LOGZILLA DOCUMENTATION

Apache

LogZilla App Store application: Apache

LogZilla App Store · Generated May 3, 2026 · logzilla.ai/docs/logzilla-appstore/apache

Overview

Apache HTTP Server is the world's most widely used open-source web server software. Apache provides web serving, reverse proxying, load balancing, and virtual hosting capabilities. Apache is commonly deployed for high-traffic websites and enterprise web applications.

App Function

The Apache app processes web server logs and extracts user tags for web traffic analysis, performance monitoring, and security analysis.

Vendor Documentation

- Apache HTTP Server Documentation (https://httpd.apache.org/docs/)
- Log Files (https://httpd.apache.org/docs/current/logs.html)
- mod_log_config (https://httpd.apache.org/docs/current/mod/mod_log_config.html)

Device Configuration

Configure Apache to send logs to LogZilla via syslog. Add the following to the Apache configuration (e.g., `/etc/apache2/conf-available/logzilla.conf`):

```
# LogZilla Log Format
LogFormat "Site=\"%v\" Server=\"%V\" DstPort=\"%p\" DstIP=\"%A\" \
Src=\"%h\" SrcIP=\"%a\" User=\"%u\" Status=\"%>s\" \
HTTP_Method=\"%m\" User_Agent=\"%{User-Agent}i\" Request=\"%U%q\"" logzilla

# Send to LogZilla (replace with actual server address)
CustomLog "|/usr/bin/logger -t apache_access -n LOGZILLA_IP -P 514" logzilla
ErrorLog "|/usr/bin/logger -t apache_error -n LOGZILLA_IP -P 514"
```

Replace `LOGZILLA_IP` with the LogZilla server address. Enable and restart Apache:

```
sudo a2enconf logzilla
sudo systemctl restart apache2
```

The `Request` field contains the full URI and is included in the message for security analysis but is not extracted as a tag due to high cardinality.

Incoming Log Format

Apache uses space-separated values in its default log format. To use the LogZilla Apache app, the log format must be customized to use key-value pairs as detailed in the Configuration section below.

The customized format provides structured data that enables detailed web traffic analysis and monitoring.

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	Apache	Vendor name for cross-vendor filtering
Product	HTTP Server	Product name for cross-vendor filtering
Event Class	web	Cross-vendor event classification
Site	www.example.com	Site being accessed
Server	web-01	Server hosting the site
DstPort	https	Destination port with service name
DstIP	10.0.0.50	Server IP address
Src	client.example.com	Source hostname or IP
SrcIP	192.168.1.100	Client IP address
User	jsmith	Authenticated username
HTTP Status Code	200 OK	HTTP status code with description
HTTP Method	GET	HTTP request method
Apache Attack Type	SQL Injection	Detected attack type
MitreId	T1190	MITRE ATT&CK technique ID
MITRE Tactic	Initial Access	MITRE ATT&CK tactic
User Agent	Mozilla/5.0	Client user agent string

Log Examples

Successful Request (200)

```
Site="www.example.com" Server="web-01" DstPort="443" DstIP="10.0.0.50"
Src="client.example.com" SrcIP="192.168.1.100" User="jsmith" Status="200"
HTTP_Method="GET" User_Agent="Mozilla/5.0" Request="/index.html"
```

Not Found (404)

```
Site="www.example.com" Server="web-01" DstPort="80" DstIP="10.0.0.50"
Src="192.168.1.100" SrcIP="192.168.1.100" User="-" Status="404"
HTTP_Method="GET" User_Agent="Mozilla/5.0" Request="/missing.html"
```

Server Error (500)

```
Site="api.example.com" Server="api-01" DstPort="443" DstIP="10.0.0.51"
Src="192.168.1.100" SrcIP="192.168.1.100" User="-" Status="500"
HTTP_Method="POST" User_Agent="curl/7.68.0" Request="/api/users"
```

Triggers

Trigger	Description
`Apache: Server Error (5xx)`	HTTP 5xx server errors indicating backend problems
`Apache: Access Forbidden (403)`	Access denied responses
`Apache: Bad Gateway (502)`	Upstream server connection failures
`Apache: Service Unavailable (503)`	Server overload or maintenance
`Apache: Gateway Timeout (504)`	Upstream server timeout
`Apache: Attack Detected`	Any detected attack pattern
`Apache: Path Traversal Attempt`	Directory traversal attack detected

Trigger	Description
`Apache: SQL Injection Attempt`	SQL injection pattern detected
`Apache: Command Injection Attempt`	Shell command injection detected
`Apache: Exploit Path Probe`	Common exploit path probes (phpMyAdmin, wp-admin)
`Apache: Log4Shell Attempt`	Log4j JNDI exploit attempt detected