KB 004 – ABAP Extractor SM04

Symptom: What does the SM04 collector extract from SAP and send to Splunk

The SM04 collector runs every hour

And executes function module /BNWVS/CL_EXT_SM04

Prerequisites: None.

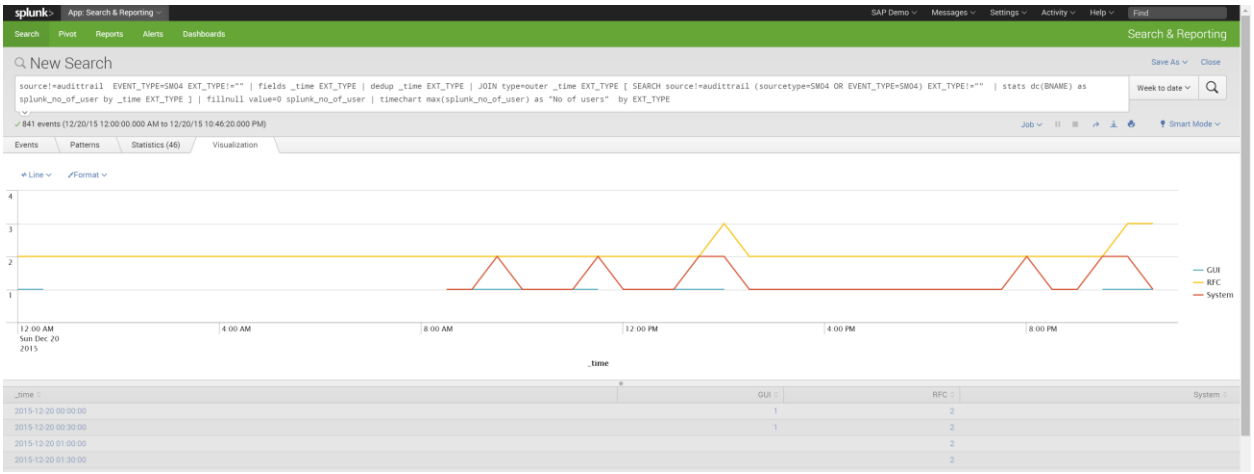
Fields: The following fields are sent to Splunk

These fields map to the ABAP dictionary types available in tcode SM20.

Reports: What reports can I run against this data?

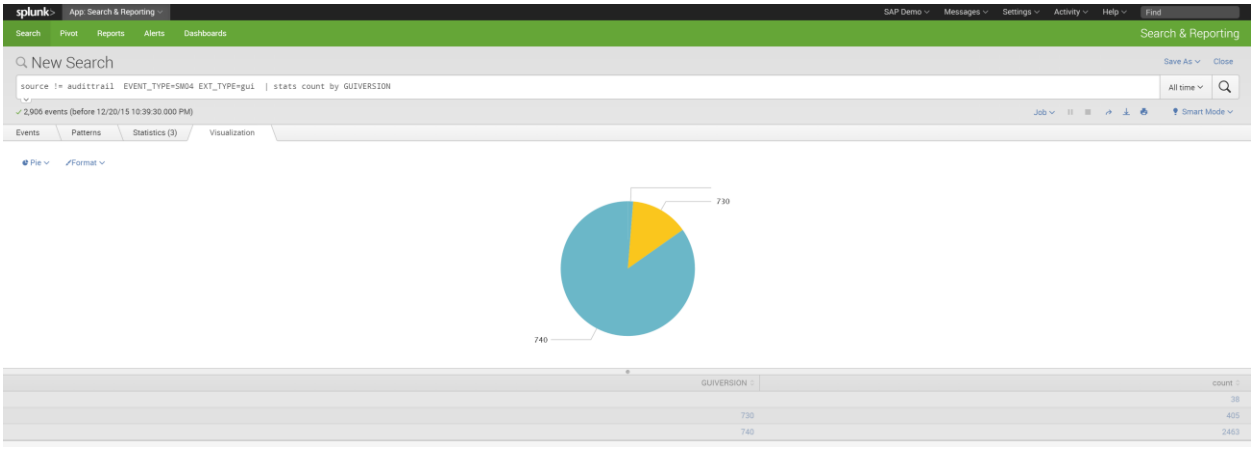
Example1: Reporting the number of users logged in

source!=audittrail EVENT_TYPE=SM04 EXT_TYPE!="" | fields _time EXT_TYPE | dedup _time EXT_TYPE | JOIN type=outer _time EXT_TYPE [SEARCH source!=audittrail (sourcetype=SM04 OR EVENT_TYPE=SM04) EXT_TYPE!="" | stats dc(BNAME) as splunk_no_of_user by _time EXT_TYPE] | fillnull value=0 splunk_no_of_user | timechart max(splunk_no_of_user) as "No of users" by EXT_TYPE



Example2: Reporting the number of users and their SAPGui version in use

source != audittrail EVENT_TYPE=SM04 EXT_TYPE=gui | stats count by GUIVERSION


splunk>
App: Search & Reporting
SAP Demo
Messages
Settings
Activity
Help
Find
Search
Pivot
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Close
source != audittrail EVENT_TYPE=SM04 EXT_TYPE=gui | stats count by GUIVERSION
All time
2,906 events (before 12/20/15 10:39:30.000 PM)
Job
Smart Mode
Events
Patterns
Statistics (3)
Visualization
Pie
Format
730
740
GUIVERSION
count
730
405
740
2463