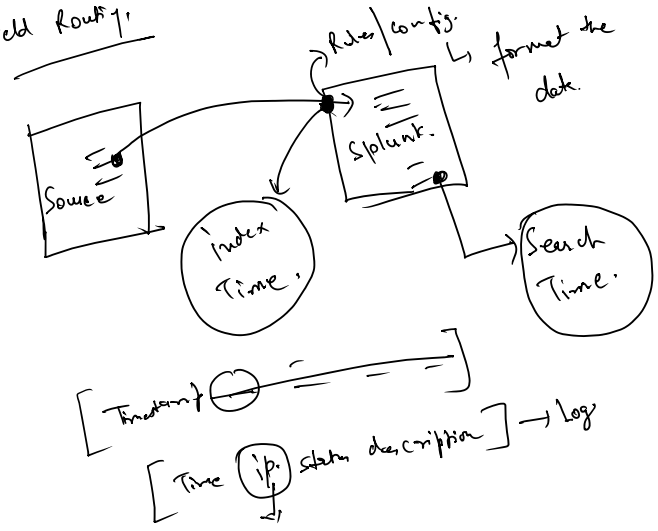
Day - 2N DAY - 3

07 October 2025 09:37

(4) Line Breaking

1. Timestamp extraction
2. event breaking
3. Index time field extraction
4. Field Routing



Event breaking / Timestamp Extraction.

+ sourcetype

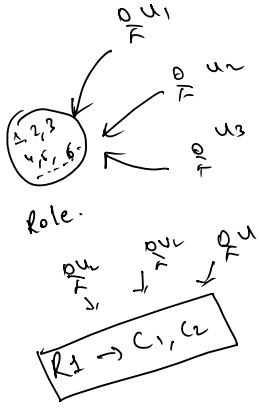
(1) Must_break_After
(2) Break_only_before
(3) Line_breaker
(4) Must_not_break_after

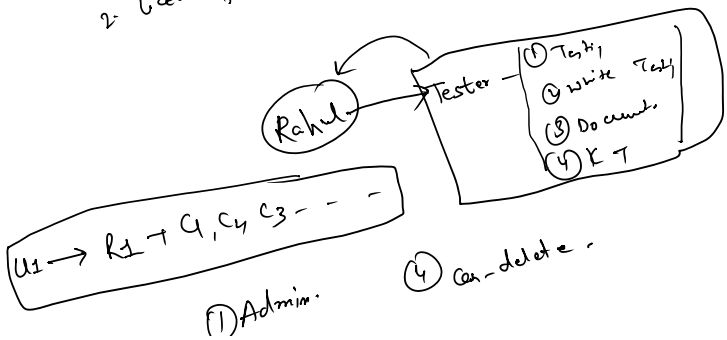
Index Time field extraction:-

Users & Role Authentication:-

1. Role
2. Capabilities
   ↓
   Set of Rules.

1. Edit: index → C1
2. License file → C2





U1 → K1

(1) Admin.
(2) Power
(3) User
(4) Can-delete.

(1) User - Basic Access, Read level.
(2) Power - Read/Write but only to its own Artifact.
(3) Admin - Overall access to the server.
(4) Can-delete - Delete the file/data.

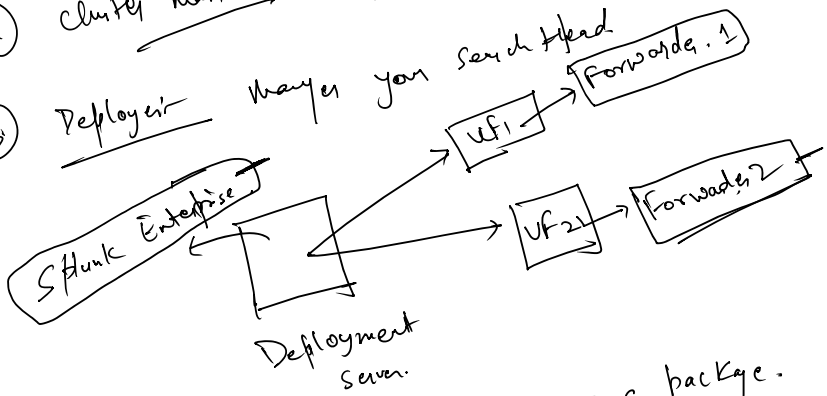
Admin will not be having can-delete role by default.

Clustering:-

(1) Deployment Server.
(2) Cluster Master.
(3) Deployer.

→ Manage instance.

(1) Deployment Server:- Manage your forwarder.
(2) Cluster Master:- Manage your indexer.
(3) Deployer:- Manages your search head

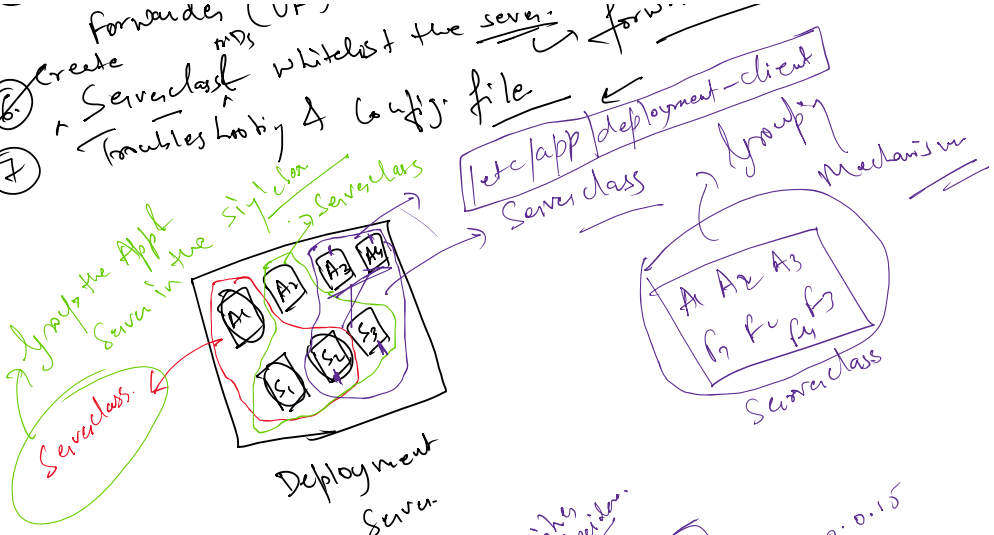


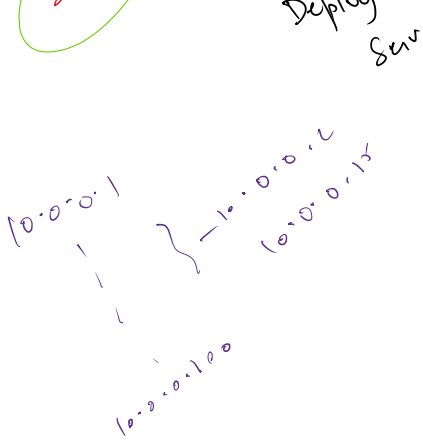
(1) Deployment Server → Splunk Enterprise as a package.
(2) UF1, UF2, → Splunk forwarder.
(3) Initialize the Server1 to act as Deployment Server.
(4) Create a Dummy App & Deploy on DS.
(5) Connect the Deployment Server with the forwarder (UF).
(6) Create serverclass.conf whitelist the server → forwarders.

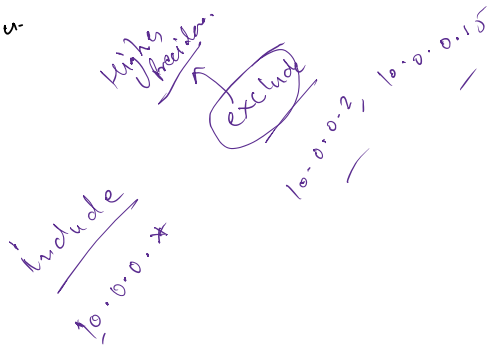
forwarder (UF)

⑥ Create Serverclass with whitelist the server → forw...

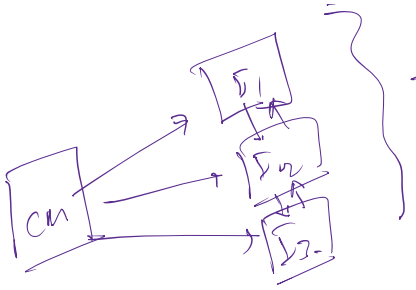
⑦ Troubleshooting & config. file







Cluster Master:-



→ ① Backup
② DR

① Replication factor → How many copy of raw data?

② Search factor → How many searchable copy you want to maintain?

Search factor ≤ Replication factor

2 ≤ 2

① Initialize the Server to Act as Cluster Master

② Connect the Indexer Peer with CM

③ Deploy the Dummy Appl from CM

④ Push the Appl to the peer Server

... file involve.

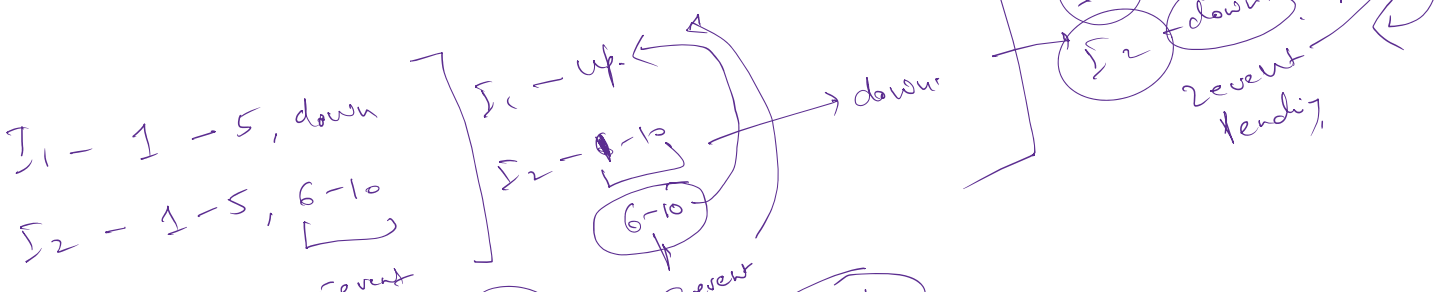
... Enterprise

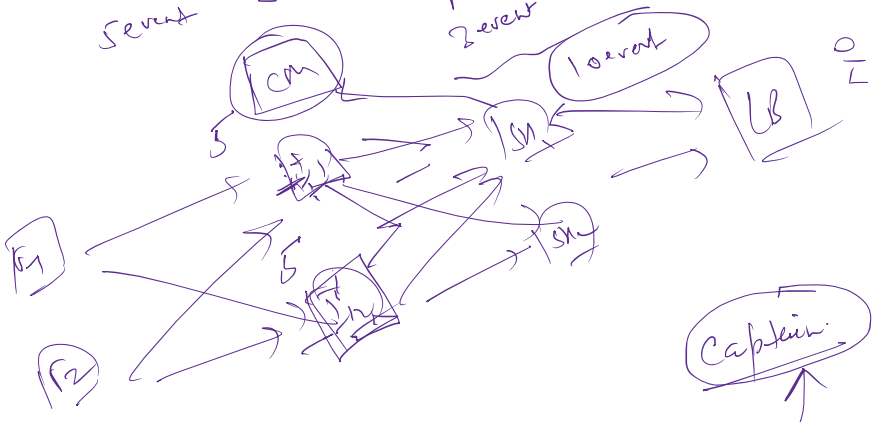
④ ⑤ Push the App to the
Troubleshoot & Config. file involve.

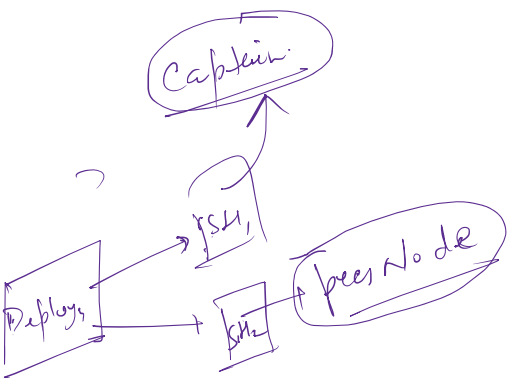
Server.conf → [clustering]

Install splunk Enterprise
in all the 3servers.

8000 - splunkweb
9997 - Receiver.
8089 - Indexer.
8080 - Indexer/Manager port.
8191 - KVstore







Search Head cluster:-

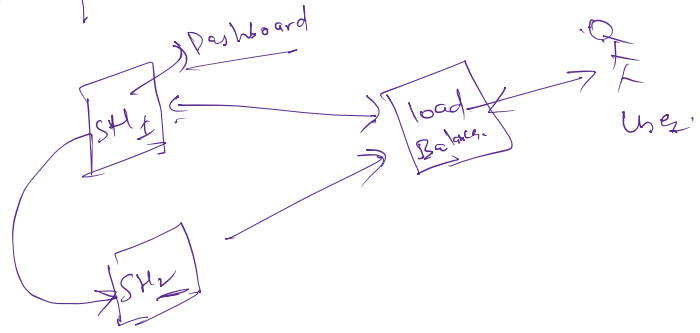
① Pre-install the SE in all

1. Reinstall the SE install 3 servers.
2. Initialize 1st Server to act as Deployer
3. connect the SH with the Deployer.
4. Election to elect one of the SH to be captain
   - Dynamic → Round Robin Method.
5. Deploy the app on Deployer.
6. Push app to the SH.
7. Troubleshooting, Validation & Config file involve.

./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>

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

Captain → parallel Syncing of the artifact.



Migration & upgrades

1. Management instances
2. Search Head.
3. forwarders

Upgrade plan

1. Pre implementation plan.
2. Implementation plan
3. Post Implementation plan.

④ Indexes.

① Pre implemation plan.

① local folder.

② Dashboards.

③ Reports.

④ Rate.

⑤ SE - 8.2.4.

lookup editor - Verify Verify

Sukey.

② Implementation Plan:

③ Post implemation

① Validation.

HEC - Http event collector.

↳ Token for token we will be

wig for the event collection.

Json