LOGZILLA DOCUMENTATION

F5

LogZilla App Store application: F5

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/f5

Overview

F5 BIG-IP is a family of application delivery controllers (ADC) and security products. BIG-IP devices provide load balancing, SSL offloading, web application firewall (WAF), and Global Traffic Manager (GTM) capabilities. Devices generate syslog messages for traffic events, system health, High Availability (HA) status, and hardware alerts.

App Function

- Parse F5 syslog messages in the format `process[pid]: code:severity: message`
- Extract metadata tags for filtering and analysis
- Categorize events by process type (traffic, GTM, HA, audit, system)
- Provide dashboards for monitoring traffic errors, HA status, and hardware
- Alert on critical hardware failures and HA conditions

Vendor Documentation

- F5 BIG-IP Documentation (https://techdocs.f5.com/en-us/bigip.html)
- BIG-IP System Logging (https://techdocs.f5.com/en-us/bigip-15-1-0/external-monitoring-of-big-ip-systems-implementations/configuring-remote-high-speed-logging.html)
- Log Message Reference (https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-13-1-0/5.html)

Device Configuration

Configure F5 BIG-IP to send syslog messages to LogZilla:

Log into the BIG-IP Configuration utility
Navigate to **System > Logs > Configuration > Remote Logging**
Click **Create** to add a new remote logging destination
Configure the following settings:

- **Name**: LogZilla
- **IP Address**: LogZilla server IP address
- **Remote Port**: 514 (or custom syslog port)
- **Protocol**: UDP or TCP

Click **Finished** to save

Verification

Generate test traffic or trigger a configuration change, then verify events appear in LogZilla with the `Vendor` tag set to `F5`.

Incoming Log Format

F5 BIG-IP syslog messages follow this format:

```
process[pid]: code:severity: message
```

- **process** - F5 process name (tmm, gtmd, mcpd, sod, httpd, syslog-ng, alertd)
- **pid** - Process ID
- **code** - 8-character hex message code (e.g., 01220001)
- **severity** - Numeric severity level (0-7)
- **message** - Event description

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`F5`	Vendor name
`Product`	`BIG-IP`	Product name
`Event Class`	`network`	Cross-vendor classification
`MitreId`	`T1078`	MITRE ATT&CK technique ID (security events)
`MITRE Tactic`	`Initial Access`	MITRE ATT&CK tactic
`F5 Process`	`tmm`	F5 process name (tmm, gtmd, big3d, mcpd, sod)
`F5 Event Type`	`tcl_error`	Categorized event type
`F5 Category`	`traffic`	Event category (traffic, gtm, ha, audit, system)
`F5 iRule`	`redirect_http`	iRule name (TCL errors)
`F5 HTTP Event`	`HTTP_REQUEST`	HTTP event type

Tag Name	Example	Description
F5 HA Status	UP	HA heartbeat status
User	admin	Username (audit events)
F5 Action	enabled	Pool member action (enabled, disabled, forced disabled)
SrcIP	192.168.1.100	Source IP address
DstIP	10.1.1.50	Destination IP address
DstPort	443	Destination port

Log Examples

TCL Error (iRule)

```
tmm[1234]: 01220001:3: TCL error: /Common/selectpool_us-east <HTTP_REQUEST>
- no such pool: /Common/web_pool_prod (line 42) invoked from within
"active_members $localpool"
```

SSL Handshake Failed

```
tmm1[5678]: 01260013:4: SSL handshake failed for TCP 192.168.1.100:54321
-> 10.1.1.50:443
```

GTM Monitor Error

```
gtmd[3456]: 011ae044:3: Could not find monitor object 10.1.1.100:443 on
server:vs /Common/dc1-prod-ltm-pair:/Common/https_vs_prod
```

HA Heartbeat

```
sod[5555]: 01140029:5: HA daemon_heartbeat status UP for bigip1.local
```

Audit Login

```
mcpd[2222]: 01070417:6: AUDIT - user admin logged in from 192.168.1.50
```

Hardware Alert

```
alertd[7777]: 010d0001:2: Cpu temperature is too high.
```

MITRE ATT&CK Mapping

Event Type	Technique	Tactic
Admin login	T1078	Initial Access
Admin command	T1059	Execution
SSL certificate errors	T1557	Credential Access
SSL handshake failures	T1573	Command and Control
Connection/pool/HA failures	T1499	Impact
License errors	T1489	Impact

Dashboards

Dashboard	Description
F5 BIG-IP: Overview	All F5 events, category breakdown, top devices
F5 BIG-IP: Traffic & Errors	SSL errors, iRule errors, connection issues
F5 BIG-IP: HA & Health	HA status, hardware alerts, critical events

Triggers

Trigger	Description
F5: CPU Temperature High	CPU temperature too high
F5: Chassis Temperature High	Chassis temperature too high
F5: Fan Speed Low	Fan speed too low
F5: PSU Issue	Power supply issue
F5: Disk Low	Low disk space
F5: Filesystem Read-Only	Filesystem in read-only mode
F5: HA Failure	HA system failure
F5: Cluster Failed	Cluster failure detected
F5: Device Unavailable	Managed device unavailable
F5: Pool Member Down	Pool member or monitor failure
F5: License Error	License not operational
F5: iRule TCL Error	iRule code error
F5: SSL Handshake Failed	SSL/TLS handshake failure
F5: SSL Certificate Error	Certificate verification failure
F5: Connection Error	Backend connection failure
F5: Monitor Error	GTM monitor failure
F5: MITRE ATT&CK Threat Detected	Events with MITRE technique mapping
F5: Admin Login	Admin login (non-notifying)
F5: Admin Command	Admin command (non-notifying)