Day - 1

24 December 2024 14:43

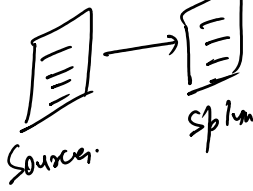
1. Splunk Architecture.
2. splunk Components.
3. Use Cases.
4. SPL Commands → table, rename, dedup, join, append, addcoltotal, addtotals, fillnull, stats, eventstats, streamstats, makeresults, rex.
5. Visualization - chart, timechart, Date & time fun^n, Custom visualization.

---

1. **Splunk:-**

(1) Monitoring tool.

(2) Logs comes different source. → Application (Infra, Operational, User, Security logs.




(1) Dashboard
(2) Alerts
(3) Reports
(4) Knowledge objects

**Adv:-**

1. Parsing of Data is Better.
2. Pull the Data from any sources & any type of data.
3. During Data Ingestion, you will find Apps/Addons for almost all the source in the splunk Appstore.
4. Learning Curve.
5. Customer support.

**Dis:-**

1. Need improvement Monitoring. [APM]
2. Architecture little Complex.

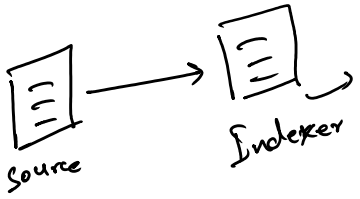
3. Indexing Delay.
4. Licensing cost.

## 2. Splunk Components:-

1. Indexer.
2. Searchhead.
3. Forwarder.
4. License Master
5. cluster Master.
6. Deployer.
7. Deployment Server.

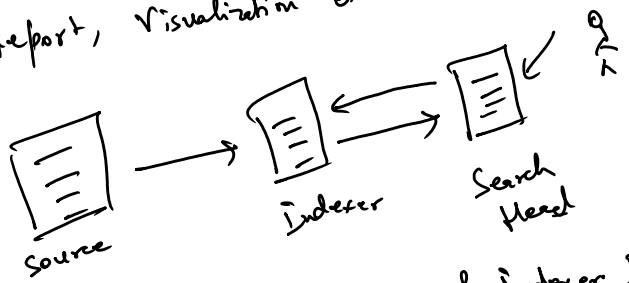
→ Management Instance.

## 1. Indexer:- Where you store the incoming data.

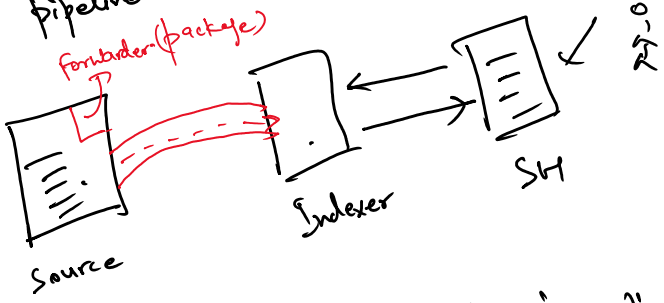



Storage of data will happen.

## 2. Search Head:- GUI where the user will go create the Dashboard, Report, visualization etc.




## 3. Forwarder:- Create pipeline b/w source & Indexer it forward the data.



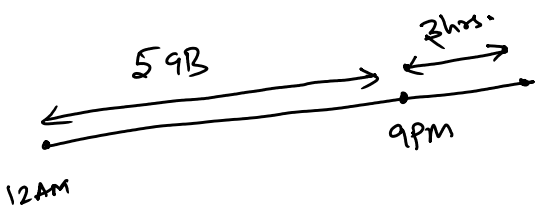

## 4. License Master:- Amount of data, you will be ingesting in splunk in 24hrs.

cycle. ∘ 5GB/d → 1year.
↳ $$

Polling Agent

5GB → 24hrs.

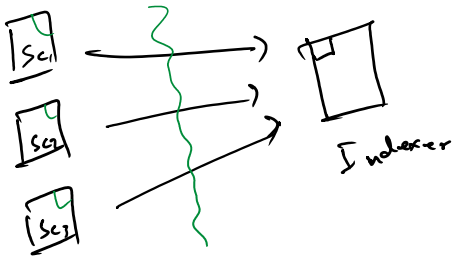
Policing:
Agent




1. No searching.
2. Increase Price for 3hrs.
3. Search for sometime & then it will stop

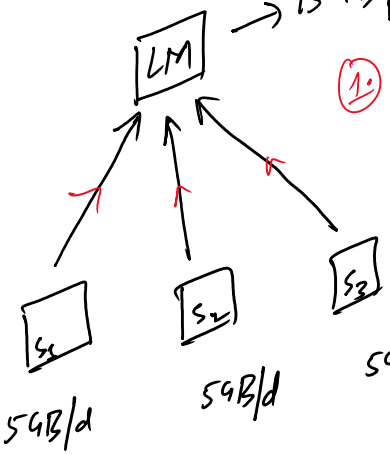
4. Fwd will store the data, No indexing.
5. Free licensy Model.
6. Slow Searchy.

1. Upfront Payment.
2. No visibility of fwd., fwd. will keep forwarding the data.
3. Indexing will happen.
4. No Searchy → Dashboard, Alert, Report
   ↳ Search Query will not work
   ↳ Stale Mode.




Today → 5 time Violation.

License Pooling:-




1. Flexibility on the Amount of data.
   S1 + S2 + S3 & 15 GB
2. Bulk license - per GB cost will be less.

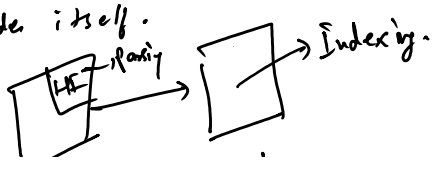
Forwarder:
- → Universal Forwarder.
- → Heavy forwarder

## Universal Forwarder

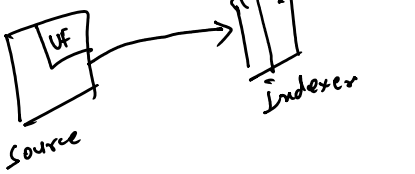
1. Forward data same as it is.
   No parsy take care.


## Heavy forwarder.

1. Parsing will be taken care at the source level/ forwarder itself.



No parsing take care. Parsing → Indexing.

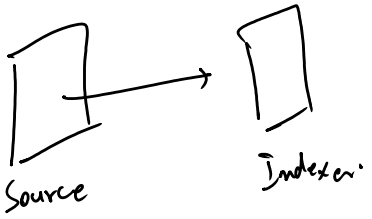


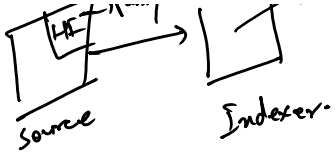

(2.) No GUI

(3.) Standalone / Individual Package.

Tar → 25MB

Unter → 150MB



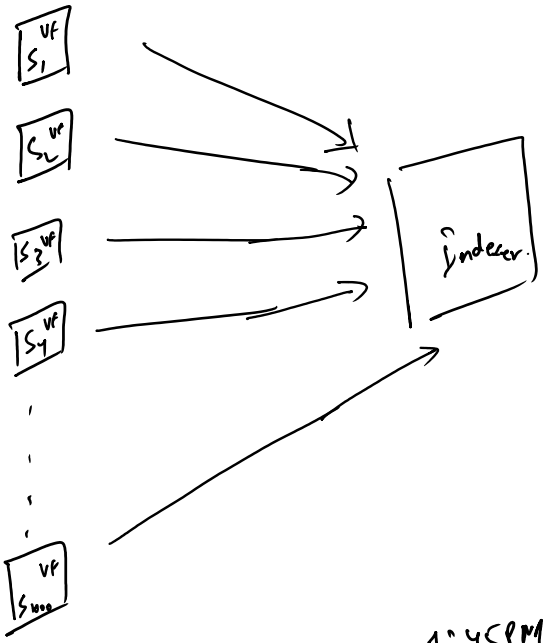




(2.) GUI

(3.) Splunk Enterprise. Tar → 450MB

Unter → ≈ 5GB Size

Parsing → Removing Unwanted data.




12:30 PM → 1:45 PM

1:15 hrs → Indexing Delay.

## UF:-

### Adv:-

(1.) Log forwarding

(2.) No Much load on the source server.

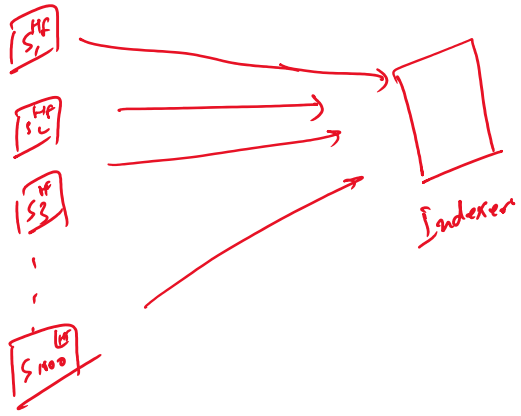
(3.) Computational Resource Consumption is less. ex → CPU, Disk, Memory etc.

### Dis:-

(1.) Load on indexer

(2.) Indexing Delay

## HF:-




### Disadv.

(1.) More load beoz. it will parse the data.

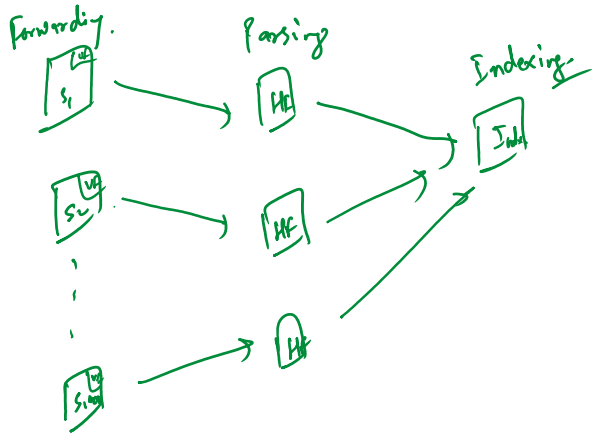
(2.) Computational Resource Consumption is More

### Adv.

(1.) Load on indexer is minimal

(2.) Less Chances of Indexing Delay.

## Hybrid:-

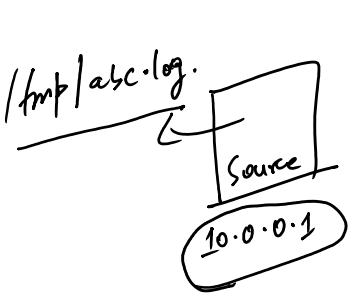



## Index:-

3 Types of Index:-

1. Predefined Index → Starting with _* . No license is consumed. It is reserved for the splunk App. logs.
2. Default Index → index=main - License is consumed. Custom data is ingested.
3. Custom Index → User specific index. Ex: VR_idx, sample_idx. etc. License is consumed. Push your custom data.

## Default Fields:-




host = 10.0.0.1
Source = /tmp/abc.log.
Sourcetype = log
(Data Type) =
_time = 12:34:55

1. Source
2. Host
3. Sourcetype
4. _time.

Field Name → Case Sensitive.
Field value → Case Insensitive.

## Searching of data:-

Fast Mode:- Fastest searching mode.
Pull the event.

1. Pull the events.
2. Extract the event.

## SPL Commands:-

... field1, field2, field3 ...

# SPL Commands :-

① Table → Tabular output. Syn:- |table field1, field2, field3

② Rename → Rename the field at Search Level. |rename old field AS newfield.

③ stats → Statiscal output. ⓐ count ⓑ list ⓒ avg. ⓓ sum ⓔ Values.

④ fillnull → fill the blank cells/spaces. Default is 0. |fillnull value=NULL total_bytes.

⑤ Eval → Evaluation Command. fx → str —, int — . eval — initialize the Variable.

⑥ Addcoltotal →

⑦ Addtotal. →