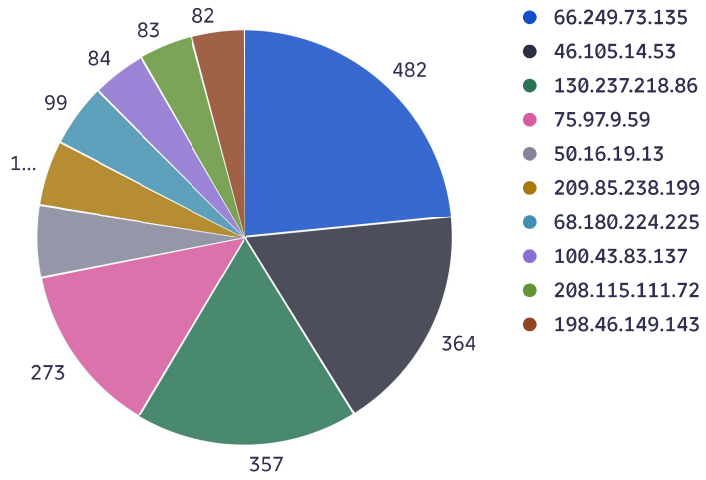
Apache Notebook

Apache logs are records maintained by the Apache HTTP Server to capture details about client requests, server activity, and errors. They are essential for monitoring performance, diagnosing issues, and enhancing security. The two most common types are access logs and error logs. Access logs record every incoming HTTP request, typically stored in /var/log/apache2/access.log on Debian/Ubuntu or /var/log/httpd/access_log on RHEL/CentOS systems. They often use the Common or Combined Log Format, which includes information such as the client IP address, user identity, timestamp, HTTP method, requested resource, protocol version, status code, and response size. The Combined Log Format also logs the referer and user-agent details. Error logs, found in /var/log/apache2/error.log or /var/log/httpd/error_log, store server-related error messages, warnings, and startup/shutdown events. Each entry usually contains the timestamp, module and severity level, process ID, client information, and a descriptive error message. Beyond these, Apache may also produce specialized logs such as mod_security audit logs, virtual host-specific logs, or custom logs defined through configuration directives like CustomLog and ErrorLog. Administrators often use commands such as tail -f to monitor logs in real time, grep to search for specific errors, or awk to analyze request patterns by IP. Together, these logs form a vital part of web server management, enabling proactive issue detection and detailed forensic analysis.

```
fetch logs
| filter matchesValue(log.source, "apache.log")
| parse content, "IPADDR:clientip LD '[' HTTPDATE:date ']' LD:url 'HTTP/' LD SPACE INT
//| filter in (status, Array($Status:noquote))
//| filter status==$Status:noquote
|summarize total_count=count() ,by:{clientip}
| sort - total_count
| limit 10
```

10 records Executed at: 8/12/2025, 20:48:08, Timeframe: 18:48:07 - 20:48:07, Scanned bytes: 5 MB



```
fetch logs
| filter matchesValue(log.source, "apache.log")
| parse content, "IPADDR:clientip LD '[' HTTPDATE:date ']' LD:url 'HTTP/' LD SPACE INT
| parse URL, "LD:referer_domain SPACE"
| parse referer_domain, "DQS:referer_domain"
| parse referer_domain, "'http://'LDATA:referer_dom'.com'"
| fieldsAdd referer_dom = concat("http://",referer_dom,".com")
| filterOut referer_dom=="http://.com"
| summarize error_404_count=countIf(status==404), by:{clientip,referer_dom}
| sort - error_404_count
| limit 10
```

10 records Executed at: 8/12/2025, 20:48:35, Timeframe: 18:48:34 - 20:48:34, Scanned bytes: 5 MB

clientip	referer_dom	error_404_count
75.97.9.59	http://semicomplete.com	6
176.92.75.62	http://www.semicomplete.com	5
130.237.218.86	http://semicomplete.com	4
78.173.140.106	http://www.semicomplete.com	3
89.107.177.18	http://semicomplete.com	2
111.199.235.239	http://semicomplete.com	2
122.166.142.108	http://semicomplete.com	2
193.244.33.47	http://semicomplete.com	2
204.62.56.3	http://semicomplete.com	2
219.64.34.68	http://semicomplete.com	2

```
fetch logs
| filter matchesValue(log.source, "apache.log")
| parse content, "IPADDR:clientip LD '[' HTTPDATE:date ']' LD:url 'HTTP/' LD SPACE INT
|summarize numOf200Errors=countIf(status==200), numOf404Errors=countIf(status==404), n
numOf206Errors=countIf(status==206), numOf403Errors=countIf(status==403) ,by:{clientip
| limit 10
```

10 records Executed at: 8/12/2025, 21:06:21, Timeframe: 19:06:18 - 21:06:18, Scanned bytes: 5 MB