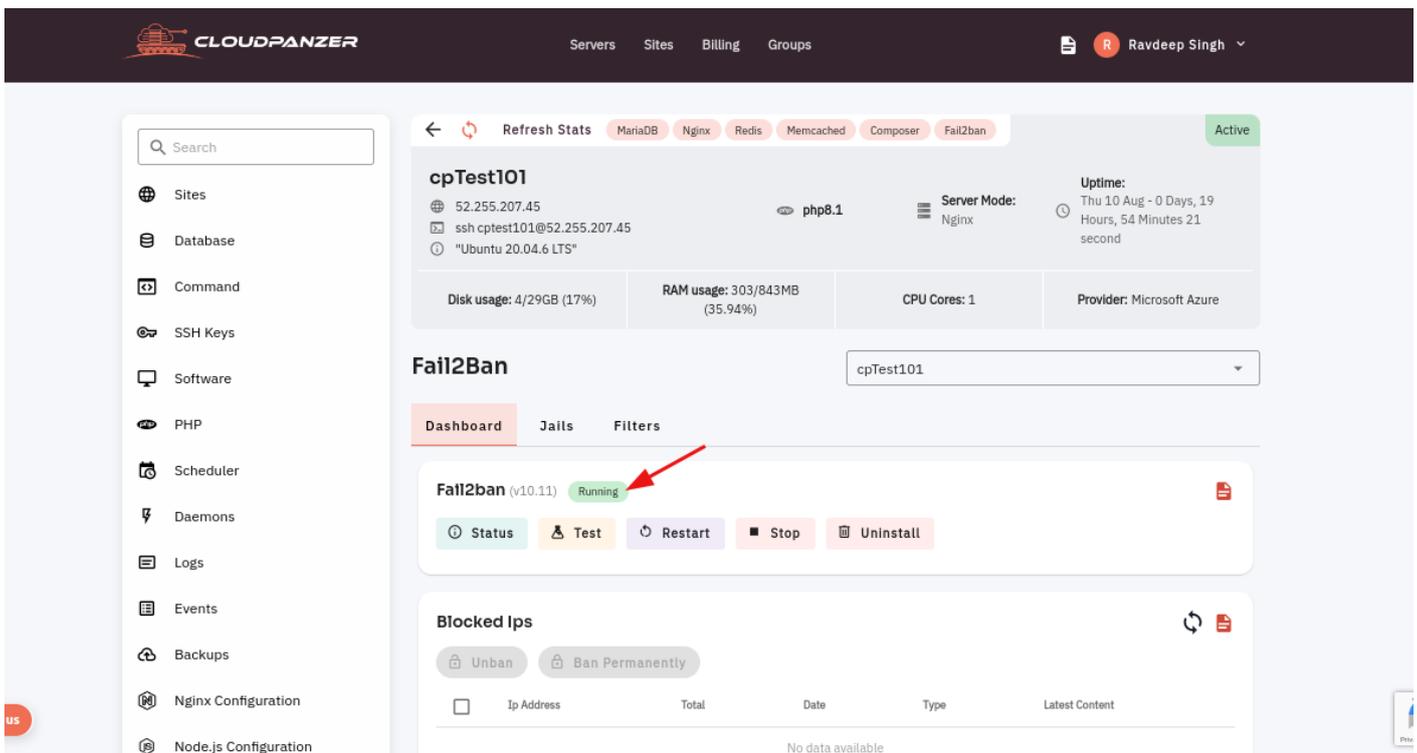
Here, you can see the Status checked successfully.



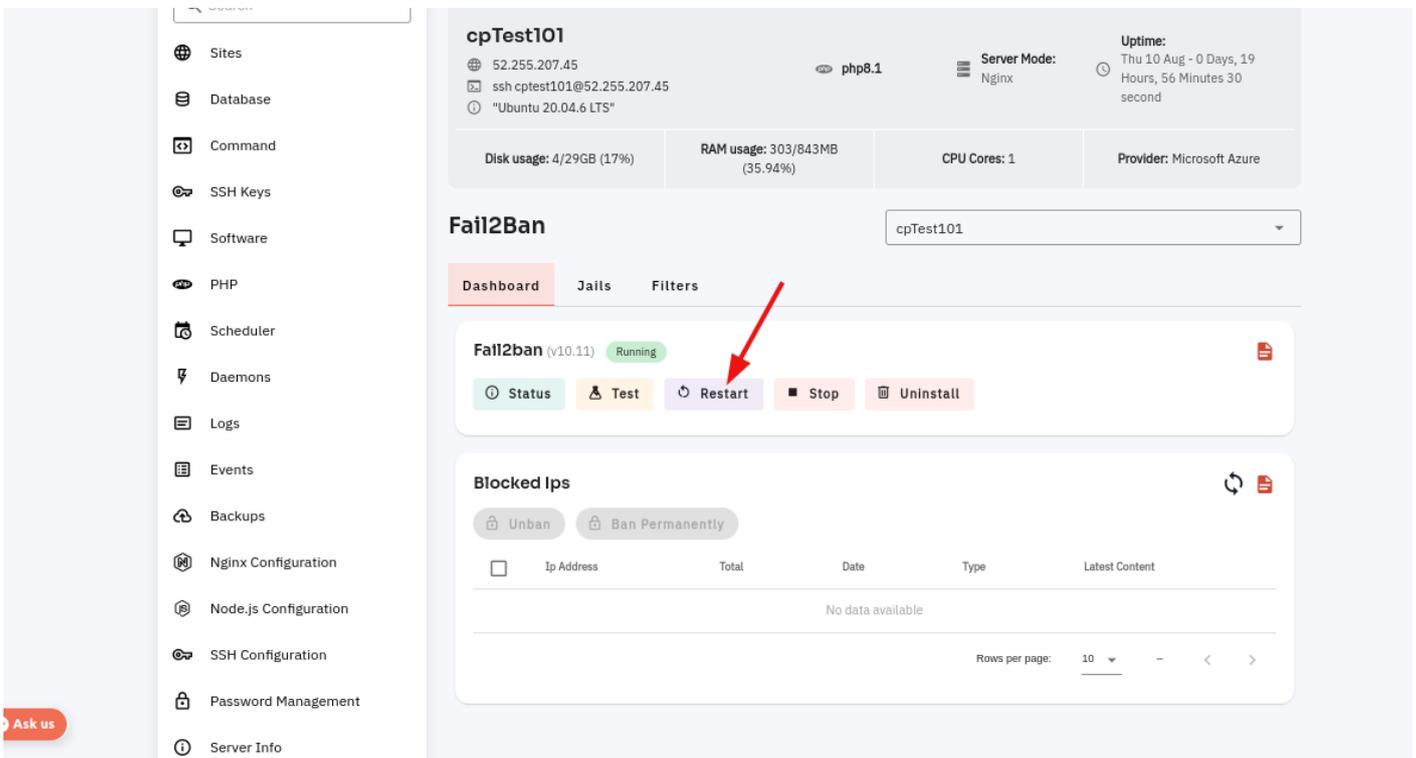
5. Click on the Test button to test a Fail2Ban.



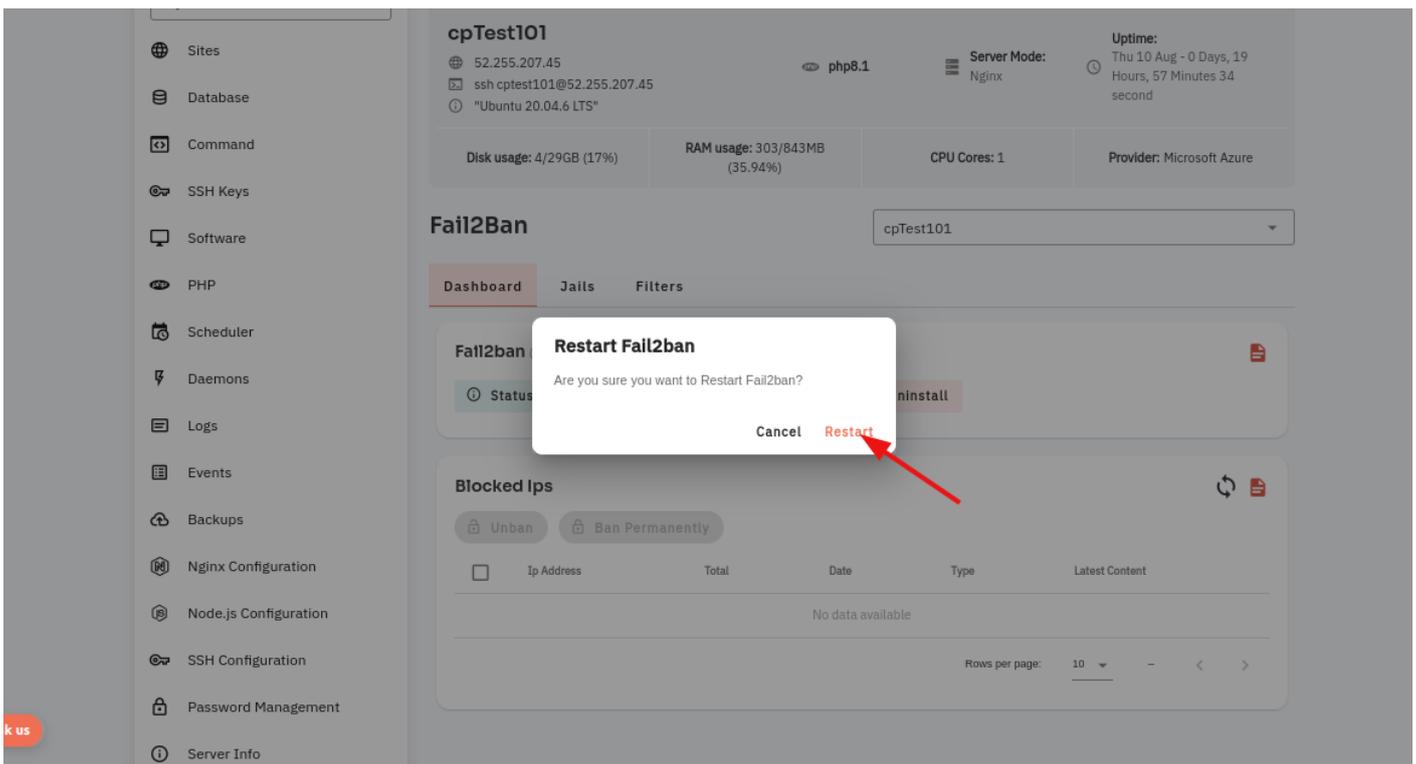
Here, you can see the server tested successfully.



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.

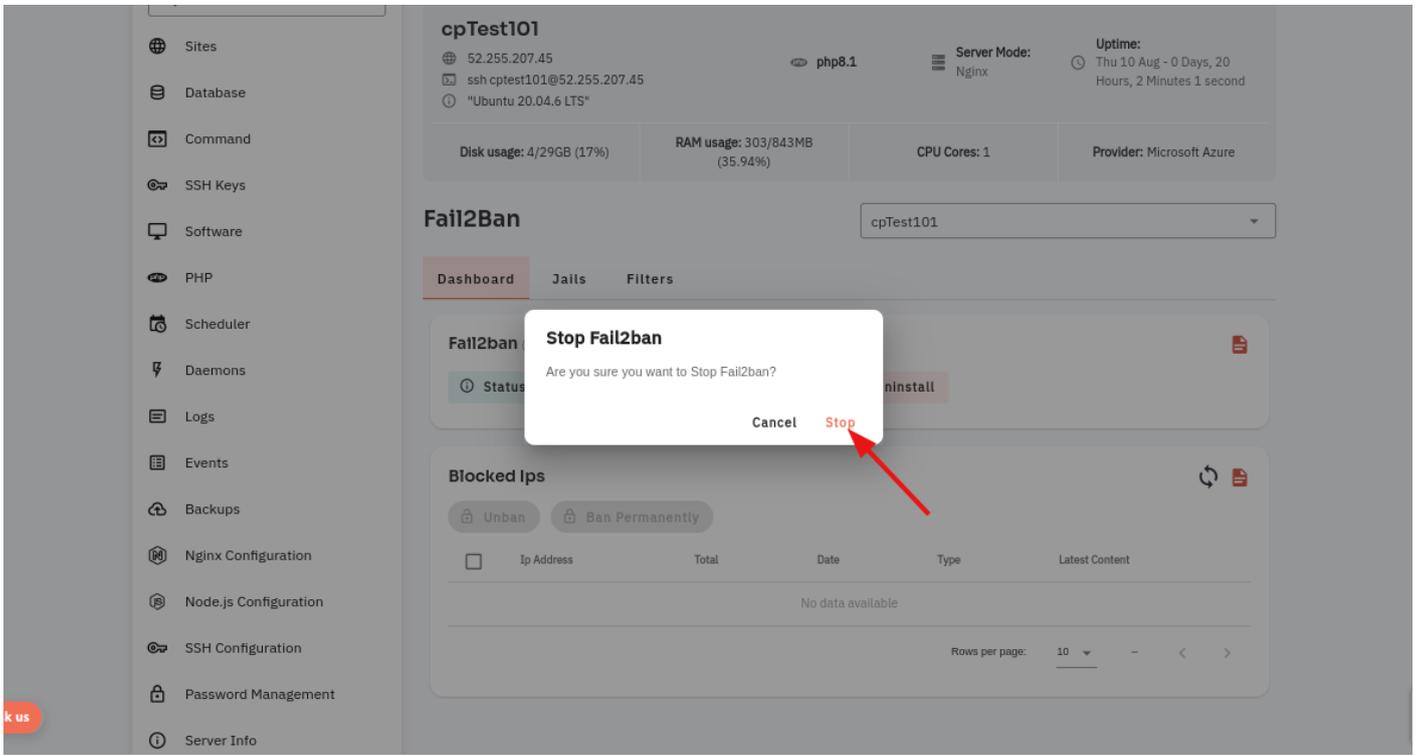
The screenshot shows the Fail2Ban dashboard for a server named 'cpTest101'. The server's IP is 52.255.207.45, running php8.1 with Nginx as the server mode. The uptime is 19 hours, 59 minutes, and 27 seconds. Resource usage is shown as Disk usage: 4/29GB (17%), RAM usage: 303/843MB (35.94%), and CPU Cores: 1. The provider is Microsoft Azure.

The Fail2Ban service is currently in a 'Running' state, indicated by a green pill. A red arrow points to this status. Below the status are buttons for 'Status', 'Test', 'Restart', 'Stop', and 'Uninstall'. The 'Blocked Ips' section is currently empty, showing 'No data available'.

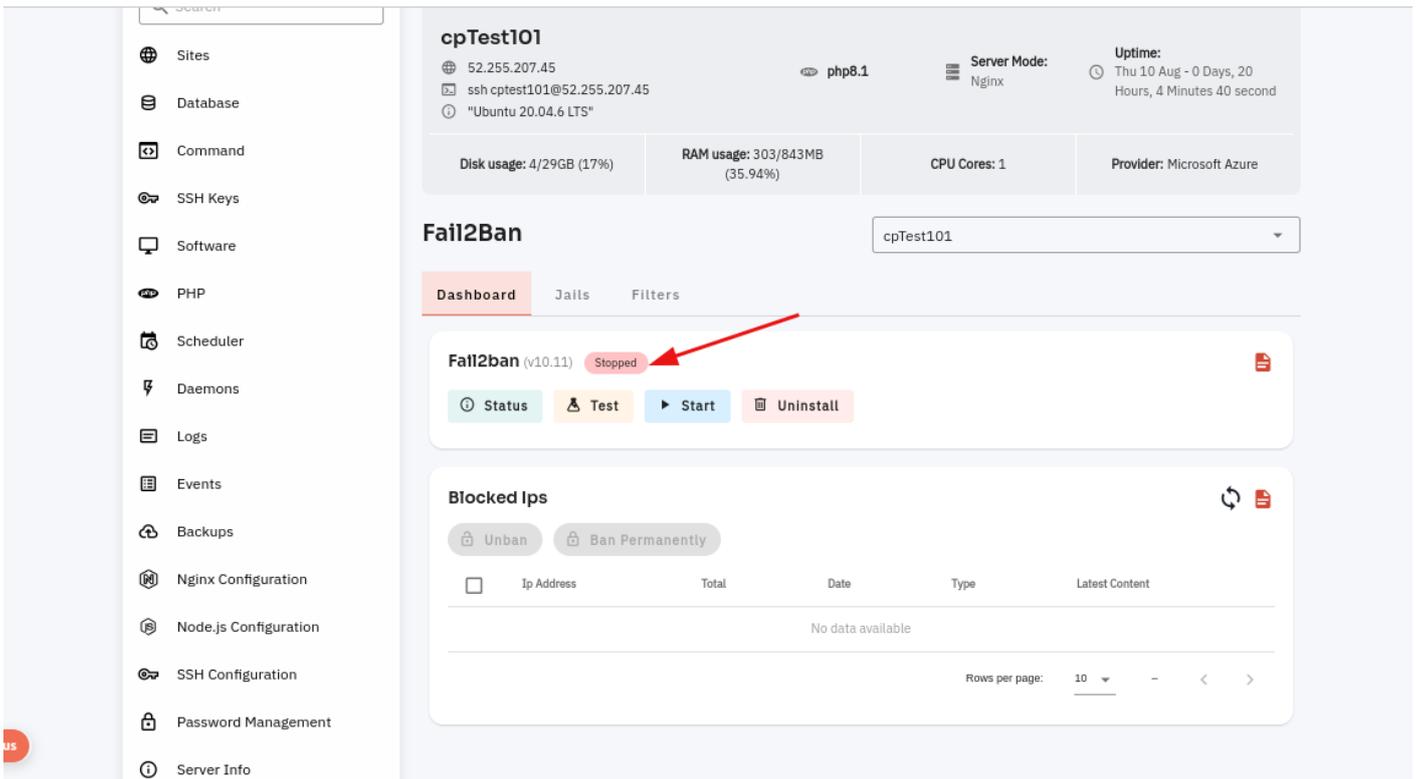
9. Click on the stop button.

This screenshot is identical to the previous one, but with a red arrow pointing to the 'Stop' button in the Fail2Ban control panel. The 'Running' status pill remains green.

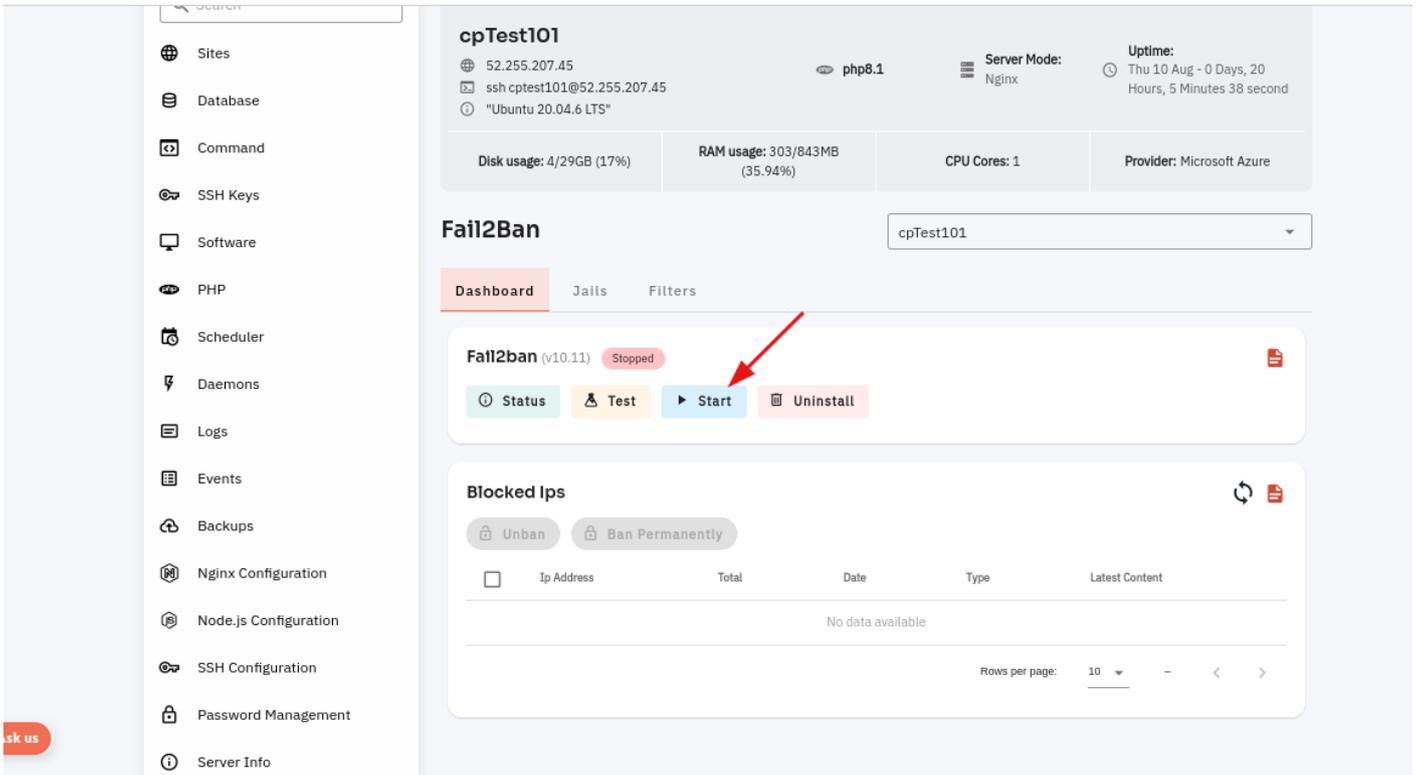
10. A dialog will open and click on the stop button.



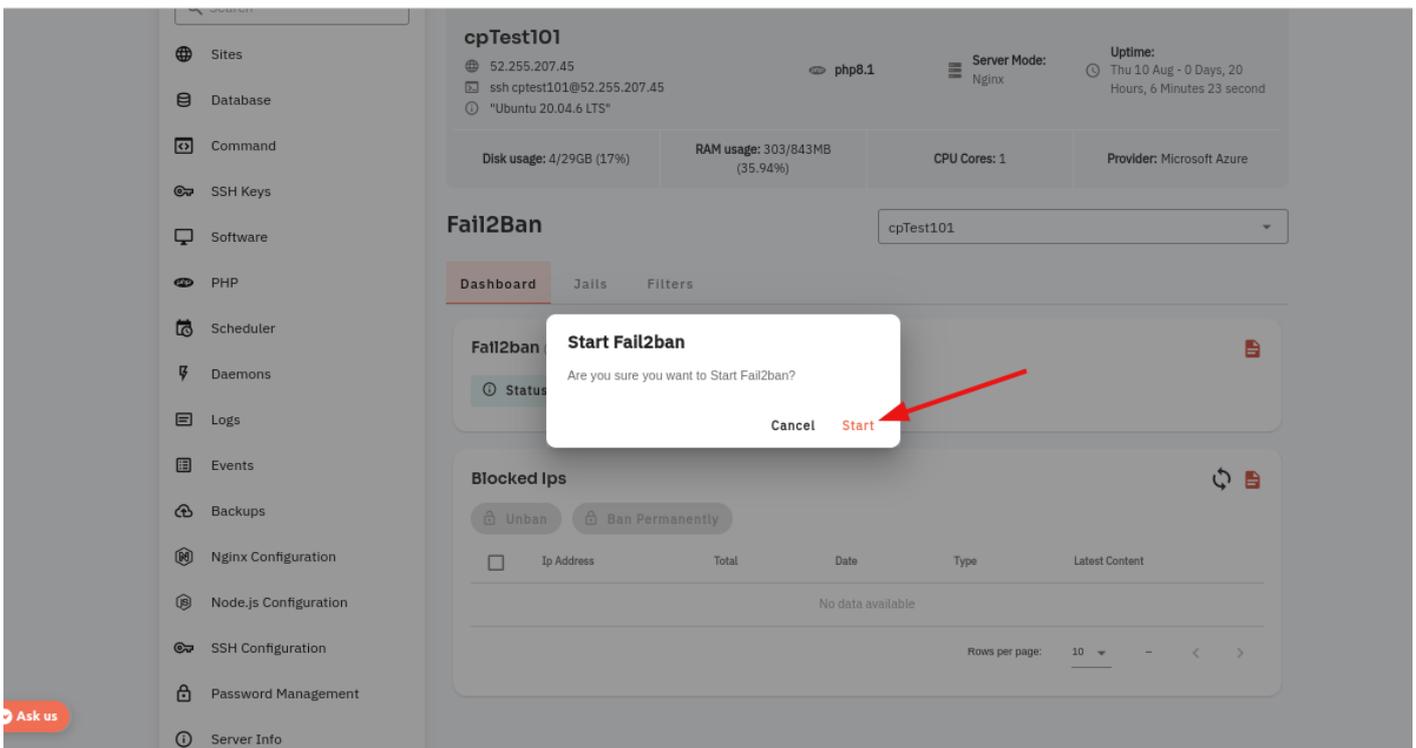
Here, you can see that Fail2Ban stopped successfully.



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.

The screenshot displays the CloudPanzer dashboard for a server named 'cpTest101'. The top navigation bar includes 'Servers', 'Sites', 'Billing', and 'Groups'. The main content area shows server statistics: IP 52.255.207.45, SSH user 'ssh cpTest101@52.255.207.45', OS 'Ubuntu 20.04.6 LTS', PHP version 'php8.1', Server Mode 'Nginx', and Uptime 'Thu 10 Aug - 0 Days, 20 Hours, 9 Minutes 58 second'. Resource usage is shown as Disk usage: 4/29GB (17%), RAM usage: 303/843MB (35.94%), and CPU Cores: 1. The provider is Microsoft Azure.

The 'Fail2Ban' section is active and shows the service is 'Running' (indicated by a green dot and a red arrow). Below this, there are buttons for 'Status', 'Test', 'Restart', 'Stop', and 'Uninstall'. The 'Blocked Ips' section is currently empty, showing 'No data available'.

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>