LOGZILLA DOCUMENTATION

Juniper MX/EX

Rules, dashboards, and triggers for Juniper MX router and EX switch (Junos) syslog events, including alarm, DDoS protection, and routing protocol alerts

LogZilla App Store · Generated September 22, 2026 · logzilla.ai/docs/logzilla-appstore/juniper-mx-ex

Overview

Juniper MX-series routers and EX-series switches run Junos OS and emit syslog for management-plane authentication, configuration changes, routing-protocol state, control-plane DDoS protection, and chassis alarms. These rules parse that general system and routing syslog stream. The security-gateway (SRX) product line has its own app, `juniper_srx`, for `RT_FLOW` session-flow logs, which are not covered here.

App Function

- Parse Junos management-plane audit events: session login/logout, configuration-mode entry/exit, and commit operations
- Parse control-plane DDoS protection policer violations
- Parse unauthorized SNMP community attempts and unconfigured-BGP-neighbor connection attempts, and map them to MITRE ATT&CK
- Parse interface link state and BGP/OSPF routing-neighbor state changes
- Parse chassis alarm set/cleared events (license, protocol feature, and hardware conditions)
- Parse NTP server unreachability (time-sync failure) events
- Classify all of the above with the standard Event Class/Type taxonomy and compliance framework tags
- Provide dashboards for general activity and for security events
- Alert on unauthorized access attempts, DDoS violations, major alarms, and routing/interface state loss

Vendor Documentation

- Overview of System Logging (https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/system-logging.html)
- System Logging on a Single-Chassis System (https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/system-logging-on-a-single-chassis-system.html)
- SNMP Traps Supported by Junos OS (https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/snmp-traps-supported-by-junos-os.html)
- Understand Chassis Alarms (https://www.juniper.net/documentation/us/en/software/junos/chassis/topics/topic-map/chassis-guide-tm-error-handling-alarms.html)
- Configuring System Log Messages and SNMP Traps for LSPs (https://www.juniper.net/documentation/en_US/junos13.1/topics/usage-guidelines/mpls-configuring-system-log-messages-and-snmp-traps-for-lsps.html)
- System Log Explorer (https://apps.juniper.net/syslog-explorer/) (interactive message-ID reference, useful for confirming exact wording per Junos release)

Device Configuration

Configure the MX or EX device to send syslog messages to LogZilla:

```
set system syslog host <logzilla-ip> any any
set system syslog host <logzilla-ip> port 514
commit
```

Messages are recognized by their daemon name and message content (`mgd`, `rpd`, `jddosd`, `snmpd`, `mib2d`, `xntpd`, `vccpd`, `alarmd`, `craftd`). The default (non-`structured-data`) Junos syslog format is parsed; RFC 5424 `structured-data` output is not.

Verification

Log into the device (or wait for a routine commit/login), then confirm events appear in LogZilla with `Vendor: Juniper` and `Product: Junos` tags.

Incoming Log Format

Junos daemons emit `<process>[<pid>]: <MSGID>: <message>` (or, for a few daemons that don't use a formal message ID, plain free-form text). Some deployments have been observed, in the field, to duplicate the hostname ahead of the process name on the wire; the rule handles both forms.

For unconfigured-BGP-neighbor connection attempts, the ephemeral source port suffix (`203.0.113.20+51413`) is stripped from the stored message so that repeated attempts from the same source deduplicate instead of being stored as thousands of unique events.

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`Juniper`	Vendor name
`Product`	`Junos`	Product name (EX and MX cannot be distinguished from this log content)
`Event Class`	`Auth`, `Config`, `Security`, `Network`, `HA`, `System`	Cross-vendor classification

Tag Name	Example	Description
Event Type	Session, Configuration, Threat, Access Control, Interface, Routing	Event subtype
MitreId	T1110	MITRE ATT&CK technique ID
MITRE Tactic	Credential Access	MITRE ATT&CK tactic
Message Type	UI_LOGIN_EVENT, DDOS_PROTOCOL_VIOLATION_SET, bgp_peer_addr_ok, Alarm set	Junos message type identifier (formal MSGID, or literal leading text for daemons without one)
Action	Up, Down, Set, Cleared	State transition or alarm state
User	user1	Management-plane username (HC)
SrcIP	203.0.113.7	Source IP: unauthorized SNMP/BGP connection attempts (HC)
DstIP	198.51.100.10	Destination IP: unauthorized SNMP connection attempts, unreachable NTP servers (HC)
Neighbor IP	10.0.0.1	BGP/OSPF routing-neighbor IP address (HC)
Interface	ge-0/0/1.0	Interface name
BGP AS	65000	BGP peer autonomous system number
Juniper User Class	super-user	Junos login class (RBAC)
Juniper Client Mode	junoscript, netconf, cli	Management channel used for the session
Juniper DDoS Protocol	OSPF:aggregate	Control-plane protocol/exception exceeding its DDoS policer bandwidth

Tag Name	Example	Description
`Juniper Alarm Level`	`Major,Minor`	Chassis alarm severity
`Juniper Alarm Reason`	`BGP Routing Protocol(47) usage requires a license`	Chassis alarm condition text
`Compliance – <framework>`	`1`	Applied per Event Type

MITRE ATT&CK Mapping

Event	MITRE ID	Tactic	Description
`SNMPD_AUTH_FAILURE`	T1110	Credential Access	Unauthorized SNMP community attempt
`bgp_peer_addr_ok` / `bgp_listen_accept`	T1110	Credential Access	Connection attempt from an unconfigured BGP neighbor

Log Examples

Management-plane login

```
mgd[12345]: UI_LOGIN_EVENT: User 'user1' login, class 'super-user'
localre[12345], ssh-connection '', client-mode 'junoscript'
```

Configuration commit

```
mgd[85992]: UI_COMMIT: User 'user1' requested 'commit' operation
(comment: scheduled maintenance)
```

DDoS protection violation

```
jddosd[5678]: DDOS_PROTOCOL_VIOLATION_SET: Warning: Host-bound traffic
for protocol/exception OSPF:aggregate exceeded its allowed bandwidth at
fpc 1 for 4821 times, started at 2026-01-15 08:30:00 CST
```

Unauthorized SNMP community

```
snmpd[5679]: SNMPD_AUTH_FAILURE: nsa_log_community: unauthorized SNMP
community from 203.0.113.7 to 198.51.100.10 (public)
```

Interface link down

```
mib2d[5680]: SNMP_TRAP_LINK_DOWN: ifIndex 512, ifAdminStatus up(1),
ifOperStatus down(2), ifName ge-0/0/12
```

BGP neighbor state change

```
rpd[1829]: RPD_BGP_NEIGHBOR_STATE_CHANGED: BGP peer 192.0.2.1
(Internal AS 65000) changed state from Established to Idle (event Stop)
(instance master)
```

OSPF neighbor down

```
rpd[2001]: RPD_OSPF_NBRDOWN: OSPF neighbor 10.0.0.2 (realm ospf-v2
ge-0/0/1.0 area 0.0.0.0) state changed from Full to Down due to KillNbr
(event reason: interface went down)
```

Chassis alarm set

```
alarmd[5681]: Alarm set: License id=0, color=YELLOW, class=CHASSIS,
reason=BGP Routing Protocol(47) usage requires a license
```

NTP server unreachable

```
xntpd[5682]: NTP Server 192.0.2.50 is Unreachable
```

Caveats

- SrcIP/DstIP/Neighbor IP extraction is IPv4-only. IPv6 unauthorized connection attempts (observed in the field) are still classified, MITRE-tagged, counted in dashboard badges, and matched by triggers, but do not appear in per-IP TopN widgets.
- The xntpd "Unreachable" wording is parsed as observed; a reachability-restored counterpart has not been confirmed on real devices and is not matched.
- Message types whose exact wording could not be verified against real output are intentionally not matched: 802.1X port authentication, LACP and STP state changes, MPLS LSP events, `UI_CFG_AUDIT_*` per-statement configuration audit, and Virtual Chassis member join/leave.
- High-volume internal diagnostics (`ifinfo`/`cprod` PVIDB attribute spam, `cscript` Mist agent bookkeeping, `craftd` "Receive FX" alarm echo lines) are deliberately left untagged.

Dashboards

Two dashboards are included:

- **Juniper MX/EX: Overview** - management-plane activity, config commits, alarm and routing status, top users, and recent events
- **Juniper MX/EX: Security** - unauthorized access attempts, MITRE tactics, DDoS protection violations, and recent security events

Triggers

Trigger	Description
`Juniper MX/EX: MITRE ATT&CK Threat Detected`	Catch-all for MITRE-tagged events
`Juniper MX/EX: Unauthorized Access Attempt`	Unauthorized SNMP or BGP connection attempt
`Juniper MX/EX: DDoS Protocol Violation`	Control-plane DDoS protection policer violation
`Juniper MX/EX: Major Alarm Set`	Major chassis alarm condition

Trigger	Description
`Juniper MX/EX: Routing Neighbor Down`	BGP or OSPF routing-neighbor adjacency lost
`Juniper MX/EX: Interface Down`	Interface link down