LOGZILLA DOCUMENTATION

Hp Aruba

LogZilla App Store application: Hp Aruba

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

Overview

HPE Aruba Networking (formerly HP ProCurve) provides enterprise network access and switching hardware. The HPE Aruba app processes log messages from HPE Aruba switches running ArubaOS-Switch (formerly ProVision) firmware, extracting event information and creating user tags for security monitoring, network operations, and system administration.

Supported devices include Aruba 2530, 2540, 2920, 2930F, 2930M, 3800, 3810, 5400R zl2 Series, and legacy HPE 3500, 5406zl, 5412zl, 6200yl, 6600, 8206, 8212 Series switches.

App Function

- Parse Aruba syslog messages using numeric event IDs and message patterns
- Extract metadata tags for filtering and analysis
- Categorize events by Event Class (auth, security, network, system)
- Map security events to MITRE ATT&CK techniques
- Provide dashboards for Network, Security, and System monitoring
- Alert on critical security threats, authentication failures, and hardware events

Vendor Documentation

- ArubaOS-Switch Event Log Message Reference Guide 16.10 (https://arubanetworking.hpe.com/techdocs/AOS-Switch/16.10/)
- HPE Aruba Networking Support Services (https://www.hpe.com/us/en/networking/hpe-aruba-networking-support-services.html)
- Aruba Central Configuration Guide (https://support.hpe.com/hpesc/public/docDisplay?docId=a00073063en_us)

Device Configuration

Configure the HPE Aruba switch to send logs to LogZilla:

```
configure terminal
logging <logzilla-ip>
logging severity info
write memory
```

For detailed options, refer to the ArubaOS-Switch Management and Configuration Guide.

Incoming Log Format

Aruba switches send log messages via standard syslog format. The message structure typically follows this pattern:

Primary timestamp and IP - Initial date-timestamp and IP address
Secondary timestamp and IP - Optional second pair (usually within seconds of primary)
Event ID - Aruba-specific numeric event identifier (e.g., "00331")
Category code - Category identifier followed by colon (e.g., "FFI:")
Event details - Descriptive text with event-specific information
Example raw message:

```
Jul 21 10:01:24 192.168.1.24  Jul 21 11:01:21 192.168.1.24 00331 FFI: port 24-High collision or drop rate. See help.
```

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	HPE	Device vendor
Product	Aruba Switch	Device product
Event Class	security	Event classification (auth/security/network/system)
Aruba Category	ARP Protect	ArubaOS-Switch event category
MitreId	T1557.002	MITRE ATT&CK technique ID
MITRE Tactic	Credential Access	MITRE ATT&CK tactic
VLAN	Vlan100	VLAN identifier
SrcIP	192.168.0.1	Source IP address (HC)
User	admin	Username from auth events (HC)

Log Examples

SSH Connection (auth)

```
Jul 20 14:45:40 192.168.1.76 00179 mgr: SME SSH from 192.168.2.235 - MANAGER Mode
```

ARP Protection Violation (security)

```
Jul 15 10:23:45 192.168.1.50 00911 arp-protect: Deny ARP REQUEST
00:11:22:33:44:55,10.0.0.100 port 24 vlan 100
```

Port State Change (network)

```
Jul  2 04:08:40 192.168.1.132 00077 ports: port 4 is now off-line
```

Chassis Event (system)

```
Jul 10 08:15:22 192.168.1.1 00350 chassis: Fan 1 failed
```

Dashboards

Dashboard	Description
HPE Aruba: Network	Port events, STP, routing protocols, VLANs
HPE Aruba: Security	MITRE threats, auth failures, users, source IPs
HPE Aruba: System Health	Chassis, stack/VSF, NTP, SNMP events

Triggers

Trigger	Description
`HPE Aruba: MITRE ATT&CK Threat Detected`	Security event with MITRE technique mapping
`HPE Aruba: ARP Spoofing Detected`	ARP protection violation (T1557.002)
`HPE Aruba: Authentication Failure`	802.1x or credential failure (T1110)
`HPE Aruba: Unauthorized Device`	MAC lock or rogue device (T1200)
`HPE Aruba: Network DoS Detected`	Flood or DoS attack (T1499)
`HPE Aruba: Port State Change`	Port online/offline events
`HPE Aruba: Spanning Tree Event`	STP topology changes
`HPE Aruba: Chassis Alert`	Hardware failure or status change
`HPE Aruba: Stack/VSF Event`	High availability state change

Event Class Mapping

Event Class	Aruba Categories
`auth`	802.1x, Authentication, SSH, Telnet, Console, Manager, RADIUS, TACACS
`security`	ARP Protect, ARP Throttle, MAC Lock, Loop Protect, BPDU, ACL, MACsec
`network`	Ports, Spanning Tree, OSPF, BGP, VLAN, LACP, LLDP, VRRP, PIM, IGMP
`system`	Chassis, System, Stacking, VSF, Fault, Licensing, Update, NTP, SNMP