

# 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

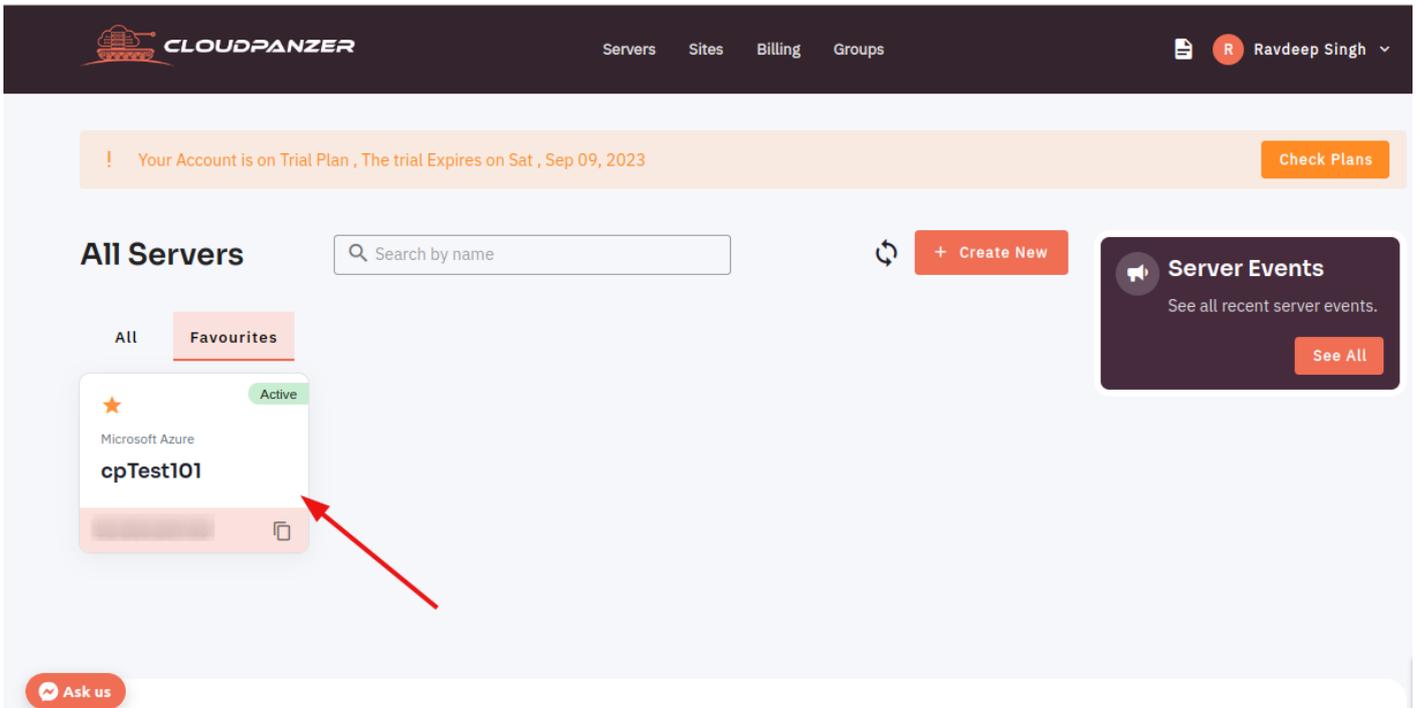
### Tutorial :

**You can watch the Video or Continue reading the post.**

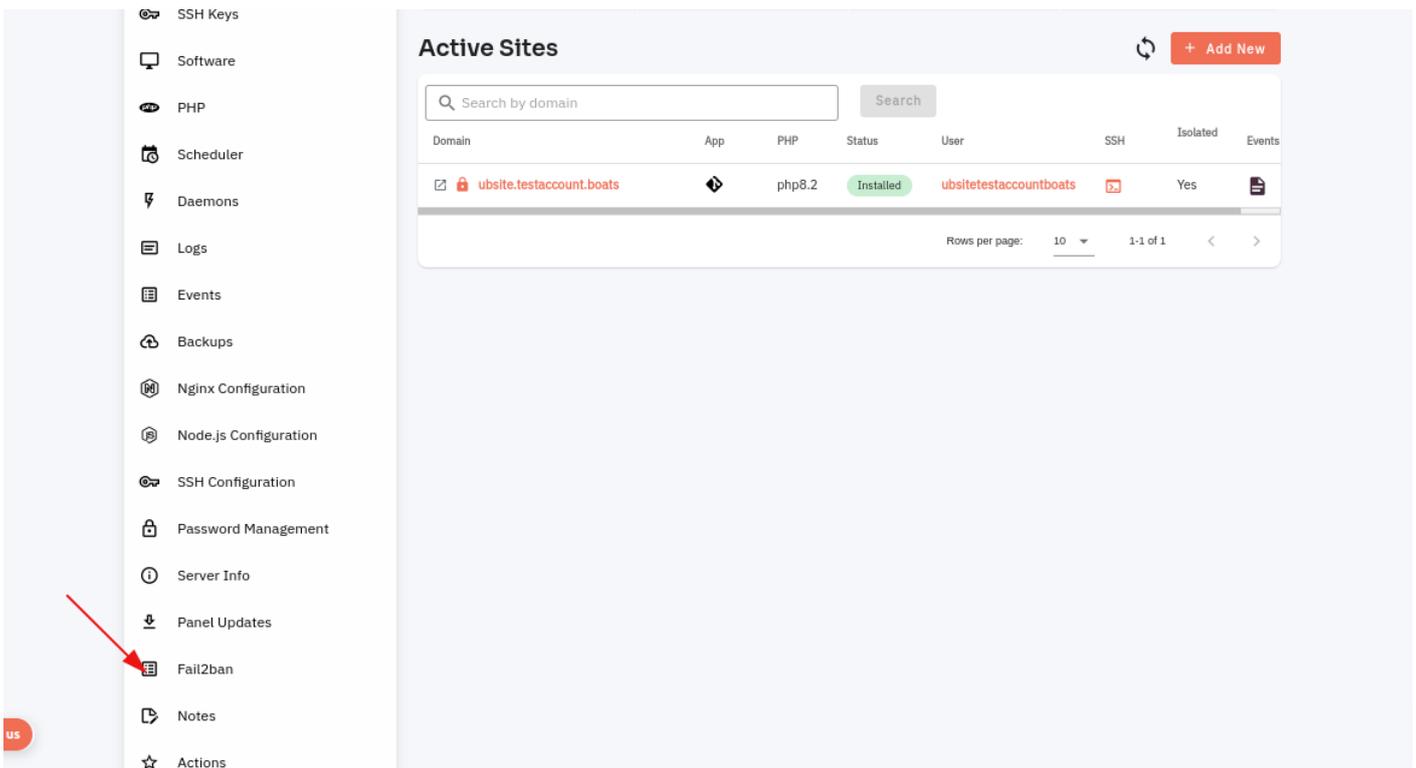
<https://www.youtube.com/embed/3pzi-vMFSMA>

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.



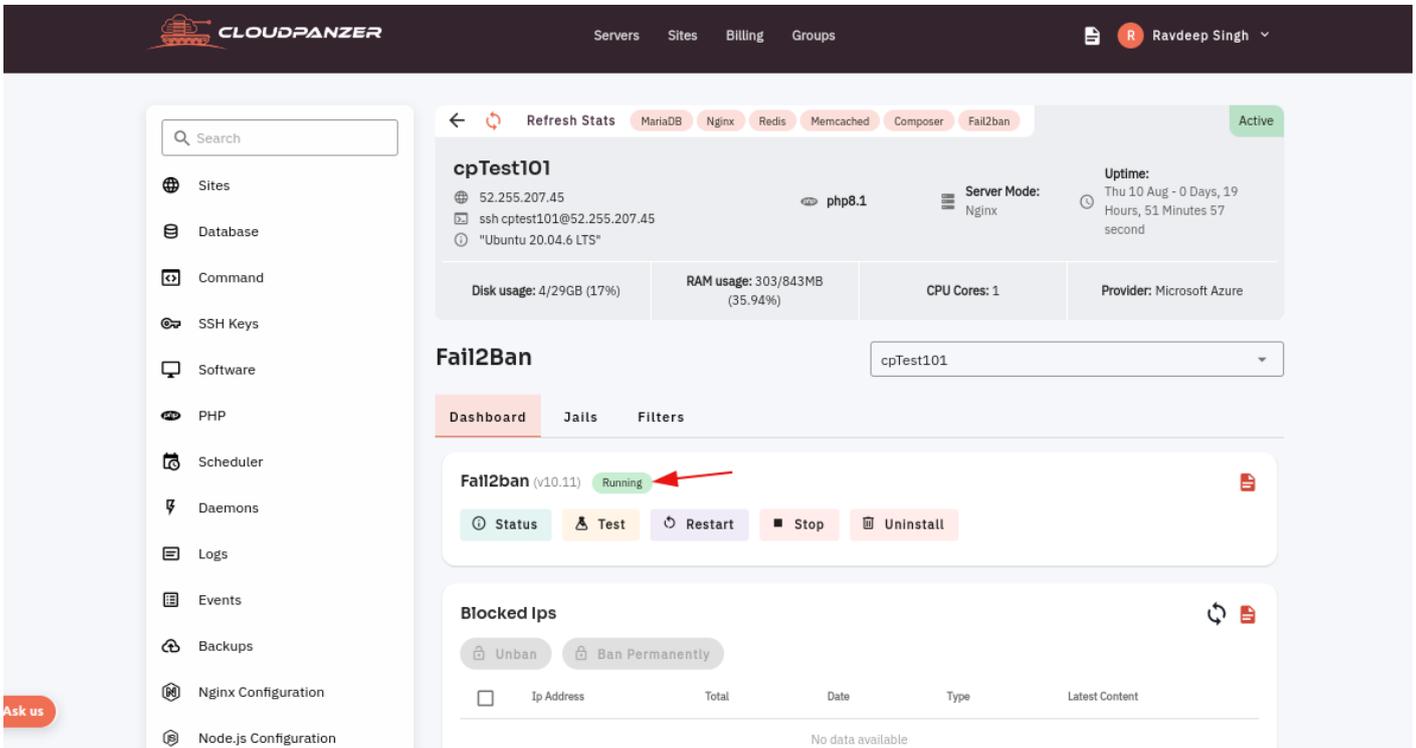
3. Select a Dashboard tab and click on the Status button.

The screenshot shows the CloudPanzer dashboard for server **cpTest101**. The server is running Fail2ban (v10.11). The dashboard includes a sidebar with navigation options like Sites, Database, Command, SSH Keys, Software, PHP, Scheduler, Daemons, Logs, Events, Backups, Nginx Configuration, and Node.js Configuration. The main content area shows server statistics (Disk usage: 4/29GB (17%), RAM usage: 303/843MB (35.94%), CPU Cores: 1, Provider: Microsoft Azure) and the Fail2ban service status (Running). Below the status, there are buttons for Status, Test, Restart, Stop, and Uninstall. A 'Blocked Ips' section is also visible, currently showing 'No data available'. Two red arrows point to the 'Status' button and the 'Dashboard' tab.

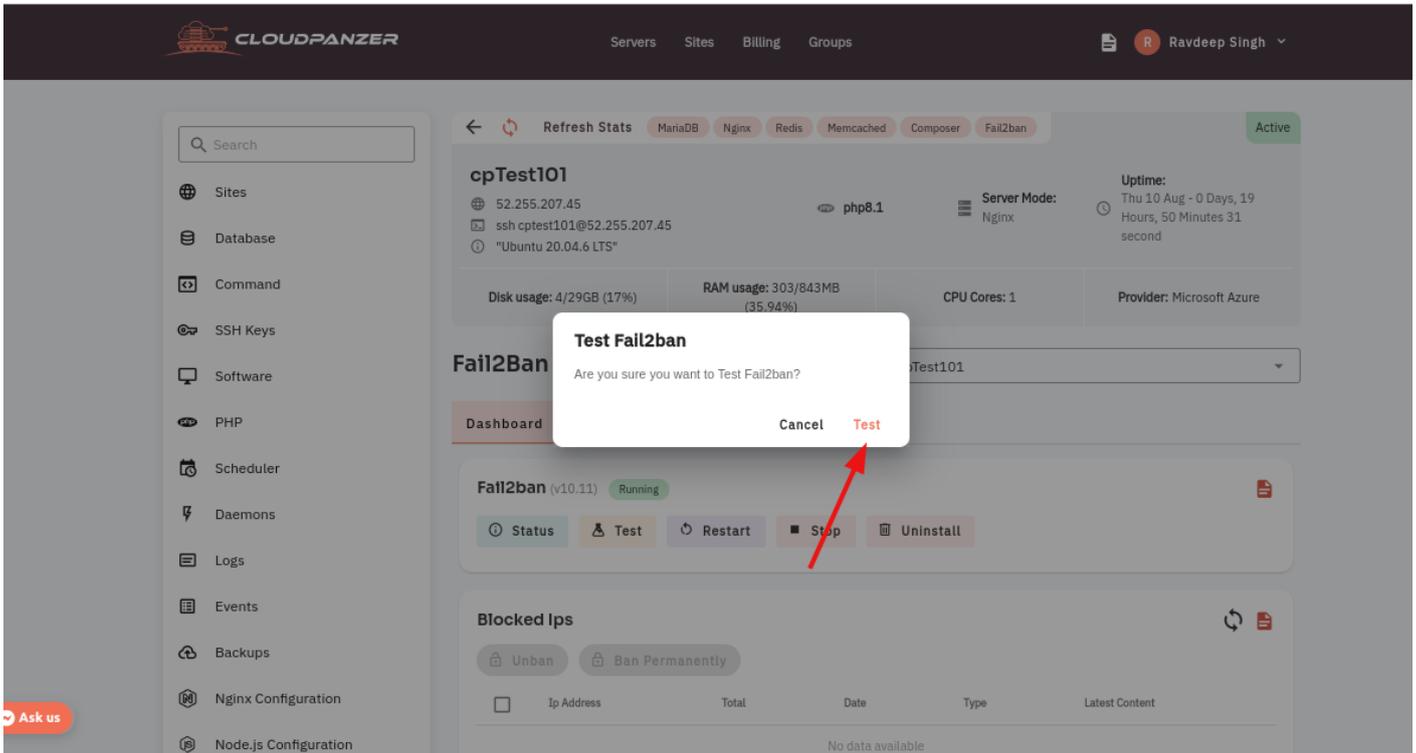
4. A dialog box will open and click on the Yes button to check the Status.

This screenshot shows the same CloudPanzer dashboard as above, but with a confirmation dialog box open. The dialog box is titled "Check Status Fail2ban" and asks "Are you sure you want to Check Status Fail2ban?". It has two buttons: "Cancel" and "Status". A red arrow points to the "Status" button. The background dashboard is dimmed.

Here, you can see the Status checked successfully.



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



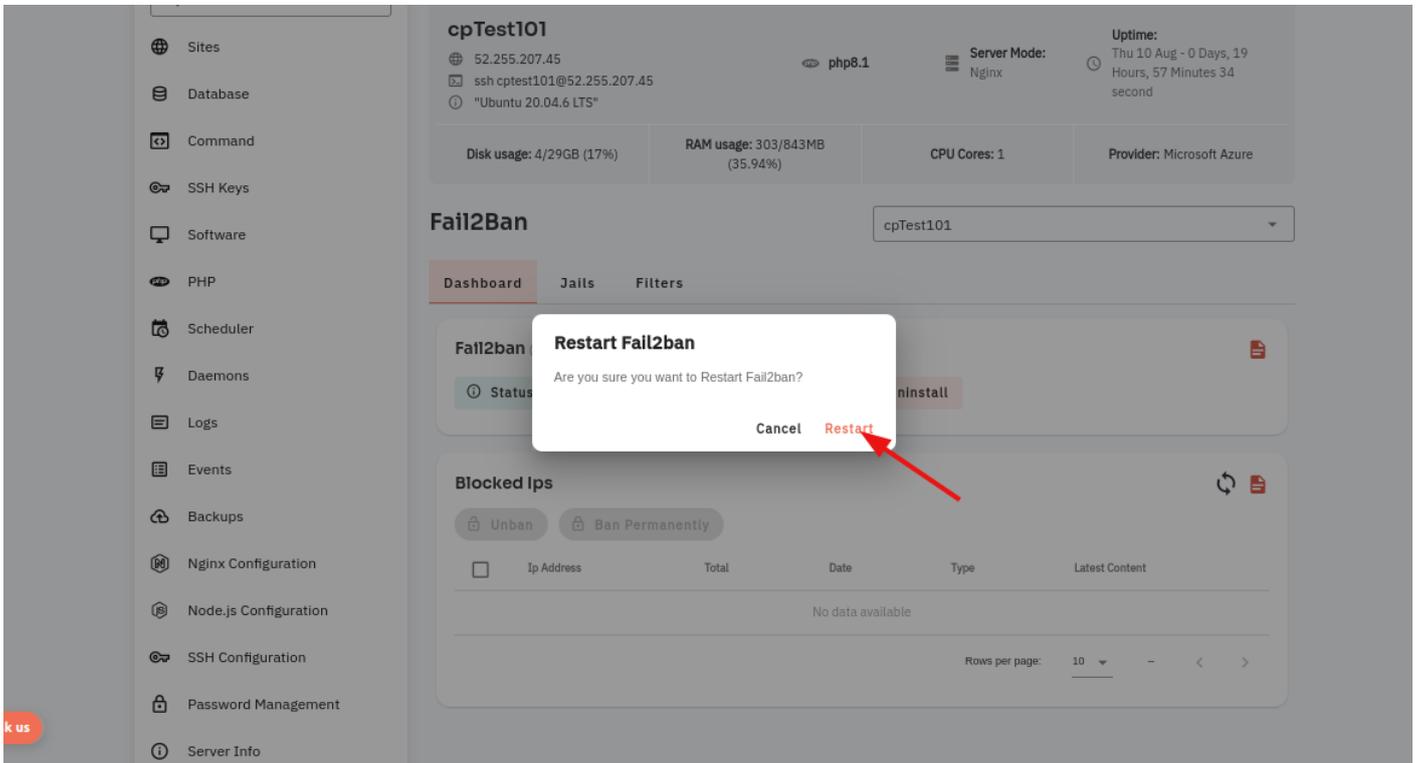
Here, you can see the server tested successfully.

The screenshot shows the CloudPanzer dashboard for a server named 'cpTest101'. The server is running Ubuntu 20.04.6 LTS with PHP 8.1 and Nginx. The Fail2Ban service is installed and currently in a 'Running' state. The dashboard includes a sidebar with navigation options like Sites, Database, Command, SSH Keys, Software, PHP, Scheduler, Daemons, Logs, Events, Backups, Nginx Configuration, and Node.js Configuration. The main content area shows the Fail2Ban service details, including its version (v10.11) and a 'Running' status indicator. Below the service status, there are buttons for 'Status', 'Test', 'Restart', 'Stop', and 'Uninstall'. A red arrow points to the 'Restart' button. Below this, there is a 'Blocked Ips' section with 'Unban' and 'Ban Permanently' buttons and a table with columns for 'Ip Address', 'Total', 'Date', 'Type', and 'Latest Content'. The table currently shows 'No data available'.

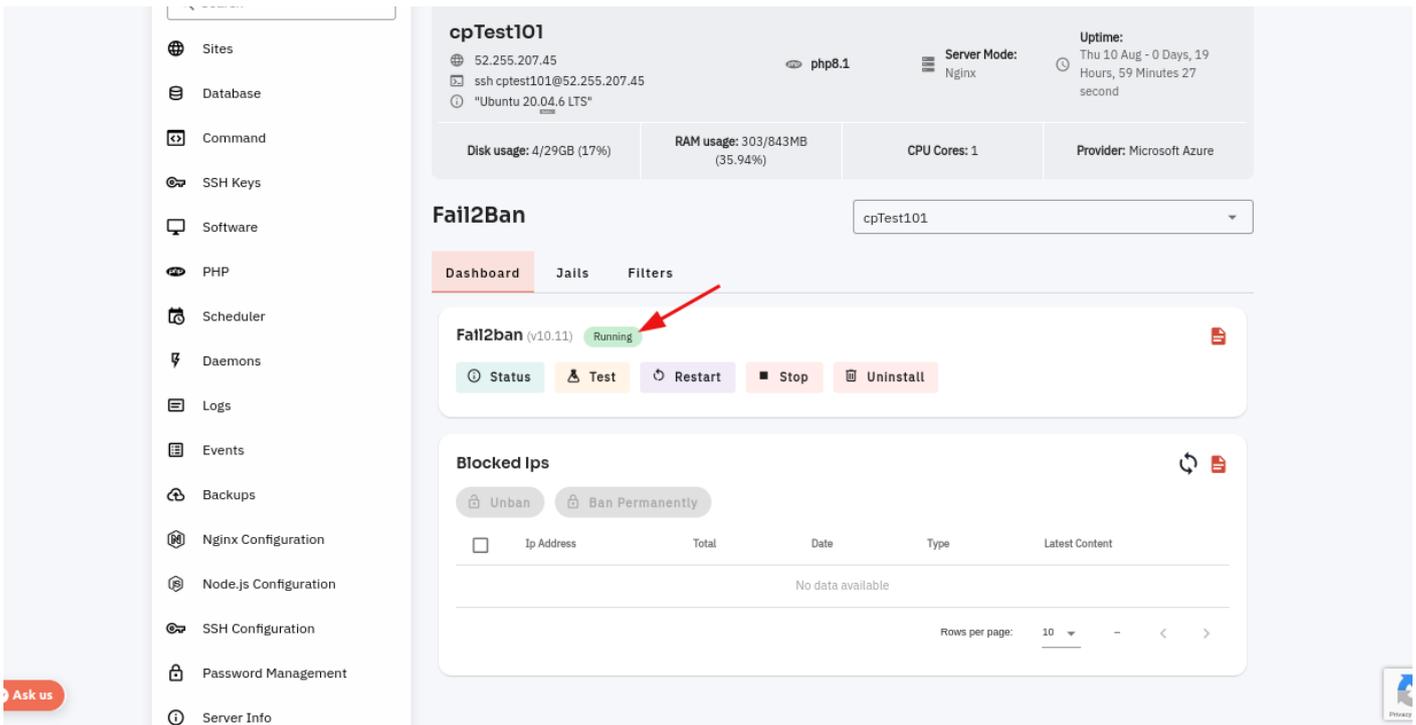
6. Click on the Restart button.

This screenshot is similar to the previous one, showing the CloudPanzer dashboard for the 'cpTest101' server. The Fail2Ban service is still 'Running'. In this view, a red arrow points to the 'Restart' button, which is highlighted. The 'Blocked Ips' section below shows the same 'No data available' status. The 'Rows per page' dropdown at the bottom right is set to 10.

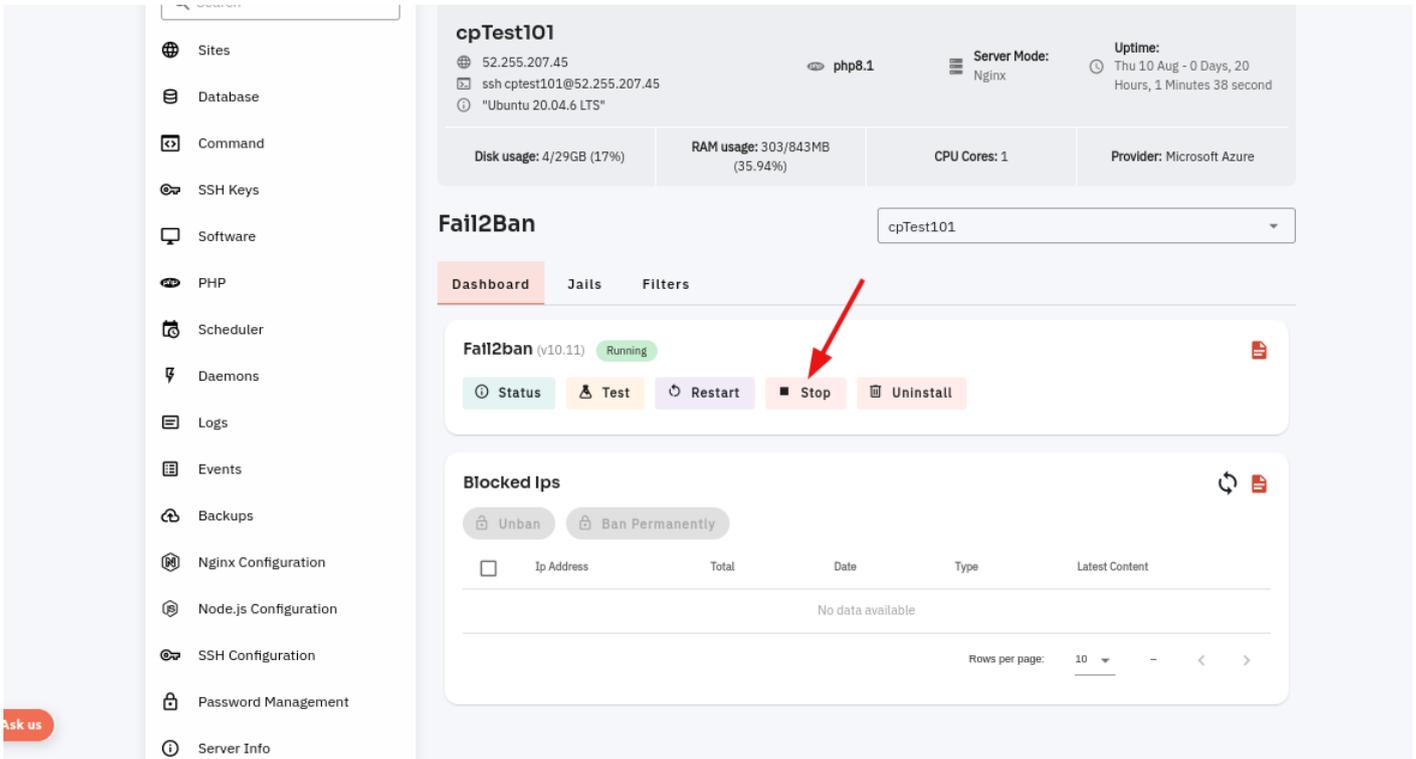
7. A dialog will open, then click on the Restart button.



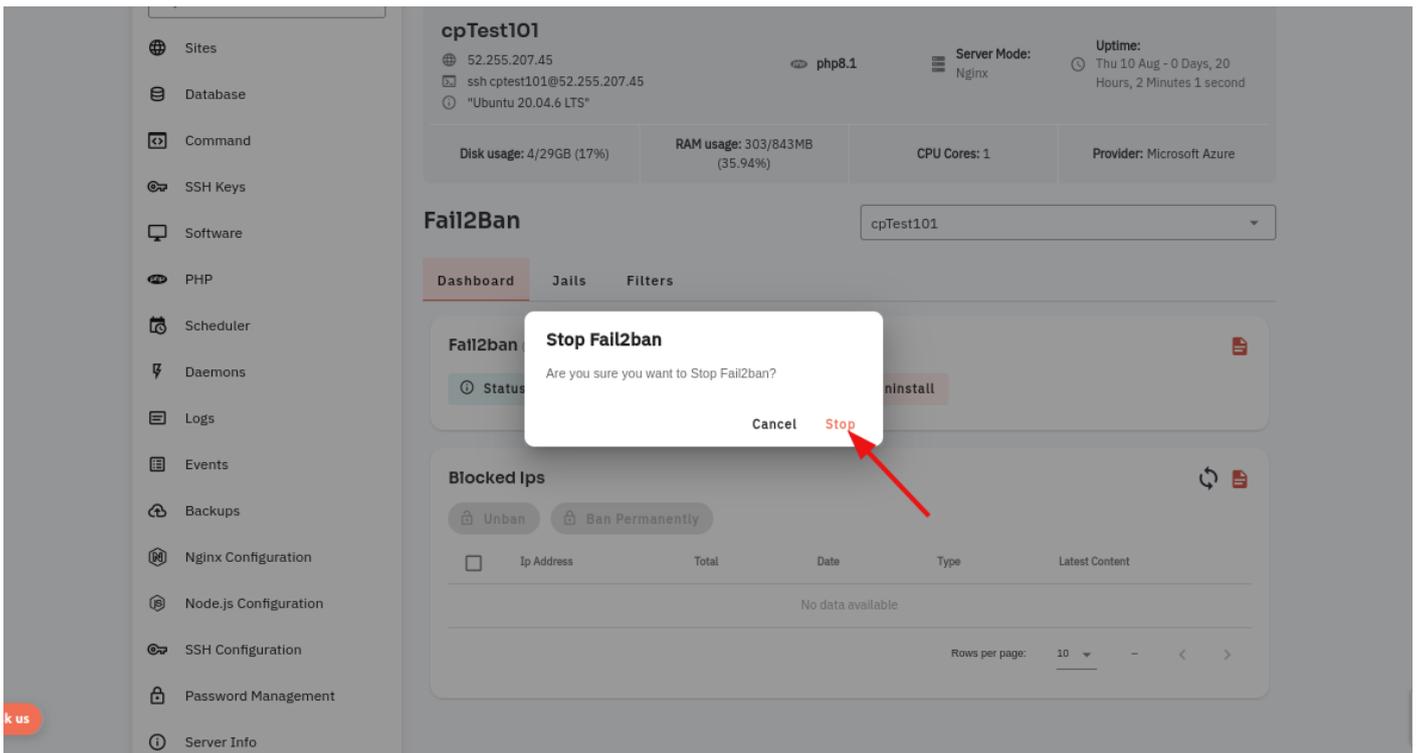
8. Here, you can see Fail2Ban restarted successfully.



9. Click on the stop button.



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



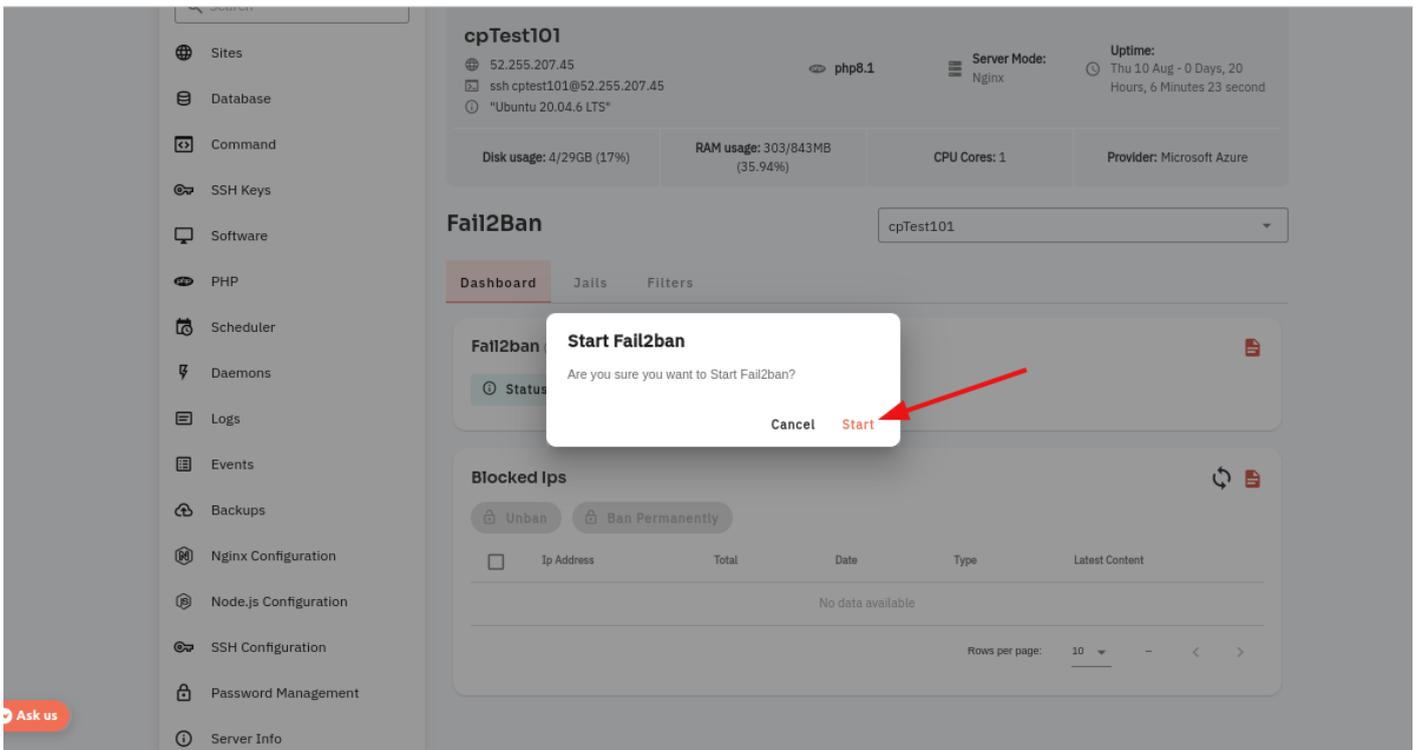
Here, you can see that Fail2Ban stopped successfully.

The screenshot shows the Fail2Ban dashboard for a server named 'cpTest101'. The server's status is 'Stopped', indicated by a red pill-shaped label. A red arrow points to the 'Start' button, which is a blue button with a play icon. Other buttons include 'Status', 'Test', and 'Uninstall'. Below the main status bar, there is a 'Blocked Ips' section with a table that currently has no data. The left sidebar contains various system management options like Sites, Database, Command, SSH Keys, Software, PHP, Scheduler, Daemons, Logs, Events, Backups, Nginx Configuration, Node.js Configuration, SSH Configuration, Password Management, and Server Info.

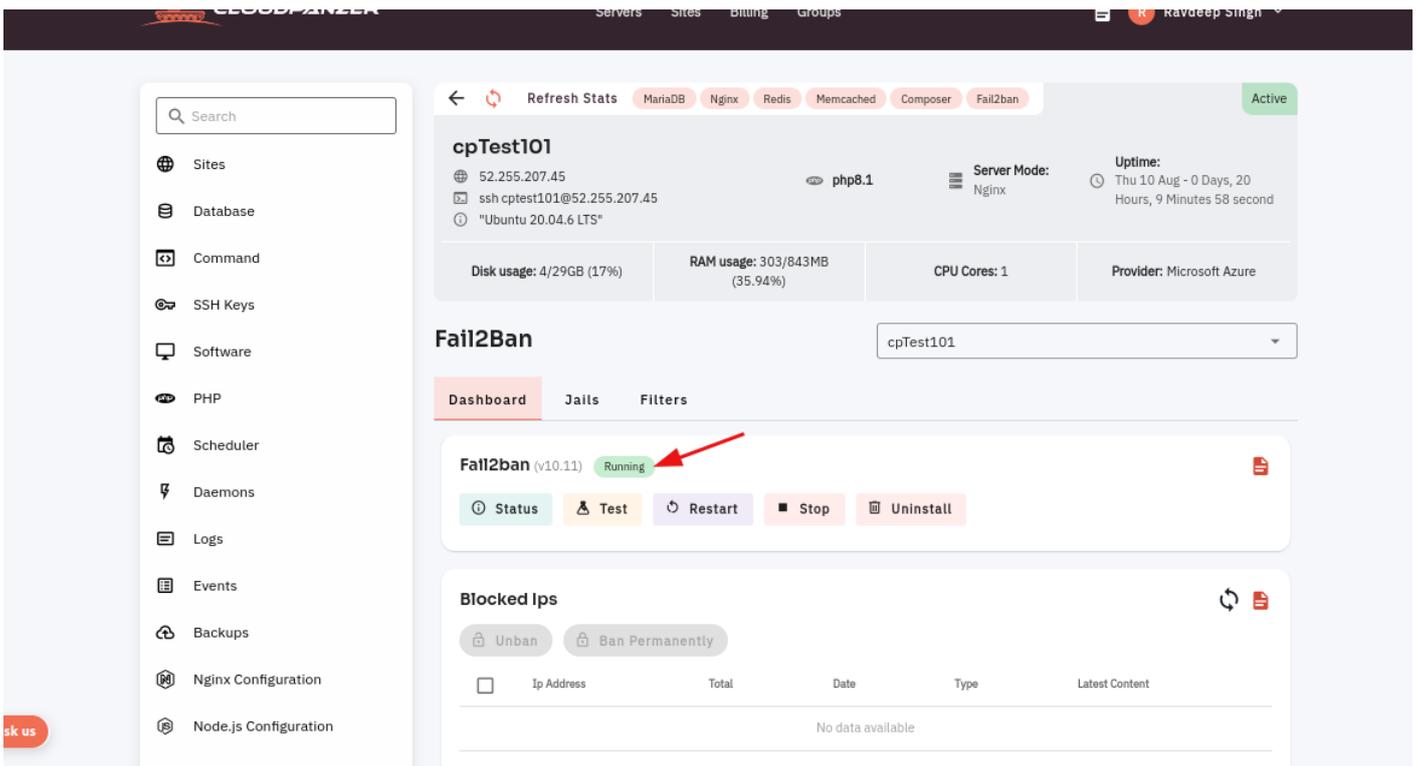
11. Click on the Start button.

This screenshot is identical to the previous one, showing the Fail2Ban dashboard. The 'Start' button is highlighted with a red arrow, indicating the next step in the process. The server status remains 'Stopped', and the 'Blocked Ips' table is empty. The interface elements and sidebar are consistent with the previous image.

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>

---

Revision #15

Created 22 June 2023 11:25:02 by Admin

Updated 9 September 2023 10:34:34 by Admin