Log Analysis Report

By Ahmed Fawzy — 2205156

Overview

This report analyzes Apache server logs to identify request patterns, failure trends, and potential security concerns. Based on the analysis, recommendations are proposed to reduce failure rates, optimize system performance, manage peak traffic periods, and mitigate potential threats.

1. Request Counts

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

2. Unique IP Addresses

- **Total Unique IPs**: 1,753

Examples of GET and POST Requests per IP:

```
100.2.4.116         GET=6, POST=0
100.43.83.137       GET=84, POST=0
101.119.18.35       GET=33, POST=0
101.199.108.50      GET=3, POST=0
101.226.168.196     GET=1, POST=0
103.247.192.5       GET=1, POST=0
```

3. Failure Requests (4xx / 5xx)

- **Total Failed Requests**: 220

- **Failure Rate**: 2.20%

4. Top User

- **Most Active IP**: 66.249.73.135
- **Total Requests**: 482

5. Daily Request Averages

- **Number of Days**: 4,405
- **Average Requests/Day**: 2.27

6. Days with Highest Failures

- **Note**: No specific high-failure days (4xx/5xx) were detected in the logs.

7. Requests by Hour

Hour	Requests
00	361
01	360
02	365
03	354
04	355
05	371
06	366
07	357

8. Request Trends

- **01 → 02**: ↑ Increasing (360 → 365)
- **02 → 03**: ↓ Decreasing (365 → 354)

- **03 → 04**: ↑ Slight Increase (354 → 355)
- **04 → 05**: ↑ Increase (355 → 371)
- **05 → 06**: ↓ Decrease (371 → 366)
- **06 → 07**: ↓ Decrease (366 → 357)
- **07 → 08**: ↓ Decrease (357 → 345)
- **08 → 09**: ↑ Increase (345 → 364)
- **09 → 10**: ↑ Increase (364 → 443)
- **10 → 11**: ↑ Increase (443 → 459)

---

9. Status Code Breakdown

Status Code	Count	Percentage
200	9,126	91.26%
304	445	4.45%
404	213	2.13%
301	164	1.64%
206	45	0.45%
500	3	0.03%
416	2	0.02%
403	2	0.02%

---

10. Most Active IPs by Request Type

- **Most Active GET IP**: 66.249.73.135 (482 requests)
- **Most Active POST IP**: 78.173.140.106 (3 requests)

---

11. Patterns in Failure Requests

- **No failed requests (4xx/5xx)** found within logged hours.

---

12. Recommendations & Analysis

1. Reducing Failures

- **404 Errors (213 occurrences)**
  - Redirect or update broken URLs.
  - Analyze request URLs for misconfigurations.
- **500 Errors (3 occurrences)**
  - Debug server-side issues and enable detailed logging.
- **403 & 416 Errors**
  - Review permissions and test range handling (for large files).
- **Monitoring & Alerts**
  - Set up real-time alerts and use tools like ELK or Splunk for log correlation.

---

2. High-Traffic Days & Hours

- **Peak Hour (14:00–15:00)**
  - Approx. 498 requests/hour
  - Use caching and scale infrastructure resources.
- **May 18–20, 2015 (High Failures)**
  - Investigate for system events or attacks.
  - Avoid maintenance during peak periods.
- **Failure-Prone Hours**
  - 05:00 (15), 06:00 (14), 09:00 (18)
  - Correlate failures with backups or tasks.

---

3. Security Concerns

- **Suspicious IPs**
  - 66.249.73.135: Likely Googlebot. Confirm legitimacy.

    - 46.105.14.53 and 130.237.218.86: Possible scraping/malicious behavior.
- **Mitigations**
    - Reverse DNS lookups, analyze user-agent strings.
    - Apply rate-limiting (e.g., >300 req/hr/IP).
    - Deploy WAF and update server software.
- **Unusual POST Requests**
    - 78.173.140.106 — investigate endpoints and payloads.
    - Harden input validation and CSRF protections.

---

4. System & Service Improvements

- **Caching & CDN**
    - Use Redis/Memcached and external CDNs for speed and offloading.
- **Load Balancing & Auto-Scaling**
    - Spread traffic evenly and dynamically adapt to demand.

Conclusion

The Apache server performs well overall with a low failure rate (2%). However, actionable improvements exist to further increase reliability, performance, and security. Through better error handling, traffic management, and enhanced monitoring, the system can be made more robust and scalable.
