LOGZILLA DOCUMENTATION

Cisco Xr

LogZilla App Store application: Cisco Xr

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

Overview

Cisco IOS-XR is the operating system for Cisco service provider routers including the ASR 9000, NCS 5500, NCS 540, NCS 560, and NCS 1000 series. IOS-XR generates syslog messages for interface state changes, BGP/OSPF/LDP/BFD routing protocol events, platform hardware alarms, SSH authentication, and licensing status.

App Function

- Child app of the base Cisco IOS rule
- Refines classification for IOS-XR compound facility mnemonics (ROUTING-BGP, PKT_INFRA-LINK, SECURITY-SSHD, PLATFORM, L2-BFD)
- Extracts XR Node identifier (RP/LC slot) for card-level triage
- Strips XR message prefix (sequence number, hostname, node, timestamp, process) for effective deduplication
- Maps security events to MITRE ATT&CK techniques
- Applies compliance framework tags
- Provides a network overview dashboard
- Triggers on actionable events (BGP/OSPF changes, interface down, hardware alarms, BFD failures, license warnings)

Vendor Documentation

- IOS-XR Logging Services (ASR 9000) (https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/711x/system-monitoring/configuration/guide/b-system-monitoring-cg-asr9000-711x/implementing-logging-services.html)

Prerequisites

The base Cisco IOS app must be installed. It detects IOS-XR messages by the `RP/` or `LC/` node identifier in the syslog message body and routes them to this child app.

Device Configuration

Ensure the base Cisco IOS app is installed in LogZilla.

On each IOS-XR router, configure syslog forwarding:

```
logging <logzilla-ip> vrf default severity informational
logging source-interface MgmtEth0/RSP0/CPU0/0
```

```
logging hostnameprefix <router-name>
```

Verify logging is active:

```
show logging
```

Incoming Log Format

```
<seqno>: <hostname> <node>:<timestamp>: <process>[<pid>]:
%<GROUP>-<SUBFAC>-<SEV>-<MNEMONIC> : <message text>
```

Field	Description
seqno	Sequence number (stripped for dedup)
hostname	Router hostname (stripped - in syslog host field)
node	RP/slot/card/CPU0 or LC/slot/card/CPU0
process	IOS-XR process name (e.g., bgp, ifmgr, ospf)
GROUP	Message group (ROUTING, PKT_INFRA, SECURITY, etc.)
SUBFAC	Subfacility within the group (BGP, LINK, SSHD, etc.)
SEV	Severity 0-7
MNEMONIC	Event identifier

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	Cisco	Vendor identifier
`Product`	IOS-XR	Product identifier
`Event Class`	Network	Event classification

Tag Name	Example	Description
`Event Type`	Routing	Event type within class
`XR Mnemonic`	ROUTING-BGP-5-ADJCHANGE_DETAIL	Full compound mnemonic
`XR Node`	RP/0/RSP0/CPU0	Route Processor or Line Card
`Interface`	TenGigE0/6/0/8	Interface name
`Neighbor IP`	10.0.0.1	Routing neighbor IP
`SrcIP`	10.1.1.100	Source IP (SSH events)
`User`	admin	Username (SSH events)
`MitreId`	T1110	MITRE ATT&CK technique
`MITRE Tactic`	Credential Access	MITRE tactic

High-Cardinality (HC) Tags

- `SrcIP` - Source IP addresses from SSH events
- `Neighbor IP` - Routing protocol neighbor IP addresses
- `User` - Usernames from SSH authentication events

Log Examples

Interface Down

```
384850: GLBR_ASR9K_11 RP/0/RSP0/CPU0:Apr  9 14:12:55.897 CDT:
ifmgr[454]: %PKT_INFRA-LINK-3-UPDOWN : Interface
GigabitEthernet1101/0/0/18, changed state to Down
```

BGP Adjacency Down

```
2151870: DRCK_ASR9K_1 RP/0/RSP0/CPU0:Apr  9 15:32:47.822 CDT:
bgp[1087]: %ROUTING-BGP-5-ADJCHANGE_DETAIL : neighbor 10.51.0.37
```

```
Down - BGP Notification sent, hold time expired
(VRF: default; AFI/SAFI: 1/1, 25/70) (AS: 40317)
```

OSPF Adjacency Change

```
268424: EMRY_ASR9K_50 RP/0/RSP0/CPU0:Apr 10 11:42:28.665 CDT:
ospf[1029]: %ROUTING-OSPF-5-ADJCHG : Process 1, Nbr 10.51.0.47
on TenGigE0/6/0/8 in area 0 from FULL to DOWN,
Neighbor Down: interface down or detached
```

BFD Session Up (from Line Card)

```
268450: EMRY_ASR9K_50 LC/0/6/CPU0:Apr 10 11:55:48.719 CDT:
bfd_agent[123]: %L2-BFD-6-SESSION_STATE_UP : BFD session to
neighbor 10.52.1.138 on interface TenGigE0/6/0/8 is up
```

SSH Authentication Success

```
384918: GLBR_ASR9K_11 RP/0/RSP0/CPU0:Apr  9 15:01:43.543 CDT:
SSHD_[65866]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully
authenticated user 'admin' from '10.1.1.100' on 'vty0'
```

Satellite DOM Sensor Alarm

```
385032: GLBR_ASR9K_11 RP/0/RSP0/CPU0:Apr 10 11:14:52.328 CDT:
sat_chassis_ctrl[1178]: %PLATFORM-SAT_CHASSIS_ENVMON-2-
SAT_DOM_SENSOR_ALARM : [Satellite 1101]: ALARM_LOW alarm SET
for DOM sensor type BIAS and port number 15
```

Dashboards

The Cisco IOS-XR Network Overview dashboard provides real-time visibility into router events including EPS, event class and type distribution, top hosts, XR nodes, interfaces, routing neighbors, and a live event stream.

Triggers

Trigger	Description
MITRE ATT&CK Threat Detected	Any event with MITRE technique
BGP Session Change	BGP adjacency state transitions
OSPF Neighbor Change	OSPF adjacency changes
Interface Down	Link/LineProto down events
Hardware Alarm	Platform/satellite hardware alerts
BFD Session Down	BFD adjacency removals
License Warning	Smart license expiration