Day - 8

03 January 2025 18:15

1. Splunk DB Connect
2. Syslog.
3. Add-on.
4. Index time field extraction. → Props → Transforms
5. All the Config. file & folder structures.

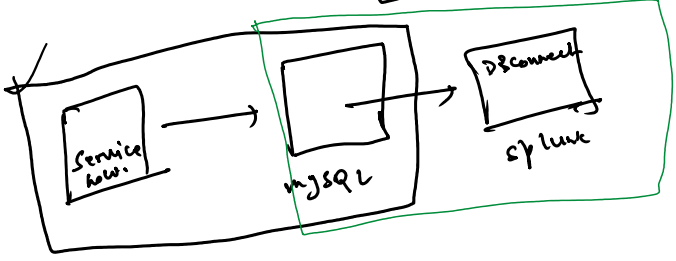
1. Splunk Aggregator:- → operator where combine data, from multiple data points into a single summarized value or dataset.

① stats → sum, count, avg
② timechart → events over time
③ chart → event over field
④ top / rare. →

2. Add-on: ① ServiceNow.

↳ ① Add servicenow account
↳ ② Add data input.
① incident
② RITM
③ CM

① Admin → Account (Read) → endusers / splunk admin.

② 

3. Index Time field extraction:-

[data is already ingested. → | rex →] extraction.

③ Index Time field extraction

field extraction → search time extraction.

field extraction → Index time field extraction

↓

During the ingestion time, we are going to pull the data.

1. event breaking.
2. timestamp extraction
3. Props + transforms → extraction → Rex.

Write_meta:- Metadata [sourcetype, host, source, index]

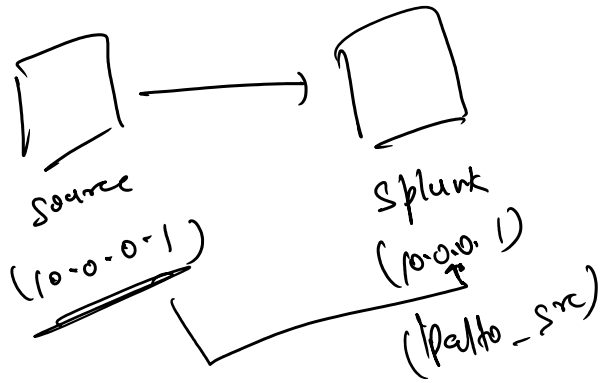
host = 10-0-0-1

Props.conf → sourcetype

① [ ]

② [source::] →

③ [host::] →



Write_meta

Write → Manipulate the data using Metadata info.

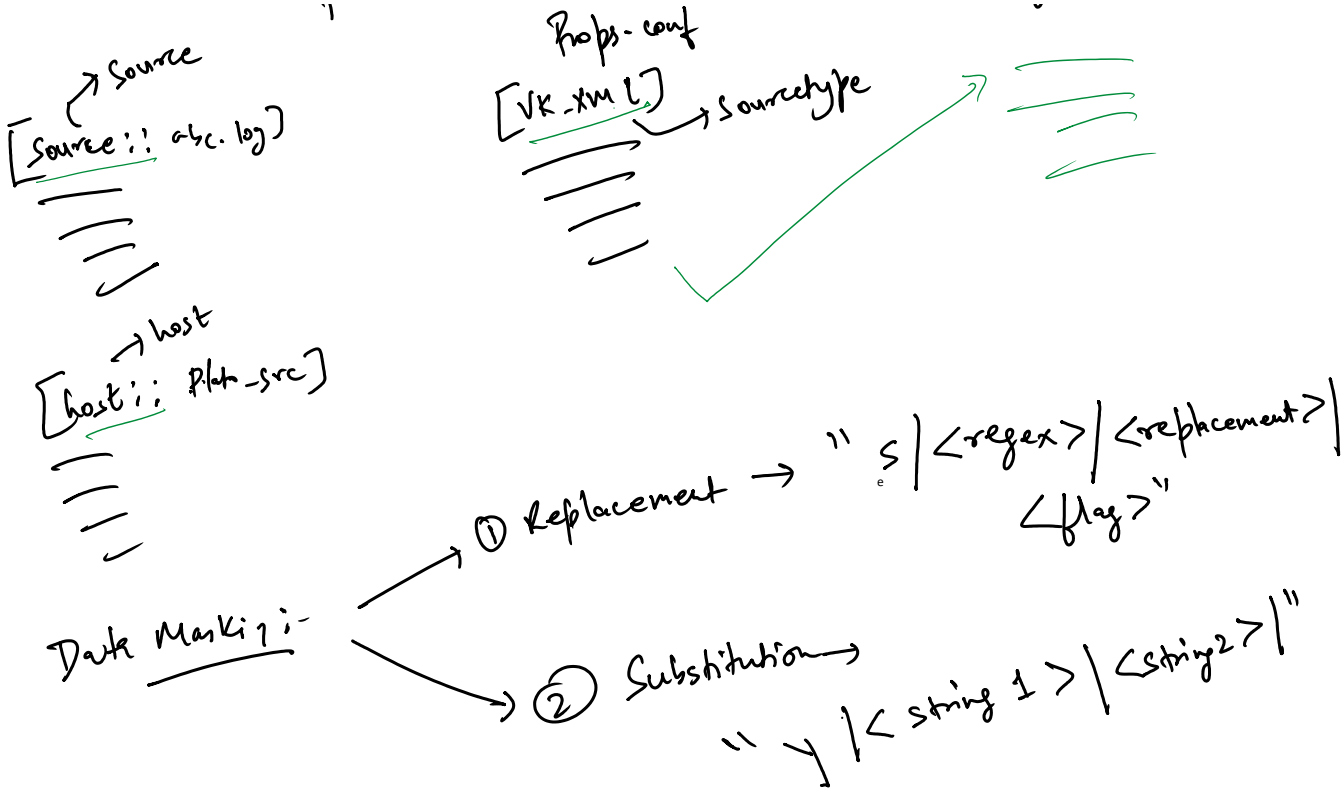
Meta → Metadata → [host, Index, source, Sourcetype]

Props.conf

[...] ...sourcetype

transforms.conf

→ Source



splunk/etc/apps --- List of Applications

Search ---

drwxr-xr-x. 3 ec2-user ec2-user 20 Dec 11 02:12 appserver ---- JS, HTML & CSS, Images
drwxr-xr-x. 2 ec2-user ec2-user 94 Dec 11 02:12 static --- App Icon
drwxr-xr-x. 2 ec2-user ec2-user 26 Dec 11 02:12 metadata --- Permission of the knowledge object
drwxr-xr-x. 2 ec2-user ec2-user 130 Dec 11 02:12 lookups --- Lookup file saved in this folder
drwxr-xr-x. 3 ec2-user ec2-user 180 Dec 11 02:12 default --- All the pre-defined Config file saved over their
Splunk/etc/apps/search/default/data/ui/views --- Dashboard XML Files are saved over here
splunk/etc/apps/search/default/data/ui/nav --- file default.xml, it will define the list in the header tab.
splunk/etc/apps/search/default/data/models --- Data Model Json file will be saved over their
drwxr-xr-x. 2 ec2-user ec2-user 16384 Dec 11 02:12 bin ---- Executable file saved in bin folder (All the Python files)
splunk/etc/licenses --- License file saved over here
splunk/etc/deployment-apps --- All the application pushed from the deployment server will be saved in this folder
splunk/etc/manager-apps --- All the application pushed from cluster master will be saved in this folder
splunk/etc/shcluster --- All the application pushed from Deployer will be saved in this folder
splunk/etc/auth --- Certificates installed over their
splunk/etc/users --- List of user activity
splunk/var/log/splunk --- List of Splunk Log files saved in this folder
splunk/var/lib/splunk --- List of indexes and the respective buckets
splunk/include --- Python package Location