SDS

z/OS Security Webinar

Automatically Deliver Filtered z/OS Security Event Records to your SIEM

About Us

Quality Mainframe Software since 1982

- Expert development & technical support teams based in Minneapolis, MN.
- 25+ products for z/OS, z/VM, z/VSE, and distributed platforms.
- Hundreds of organizations worldwide rely on SDS solutions.
- Focus on mainframe security and compliance.
- Cost savings and legacy tool replacements: DO MORE WITH LESS!
- Long-standing global partnerships complement SDS software.
- Recognized for providing highest quality technical support.

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

Silver Business Partner IBM

database TREND-SETTING PRODUCTS 2020

Presenters

Colin van der Ross

Sr. Systems Engineer

SMF record types overview, filtering options, VSA demo.

Jed Lampi

Operations/Marketing Lead

Introduction

Gain Real-Time Visibility into Z

Agenda

- Why filter events from z/OS to your SIEM ?
- VSA Filtering options
- Live Demo sending selected events to Splunk using VSA Filtering

Gain Real-Time Visibility into Z

Why should you filter ?

- z/OS has many SMF records that can be enabled
  - Most SMF records have subtypes
- Customer sites are selective on what SMF records are enabled because of the sheer volume of SMF records
- DASD considerations if too much is enabled
- Customers should apply “separation of duties” principles to decide what events to be forwarded to the SIEM

Gain Real-Time Visibility into Z

Why should you filter ?

- SIEM Pricing model is different
- Most SIEM vendors use the quantity of events collected to determine cost
- Smaller customers with a limited budget often “throttle” back on events to be sent to the SIEM
- Annual costs of a SIEM can run from $10,000 to over $100,000

Gain Real-Time Visibility into Z

Why should you filter ?

- According to some market research studies, SIEM and related technologies were a $5.3 billion market in 2018
- It is expected to grow at a compound annual growth rate of 19.7 % to $12.9 billion by 2023
- Fastest growing segment of the market
- Customers should be selective on what SMF events are sent to the SIEM
- Hence the need to filter events on z/OS

Gain Real-Time Visibility into Z

VSA Filtering

- Complex filtering allows you to escalate or suppress SMF records at the field level
- Data Dictionary containing over 900 individual fields and Boolean values, together with filtering semantics that provide you with unprecedented control over the decision to escalate a record into a SIEM or drop it from consideration

VSA Filtering – SMF14 /15 (DSN Activity)

Name	FORMAT	Len	Description
SMF14TME	SMFTIME	4	Time since midnight, in hundredths of a second, that the record was moved into the SMF buffer.
SMF14DTE	SMFDATE	4	Date when the record was moved into the SMF buffer, in the form 0cyydddF.
SMF14SID	DSTRING	4	System identification (from the SID parameter).
SMF14JBN	EBCDIC	8	Job name. The job name, time, and date that the reader recognized the JOB card (for this job) constitute the job log identification, or transaction name (for APPC output).
SMF14UID	EBCDIC	8	User-defined identification field (taken from common exit parameter area, not from USER=parameter on job statement).
First byte of SMF14RIN: Record Indicators			
SMF14EOV	BOOLEAN	-	Record written by end of volume (EOV). (Bit 1 of SMF14RIN)
SMF14DAD	BOOLEAN	-	DASD. (Bit 2 of SMF14RIN)
SMF14TDS	BOOLEAN	-	Temporary data set. (Bit 3 of SMF14RIN)
SMF14DDA	BOOLEAN	-	DCBDSORG=DA (the data set organization being used is direct access-BDAM). (Bit 4 of SMF14RIN)
SMF14IS	BOOLEAN	-	DCBDSORG=IS and DCBMACRF not EXCP (the data set organization being used is indexed sequential and the EXCP access method is not being used). (Bit 5 of SMF14RIN)
SMF14JIS	BOOLEAN	-	JFCDSORG=IS (the data set organization being used is indexed sequential). (Bit 6 of SMF14RIN)
SMF14VIO	BOOLEAN	-	Virtual input output (VIO) data set access. (Bit 7 of SMF14RIN)
Second byte of SMF14RIN			
SMF14IPD	BOOLEAN	-	Partitioned data set directory entries (PDSE) data set. (Bit 0 of SMF14RIN+1)
SMF14TRC	BOOLEAN	-	The QSAM TRUNC macro has been issued against a PDSE. (Bit 1 of SMF14RIN+1)
SMF14NSG	BOOLEAN	-	Null segment encountered in a PDSE. (Bit 2 of SMF14RIN+1)
SMF14STR	BOOLEAN	-	Extended format sequential data set indicator. (Bit 3 of SMF14RIN+1)
SMF14HBT	BOOLEAN	-	Hiperbatch section present. (Bit 4 of SMF14RIN+1)

VSA Filtering – SMF 17 (Delete of DSN)

Name	FORMAT	Len	Description
SMF17TME	SMFTIME	4	Time since midnight, in hundredths of a second, when the record was moved into the SMF buffer.
SMF17DTE	SMFDATE	4	Date when the record was moved into the SMF buffer, in the form 0cyydddF.
SMF17SID	DSTRING	4	System identification (from the SID parameter).
SMF17JBN	EBCDIC	8	Job name. The job name, time, and date that the reader recognized the JOB card (for this job) constitute the job log identification, or transaction name (for APPC output).
SMF17RST	SMFTIME	4	Time since midnight, in hundredths of a second, that the reader recognized the JOB card (for this job).
SMF17RSD	SMFDATE	4	Date when the reader recognized the JOB card (for this job), in the form 0cyydddF.
SMF17UID	EBCDIC	8	User-defined identification field (taken from common exit parameter area, not from USER=parameter on job statement).
SMF17DSN	EBCDIC	44	Data set name.
SMF17FVL	EBCDIC	6	List of volume serial numbers. The filter engine will scan the list for a match to the comparand.

VSA Filtering – SMF 30 Job Step Termination, Batch TSO, STC

Name	FORMAT	Len	Description
SMF30TME	SMFTIME	4	Time since midnight, in hundredths of a second, that the record was moved to the SMF buffer.
SMF30DTE	SMFDATE	4	Date that the record was moved to the SMF buffer, in the form 0cyydddF (in local time).
SMF30SID	DSTRING	4	System identification (from the SID parameter).
SMF30STP	UINT	2	Record subtype. This is a two-byte field.
SMF30TYP	UINT	2	Subtype identification. Two-byte field. (Used to determine record subtype.)
SMF30JBN	EBCDIC	8	Job or session name. The job name, time and date that the reader recognized the JOB card (for this job) constitute the job log identification.
SMF30PGM	EBCDIC	8	Program name (taken from PGM= parameter on EXEC card). If a backward reference was used, this field contains PGM=*.DD.
SMF30STM	EBCDIC	8	Step name (taken from name on EXEC card).
SMF30UIF	EBCDIC	8	User-defined identification field (taken from common exit parameter area, not from USER=parameter on job statement).
SMF30JNM	EBCDIC	8	JES job identifier. Jobs scheduled by the APPC/MVS transaction scheduler (ASCH) start with an "A" followed by a seven-digit number.
SMF30STN	UINT	2	Step number (first step = 1, etc.). Two-byte field.
SMF30CLS	UINT	1	Job class (blank for TSO/E session or started tasks). One-byte field.
SMF30RST	SMFTIME	4	Time since midnight, in hundredths of a second, that the reader recognized the JOB card (for this job).
SMF30RSD	SMFDATE	4	Date that the reader recognized the JOB card (for this job), in the form 0cyydddF.
SMF30USR	DSTRING	20	Programmer's name.
SMF30GRP	EBCDIC	8	RACF group ID. 0 = RACF is not active.
SMF30RUD	EBCDIC	8	RACF user ID. 0 = RACF is not active.
SMF30TID	EBCDIC	8	RACF terminal ID. This field is zero if RACF is not active (or the user is not a terminal user).
SMF30TSN	EBCDIC	8	Terminal symbolic name.

VSA Filtering – SMF 80 RACF Security Events

Name	FORMAT	Len	Description
SMF80TME	SMFTIME	4	Time since midnight, in hundredths of a second, that the record was moved into the SMF buffer.
SMF80DTE	SMFDATE	4	Date when the record was moved into the SMF buffer, in the form 0cyydddF.
SMF80SID	DSTRING	4	System identification (from the SID parameter).
T80DES_VIOLATION	BOOLEAN	-	The event is a violation. (Bit 0 of field SMF80DES+0.)
T80DES_USER_NDEF	BOOLEAN	-	User Not Defined to RACF. (Bit 1 of field SMF80DES+0 .)
T80DES_WARNING	BOOLEAN	-	The event is a warning. (Bit 3 of field SMF80DES+0.)
SMF80EVT	UINT	1	Event code. For information about RACF event codes, see the IBM manual *z/OS Security Server RACF Macros and Interfaces*.
SMF80EVQ	UINT	1	Event code qualifier. For information about RACF event codes, see the IBM manual *z/OS Security Server RACF Macros and Interfaces*.
SMF80USR	EBCDIC	8	Identifier of the user associated with this event (jobname is used if the user is not defined to RACF).
SMF80GRP	EBCDIC	8	Group to which the user was connected (stepname is used if the user is not defined to RACF).
Authorities used for processing commands or accessing resources			
SMF80ATH	BIT8MASK	1	Authorities used for processing commands or accessing resources. These flags indicate the authority checks made for the user who requested the action. The RACF commands use bits 0, 1, and 3; the RACF requests use bits 0, 2, and 4-7.
T80ATH_NORMAL	BOOLEAN	-	Normal authority check. (Bit 0 of field SMF80ATH.)
T80ATH_SPECIAL	BOOLEAN	-	SPECIAL attribute (command processing). (Bit 1 of field SMF80ATH.)
T80ATH_OPER	BOOLEAN	-	OPERATIONS attribute (resource access, command processing). (Bit 2 of field SMF80ATH.)
T80ATH_AUDIT	BOOLEAN	-	AUDITOR attribute (command processing). (Bit 3 of field SMF80ATH.)

VSA Filtering – SMF 80 RACF Security Events

T80ATH_BYPASS	BOOLEAN	-	Bypassed-userid = *BYPASS* (resource access). (Bit 6 of field SMF80ATH.)
T80ATH_TRUSTED	BOOLEAN	-	Trusted attribute (resource access). (Bit 7 of field SMF80ATH.)
Reason for logging			
SMF80REA	BIT8MASK	-	Reason for logging. These flags indicate the reason RACF produced the SMF record
T80REA_SETROPTS	BOOLEAN	-	SETROPTS AUDIT(class). (Bit 0 of field SMF80REA.)
T80REA_USERAUDIT	BOOLEAN	-	User being audited. (Bit 1 of field SMF80REA.)
T80REA_SPEC_OPER	BOOLEAN	-	SPECIAL or OPERATIONS user being audited. (Bit 2 of field SMF80REA.)
T80REA_AUDIT	BOOLEAN	-	Access to the resource is being audited due to the AUDIT option. (Bit 3 of field SMF80REA.)
T80REA_VERIFY	BOOLEAN	-	RACINIT failure. (Bit 4 of field SMF80REA.)
T80REA_ALWAYS	BOOLEAN	-	This command is always audited. (Bit 5 of field SMF80REA.)
T80REA_CMDVIOL	BOOLEAN	-	Violation detected in command and CMDVIOL is in effect. (Bit 6 of field SMF80REA.)
T80REA_GLOBALAUDIT	BOOLEAN	-	Access to entity being audited due to GLOBALAUDIT option. (Bit 7 of field SMF80REA.)
SMF80ERR	BIT8MASK	1	Command processing error flag. These flags indicate errors during command processing and the extent of the processing.
SMF80TRM	EBCDIC	8	Terminal ID of foreground user (zero if not available).
SMF80JBN	EBCDIC	8	Job name. For RACINIT records for batch jobs, this field can be zero. The job name, time, and date that the reader recognized the JOB card (for this job) constitute the job log identification, or transaction name (for APPC output).
SMF80UID	EBCDIC	8	User identification field from the SMF common exit parameter area. For RACINIT records for batch jobs, this field can be zero.

VSA Filtering – SMF 80 RACF Security Events

T80DT3_AR_CONTROL	BOOLEAN	-	Access requested = CONTROL. (Bit 1 of field T80DT3_ACCESS_REQ.)
T80DT3_AR_UPDATE	BOOLEAN	-	Access requested = UPDATE. (Bit 2 of field T80DT3_ACCESS_REQ.)
T80DT3_AR_READ	BOOLEAN	-	Access requested = READ. (Bit 3 of field T80DT3_ACCESS_REQ.)
T80DT3_AR_NONE	BOOLEAN	-	Access requested = NONE. (Bit 4 of field T80DT3_ACCESS_REQ.)
T80DT3_AR_WRITE	BOOLEAN	-	Access requested = WRITE. (Bit 6 of field T80DT3_ACCESS_REQ.)
T80DT3_AR_READWRITE	BOOLEAN	-	Access requested = READWRITE. (Bits 3 & 6 of field T80DT3_ACCESS_REQ.)
Data Type 4			
T80DT4_ACCESS_ALLOWED	BIT8MASK	1	Access allowed
T80DT4_AA_ALTER	BOOLEAN	-	Access allowed = ALTER. (Bit 0 of field T80DT4_ACCESS_ALLOWED.)
T80DT4_AA_CONTROL	BOOLEAN	-	Access allowed = CONTROL. (Bit 1 of field T80DT4_ACCESS_ALLOWED.)
T80DT4_AA_UPDATE	BOOLEAN	-	Access allowed = UPDATE. (Bit 2 of field T80DT4_ACCESS_ALLOWED.)
T80DT4_AA_READ	BOOLEAN	-	Access allowed = READ. (Bit 3 of field T80DT4_ACCESS_ALLOWED.)
T80DT4_AA_NONE	BOOLEAN	-	Access allowed = NONE. (Bit 4 of field T80DT4_ACCESS_ALLOWED.)
T80DT4_AA_EXECUTE	BOOLEAN	-	Access allowed = EXECUTE. (Bit 5 of field T80DT4_ACCESS_ALLOWED.)
Data Type 5			
T80DT5_DSN_LEVEL	UINT	1	Data set level number (00-99). 1-byte field.

VSA Filtering – SMF 80 RACF Security Events

T80ADDSD_NOTIFY	EBCDIC	8	User to be notified when this profile denies access
T80ADDSD_KW2_SPEC+0	BIT8MASK	1	More flags for keywords specified. Bit settings: 0 SETONLY 1 TAPE 2 FILESEQ 3 RETPD 4 ERASE 5 FROM 6 FCLASS 7 FVOLUME
T80ADDSD_KW2_SPEC+1	BIT8MASK	1	More flags for keywords specified, byte 2. Bit settings: 0 FGEABEL 2–7 Reserved for IBM's use
T80ADDSD_KW2_ISA+0	BIT8MASK	1	More flags for keywords ignored. Same format as T80ADDSD_KW2_SPEC+0
T80ADDSD_KW2_ISA+1	BIT8MASK	1	More flags for keywords ignored, byte 2. Same format as T80ADDSD_KW2_SPEC+1
T80ADDSD_FSEQ#	UINT	2	File sequence number. 2-byte field.
T80ADDSD_RETPD	UINT	2	Retention period. 2-byte field.
T80ADDSD_FCLASS	EBCDIC	8	FROM class name
T80ADDSD_FRESNAM	EBCDIC	44	FROM resource name
T80ADDSD_FVOLUME	EBCDIC	8	FROM volume serial
T80ADDSD_SECLEVEL	EBCDIC	44	SECLEVEL name
T80ADDSD_SECLABEL	EBCDIC	8	SECLABEL

VSA Filtering – SMF 102 DB2

Name	FORMAT	Len	Description
SM102TME	SMFTIME	4	Time since midnight, in hundredths of a second, when the record was moved into the SMF buffer
SM102DTE	SMFDATE	4	Date when the record was moved into the SMF buffer, in the form 0cyydddF
SM102SID	DSTRING	4	System identification (from the SID parameter)
QWHSRMID	UNIT	1	Resource Manager ID
QWHSIID	UNIT	2	IFCID (Instrumentation Facility Component Identifier)
QWHCAID	EBCDIC	8	Correlation authorization ID
QW0105DN	EBCDIC	8	IFCID 105 database name
QW0105TN	EBCDIC	8	IFCID 105 table space name
QW0141OR	EBCDIC	8	IFCID 141 grantor or revoker
QW0141AC	EBCDIC	1	IFCID 141 access type ('G' or 'R')
QW0141RE	EBCDIC	1	IFCID 141 reason access granted (only for grant)

VSA Filtering – SMF 119 TCP/IP, Telnet, FTP, FTP Client, UDP Close, TN3270

Name	FORMAT	Len	Description
SMF119HDTime	SMFTIME	4	Time since midnight, in hundredths of a second, that the record was moved into the SMF buffer
SMF119HDDate	SMFDATE	4	Date when the record was moved into the SMF buffer, in the form 0cyydddF
SMF119HDSID	DSTRING	4	System identification (from the SMFPRMxx SID parameter)
SMF119HDSubType	UINT	2	Record sub-type. Two (2) byte field
Common TCP/IP identification section			
SMF119TI_SYSName	EBCDIC	8	System name from SYSNAME in IEASYSxx
SMF119TI_SysplexName	EBCDIC	8	Sysplex name from SYSPLEX in COUPLExx
SMF119TI_Stack	EBCDIC	8	TCP/IP stack name
SMF119TI_Comp	EBCDIC	8	TCP/IP subcomponent (right padded with blanks): FTPC FTP Client FTPS FTP server IP IP layer STACK Entire TCP/IP stack TCP TCP layer TN3270C TN3270 Client TN3270S TN3270 server UDP UDP layer
SMF119TI_ASName	EBCDIC	8	Started task qualifier or address space name of address space that writes this SMF record
SMF119TI_UserID	EBCDIC	8	User ID of security context under which this SMF record is written
SMF119TI_Reason	UINT	1	Reason for writing this SMF record: X'08' Event record X'C0' Interval statistics record, more records follow

VitalSigns SIEM Agent for z/OS

Product Demonstration

- VSA Granular Filtering
- SMF Events sent to Splunk in Real Time

VitalSigns SIEM Agent for z/OS

VSA Filtering Demo

- SMF 17 – Delete of a DSN and Send / Reject only specific DSN info to Splunk
- SMF 42 DSN Edit- Select PDS information to be sent to SPLUNK
- SMF 80 – Send specific events to Splunk based on TSO User ID
- SMF 92 Reject activity for job SDS1STC to be sent to SPLUNK
- SMF 119 – Select events with specific IP address to be sent to SPLUNK

Gain Real-Time Visibility into Z

Summary

- Real-time SMF monitoring is key
- Compliance requirement
- Separation of Duties – Decide as a team what's important
- Implement filtering to cut down on "unnecessary" events forwarded to the SIEM

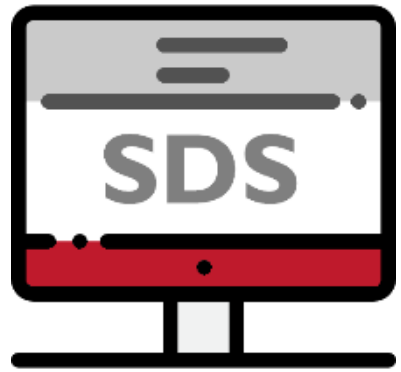
SDS

Questions?

Would you like additional information?

info@sdsusa.com

(800) 443-6183
(763) 571-9000



www.sdsusa.com