Name: Abdelrahman Ayman Saad Abdelhalim Mohamed Id: 2205033

Log File Analysis

Mentioning to task 3 repository we have log report file

Log Analysis Report & Actionable Recommendations

1. Reducing Failures (Current Error Rate: 3.02%)

Top Error URLs (100% failure rates):

sitemap.xml.gz (586 errors)

/admin.php (239 errors)

/comments/feed (527 errors, 98.5% failure rate)

Status Code Analysis:

404 Not Found: 4,533 (99.6% of all errors)

405 Method Not Allowed: 9

500 Server Error: 6 (critical)

High-Error Periods:

18/00/2011: 40.8% failure rate (481 failures)

15/00/2012: 11.15% failure rate (363 failures)

14/00/2012: 8.67% failure rate (286 failures)

Recommendations:

Fix Broken Resources:

Prioritize fixing /sitemap.xml.gz and /admin.php (100% error rates).

Investigate why /comments/feed and /feed return high 404 rates (potential misconfiguration).

Implement Custom 404 Pages:

Redirect users to relevant content instead of generic 404s.

Monitor 500 Errors:

The 6 server errors indicate backend issues; check application logs for stack traces.

Review API Endpoints:

405 Method Not Allowed errors suggest incorrect HTTP method usage (e.g., POST instead of GET).

2. Critical Days/Times Needing Attention

Traffic Patterns:

Peak Hour: 22:00-22:59 (9,012 requests, 5.97% of daily traffic).

Lowest Hour: 02:00-02:59 (3,902 requests).

High-Failure Hours:

07:00-07:59: 7.71% failure rate (415 failures).

19:00-19:59: 6.13% failure rate (400 failures).

14:00-14:59: 6.79% failure rate (592 failures).

Recommendations:

Maintenance Window:

Schedule deployments/updates during 02:00-03:00 (lowest traffic).

Scale Resources:

Allocate additional servers/autoscaling for 22:00-23:00 peak.

Debug High-Error Hours:

Investigate why failures spike at 07:00, 14:00, and 19:00 (e.g., cron jobs, backup processes

3. Security Concerns & Anomalies

Critical Issues:

Potential DoS Attacks:

76.108.110.119: 10,088 rapid requests (10088/sec).

95.108.151.244: 2,134 rapid requests.

188.40.97.2: 1,527 rapid requests.

Suspicious Activity:

221.224.13.25: 249 suspicious requests (e.g., /admin.php access).

195.238.176.90: 237 suspicious requests.

61.221.28.243: 191 suspicious requests.

Recommendations:

Immediate Actions:

Block IPs with >1,000 rapid requests (e.g., 76.108.110.119).

Rate limiting: 1,000 requests/minute per IP (stricter for /admin* paths).

Long-Term Measures:

Deploy a Web Application Firewall (WAF) to filter malicious traffic.

Monitor /admin.php and /wp-login.php for brute-force attempts.

Enable CAPTCHA for high-risk endpoints.

4. System/Service Improvements

Performance & Reliability:

Caching:

Cache static resources (e.g., /sitemap.xml.gz, /feed).

Implement CDN for assets with high 404 rates.

Error Handling:

Replace broken links with redirects (e.g., /comments/feed → /feed).

Capacity Planning:

Scale horizontally during peak hours (22:00-23:00).

Optimize database queries for high-traffic endpoints.

Security Hardening:

IP Whitelisting:

Restrict /admin.php to trusted IPs.

Logging:

Log all 4xx/5xx errors with request payloads for forensic analysis.

Alerting:

Set up alerts for:

500 errors/day.

IPs with >500 requests/minute.

Key Decisions & Next Steps

Urgent:

Patch /admin.php and disable if unused.

Block DoS IPs (76.108.110.119, 95.108.151.244, etc.).

Short-Term (1-2 Weeks):

Fix high-error URLs (e.g., /sitemap.xml.gz).

Deploy rate limiting and WAF.

Long-Term:

Implement automated scaling for peak traffic.

Migrate to structured logging for better analysis.