Day - 2

23 July 2024 10:08

1. geostats Command
2. Rex
3. join.
4. Append
5. Where.
6. Addtotal / Addcoltotal → Addition of the numeric field column wise.

Addtotal → Addition of numeric field Row wise

## 2) Rex :-

Field extraction is not happening.

Extract field → Regular expression → call in splunk → using Rex Command

Rex → 1. Extracting the Fields from Dataset
Rex → 2. Data Masking.

Account Number :- XXXXXX123 → Masking.

index
↳ sc
↳ source

Data Masking → Substitution Method
Data Masking → Replacement Method

Replacement Method :-
" s/<regex>/<replacement>/<flags> "

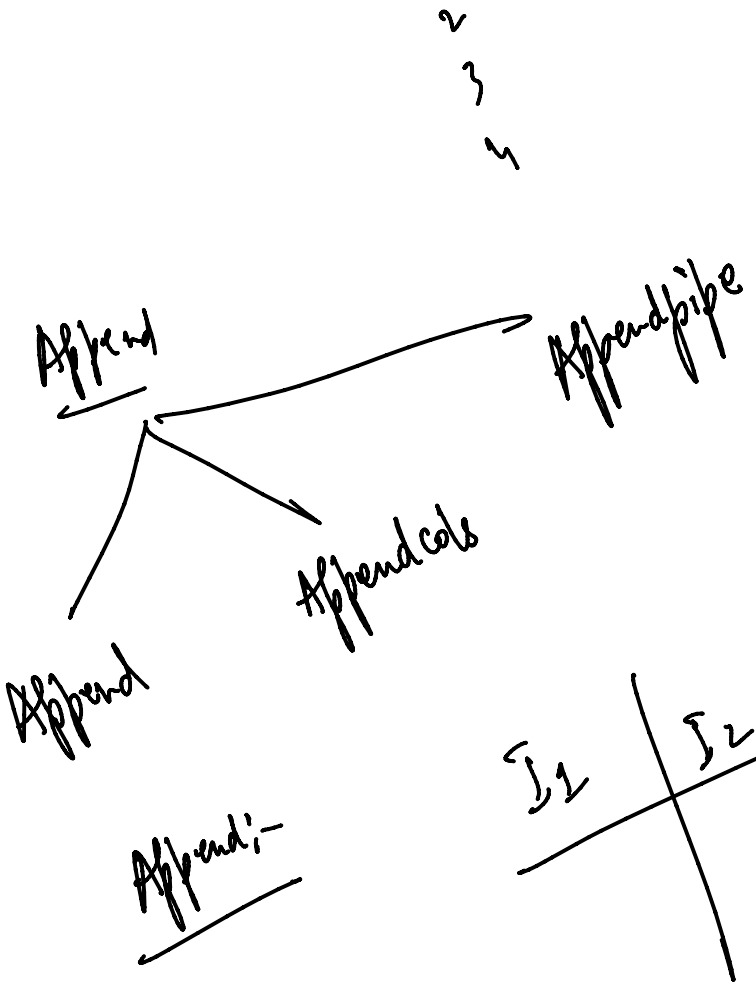
Substitution Method :-
" y/<string1>/<string2> "

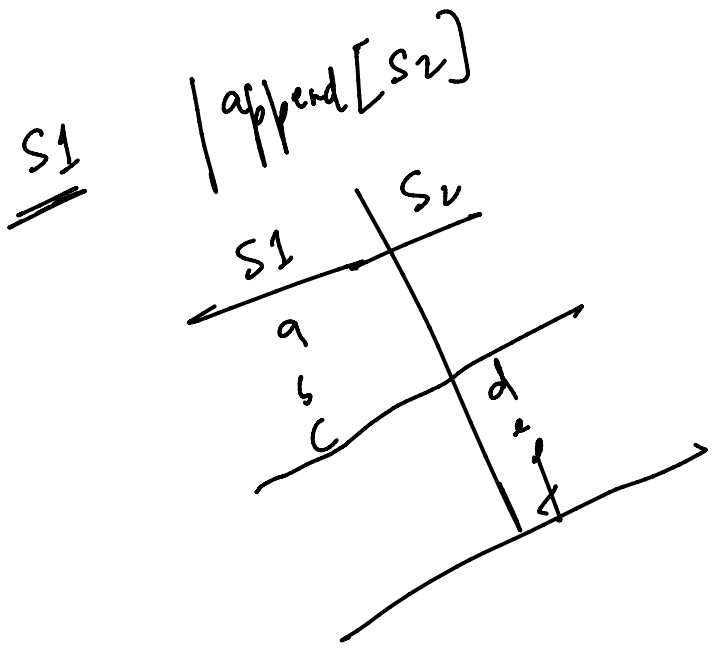
Searches ✓ Search / filter the value in the same field itself

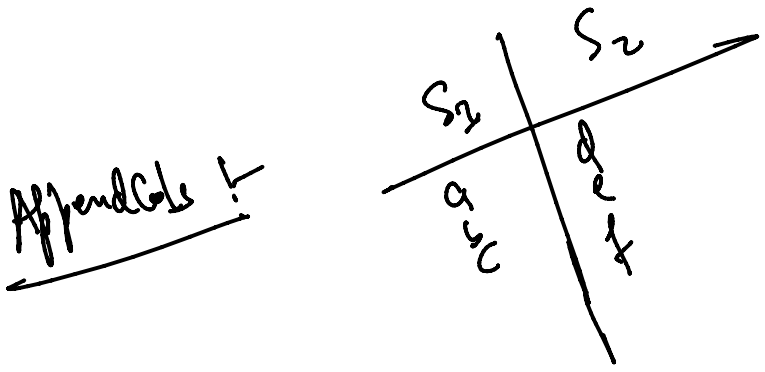
Severity, Severity=2
1

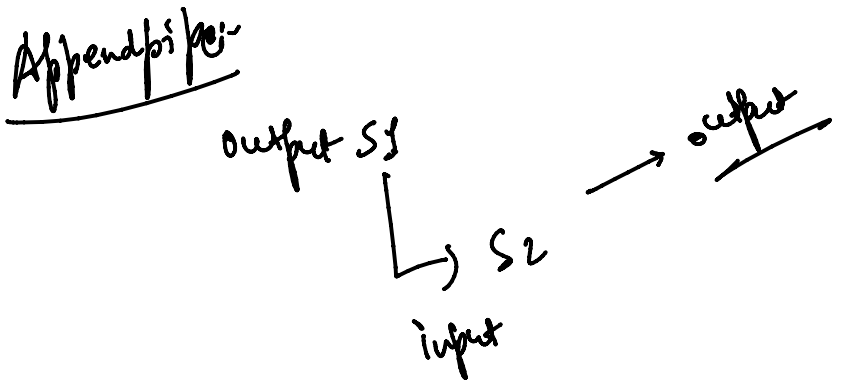
Where ✓ compare b/w two fields.
where count > threshold

| Sev | Count |
|---|---|
| 1 | 10 |
| 2 | 20 |
| 3 | 5 |

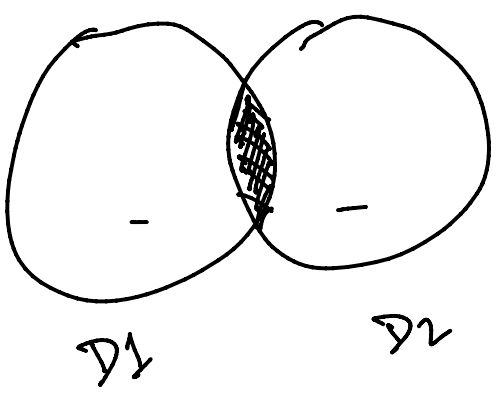


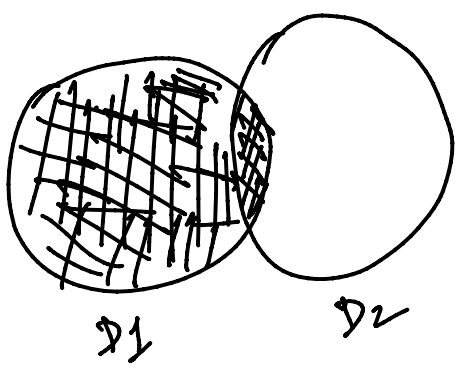



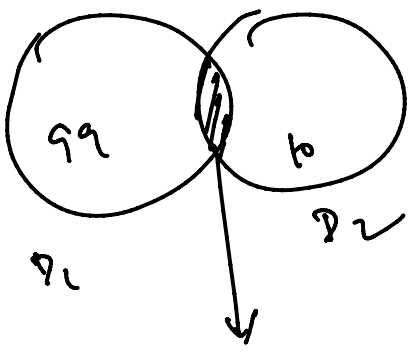

join:- Combine the dataset from two different index. At that time use join, using unique field.



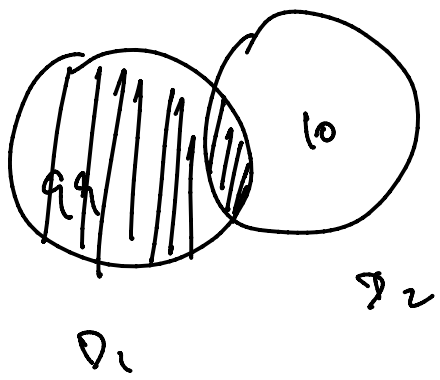

Innerjoin




Left join




Both the inner join




Outer

qq

## Knowledge object :-

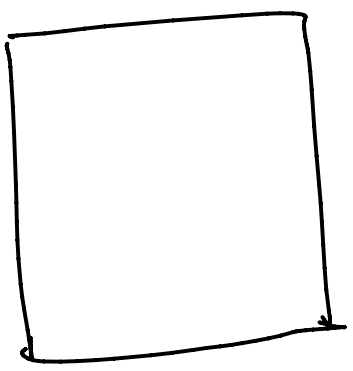
1. Tag.
2. Eventtype.
3. Field extraction → Regex, Delimiter
4. LookUp.
5. Workflow Action.
6. Data Model & Pivot.
7. Alert.
8. Report.
9. Field Alias.

① Tag :- Book | shop → shelf. → Category → Fiction, Non-fiction, Auto Bio. / Biography

Severity → 3 → Normal.

Field extraction :- Rex → extract the fields

Lookup :-



csv.

① csv file → small & static in nature.

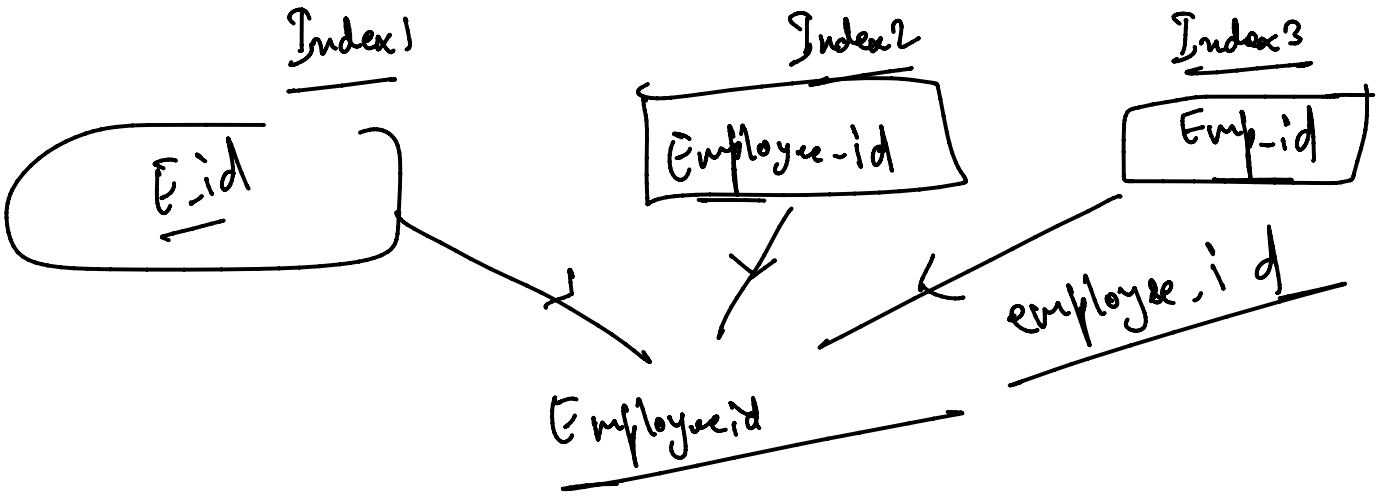
② lookup table in splunk
↓
upload
↓
to license.

③ Combine the index data & lookup

Field Alias :-

Employee-id

Employee_id

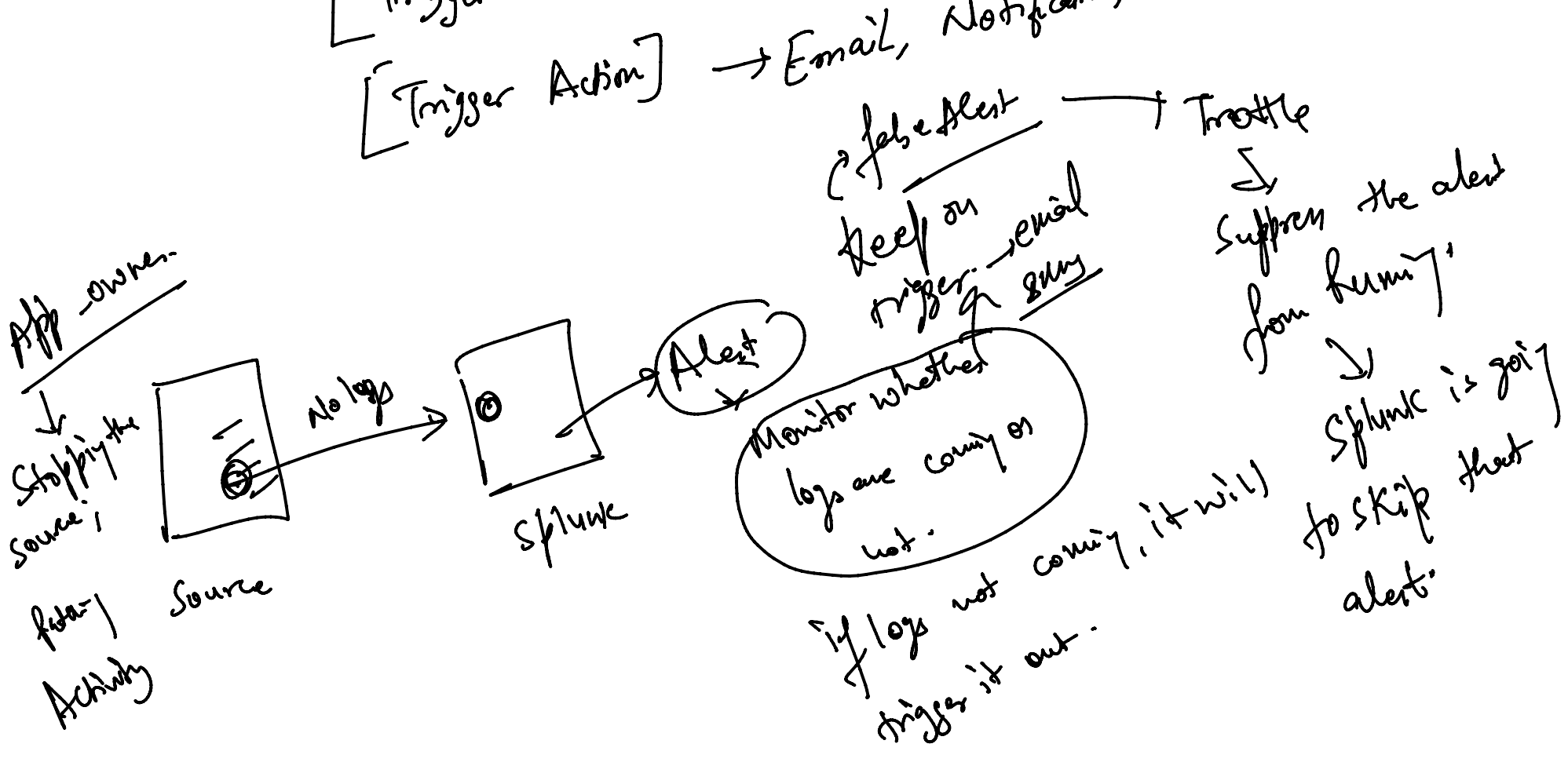



Alerts:-

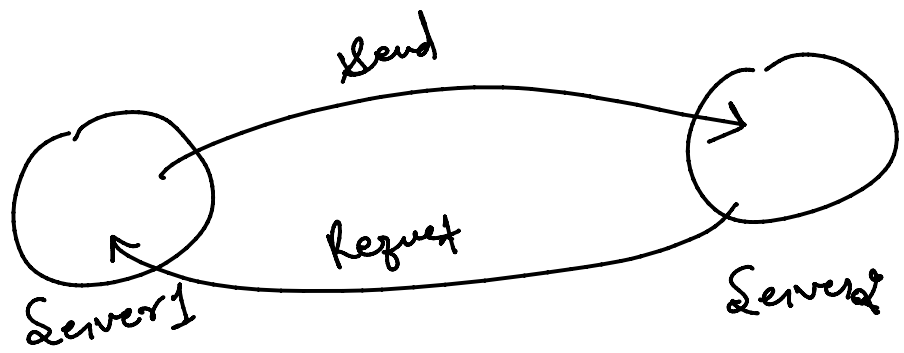
[Definition] → Search Query

[Trigger Condition] → Condition: Result > 0 ; count > 5

[Trigger Action] → Email, Notification, Webhook, SMS, Script.

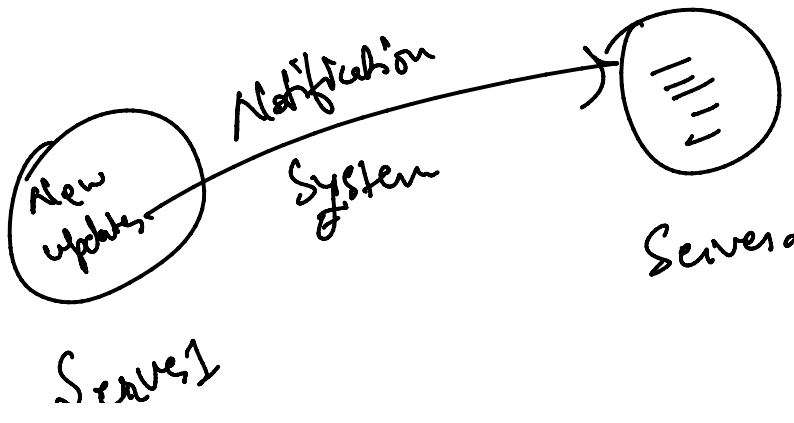



API :-




① Two way Communication.

Webhook




① One way Communication.

Server1

Reports- [Definition]

Not condition-

Whether condition will met or not.

[Trigger]

Work flow Action:-

When you want to sent a certain data from the source & other website

Asset. id:- Directory → Services.
google
external website-

24th july:-

1. Data Model & Pivot
2. Transaction.
3. classic Dashboard → saved search
→ Summary Index.