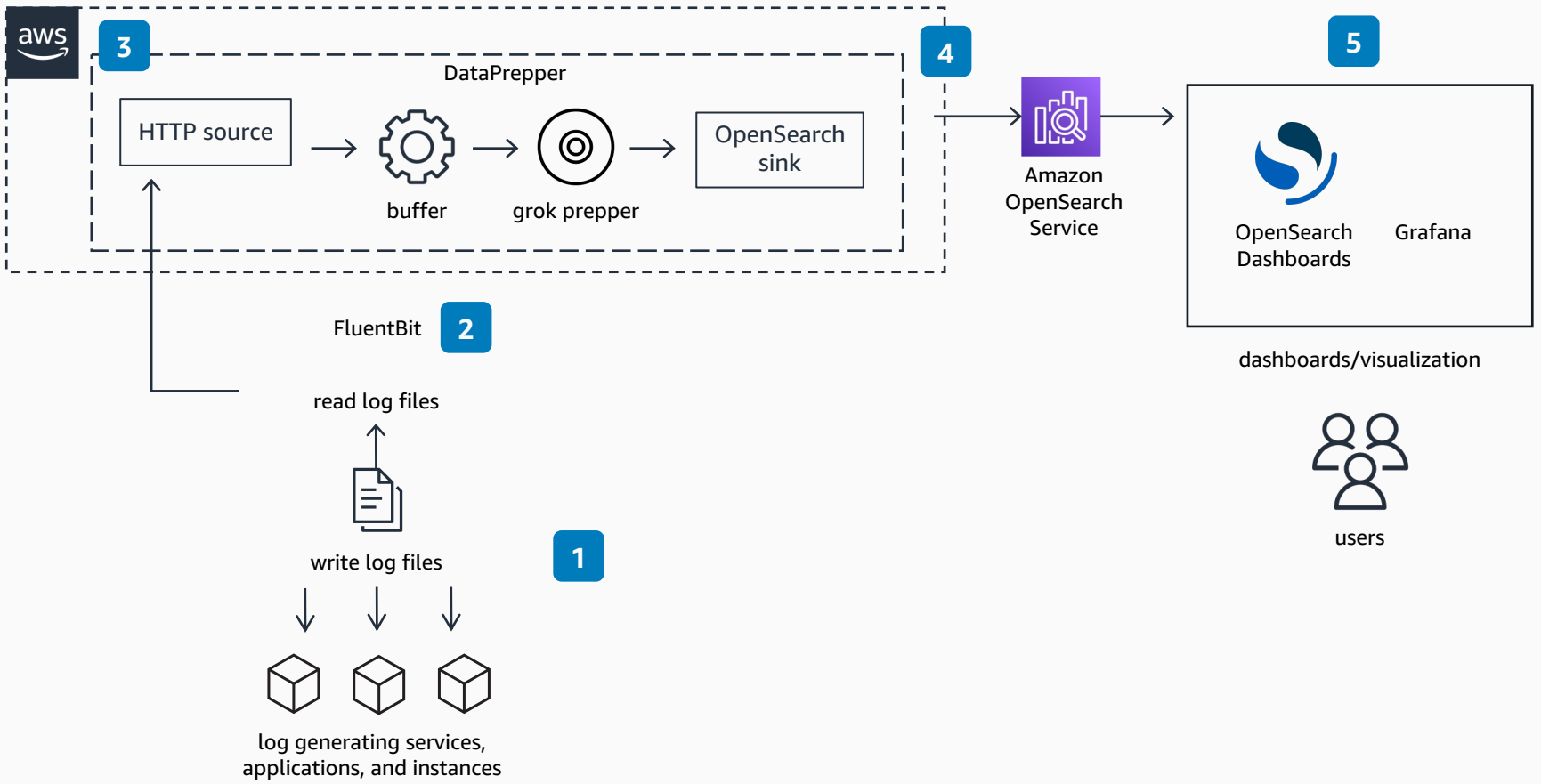
Log Analytics with Open Source Patterns

This diagram shows an architecture using FluentBit and Data Prepper to collect, aggregate, and transform logs into OpenSearch.



1. The application, container system, and associated services generate logs. These can include Docker containers, Kubernetes pods, **Amazon Elastic Compute Cloud** (Amazon EC2) instances, **Elastic Load Balancer** (ELB) logs, **AWS Lambda**, relational database systems, and so on.

2. FluentBit, a popular Apache-licensed log forwarder, reads the log files and forwards them to Data Prepper over HTTP.

3. Data Prepper is a server-side data collector capable of filtering, enriching, transforming, normalizing, and aggregating data for downstream analytics and visualization. Data Prepper receives the logs, buffers them, then optionally structures the data through a grok prepper.

4. Data Prepper creates the service map and assembles the traces into trace groups. It then sends the log lines, formatted for easy searching and analysis, to **Amazon OpenSearch Service**.

5. The user logs into OpenSearch Dashboards (or another open source visualization tool like Grafana) to do interactive log analytics.

Reviewed for technical accuracy December 13, 2022

AWS Reference Architecture