

LOGZILLA DOCUMENTATION

Webops

LogZilla App Store application: Webops

LogZilla App Store · Generated April 29, 2026 · logzilla.ai/docs/logzilla-appstore/webops

Overview

WebOps provides unified web monitoring across all log sources. Web events from web servers, load balancers, CDNs, and WAFs are aggregated into a single dashboard with consistent severity levels.

App Function

- Aggregate web events from installed vendor apps
- Provide unified dashboard for cross-vendor web visibility
- Assign severity levels based on Event Type and HTTP Status Code
- Alert on HTTP errors and web security events

Vendor Documentation

This is a LogZilla aggregate app. No external vendor documentation applies.

Device Configuration

No device configuration is required. WebOps automatically processes events from any app that sets `Event Class` containing `Web`.

Incoming Log Format

WebOps processes events tagged by vendor apps. It does not parse raw log formats directly. Vendor apps set:

- `Event Type`: Web Security, Web Error
- `HTTP Status Code`: Response status code

Parsed Metadata Fields

Tag Name	Example	Description
<code>WebOps Event</code>	1	Rollup tag for web events

Tag Name	Example	Description
WebOps Severity Level	High	Aggregated severity based on Event Type

Severity Level Assignment

Severity	Condition
Critical	Web Security (WAF blocks, bot detection)
High	Web Error, 5xx server errors
Medium	4xx client errors
Low	2xx successful requests

Log Examples

HTTP 500 Error

```
nginx: 192.168.1.100 - - "GET /api/users HTTP/1.1" 500 0 "-" "curl/7.68.0"
```

WAF Security Event

```
modsecurity: [id "941100"] [msg "XSS Attack Detected"] [severity "CRITICAL"]
```

SSL Error

```
nginx: SSL_do_handshake() failed (SSL: error:1408F10B)
```

Dashboard

The WebOps dashboard provides:

- Key metrics: Total events, web security, web errors
- Unique hosts, status codes, and URIs
- EPS gauge and time chart for rate monitoring
- HTTP Status Code distribution over time
- Top hosts, URIs, and client IPs
- Severity distribution and HTTP methods
- Live event stream with web context

Triggers

Trigger	Description
WebOps: Web Security	WAF block or bot detection
WebOps: Web Error	HTTP or SSL error
WebOps: Server Error	5xx server error