# Build Operational Analytics Pipeline on AWS Modern Data Architecture

This architecture enables customers to perform operational analytics in batch and real-time using log information from operational data sources. Operational insights are visualized using an OpenSearch Dashboard and alerts are distributed using Amazon Simple Notification Service (Amazon SNS).
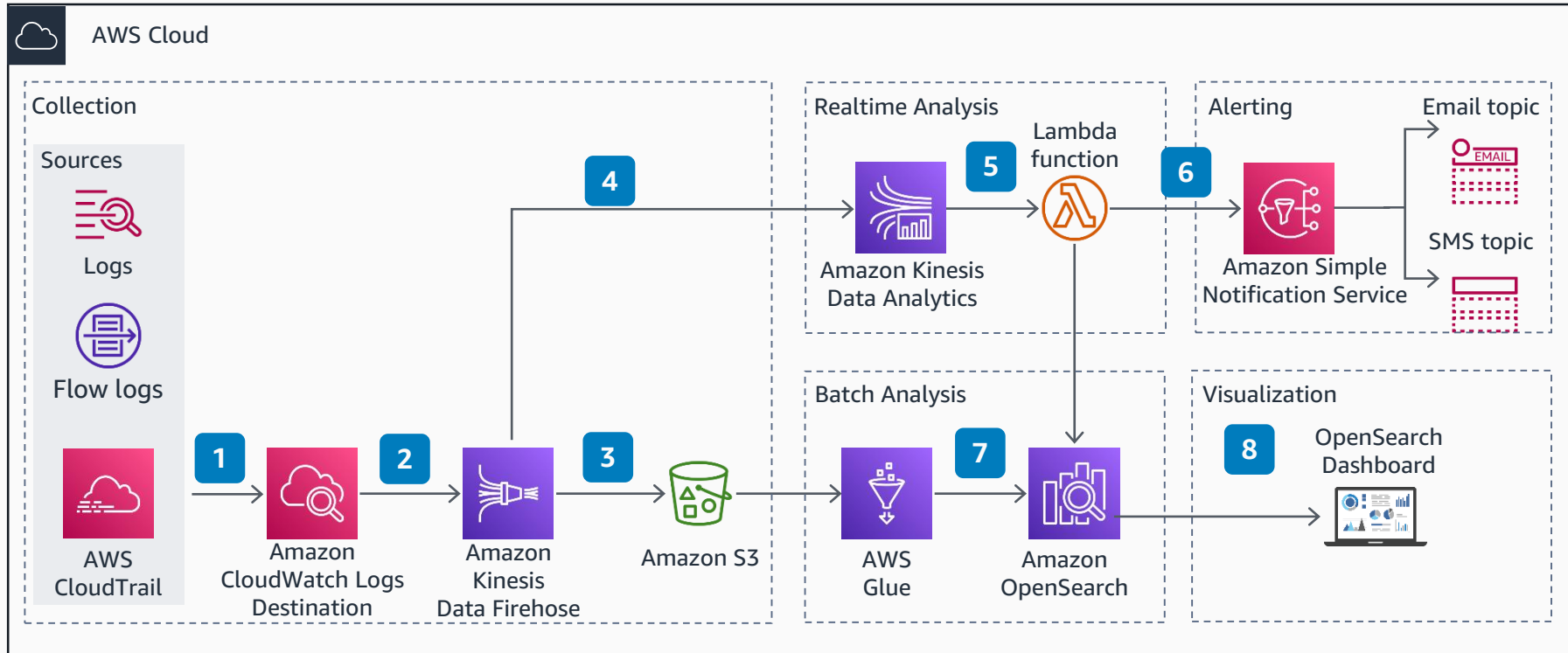
1 Logs are streamed to **Amazon CloudWatch** from various data sources.

2 Amazon CloudWatch subscription filters stream log data to **Amazon Kinesis Firehose** for distribution.

3 Logs intended for Batch Processing are delivered to an **Amazon Simple Storage Service (Amazon S3)** bucket. It will serve as a back up for storing the raw logs.

4 Logs intended for Realtime Analysis are delivered to **Amazon Kinesis Data Analytics**.

5 **Amazon Kinesis Data Analytics** derives metrics, which are sent to a Lambda function for processing. The Lambda function transforms the metrics and ingests them into **Amazon OpenSearch**. If a condition is met that requires alerting, the Lambda function will publish a message to the **Amazon Simple Notification Service (Amazon SNS)** for distribution.

6 **Amazon Simple Notification Service** notifies consumers of the alerts by publishing the alert to an Email and SMS notification topics.

7 **AWS Glue** collects the logs from **Amazon S3** and performs bulk processing, transformation and analysis. AWS Glue uses the Amazon OpenSearch connector to ingest the results into **Amazon OpenSearch**.

8 An OpenSearch Dashboard is used to visualize the metrics from **Amazon OpenSearch**.

AWS Reference Architecture