Fail2Ban

- How to add Filters in Fail2Ban on CloudPanzer?
- How to add Jails in Fail2Ban on CloudPanzer?
- How to Manage Fail2ban on CloudPanzer Servers?

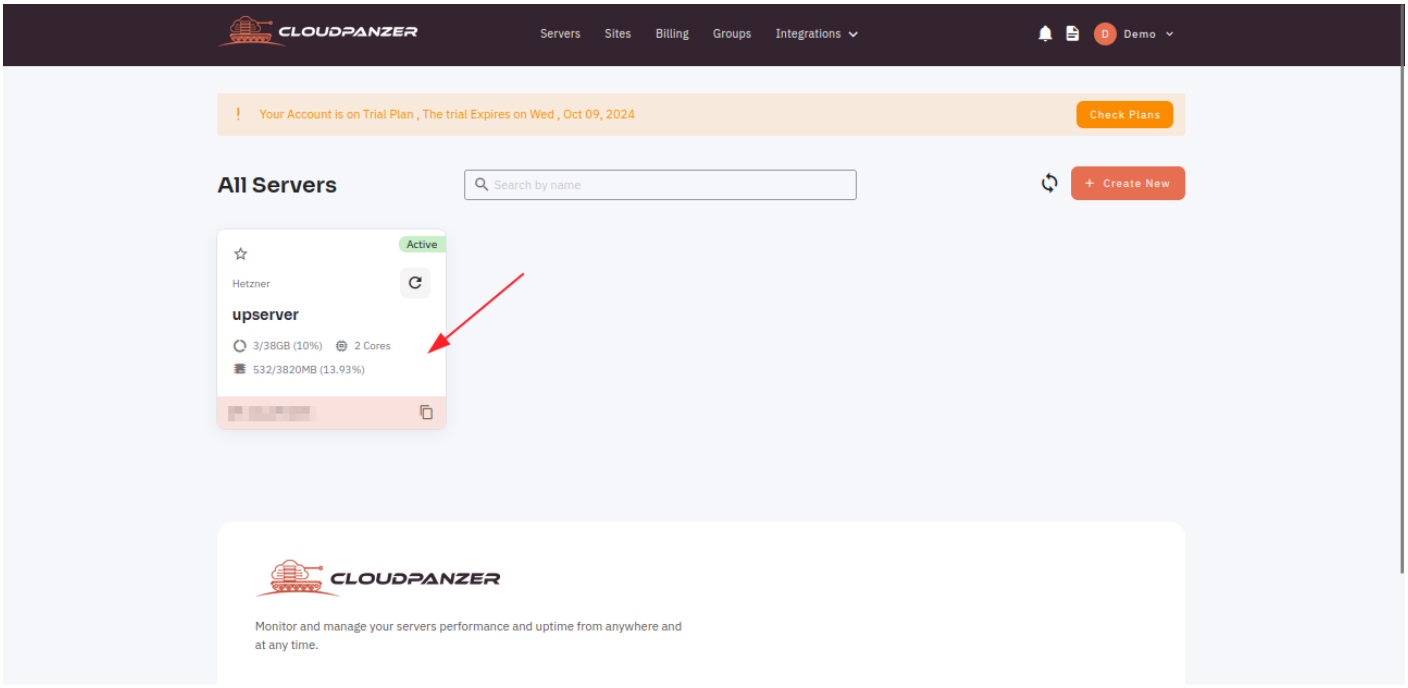
How to add Filters in Fail2Ban on CloudPanzer?

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.

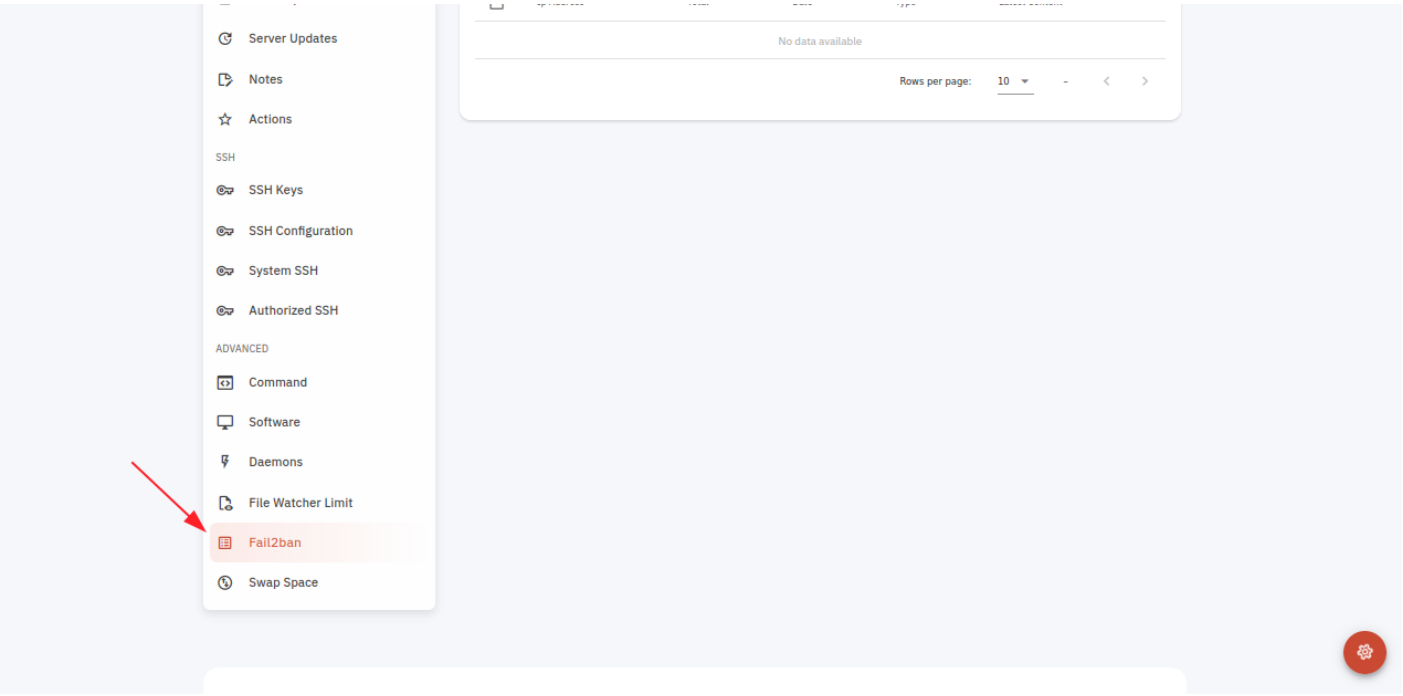
How to install a Server

Follow the steps below to add Filters in Fail2Ban.

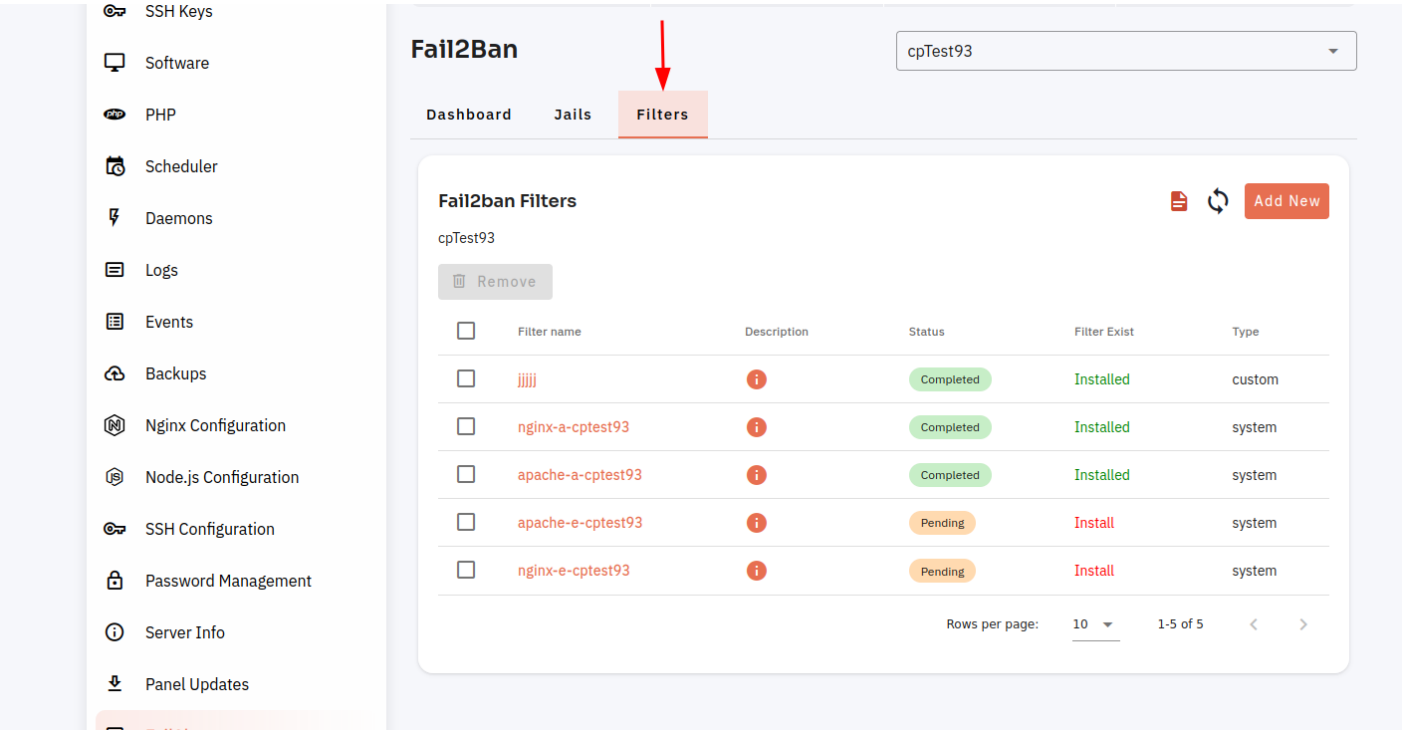
1: Once you are logged in, look for a "Server" and click on it.



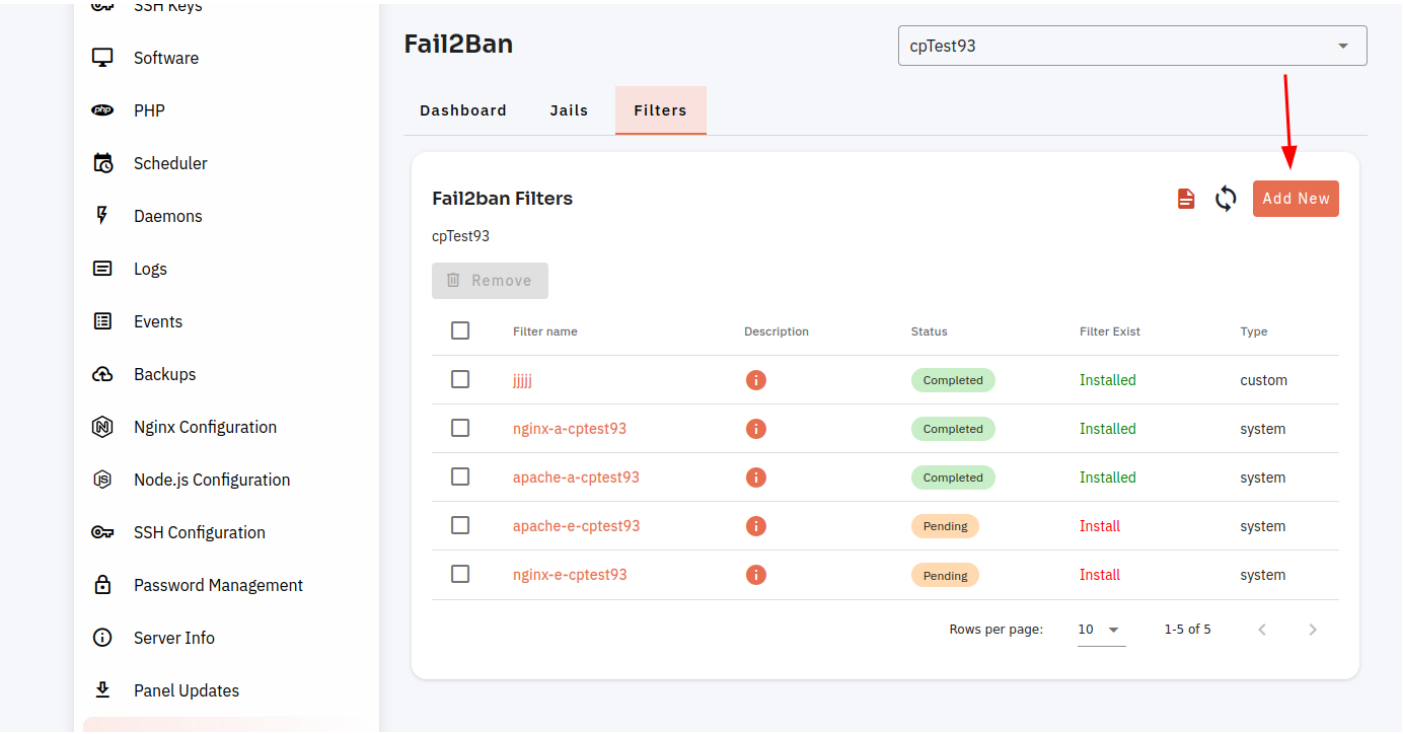
2. Select the Fail2ban option.



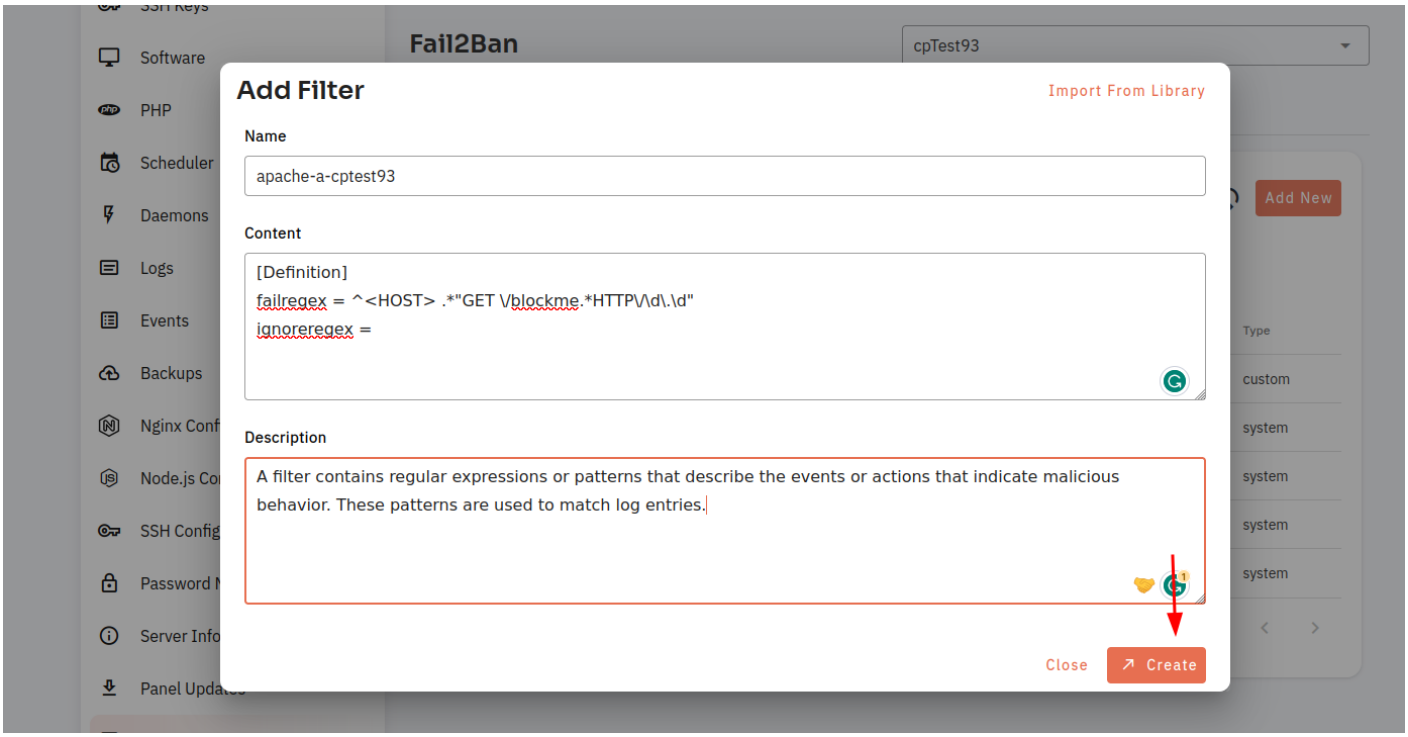
3. Click on the Filters button.



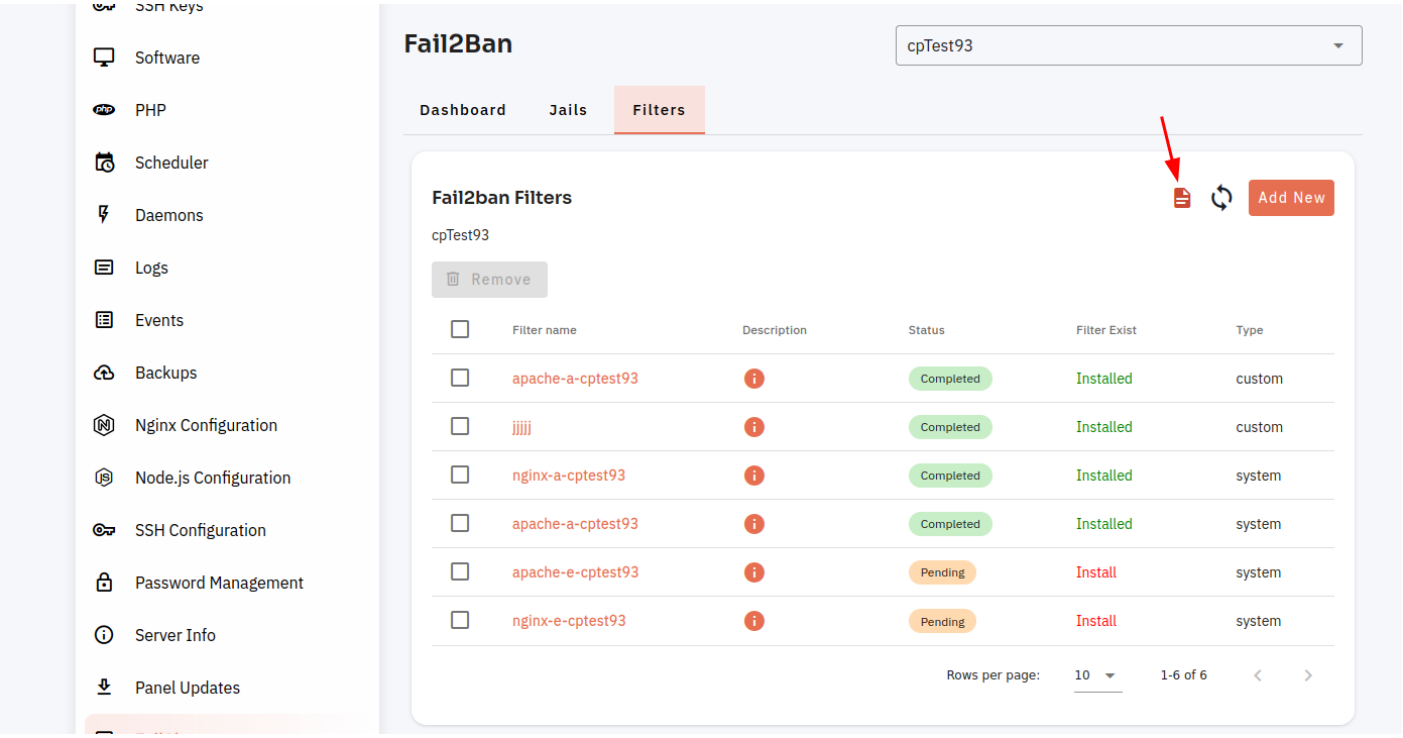
4. Click on the Add New button.



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.



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

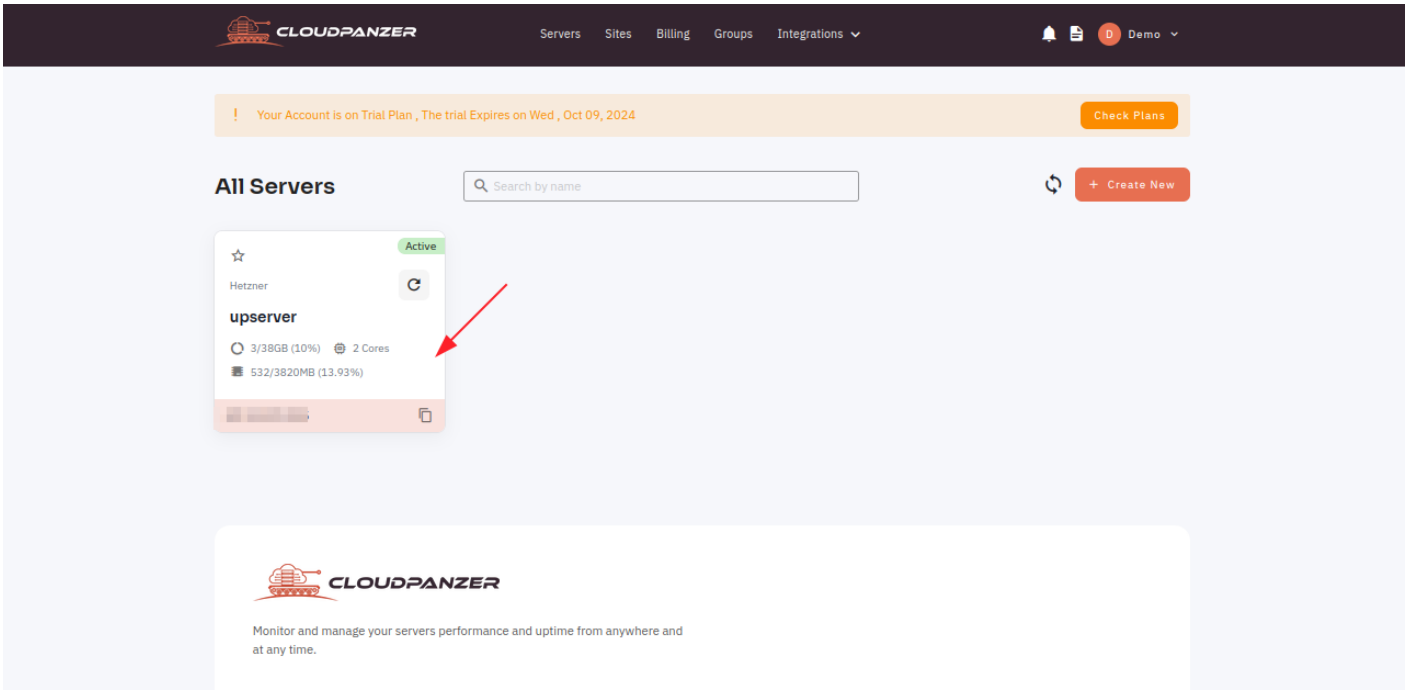
How to add Jails in Fail2Ban on CloudPanzer?

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.

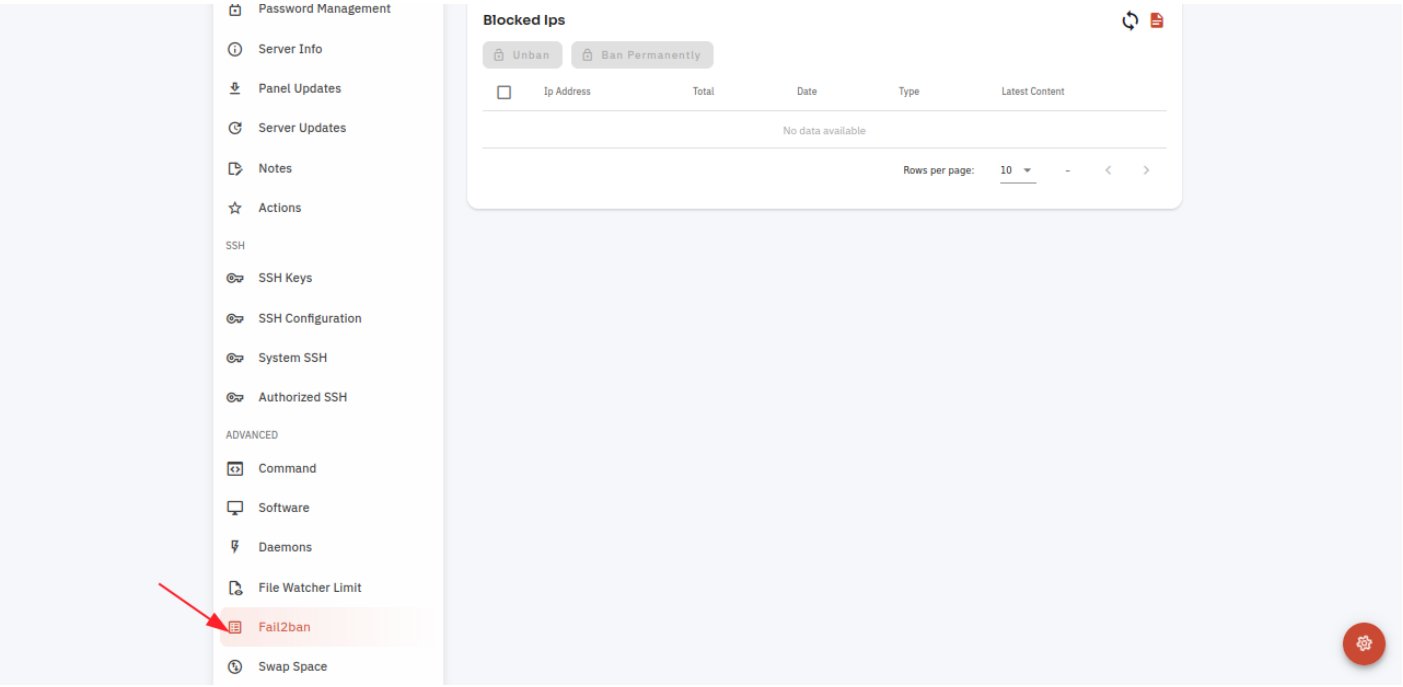
How to install a Server

Follow the steps below to add Jails in Fail2Ban.

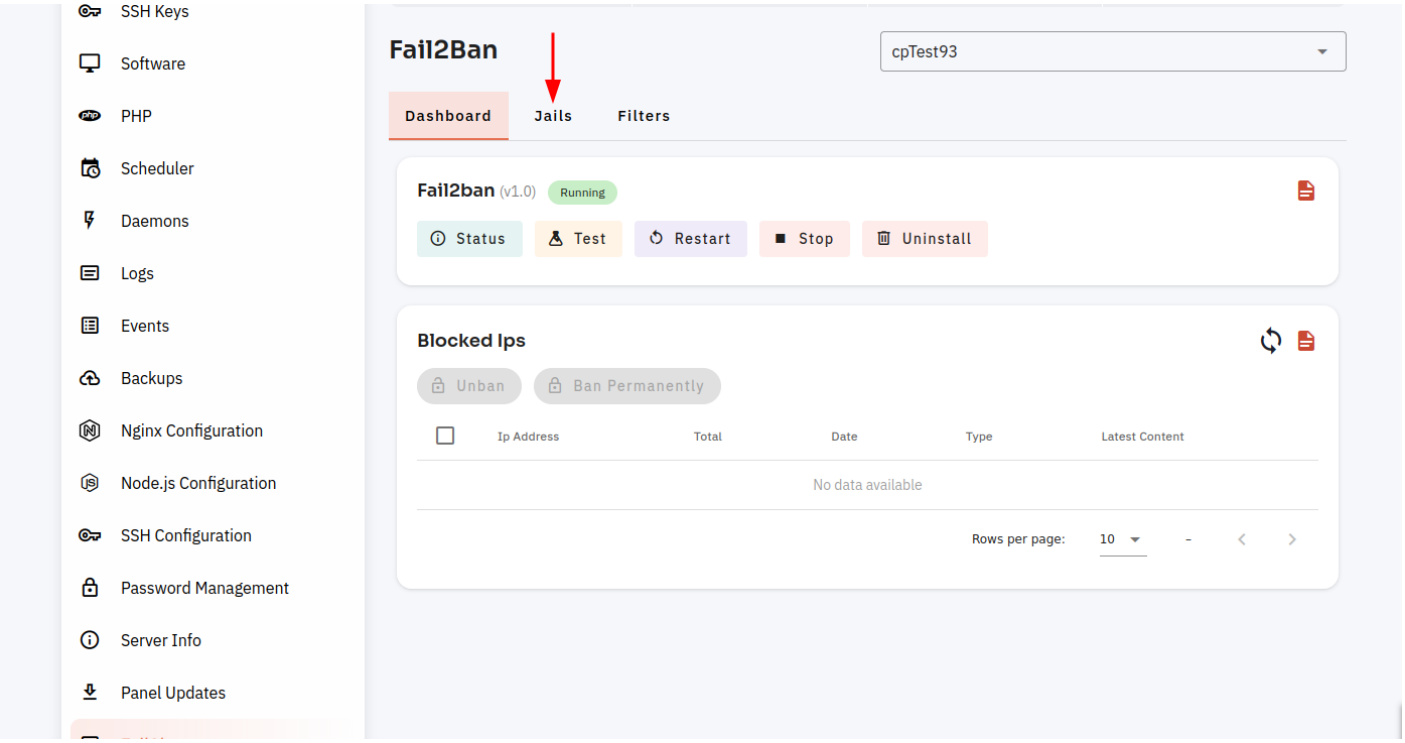
1: Once you are logged in, look for a "Server" and click on it.



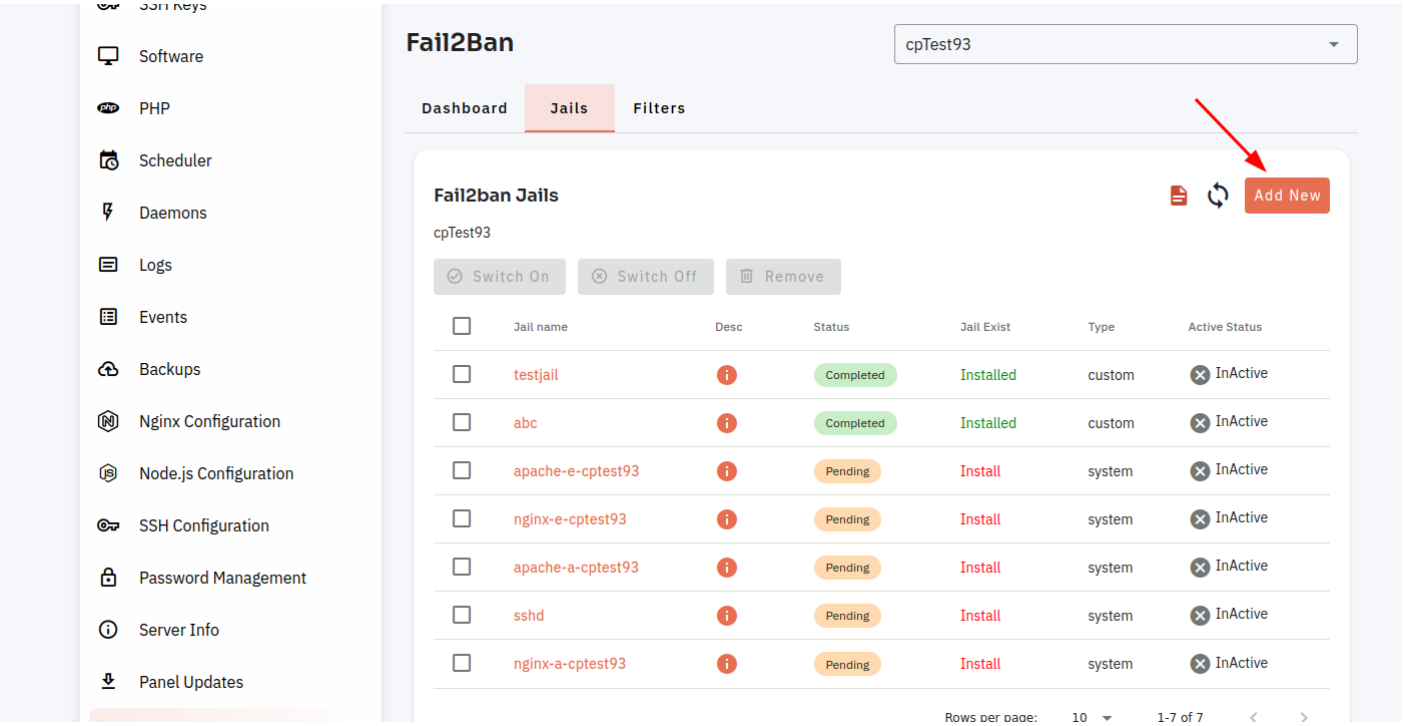
2. Select the Fail2ban option.



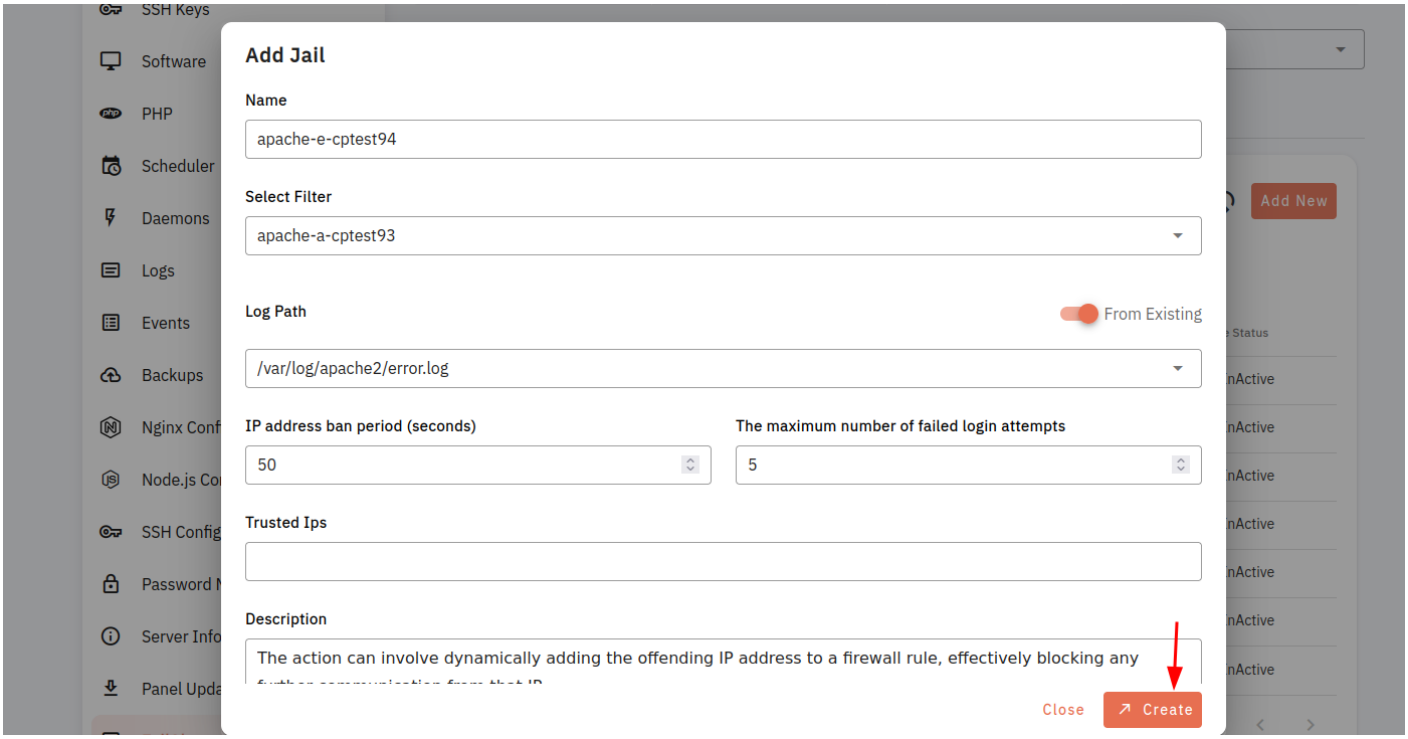
3. Click on the Jails button.



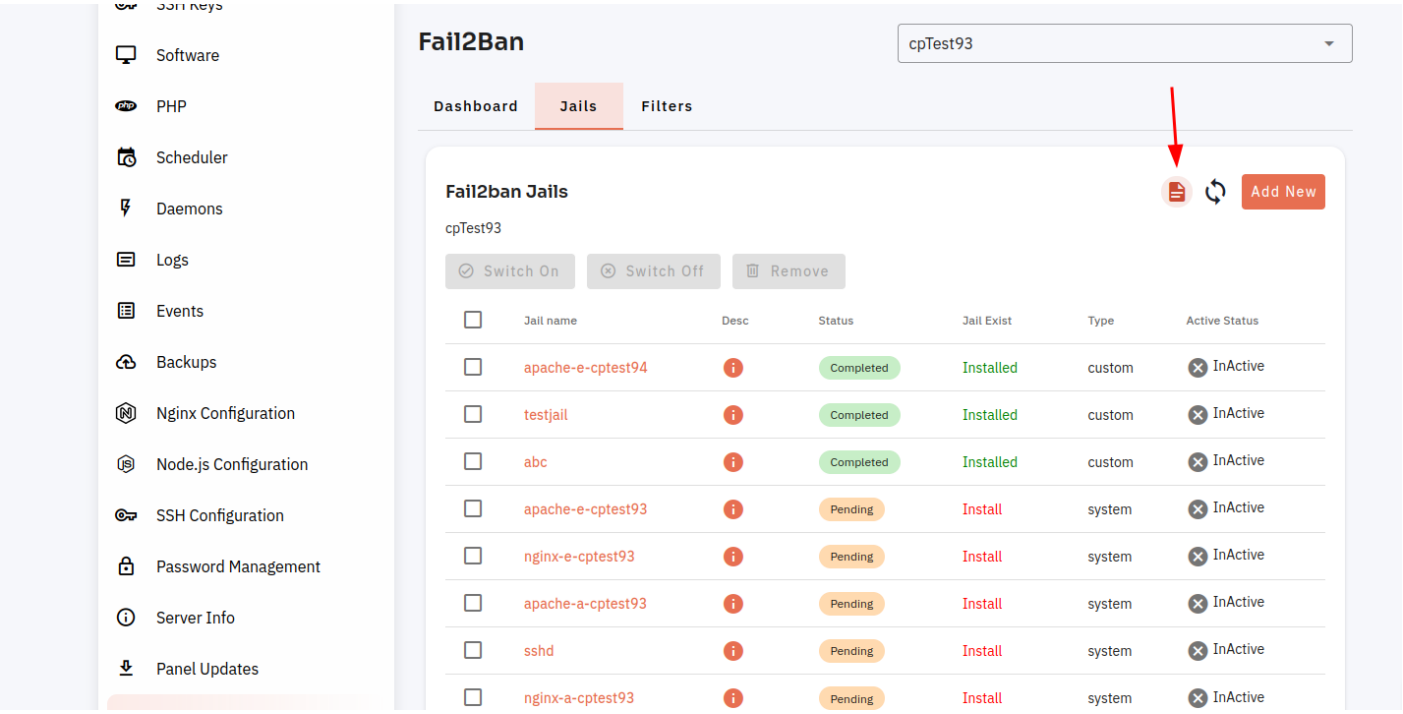
4. Click on the Add New Button.



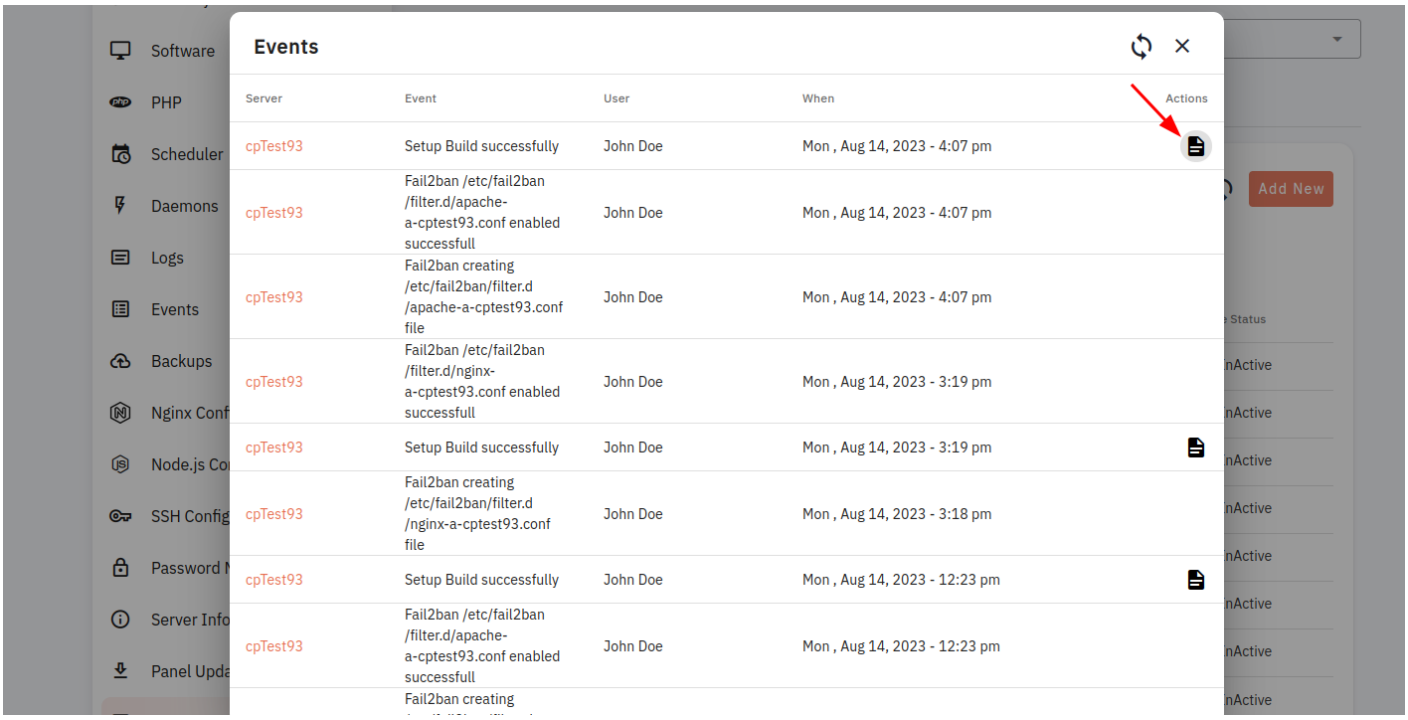
5. Fill in the details and click on the Create button.



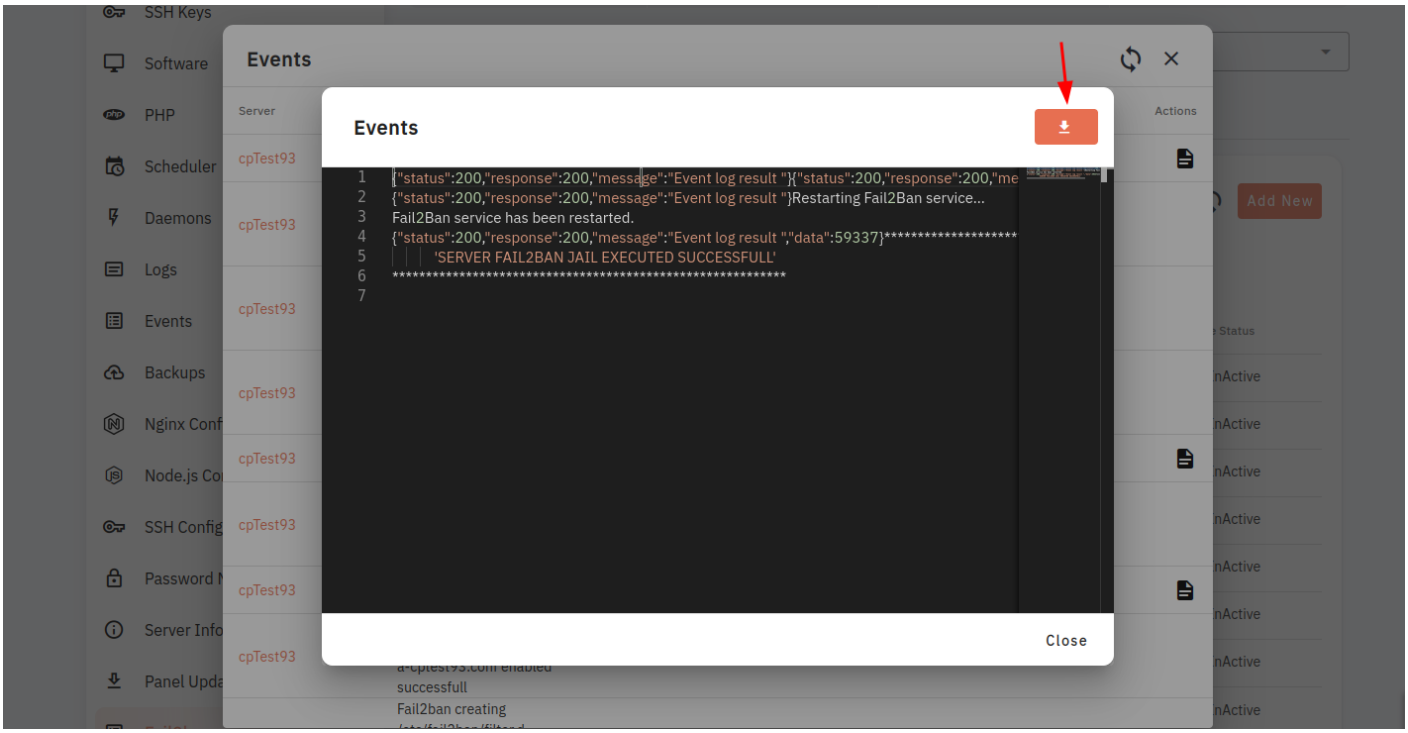
6. Here, a new jail has been created. You can also check events by clicking on the file icon.



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



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

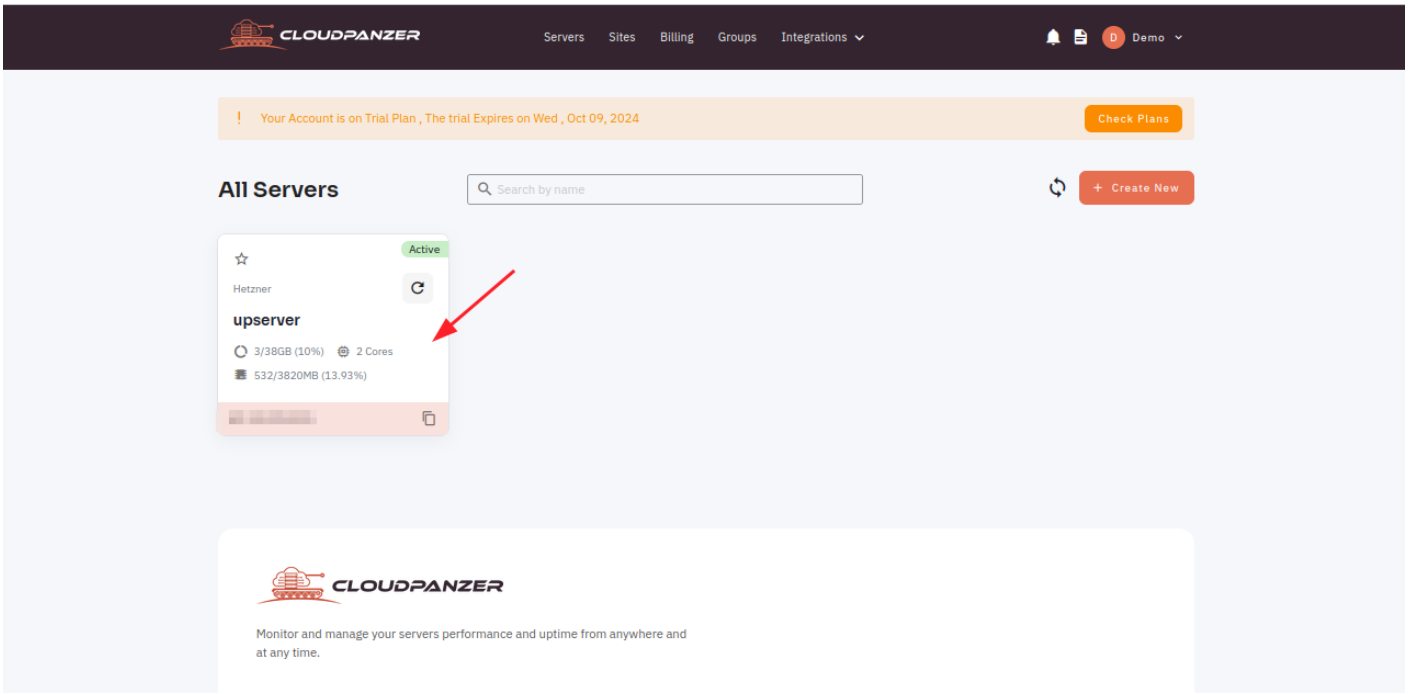
Tutorial :

You can watch the Video or Continue reading the post.

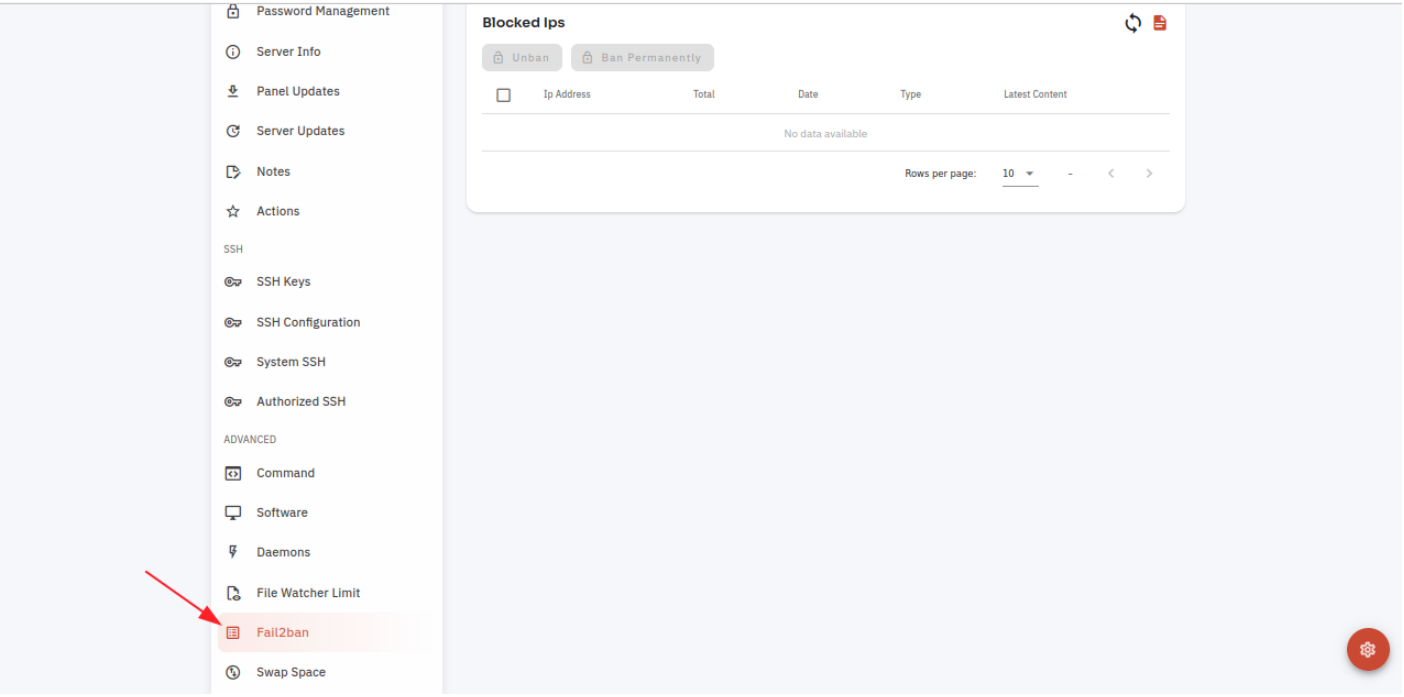
https://www.youtube.com/embed/3pzI-vMFSMA

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

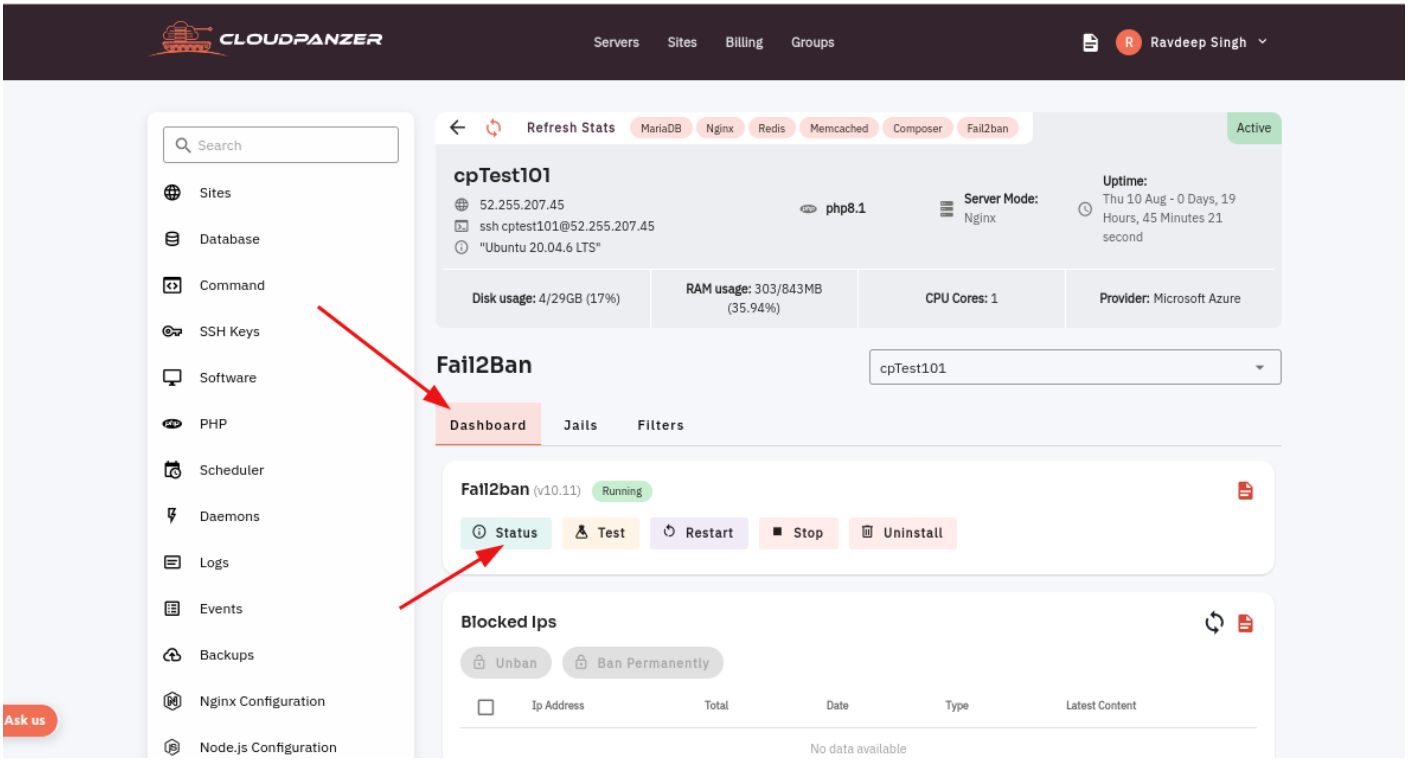
1: Once you are logged in, look for a "Server" and click on it.



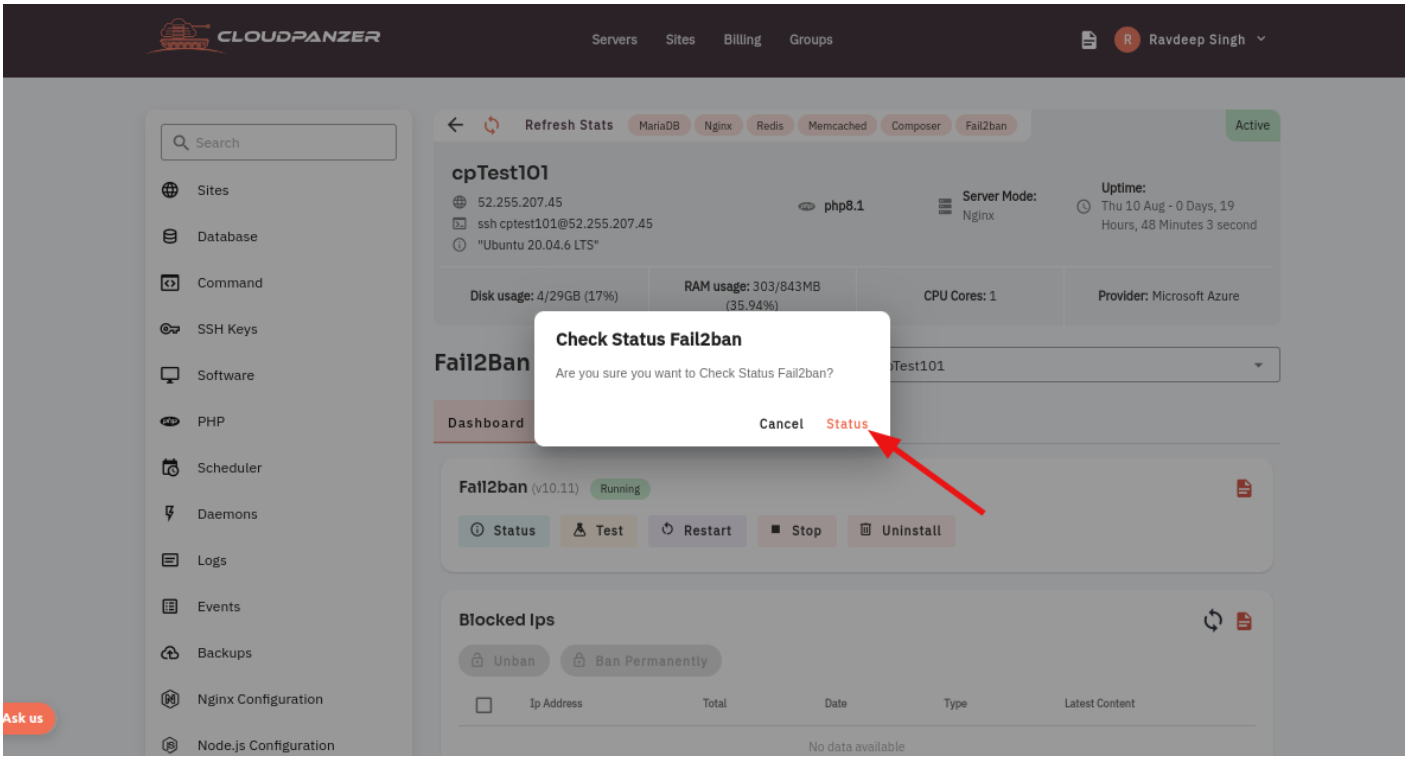
2. Select the Fail2ban option.



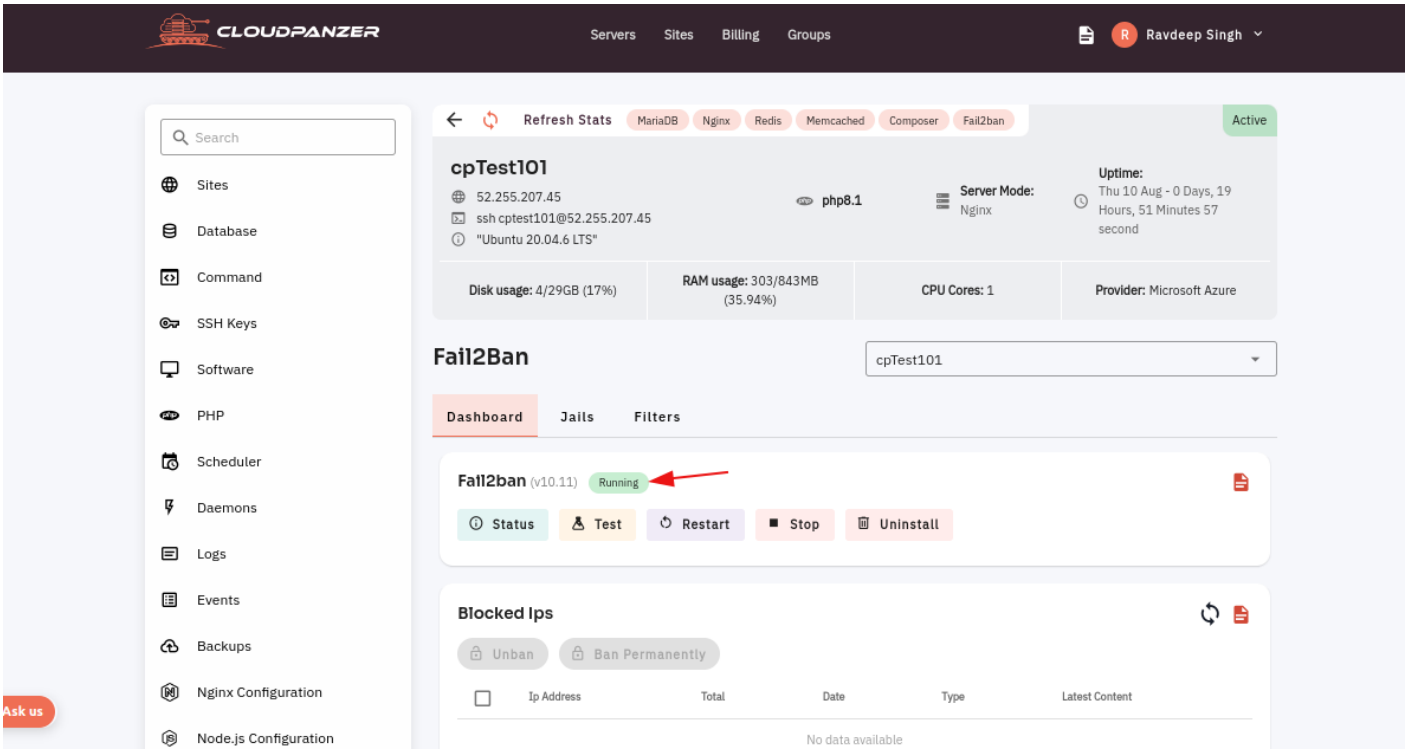
3. Select a Dashboard tab and click on the Status button.



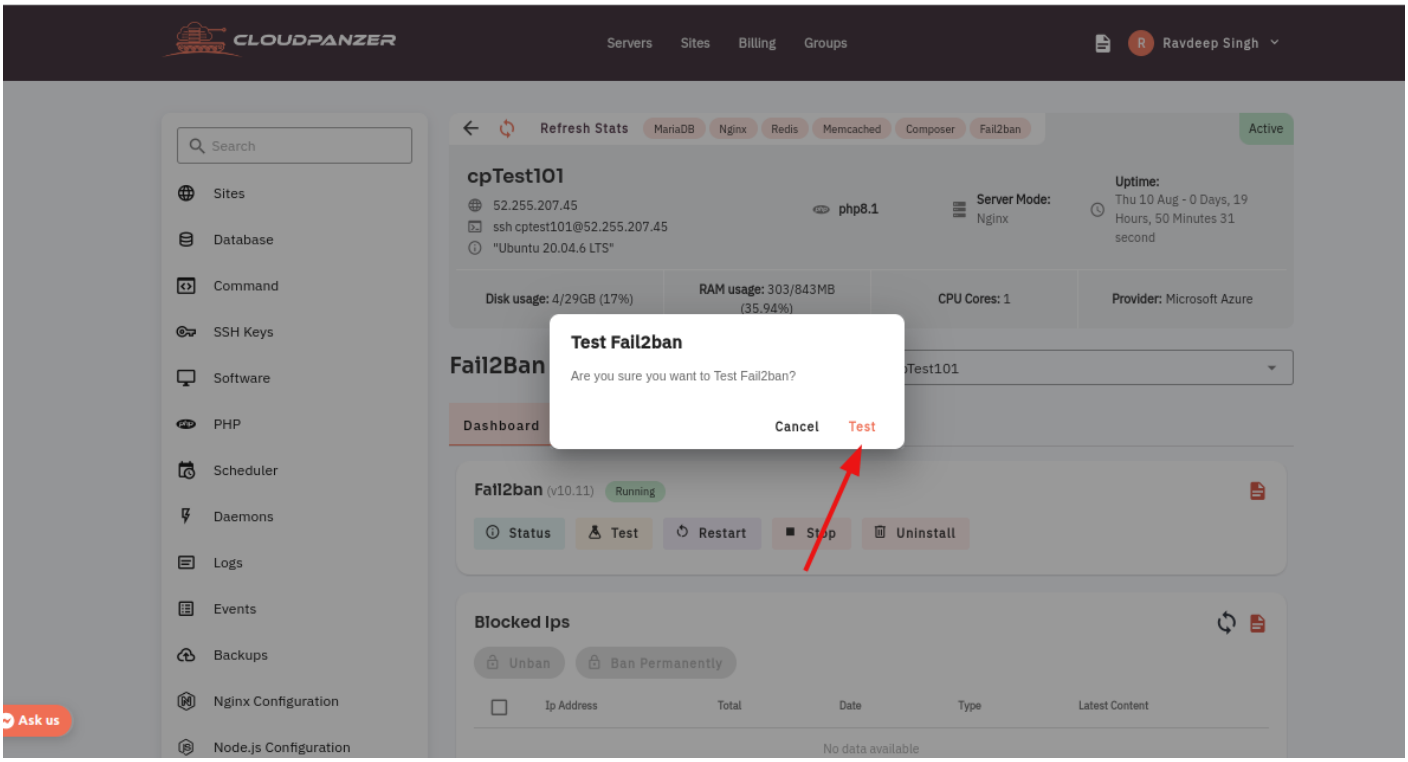
4. A dialog box will open and click on the Yes button to check the Status.



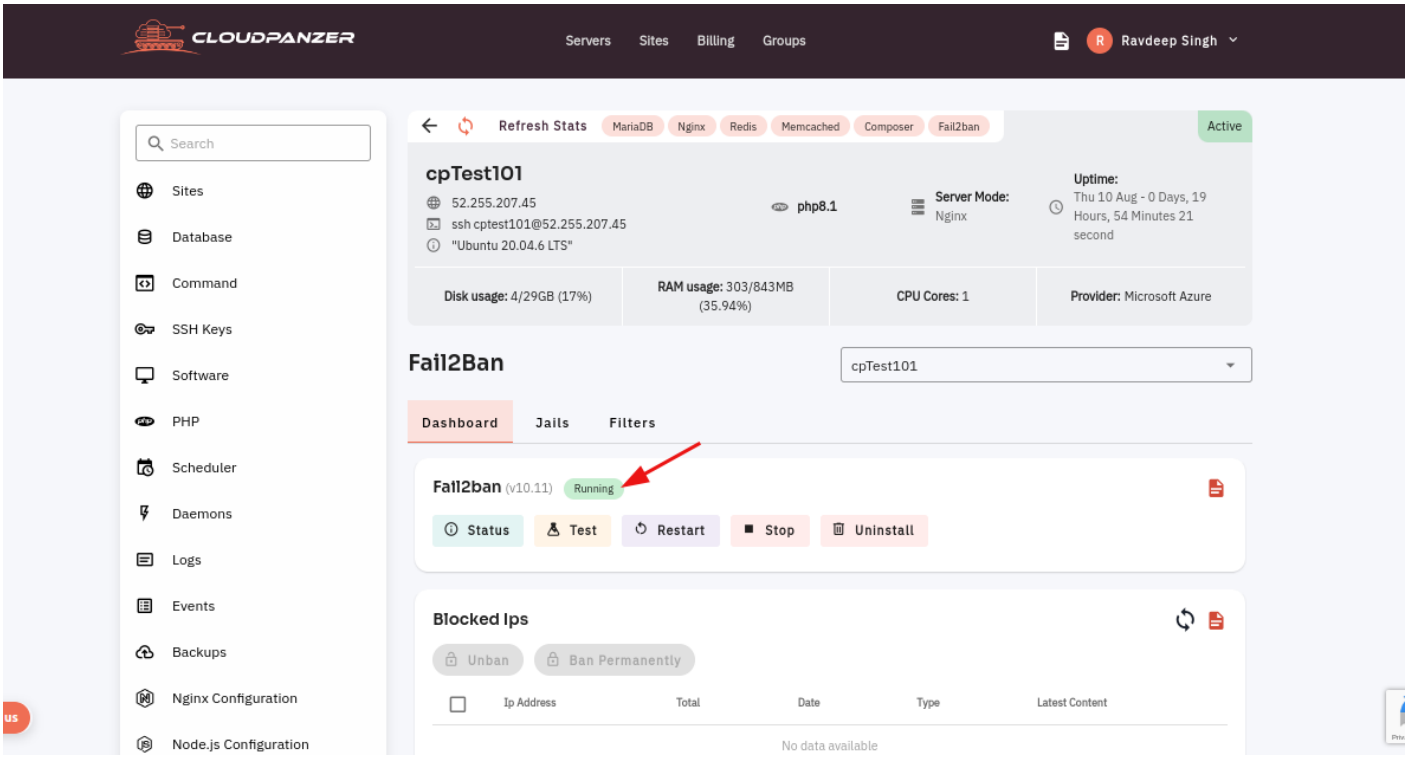
Here, you can see the Status checked successfully.



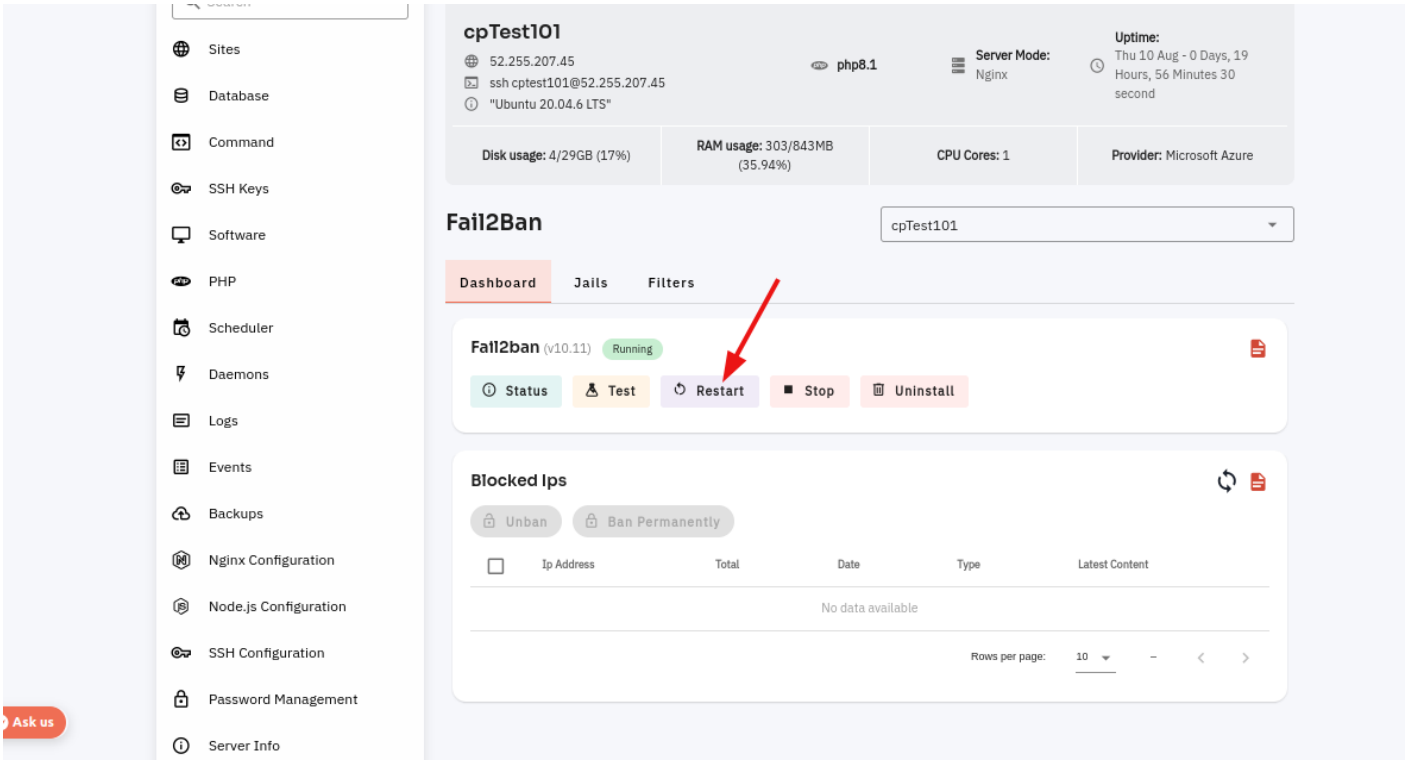
5. Click on the Test button to test a Fail2Ban.



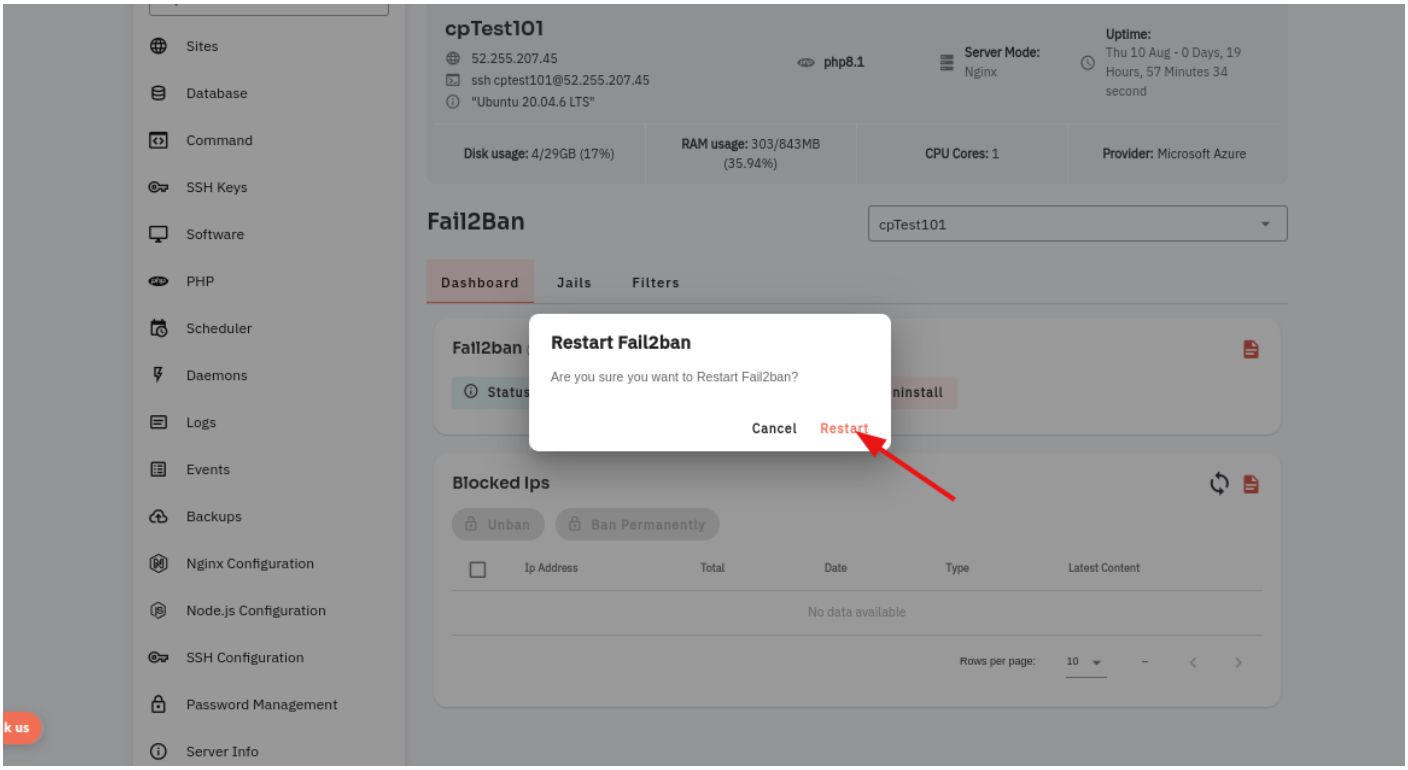
Here, you can see the server tested successfully.



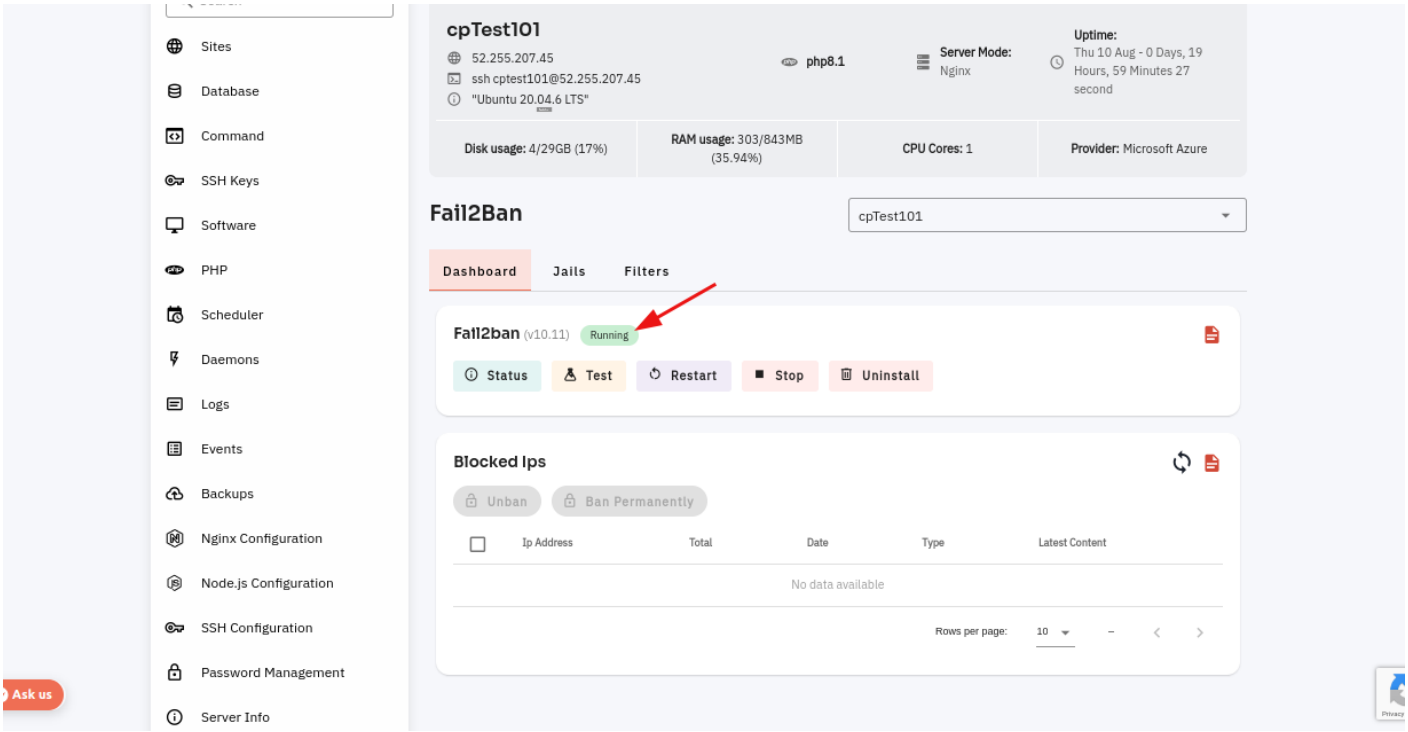
6. Click on the Restart button.



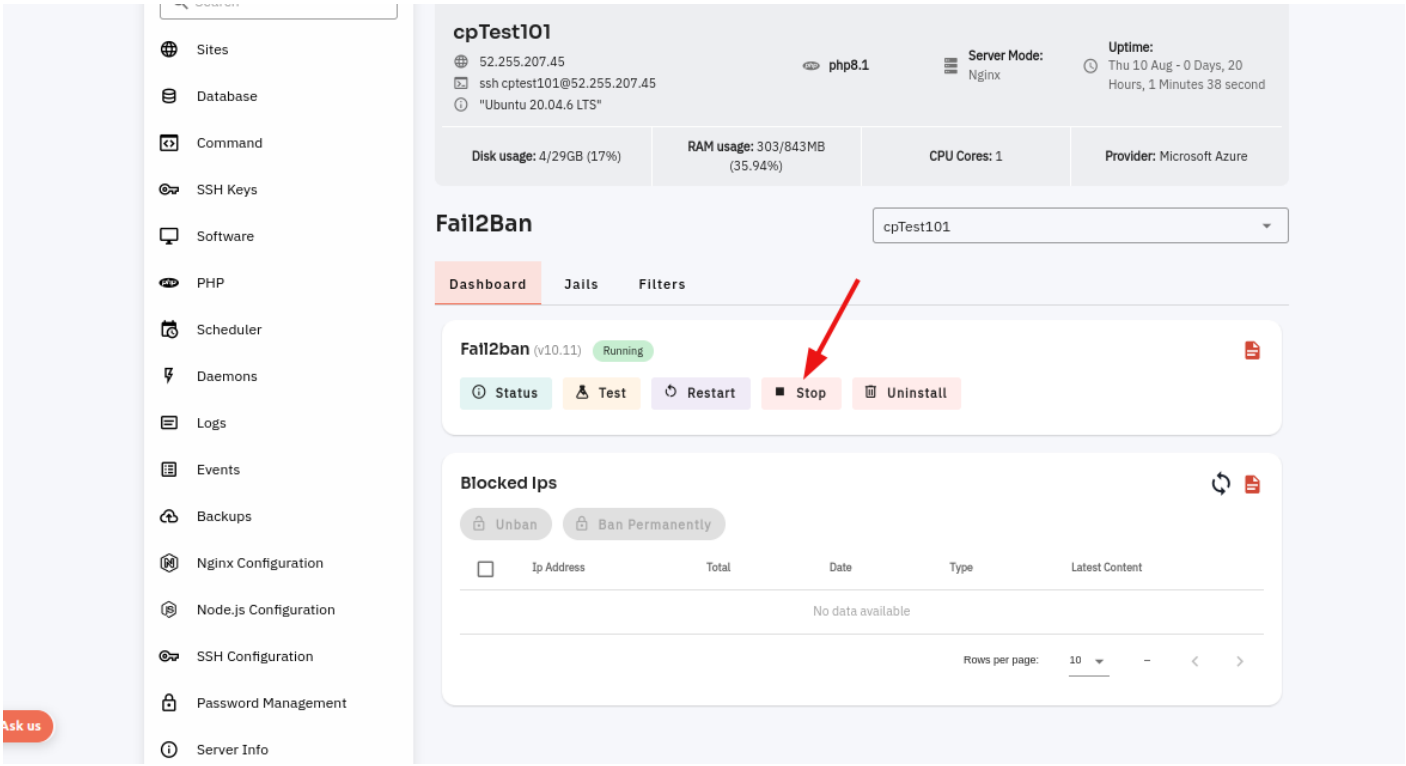
7. A dialog will open, then click on the Restart button.



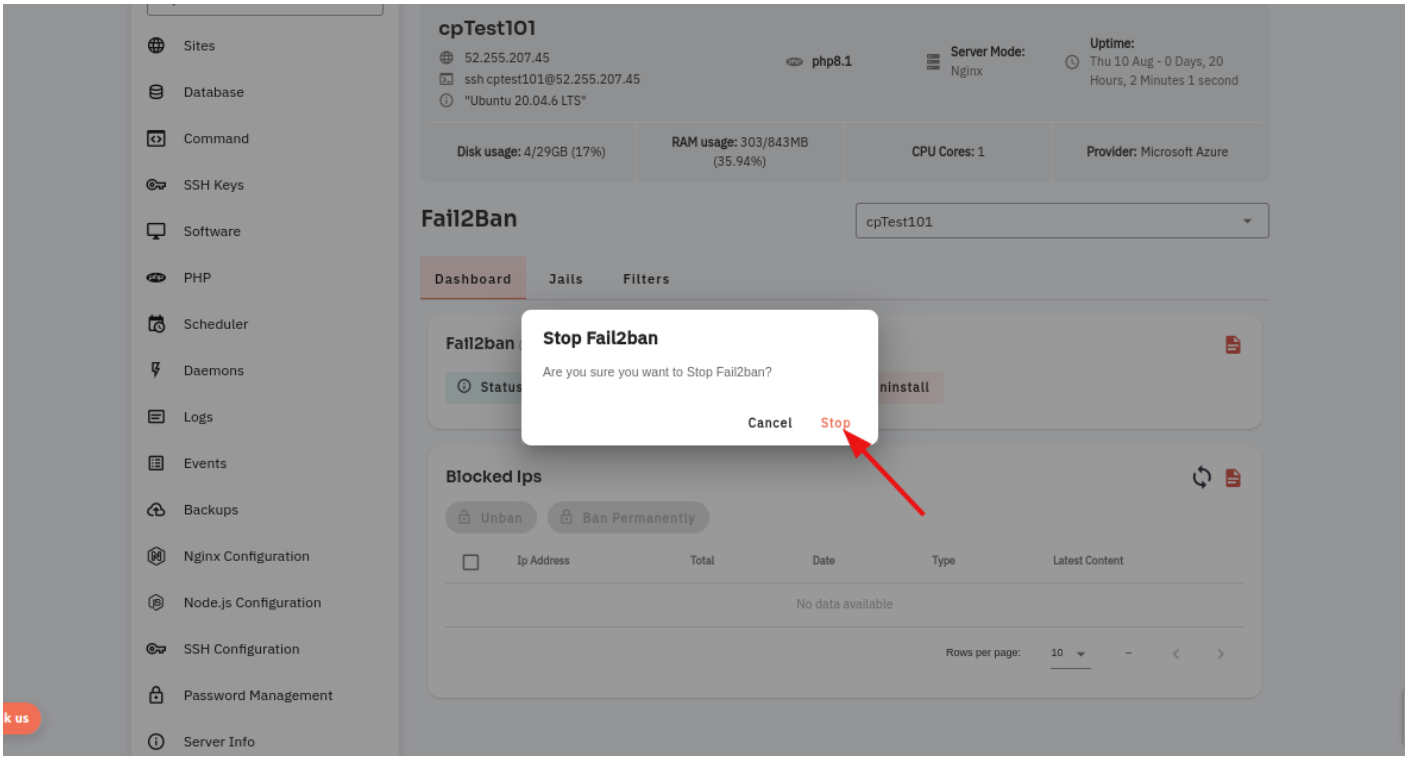
8. Here, you can see Fail2Ban restarted successfully.



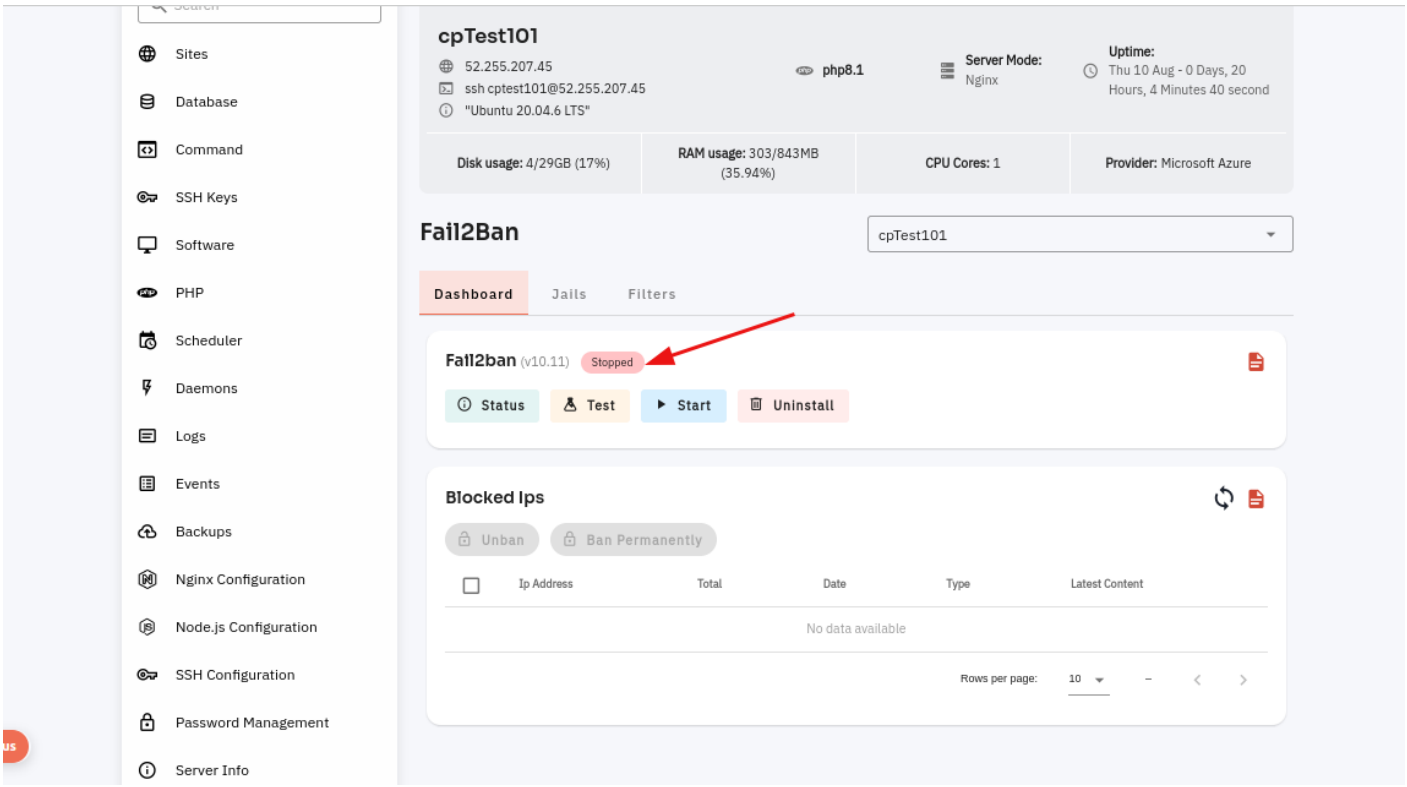
9. Click on the stop button.



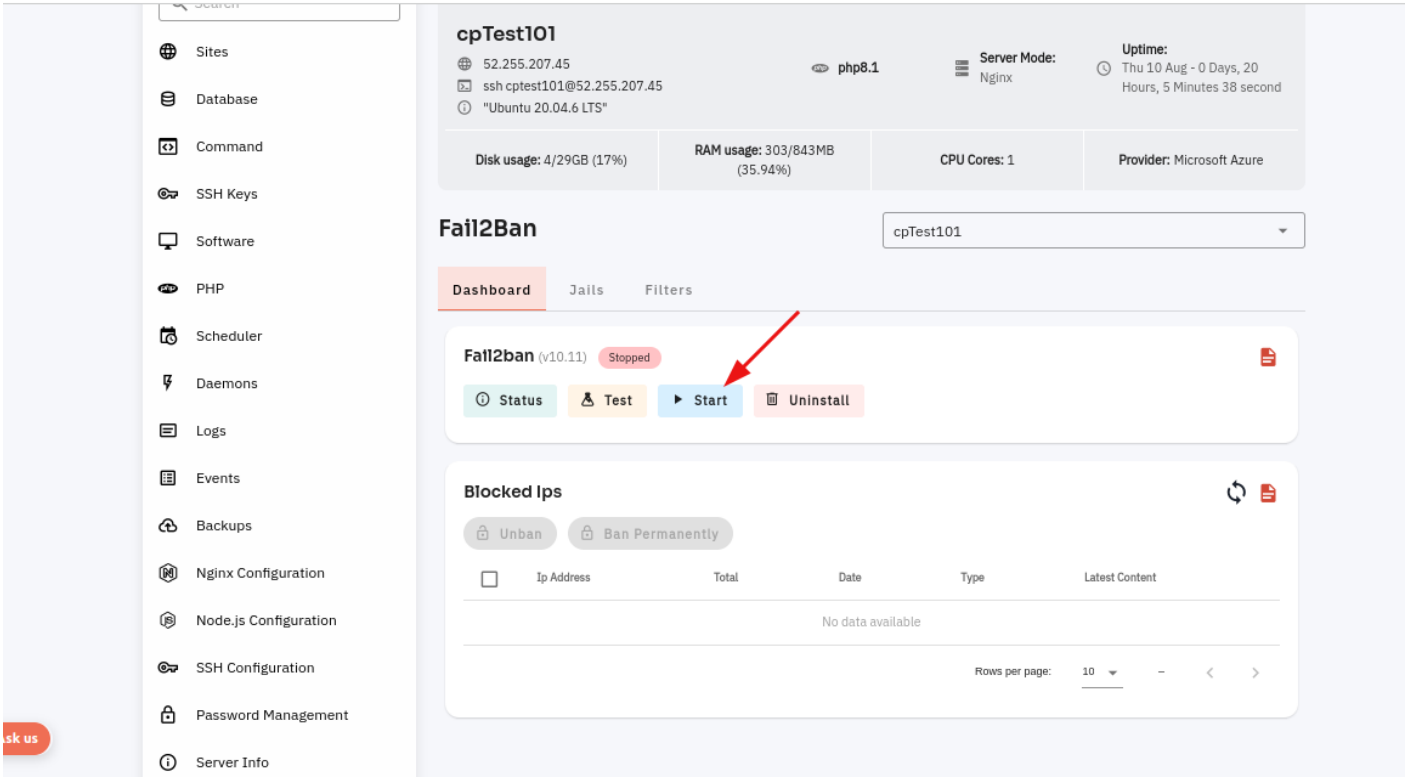
10. A dialog will open and click on the stop button.



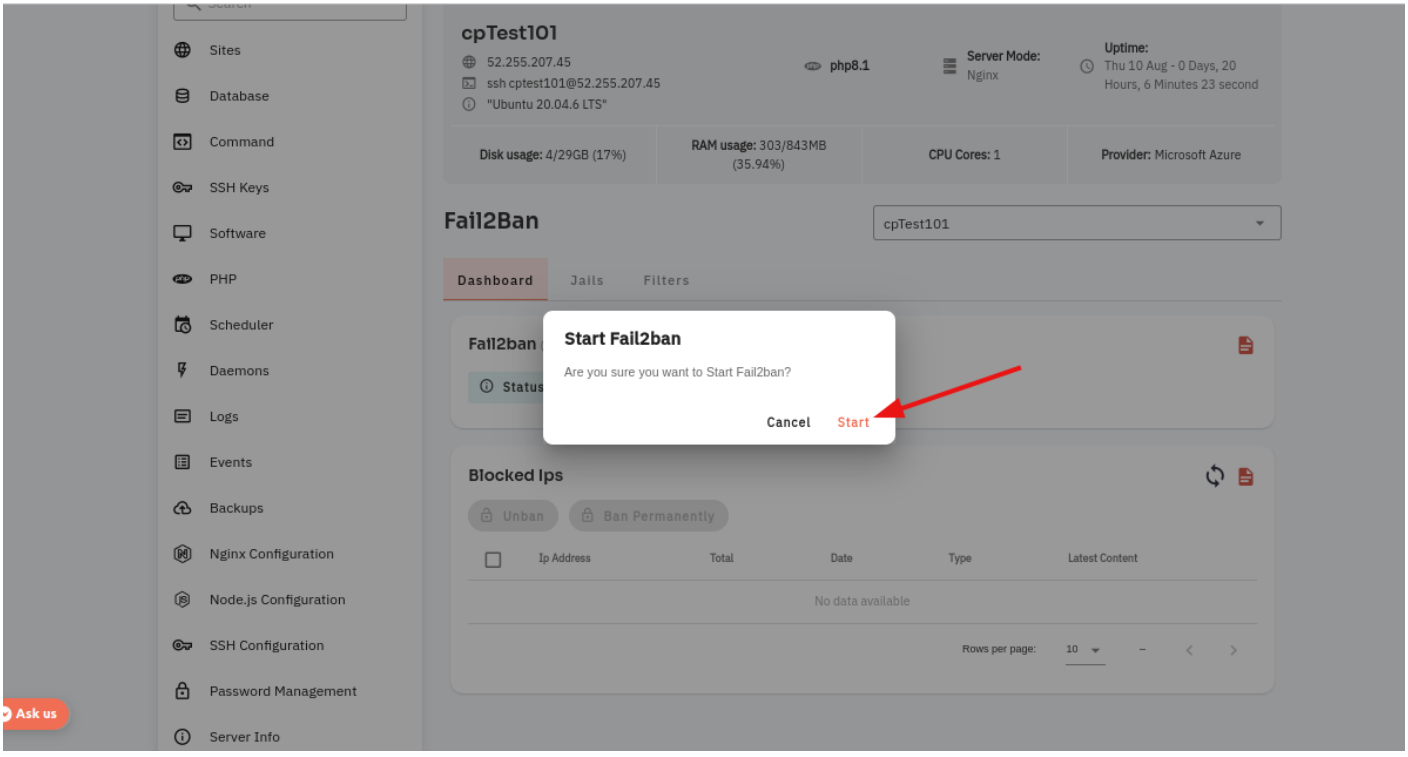
Here, you can see that Fail2Ban stopped successfully.



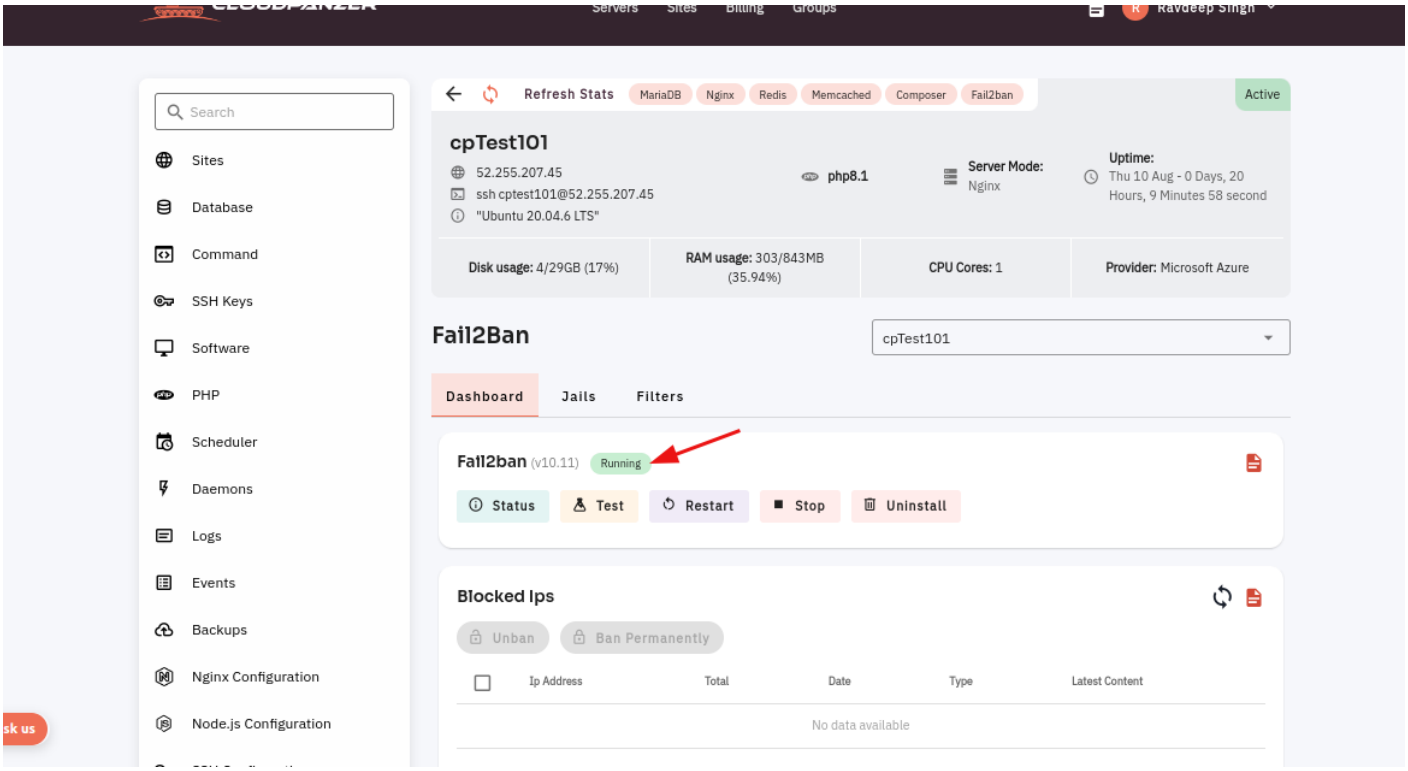
11. Click on the Start button.



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