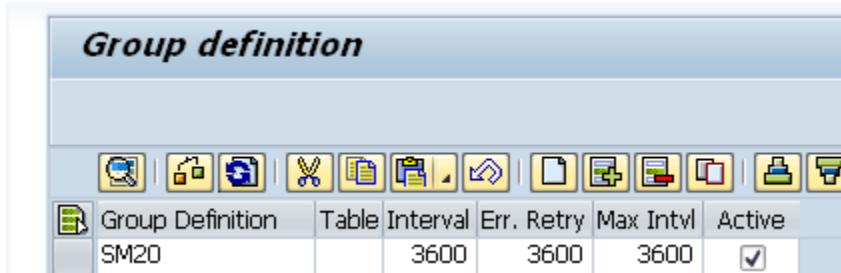


KB 003 – ABAP Extractor SM20

Symptom: What does the SM20 collector extract from SAP and send to Splunk

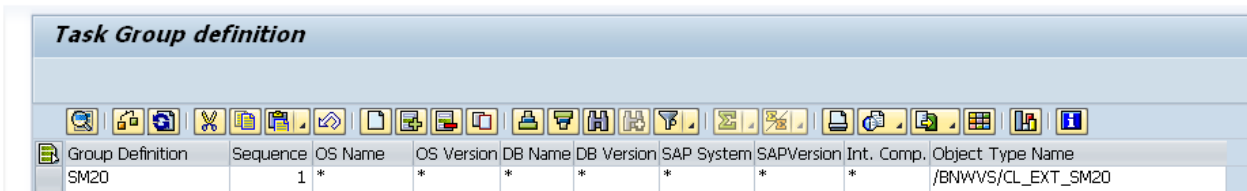
The SM20 collector runs every hour



The screenshot shows the 'Group definition' table in SAP. The table has columns for Group Definition, Table, Interval, Err. Retry, Max Intvl, and Active. The row for SM20 shows an interval of 3600, an error retry of 3600, a maximum interval of 3600, and is marked as active with a checked box.

Group Definition	Table	Interval	Err. Retry	Max Intvl	Active
SM20		3600	3600	3600	<input checked="" type="checkbox"/>

And executes function module /BNWVS/CL_EXT_SM20



The screenshot shows the 'Task Group definition' table in SAP. The table has columns for Group Definition, Sequence, OS Name, OS Version, DB Name, DB Version, SAP System, SAPVersion, Int. Comp., and Object Type Name. The row for SM20 shows a sequence of 1, OS Name of *, OS Version of *, DB Name of *, DB Version of *, SAP System of *, SAPVersion of *, Int. Comp. of *, and Object Type Name of /BNWVS/CL_EXT_SM20.

Group Definition	Sequence	OS Name	OS Version	DB Name	DB Version	SAP System	SAPVersion	Int. Comp.	Object Type Name
SM20	1	*	*	*	*	*	*	*	/BNWVS/CL_EXT_SM20

Prerequisites: For this collector to work the SAP Audit log must be configured in SAP tcode SM19 and active. If you can see the audit information in SM20 then it will be collected by SAP PowerConnect for Splunk and sent to the Splunk server.

Fields: The following fields are sent to Splunk

splunk> App: Search & Reporting

Search Pivot Reports Alerts Dashboards

New Search

EVENT_TYPE=SM20

193,252 of 193,252 events matched

Events (193,252) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection x Deselect

Dec 18, 2015 5:00 PM

List Format 20 Per Page

i	Time	Event
>	12/20/15 9:56:58.000 PM	<pre>{ [-] ALGAREA: AU ALGCLIENT: 100 ALGDATE: 20151220 ALGFILENO: 000001 ALGFILEPOS: 0013249080 ALGINST: SAPN71D_N71_00 ALGLTERM: ALGREPNA: SAPMSSY1 ALGSUBID: K ALGSYSTEM: SAPN71D ALGTASKNO: 005 ALGTASKTYPE: D ALGTCODE: ALGTEXT: Successful RFC Call THUSRINFO (Function Group = STUN) ALGTIME: 215658 ALGUSER: DDIC EVENT_TYPE: SM20 IPADDRESS: PARAM1: STUN PARAM2: PARAM3: THUSRINFO PARAM4: TIMESTAMP: 20151220105658.0000000 TXSEVERITY: Severe and critical TXSUBCLSID: RFC call }</pre> <p>Show as raw text</p> <p>host = SAPN71D source = N71 sourcetype = sap_abap</p>

Selected Fields

- a host 1
- a source 1
- a sourcetype 1

Interesting Fields

- a ALGAREA 1
- # ALGCLIENT 1
- # ALGDATE 3
- # ALGFILENO 1
- # ALGFILEPOS 100+
- a ALGINST 1
- a ALGLTERM 4
- a ALGREPNA 100+
- a ALGSUBID 6
- a ALGSYSTEM 1
- # ALGTASKNO 13
- a ALGTASKTYPE 2
- a ALGTCODE 9
- a ALGTEXT 100+
- # ALGTIME 100+
- a ALGUSER 4
- # date_hour 24

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

Analysis of Security Audit Log

Period Requested 20.12.2015 21:00:00 - 20.12.2015 22:12:06
 Period Selected 20.12.2015 21:00:01 - 20.12.2015 22:11:57
 Server
 Audit Classes
 Dialog Logon
 RFC/CPIC Logon
 RFC Function Call
 Transaction Start
 Report Start
 User Master Change
 Other Events
 System Events

Creation Date	Date/Time	User Name	Terminal	TCode	Program	Security Audit Log message text
20.12.2015	21:00:01	DDIC			SAPMSSY1	RFC/CPIC Logon Successful (Type = F)
20.12.2015	21:00:01	DDIC			SAPMSSY1	Successful RFC Call /BNWVS/PARALLEL_METRIC (Function Group = /BNWVS/MTR_FUNCTIONS)
20.12.2015	21:00:02	DDIC			SAPMSSY1	RFC/CPIC Logon Successful (Type = F)
20.12.2015	21:00:02	DDIC			SAPMSSY1	Successful RFC Call /BNWVS/PARALLEL_METRIC (Function Group = /BNWVS/MTR_FUNCTIONS)

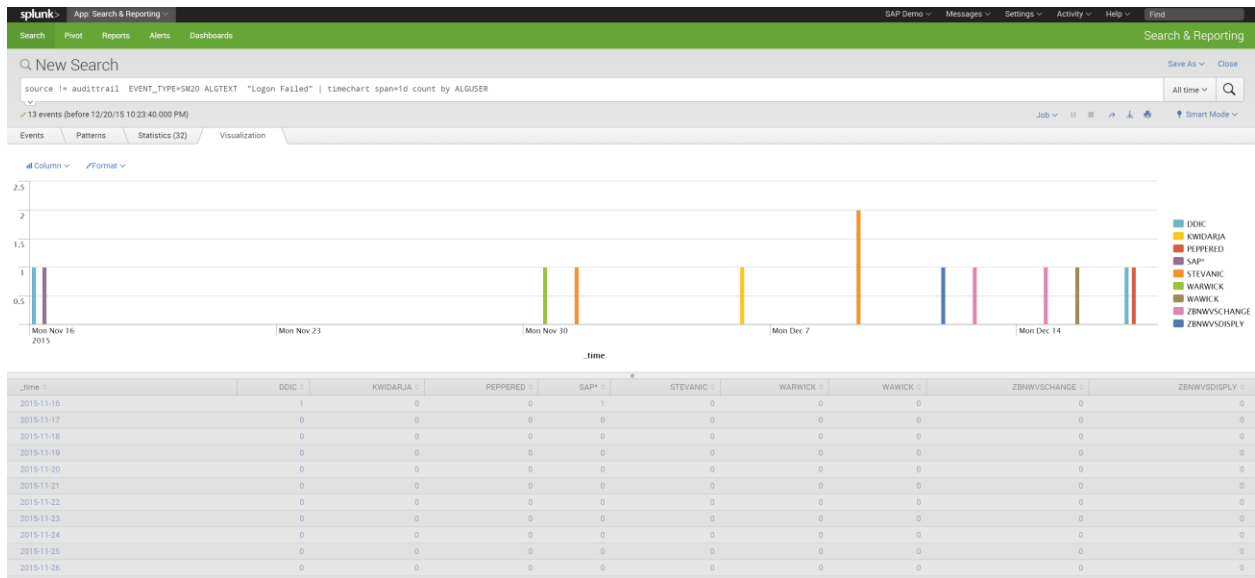
Group description	Cell Content
Server Name	SAPN71D
Creation Date	20.12.2015
Instance name	SAPN71D_N71_00
Creation time of audit entry	21:00:01
User Name	DDIC
Work Process Type	D
Program	SAPMSSY1
Work Process Number	003
Client	100
Security Audit Log message text	RFC/CPIC Logon Successful (Type = F)
SysLog msg. group	AU
Sub-name	5
Audit class	RFC logon
Security Level	Severe and critical
File Number	1
Address in File	12744900
Parameter 1	F
Parameter 2	0
Parameter 3	R

Reports: What reports can I run against this data?

Example1: Recording failed logins.

By running a search query where the login text contains the text "Failed" you can find the number of failed logins per day.

```
source != audittrail EVENT_TYPE=SM20 ALGTEXT "Logon Failed" | timechart span=1d count by ALGUSER
```



Drilling down on the raw data show us the IP address from where the user logged in from and their terminal ID.

New Search

source != audittrail EVENT_TYPE=SM20 ALGTEXT "Logon Failed" ALGUSER=STEVANIC

✓ 2 events (12/9/15 12:00:00.000 AM to 12/10/15 12:00:00.000 AM)

Events (2)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

List

Format

20 Per Page

< Hide Fields

All Fields

Selected Fields

a host 1

a source 1

a sourcetype 1

Interesting Fields

a ALGAREA 1

ALGCLIENT 1

ALGDATE 1

ALGFILENO 1

ALGFILEPOS 1

a ALGINST 1

a ALGLTERM 1

a ALGREPNA 1

ALGSUBID 1

a ALGSYSTEM 1

ALGTASKNO 1

a ALGTASKTYPE 1

a ALGTCODE 1

a ALGTEXT 1

ALGTIME 1

i

Time

Event

>

12/9/15

{ [-]

9:11:00.000 AM

```

ALGAREA: AU
ALGCLIENT: 100
ALGDATE: 20151209
ALGFILENO: 000001
ALGFILEPOS: 0000858060
ALGINST: SAPN71D_N71_00
ALGLTERM: stevanic-PC
ALGREPNA: SAPMSYST
ALGSUBID: 2
ALGSYSTEM: SAPN71D
ALGTASKNO: 005
ALGTASKTYPE: D
ALGTCODE: SESSION_MANAGER
ALGTEXT: Logon Failed (Reason = 1, Type = A)
ALGTIME: 091100
ALGUSER: STEVANIC
EVENT_TYPE: SM20
IPADDRESS: 10.5.1.22
PARAM1: A
PARAM2: 1
PARAM3: P
PARAM4:
TIMESTAMP: 20151208221100.0000000
TXSEVERITY: All
TXSUBCLSID: Logon
  
```

}