**Log Analysis Report**
**By Youssef Mohamed Ahmed Abdelwahed – 2205168**

---

## Overview

This report presents a comprehensive analysis of Apache server logs to identify trends in web traffic, error rates, and potential security risks. The findings offer insights into user behavior, system performance, and areas requiring attention. Recommendations are provided to enhance reliability, efficiency, and security.

## 1. Request Summary

- Total Number of Requests: 10,000
- GET Requests: 9,952
- POST Requests: 5

## 2. Unique IP Addresses

- Total Unique IPs: 1,753
- Sample Request Activity by IP:
    - 100.2.4.116: 6 GET, 0 POST
    - 100.43.83.137: 84 GET, 0 POST
    - 101.119.18.35: 33 GET, 0 POST
    - 101.199.108.50: 3 GET, 0 POST
    - 101.226.168.196: 1 GET, 0 POST
    - 103.247.192.5: 1 GET, 0 POST

## 3. Error Requests (HTTP 4xx and 5xx)

- Total Failed Requests: 220
- Failure Rate: 2.20%

## 4. Most Active User

- IP Address: 66.249.73.135
- Total Requests: 482

## 5. Daily Request Averages

- Average Requests per Day: 2500
- Average Requests per Day: 2.27

## 6. High Failure Days

- 19/May/2015: 66 failures
- 18/May/2015: 66 failures
- 20/May/2015: 58 failures
- 17/May/2015: 30 failures

## 7. Requests by Hour (00:00–07:00)

- 00:00 – 361
- 01:00 – 360
- 02:00 – 365
- 03:00 – 354
- 04:00 – 355
- 05:00 – 371
- 06:00 – 366
- 07:00 – 357

## 8. Hourly Request Trends

- 01:00 to 02:00: Increase (360 to 365)
- 02:00 to 03:00: Decrease (365 to 354)
- 03:00 to 04:00: Slight Increase (354 to 355)
- 04:00 to 05:00: Increase (355 to 371)
- 05:00 to 06:00: Decrease (371 to 366)
- 06:00 to 07:00: Decrease (366 to 357)
- 07:00 to 08:00: Decrease (357 to 345)
- 08:00 to 09:00: Increase (345 to 364)
- 09:00 to 10:00: Increase (364 to 443)
- 10:00 to 11:00: Increase (443 to 459)

## 9. HTTP Status Code Breakdown

- 200 OK: 9,126 (91.26%)
- 304 Not Modified: 445 (4.45%)
- 404 Not Found: 213 (2.13%)
- 301 Moved Permanently: 164 (1.64%)
- 206 Partial Content: 45 (0.45%)
- 500 Internal Server Error: 3 (0.03%)
- 416 Range Not Satisfiable: 2 (0.02%)
- 403 Forbidden: 2 (0.02%)

## 10. Most Active IPs by Request Type

- GET: 66.249.73.135 (482 requests)

- POST: 78.173.140.106 (3 requests)

## 11. Failure Request Patterns

Hour 00: 6 failures (2.73% of total failures)
Hour 01: 10 failures (4.55% of total failures)
Hour 02: 10 failures (4.55% of total failures)
Hour 03: 7 failures (3.18% of total failures)
Hour 04: 9 failures (4.09% of total failures)
Hour 05: 15 failures (6.82% of total failures)
Hour 06: 14 failures (6.36% of total failures)
Hour 07: 7 failures (3.18% of total failures)
Hour 08: 2 failures (0.91% of total failures)
Hour 09: 18 failures (8.18% of total failures)
Hour 10: 12 failures (5.45% of total failures)
Hour 11: 11 failures (5.00% of total failures)
Hour 12: 7 failures (3.18% of total failures)
Hour 13: 12 failures (5.45% of total failures)

---

## Recommendations

### 1. Minimizing Failures

- Address 404 Errors by fixing broken URLs and checking for misconfigurations.
- Investigate 500 Errors with detailed server-side diagnostics and logging.
- Evaluate causes of 403 and 416 errors by reviewing permissions and handling of file range requests.

### 2. Managing High Traffic

- Peak Activity Hour: 14:00–15:00 (approx. 498 requests/hour)
- Strategies:
    - Implement caching mechanisms.
    - Scale infrastructure resources dynamically.
    - Schedule maintenance outside peak traffic windows.

### 3. Security Enhancements

- Flag and verify suspicious IPs such as 46.105.14.53 and 130.237.218.86.
- Validate the legitimacy of bots (e.g., Googlebot – 66.249.73.135).
- Use reverse DNS, analyze user-agent headers, and apply rate-limiting (e.g., max 300 req/hr/IP).
- Protect POST endpoints against CSRF and injection attacks.

### 4. System and Performance Improvements

- Utilize caching (Redis/Memcached) and CDN services to reduce load time.
- Apply load balancing to evenly distribute requests.
- Enable auto-scaling to manage fluctuating demand.
- Use real-time monitoring tools like ELK Stack or Splunk for efficient log analysis and alerting.

---

## Conclusion

Overall, the Apache server logs demonstrate a stable system with a low failure rate of 2.2%. By addressing the identified error patterns, managing peak traffic more efficiently, and implementing robust security practices, the system's reliability and performance can be further enhanced.