
📝 Cheat Sheet: Onboarding Log Sources into Sumo Logic

Objective: Quickly explain how to bring logs from a customer's environment into Sumo Logic for monitoring and analysis.

---

1. Understand the Flow

Think of onboarding logs as a **3-step journey**:

1. **Collect** → Get the logs from the customer's systems.
2. **Send** → Forward them securely into Sumo Logic.
3. **Parse & Store** → Organize them in Sumo Logic so they're usable.

---

2. Choose a Collector

- **Installed Collector (Agent)**
  - Runs on a customer's server/VM.
  - Best for on-premise logs (Windows, Linux, apps).
- **Hosted Collector (Cloud)**
  - Created inside Sumo Logic's cloud (no agent).
  - Best for cloud-native sources like AWS CloudTrail, Azure Event Hub, GCP Pub/Sub, SaaS logs.

👉 Rule of Thumb:

- On-prem logs → Installed Collector.
- Cloud logs → Hosted Collector.

---

3. Adding a Hosted Collector (Linux Example)

If you want to pull logs from a Linux system into Sumo Logic via a **Hosted Collector**, follow these steps:

1. **Create the Hosted Collector in Sumo Logic UI**
   - Go to **Manage Data > Collection > Collectors > Add Collector**.
   - Select **Hosted Collector**.

   - Give it a name and save.

2. **Add a Source to the Hosted Collector**
   - Example: If you want to stream syslogs, select **Syslog Source**.
   - Or for cloud integrations, pick AWS, Azure, GCP sources.

3. **(If using a Linux Instance to push logs)**
   - Install the Installed Collector (agent) on Linux and configure it to send logs to the Hosted Collector.
   - **Steps to install the collector on Linux:**
   - # Download the collector installer
   - wget https://collectors.sumologic.com/rest/download/linux/64 -O SumoCollector.sh
   -
   - # Make it executable
   - chmod +x SumoCollector.sh
   -
   - # Run installer
   - sudo ./SumoCollector.sh -q -Vsumo.accessid=<ACCESS_ID> -Vsumo.accesskey=<ACCESS_KEY> -VsyncSources=/path/to/sources.json -Vsources=""
   -
   - # Verify collector is running
   - sudo systemctl status collector
   - Replace <ACCESS_ID> and <ACCESS_KEY> with your Sumo Logic API credentials.

4. **Verify in Sumo Logic UI**
   - Go back to **Manage Data > Collection** and check that logs are flowing.

---

4. Configure Metadata (Organize Your Logs)

Metadata tags = labels that help you search later. Common tags:

- _sourceCategory → logical grouping (e.g., Apache/Prod or Firewall/Edge).
- _sourceHost → hostname of the system.
- _sourceName → actual log file name or stream.

👉 Pro Tip: Consistent naming makes searching & dashboards easier.

---

5. Verify & Parse Logs

- Once logs start flowing, check them in **Log Search**.
- Apply or edit **parsing rules** (e.g., JSON, CSV, regex) to turn raw logs into structured fields.
- Parsed logs = easier searches, alerts, and dashboards.

---

6. Enable Security & Alerts

- Ensure TLS encryption for collectors.
- Set up alerts to notify teams if a collector stops sending logs.

Onboarding Log Sources to Sumo Logic (Linux Collector Example)

This guide explains how to onboard log sources from a customer's environment into Sumo Logic using a **Hosted Collector** installed on a Linux instance. It covers both installing the collector and adding a log source (Syslog) for collection.

Lab 1: Install the Linux Collector

A **Collector** is an agent that gathers logs and metrics from your environment and sends them securely to Sumo Logic. On Linux, we install a Hosted Collector using the Sumo-provided installation script.

Steps:

1. **Open a terminal session** on your Linux host (64-bit).
2. **Download the latest Collector package**:
3. wget "https://collectors.sumologic.com/rest/download/linux/64" -O SumoCollector.sh && chmod +x SumoCollector.sh

4. **Run the installer with your details**:
5. sudo ./SumoCollector.sh -q \
6. -Vcollector.name=Training-admin-<YourInitials> \
7. -Vsumo.token_and_url=<Token>
    - Replace <YourInitials> with your initials.
    - Replace <Token> with your **Collector Registration Token** from the Sumo UI.

Example:

```
sudo ./SumoCollector.sh -q \

-Vcollector.name=Training-admin-JWM \

-Vsumo.token_and_url=XXXXXXXXXXXXXXXX
```

🔹 The -q flag ensures a **quiet installation** (no prompts).

8. **Verify installation**:
   Make note of the **Collector Name** (e.g., Training-admin-JWM). You will need this later to configure log sources.

✅ At this point, your Collector is installed and ready to receive logs.

Lab 2: Add a Source (Syslog)

A **Source** tells the Collector *what logs to collect*. Here, we'll configure it to collect Linux syslog data.

Steps:

1. In the **Sumo Logic UI**, click **Configuration → Collection**.
2. Locate the Linux Collector you just installed.
3. Click **Add → Add Source**.
4. Choose **Local File** as the Source type.
5. Provide details:
    - **Name**: A unique identifier for the source.
      Example: RS-labs-linux-messages (use your initials for clarity).
    - **File Path**:
    - /var/log/syslog

  - **Source Category**:
  - labs/Linux/messages

⚡ Best Practice: Use a structured naming convention for Source Categories (e.g., environment/os/component).

6. Click **Save**. Your Linux syslog source is now added.

Verify Log Ingestion

You can verify that logs are flowing in two ways:

1. Live Tail

- Go to **Live Tail** in Sumo Logic.
- Run:
- _sourceCategory=labs/Linux/messages
- You should see logs streaming in real time.

2. Log Search

- Go to **Log Search**.
- Run:
- _sourceCategory=labs/Linux/messages
- You'll see stored syslog events from your Linux machine.
