

Server logs

- [How to check Server Apache Error logs through the cloudpanzer website?](#)
- [How to check Server Apache Access logs through the cloudpanzer website?](#)
- [How to check Server Nginx Access logs through the cloudpanzer website?](#)
- [How to check Server Nginx Error Logs through the cloudpanzer website?](#)
- [How to check Server PHP logs through the cloudpanzer website?](#)
- [How to check Redis Server Logs through the cloudpanzer website?](#)
- [How to navigate Server Logs?](#)
- [How to view SSH Auth Logs and Events on CloudPanzer?](#)
- [How to check Server Fail2ban logs through the cloudpanzer website?](#)
- [How to check Server Supervisor logs through the cloudpanzer website?](#)

How to check Serevr Apache Error logs through the cloudpanzer website?

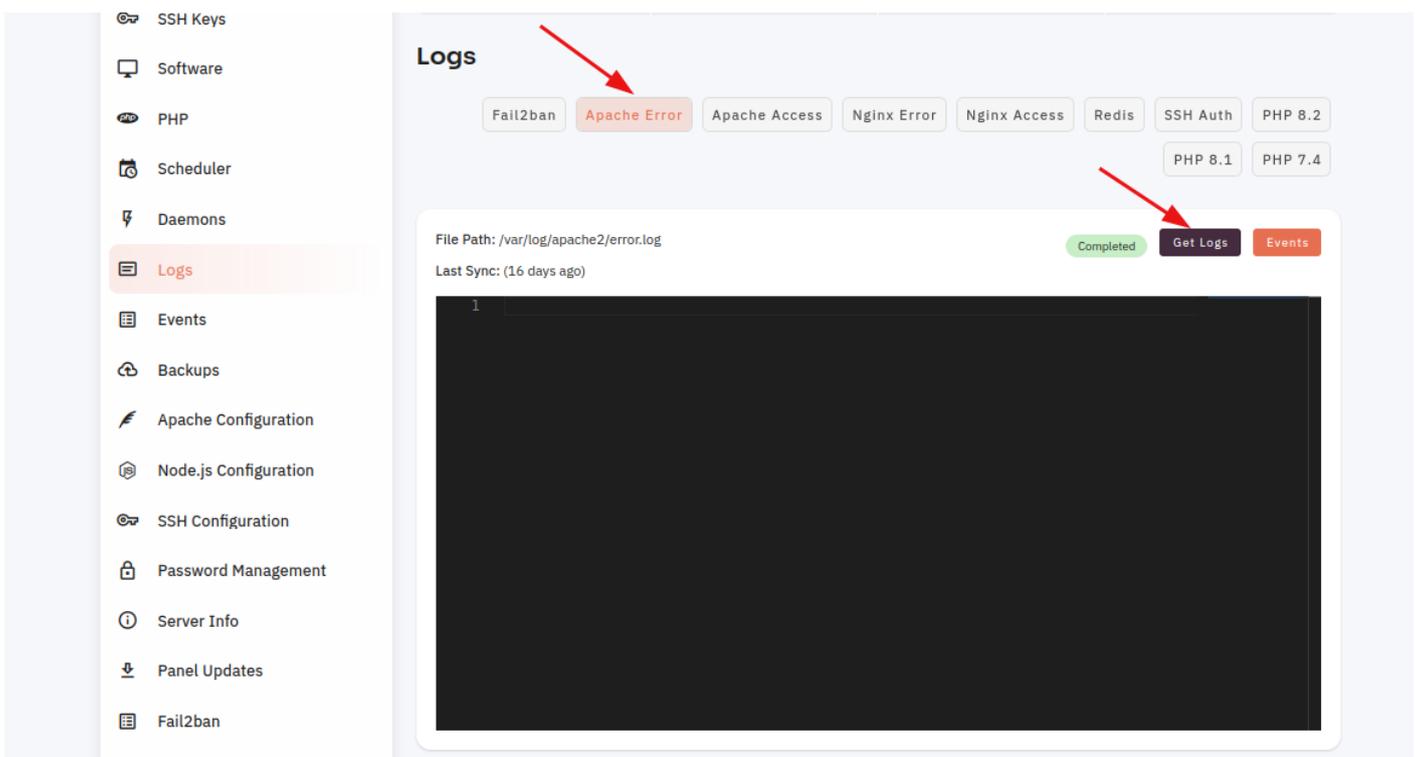
As a website owner or developer, you may encounter errors on your Apache server from time to time. Apache is one of the most widely used web servers on the internet, and its error logs contain valuable information about any issues that may be occurring on your server.

Follow the steps below to check the Apache Error in the server

Navigate to the Server Logs

(Use this link to view How to Navigate

3: Click on the Apache Error button then click on the get log button to see the logs.



The screenshot displays the Cloudpanzer website interface. On the left is a sidebar menu with various system management options. The main content area is titled "Logs" and features a row of buttons for different log types: Fail2ban, Apache Error, Apache Access, Nginx Error, Nginx Access, Redis, SSH Auth, PHP 8.2, PHP 8.1, and PHP 7.4. A red arrow points to the "Apache Error" button. Below this row, the "Apache Error" log is selected, showing the file path "/var/log/apache2/error.log" and the last sync time "(16 days ago)". A "Completed" status indicator is visible. A red arrow points to the "Get Logs" button, which is highlighted in dark purple. To the right of "Get Logs" is an "Events" button. The log content area is currently empty, showing only a line number "1" at the top.

Here, you can show the Error successfully.

The screenshot displays the CloudPanzer management interface. On the left is a sidebar menu with options: SSH Keys, Software, PHP, Scheduler, Daemons, Logs (highlighted), Events, Backups, Nginx Configuration, Apache Configuration, Password Management, Server Info, Notes, and Actions. A red arrow points from the 'Logs' menu item to the main content area. The main area shows system statistics: Disk usage: 5/29GB (20%), RAM usage: 262/906MB (28.92%), CPU Cores: 1, and Provider: Microsoft Azure. Below this is a 'Logs' section with a filter for 'Apache Error'. The log viewer shows the file path '/var/log/apache2/error.log' and a 'Last Sync: (a few seconds ago)' status. The log content includes several entries, such as 'Warning: DocumentRoot [/home/cp2SiteTesttestaccountlive/cp2sitetest.testaccount.live/public] does not exist' and 'Graceful restart requested'.

Looking for App Instructions?

Available at <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-check-apacpe-error-in-server>

How to check Server Apache Access logs through the cloudpanzer website?

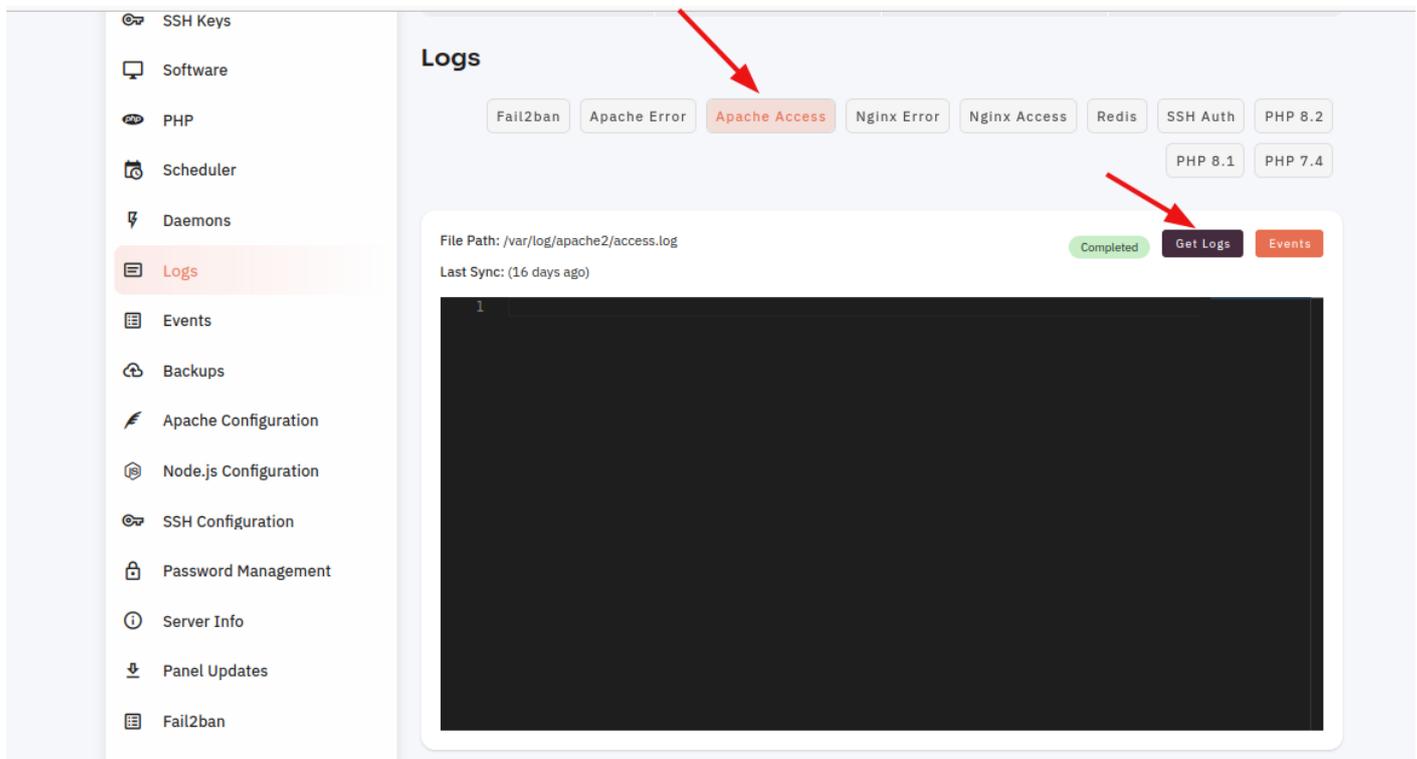
Checking the Apache access logs on your server is an important task for any website owner or developer. Apache is one of the most popular web servers on the internet, and its access logs contain valuable information about the traffic to your website.

Follow the steps below to check Apache Access logs.

Navigate to the Server Logs

(Use this link to view How to Navigate

3: Click on the Apache Access button then click on the Get Log button to see the logs.



The screenshot displays the CloudPanzer management interface. On the left is a sidebar menu with various system management options. The main area is titled 'Logs' and features a row of buttons for different log types: Fail2ban, Apache Error, Apache Access (highlighted with a red arrow), Nginx Error, Nginx Access, Redis, SSH Auth, PHP 8.2, PHP 8.1, and PHP 7.4. Below this row, the 'File Path' is shown as /var/log/apache2/access.log, and the 'Last Sync' is noted as (16 days ago). A 'Completed' status indicator is visible next to a 'Get Logs' button (highlighted with a red arrow) and an 'Events' button. The log content area below is currently empty, showing only a line number '1'.

Here, you can show the Error successfully.

The screenshot displays a web management interface with a sidebar on the left and a main content area on the right. The sidebar contains various system management options, with 'Logs' highlighted in orange. The main content area is titled 'Logs' and features a horizontal menu of log categories: Fail2ban, Apache Error, Apache Access (highlighted in orange), Nginx Error, Nginx Access, Redis, SSH Auth, PHP 8.2, PHP 8.1, and PHP 7.4. Below this menu, a card displays the file path '/var/log/apache2/access.log' and a 'Last Sync: (a few seconds ago)' message. A green 'Completed' status indicator is shown next to the file path, with a red arrow pointing to it. To the right of the status are two buttons: 'Get Logs' and 'Events'. The main content area is mostly black, suggesting a large log file or a placeholder image.

How to check Server Nginx Access logs through the cloudpanzer website?

Nginx is a popular web server that is used to host websites and serve web content to users. It is important to periodically check the access logs of Nginx to ensure that it is functioning properly and to identify any potential issues or security concerns.

Tutorial :

You can watch the Video or Continue reading the post.

https://www.youtube.com/embed/v6xCi2_xLSk

Follow the steps below to check Nginx Access

Navigate to the Logs

(Use this link to view How to Navigate

5: Click on the Nginx Error button then click on the get log button to see the logs.

Here, you can check Nginx Access logs successfully.

6 Click on the Events Button.

Scheduler/Cron
Logs
Logrotates
Events
Backups
Nginx Configuration
Node.js Configuration
Password Management
Server Info
Panel Updates
Server Updates
Notes
Actions
SSH
SSH Keys

Disk usage: 3/38GB (10%) RAM usage: 594/3820MB (15.55%) CPU Cores: 2 Provider: Hetzner

Manage Logs

Server Sites

Clean All Sync All Events

Fail2ban Logs Nginx Error **Nginx Access (8.0K)** Redis (4.0K) Ssh Auth (2.3M) Supervisor PHP 8.3 PHP 8.1

PHP 8.2

File Path: /var/log/nginx/access.log
Last Sync: (a few seconds ago)

Completed Download Clean Get Logs **Events**

Please click Get Logs to get the newest logs.

```
1 185.224.128.84 - - [13/Sep/2024:08:11:09 +0000] "GET /cgi-bin/luci/stok=/locale HTTP/1.1" 404 153 "-"
2 185.191.126.213 - - [13/Sep/2024:07:59:22 +0000] "GET / HTTP/1.1" 200 10438 "-" "-"
3 178.211.139.188 - - [13/Sep/2024:07:54:56 +0000] "GET / HTTP/1.1" 200 2287 "-" "Mozilla/5.0 (Windows
4 134.209.207.251 - - [13/Sep/2024:06:59:26 +0000] "GET / HTTP/1.1" 200 2287 "-" "Mozilla/5.0 (Windows
5 178.62.229.24 - - [13/Sep/2024:06:50:49 +0000] "GET / HTTP/1.1" 200 2287 "-" "Mozilla/5.0 (Windows
6 185.224.128.83 - - [13/Sep/2024:06:19:24 +0000] "GET /cgi-bin/luci/stok=/locale HTTP/1.1" 404 153 "-"
7 149.50.103.48 - - [13/Sep/2024:06:03:19 +0000] "GET / HTTP/1.1" 200 10438 "-" "-"
8 136.244.119.115 - - [13/Sep/2024:05:53:16 +0000] "POST / HTTP/1.1" 405 559 "-" "Mozilla/5.0 (X11; Li
9 136.244.119.115 - - [13/Sep/2024:05:53:16 +0000] "GET /env HTTP/1.1" 404 185 "-" "Mozilla/5.0 (X11
10 89.190.156.137 - - [13/Sep/2024:05:32:33 +0000] "GET / HTTP/1.0" 200 10438 "-" "ivire-masscan/1.3 h
11 45.148.10.242 - - [13/Sep/2024:05:29:31 +0000] "GET /cgi-bin/luci/stok=/locale HTTP/1.1" 404 153 "-"
12 109.74.200.218 - - [13/Sep/2024:05:24:11 +0000] "\x16\x03\x01\x00\xFC\x01\x00\x00\xF8\x03\x03\x
13 109.74.200.218 - - [13/Sep/2024:05:24:11 +0000] "\x16\x03\x01\x00\xFC\x01\x00\x00\xF8\x03\x03\x
```

7. Click on the Eye Icon.

Scheduler/Cron
Logs
Logrotates
Events
Backups
Nginx Configuration
Node.js Configuration
Password Management
Server Info
Panel Updates
Server Updates
Notes
Actions
SSH
SSH Keys

Disk usage: 3/38GB (10%) RAM usage: 594/3820MB (15.55%) CPU Cores: 2 Provider: Hetzner

Manage Logs

Server Sites

Clean All Sync All Events

Fail2ban Logs Nginx Error **Nginx Access (8.0K)** Redis (4.0K) Ssh Auth (2.3M) Supervisor PHP 8.3 PHP 8.1

PHP 8.2

File Path: /var/log/nginx/access.log
Last Sync: (a few seconds ago)

Completed Download Clean Get Logs Events

Please click Get Logs to get the newest logs.

```
1 185.224.128.84 - - [13/Sep/2024:08:11:09 +0000] "GET /cgi-bin/luci/stok=/locale HTTP/1.1" 404 153 "-"
2 185.191.126.213 - - [13/Sep/2024:07:59:22 +0000] "GET / HTTP/1.1" 200 10438 "-" "-"
3 178.211.139.188 - - [13/Sep/2024:07:54:56 +0000] "GET / HTTP/1.1" 200 2287 "-" "Mozilla/5.0 (Windows
4 134.209.207.251 - - [13/Sep/2024:06:59:26 +0000] "GET / HTTP/1.1" 200 2287 "-" "Mozilla/5.0 (Windows
5 178.62.229.24 - - [13/Sep/2024:06:50:49 +0000] "GET / HTTP/1.1" 200 2287 "-" "Mozilla/5.0 (Windows
6 185.224.128.83 - - [13/Sep/2024:06:19:24 +0000] "GET /cgi-bin/luci/stok=/locale HTTP/1.1" 404 153 "-"
7 149.50.103.48 - - [13/Sep/2024:06:03:19 +0000] "GET / HTTP/1.1" 200 10438 "-" "-"
8 136.244.119.115 - - [13/Sep/2024:05:53:16 +0000] "POST / HTTP/1.1" 405 559 "-" "Mozilla/5.0 (X11; Li
9 136.244.119.115 - - [13/Sep/2024:05:53:16 +0000] "GET /env HTTP/1.1" 404 185 "-" "Mozilla/5.0 (X11
10 89.190.156.137 - - [13/Sep/2024:05:32:33 +0000] "GET / HTTP/1.0" 200 10438 "-" "ivire-masscan/1.3 h
11 45.148.10.242 - - [13/Sep/2024:05:29:31 +0000] "GET /cgi-bin/luci/stok=/locale HTTP/1.1" 404 153 "-"
12 109.74.200.218 - - [13/Sep/2024:05:24:11 +0000] "\x16\x03\x01\x00\xFC\x01\x00\x00\xF8\x03\x03\x
13 109.74.200.218 - - [13/Sep/2024:05:24:11 +0000] "\x16\x03\x01\x00\xFC\x01\x00\x00\xF8\x03\x03\x
```

Events

Search by event

Event	User	Device	When	Actions
SERVER upserver sync Log Nginx Access	demo	Firefox	Fri, Sep 13, 2024 - 1:42:05 pm	

Rows per page: 50 1-1 of 1

8. Click on the file icon.

Looking for Mobile Instructions?

Available at <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-checks-nginx-access>

How to check Server Nginx Error Logs through the cloudpanzer website?

If you are running a web server using Nginx, it is important to regularly check the error logs to troubleshoot any issues that may arise.

Tutorial :

You can watch the Video or Continue reading the post.

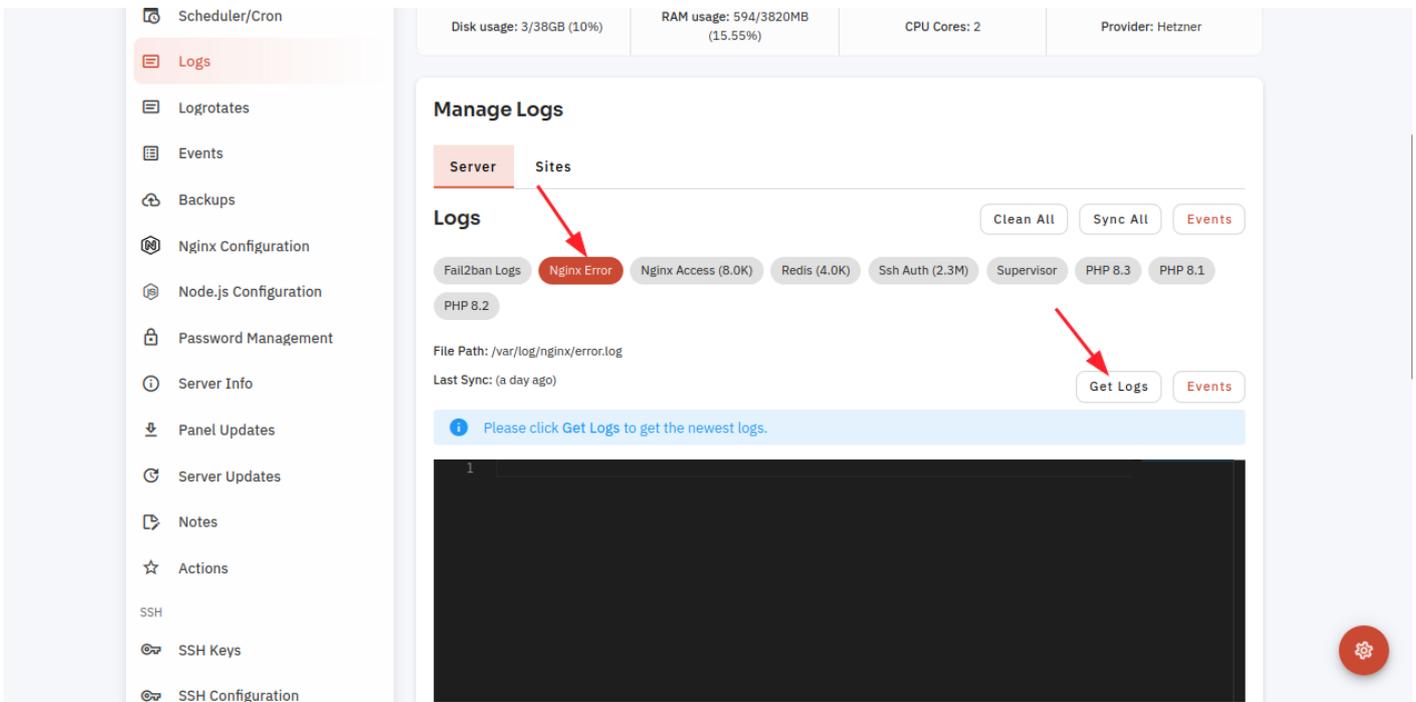
<https://www.youtube.com/embed/-aOrQjilDpE>

Follow the steps below to check the Nginx Error Logs

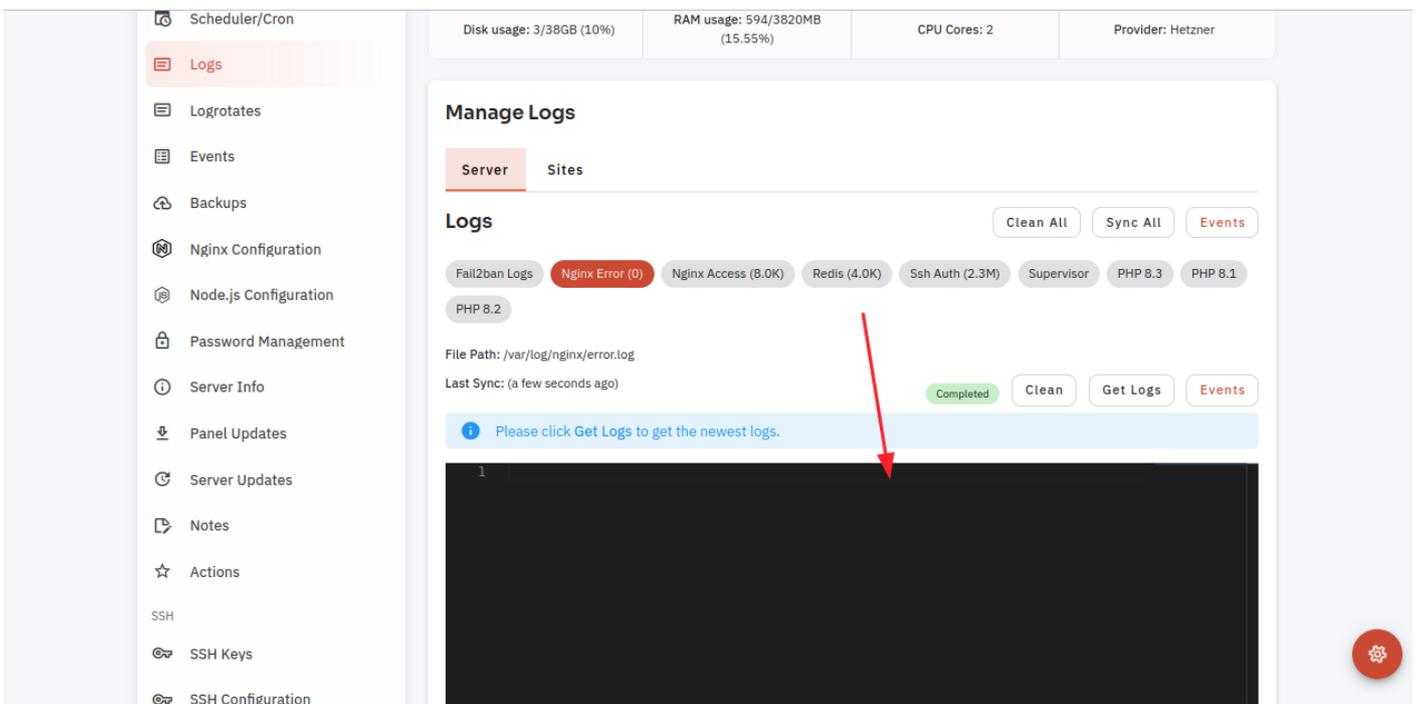
Navigate to the Logs

(Use this link to view How to Navigate

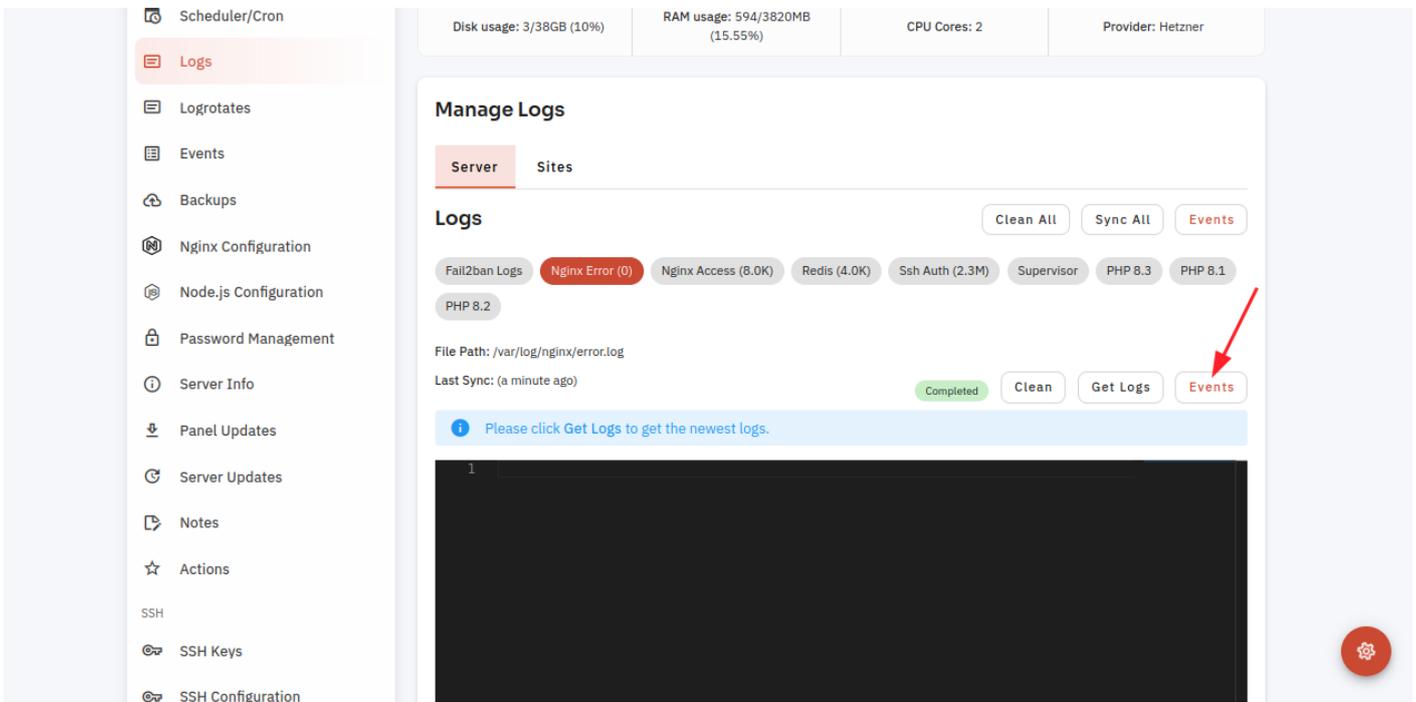
3: Click on the Nginx Error button then click on the get log button to see the logs.



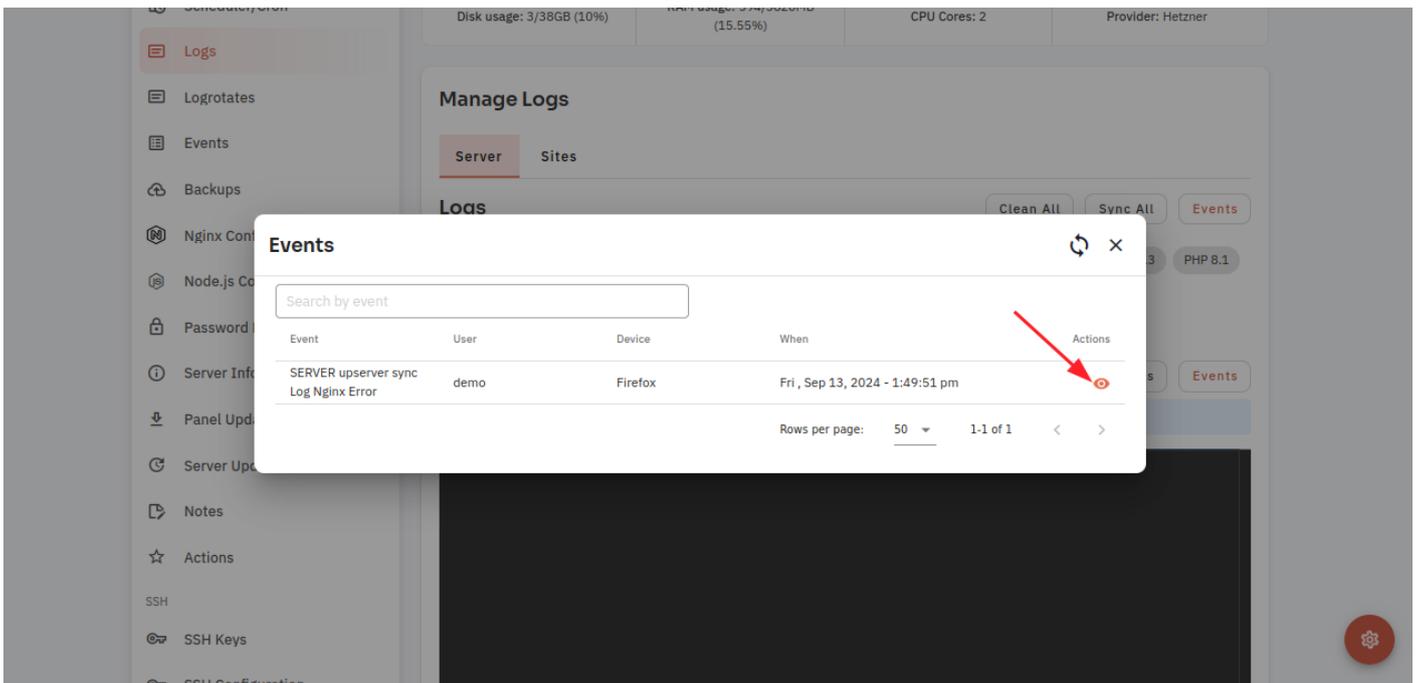
Here, you can see the Error data.



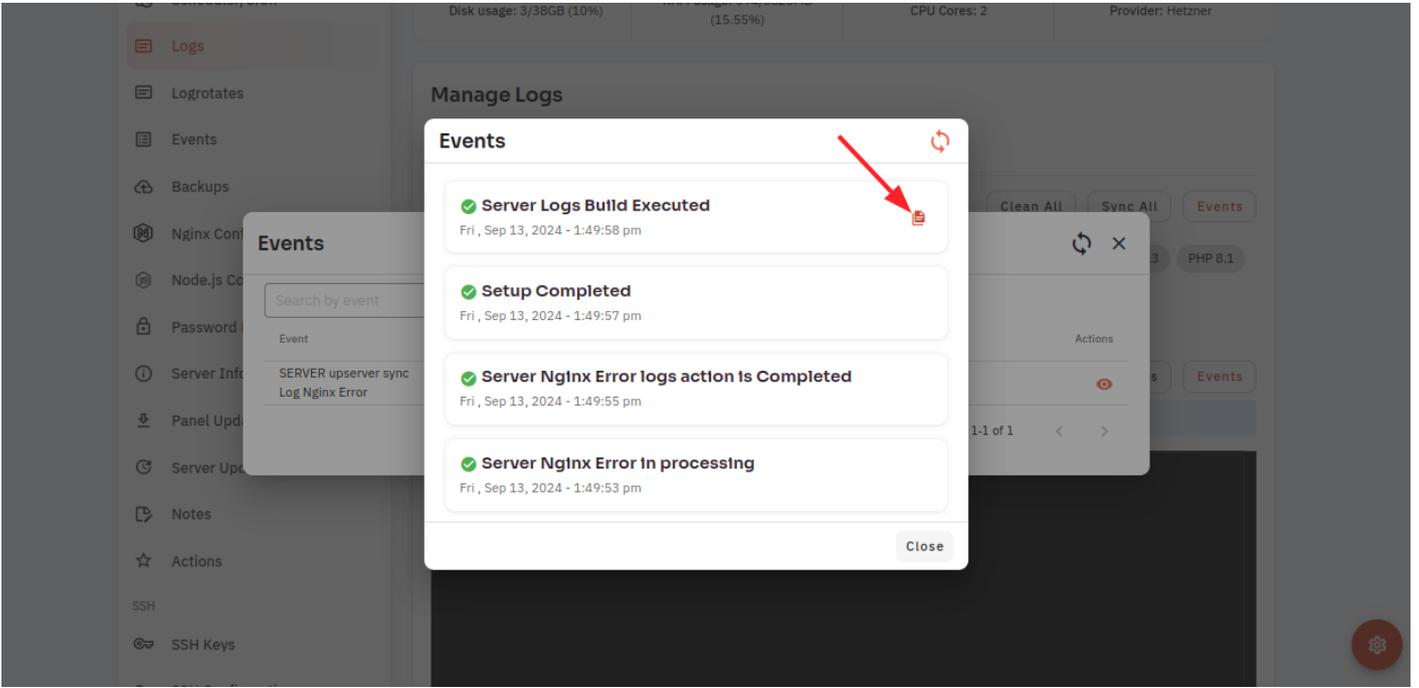
6 Click on the Events Button.



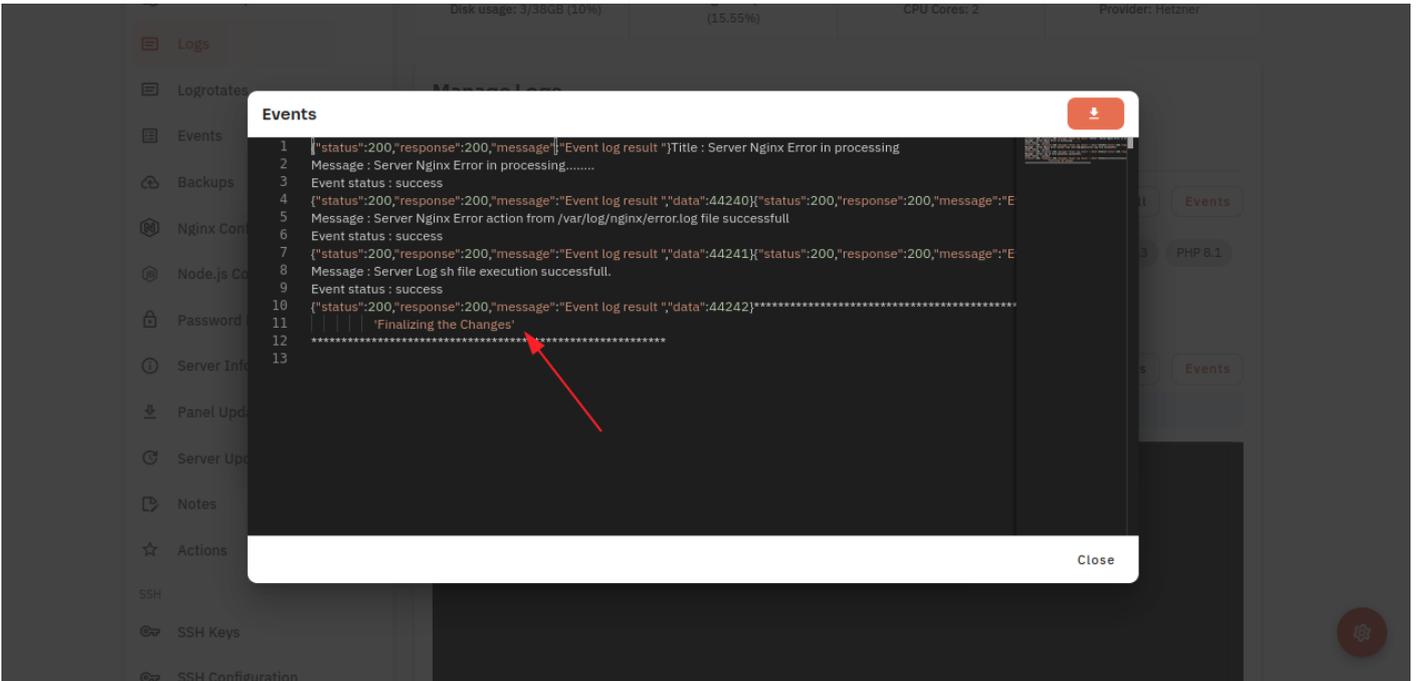
7. Click on the Eye Icon.



8. Click on the file icon.



Here, you can see the event data.



Looking for Mobile App Instructions?

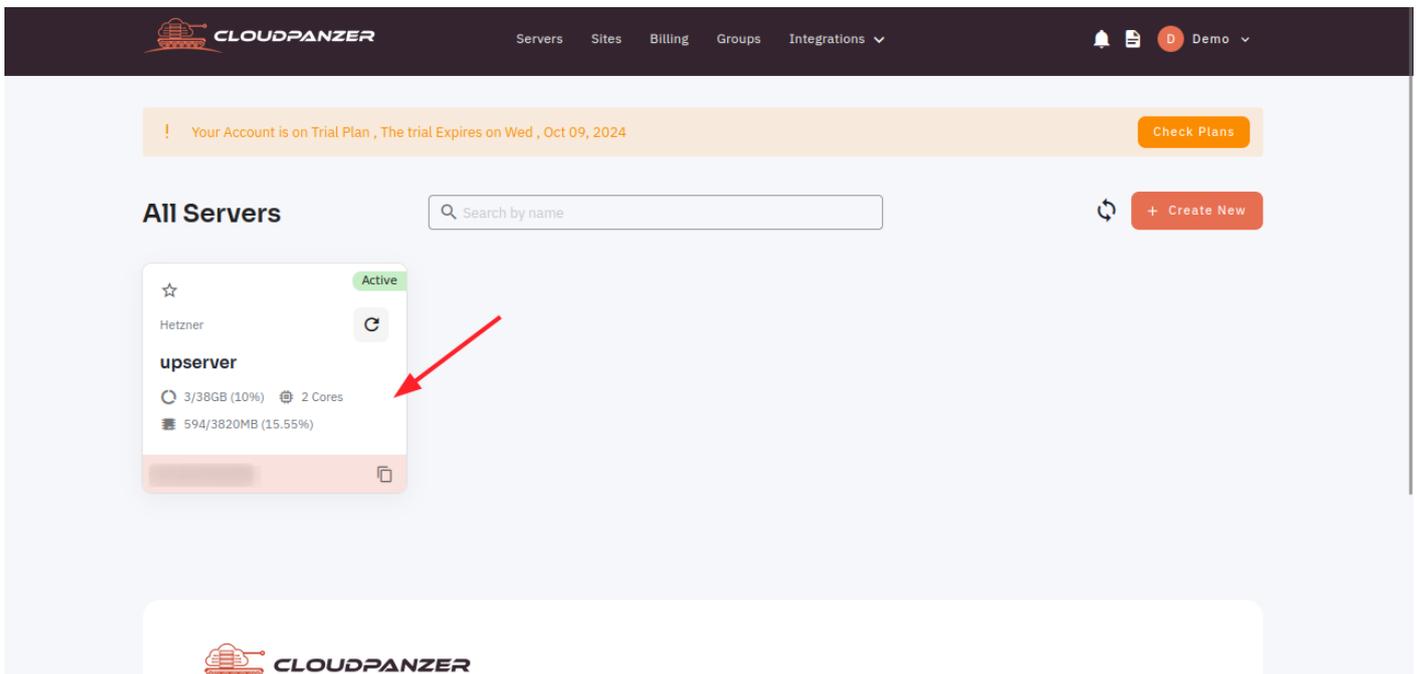
Available at <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-check-nginx-error-logs>

How to check Server PHP logs through the cloudpanzer we ?

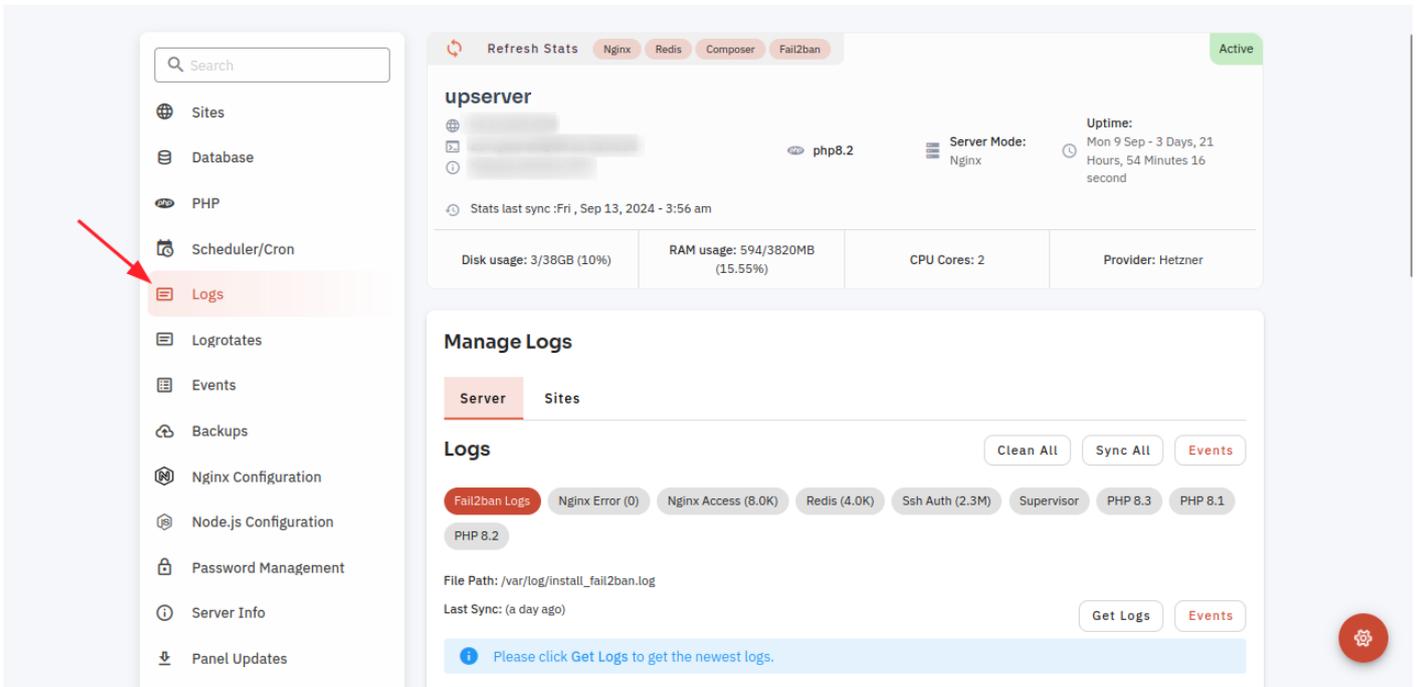
PHP is a popular server-side scripting language that is widely used for creating dynamic web applications. It is essential to keep track of errors and other important events that occur during the execution of a PHP script. This can be done using PHP logs, which provide a record of all the errors and other events that occur during the execution of a PHP script.

Follow the steps below to check the PHP logs server

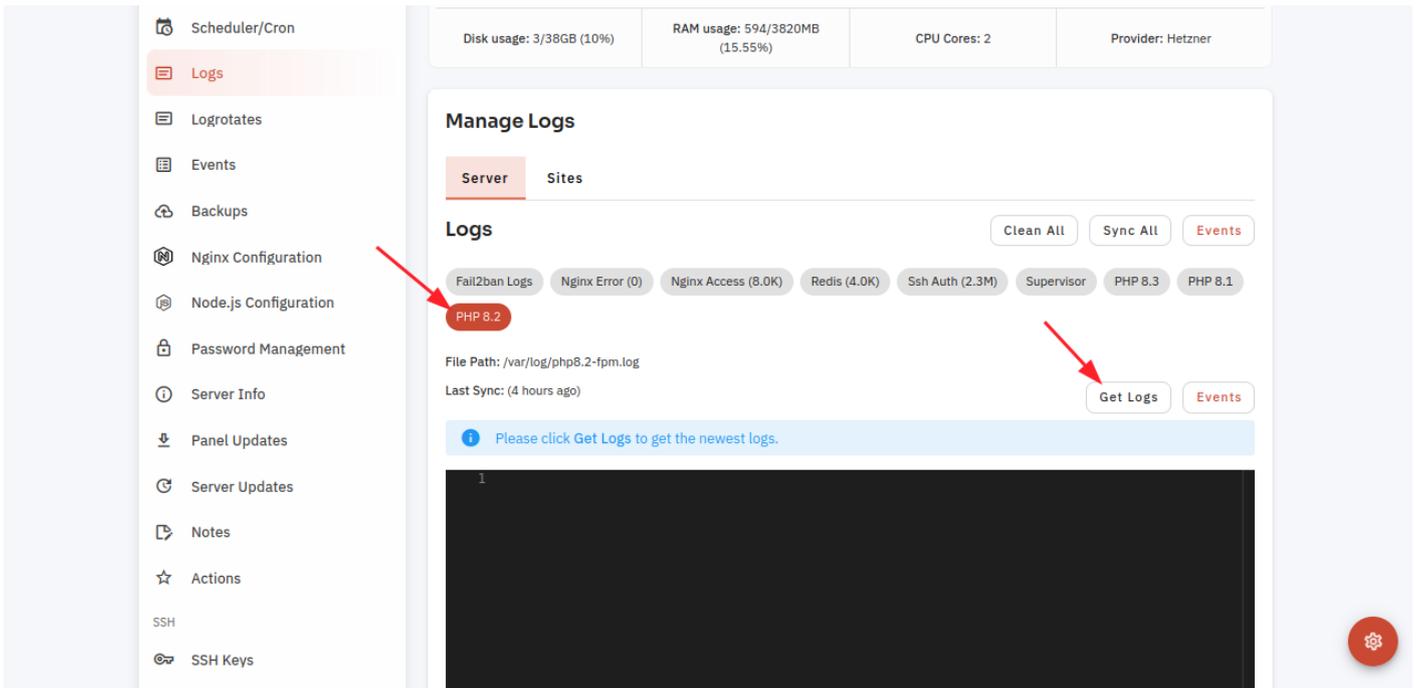
1: Firstly you are logged in, look for a "Server" and click on it.



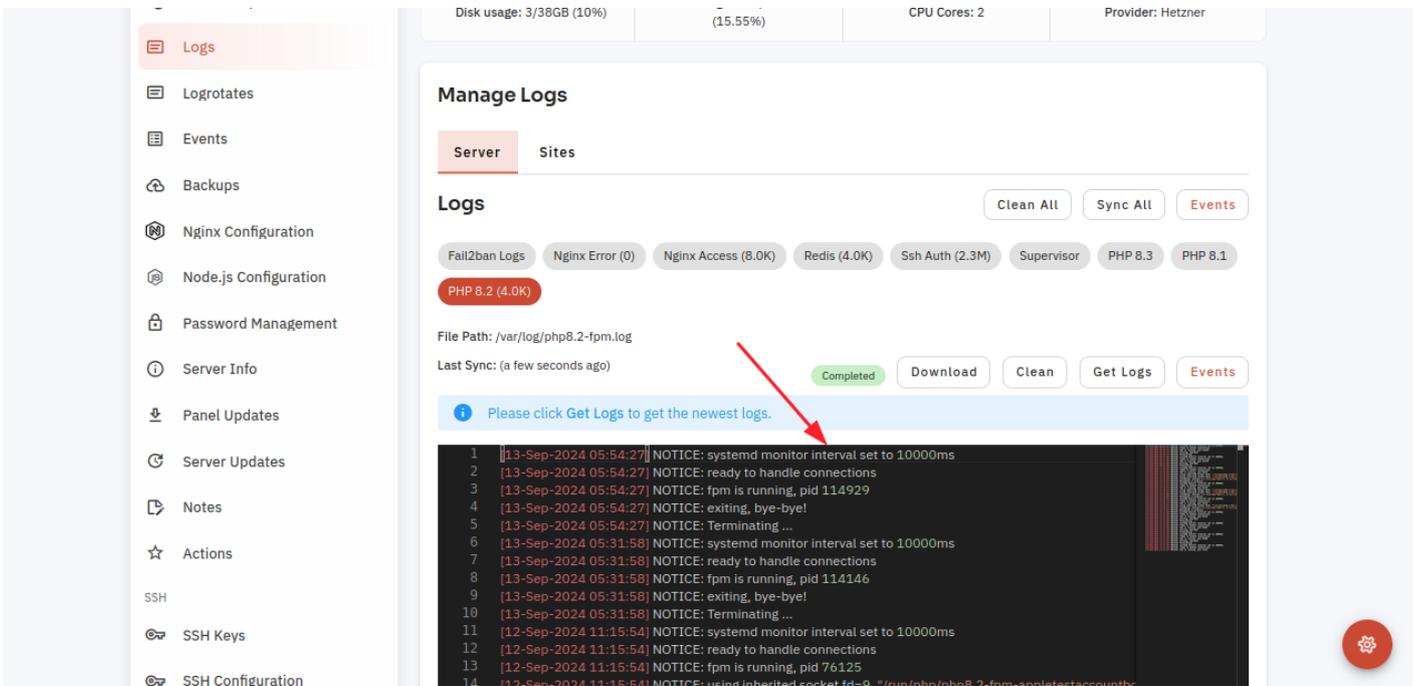
2. Click on the Logs option.



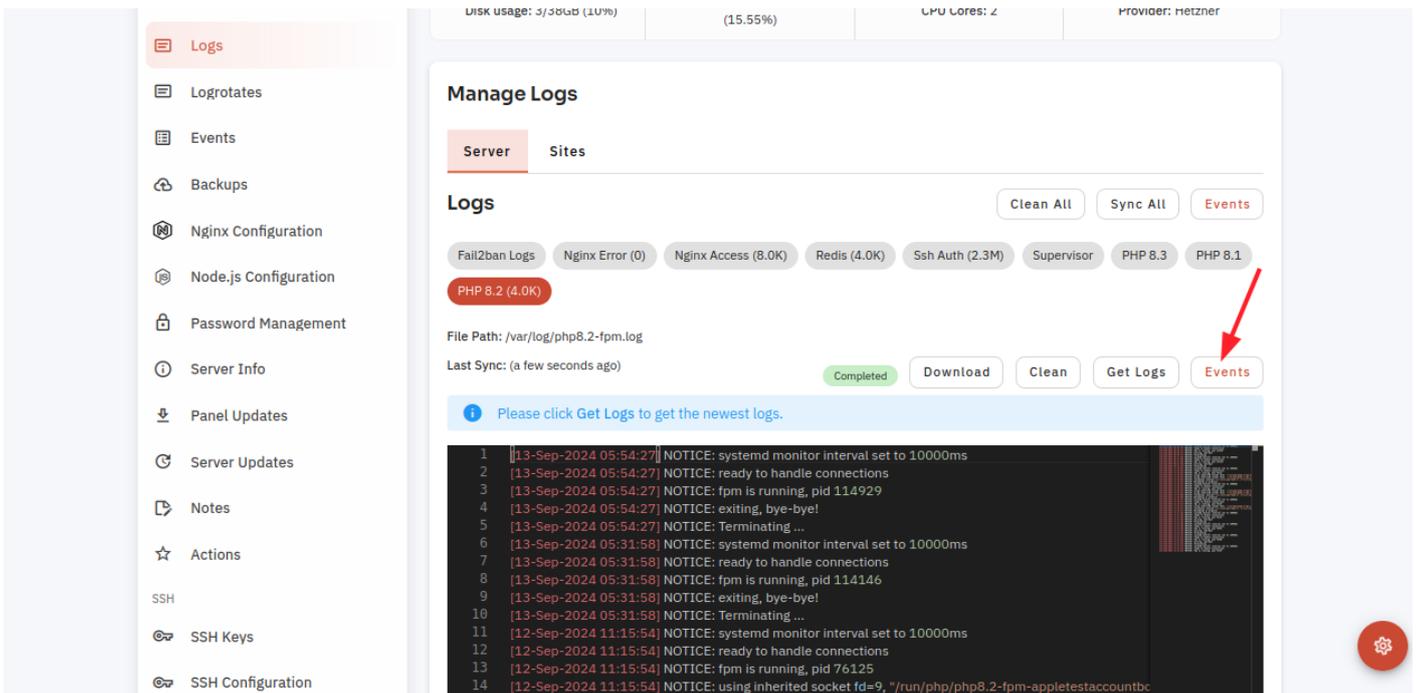
3: Click on the Nginx Error button then click on the get log button to see the logs.



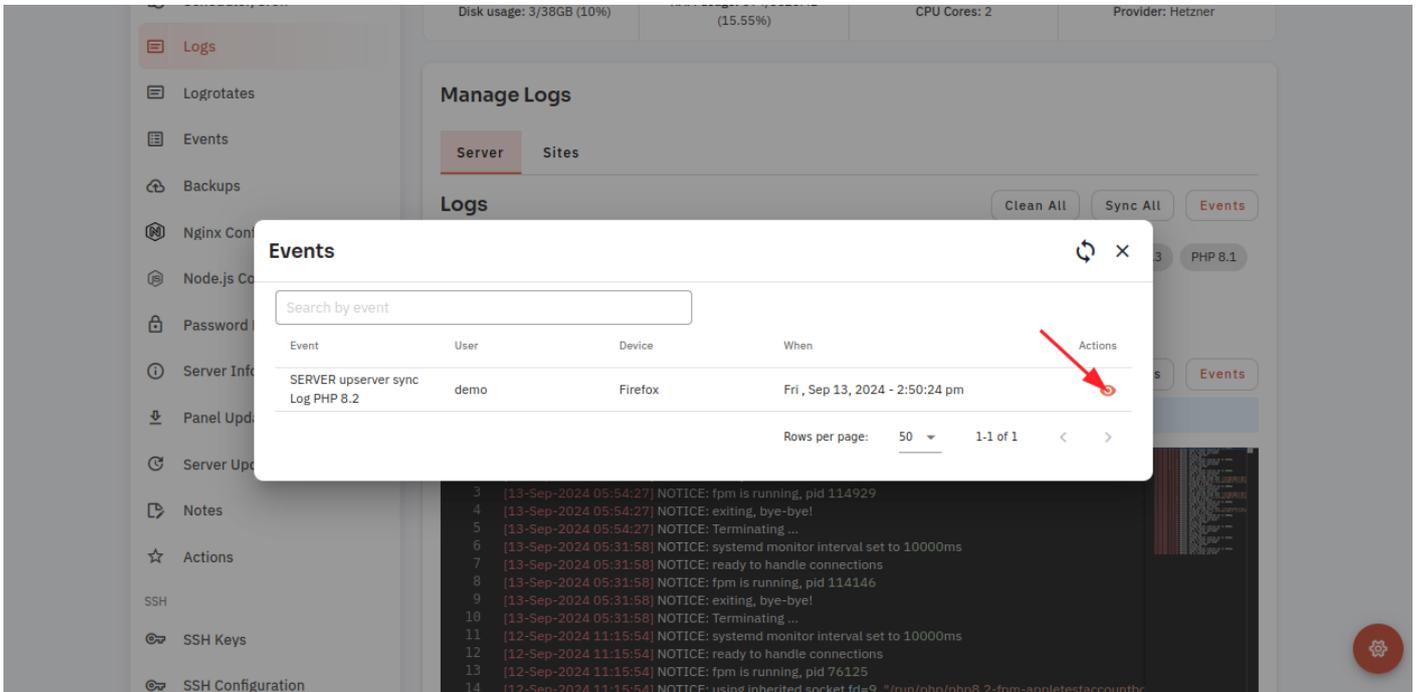
Here, you can see PHP Version Logs data.



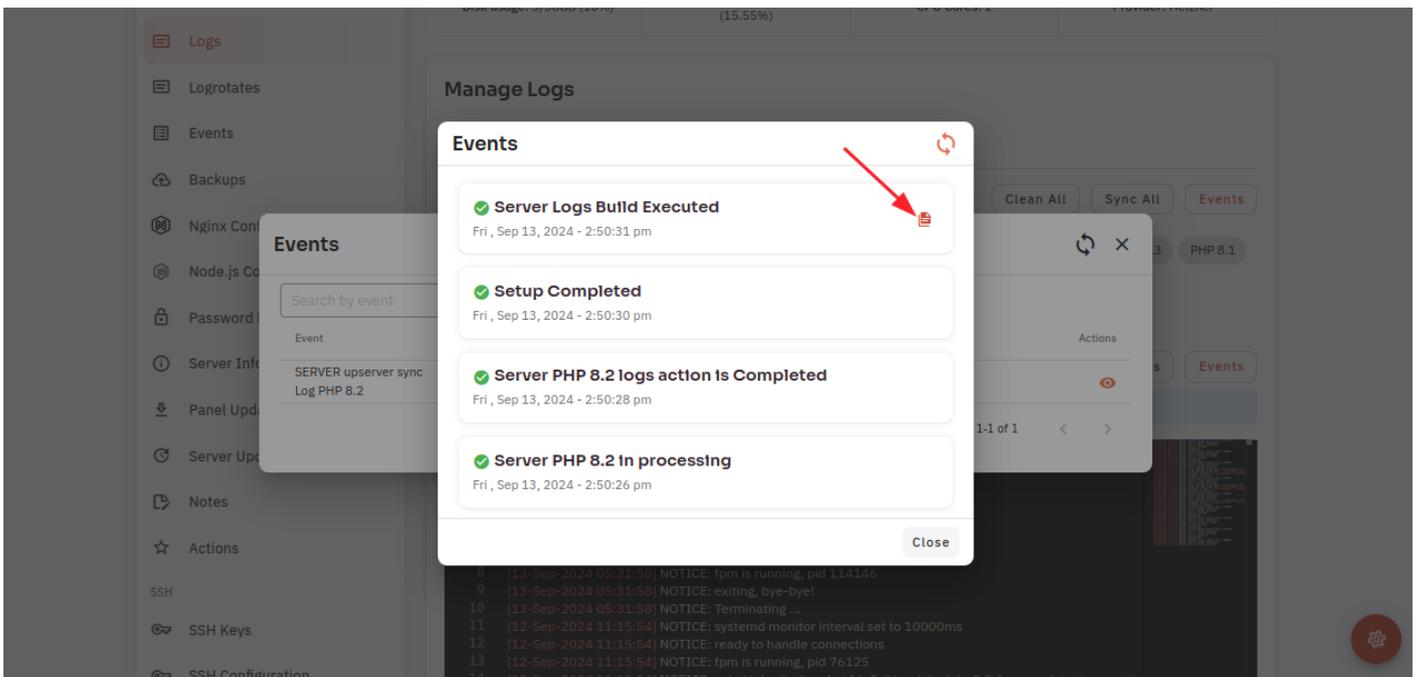
4. Click on the Events Button.



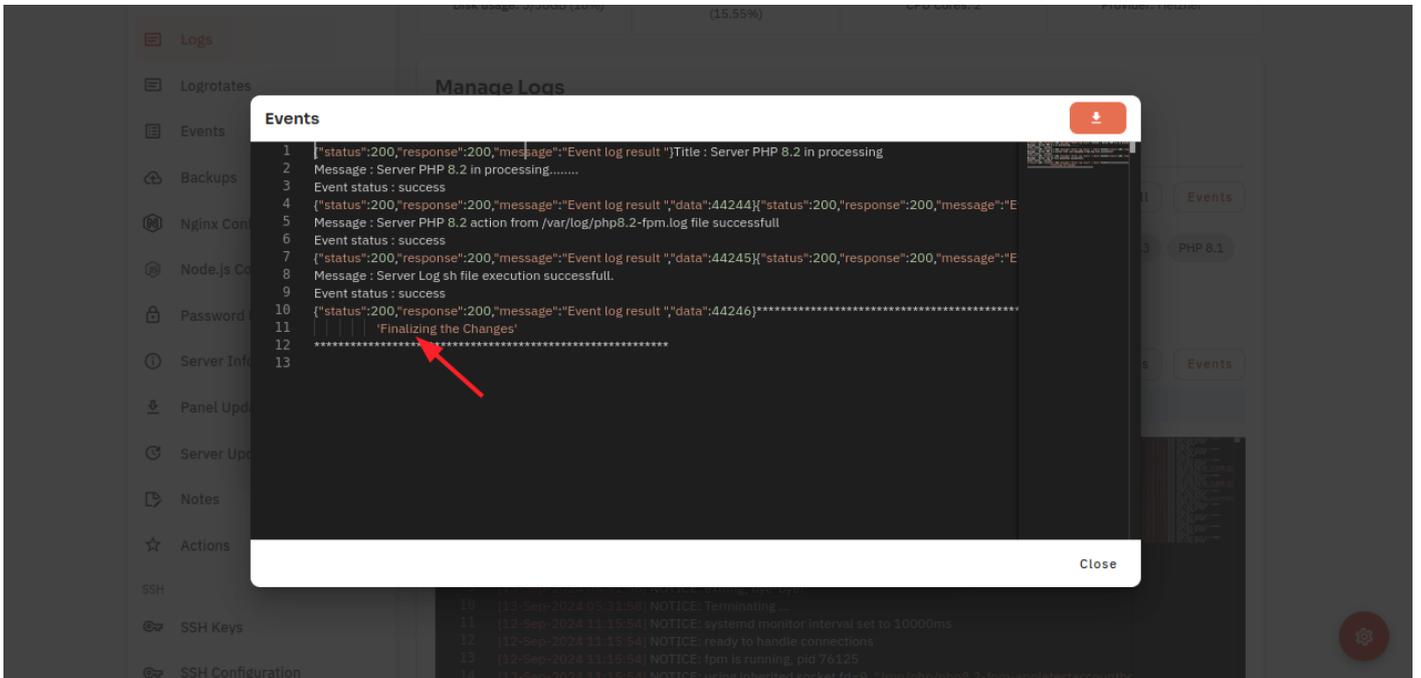
7. Click on the Eye Icon.



8. Click on the file icon.



Here, you can see the event data.



Looking for Mobile App Instructions?

Available at <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-checks-php-logs-in-server>

How to checks Redis Server Logs through the cloudpanzer website?

Redis is a popular in-memory data structure store that is often used as a database, cache, and message broker. It can be useful to check the logs of a Redis server to troubleshoot issues or monitor its performance.

Prerequisites :

You must have an Active Server. You can jump to the tutorial section if the above conditions are proper, Or first follow the links below to set up the prerequisites.

How to install a Server

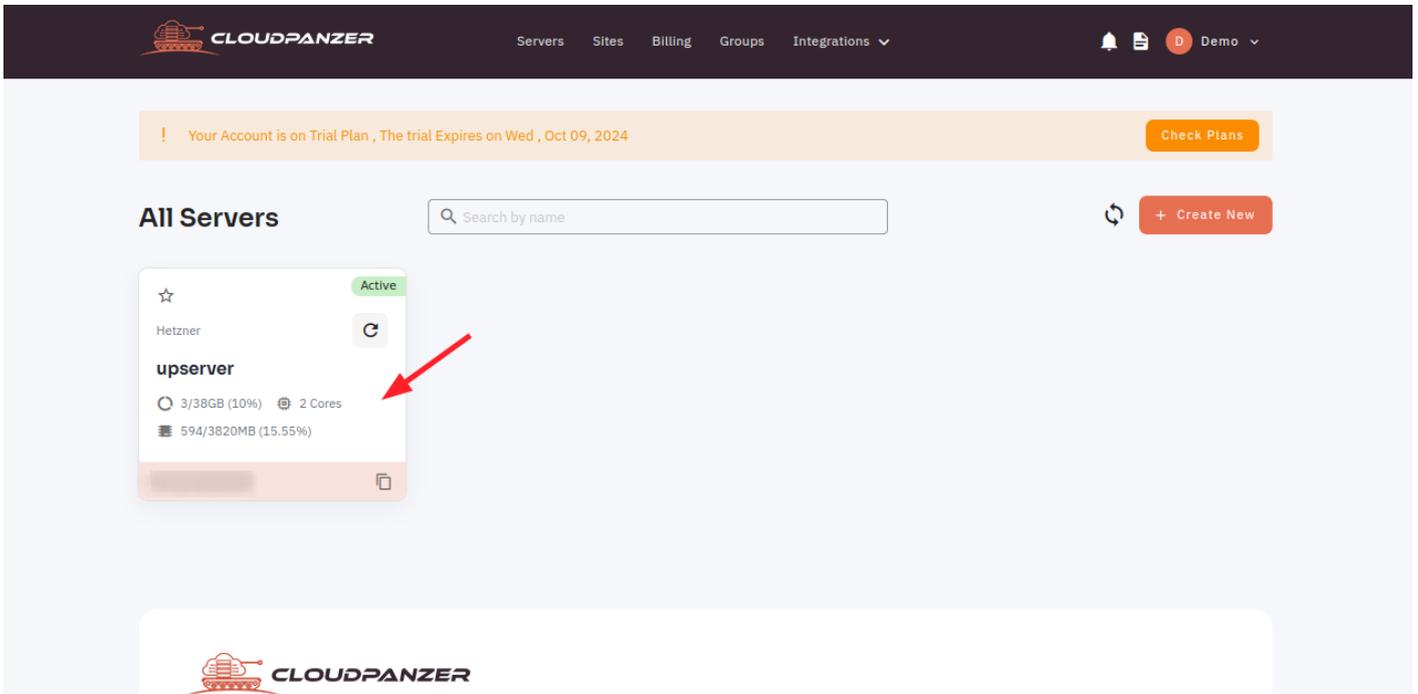
Tutorial :

You can watch the Video or Continue reading the post.

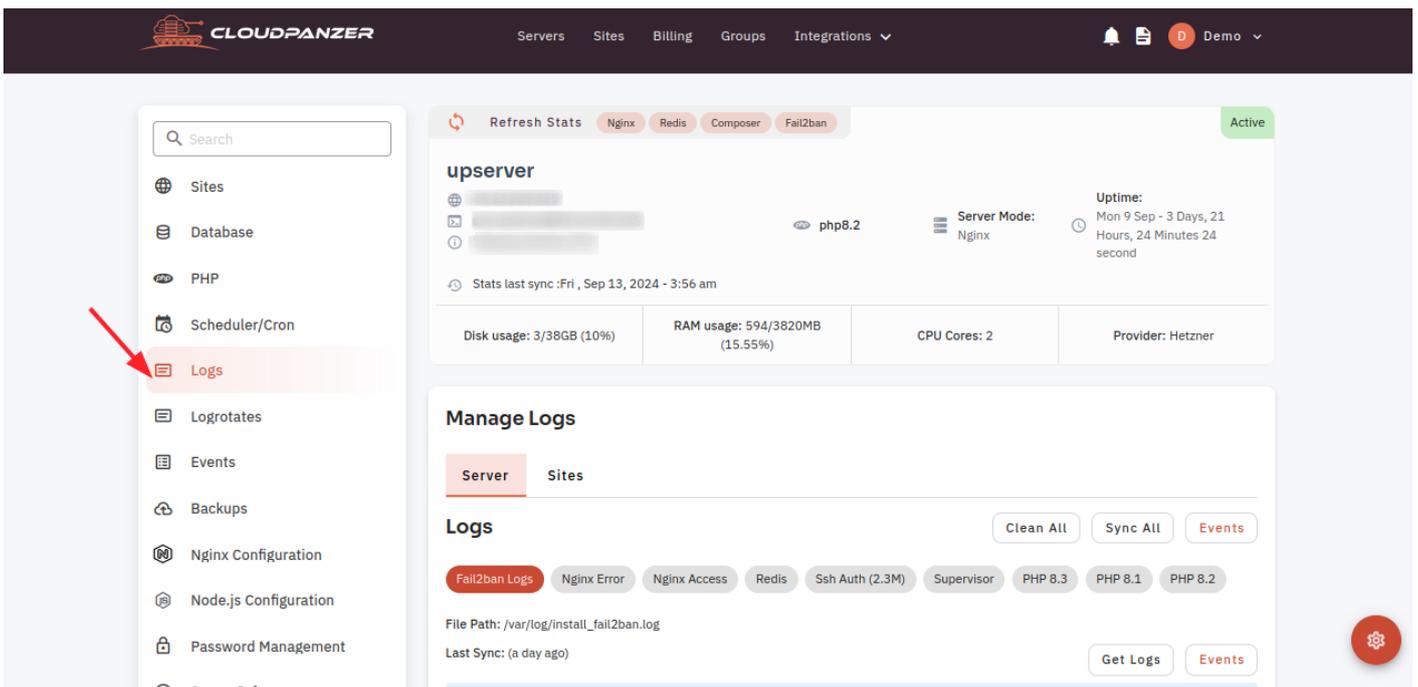
<https://www.youtube.com/embed/yqfqAKA3ArE>

Follow the steps below to check the Redis Logs.

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



2. Select the Logs Option.



3. Click on the Redis button and the Get Log Button.

Scheduler/Cron

Logs

Logrotates

Events

Backups

Nginx Configuration

Node.js Configuration

Password Management

Server Info

Panel Updates

Server Updates

Notes

Actions

SSH

SSH Keys

SSH Configuration

Disk usage: 3/38GB (10%)

RAM usage: 594/3820MB (15.55%)

CPU Cores: 2

Provider: Hetzner

Manage Logs

Server Sites

Logs

Clean All Sync All Events

Fail2ban Logs Nginx Error Nginx Access **Redis** Ssh Auth (2.3M) Supervisor PHP 8.3 PHP 8.1 PHP 8.2

File Path: /var/log/redis/redis-server.log

Last Sync: (a day ago)

Get Logs Events

Please click Get Logs to get the newest logs.

Here, you can see Redis Logs data.

Disk usage: 3/38GB (10%)

(15.55%)

CPU Cores: 2

Provider: Hetzner

Manage Logs

Server Sites

Logs

Clean All Sync All Events

Fail2ban Logs Nginx Error Nginx Access **Redis (4.0K)** Ssh Auth (2.3M) Supervisor PHP 8.3 PHP 8.1

PHP 8.2

File Path: /var/log/redis/redis-server.log

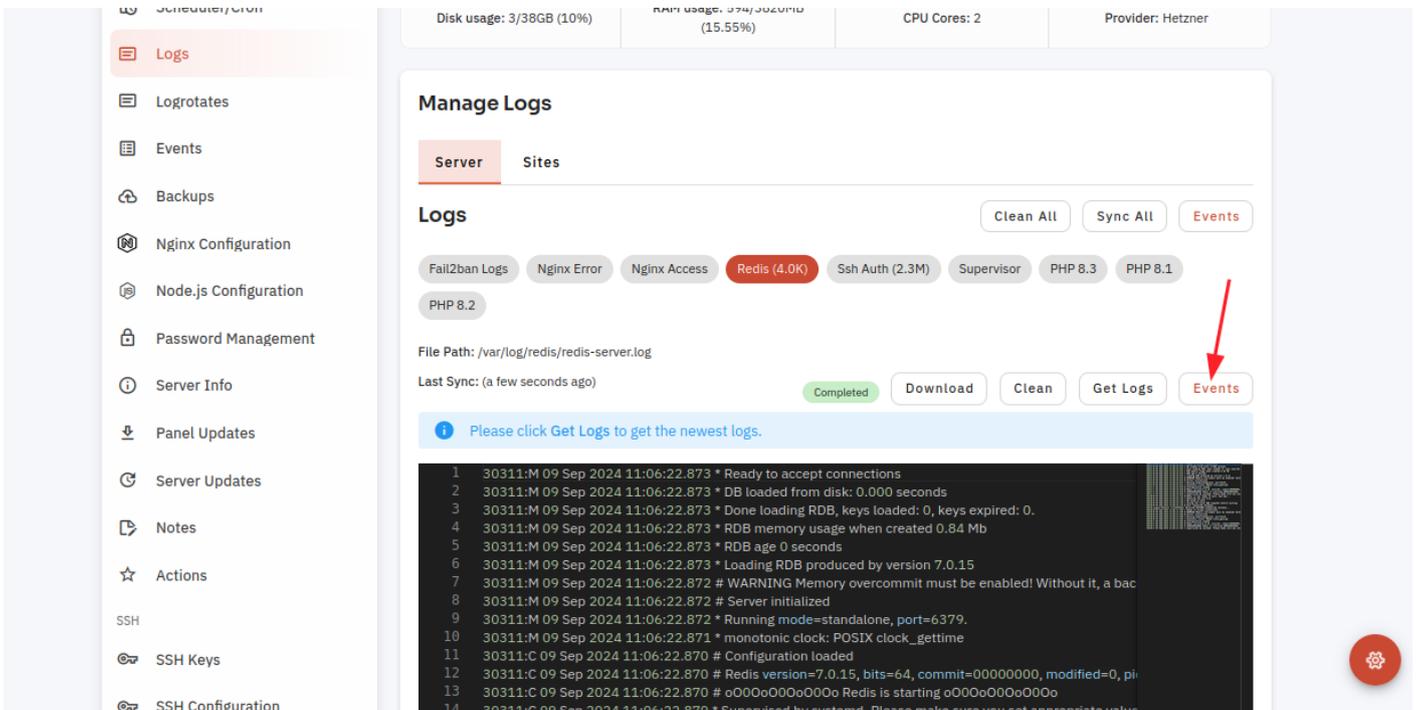
Last Sync: (a few seconds ago)

Completed Download Clean Get Logs Events

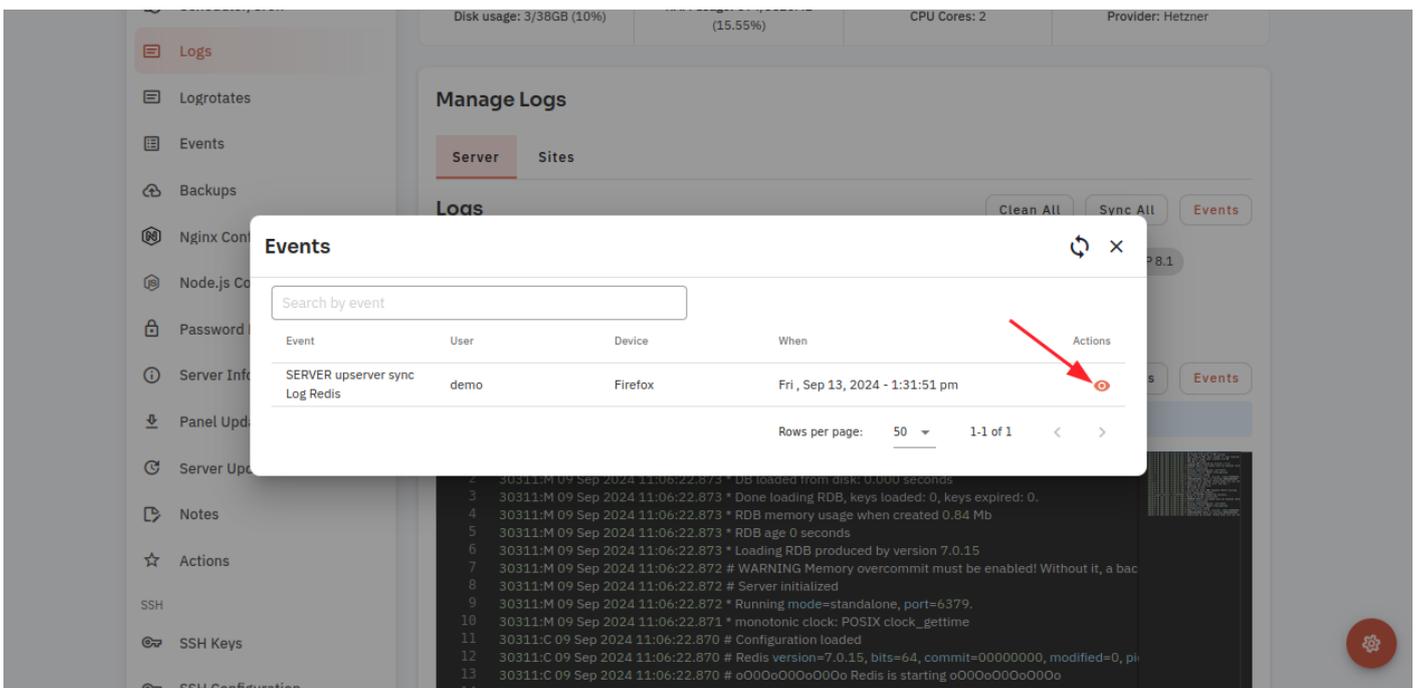
Please click Get Logs to get the newest logs.

```
1 30311:M 09 Sep 2024 11:06:22.873 * Ready to accept connections
2 30311:M 09 Sep 2024 11:06:22.873 * DB loaded from disk: 0.000 seconds
3 30311:M 09 Sep 2024 11:06:22.873 * Done loading RDB, keys loaded: 0, keys expired: 0.
4 30311:M 09 Sep 2024 11:06:22.873 * RDB memory usage when created 0.84 Mb
5 30311:M 09 Sep 2024 11:06:22.873 * RDB age 0 seconds
6 30311:M 09 Sep 2024 11:06:22.873 * Loading RDB produced by version 7.0.15
7 30311:M 09 Sep 2024 11:06:22.872 # WARNING Memory overcommit must be enabled! Without it, a bac
8 30311:M 09 Sep 2024 11:06:22.872 # Server initialized
9 30311:M 09 Sep 2024 11:06:22.872 * Running mode=standalone, port=6379.
10 30311:M 09 Sep 2024 11:06:22.871 * monotonic clock: POSIX clock_gettime
11 30311:C 09 Sep 2024 11:06:22.870 # Configuration loaded
12 30311:C 09 Sep 2024 11:06:22.870 # Redis version=7.0.15, bits=64, commit=00000000, modified=0, pi
13 30311:C 09 Sep 2024 11:06:22.870 # oOoOoOoOoOoOo Redis is starting oOoOoOoOoOoOo
```

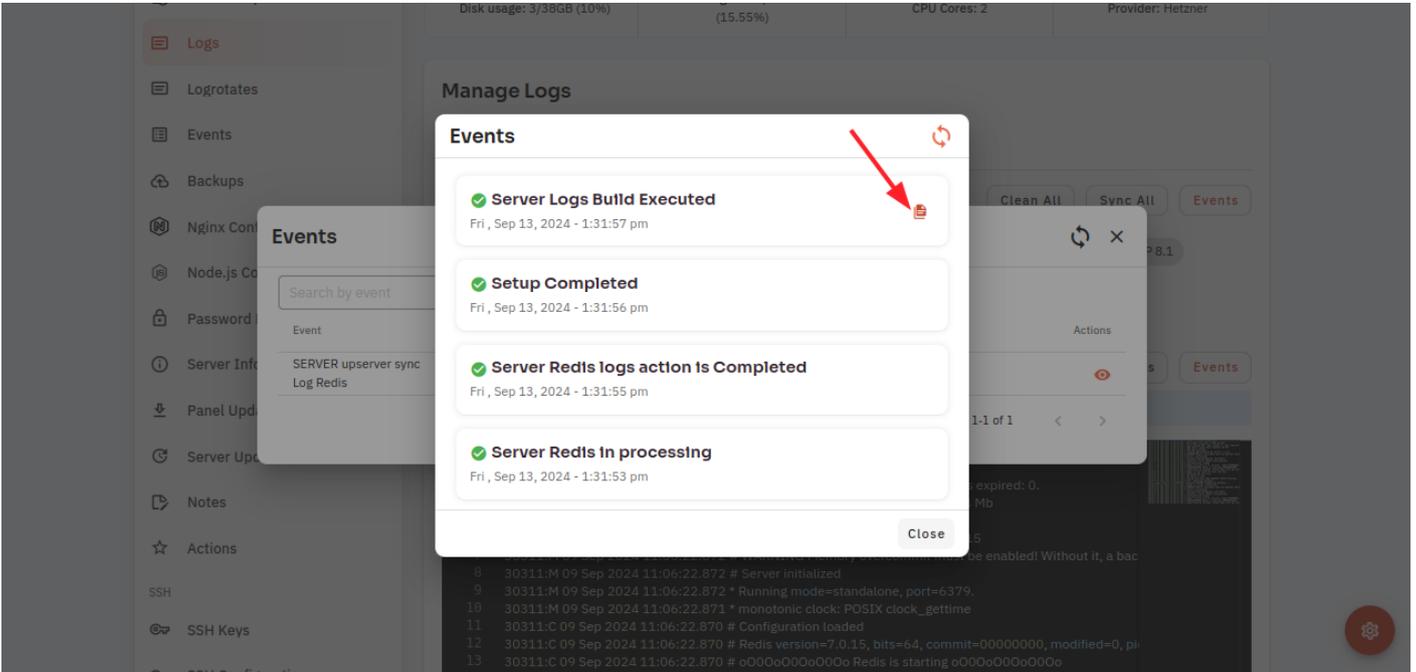
4. Click on the Event Button.



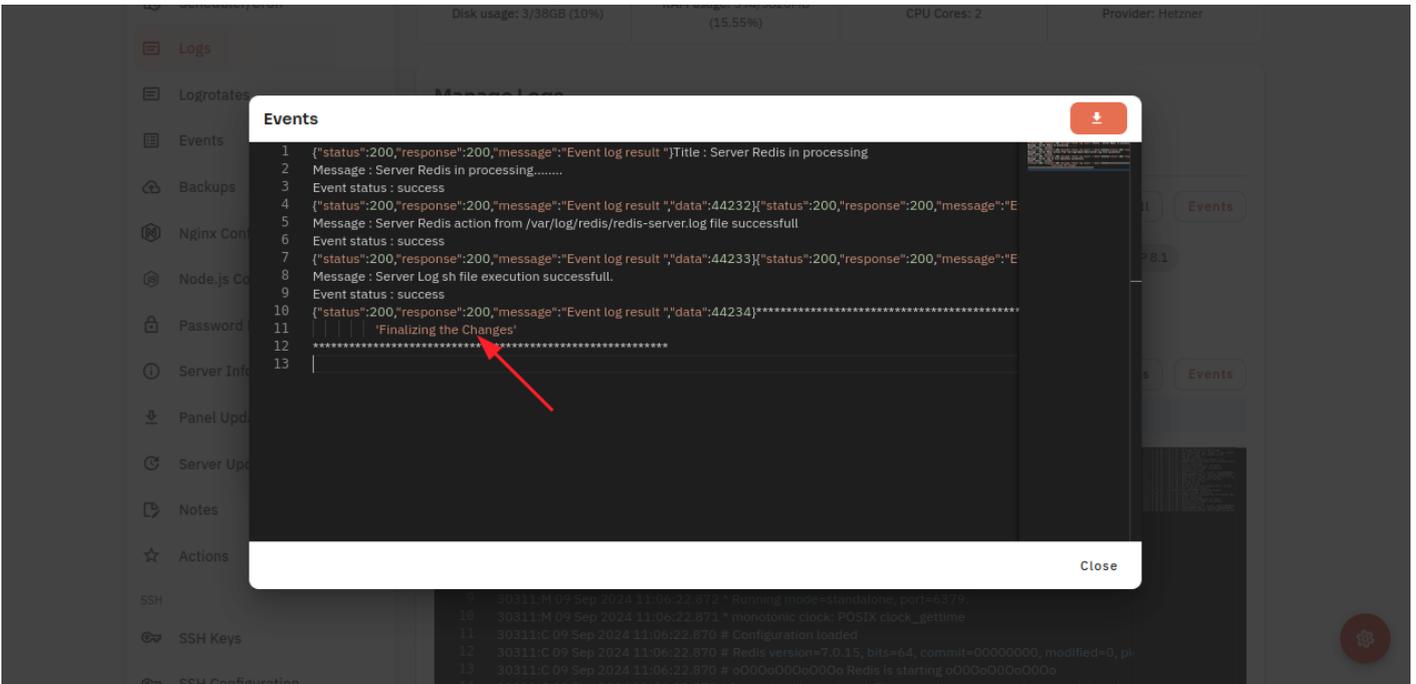
5. Click on the Eye icon.



6. Click On the file icon.



Here, you can see event data.

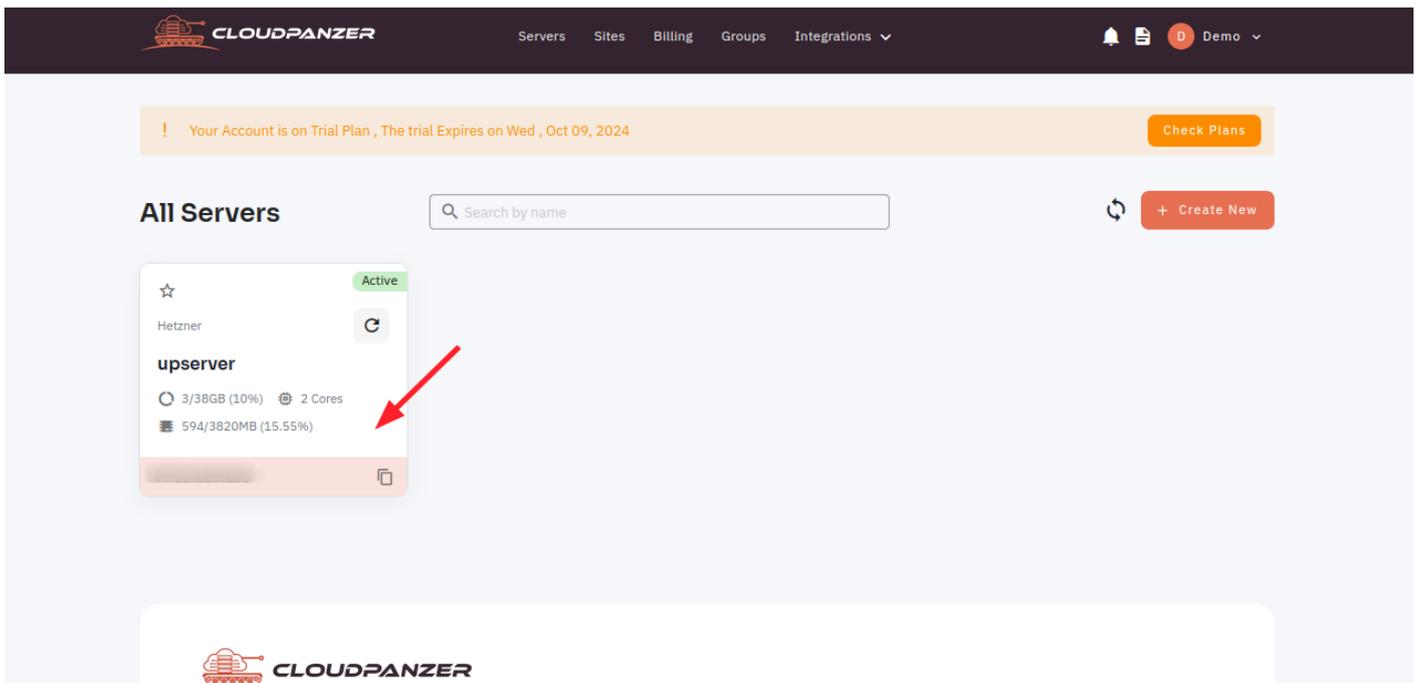


Looking for mobile Instructions?

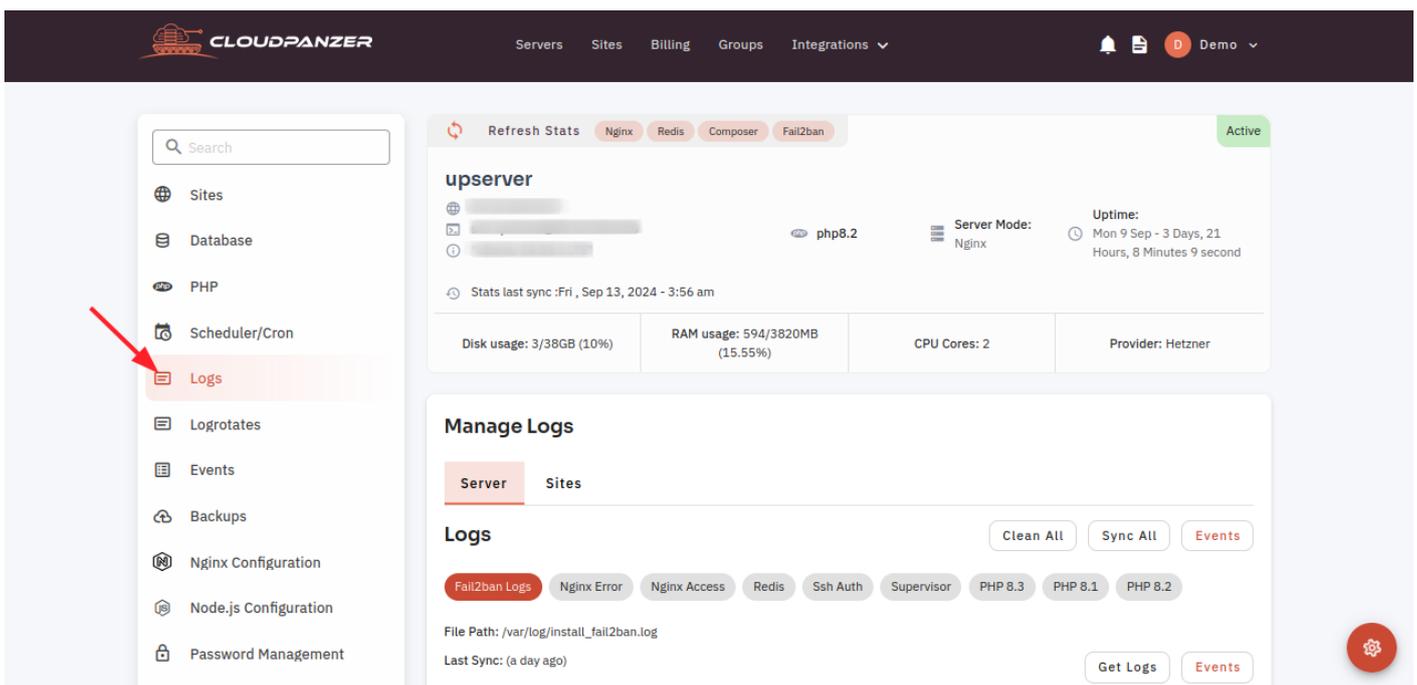
Available at <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-checks-redis-logs>

How to navigate Server Logs?

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



2: Select a Logs Option.



How to view SSH Auth Logs and Events on CloudPanzer?

One important aspect of managing an SSH server is monitoring and analyzing the authentication logs. These logs contain information about successful and failed login attempts and can be used to detect and prevent unauthorized access to the server.

Prerequisites :

You must have an Active Server. You can jump to the tutorial section if the above conditions are correct, or first follow the links below to set up the prerequisites.

How to install a Server

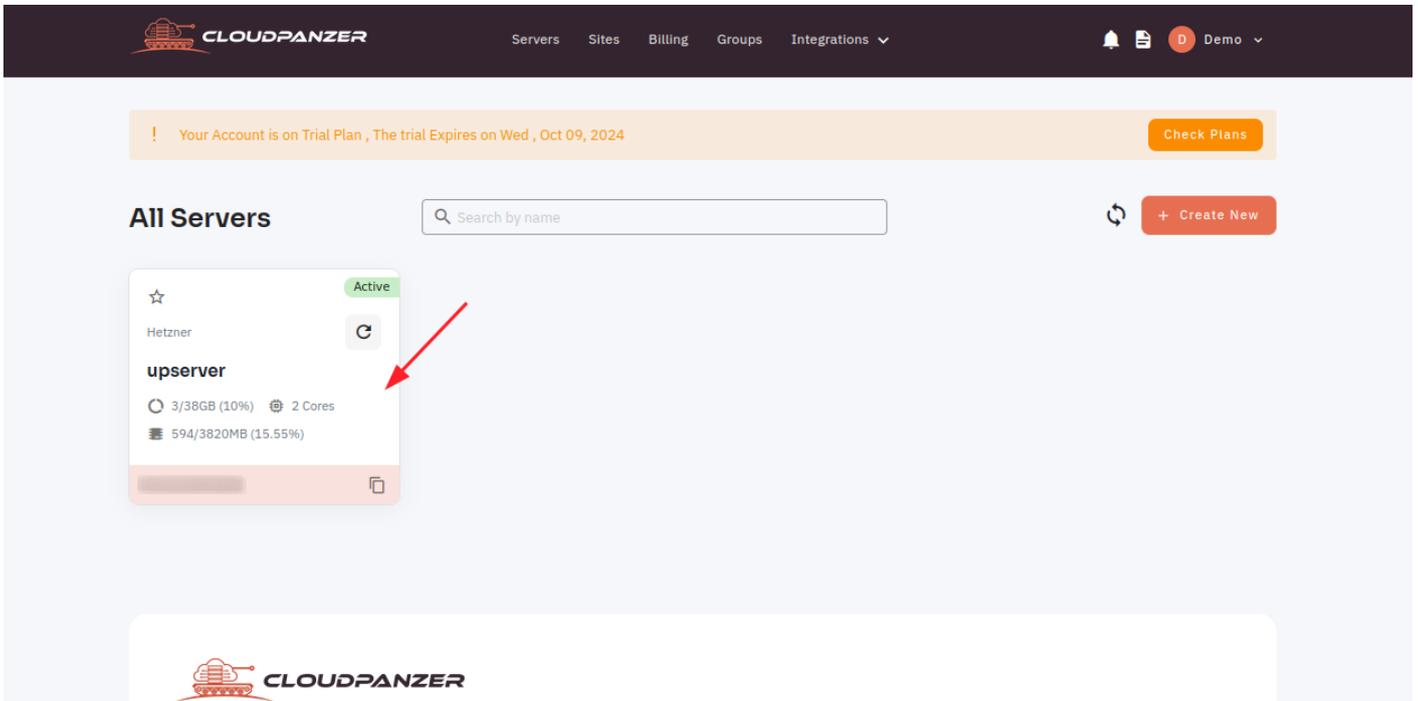
Tutorial :

You can watch the Video or Continue reading the post.

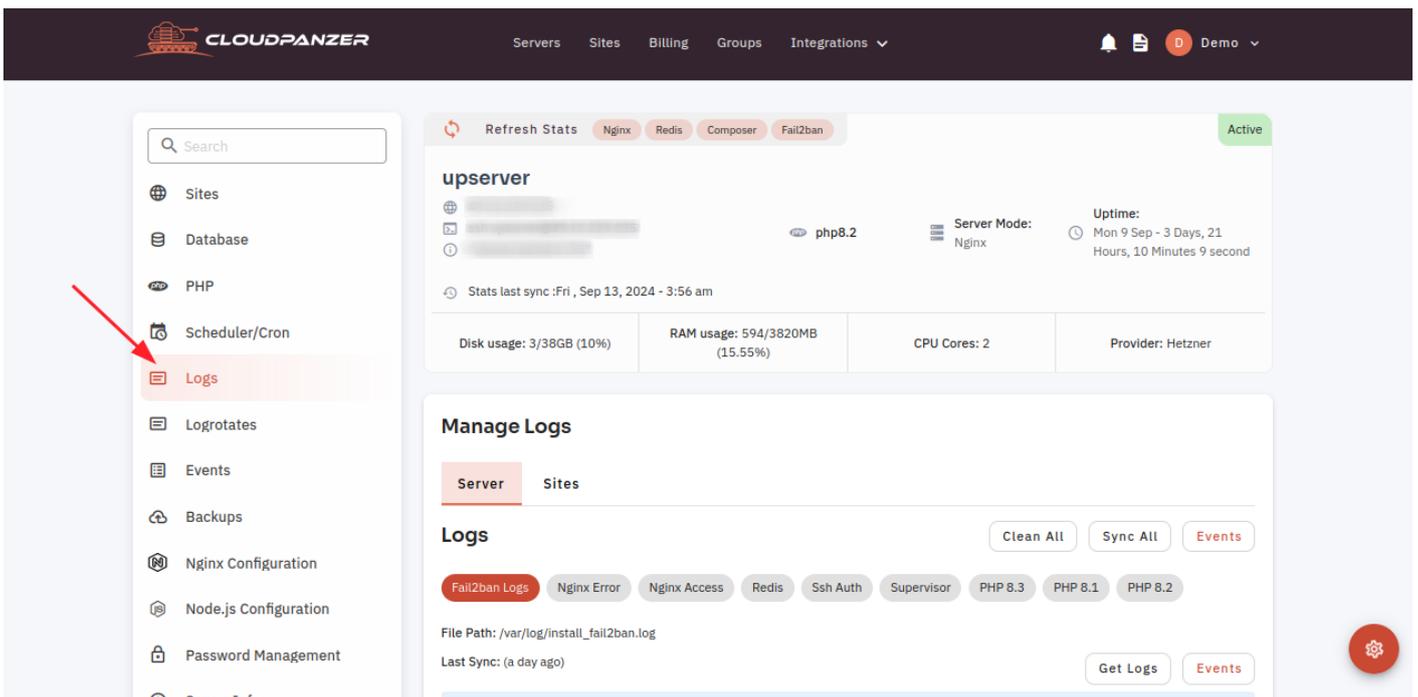
https://www.youtube.com/embed/_wEnsGm10Wk

Follow the steps below to SSH Auth Logs.

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



2. Click on the Logs button.



3. Click on the SSH Auth button and the Get Logs Button.

Disk usage: 3/38GB (10%) RAM usage: 594/3820MB (15.55%) CPU Cores: 2 Provider: Hetzner

Manage Logs

Server Sites

Logs

Clean All Sync All Events

Fail2ban Logs Nginx Error Nginx Access Redis Ssh Auth Supervisor PHP 8.3 PHP 8.1 PHP 8.2

File Path: /var/log/auth.log
Last Sync: (a day ago)

Get Logs Events

Please click Get Logs to get the newest logs.

Here, you can see SSH Auth Logs data.

Disk usage: 3/38GB (10%) (15.55%) CPU Cores: 2 Provider: Hetzner

Manage Logs

Server Sites

Logs

Clean All Sync All Events

Fail2ban Logs Nginx Error Nginx Access Redis Ssh Auth (2.3M) Supervisor PHP 8.3 PHP 8.1 PHP 8.2

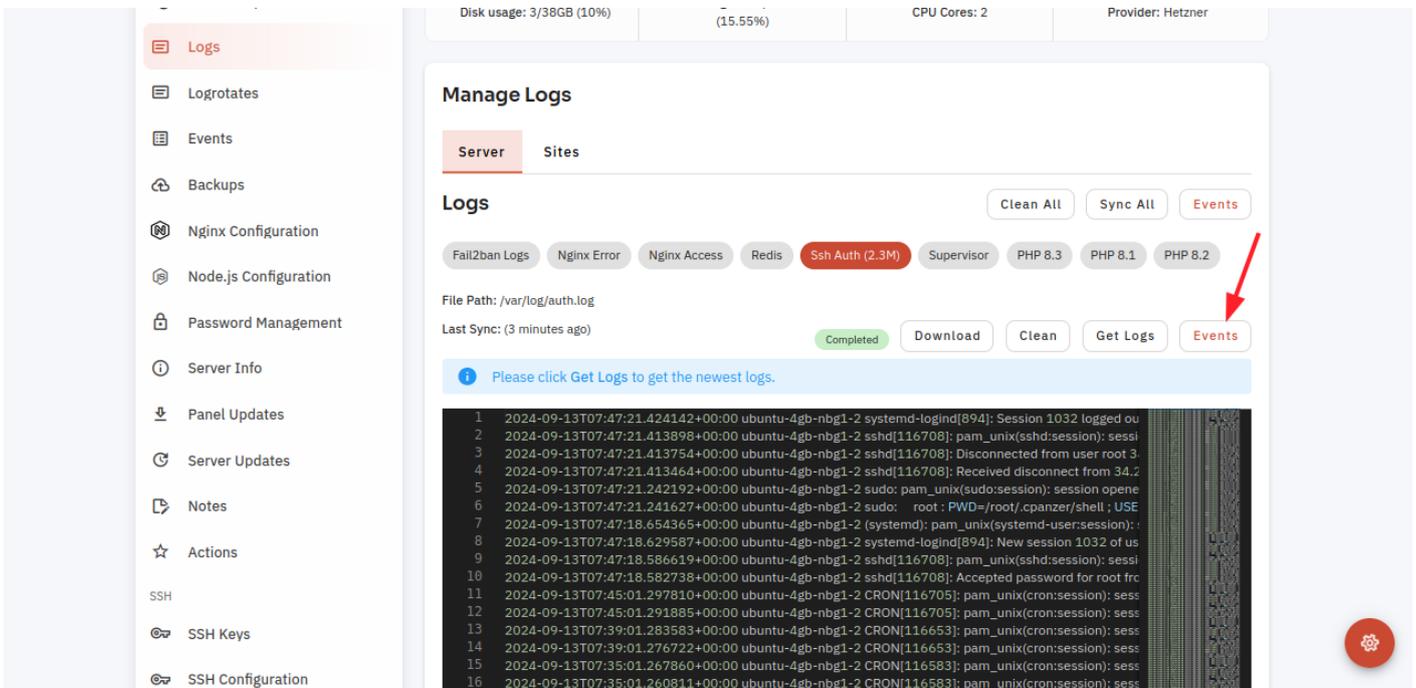
File Path: /var/log/auth.log
Last Sync: (a few seconds ago)

Completed Download Clean Get Logs Events

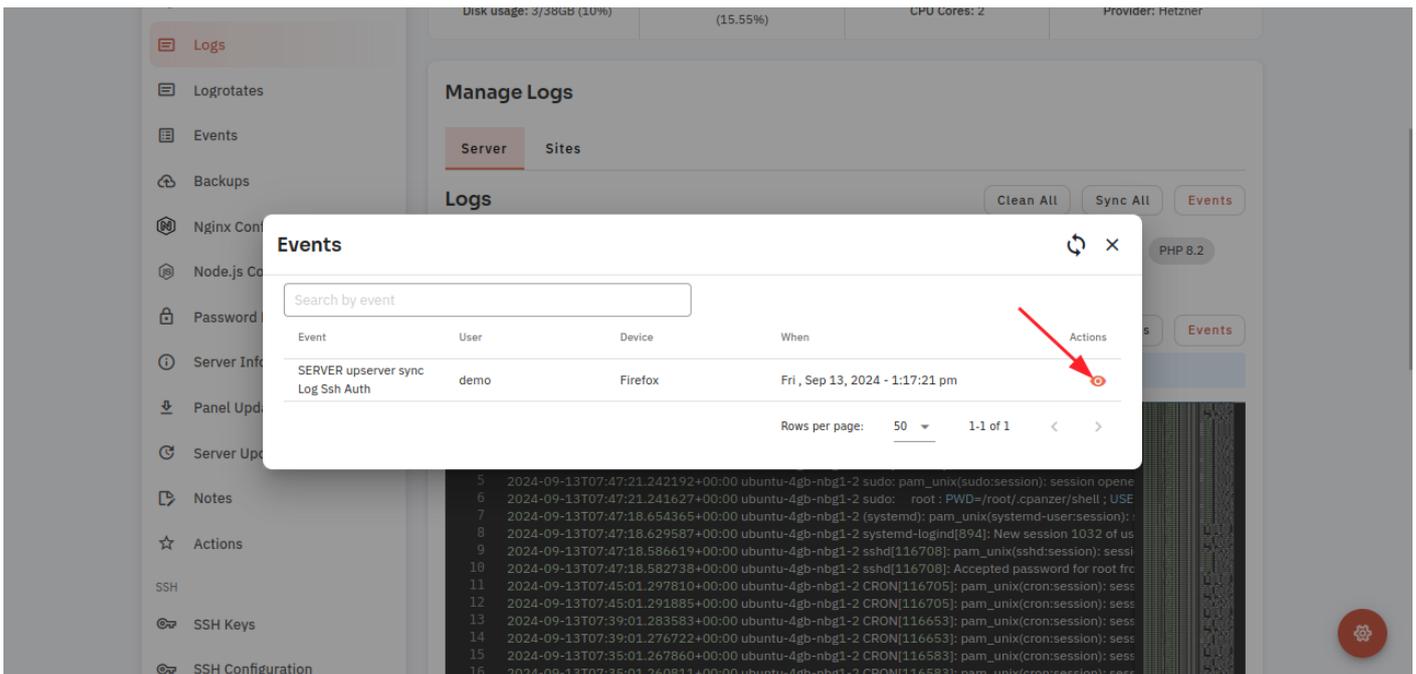
Please click Get Logs to get the newest logs.

```
1 2024-09-13T07:47:21.424142+00:00 ubuntu-4gb-nbg1-2 systemd-logind[894]: Session 1032 logged ou
2 2024-09-13T07:47:21.413898+00:00 ubuntu-4gb-nbg1-2 sshd[116708]: pam_unix(sshd:session): sessi
3 2024-09-13T07:47:21.413754+00:00 ubuntu-4gb-nbg1-2 sshd[116708]: Disconnected from user root 3.
4 2024-09-13T07:47:21.413464+00:00 ubuntu-4gb-nbg1-2 sshd[116708]: Received disconnect from 34.2
5 2024-09-13T07:47:21.242192+00:00 ubuntu-4gb-nbg1-2 sudo: pam_unix(sudo:session): session opene
6 2024-09-13T07:47:21.241627+00:00 ubuntu-4gb-nbg1-2 sudo: root : PWD=/root/cpanzer/shell ; USE
7 2024-09-13T07:47:18.654365+00:00 ubuntu-4gb-nbg1-2 (systemd): pam_unix(systemd-user:session):
8 2024-09-13T07:47:18.629587+00:00 ubuntu-4gb-nbg1-2 systemd-logind[894]: New session 1032 of us
9 2024-09-13T07:47:18.586619+00:00 ubuntu-4gb-nbg1-2 sshd[116708]: pam_unix(sshd:session): sessi
10 2024-09-13T07:47:18.582738+00:00 ubuntu-4gb-nbg1-2 sshd[116708]: Accepted password for root fr
11 2024-09-13T07:45:01.297810+00:00 ubuntu-4gb-nbg1-2 CRON[116705]: pam_unix(cron:session): sess
12 2024-09-13T07:45:01.291885+00:00 ubuntu-4gb-nbg1-2 CRON[116705]: pam_unix(cron:session): sess
13 2024-09-13T07:39:01.283583+00:00 ubuntu-4gb-nbg1-2 CRON[116653]: pam_unix(cron:session): sess
14 2024-09-13T07:39:01.276722+00:00 ubuntu-4gb-nbg1-2 CRON[116653]: pam_unix(cron:session): sess
15 2024-09-13T07:35:01.267860+00:00 ubuntu-4gb-nbg1-2 CRON[116583]: pam_unix(cron:session): sess
16 2024-09-13T07:35:01.260811+00:00 ubuntu-4gb-nbg1-2 CRON[116583]: pam_unix(cron:session): sess
```

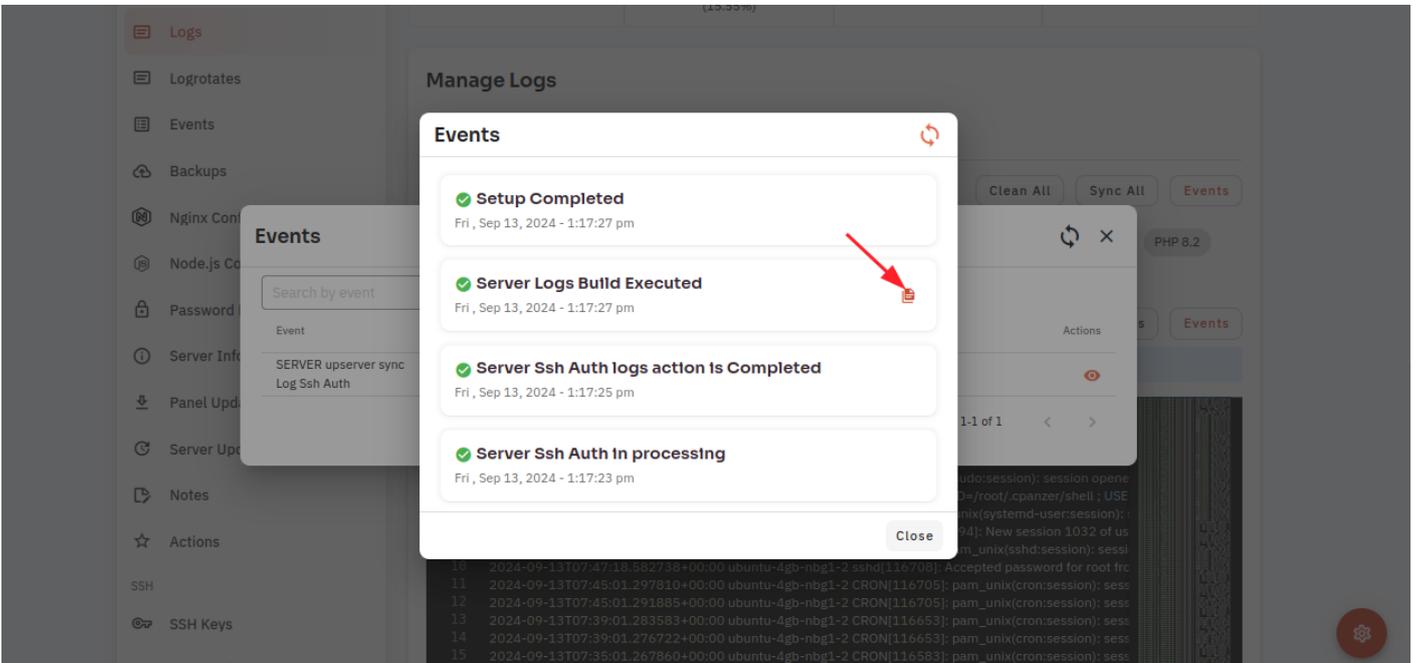
4. You can also check Events by clicking on the Events Button.



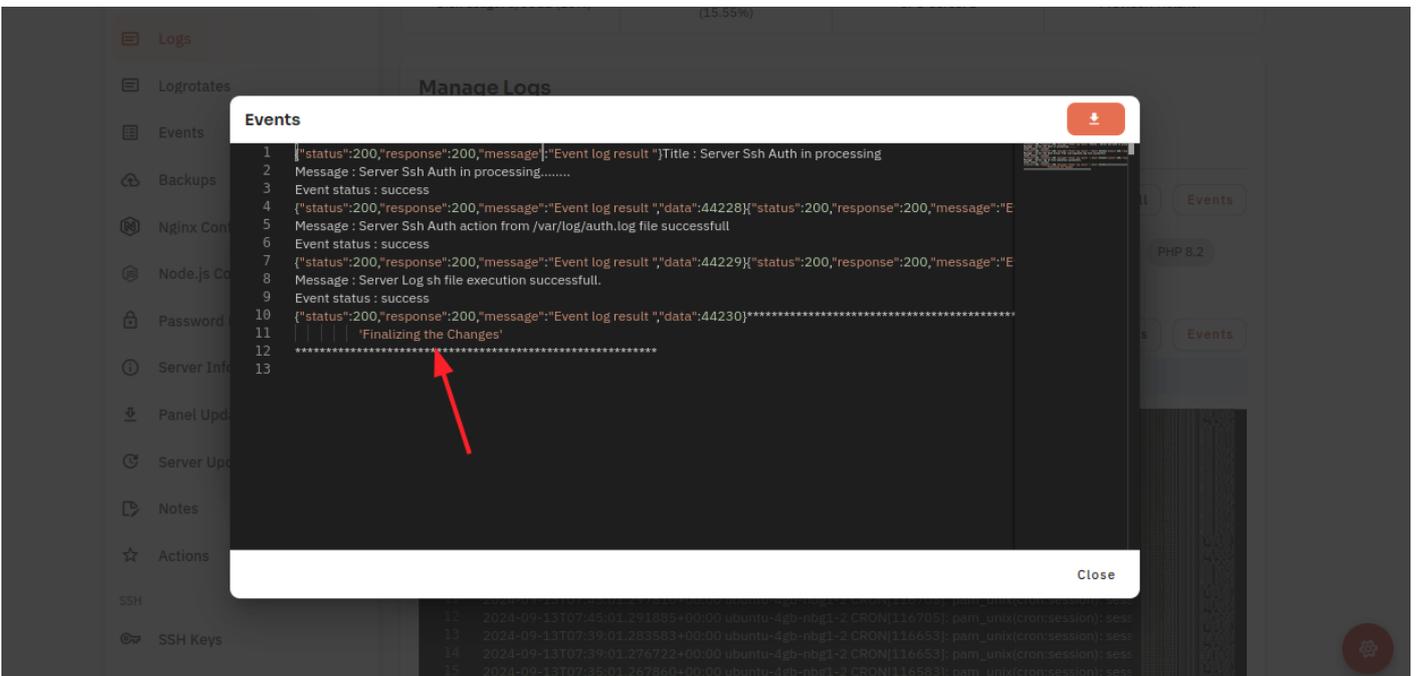
5. Click on the Eye icon.



6. Click on File Icon.



5. Here, you can see the event data.



Looking for mobile Instructions?

Available at <https://kb.cloudpanzer.com/books/mobile-app/page/how-to-checks-ssh-auth-logs-3iM>

How to check Server Fail2ban logs through the cloudpanzer website?

Fail2ban is a popular open-source intrusion prevention software that helps protect your server by monitoring log files and blocking IP addresses that show signs of malicious activity.

Tutorial :

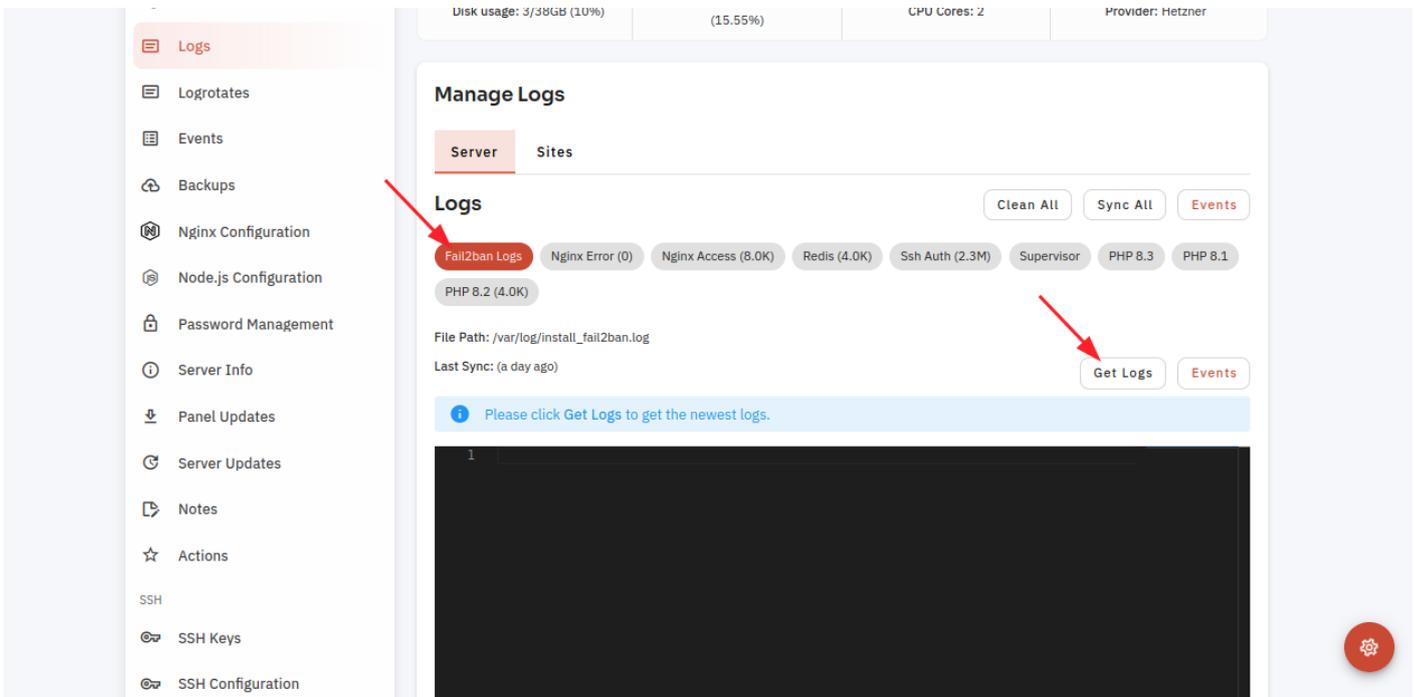
You can watch the Video or Continue reading the post.

Follow the steps below to check fail2ban

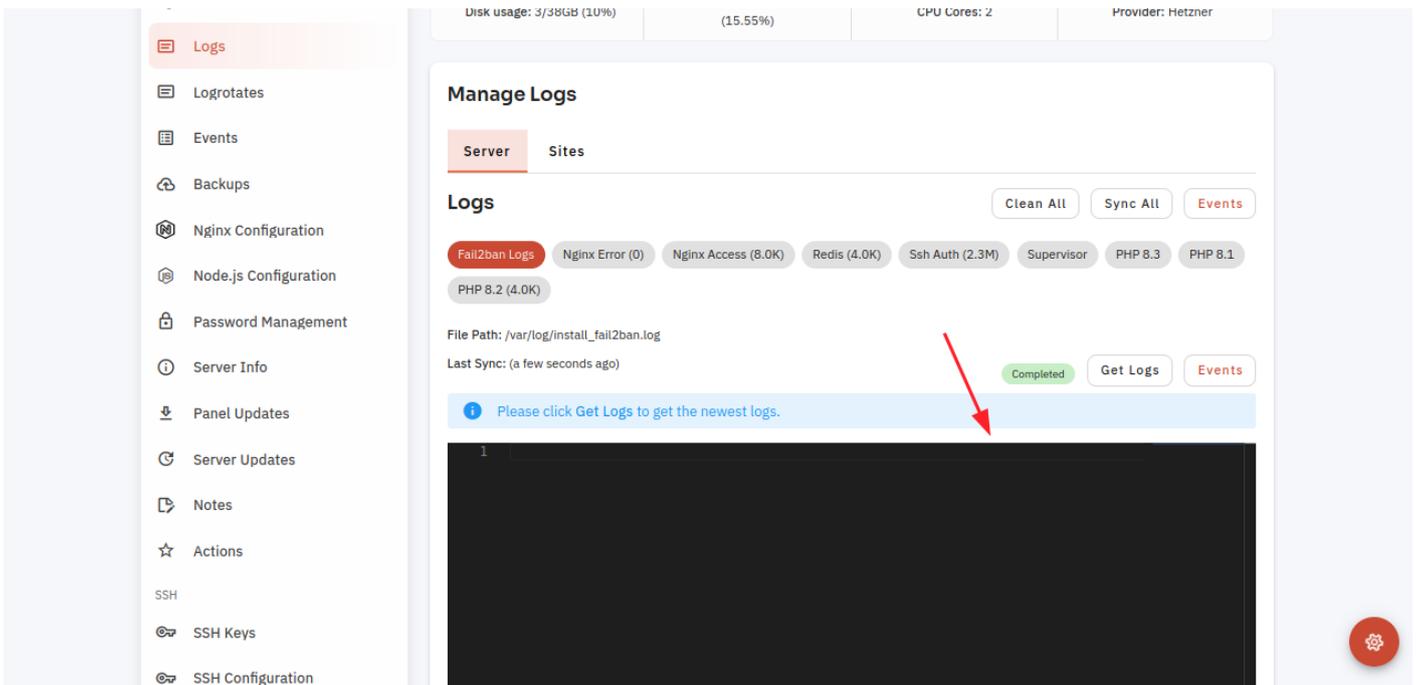
Navigate to the Logs

(Use this link to view How to Navigate

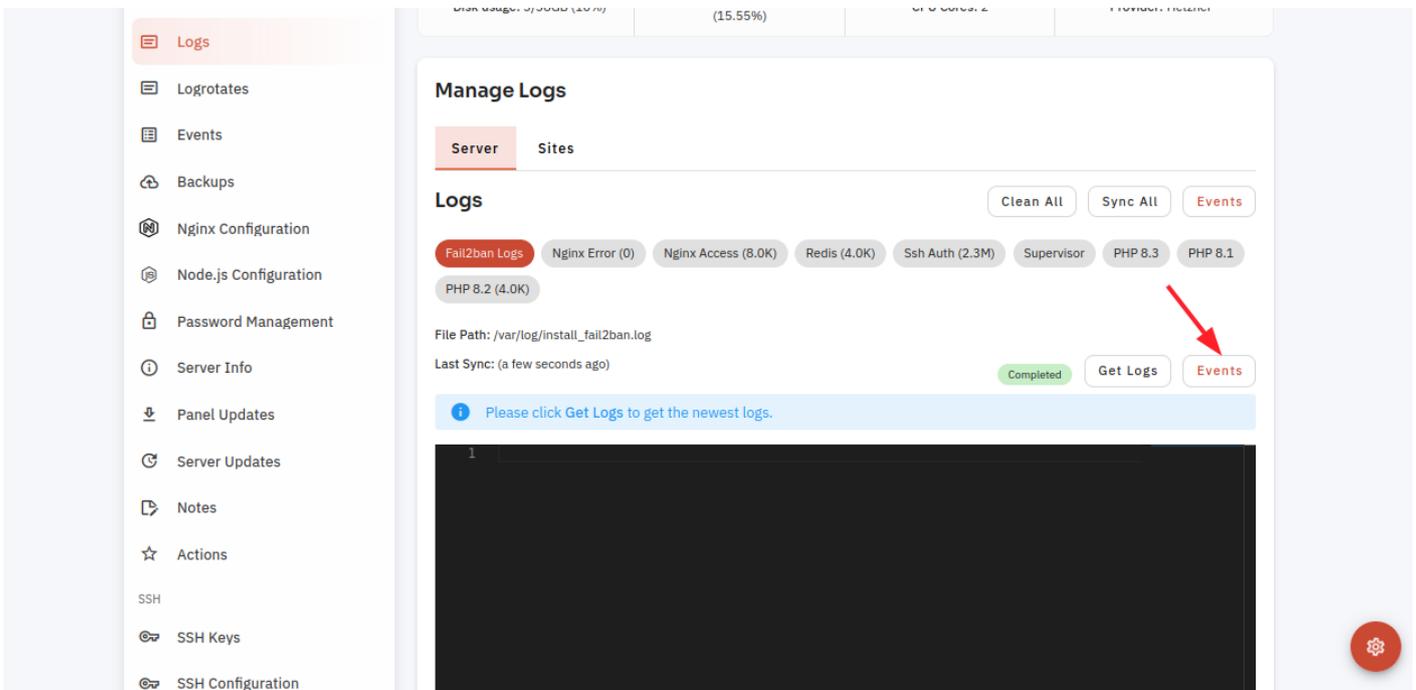
5: Click on the Fail2ban button then click on the get log button to see the logs.



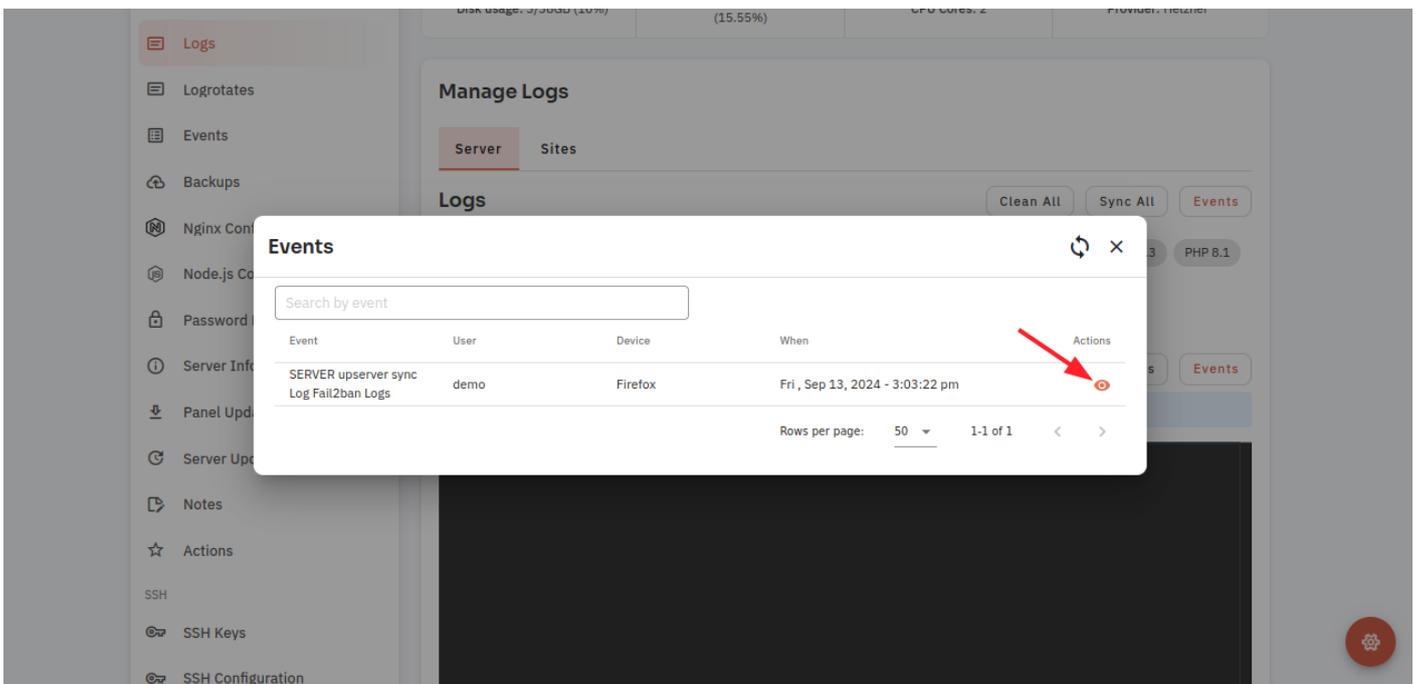
Here, you can check Fail2ban logs successfully.



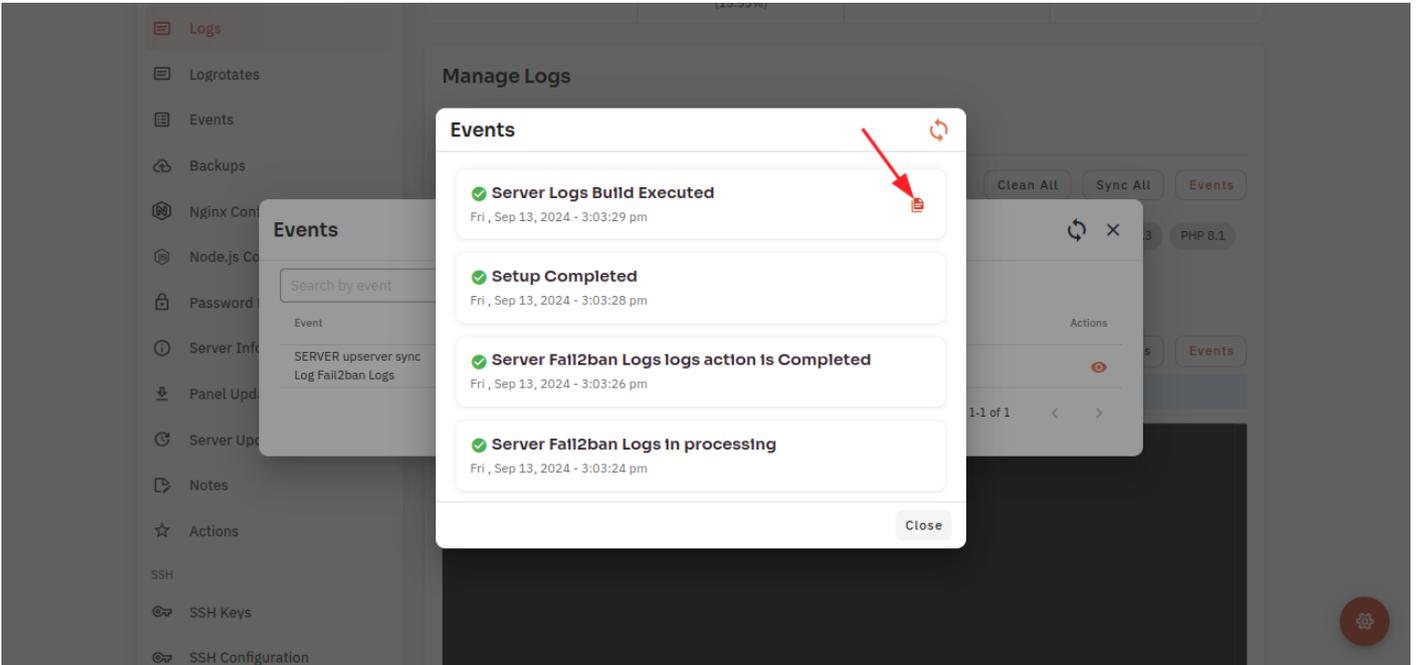
6 Click on the Events Button.



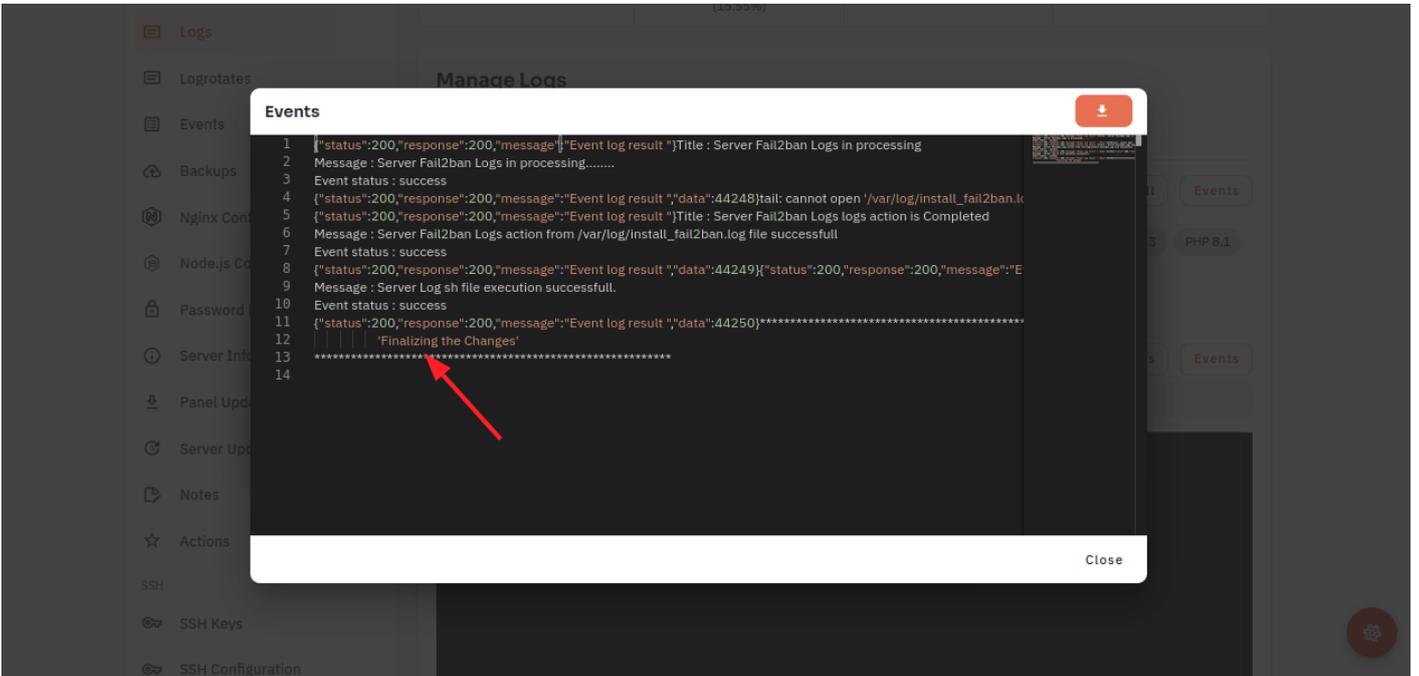
7. Click on the Eye Icon.



8. Click on the file icon.



Here, you can see the event data.



How to check Server Supervisor logs through the cloudpanzer website?

Supervisor is a process control system used to manage and monitor processes on Unix-like operating systems. It's often used to control processes, restart them if they crash, and manage their lifecycle.

Tutorial :

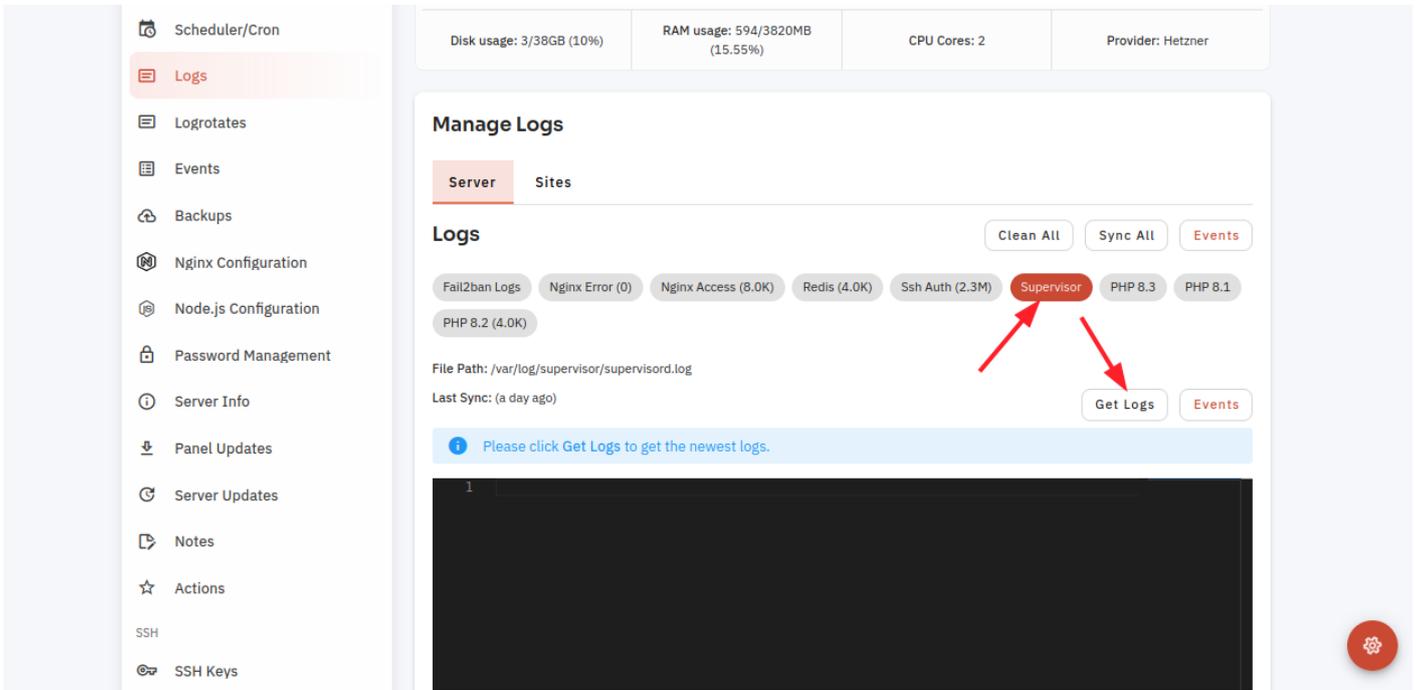
You can watch the Video or Continue reading the post.

Follow the steps below to check the Supervisor

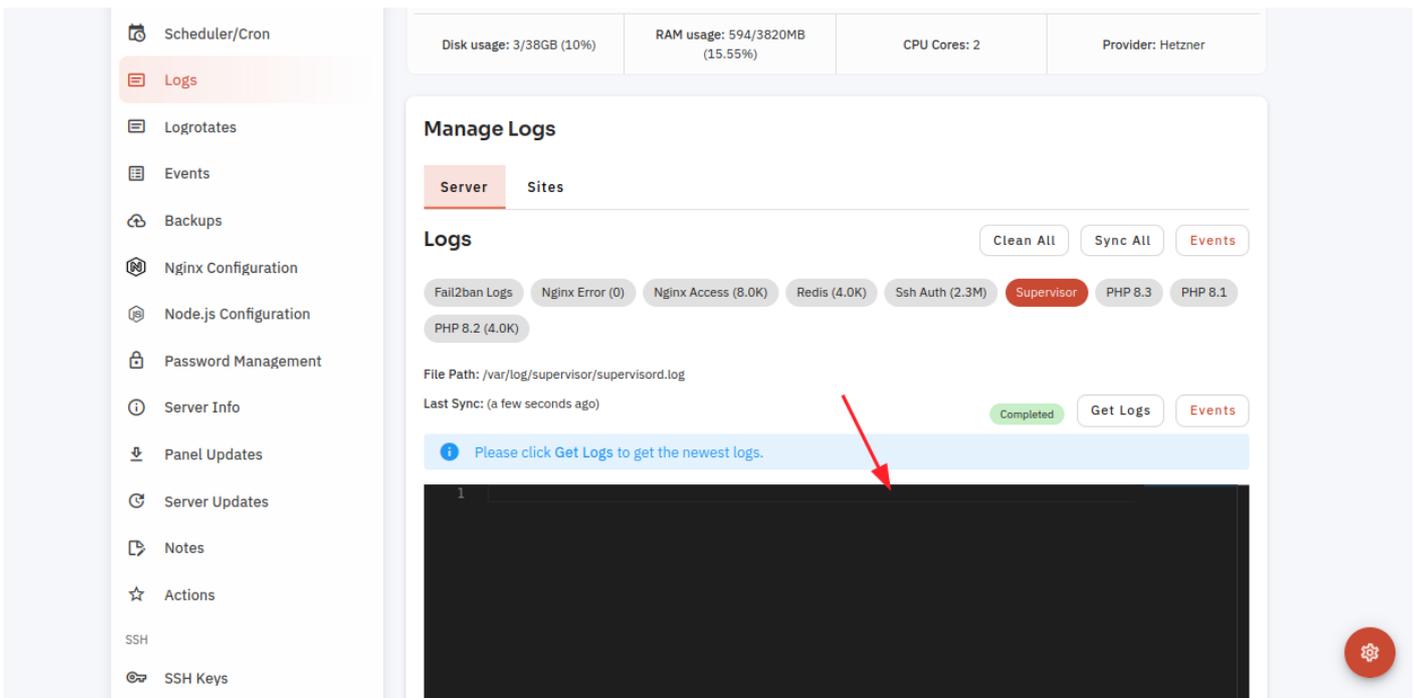
Navigate to the Logs

(Use this link to view How to Navigate

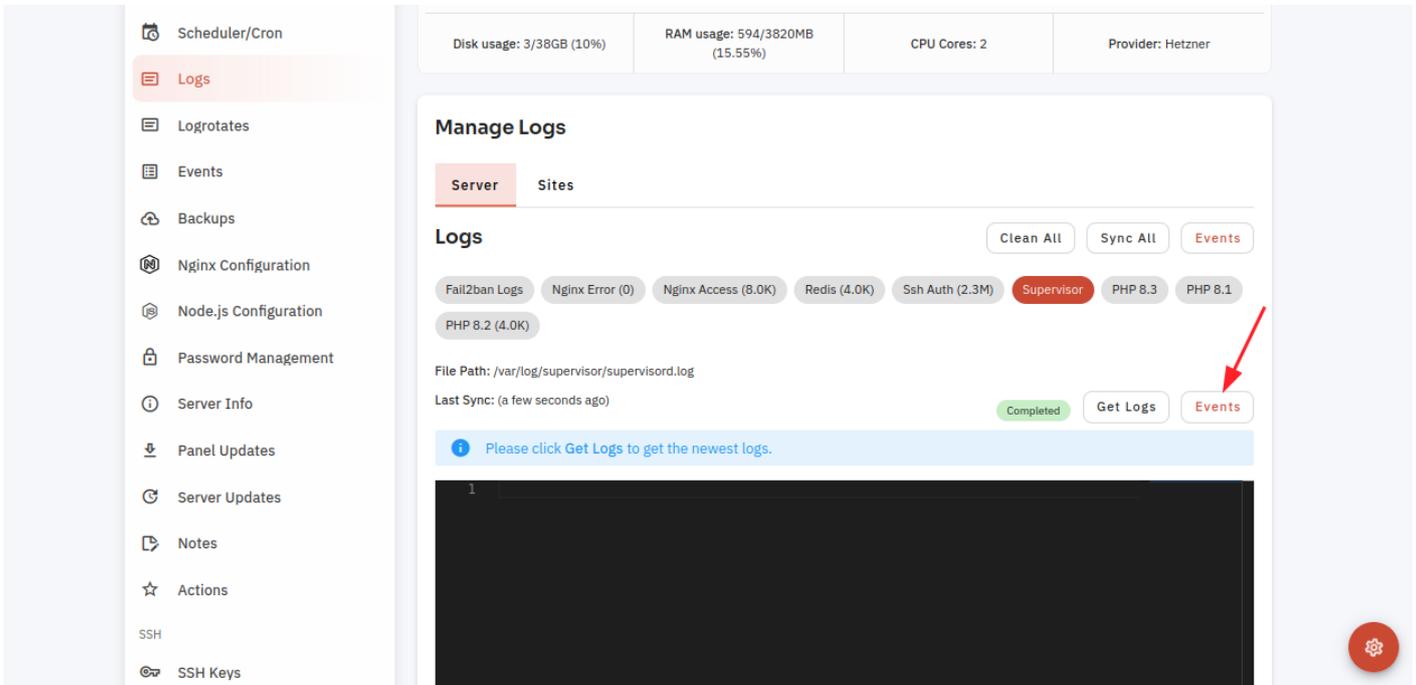
5: Click on the Supervisor button then click on the Get Log button to see the logs.



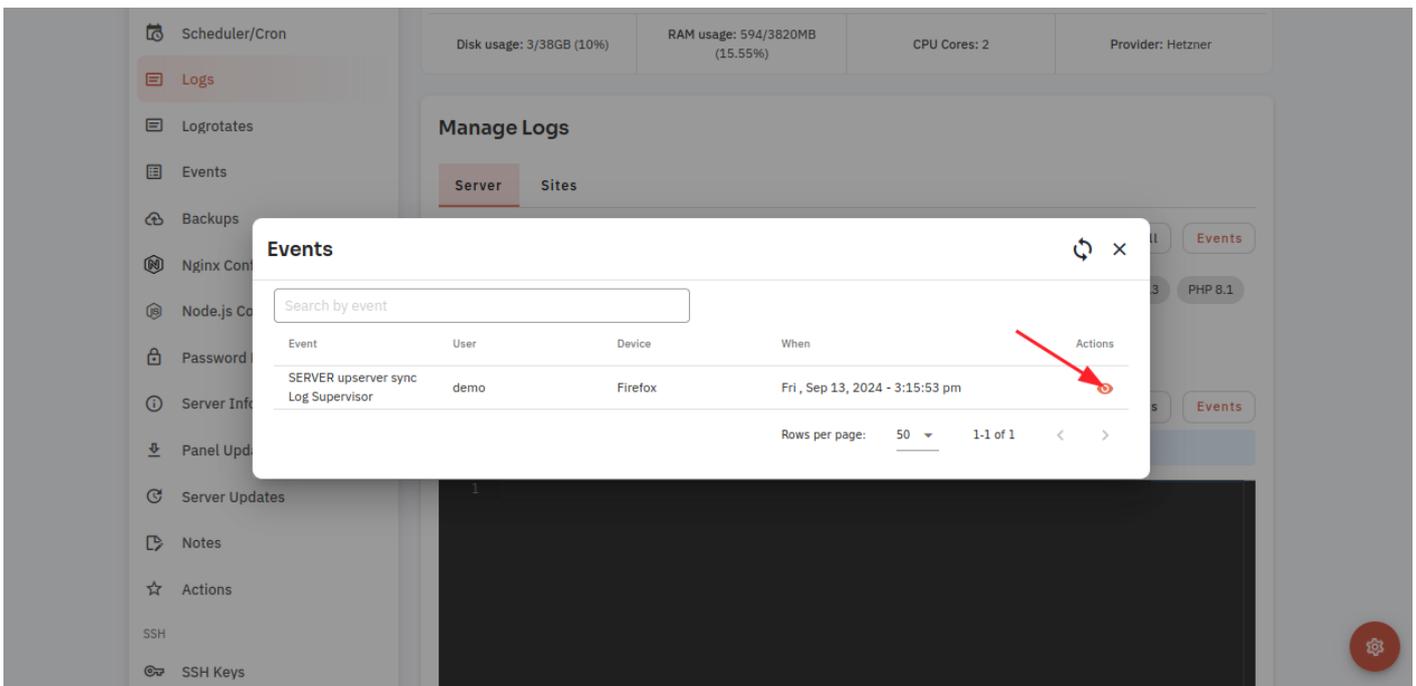
Here, you can check the Supervisor logs successfully.



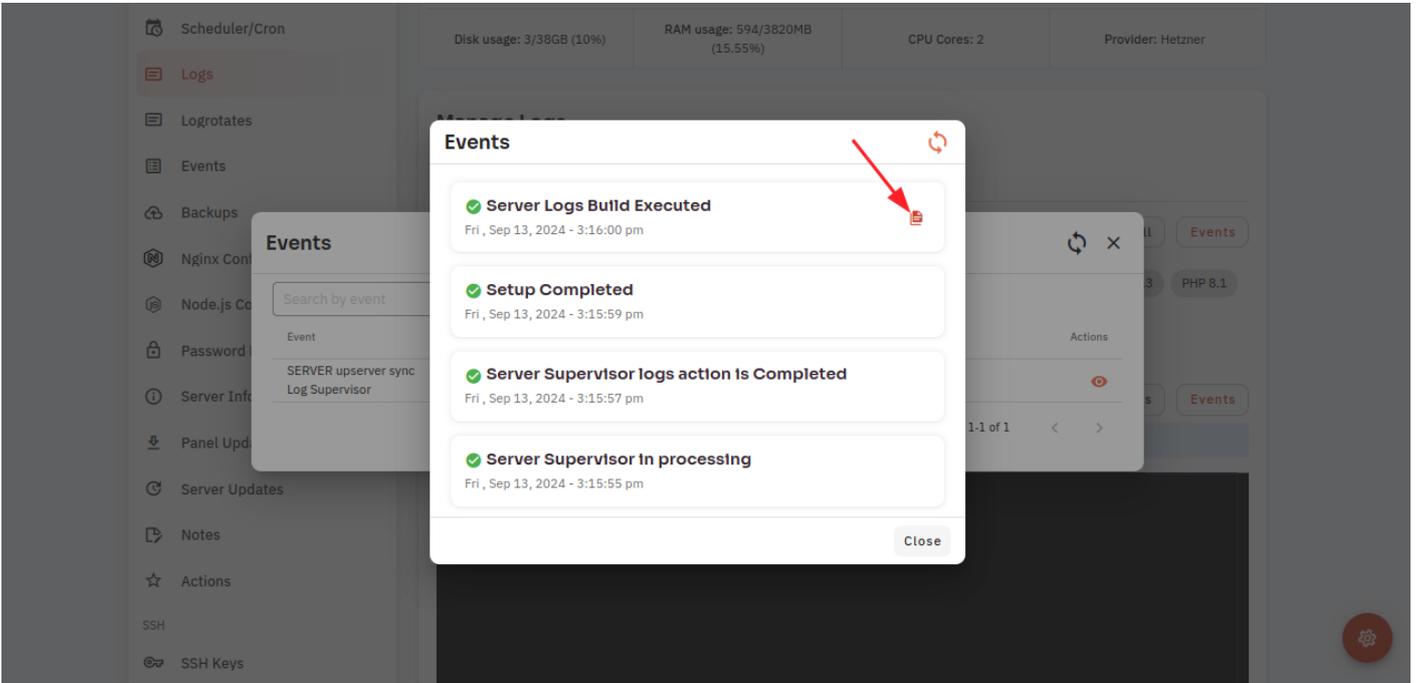
6 Click on the Events Button.



7. Click on the Eye Icon.



8. Click on the file icon.



Here, you can see the event data.

