Vendor-specific logs are logs generated by devices or systems that are unique to a particular manufacturer.

Logs contain details about specific vendor's hardware or software.

Used to check health, performance, and security of network devices, servers, or applications

These logs are used to record detailed information about the operation, status, and events within the system.

Vendor-Specific Log Format:

1. **Timestamp**: Date and time of the event occurred.
2. **Severity Level**: Indicates the importance of the event (e.g., info, warning, critical, error).
3. **Event ID**: A unique identifier for the event type.
4. **Device Name/ID**: Identifies which device generated the log.
5. **Description**: Detailed description of the event or issue.
6. **Source/Destination IP**: The IP addresses involved in the event (useful in security logs).
7. **Process/Service Name**: The component responsible for generating the log.

Cisco Log:

Cisco devices - routers , switches

Sample Log:

%SYS-5-RELOAD: Reload requested by console. Reason: Configuration change.

Fortinet Logs:

Fortinet firewalls – We capture security events like intrusion detection, VPN activity, or firewall rule from their logs.

date=2025-08-07 time=12:34:56 devname="FGT-60D" devid="FGT60FTK19030376" eventtime=1596823496

logid="0419016247" type="utm" subtype="ips" eventtype="attack" level="alert"

vd="root" srcip=192.168.1.100 srcport=12345 dstip=192.168.2.100 dstport=80

Dell Logs:

Provides logs of real-time hardware status for devices

[Server Name] iDRAC: Event Type: System Event

Timestamp: 2025-08-07 10:00:00

Description: Power Supply 1 Degraded

Severity: Critical

HP Server Logs:

[Date] Server: [Server Name] - Critical event: Temperature exceeded threshold. CPU temperature: 85°C.

To access different vendor specific logs, we need to centralize logs.

Combine vendor-specific logs with other system logs (e.g., firewall, application) to get a detailed view of system health and security.

We can use Syslog servers or SIEM systems to aggregate logs from all devices.

Advantages:

1. Optimized for specific Vendor's Hardware/Software
2. Detailed Diagnostic Data
3. Enhanced Security and Monitoring
4. Event Handling
5. Better Integration with Vendor's Management Tools
6. Efficient Troubleshooting

Disadvantages:

1. Lack of Interoperability
2. Vendor Lock-in
3. Learning Multi-Vendor Environment is difficult.
4. Limited documentation we cannot get details from outside.
5. Vendor's Support dependency.