## Onboarding Network Devices via Syslog Server

1. **Prerequisites**

* + Microsoft Sentinel workspace deployed and connected to a Log Analytics workspace.
  + A Linux-based Syslog server.
  + Network devices capable of sending logs via Syslog.
  + Port UDP/514 or TCP/514 open between the network devices and the Syslog server.
  + Azure Monitor Agent (AMA) or Log Analytics Agent installed on the Syslog server.

2. **Configure Network Devices to Send Syslog**

* **For each network device:**
* Access the device’s logging configuration (CLI or GUI).
* Set the Syslog destination IP to the Syslog server’s IP.
* Set the port to 514 (UDP or TCP as per your setup).
* Choose the appropriate severity level (e.g., informational, warning, error).

3. **Install and Configure Azure Monitor Agent (AMA)**

**a. Install AMA:**

* Follow Microsoft’s official guide: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-install-linux

b. **Connect to Log Analytics Workspace:**

* Use the azcmagent tool or Azure portal to connect the Syslog server to your Sentinel workspace.

4. **Configure Data Collection Rules (DCR)**

* In Azure Portal:

- Go to Microsoft Sentinel > Configuration > Data connectors.

- Select Syslog.

- Click Open connector page.

- Create a Data Collection Rule (DCR):

- Select the Syslog server.

- Choose the facilities and severity levels to collect.

- Map to appropriate tables (e.g., Syslog, CommonSecurityLog).

5. **Validate Log Ingestion**

* On the Syslog server, check incoming logs:

tail -f /var/log/syslog

* In Sentinel, go to Logs and run a query:

Syslog

| where TimeGenerated > ago(1h)