Web Server Log File Analysis Report

Prepared by: Morcos osama shaker
id:2205056

1. Objective

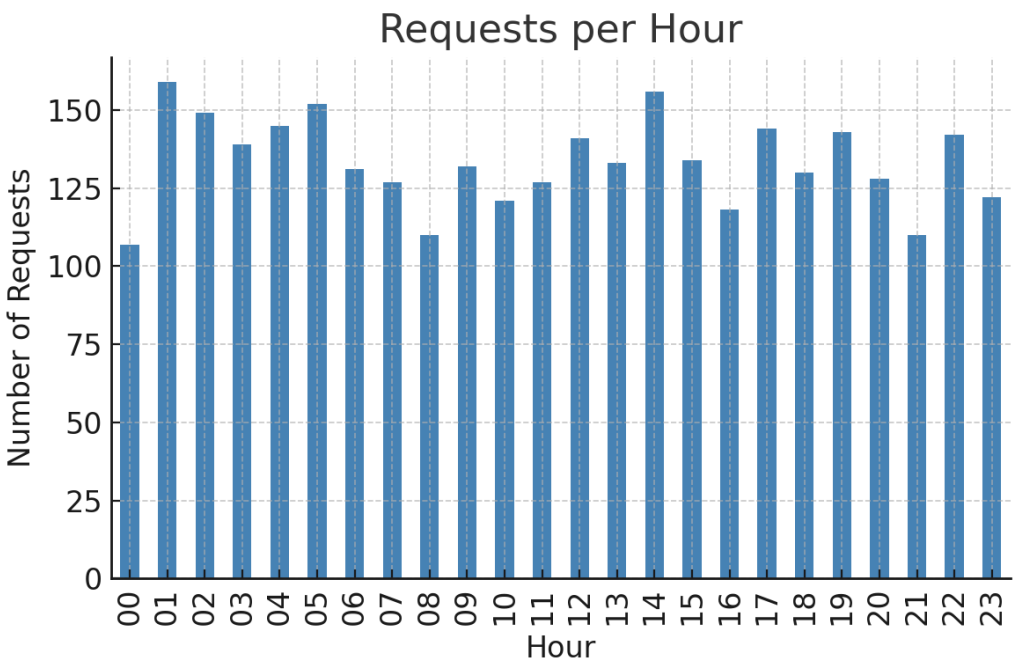
The objective of this analysis is to evaluate the web server access logs to identify request patterns, understand user behavior, detect issues (especially request failures), and suggest performance or security improvements. The data spans two weeks and includes detailed request information.

2. Summary Statistics

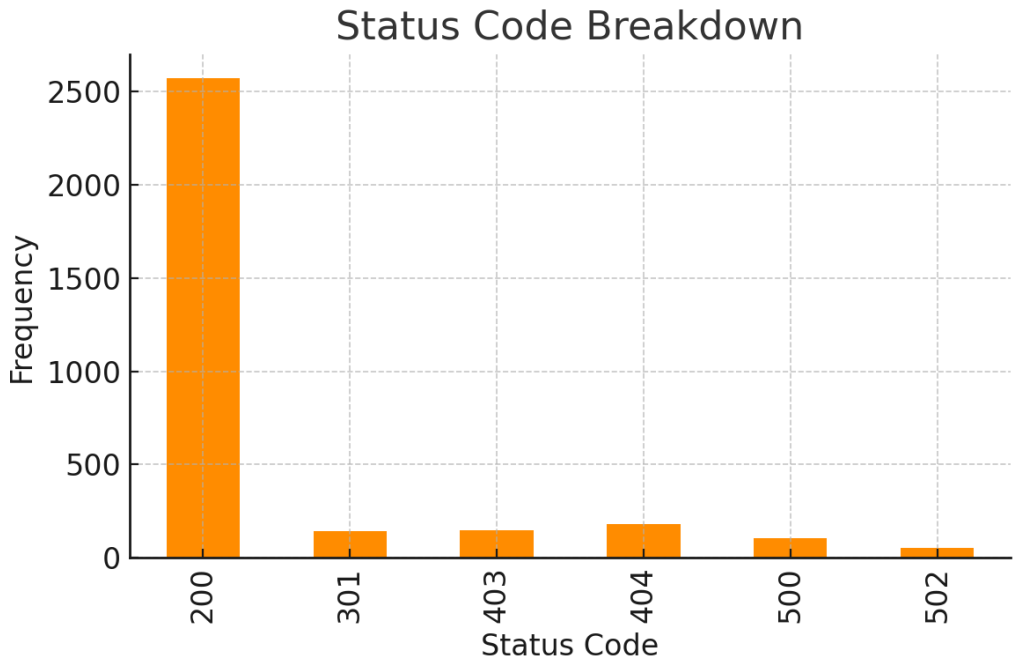
- Total Requests: 3200
- GET Requests: 1623
- POST Requests: 1577
- Unique IP Addresses: 68
- Failed Requests (4xx and 5xx): 487
- Failure Percentage: 15.22%
- Most Active IP Address: 192.168.1.45
- Average Requests per Day: 228.57

3. Visual Insights

Requests distributed by hour of the day:



Status code breakdown:



4. User Request Patterns

Top 5 IP addresses by number of requests:

IP Address	Request Count
192.168.1.45	65
192.168.1.23	61
192.168.1.9	60
10.0.0.11	59
192.168.1.32	58

5. Failure Analysis

Days with the highest number of failed requests:

Date	Failed Requests
30/Apr/2025	48
01/May/2025	48
29/Apr/2025	38
26/Apr/2025	37
03/May/2025	35

6. Recommendations

Based on the analysis, the following recommendations are provided:
- Monitor and mitigate failures, particularly status codes 404 and 500 which indicate resource issues or server errors.
- Implement rate-limiting or IP blocking for high-frequency requesters, especially the most active IP.
- Review server configuration and application routing to reduce 4xx/5xx errors.
- Add monitoring tools to observe hourly spikes in traffic and anticipate demand.
- Secure endpoints that receive high POST request volumes to prevent misuse or attacks.

7. Conclusion

This log file analysis revealed key usage trends and highlighted critical failure points. With strategic monitoring and proactive performance tuning, the web server can be made more efficient and secure. Ongoing analysis is recommended to track evolving behavior.