LOGZILLA DOCUMENTATION

Nginx

LogZilla App Store application: Nginx

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/nginx

Overview

NGINX is open-source web server software for web serving, reverse proxying, caching, load balancing, media streaming, and more. NGINX is widely used for high-performance web applications and microservices architectures.

App Function

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

Vendor Documentation

- Configuring Logging (https://docs.nginx.com/nginx/admin-guide/monitoring/logging/)
- Module ngx_http_log_module (http://nginx.org/en/docs/http/ngx_http_log_module.html)
- Logging to syslog (https://nginx.org/en/docs/syslog.html)

Device Configuration

Configure nginx to send logs to LogZilla via syslog. Add the following to `/etc/nginx/conf.d/logzilla.conf`:

```
# LogZilla Log Format
log_format logzilla
    'Site="$server_name" '
    'Server="$host" '
    'DstPort="$server_port" '
    'DstIP="$server_addr" '
    'Src="$remote_addr" '
    'SrcIP="$realip_remote_addr" '
    'User="$remote_user" '
    'Status="$status" '
    'HTTP_Method="$request_method" '
    'User_Agent="$http_user_agent" '
    'Request="$request_uri"';

# Send to LogZilla (replace with actual server address)
access_log syslog:server=LOGZILLA_IP:514,tag=nginx_access logzilla;
error_log syslog:server=LOGZILLA_IP:514,tag=nginx_error warn;
```

Replace `LOGZILLA_IP` with the LogZilla server address. Restart nginx:

```
sudo systemctl restart nginx
```

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

NGINX uses space-separated values in its default log format. To use the LogZilla NGINX 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`	`Nginx`	Vendor name for cross-vendor filtering
`Product`	`Web 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

Tag Name	Example	Description
Nginx 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
Nginx: Server Error (5xx)	HTTP 5xx server errors indicating backend problems

Trigger	Description
`Nginx: Access Forbidden (403)`	Access denied responses
`Nginx: Bad Gateway (502)`	Upstream server connection failures
`Nginx: Service Unavailable (503)`	Server overload or maintenance
`Nginx: Gateway Timeout (504)`	Upstream server timeout
`Nginx: Attack Detected`	Any detected attack pattern
`Nginx: Path Traversal Attempt`	Directory traversal attack detected
`Nginx: SQL Injection Attempt`	SQL injection pattern detected
`Nginx: Command Injection Attempt`	Shell command injection detected
`Nginx: Exploit Path Probe`	Common exploit path probes (phpMyAdmin, wp-admin)
`Nginx: Log4Shell Attempt`	Log4j JNDI exploit attempt detected