



Introduction

Architecture

Data flows

Ingestion Path

Search Path

Kind of data Sumo Logic ingest

Architecture

▼ Cloud-Native

- Built in AWS from the start
- Leverages powerful AWS services to their fullest potential
- Partnership with AWS
- We monitor availability and performance 24/7 and make constant improvements

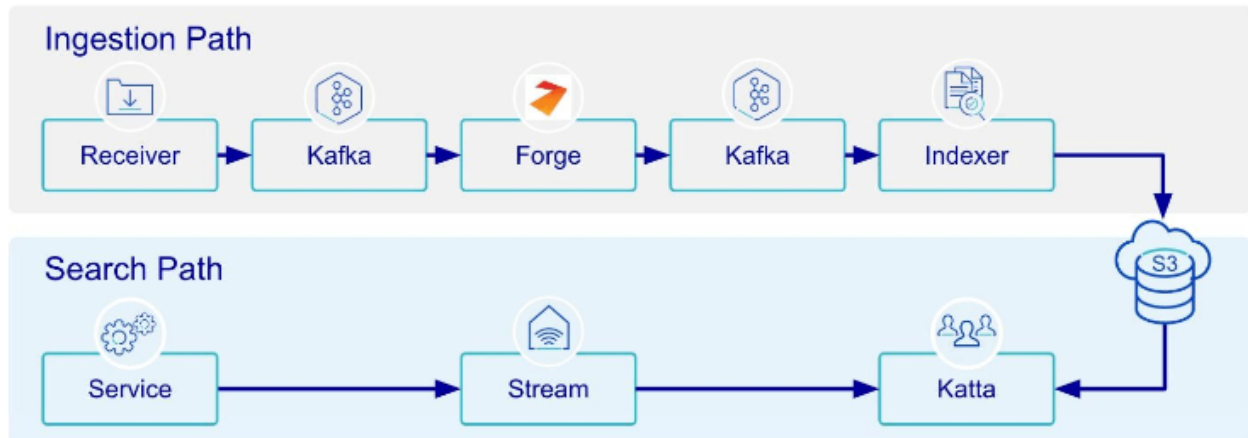
▼ Microservices

- Autoscaling
- Teams at Sumo Logic push software daily
- Increased reliability due to smaller failure domains and availability zone distribution

▼ Multi-tenant

- Resources are shared
- Headroom to scale on short notice
- Adapts to load dynamically

Data flows



Ingestion Path

- Before logs can be searched, the data has to be **ingested** by Sumo Logic.
- Data arrives at The receiver where a pile of messages is created.
 - This pile is uploaded to raws S3 storage and pointers are queued to a streaming process that uses Apache Kafka and Forge
 - This combination provides distributed event store and stream-processing management.
- Once data is ingested in Sumo Logic, it is organized and indexed, then it's ready to be searched.

Search Path

- A search event starts when services ask to execute query
 - Uses Kafka Stream to find indexes matching time range
- The results are processed through the remainder of the aggregations.

Kind of data Sumo Logic ingest

- **Logs:** Identifies why it's happening
- **Metrics:** Identifies what's going on
- **Traces:** End to end visibility into user transactions across services

- **Collection:** Sumo Logic can collect all your logs and metrics, and put them in one place.