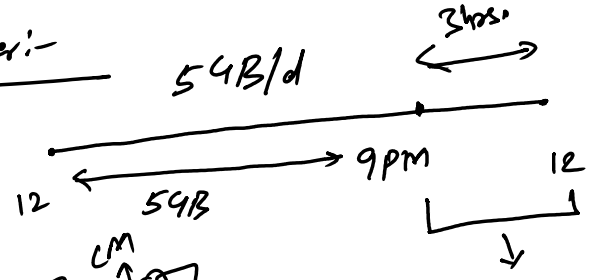
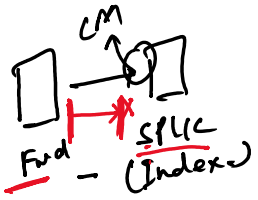
Day - 1

13 January 2025 11:25

① License Master:-



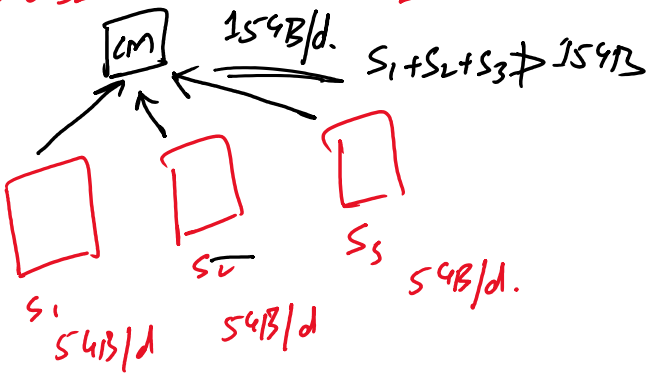


→ 1. Stop the storage
2. Removing of older data.
3. charges will be extra.
4. Lending from the next day.
5. Carry fwd. from previous day.

1. Indexing will happen.
No Searching.

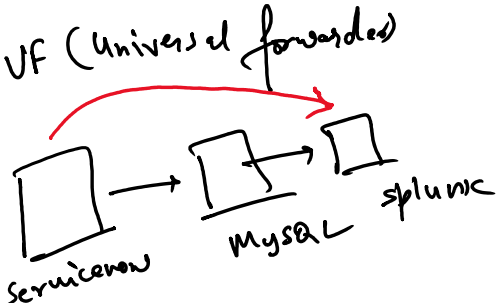
② Max. Violation of 5 days → window of 30 days.

License Pooling:-



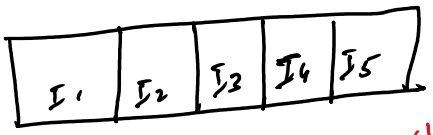
① Splunk Enterprise → Indexer, Heavy fwd, CM, SH, DS, CM, Deployer

② Splunk UF (Universal forwarder)



Splunkd - 8090
Mang. Port - 8089
Web Port - 8000

Kvstore - 8191
Recieving Port - 9997
Collection Port - 8088



Indexer.

No License Consumption.

→ Splunk specific logs

Predefined Index → _*, No license Consumption.

Index → Default Index → Main.

→ Custom Index.

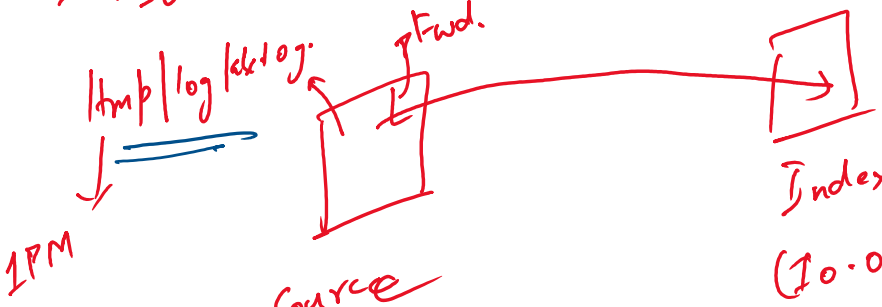
↓

VK-idx, secure_access

License Consumed.

Default Field:-

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



→ data Path.

Source → /tmp/log/abc.log.

Sourcetype → data type.

host → 10.0.0.1

time → Last modified time.

Index → main / Custom once.

~~10.0.0.1~~

~~10.0.0.5~~

ingestion time.

10.0.0.6

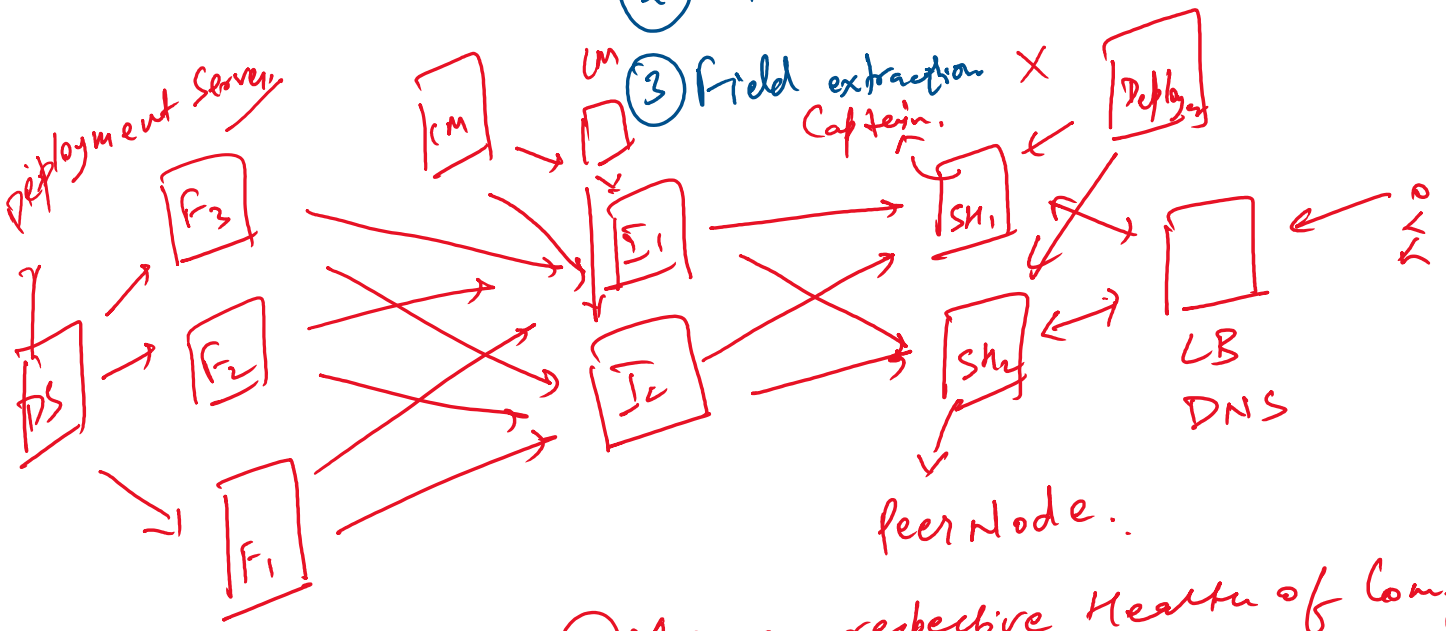
Searching Mode:-

1. Fast Mode. → Fastest method
2. Smart Mode. → optimized.
3. Verbose Mode. → Max. time.

(3) Verbose Mode. → Max. time.

Index-_interval :-

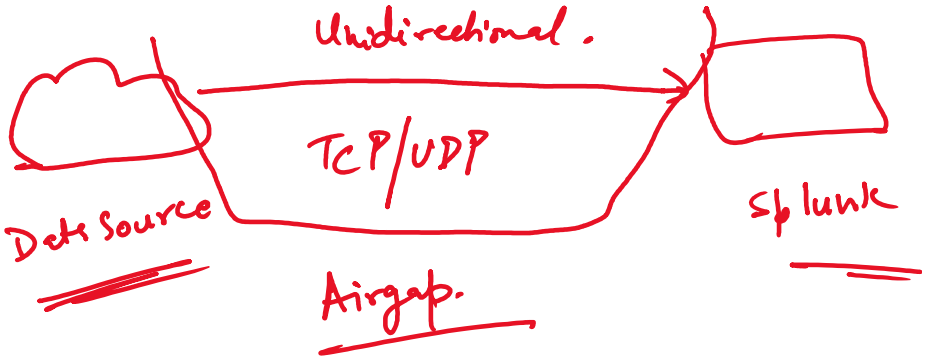
(1) Index ✓
(2) Pull the event
→ Fast Mode.



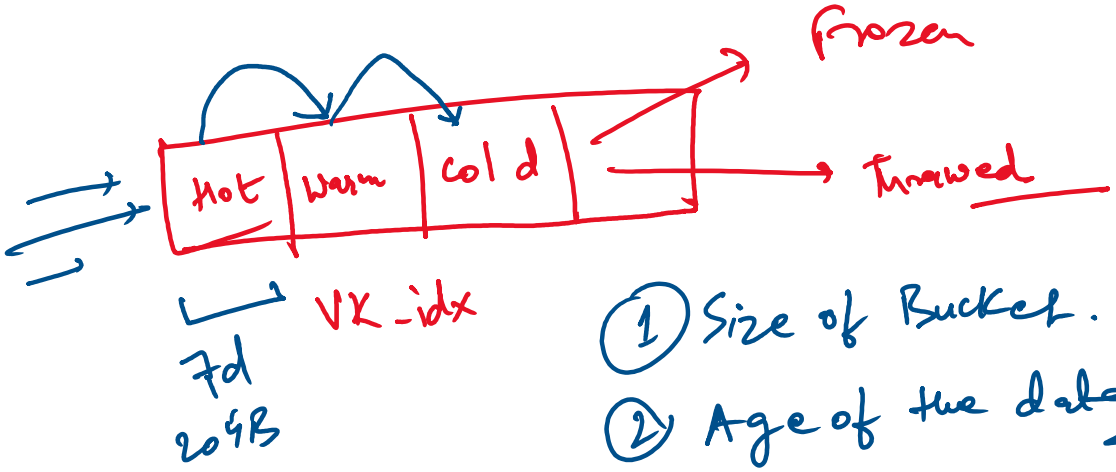
(1) Mang. respective Health of Comp.
(2) Config.

Day - 2

14 January 2025 09:07



Indexer → Index.



SPL (Search Processing lang.) :-

1. Table :- Tabular format. Syn :- | table field1, field2, field3.
2. Rename :- change to new name. Syn :- rename old_name AS new_name
3. Sort → sort +1 —, +Ascending, sort - fieldName → Descending
4. Dedup → dedup f1, f2 → Remove Duplicate Value.
5. Stats :- (1) Count → Count on basis of certain Condn.
   (2) avg → Avg. on the basis of certain cond...
   (3) Sum → Sum of Numeric field ..
   (4) list → group the field with certain Value
   (5) Values → group the fields with unique Values

purpose. eval a

(4) [illegible]

(5) Values → Group the fields

6. eval (1) Calculation → evaluation purposes. eval a,

(2) if-else. → if condition

(3) Case statement. → Switch Condition.

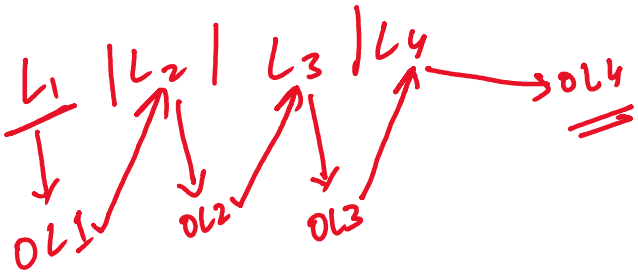
7. Chart. →

8. Time chart

(1) Date & Time fun:—

9. Single value Visualization.

10. GeoMaps —



fillnull value="NA" b | —

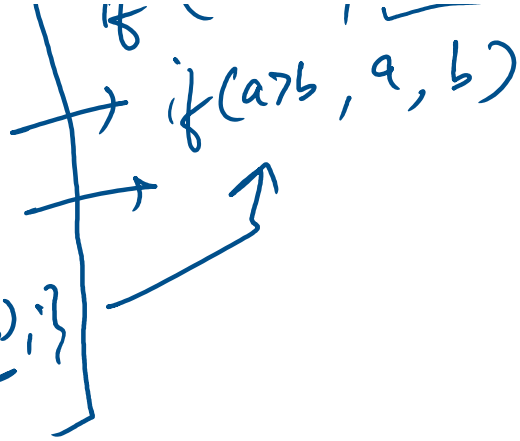
a	b	c
NA		
NA		
NA		

if (condt, True, false)

if(a>b, a, b)

if else →

```
if(a>b)
{
print(a);
}
else { print(b); }
```



Case Statements:-

```
switch(a):
switch(s):
default:
```

→ Case(Cond1, "true", Cond2, "_", Cond3, "_", 1=1, "_")

Chart:-

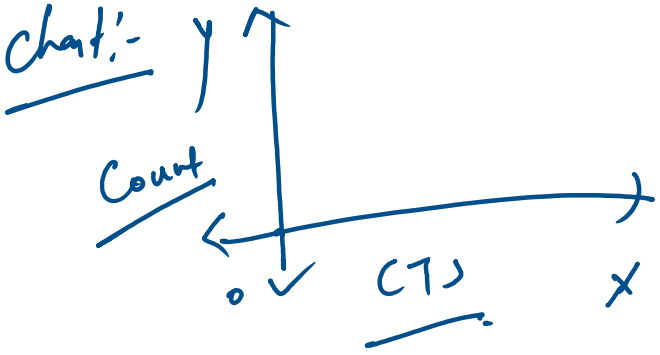
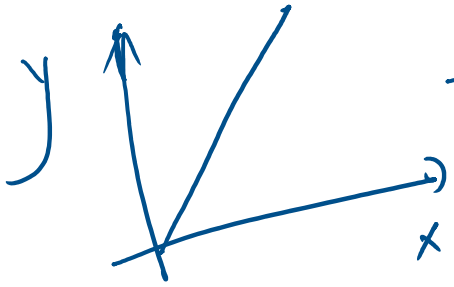
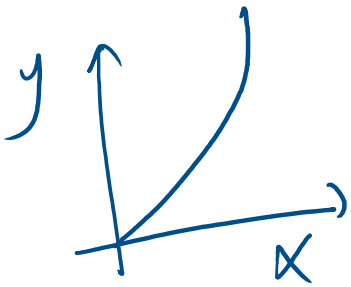


chart count by Current_ticket : State

↓ Y_axis ↓ X_axis

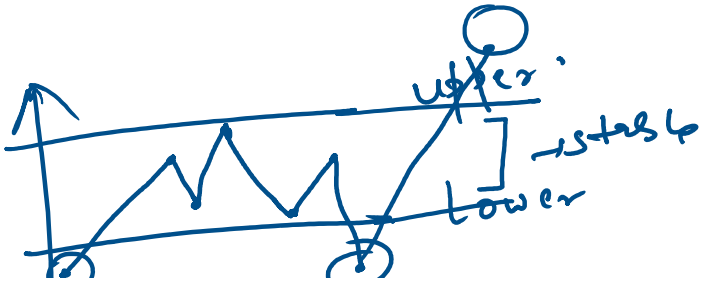


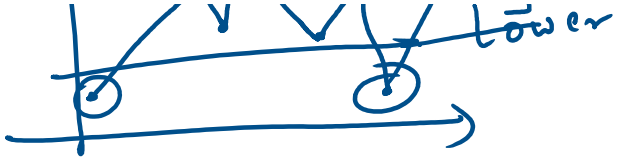
→ 10, 20, 30, 40 - - - -



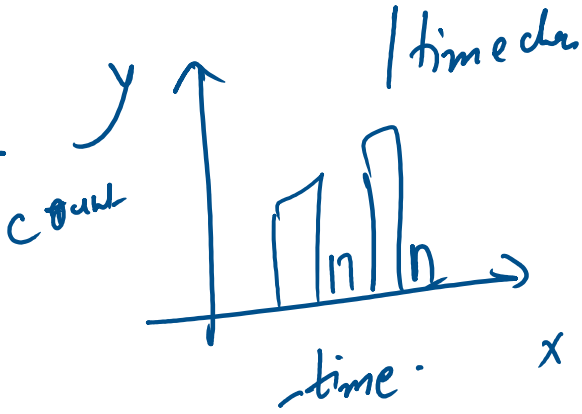
10^x

10, 100, 1000, 10000





Timechart:-



timechart created by CTS.

09-09-09 09:09:09

US - %m-%d-%y

EMEA - %y-%m-%d

AIAL - %d-%m-%y

D1 -

D2 -

(D2 - D1)

Strptime - function that will convert the date & time function to epoc format.

13-01-17 09:01 → Strptime, Strftime.

13-Jan-2017 09:01 (Sunday)

Day - 3

15 January 2025 09:09

1. Single Value Visualization.

2. GeoMap.

3- Custom Visualization. (Pre Req.)

4. Adv. SPL. (1) join.

(2) Append / Appendcol / Appendpipe.

(3) Rex

(4) Addcoltotal.

(5) Addtotal.

(6) spath.

(7) Makeresults.

5. Knowledge object:-

(1) tags & eventtype.

(2) Calculated fields.

(3) Macros.

(4) Data model & Pivot

(5) Alerts.

(6) Report.

(7) LookUps.

1. Single Value Visualizations

1. Single Value Visualizations

- ① Single Value.
- ② Radial Gauge
- ③ filler gauge.
- ④ Marker Gauge

→ Single Visualization.

2. Geo Map:-

① Coordinates

- Latitude
- Longitude.

3. Custom Visualization:-

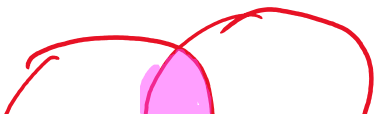
1. Compatability with splunk Version & Products.
2. Support
   - ① splunk
   - ② Developer
   - ③ alone.

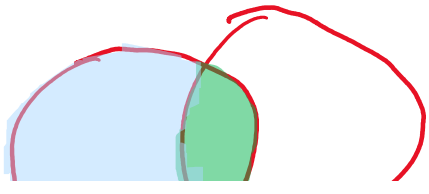
4. Adv. SPL:-

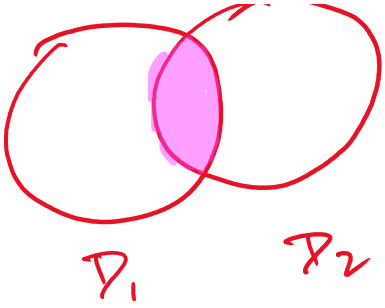
① join:-

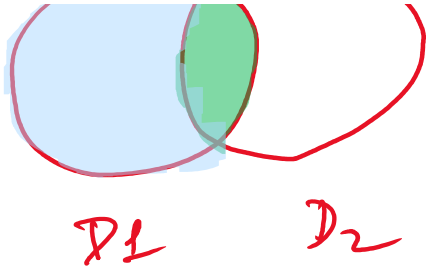
② left/outer:-

① Inner:-



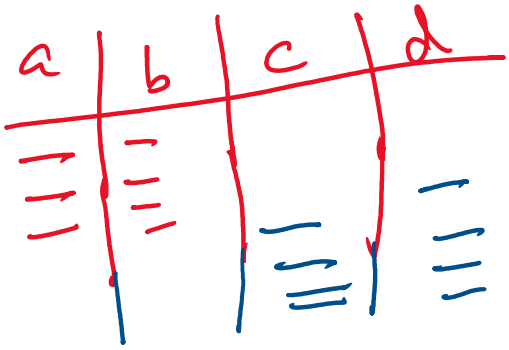






Syntax:- S1 | join type = "inner" unique field [search S2]

Append:- S1 | append [search S2]



Append pipe:-

Sum(count) by ser) —— : —

S1 | appendpipe [search S2]

Rex:-

Addcoltotal:- Addition Column Wise.

Addrowtotal:- Addition Row Wise.

Day - 4

16 January 2025 09:05

Spath:- → Json. → -json, kvstore-mode =yes.
→ XML
→ Mixed structure either xml or json

Structured → csv
Semi-structured → json, xml
Unstructured. → No sequence / Email / Pdf / txt

Search & where:- Both use for filtering purpose.

a
1
2
4
5
6
5

Search a > 3
a
4
5
6

filter the value from the same field itself.

a	b
1	2
2	2
3	1
5	1
7	1
8	1

where a > 3

→ Compare 4 filter two diff. fields.

a	b
3	1
5	1
7	1
8	1

Knowledge object:-

1. Calculated field:-

eval Kb = round(bytes / 1024, 2) . "KB"

bytes

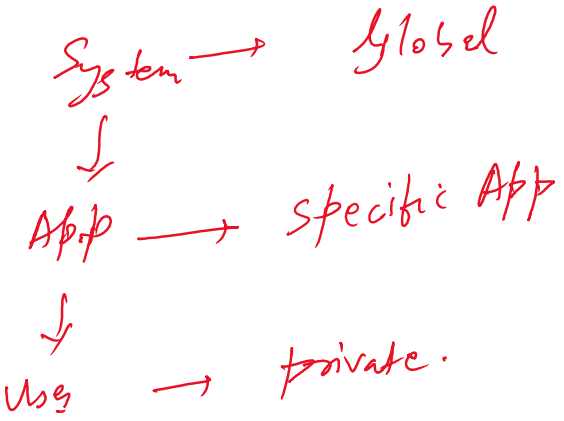
Template

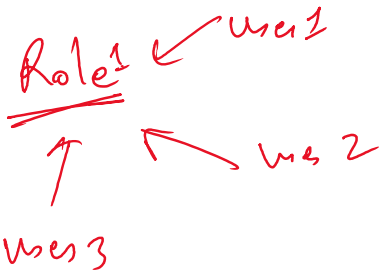
1. Eval expression
2. field. —
3. Dataset

Adv:-

1. flexible to Manage & make change in expression
2. Avoid the repetitive defining of expression.

Access:





② Tags & Eventtype:-

Tags:- Categorise the certain field.

2 new fields:-

1. tag.
2. tag :: severity

③ Macros:-

```
function a(b,c)
{
d = b+c;
returnd;
}
```

a(3,4)

a(5,6)

1. No Arg. →
2. Single Arg. →
3. Multi Arg. →

4 Alert :-

[Definition] → SPL Schedule

[Trigger Condition] → When you want alert to be triggered ??

[Trigger Action] → After Alert Trigger ??
1. Email
2. Triggered Alert
3. Webhook
4. Script

Assignment-3 :-

Cron Expression – Mon-Fri, 10AM – 7PM, every hour, Jan, March, April → Cron expression.

~~No~~ no. of event > 0 → Trigger Alert

Once – 1 Alert
for each result = 1 Alert

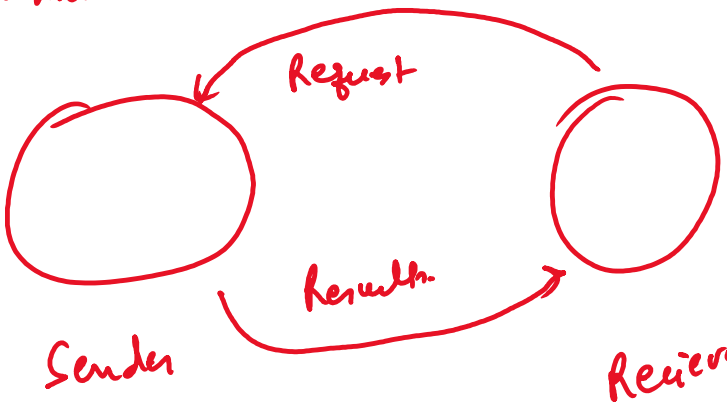
Assignment -4 :- API vs Webhook ?

Assignment -5 :- Interdependence of Time Range & Schedule lead to false Alert ??

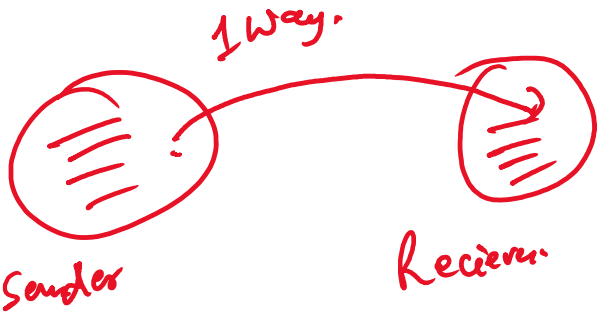
Day - 5

17 January 2025 08:50

API :- 2 way Communicat'n



Webhook :- 1 way Communicat'n



Lookup :-

1. csv lookup
2. Kvstore lookup
3. Geospatial
4. External lookup
5. database lookup

1. csv lookup :-

1. Lookup Table

3. Automatic Lookup.

(1) Lookup

(2) lookup Definition.

Commands:- (1) inputlookup (3) outputlookup

(2) lookup

Lookup Editor Application.

(1) csv file.

(2) small & static in nature.

@outputlookup command - edit & save the changes in the lookup file.

KV store → Key value pairs

(1) Dynamic.

(2) Large file size.

each entry → mapped → record

↓

_key

"

"

1. collections.conf → Structure of the KV store
2. LookUp Definition
3. inputlookup → commands.

Day - 6

20 January 2025 09:10

Dashboard.

- Classic Dashboard
  - XML → Tags
  - Input filter.
  - Drilldown.
  - optimization.
    - Base Search.
    - Saved Search.
    - Summary Index.

Severity	Count
1	5
2	10
3	25
4	35

S1 → 1
S2 → 2
S3 → 3 → value.
S4 → 4

Label

User → Sev → 3, 4

App → Admin

S1, S2, ALL → ALL

Deselected

ALL, S1 → S1

Deselect

click.name = Severity

click.value = 1, 2, 3, 4, 5, 6

click.name2 = Sum

click.name2 = Sum

click.value2 = 10, 20, 5, 25, 7, 18

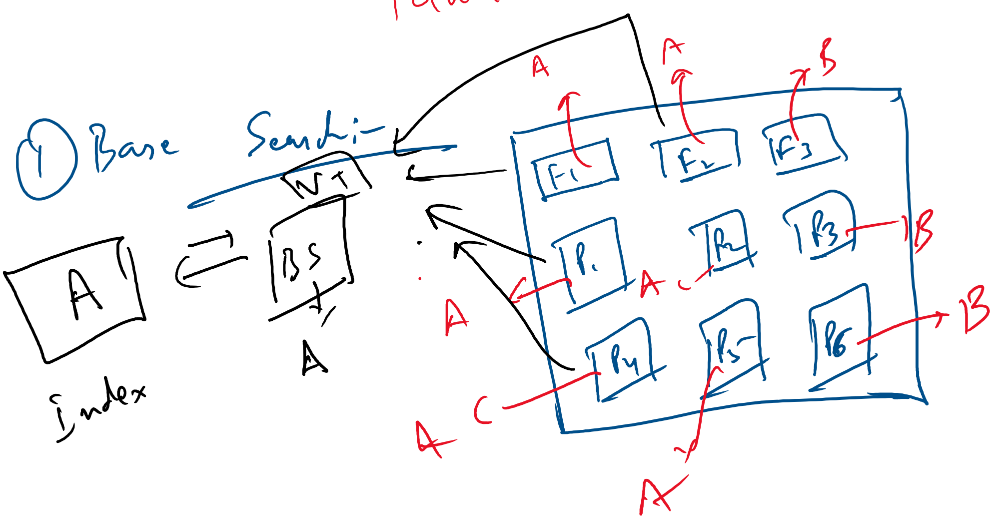
earliest → earliest time

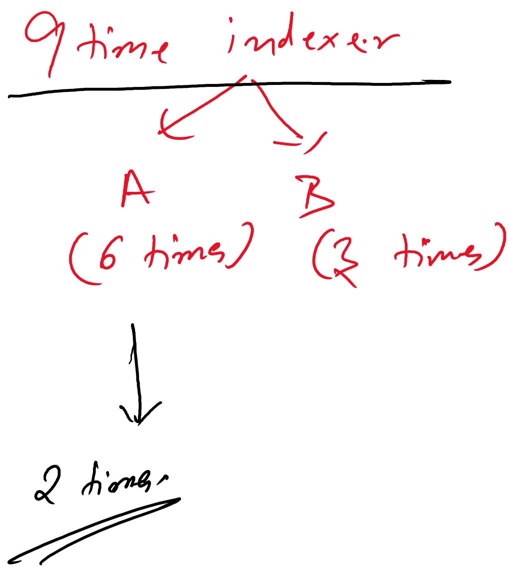
latest → latest time

Optimization = Search Query + Panel level.

Search Query = join / Append / lookups.

Panel level = To avoid involving indexes unnecessarily.



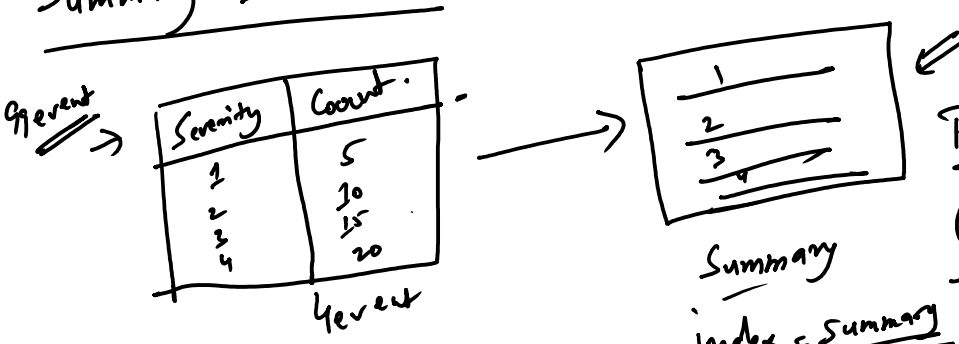


Day - 7

21 January 2025 09:06

Summary Index:-

index = VK-snow | stats count by severity



Props:-

1. Increase the searching speed

index = summary

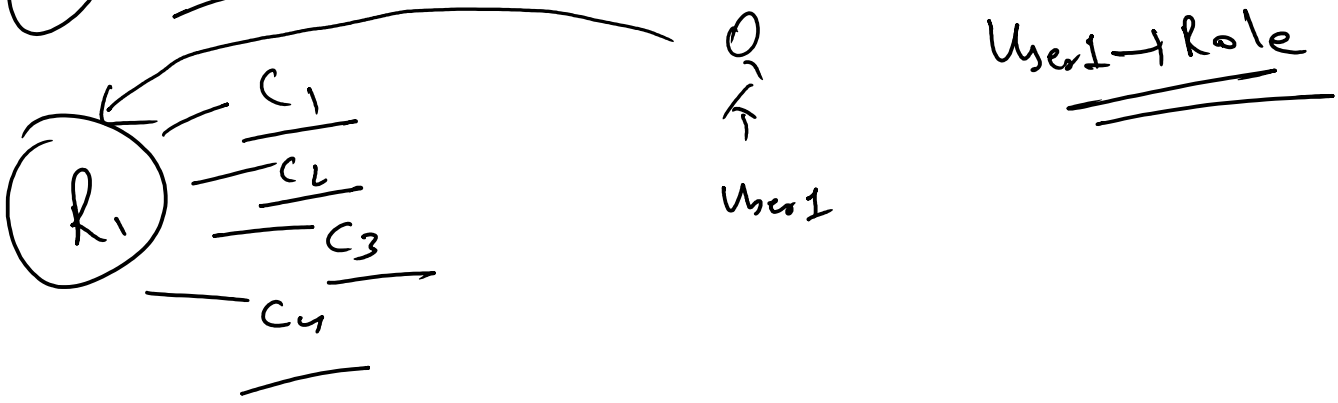
Cons: 1. Computational resource consumption.

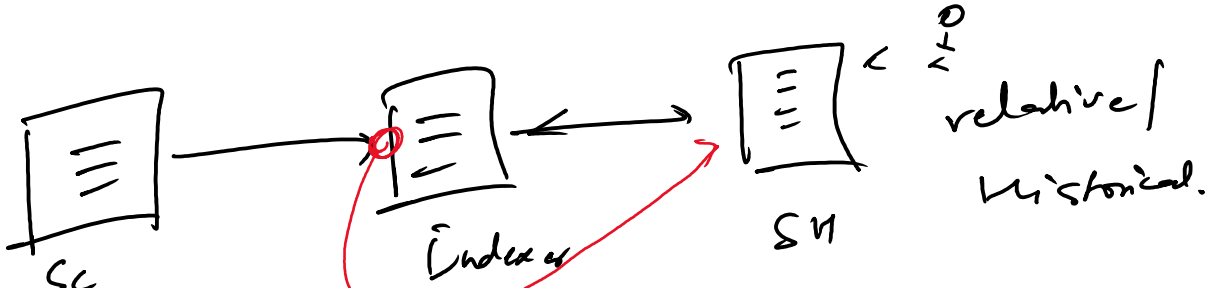
License Not required.

Sourcetype = stash.

User & Role Creation:-

1. Capabilities:- Set the Rules.
2. Role:- Abstract Value.
3. User:- Normal User.





Index

Real Time

SM

Data Model:

1. Tsidx file → Timestamp Summary file.
2. Define the field in the Advance
3. Inheritance - Root → child + C'
   ↳ SC + C''
   ↳ SSC + C'''
4. Accelerate Data Model.
   ↳ Backfill → 24 hrs.

Pivot → to Visualize Data Model.

chart / time chart → index.

Pivot → Data Model.

Day - 8

22 January 2025 09:04

Module 9 Advanced Data Input in Splunk Compress the Data Feed Indexer Acknowledgment Securing the Feed Queue Size Input ● Monitor ● Scripted ● Network Pulling Data Using Agentless Input

Module 10 Splunk's Advanced .conf File and Diag Understanding Splunk .conf Files Setting Fine-Tuning Input Anonymising the Data Understanding Merging Logic in Splunk Debugging Configuration Files Creating a Diag

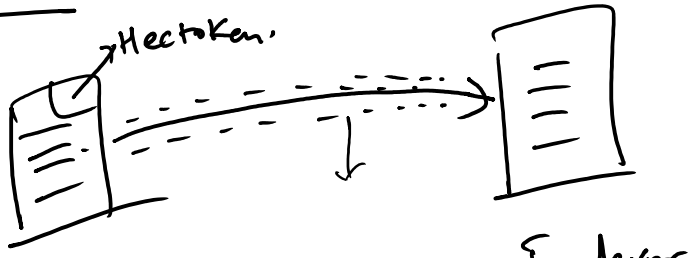
Module 11 Infrastructure Planning with Indexer and Search Head Clustering Capacity Planning for Splunk Enterprise Configuring ● Search Peer ● Search Head Search Head Clustering Multisite Indexer Clustering Splunk Architecture Practices

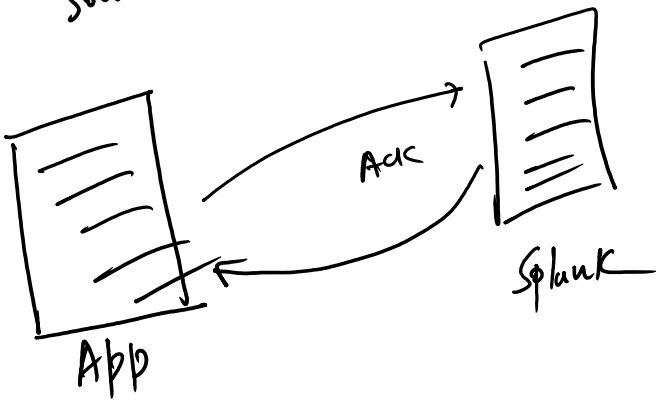
Module 12 Troubleshooting in Splunk Monitoring Console Log Files for Troubleshooting Metrics.log File Job Inspector Troubleshooting ● License Violations ● Deployment Issues ● Clustering Issues

Module 13 Advanced Deployment Deploying Apps Through the Deployment Server Creating a Server Group Using ServerClass.conf Deploy Configuration File Through Cluster Master Deploy App on Search Head Clustering Load Balancing Indexer Discovery SOCKS Proxy

1. Http Event collector (HEC Token).
2. Python Script (scripted input).
3. Connect with VF
4. Forwarder Management
5. Indexer Management
6. Search Head Clustering.

1. HEC Tokens-





(2) Scripted Input:-

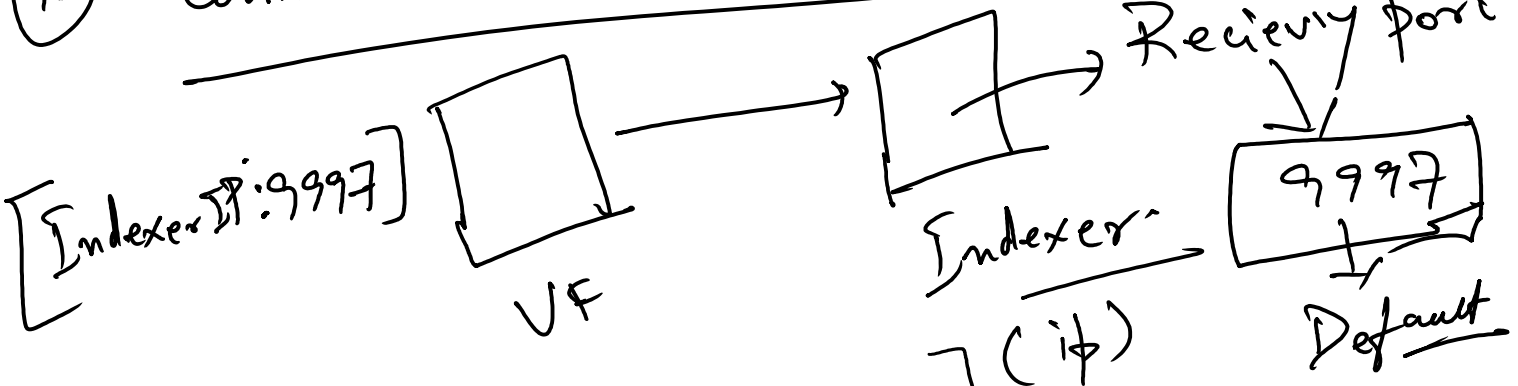
(2) Scripted Input :-

Diag report → Diagnostic report

↓

Summary →

(4.) Connect UF & Indexer :-



(1.) Monitor Stanza.

(2.) Index, Sourcetype → inputs.conf

(3) Outputs.conf → indexer_ip:9997

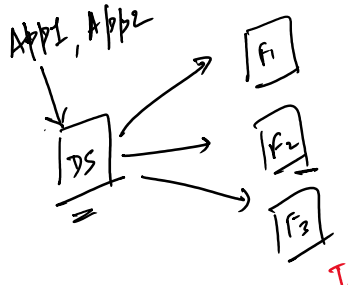
→ UF Level.

Day - 9

23 January 2025 09:13

1. Deployment Server
2. Cluster Master.
3. Search Head cluster.
4. Monitoring Console.

1. Deployment Server



① Centralised Unit
1- Health
2- config. Activity.
3- App push.

/etc/deployment-apps.

↑ A1, A2

Initialize

I. 1 → splunk Enterprise (DS)

II. 2, 3, 4 → UF

III. 1 → DS → Connect DS with forwarder.

IV. Serverclass → Grouping purposes → A1 (F2, F3) → etc/system/local/serverclass.conf

V. Push the App. to the Forwarder level.

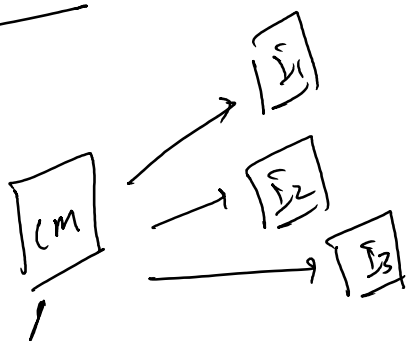
VI. CLI Commands, Troubleshooting & Config. file.

10.0.0.1
:
10.0.0.99

10.0.0.5
10.0.0.25

Include = 10.0.0.* → High Precidence
Exclude = 10.0.0.5, 10.0.0.25

2. Cluster Master:



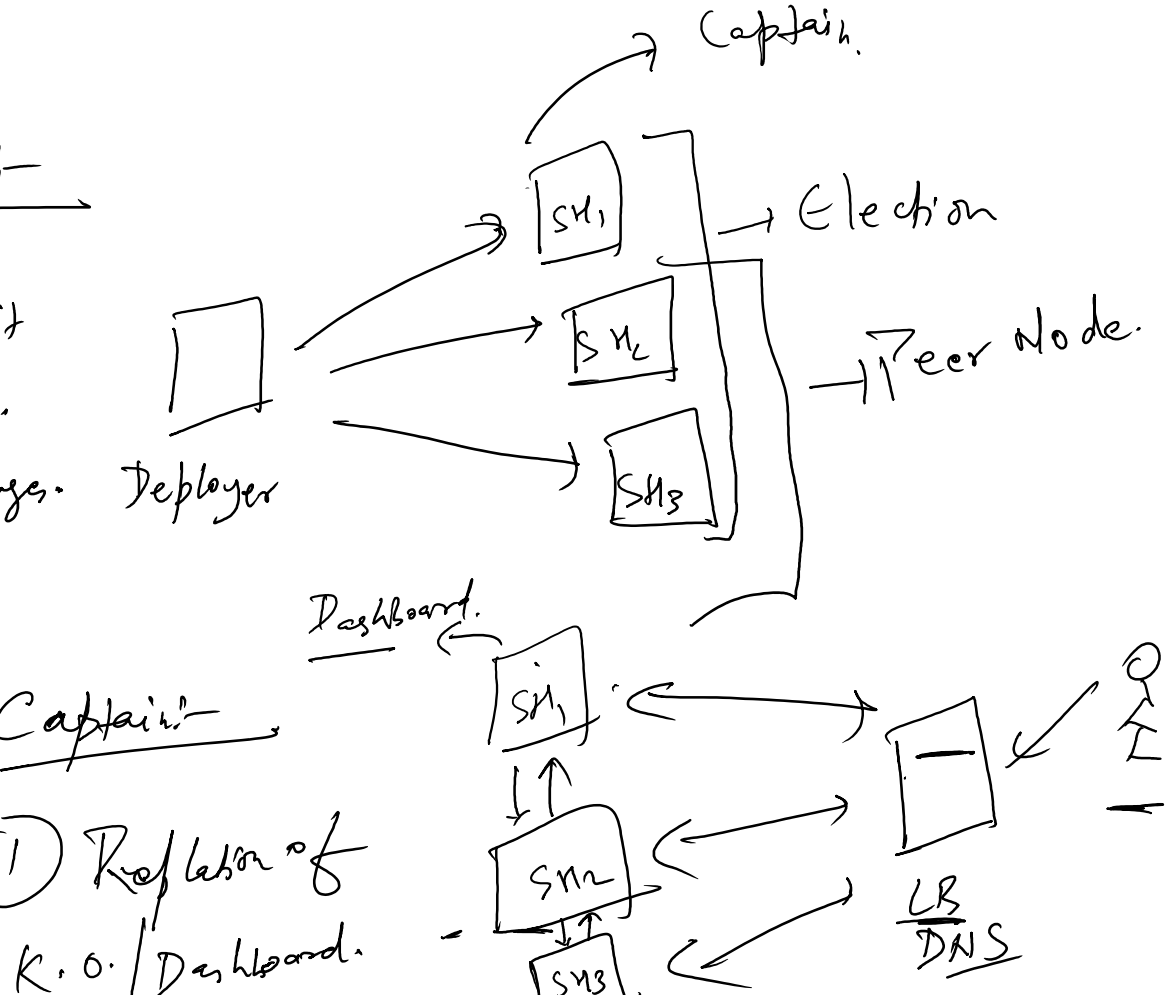
① Centralized Unit
② Health of the Index
③ Continous replication of data is insured.
④ Send/Deploy the config.

1. Q → Splunk Enterprise (CM, Indexers)
2. Initialize Server 1 (DS) → make it as CM.
3. Rest 3 Server → Connect with CM
4. Dummy App in cluster master (etc/system/master-app)
5. Push the change via bundle Mechanism.
6. No Concept of Serverclass as you have learnt in DS.
7. Config → server.conf.
8. CLI Command.

./splunk apply cluster-bundle
./splunk show cluster-bundle-status

3. Deployer:-

1. Centralised Unit
2. Push Config. related changes.



1. Fresh Splunk Enterprise in all the 4 servers.
2. 1 Server → Initialized as Deployer.
3. 2, 3, 4 Servers → Connected to Deployer
4. Election s/w 2, 3, 4 → SH.
5. Add Dummy App in the Deployer.
6. Push the changes via Deployer to the Searchhead.
7. Config. files.
8. CLI Commands.

Day - 10

24 January 2025 09:16

1. Search Head clustering.
2. Monitoring Console.
3. CM
4. Bucket Management
5. Bloom Filter
6. Custom Sourcetype Rules.
7. Splunk App. Structure.

1. Search Head clustering:-

./splunk init shcluster-config -auth <username>:<password> -mgmt_uri <URI>:<management_port> -replication_port <replication_port> -replication_factor <n> -conf_deploy_fetch_url <URL>:<management_port> -secret <security_key> -shcluster_label <label>

SH1- → SH1 login Credential. → SH1 URL

./splunk init shcluster-config -auth admin:admin@123 -mgmt_uri https://172.174.106.180:8089 -replication_port 9999 -replication_factor 3 -conf_deploy_fetch_url https://20.51.216.159:8089 -secret admin@123 -shcluster_label shcluster1

- admin@123 → Pass4SymmKey which you define at deployer end in server.conf etc/system/local
- shcluster1 → Cluster Label.
- https://20.51.216.159:8089 → Deployer URL

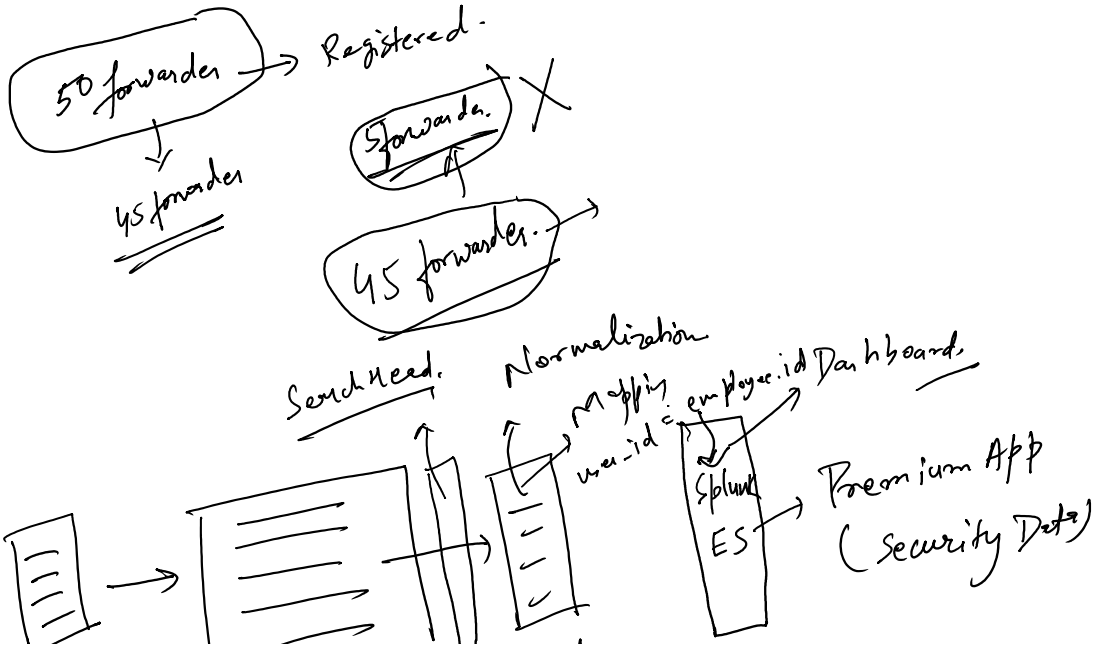
./splunk bootstrap shcluster-captain -servers_list "<URI>:<management_port>,<URI>:<management_port>,..." -auth <username>:<password>

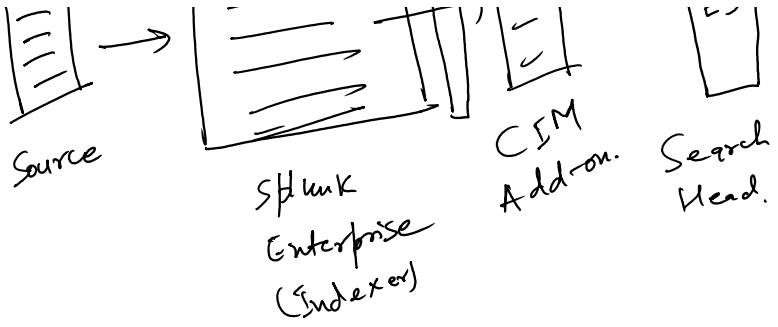
SH1 → any SH

./splunk bootstrap shcluster-captain -servers_list "https://172.174.106.180:8089,https://74.235.81.41:8089,https://20.55.69.103:8089" -auth admin:admin@123

Need to run on any one SH. That SH will be given the first preference to become the Captain.

- admin:admin@123 → login Credential.
- URL of All 3 SHs.





Search →

where →

severity =3

where a>5

DBConnect → Rising Column.

DBConnect → Batch Proces

1
2
3
4
5 ←
6
7
8