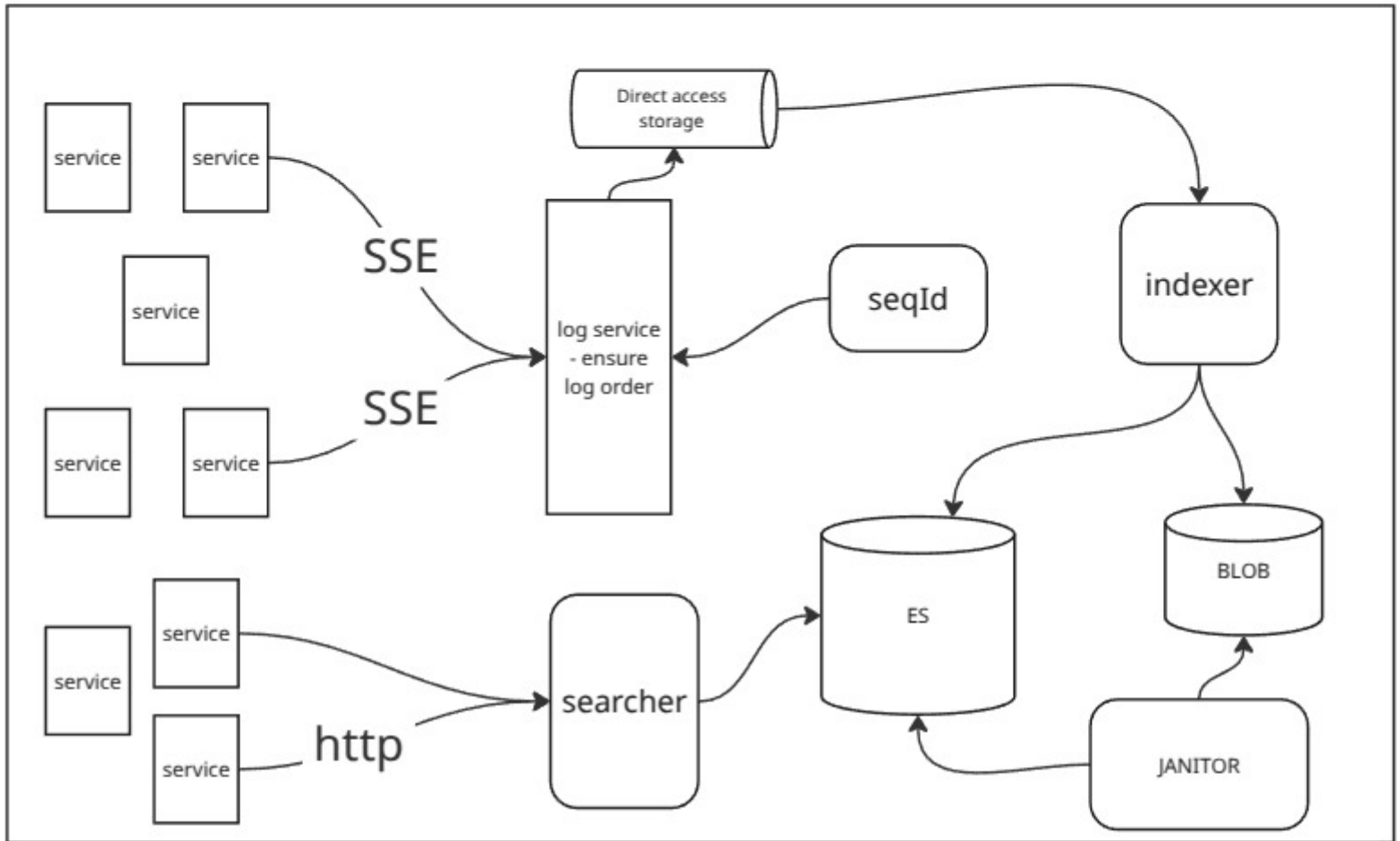


requirements:

- consume logs from diff services
- maintain log order
- make log searchable
- search by: (time, service, content)
- rollover



open questions

- is it http or rest
- why sse? what is the benefit and why udp?
- why introduce a log service? why not push to kafka directly?
- how message in-order is ensured? it is so far sequenced by the time of arrival
- use NTP to sync systems for time