Loki: like Prometheus, but for logs

Loki, started by Grafana Labs in 2018, is an open-source, horizontally-scalable log aggregation system. The demand for a tool like Loki arises from the complexities encountered in modern distributed environments, where logs are generated by numerous components spread across multiple nodes. It differs from other log aggregation systems by not doing full-text indexing and instead stores compressed, unstructured logs and only indexes metadata (e.g., labels and timestamps). This approach optimizes storage efficiency and cost-effectiveness while still providing rapid and accurate log querying capabilities. [1][2]

In a presentation [3] given by Red Hat OpenShift developers, they describe their decision to move from using Elasticsearch, Fluentd, and Kibana to using Loki and Vector:

1. Loki uses a similar query language to Prometheus, enabling it to switch between metrics and logs using the same labels easily.
2. The way that Loki uses memory vie chunking is a lot more efficient, allowing for faster queries.
3. There are a lot of native plugins for Loki and Vector that they could utilize, and there's a lot more integration with third-party components.

Loki is most related to monitoring and Kubernetes labs. Logs are stored locally on nodes and can be fetched and aggregated on demand. But logs are often lost when a pod or node disappears, which is often one of the first triggers for a buyer to realize they need log aggregation.

References:

[1] https://github.com/grafana/loki

[2] https://docs.google.com/document/d/11tjK_lvp1-SVsFZjgOTr1vV3-q6vBAsZYIQ5ZeYBkyM/view

[3] https://www.youtube.com/watch?v=QZ4Hv85lEJ0&t=938s