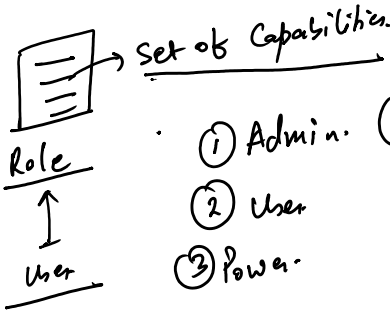
Day - 7

03 January 2025 14:34

1. User & Role Creation.
2. Eventbreaking.
3. Timestamp extraction.
4. Data ingestion using Heavy forwarder.

1. User & Role Creation:-



Capabilities:-

(1) Native -
(2) Inherited -

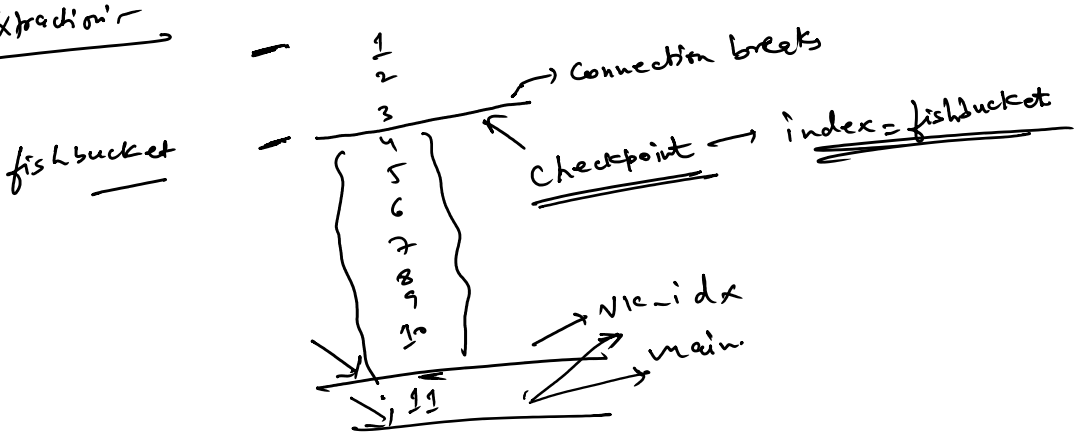
(1) Native:- Capabilities assigned to a particular Role.

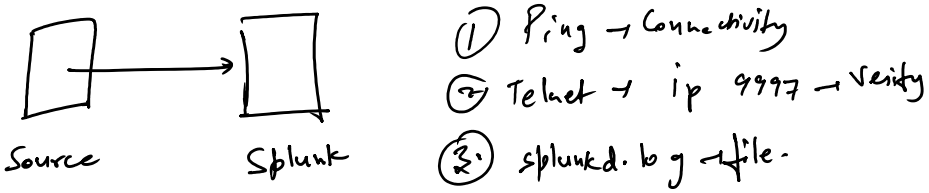
(2) Inherited:- Inherit set of Capabilities to a particular user.

(2.) Eventbreaking:-

Split the events on the basis of certain conditions.

(3.) Timestamp Extraction:-





index=_internal log_level=ERROR *read* source="/home/ec2-user/splunk/var/log/splunk/splunkd.log"

(4.) btool → Splunk Config.

(5.) ./splunk restart → error

(4.) btool → splunk config.

(5.) splunk restart → error