LOGZILLA DOCUMENTATION

Cisco Nexus

LogZilla App Store application: Cisco Nexus

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

Overview

Cisco Nexus is a family of data center switches running the NX-OS operating system. These switches provide high-performance Layer 2 and Layer 3 switching for enterprise networks and cloud environments.

App Function

- Parse NX-OS events including authentication, system, network, and security
- Extract metadata tags for filtering and analysis
- Map security events to MITRE ATT&CK techniques
- Provide security-focused dashboard and triggers

Vendor Documentation

- Cisco Nexus 9000 Series NX-OS System Management Configuration Guide (https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/106x/config-guides/sys-mgmt/cisco-nexus-9000-series-nx-os-system-management-configuration-guide-release-106x/m-configuring-system-message-logging.html)

Device Configuration

Configure the Nexus switch to send syslog messages to LogZilla:

```
configure terminal
logging server <logzilla-ip> 5 facility local0
logging level authpriv 5
logging level stp 5
logging level ethport 5
copy running-config startup-config
```

Incoming Log Format

NX-OS messages follow standard Cisco syslog format with mnemonics:

```
%FACILITY-SEVERITY-MNEMONIC: Message text
```

Parsed Metadata Fields

Tag	Example	Description
Vendor	Cisco	Device vendor
Product	Nexus	Product line
Event Class	auth	Event classification (auth, security, network, system)
cisco_mnemonic	STP-2-BRIDGE_ASSURANCE_BLOCK	NX-OS syslog mnemonic (set by base Cisco app)
MitreId	T1110	MITRE ATT&CK technique ID
MITRE Tactic	Credential Access	MITRE ATT&CK tactic
User	admin	Username
SrcIP	192.168.1.100	Source IP address
Interface	Ethernet1/1	Network interface

Log Examples

Authentication Failure

```
Feb 14 00:12:34 nexus-core : 2024 Feb 14 00:12:34 UTC: pam_aaa:Authentication
failed for user admin from 192.168.1.100
```

Bridge Assurance Block

```
%STP-2-BRIDGE_ASSURANCE_BLOCK: Bridge Assurance blocking port Ethernet1/1
VLAN 100
```

System Restart

```
%SYSTEM-5-RESTART: System restarted
```

MITRE ATT&CK Mapping

Event Type	Technique	Tactic
Authentication failures	T1110	Credential Access
ACL denies (scanning)	T1046	Discovery
DHCP snooping/DAI violations	T1557	Credential Access
Port security violations	T1200	Initial Access
STP BPDU Guard	T1499	Impact
Config changes	T1562	Defense Evasion

Dashboards

Dashboard	Description
Cisco Nexus: Security	Auth failures, port security, DHCP snooping, MITRE mapping
Cisco Nexus: Network	Interface events, VPC status, STP events
Cisco Nexus: System	Hardware health, service crashes, config changes

Triggers

Trigger	Description
Cisco Nexus: MITRE ATT&CK Threat Detected	Events with MITRE technique mapping
Cisco Nexus: Authentication Failure	Failed authentication attempts

Trigger	Description
Cisco Nexus: BPDU Guard Violation	STP BPDU guard blocking port
Cisco Nexus: Port Security Violation	MAC address security violations
Cisco Nexus: System Critical Event	Critical system events
Cisco Nexus: Interface Down	Interface state changes