LOGZILLA DOCUMENTATION

Juniper SRX Configuration

Configure Juniper SRX devices to forward security logs to LogZilla in RFC5424 sd-syslog structured format using stream mode and a source address

Receiving Data in LogZilla · Generated May 3, 2026 · logzilla.ai/docs/receiving-data/juniper-srx-configuration

Juniper SRX Configuration

Juniper SRX devices should send logs in RFC5424 structured format (key-value pairs) rather than legacy RFC3164. The SRX `sd-syslog` format is recommended.

Prerequisites

- Confirm syslog listener ports on the LogZilla server (see Syslog Settings (https://www.logzilla.ai/docs/administration/syslog-settings)).
- Choose a stable source IP/interface on the SRX for logging.
- Ensure network policy allows the SRX to reach LogZilla on the selected syslog port.

Configure SRX security logging (structured syslog)

Enter configuration mode and apply settings similar to the following. Replace the sample addresses with the correct SRX source and LogZilla destination.

```
edit
set security log mode stream
set security log format sd-syslog
set security log source-address 1.1.1.1
set security log stream logzilla host 10.1.1.2
show | compare
commit check
commit
```

Notes:

- `format sd-syslog` enables RFC5424 structured data.
- `source-address` is the SRX interface address used as the syslog source.
- The `stream logzilla host` command sets the LogZilla destination address.

Verification

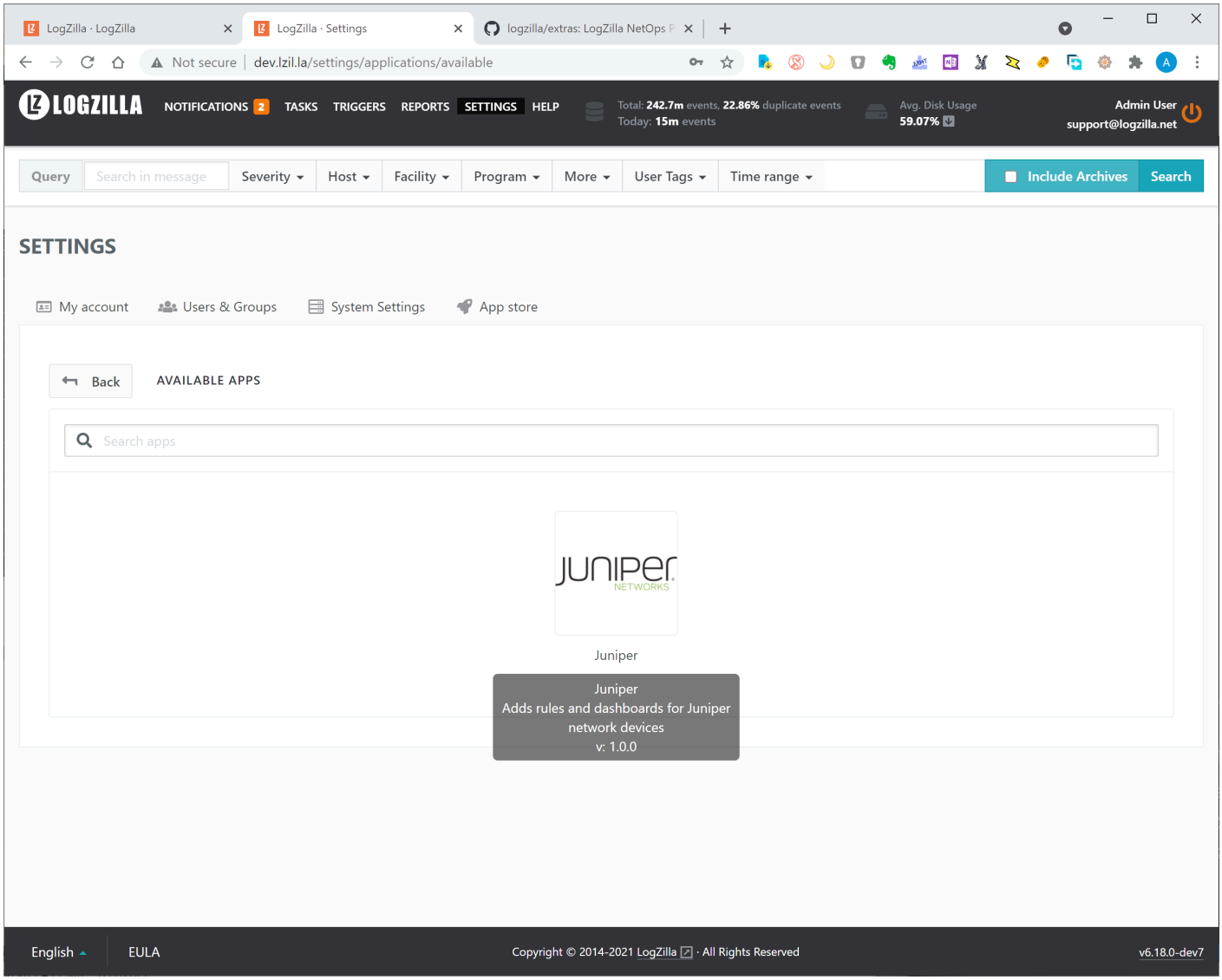
Generate traffic or events that produce logs on the SRX.
In LogZilla, search by host or program to confirm reception. For example:

- `host:"1.1.1.1"` (the configured SRX source address)
- Text from expected messages

For packet-level checks and capture examples, see Syslog Troubleshooting (https://www.logzilla.ai/docs/administration/syslog-troubleshooting).

Juniper appstore rule (optional)

The Juniper appstore rule improves readability and adds user tags for key fields. Install from the `Settings → App store` page.



Related topics

- Syslog Relays (https://www.logzilla.ai/docs/administration/syslog-relays)