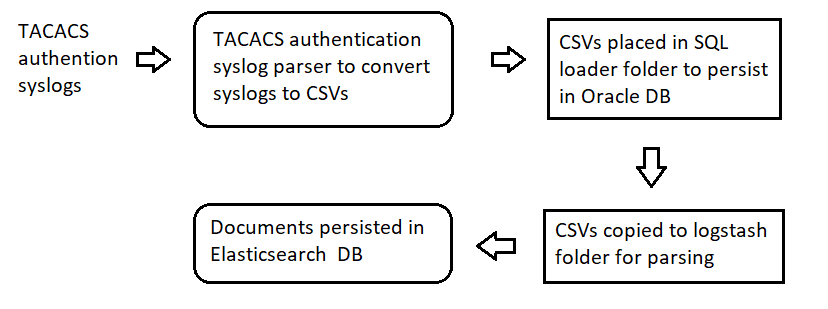
**TACACS authentication discrepancy issue**

Discrepancy issue and invalid documents observed in elasticsearch DB for TACACS authentication traffic being sent from PEZ tool of SST team. It was challenging to find the RCA because there were multiple reasons this might get affected.

**System design:**

TACACS authentication syslogs will be parsed and converted into CSVs by respective syslog parser, further CSVs will be placed in SQL loader folder. Tauth SQL loader scan destine folder to persist data in Oracle db. We copied CSVs from loader folder and placed inside Logstash folder, CSVs will be parsed by logstash and placed inside Elasticsearch DB.



**Steps to reproduce the issue:**

1. Use PEZ tool of SST team and trigger 500000 TACACS Authentication traffic with stress count 1024.
2. Elasticsearch DB was failing to persist all documents, and some were observed as invalid because if missing in some records
3. From my observation, I also found out that there were missing records in Oracle db as well

**Values reflected in both DBs post traffic being sent,**

|  |  |  |
| --- | --- | --- |
| **TACACS Authentication** | **Count** | **Missing records** |
| **Traffic sent** | **521618** |  |
| **Oracle DB** | **444997** | **76621** |
| **Elastic DB** | **509528** | **12090** |

**Root cause analysis:**

**A. Elasticsearch DB discrepancy issue:**

While debugging I found out that issue was with Logstash codec plugin, which was failing to parse the TACACS authentication CSVs with multiline gibberish characters appended in each document. And there was no plugin supported from Logstash end to fix this issue.

**B. Oracle DB discrepancy issue.**

Records were dropping because large number of files got appended to individual file and further bulky file fed to SQL loader to process.

**Solution:**

**A. Elasticsearch DB discrepancy issue:**

Instead relying on Logstash, I added cron job which does following functionalities,

1. CSVs from SQL loader folder copied to temporary folder
2. Filtering out gibberish characters from each document in CSV
3. Valid CSVs further placed into destined Logstash folder to parse and place documents in Elasticsearch DB

**B. Oracle DB discrepancy issue.**

Modified SQL loader file to optimize the file processing in each run.