SumoLogic Log Collectors:

## 1. Installed Collectors

These are locally installed agents that run on your own infrastructure (servers, VMs, containers, etc.).

- Installed on Windows or Linux machines.
- Can collect local log files, system metrics, and application logs.
- Can run source types like:
    - Local file source
    - Syslog source
    - Script source
    - Docker or Kubernetes logs

- Data is encrypted and securely sent to Sumo Logic Cloud.
- Useful when your system is behind a firewall or not directly exposed to the internet.

2. Hosted Collectors:

These are cloud-based collectors hosted directly in the Sumo Logic Cloud — no installation required.

- Fully managed by Sumo Logic.
- You just configure data sources that push data via:
    - HTTP Source (via API or webhook)
    - Cloud-to-cloud integrations (e.g., AWS CloudTrail, Azure Monitor, GCP Stackdriver)
- Ideal for cloud-native and SaaS-based environments.

Example:

AWS → CloudTrail logs → HTTP Source in a Hosted Collector

Cloud services (AWS, Azure, GCP)

SaaS applications (Okta, Salesforce, etc.)

Systems that already support HTTP/S endpoints or API-based log export

3. Cloud Collectors:

A **Cloud Collector** is created and managed within the **Sumo Logic UI** or via **API**.
Each collector can have one or more **Sources** that define **what data is being collected**.

No installation or maintenance
Scalable and serverless
Secure HTTPS data transfer
Ideal for multi-cloud or SaaS environments

Easier setup for remote or distributed systems