Day - 2

03 June 2025 18:37

Commands:-

1. Head
2. Tail
3. Dedup.
4. field

Knowledge object:-

1. Field extraction.
2. Alert & report
3. Dashboard — classic Dashboard

---

1. Field extraction:-
   - Delimiter.
   - Regular exp

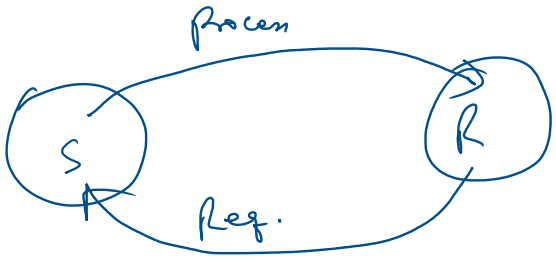
Rex Command:-

2. Alert & Report:-

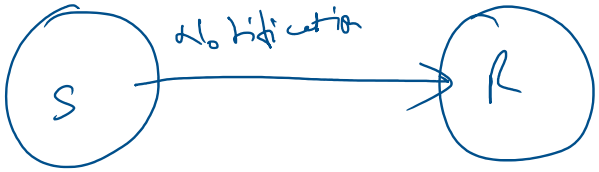
Report →
- [Description]
- [Schedule]
- [Notification]

Alert:-
- [Description]
- [Trigger Condition]
- [Trigger Notificati]

Webhook / API



API



Webhook

Tags & Eventtype:- → Categorize the data on the basis of certain condition

Categorize Data on the basis of certain value.

Macros:- function in splunk.

```
func a (b, c)
{
d = b + c;
return d;
}
```

→ ① Reusability of Code.
② Time taken will be less

Macros → Multi Arg.
→ No Arg.
→ Single Arg.

(a) (3, 4)

Multi Arg.

Calculated fields:- eval Kb = (byte | 1024)

Avoid recursive work

Calculated field → template → expression (every thing)

every time we call it.

Dashboard
- classic Dashboard → XML
- Studio Dashboard → json.

classic
- Static → fixed in nature.
- Dynamic → changeable filter

Drilldown

Dash board optimization