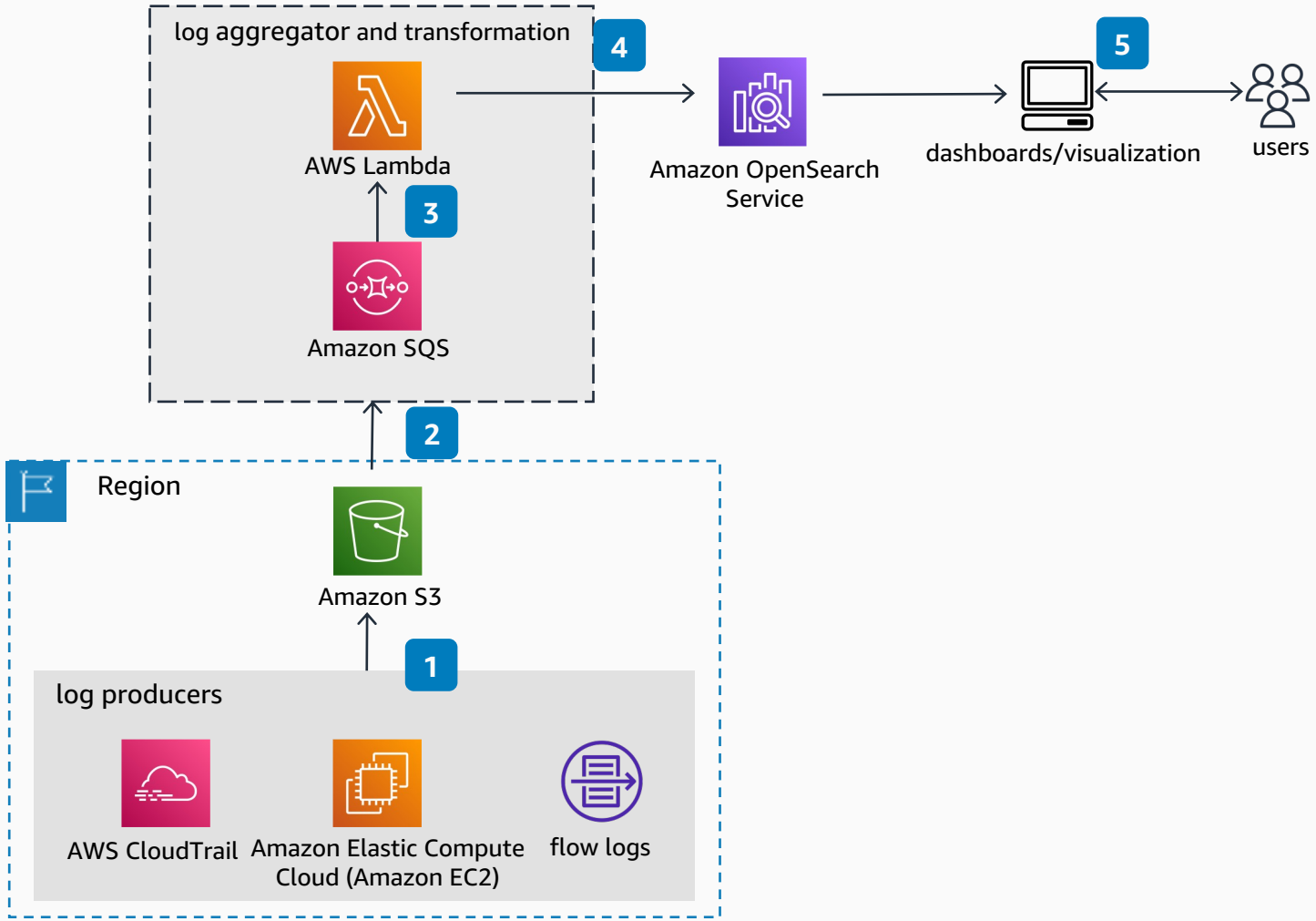
Centralized Log Analytics

Log analytics involves searching, analyzing, and visualizing machine data generated by IT systems and technology infrastructure to gain operational insights. The challenge is knowing which tool to choose for the job. This high-level architecture outlines the different stages of log flow and which tools could be used when.



1. Collectors such as FluentBit, **Amazon Kinesis Agent**, and **Amazon CloudWatch Agent** or services such as **AWS CloudTrail** collect log lines and store them in **Amazon Simple Storage Service** (Amazon S3).
2. **Amazon S3** sends an object create event to **Amazon Simple Queue Service** (Amazon SQS).
3. **Amazon SQS** invokes an **AWS Lambda** function that transforms the log lines from strings to structured JSON (if necessary).
4. The **Lambda** function uses the **OpenSearch** _bulk API to deliver the JSON-formatted log lines to **Amazon OpenSearch Service**.
5. The user logs into **OpenSearch Dashboards** to perform interactive log analytics, build visualizations or notebooks, and monitor their dashboards.

Reviewed for technical accuracy November 7, 2022

AWS Reference Architecture