LOGZILLA DOCUMENTATION

Arista Eos

LogZilla App Store application: Arista Eos

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

Overview

Arista EOS is the operating system for Arista Networks datacenter and campus switches, including the 7050, 7124, 7280, and 7500 series. EOS generates syslog messages for environmental monitoring, link state changes, routing protocol events, LLDP neighbor discovery, spanning tree transitions, authentication, and access control events.

App Function

Parses Arista EOS switch logs and extracts:

- Environmental monitoring events (system overheat, transceiver alarms)
- Interface state changes (link up/down, line protocol up/down)
- Routing protocol events (BGP, OSPF, ISIS, BFD adjacency changes)
- LLDP neighbor discovery, timeout, and departure events
- Spanning tree topology changes
- IGMP snooping events
- Authentication events (SSH login success/failure)
- ACL permit/deny logging
- MLAG high-availability events
- Port security and DHCP snooping violations

Provides a network overview dashboard and triggers for hardware alarms, routing instability, interface failures, and security events.

Vendor Documentation

- EOS System Event Logging (https://www.arista.com/en/um-eos/eos-system-event-logging)
- EOS Logging of Event Notifications (https://www.arista.com/en/um-eos/eos-logging-of-event-notifications)
- EOS Logging Explained (https://arista.my.site.com/AristaCommunity/s/article/eos-logging-explained)

Prerequisites

LogZilla Dedicated Port

Arista EOS switches emit Cisco IOS-format syslog messages (`%LINK-3-UPDOWN`, `%BGP-5-ADJCHANGE`, etc.) that are indistinguishable from actual Cisco devices. A dedicated port is required to route these events to the Arista parser instead of the

Cisco parser.

Navigate to **Settings > System > Application Ports**
Set **Arista EOS syslog port** to a dedicated port (e.g., `5524`)
Click **Save**
Both TCP and UDP listeners are enabled on the configured port.

Arista Switch Configuration

Configure each Arista EOS switch to send syslog to the dedicated port:

Access the switch CLI via console or SSH

Enter configuration mode:

```
configure terminal
```

Configure syslog server with the dedicated port:

```
logging host <logzilla-ip> <port> protocol udp
logging trap informational
logging facility local0
logging source-interface Management1
```

Replace `<logzilla-ip>` with the LogZilla server IP and `<port>` with the dedicated port configured in step 1 (e.g., `5524`).

Save the configuration:

```
write memory
```

Verification

Generate a link event by toggling an interface (`shutdown` / `no shutdown`), then verify events appear in LogZilla with `Vendor` tag set to `Arista`.

Incoming Log Format

```
%<FACILITY>-<SEVERITY>-<MNEMONIC>: <message text>
```

Field	Description
FACILITY	Subsystem generating the message (e.g., ENVMON, LLDP)
SEVERITY	Numeric severity 0-7
MNEMONIC	Event identifier within the facility
message text	Human-readable event description

Example:

```
%ENVMON-0-SYSTEMOVERHEATWARNING: The system is overheating
```

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	Arista	Vendor identifier
`Product`	EOS	Product identifier
`Event Class`	Network	Event classification
`Event Type`	Interface	Event type within class
`Arista Mnemonic`	LINK-3-UPDOWN	Full EOS mnemonic
`Interface`	Ethernet48	Interface name
`VLAN`	910	VLAN identifier
`Neighbor IP`	10.0.0.1	Routing neighbor IP
`SrcIP`	10.1.1.100	Source IP (auth/ACL events)
`User`	admin	Username (auth events)
`MitreId`	T1110	MITRE ATT&CK technique

Tag Name	Example	Description
`MITRE Tactic`	Credential Access	MITRE tactic

High-Cardinality Tags

The following tags are stored on disk due to high cardinality:

- `SrcIP` - Source IP addresses from auth and ACL events
- `Neighbor IP` - Routing protocol neighbor IP addresses
- `User` - Usernames from authentication events

Log Examples

Environmental - System Overheat Warning

```
%ENVMON-0-SYSTEMOVERHEATWARNING: The system is overheating
```

Environmental - Transceiver Overheat

```
%ENVMON-0-XCVR_OVERHEAT_CRITICAL: Xcvr3 temperature critical
```

LLDP - Neighbor Discovered

```
%LLDP-5-NEIGHBOR_NEW: LLDP neighbor with chassisId "switch-01"
and portId 0011.2233.4455 added on interface Ethernet2
```

IGMP Snooping - No Querier

```
%IGMPSNOOPING-6-NO_IGMP_QUERIER: No IGMP querier detected in
VLAN 910. IGMP report received from 192.0.2.10 on Ethernet48
for 224.0.1.60
```

Spanning Tree - Interface State Change

```
%SPANTREE-6-INTERFACE_STATE: Interface Ethernet24 instance V150
moving from discarding to learning
```

Interface - Link Down

```
%LINK-3-UPDOWN: Interface Ethernet5, changed state to down
```

Routing - BGP Adjacency Change

```
%BGP-5-ADJCHANGE: peer 10.0.0.1 (AS 65001) old state Established
event Stop new state Idle
```

Authentication - Login Success

```
%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success from 10.1.1.100
user admin vty1
```

Authentication - Login Failure

```
%SEC_LOGIN-4-LOGIN_FAIL: Login Fail from 10.1.1.200 user unknown
```

ACL - Packet Denied

```
%ACL-6-ACLLOG: list mgmt-acl denied tcp 10.2.2.2(12345) ->
10.3.3.3(80), 1 packet
```

Dashboards

The Arista EOS Network Overview dashboard provides real-time visibility into switch events including EPS, event class and type distribution, top reporting hosts, interfaces, VLANs, routing neighbors, and a live event stream.

Triggers

Trigger	Description
MITRE ATT&CK Threat Detected	Any event with MITRE technique
System Overheat Warning	ENVMON thermal alerts
BGP Session Change	BGP adjacency state transitions
OSPF Neighbor Change	OSPF adjacency state transitions
Interface Down	LINK/LINEPROTO down events
MLAG State Change	MLAG HA events
Authentication Failure	Login failures (MITRE T1110)
Port Security Violation	Unauthorized device events