How to truncate the ssh session logs recorded
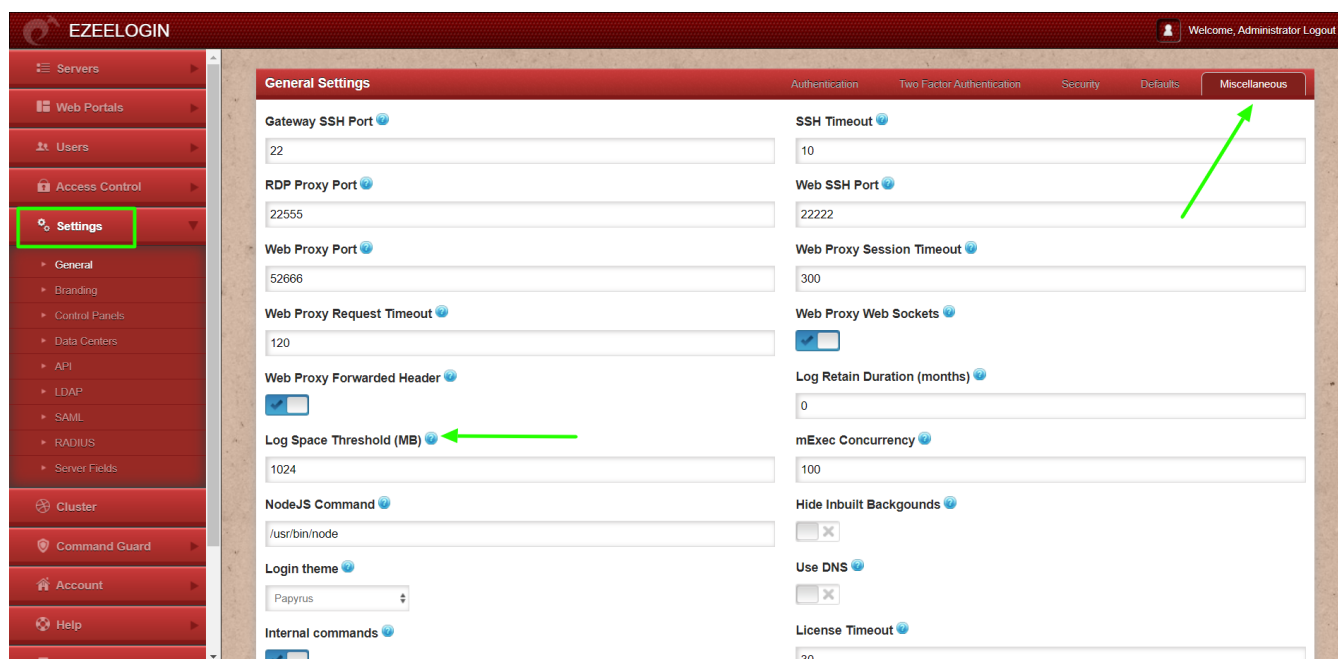
168 admin August 7, 2023 <u>Migration & Maintenance</u> 7185

SSH Log Rotation | Prune SSH logs recorded

In order to prevent a full disk its is important to prune the ssh log files regularly. It is possible to auto-delete logs when the log size exceeds a limit.

Navigate to **Settings**->**Miscellaneous**->**Log space threshold**

<u>https://www.ezeelogin.com/user_manual/Miscellaneous.html</u>

You can also set Log Space Threshold from the database. You can replace the value with the value of your choosing.

You can also set the period for which the ssh user log and the rdp user logs has to be retained in the system after which it would be truncated by daily cronjobs. A value 0 means the logs would be retained for ever.

Navigate to **Settings**->**Miscellaneous**->**Log Retain Duration**
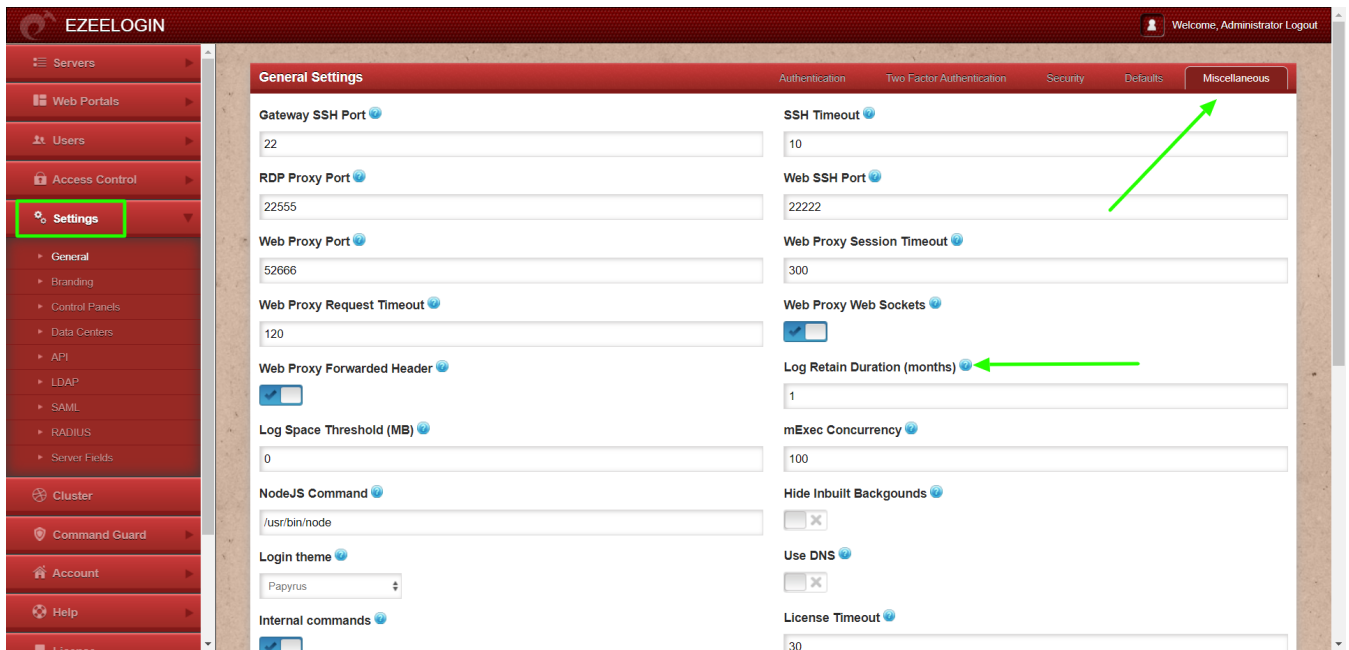
You can also set Log Retain Duration from the database. You can replace the value with the value of your choosing.

```
root@jumpserver:~#
```

Set a cronjob for root user to run daily or once a week so that log files stored on the server in the directory (/var/log/ezlogin/) are truncated when it exceeds a particular size or when it older than the specified number of days.

The path to the command that needs to be set in cron is

The ssh log files recorded are stored in the directory /var/log/ezlogin/full , /var/log/ezlogin/input, /var/log/ezlogin/output, /var/log/ezlogin/rdp. The 'full' directory store the entire ssh sessions. The 'input' directory store the recording from the STDIN . The 'output' directory stores the recording from the STDOUT and the 'rdp' directory stores the rdp session recorded.

Deleting SSH recording from the GUI.

 You can also delete ssh log from the GUI by selecting the ssh log session and by clicking on the trash icon.
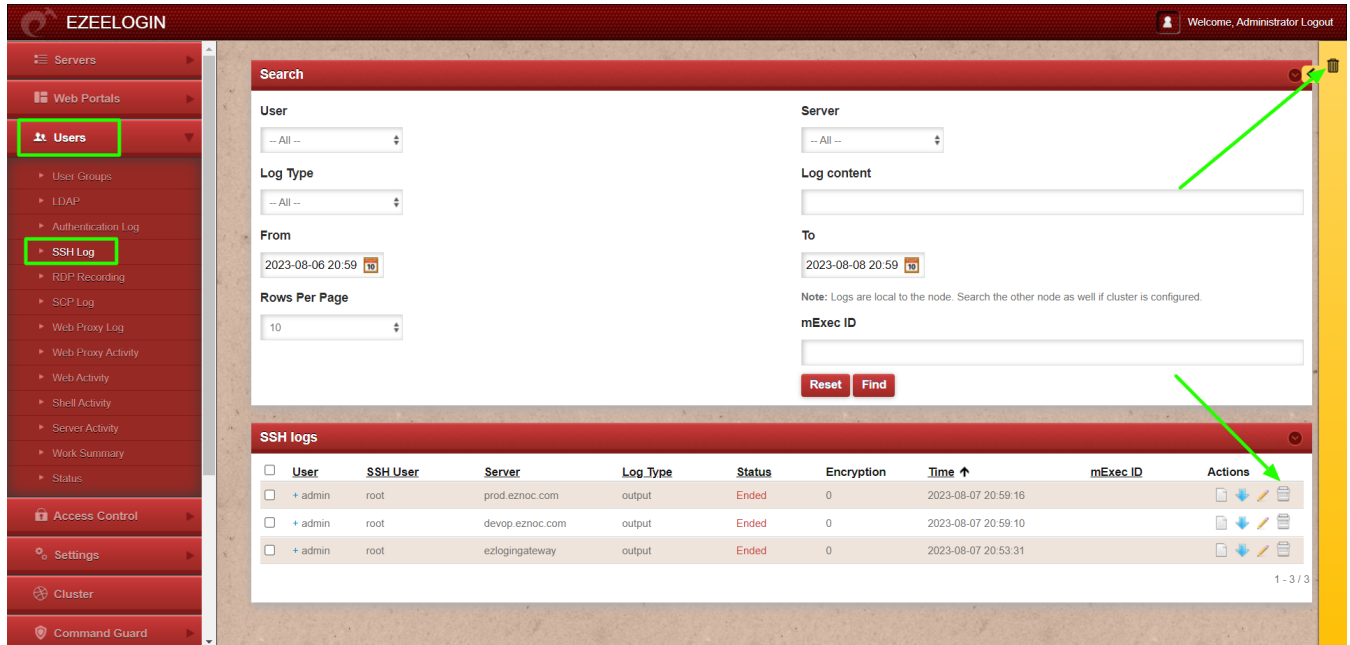
Ensure the housekeeping script is set to run in cron (0 6 * * * php /usr/local/ezlogin/house_keeping.php) so that the ssh sessions recorded which are stored in files are deleted from the backend server. You may also run the command manually to ensure that files are deleted from the backend almost instantly . You may wonder why the ssh log recorded stored in the directory /var/log/ezlogin is not deleted when the ssh recording is deleted from the gui, this is because the webserver user does not have the privileges to delete the ssh log recording in the ownership of the ssh gateway user.

If you are unable to login to Ezeelogin software GUI, you can delete the log files from database using below command

root@jumpserver:~# find /var/log/ezlogin -type f -mtime +365 -exec ls -al {} ;

The above command will list the log files in the directory "/var/log/ezlogin" that is older than 365 days.

root@jumpserver:~# find /var/log/ezlogin -type f -mtime +365 -exec rm {} ;

The above command will find log files older than 365 days in the directory "/var/log/ezlogin" and deletes them.

Related Articles

[Deleting entries in the mysql database table gwactivity_logs](#)

[Issue with Log Retain Duration](#)