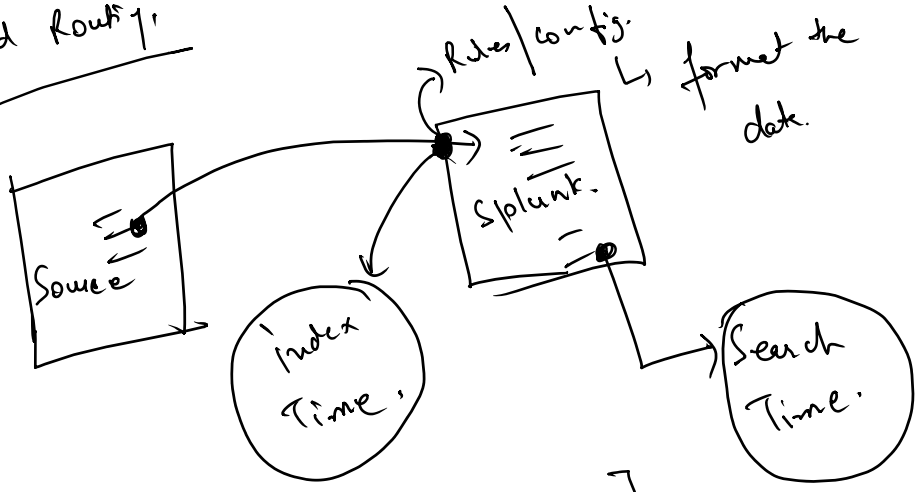
Day - 2

07 October 2025 09:37

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

Time Breaking



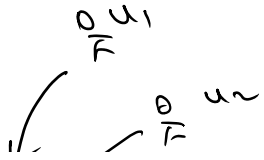

[Timestamp] → [Time ip. status description] → Log

Event breaking / Timestamp Extraction → + sourcetype

1. Must_break_After
2. Break_only_before
3. line_breaker
4. Must_not_break_after

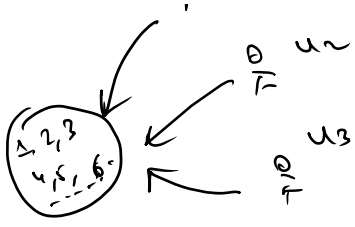
Index Time field extraction:-

Users & Role Authentication:-

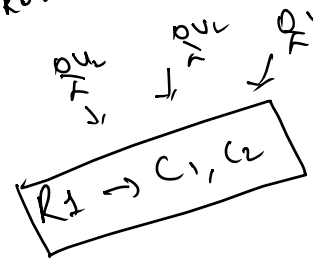


Users & Role

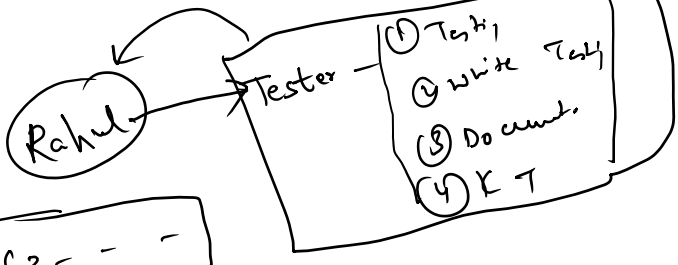
1. Role
2. Capabilities
   ↓
   Set of Rules.




Role.




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




U1 → R1 → C4, C4, C3 - - -

(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 :-

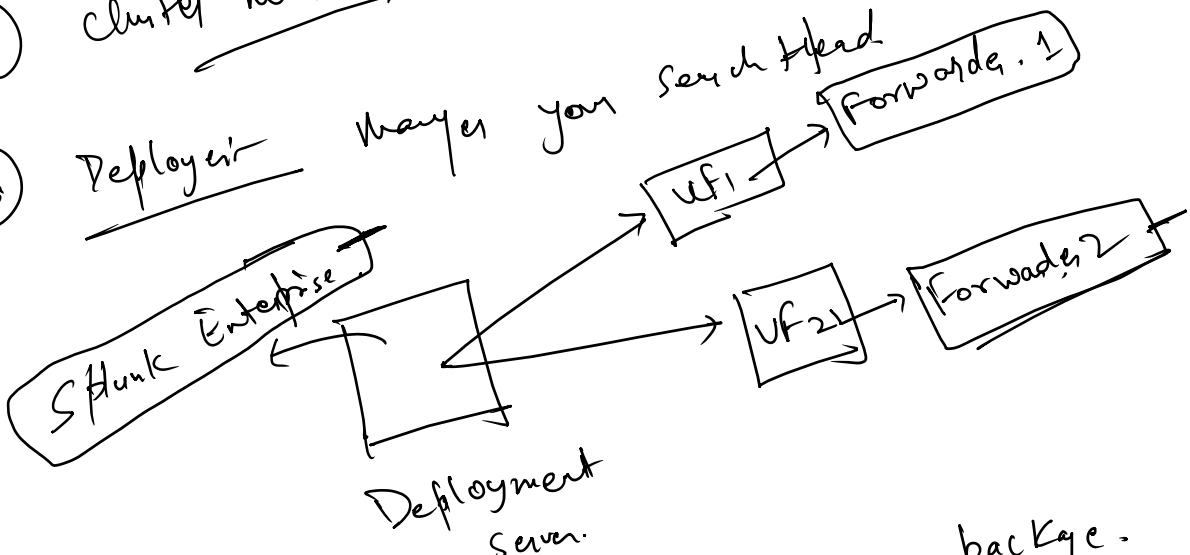
instance.

Clustering:

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

→ Manage instance.

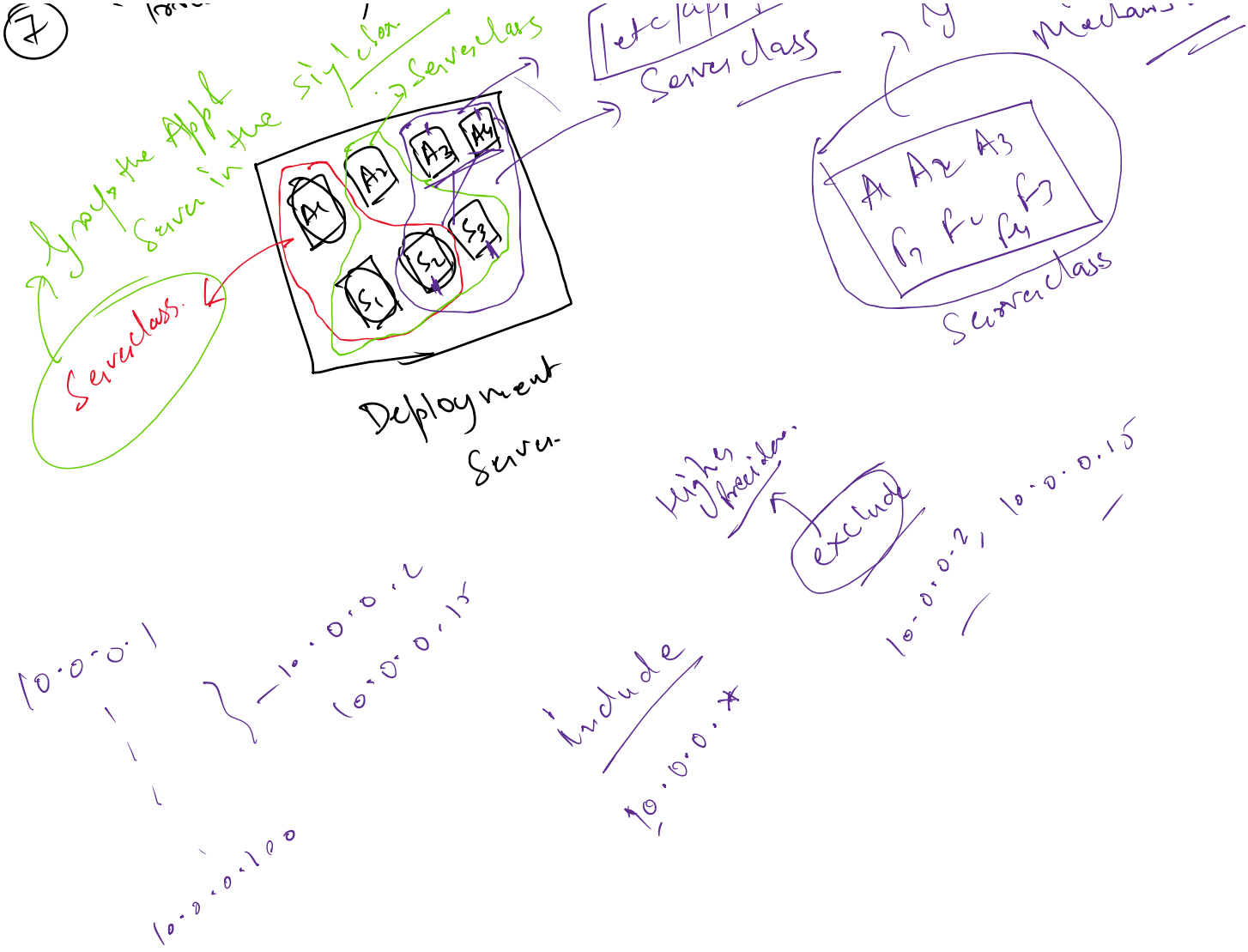
1. Deployment Server: Manage your forwarder.
2. Cluster Master: Manage your indexer.
3. Deployer: Manages your search head.




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 in DS whitelist the server. → forwarder.
7. Troubleshooting & Config. file

/etc/app/deployment-client

Serverclass → Grouping Mechanism


Deployment
Server
Serverclass
Serverclass
A A2 A3
f1 f2 f3
Serverclass
exclude
10.0.0.2, 10.0.0.15
include
10.0.0.*
10.0.0.1
10.0.0.2
10.0.0.15
10.0.0.100