Apache Log Analysis Report

Name: Ahmed Ehab Abdelmoneim

ID: 2205250

Log File: apache_logs

Summary of Findings

This report presents an analysis of the Apache log file apache_logs over a 4-day period, from 17 May 2015 to 20 May 2015. The analysis provides insights into server performance, traffic patterns, user activity, and highlights potential issues such as request failures and security concerns.

Key Output from Bash Script Analysis

- Total Requests: 10,000

- GET Requests: 9,952 (99.52%)

- POST Requests: 5 (0.05%)

- Unique IP Addresses: 1,753

- Failed Requests (4xx/5xx): 220 (2.00%)

- Most Active IPs:

- 66.249.73.135 (482 GET requests)

- 78.173.140.106 (3 POST requests)

- Average Daily Requests: 2,500

- Peak Request Hour: Hour 14 (2 PM) - 498 requests

- Hour with Most Failures: Hour 09 (9 AM) - 18 failures

Detailed Analysis

1. Request Types

GET requests dominated the traffic (9,952 requests), indicating that content retrieval is the primary function of the server. POST requests were minimal (5), with only 3 HEAD requests observed, likely for metadata checks.

2. Unique IPs

A total of 1,753 distinct IP addresses accessed the server during the analysis period, reflecting a varied and widespread user base.

3. Request Failures

There were 220 failed requests (2% of total), with 404 Not Found errors being the most common (213). Other errors included 500 Internal Server Error (3), 416 Range Not Satisfiable (2), and 403 Forbidden (2).

4. Top IP Addresses

The IP 66.249.73.135, likely a web crawler like Googlebot, was the most active. The unusual POST activity from 78.173.140.106 should be monitored.

5. Daily Request Distribution

Traffic ranged from 1,632 to 2,896 requests per day, indicating moderate to high usage.

6. Days with Highest Failure Counts

18 and 19 May had the most failures (66 each), suggesting potential recurring issues.

7. Hourly Request Trends

Highest activity was at Hour 14 (498 requests), and lowest at Hour 08 (345 requests). Failure spikes were observed in the early morning.

8. Status Code Distribution

- 200 OK: 9,126 (91.26%)

- 304 Not Modified: 445 (4.45%)

- 301 Moved Permanently: 164 (1.64%)

- 404 Not Found: 213 (2.13%)

- Other error codes: <0.1%

9. Failure Time Patterns

Failure spikes in Hours 05, 06, and 09 may indicate automated task issues.

10. Request Patterns

Peak activity in afternoons, highest traffic on 19 May, lowest on 17 May.

Recommendations

1. Reducing Failures

Audit links, improve error handling, and check access controls.

2. Critical Time Response

Optimize performance during peak hours and investigate morning failures.

3. Security Measures

Verify high-activity IPs and monitor POST requests. Use WAF and rate limiting.

4. System Improvements

Implement caching, monitoring tools (e.g., Prometheus), and enhance error page management.