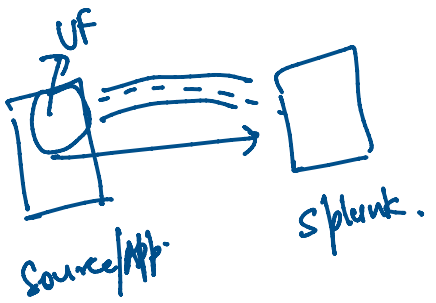
Day - 1

10 August 2024 11:51

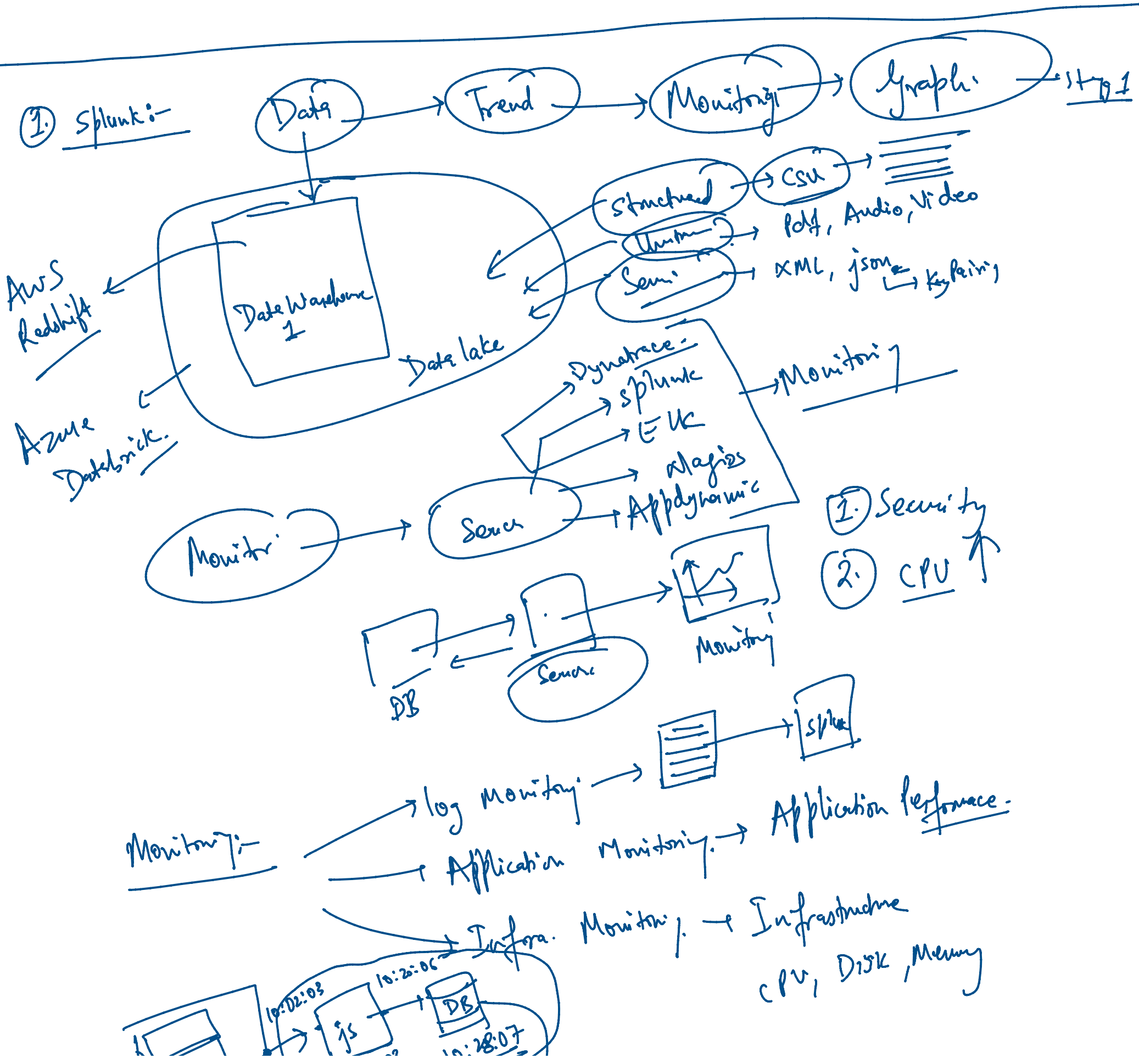
1. Splunk Intro.

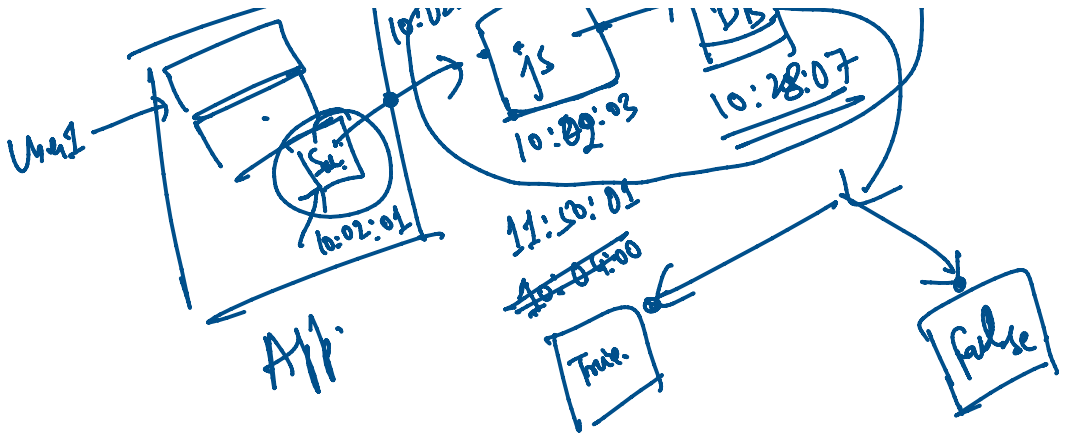
2. Splunk Component
   - forwards
   - Indexer
   - SearchHead
   - LicenseMaster
   - Cluster Master
   - Deployer
   - Deployment Server.
   - Search Head Captain

3. Splunk UF to Indexer
   1. Installation
   2. Config.
   3. Forward Data.
   4. Troubleshooting → logs
      → Commands / connection



1. Splunk:-





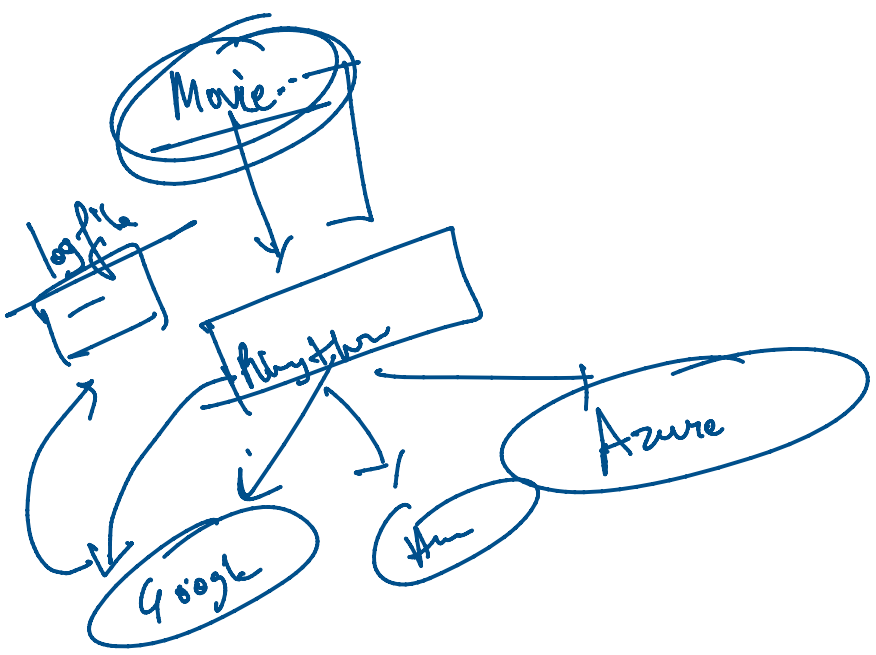
Splunk :- Dashboard, Alert, Report, Knowledge object, Predict, ML TK → ML Toolkit

9.0.2

cloud
SRE/Devops
Cybersecurity
Data Engineering
Machine learning

Adv. :-

1. All the component coming in single package.
2. Learning Curve. SPL → Search Process Language → MySQL
3. Customer support.
4. Any Source / Any type of Data

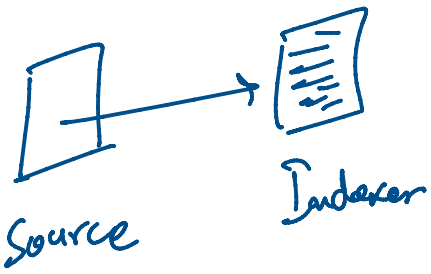


Dis Adv. :-

1. Costly ↑

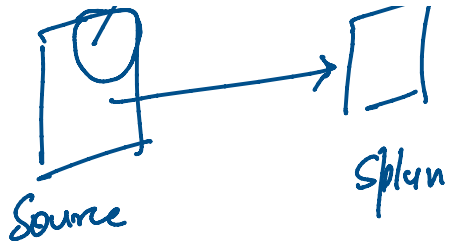
Components of Splunk :-

1. Indexer's Database where the data from source is saved.



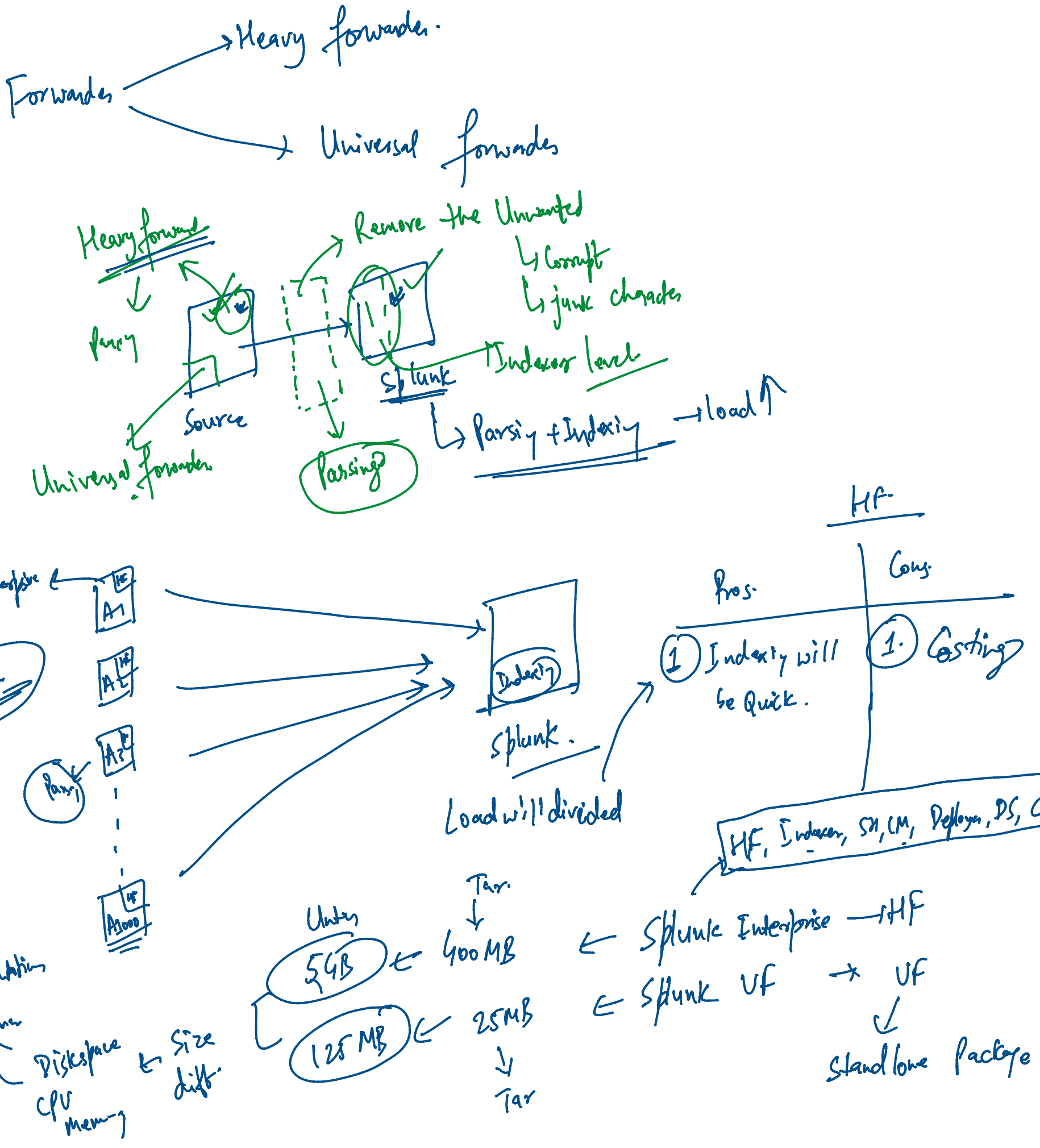
2. Forwarder :- Component that will forward the data from source to the destination.

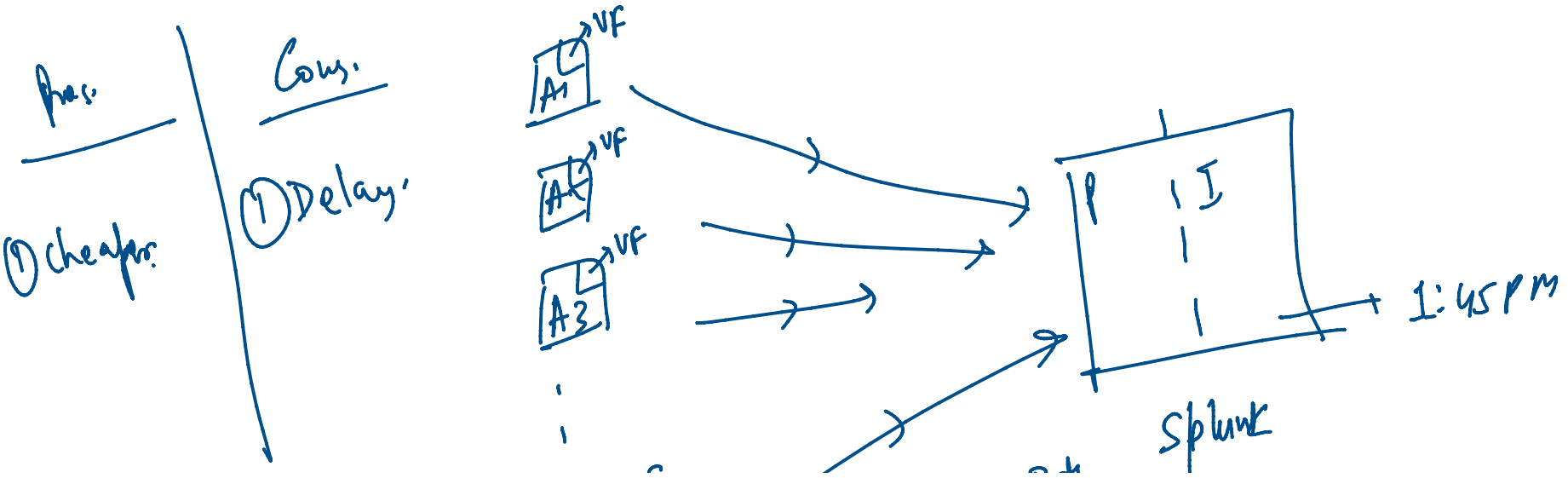
1. What data !?
2. Where to send !?

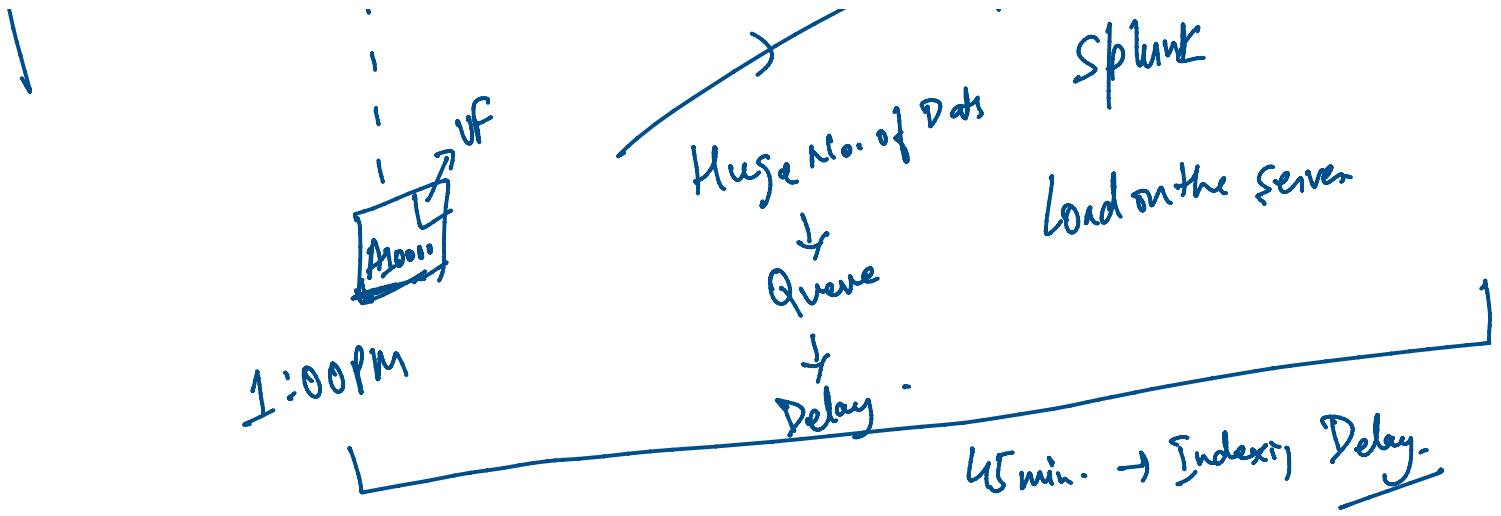


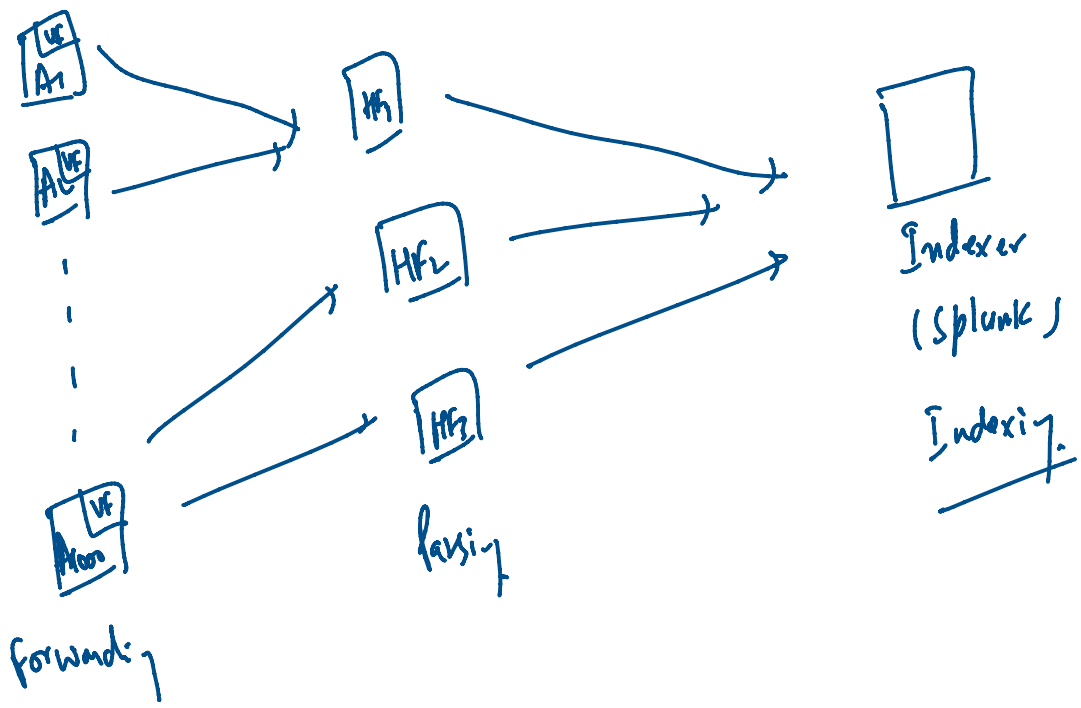
② Where to send !!

③ Filter/Parsing !!

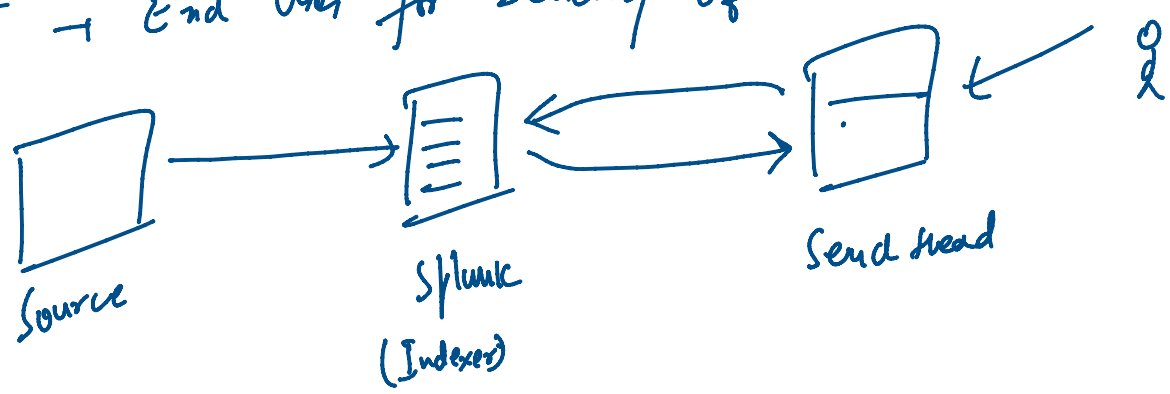






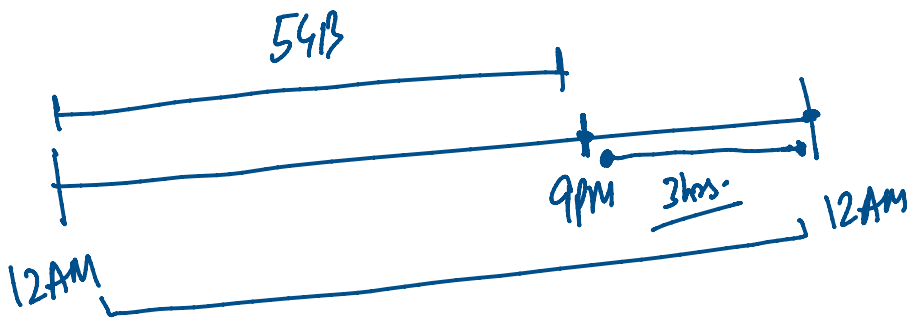


③ Search Heads- GUI → End User for Searching of Data.



④ License Master- Policy → Breach license or Not.

① Volume of Data

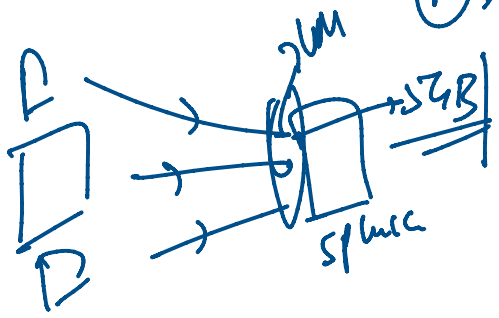


5 GB/day → 1 year.

↓

$ $ $

① 5 time → 30 day Window

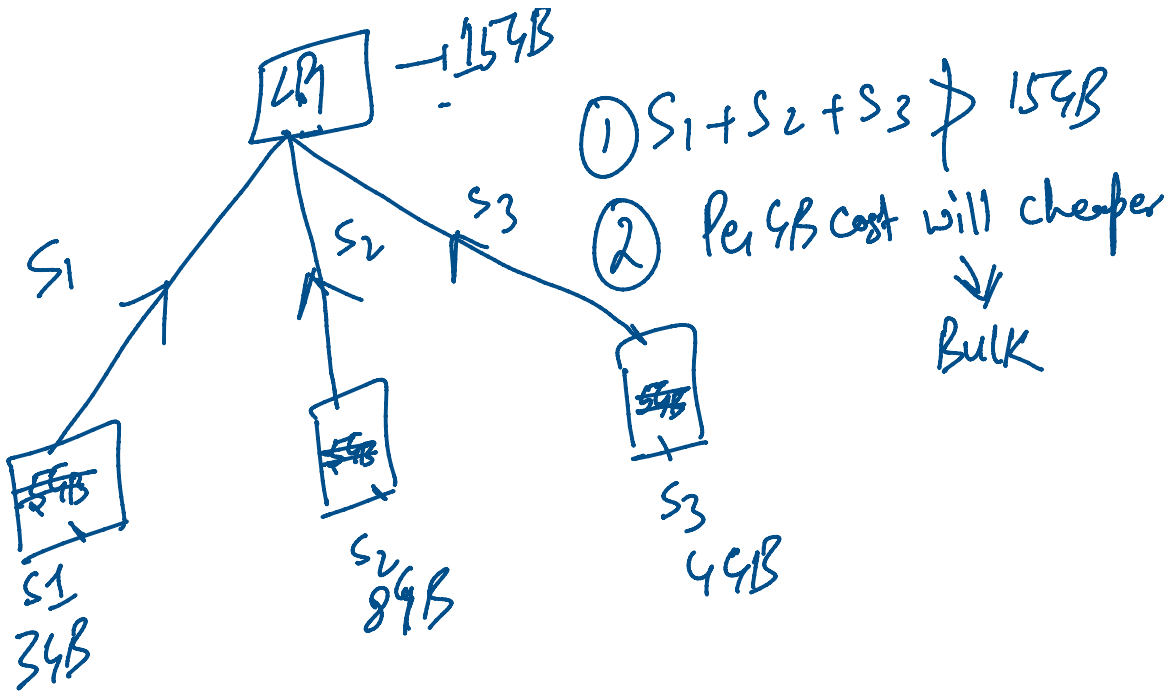


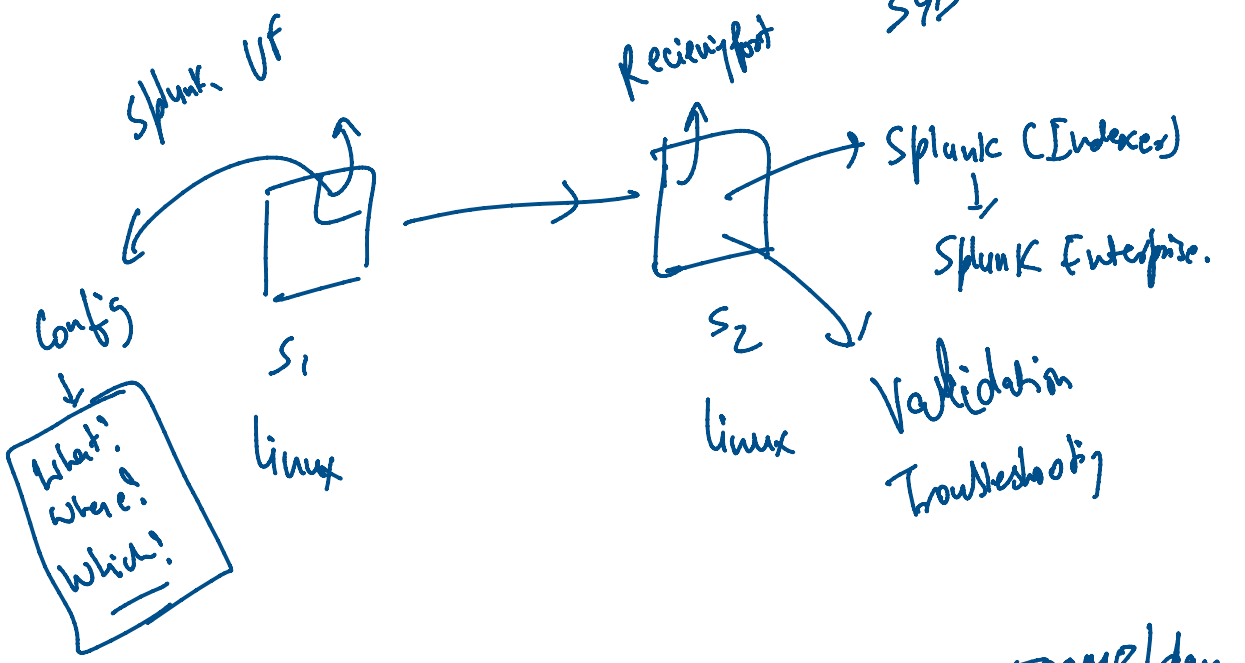
① Data Ingestion will Continue.

② Searching will be disabled.

License Pooling- 15GB → 15GB + 15GB

License Policy:





Splunk
- Free license → 500MB/day, Authentication, Role & User, Real time Monitoring
- Trial license → 60days, 500 MB/day
- Enterprise license → Paid, GB/day, How many days? ? $$