LOGZILLA DOCUMENTATION

Ibm Datapower

LogZilla App Store application: Ibm Datapower

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

Overview

IBM DataPower Gateway is an enterprise API gateway and security appliance that provides API management, XML/JSON transformation, security enforcement, and integration services. DataPower appliances generate syslog messages for API transactions, security events, authentication, and system operations.

App Function

- Parse DataPower syslog messages in timestamped bracket format
- Extract metadata tags for filtering and analysis
- Categorize events by Event Class (auth, security, network, system)
- Map security events to MITRE ATT&CK techniques
- Provide dashboards for API gateway monitoring
- Alert on XML attacks, authentication failures, rate limits, and SSL errors

Vendor Documentation

- IBM DataPower Gateway Documentation (https://www.ibm.com/docs/en/datapower-gateway)
- DataPower Logging Configuration (https://www.ibm.com/docs/en/datapower-gateway/10.6.x?topic=bcbtlt-creating-log-target-use-udp-forward-entries-remote-syslog-daemon)

LogZilla Configuration

IBM DataPower requires a dedicated syslog port in LogZilla due to its non-RFC timestamp format:

Navigate to **Settings > System > Application Ports**
Set **IBM DataPower syslog port** to a dedicated port (e.g., `5515`)
Click **Save**
The syslog and parser services reload automatically. Both TCP and UDP listeners are enabled on the configured port.

Device Configuration

Configure DataPower to send syslog messages to the dedicated port configured above:

Log into the DataPower WebGUI
Navigate to **Objects > Logging Configuration > Log Target**

Click **Add** to create a new log target
Set **Type** to **syslog-tcp** or **Syslog**
Configure the remote host as the LogZilla server IP address
Set the port to the dedicated port configured in LogZilla (e.g., `5515`)
Add event subscriptions for desired categories
Click **Apply** and save the configuration

Verification

Generate API traffic through the DataPower gateway, then verify events appear in LogZilla with `Vendor` tag set to `IBM` and `Product` tag set to `DataPower Gateway`.

Incoming Log Format

DataPower syslog messages follow this format:

```
<timestamp> [<code>][<category>][<level>] <object>(<name>): <message>
```

- **timestamp** - ISO format timestamp (e.g., 20210415T222042.990Z)
- **code** - Hex message code (e.g., 0x00a60002)
- **category** - Log category (mpgw, xmlparse, ssl, auth, etc.)
- **level** - Log level (info, warn, error, critic, alert, emerg)
- **object** - DataPower object type
- **name** - Object instance name
- **message** - Event description with transaction details

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`IBM`	Vendor name
`Product`	`DataPower Gateway`	Product name
`Event Class`	`security`	Cross-vendor classification
`MitreId`	`T1059`	MITRE ATT&CK technique ID

Tag Name	Example	Description
MITRE Tactic	Execution	MITRE ATT&CK tactic
DataPower Category	mpgw	Log category
DataPower Level	error	Log level
DataPower Object	mpgw	Object type
SrcIP	10.11.66.50	Source IP address (HC)

Log Examples

API Gateway Transaction

```
20210415T222042.990Z [0x00a60002][mpgw][info] mpgw(simple):
tid(35169)[error][10.11.66.50]: Message rejection
```

XML Attack Detection

```
20210415T223737.028Z [0x80e003aa][xmlparse][error] mpgw(simple):
tid(39617)[response][10.11.66.50]: attribute limit exceeded
```

Rate Limit Triggered

```
20210415T222042.990Z [0x80e00183][monitor][error]
monitor-action(simple-monitor-action): tid(35169)[10.11.66.50]:
Message monitor triggers filter
```

MITRE ATT&CK Mapping

Event Type	Technique	Tactic
XML Parse Error	T1059	Execution

Event Type	Technique	Tactic
Auth Failure	T1110	Credential Access
SSL/TLS Error	T1573	Command and Control
Rate Limit/DoS	T1499	Impact
OAuth/JWT Attack	T1528	Credential Access
SAML Attack	T1606	Credential Access

Dashboards

Dashboard	Description
IBM DataPower: Overview	Events, errors, security, sources, MITRE tactics

Triggers

Trigger	Description
`IBM DataPower: MITRE ATT&CK Threat Detected`	Events with MITRE mapping
`IBM DataPower: XML Attack Detected`	XML parsing errors (T1059)
`IBM DataPower: Authentication Failure`	Auth failures (T1110)
`IBM DataPower: Rate Limit Triggered`	DoS/rate limit events (T1499)
`IBM DataPower: SSL/TLS Error`	SSL/crypto errors (T1573)
`IBM DataPower: Critical System Event`	Critical/alert/emergency events

© LogZilla Corporation · logzilla.ai