Day - 4

09 October 2025 09:41

Mstats :-

index = main

Query the metrics data.

└) metrics index

↓

metrics store after 7.0

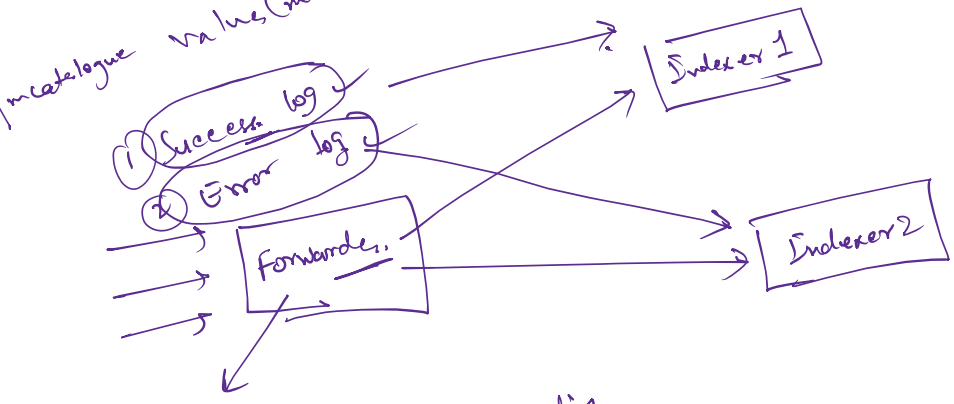
Syn:- |mstats [Stats fn] where <filter> BY <dimension>

|mstats avg(cpu_usage_percent) where index=metrics BY host.

mcatalog:- Search command used to discover metric names, dimension, & indexes within Splunk metrics store.

|mcatalog [function (metric name)] where <Criteria> BY <fields>

ex:- |mcatalog values(metrics_name) where index=metrics.



Data Routing

1. Inputs.conf.
2. outputs.conf
3. Props.conf
4. Transforms.conf.

HF, Indexer → Splunk Enterprise

③ Props.conf

Enterprise

① 3 server → Splunk enterprise

② 1 server → HF

③ other 2 server → Indexer → create receiving port → 9997

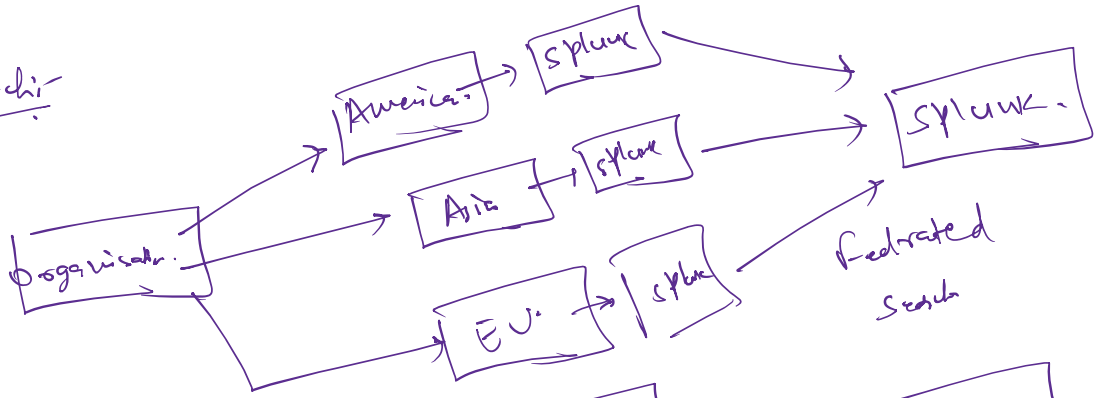
④ Connect HF with Indexers.

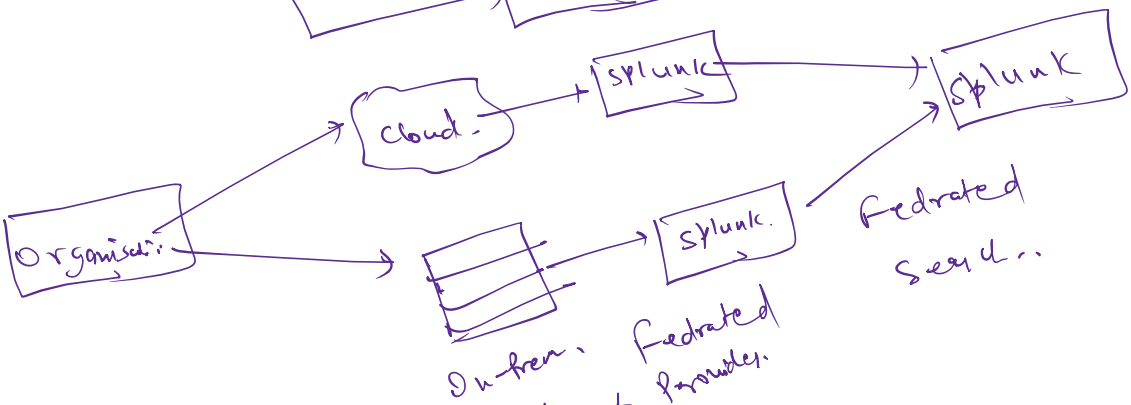
⑤ Grouping the indexer → Success. / failure.

⑥ Regex → split the data.

⑦ Validation of the data at the indexer end.

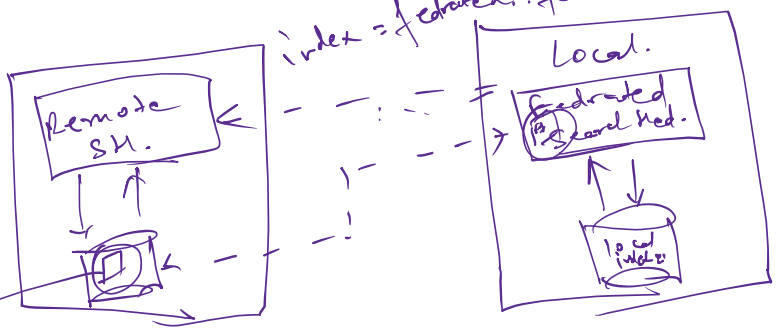
Federated Search:





Different Federated Providers.

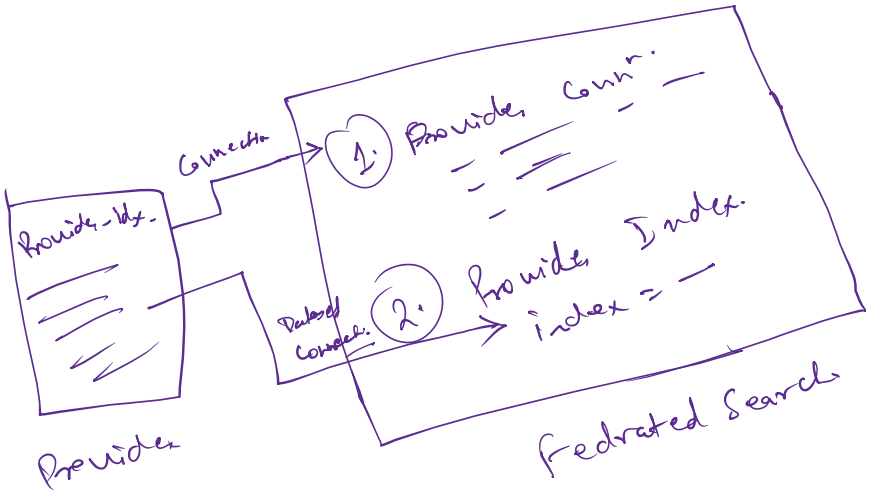
index = federated:: federated_search



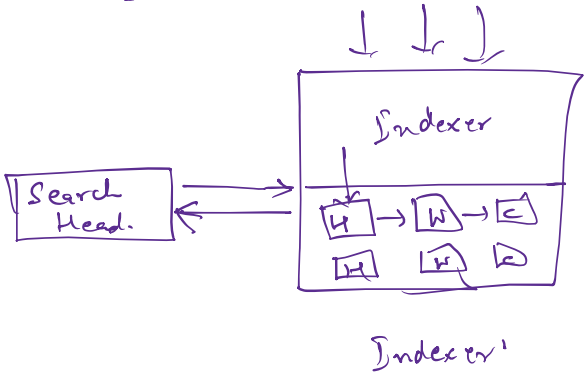
| union search index = federated:: federated_index | -

Remote Dataset.

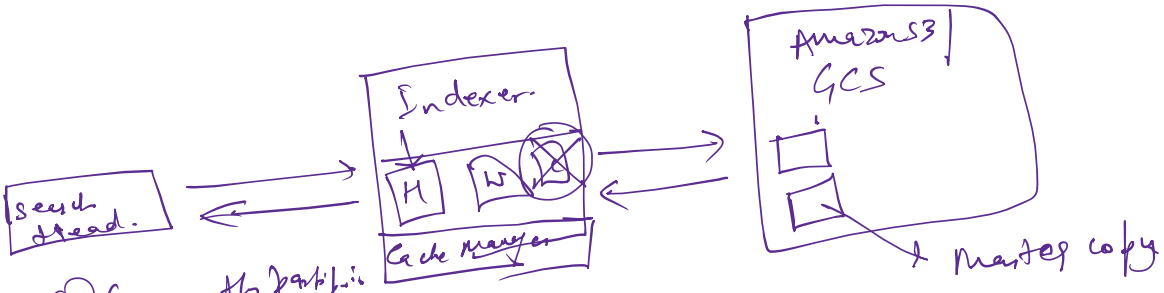
Federated Providers.



Smartstore Soln:-



1. High storage cost.
2. Higher time for recovery from peer failure.
3. Higher time data rebalancing & backup fixup etc..



1. Currently participating Search
2. Participate in future search.

4. Config. at index level.

1. Reduce storage cost.
2. High Availability of data
3. Ability to scale compute & storage resource separable

[Volume: remote store]

StorageType = remote.

path = _____

remote _____ = _____

Scripted input:- Python script

↳ pull the data inside splunk.

Management instance

↳ forwarder, Search Head.

Management instance: