Common Event Format Configuration Guide

CorreLog, Inc.

CorreLog Agent for z/OS (CZAGENT) 5.4.0

Date: Monday, January 13, 2014

CEF Connector Configuration Guide

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to HP. HP does not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

Certified CEF:

The event format complies with the requirements of the HP ArcSight Common Event Format. The HP ArcSight CEF connector will be able to process the events correctly and the events will be available for use within HP's ArcSight product. In addition, the event content has been deemed to be in accordance with standard SmartConnector requirements. The events will be sufficiently categorized to be used in correlation rules, reports and dashboards as a proof-of-concept (POC) of the joint solution

CorreLog Agent for z/OS (CZAGENT) 5.4.0

December 5, 2013

Revision History

Date	Description
1/7/2014	First edition of this Configuration Guide.
1/10/2014	Version 5.4.0 Certified by HP Enterprise Security

CEF Connector Support Information when an issue is outside of the ArcSight team's ability

In some cases the ArcSight customer service team is unable to help with issues that lie within the configuration itself in which case, the certified vendor should be contacted for assistance:

CorreLog Customer Support

Phone 1-800-CORRELOG (1-800-267-7356) and press 2

Email support@CorreLog.com

Instructions – Please mention that you are an ArcSight ESM integration customer.

CorreLog Agent for z/OS (CZAGENT) Configuration Guide

This guide provides information for configuring CZAGENT for syslog event collection. This Connector is supported on z/OS (“mainframe,” formerly known as MVS and/or OS/390) platforms. Device versions starting at V5-4-0 and above are supported. z/OS releases V1R11 and above are supported.

Overview

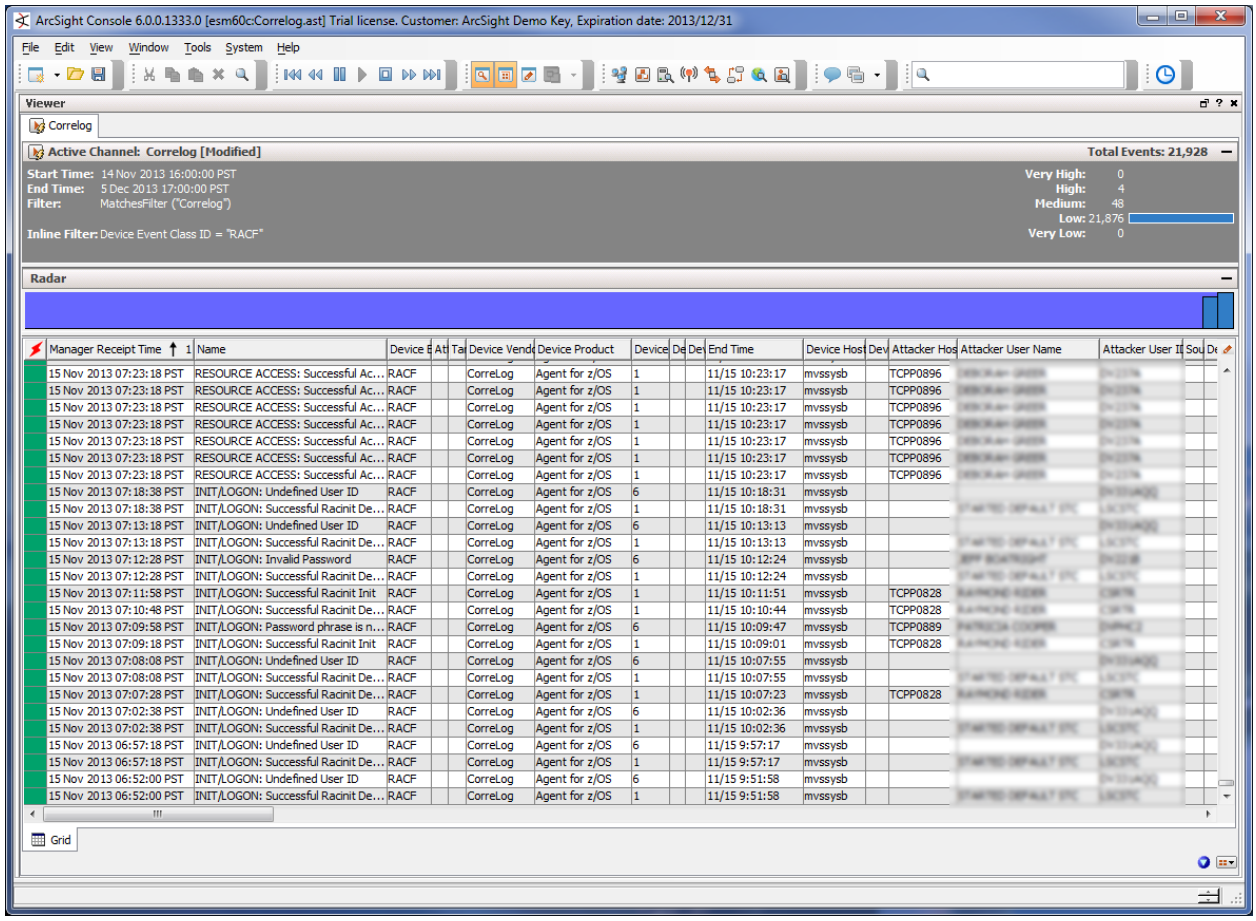
The CorreLog Agent for z/OS integrates your z/OS mainframe into your enterprise ArcSight ESM strategy. It forwards security, TCP/IP, job, TSO session, and DB2 events to ESM in real time. The agent helps to assure mainframe compliance with PCI DSS, HIPAA, Sarbanes-Oxley and similar regulatory requirements.

Configuration

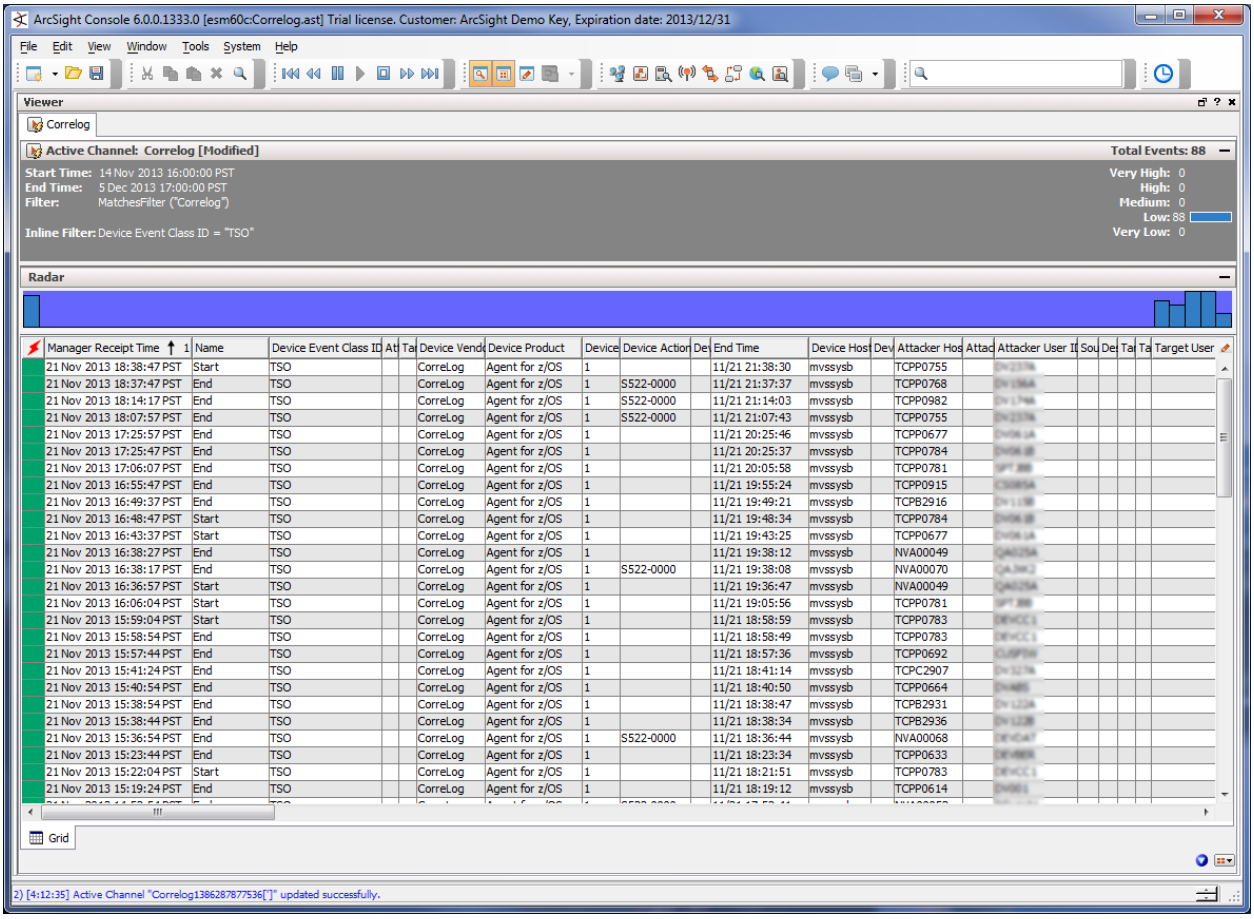
CZAGENT is configured for CEF simply by configuring it to use the supplied parameter file CZAPCEF, as described in the CZAGENT reference manual section **ArcSight CEF**. Alternatively, you may specify SIEM(CEF) in any CZAGENT parameter file.

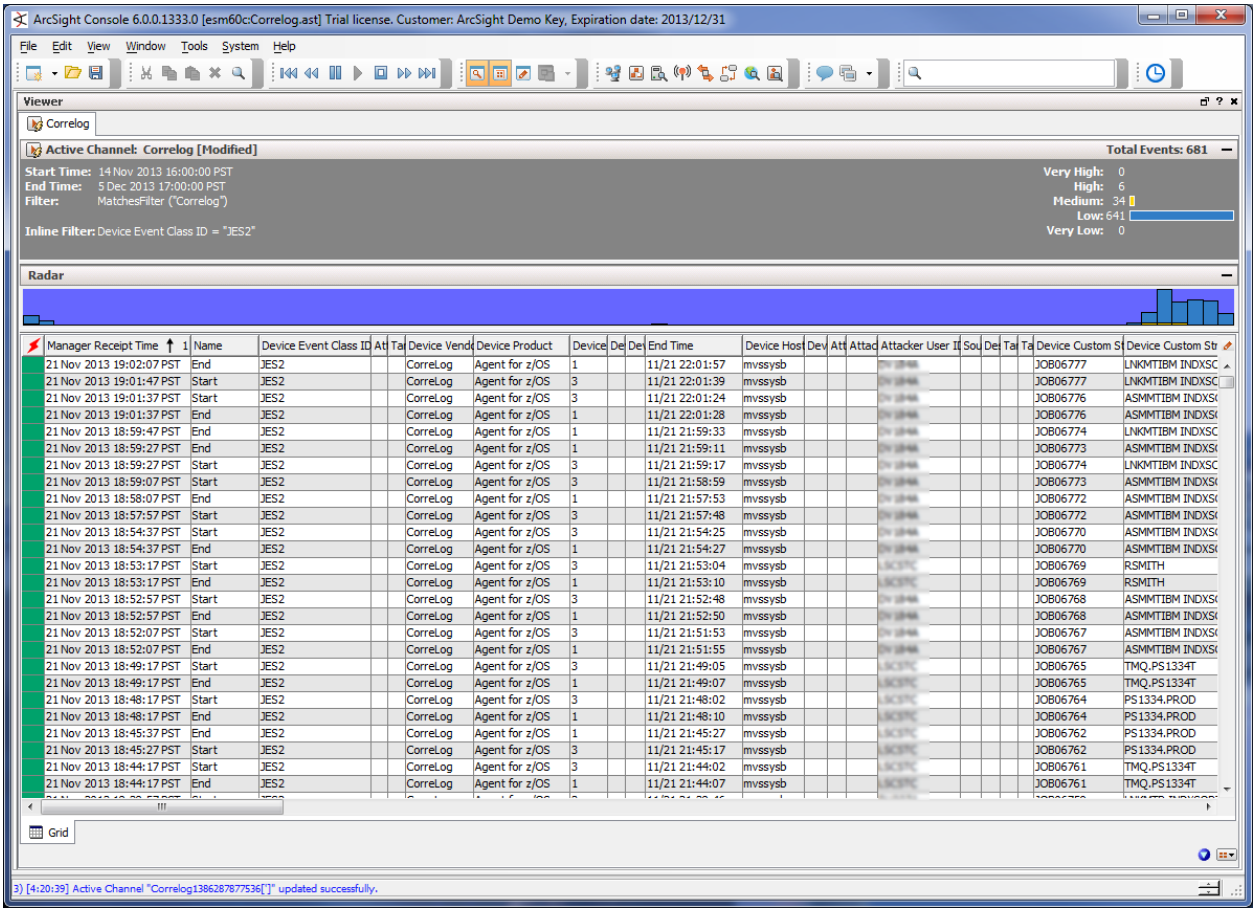
Screen Shot

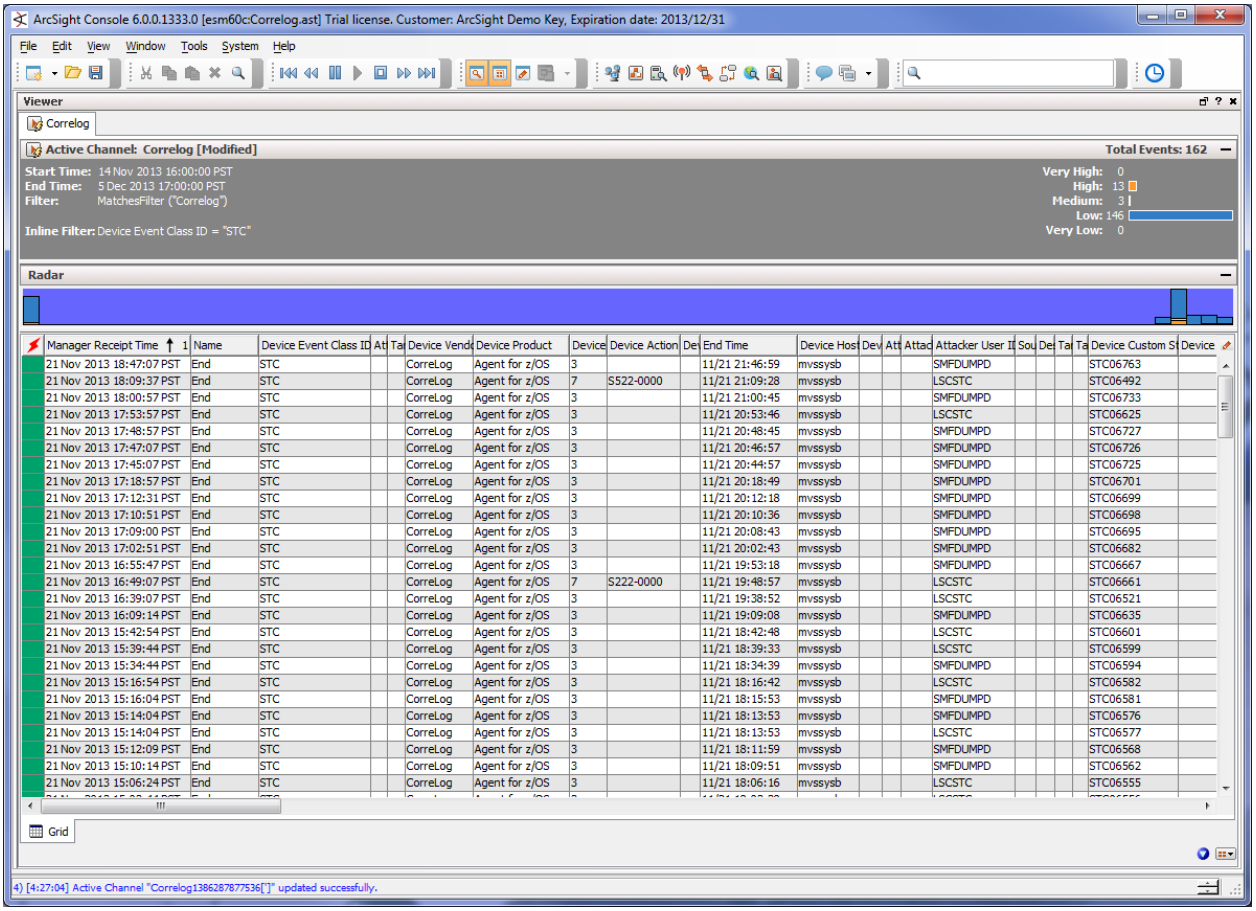
Sample RACF (security) events



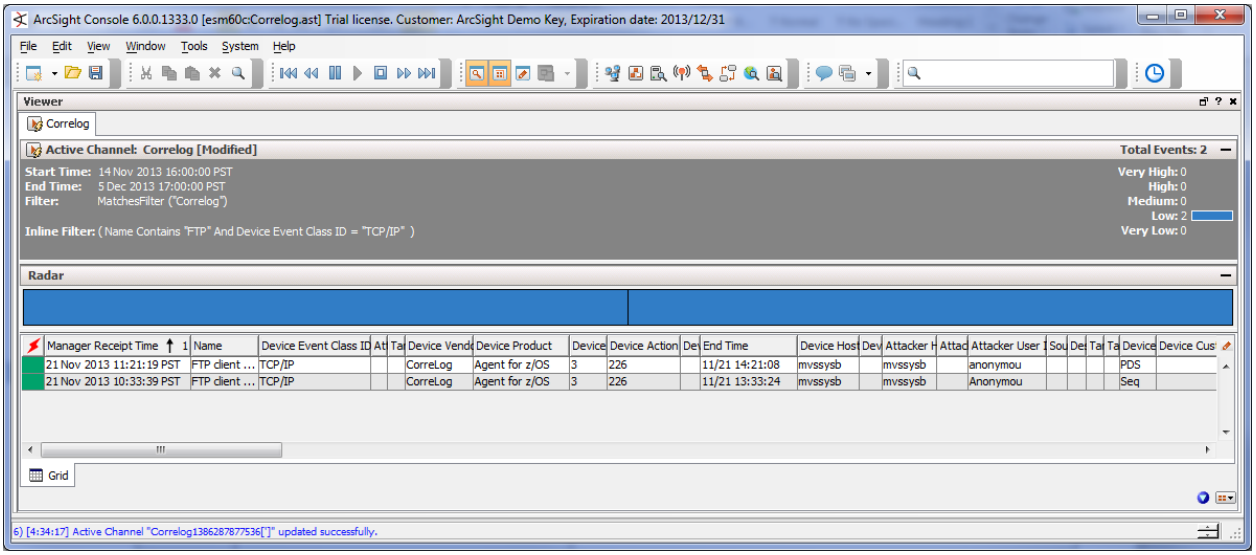
Sample TSO Session, Job and Started Task Events



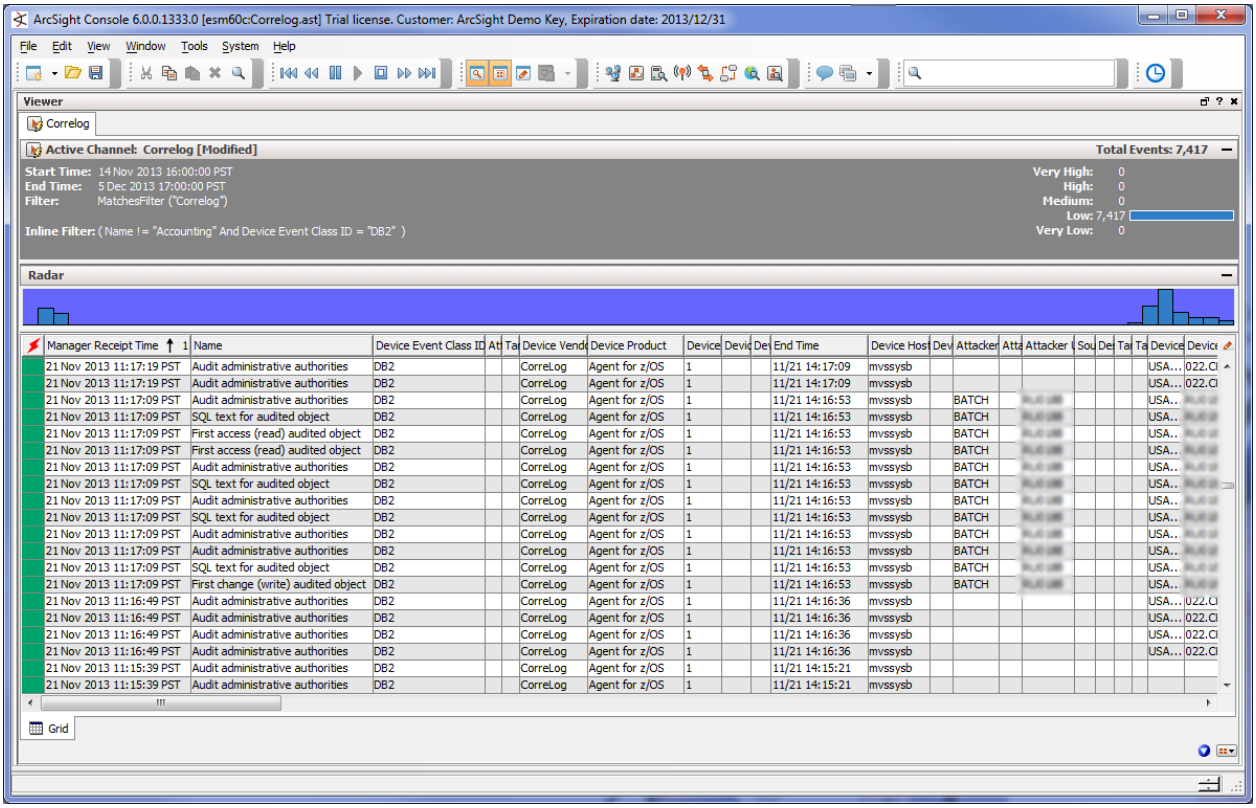

ArcSight Console 6.0.0.1333.0 [esm60c:Correlog.ast] Trial license. Customer: ArcSight Demo Key, Expiration date: 2013/12/31
File Edit View Window Tools System Help
Viewer
Correlog
Active Channel: Correlog [Modified]
Total Events: 681
Start Time: 14 Nov 2013 16:00:00 PST
End Time: 5 Dec 2013 17:00:00 PST
Filter: MatchesFilter ("Correlog")
Inline Filter: Device Event Class ID = "JES2"
Very High: 0
High: 6
Medium: 34
Low: 641
Very Low: 0
Radar
Manager Receipt Time
Name
Device Event Class ID
Device Vend
Device Product
End Time
Device Host
Device Custom St
Device Custom Str
21 Nov 2013 19:02:07 PST End JES2 CorreLog Agent for z/OS 1 11/21 22:01:57 mvssysb JOB06777 LNKMTIBM INDXSC
21 Nov 2013 19:01:47 PST Start JES2 CorreLog Agent for z/OS 3 11/21 22:01:39 mvssysb JOB06777 LNKMTIBM INDXSC
21 Nov 2013 19:01:37 PST Start JES2 CorreLog Agent for z/OS 3 11/21 22:01:24 mvssysb JOB06776 ASMMTIBM INDXS
21 Nov 2013 19:01:37 PST End JES2 CorreLog Agent for z/OS 1 11/21 22:01:28 mvssysb JOB06776 ASMMTIBM INDXS
21 Nov 2013 18:59:47 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:59:33 mvssysb JOB06774 LNKMTIBM INDXSC
21 Nov 2013 18:59:27 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:59:11 mvssysb JOB06773 ASMMTIBM INDXS
21 Nov 2013 18:59:27 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:59:17 mvssysb JOB06774 LNKMTIBM INDXSC
21 Nov 2013 18:59:07 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:58:59 mvssysb JOB06773 ASMMTIBM INDXS
21 Nov 2013 18:58:07 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:57:53 mvssysb JOB06772 ASMMTIBM INDXS
21 Nov 2013 18:57:57 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:57:48 mvssysb JOB06772 ASMMTIBM INDXS
21 Nov 2013 18:54:37 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:54:25 mvssysb JOB06770 ASMMTIBM INDXS
21 Nov 2013 18:54:37 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:54:27 mvssysb JOB06770 ASMMTIBM INDXS
21 Nov 2013 18:53:17 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:53:04 mvssysb JOB06769 RSMITH
21 Nov 2013 18:53:17 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:53:10 mvssysb JOB06769 RSMITH
21 Nov 2013 18:52:57 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:52:48 mvssysb JOB06768 ASMMTIBM INDXS
21 Nov 2013 18:52:57 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:52:50 mvssysb JOB06768 ASMMTIBM INDXS
21 Nov 2013 18:52:07 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:51:53 mvssysb JOB06767 ASMMTIBM INDXS
21 Nov 2013 18:52:07 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:51:55 mvssysb JOB06767 ASMMTIBM INDXS
21 Nov 2013 18:49:17 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:49:05 mvssysb JOB06765 TMQ.PS1334T
21 Nov 2013 18:49:17 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:49:07 mvssysb JOB06765 TMQ.PS1334T
21 Nov 2013 18:48:17 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:48:02 mvssysb JOB06764 PS1334.PROD
21 Nov 2013 18:48:17 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:48:10 mvssysb JOB06764 PS1334.PROD
21 Nov 2013 18:45:37 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:45:27 mvssysb JOB06762 PS1334.PROD
21 Nov 2013 18:45:27 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:45:17 mvssysb JOB06762 PS1334.PROD
21 Nov 2013 18:44:17 PST Start JES2 CorreLog Agent for z/OS 3 11/21 21:44:02 mvssysb JOB06761 TMQ.PS1334T
21 Nov 2013 18:44:17 PST End JES2 CorreLog Agent for z/OS 1 11/21 21:44:07 mvssysb JOB06761 TMQ.PS1334T
Grid
3) [4:20:39] Active Channel "Correlog1386287877536[']" updated successfully.



Sample TCP/IP FTP Events



Sample DB2 Events



Events

Message Type	Category	Description
CZAGENT Internal Messages	Internal	Numbered messages generated by the agent itself such as Jan 04 19:25:52 mvssysb CEF:0|CorreLog|Agent for z/OS|5-4-0|CZA0134I|CZAGENT CZA0134I|3|cat=Internal msg=Termination in progress.
CZASEND-generated user messages	CZASEND	Free-format user messages transmitted by the utility program CZASEND. For example Dec 28 12:51:08 mvssysb CEF:0|CorreLog|Agent for z/OS|5-4-0| User Message| CZASEND User Message|1|cat=CZASEND msg=JOB05628 - DEV239ZS - BILLING - UPDATE - Customer update completed. 38,569 records inserted.
SMF Type 15	DS_Output	File integrity monitoring of all QSAM and BSAM datasets opened for output or update and then closed.
SMF Type 18	Rename	Dataset renames.
SMF Type 30	JES2 or JES3	Job start, end, step end and ABEND events
SMF Type 30	STC	Started task start, end and ABEND events
SMF Type 30	TSO	TSO session start, end and ABEND events
SMF Type 42	DFSMS	File integrity monitoring of all partitioned dataset members updated, renamed or deleted.
SMF Type 64	VSAM_Status	File integrity monitoring of all VSAM datasets opened and then closed.
SMF Type 80	RACF	Security-related events from RACF or Top Secret.

Message Type	Category	Description
SMF Type 100, 101 or 102	DB2	Database activity monitoring events from DB2.
SMF Type 110	CICS	Audited CICS transactions.
SMF Type 230	ACF2	Security-related events from ACF2.
Any SMF	Diag	Used to log common fields from any SMF record type for diagnostic purposes.

Device Event Class IDs

Please refer to CorreLog documentation for a complete list of the RACF and DB2 event IDs. The other events IDs are listed below.

Signature ID Major Name	Event Name	Description
ACF2	ACF2 S/F/P command	Self-descriptive.
ACF2	CA statistics records	Self-descriptive.
ACF2	Dataset violation	Self-descriptive.
ACF2	Distributed DataBase Function	Self-descriptive.
ACF2	Intercept journal	Self-descriptive.
ACF2	Invalid GSO infostg record	Self-descriptive.
ACF2	Invalid password/authority	Self-descriptive.
ACF2	Logonid modification"	Self-descriptive.
ACF2	MAC records	Self-descriptive.
ACF2	OpenEdition MVS events	Self-descriptive.
ACF2	RACROUTE REQUEST=DIRAUTH	Self-descriptive.
ACF2	Resource event (infostg update)	Self-descriptive.
ACF2	Resource violation	Self-descriptive.
ACF2	Restricted logonid	Self-descriptive.
ACF2	Rule insert/update/delete	Self-descriptive.
ACF2	SAF trace records	Self-descriptive.
ACF2	TSO transaction	Self-descriptive.
CICS	Audit	Audited CICS transactions.
CZASEND	User Message	Free-format user messages transmitted by the utility program CZASEND.
DB2	IFCID name	See the CZAGENT parameter file member CZADDB2I, documented in **The SMF Type DB2 IFCID Description File (CZADDB2I)** in the CorreLog Agent Users Manual; and the IBM DB2 documentation file DSNDQWHS.
DFSMS	Add/Replace	The addition or replacement of a member in a Partitioned Dataset (Extended).
DFSMS	Delete	The deletion of a member in a Partitioned Dataset (Extended).

DFSMS	Initialize	The initialization (deletion of all members of) a Partitioned Dataset (Extended).
DFSMS	Rename	The renaming of a member in a Partitioned Dataset (Extended).
Diag	Diag	Used to log common fields from any SMF record type for diagnostic purposes.
DS_Output	Close	File integrity monitoring of all QSAM and BSAM datasets opened for output or update and then closed.
Internal	CZA*nnnnx*	Various diagnostic and status messages generated by the agent itself. For a description, see **Appendix I: Syslog Messages Internal to CZAGENT** and **Appendix B: Messages and Return Codes** in the CorreLog Agent Users Manual.
JES2, JES3, STC or TSO	Start, Step End, or End	Job, started task, and TSO session start, step end, and end events.
RACF	RACF event and qualifier description	See the CZAGENT parameter file member CZAD80EQ, documented in **The SMF Type 80 Record Description File (CZAD80EQ)** in the CorreLog Agent Users Manual; and **Table of event codes and event code qualifiers** in the IBM manual "z/OS Security Server RACF Macros and Interfaces."
Rename	Status	Renames of non-VSAM datasets.
TCP/IP	Connect init	TCP connection initiation record (subtype 1)
TCP/IP	Connect terminate	TCP connection termination record (subtype 2)
TCP/IP	Dynamic tunnel active	IPSec dynamic tunnel activation and refresh record (subtype 75)
TCP/IP	Dynamic tunnel added	IPSec dynamic tunnel added record (subtype 77)
TCP/IP	Dynamic tunnel deactive	IPSec dynamic tunnel deactivation record (subtype 76)
TCP/IP	Dynamic tunnel removed	IPSec dynamic tunnel removed record (subtype 78)
TCP/IP	FTP client complete	FTP client transfer completion record (subtype 3)
TCP/IP	FTP server complete	FTP server transfer completion record (subtype 70)
TCP/IP	FTP server logon fail	FTP server logon failure record (subtype 72)
TCP/IP	IKE tunnel active	IPSec IKE tunnel activation and refresh record (subtype 73)
TCP/IP	IKE tunnel deactive	IPSec IKE tunnel deactivation and expire record (subtype 74)
TCP/IP	Interface stats	Interface statistics record (subtype 6)
TCP/IP	Manual tunnel active	IPSec manual tunnel activation record (subtype 79)
TCP/IP	Manual tunnel deactive	IPSec manual tunnel deactivation record (subtype 80)
TCP/IP	Server port stats	Server port statistics record (subtype 7)
TCP/IP	Stack start/stop	TCP/IP stack start/stop record (subtype 8)
TCP/IP	TCP/IP stats	TCP/IP statistics record (subtype 5)
TCP/IP	Telnet SNA init	TN3270E Telnet server SNA session initiation record (subtype 20)
TCP/IP	Telnet SNA terminate	TN3270E Telnet server SNA session termination record (subtype 21)
TCP/IP	TSO Telnet init	TSO Telnet client connection initiation record (subtype 22)
TCP/IP	TSO Telnet terminate	TSO Telnet client connection termination record (subtype 23)
TCP/IP	UDP close	UDP socket close record (subtype 10)
VSAM	Status	File integrity monitoring of all VSAM datasets opened and then closed.

Device Event Mapping to ArcSight Data Fields

The following is a list of all CEF fields supported by CZAGENT.

CEF Name is the field name as it appears in a CEF-format Syslog message.

CEF Label is the value of the label field that describes a custom CEF name (if applicable).

CZAGENT Field Name is the name that you would code as one of the operands of a CZAGENT parm file FIELDS parameter. Generally speaking, the field name is the same as, or closely derived from, the IBM SMF record field name. Field names suffixed with a D are textual descriptions. For example, SYSLOG_FACILITY_D is the RFC3164 facility number converted to text. The FIELDS parameter is not case-sensitive; field names may be specified in upper, lower, or mixed case.

Universal Fields

These fields may be specified in the FIELDS parameter of any SMF statement.

CEF Name	CEF Label	CZAGENT Field Name	Description
deviceFacility		SYSLOG_FACILITY	The RFC3164 “facility” expressed as a number from 0 to 23.
deviceFacility		SYSLOG_FACILITY_D	The RFC3164 “facility” expressed as a character string.
dvc		HOST_IPV4	The primary IPv4 address.
dvcHost		HOST_CPUID	The CPU ID (CPU serial number).
dvcHost		HOST_HOSTNAME	The TCP/IP hostname.
dvcHost		HOST_IPV6	The primary IPv6 address.
dvcHost		HOST_JESNODE	The JES node name.
dvcHost		HOST_LPARNAME	The LPAR name. Do not code HOST_LPARNAME if you are not running in logical partition mode.
dvcHost		HOST_SMFID	The SMF ID.
dvcHost		HOST_SYSNAME	The system name (&SYSNAME as defined in the IEASYSxx or IEASYMxx parmlib member).
rt		CURRENT_TIME	The current date and time.
rt		SMFXXDTETME	The SMF record timestamp.

SMF 15 Fields

In accordance with SMF conventions SMF Type 15 fields have names beginning with SMF14.

CEF Name	CEF Label	CZAGENT Field Name	Description[1]
cat		SMF14CAT	Constant “DS_Output”
cs2	DDN	SMF14TIOEDDNM	Data definition name (DDname).
filePath		SMF14JFCBDSNM	Dataset name.
fname		SMF14JFCBELNM	Member name or relative generation number.
sproc		SMF14JBN	Job name.
start		SMF14RST	Time that the reader recognized the JOB card (for this job).

SMF 18 Fields

CEF Name	CEF Label	CZAGENT Field Name	Description[1]
cat		SMF18CAT	Constant “Rename”
cn1	Vol#	SMF18NVL	Number of volumes.
cs2	Indic1	SMF18IN1D	Record indicator byte 1, expressed as text.
fileID		SMF18FVL	First volume serial number.
filePath		SMF18NDS	New dataset name.
oldFilePath		SMF18ODS	Old dataset name.
sproc		SMF18JBN	Job name.
start		SMF18RST	Time that the reader recognized the JOB card (for this job).

SMF 30 Fields

CEF Name	CEF Label	CZAGENT Field Name	Description[1]
cat		SMF30CAT	Subsystem name “JES2”, “JES3”, “TSO”, “STC” or “APPC”
cn1	*Step#*	SMF30STN	Step number (first step = 1, etc.).
cn2	SubStep	SMF30SSN	Substep number. This field is set to zero for non-z/OS UNIX System Services steps. When the z/OS UNIX System Services exec function is requested, a new substep is begun and this value is incremented.

[1] Most of these descriptions are taken directly from “z/OS MVS System Management Facilities (SMF)” © Copyright International Business Machines Corporation 1988, 2008

CEF Name	CEF Label	CZAGENT Field Name	Description[1]
cs2	Class	SMF30CL8	8-character job class (left justified, padded with blanks). For JES2, taken from the SMF30CLS field (if not specified), blank for TSO session or started tasks. For JES3, taken from CLASS: parameter on //* MAIN card (if valid), or the default (JES3BATCH).
cs3	JobID	SMF30JNM	JES job identifier. Jobs scheduled by the APPC/MVS transaction scheduler (ASCH) start with an “A” followed by a seven-digit number.
cs4	ProcStep	SMF30PSN	The name of the step that invoked the procedure. This field contains blanks if not part of a procedure.
cs5	TermID	SMF30TID	RACF terminal ID. This field is blank if RACF is not active (or the user is not a terminal user).
cs6	Pgmr	SMF30USR	So-called programmer’s name field. More accurately, a 20-byte description field on the JOB statement.
destinationServiceName		SMF30WID	Work type indicator for the address space. The value identifies the type of address space that is being reported on (for example: “STC” for started tasks and system address spaces, “TSO” for TSO/E users, etc)
deviceExternalId		SMF30SYN	System name (from the SYSNAME parameter in the IEASYSxx parmlib member).
deviceProcessName		SMF30PGM	Program name (taken from PGM= parameter on EXEC card). If a backward reference was used, this field contains PGM=*.DD.
outcome		SMF30SCC	Job or Step completion code and ABEND reason code. System ABENDs are reported as Sxxx-xxxx. User ABENDs are reported as Unnnn-xxxx.
shost		SMF30TSN	Terminal symbolic name.
spriv		SMF30GRP	RACF group ID. Blank = RACF is not active.
sproc		SMF30JBN	Job or session name
suid		SMF30RUD	RACF user ID. Blank = RACF is not active.

SMF 42 Fields

CEF Name	CEF Label	CZAGENT Field Name	Description[1]
cat		SMF42CAT	Constant “DFSMS”
cs2	Alias	SMF42XAA	List of alias names deleted in sympathy of a delete or replace
cs3	Step	SMF42XST	Step name.
cs4	Proc	SMF42XPR	Proc name (or blanks).
cs5	Flag	SMF42XF1	Flag expressed as a textual description: “Add” or “Replace”
end		SMF42PTE	Interval End or CLOSE time of day. This is zero if not available. Formatted in accordance with the TIME statement parameters.
fileID		SMF42XVS	VOLSER
filePath		SMF42XDS	Data set name
fname		SMF42XMN	Member name. For a rename, this is the name after the rename (new name).
oldFileName		SMF42QOL	Member name before the rename (old name).
outcome		SMF42STY	Record subtype, expressed as an integer: 20 STOW Initialize 21 Member Delete 24 Member Add/Replace 25 Member Rename
outcome		SMF42STYD	Record subtype, expressed as a textual description: “Initialize”, "Delete", "Add/Replace", or "Rename"
shost		SMF42XUI_TOKPOE	User information of the caller of STOW or DESERV macro: Port of entry(CONS ID,TERM ID-first half of IP value for SERVAUTH)
spriv		SMF42XUI_TOKGRUP	User information of the caller of STOW or DESERV macro: GROUPNAME
sproc		SMF42XJB	Job name, started task control, or time sharing user who issued the STOW or DESERV
start		SMF42PTS	Interval Start or OPEN time of day. This is zero if not available. Formatted in accordance with the TIME statement parameters.
suid		SMF42XUI_TOKUSER	User information of the caller of STOW or DESERV macro: USERID

SMF 64 Fields

CEF Name	CEF Label	CZAGENT Field Name	Description[1]
cat		SMF64CAT	Constant “VSAM”
filePath		SMF64DNM	Name of the component or cluster being processed. For a CRA record, this field does not contain meaningful information. For a catalog record, this field contains the catalog or cluster name.
fileType		SMF64DTY	Indicator of component being processed, expressed in hex.
fileType		SMF64DTYD	Indicator of component(s) being processed, expressed as one or more textual descriptions such as Dataset or Index.
reason		SMF64RIN	Situation indicator, expressed in hex.
reason		SMF64RIND	Situation indicator, expressed as one or more textual descriptions such as Closed or Volume Switch.
sproc		SMF64JBN	Job name.
start		SMF64RST	Time that the reader recognized the JOB card (for this job).

SMF 80 Fields

CEF Name	CEF Label	CZAGENT Field Name	Description[2]
cat		SMF80CAT	Constant “RACF”
cs1	Req	SMF80R3Req	Access requested.
cs2	Owner	SMF80R38Owner	User ID or group name that owns the profile (RACROUTE REQUEST=AUTH and RACROUTE REQUEST=DEFINE and all the RACF commands that produce log records, except SETROPTS and RVARY). During DEFINE operations, this field contains the owner that the profile is defined with; in all other operations, it contains the current owner. Thus, for owner changes, it contains the old owner.
cs2	Class	SMF80R42Class	Class name from SETROPTS RACLIST/NORACLIST
cs2	Class	SMF80R43Class	Class name from SETROPTS GENLIST/NOGENLIST

[2] Most of these descriptions are taken directly from “z/OS Security Server RACF Macros and Interfaces” © Copyright International Business Machines Corporation 1994, 2008.

CEF Name	CEF Label	CZAGENT Field Name	Description[2]
cs3	CmdUserID	SMF80R6E10User	User ID specified on ADDUSER or ALTUSER command.
cs4	GenClass	SMF80R43ClassGen	Class name from SETROPTS GENLIST/NOGENLIST.
cs5	Auth	SMF80ATHD	Authorities used for processing commands or accessing resources, expressed as text.
cs6	POE	SMF80TOKPOE	User “port of entry” taken from SMF 80 Relocatable section 53 User security token “RUTKN.”
fileID		SMF80R15Vol	VOLSER volume serial (RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE) (Note that when RACROUTE REQUEST=AUTH receives a DATASET profile as input, the volume serial logged is the first volume serial contained in the profile’s list of volume serials.)
filePath		SMF80R1Res	Resource name or old resource name (RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE)
filePermission		SMF80R4Allow	Access allowed.
fileType		SMF80R17Type	Class name (RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE, RDEFINE, RALTER, RDELETE, PERMIT, or VMXEVENT auditing). For z/OS UNIX, class controlling auditing for the request.
reason		SMF80READ	Reason for logging, expressed as text. These flags indicate the reason RACF produced the SMF record. The reason is expressed as, for example, OPERATIONS, Normal check.
reason		SMF80READX	Reason for logging, expressed as hex. These flags indicate the reason RACF produced the SMF record.
shost		SMF80TRM	Terminal ID of foreground user (blank if not available).
spriv		SMF80GRP	Group to which the user was connected (stepname is used if the user is not defined to RACF).
sproc		SMF80JBN	Job name. For RACROUTE REQUEST=VERIFY records for batch jobs, this field can be blank.
suid		SMF80USR	Identifier of the user associated with this event (jobname is used if the user is not defined to RACF).

CEF Name	CEF Label	CZAGENT Field Name	Description[2]
suser		SMF80R49UserNm	User name from ACEE

SMF 110 Fields

CEF Name	CEF Label	Name	Description[3]
cat		SMF110CAT	Constant “CICS”
cs2	Class	SMFMNCL	Class of data
cs3	JobNm	SMFSTJBN	Jobname
cs4	Net	DFHTASK_NETUOWPX	Network Unit-of-Work Netname
cs5	ReptCls	DFHCICS_RPTCLSNM	Workload Manager report class name
cs6	ServCls	DFHCICS_SRVCLSNM	Workload Manager service class name
deviceProcessName		DFHPROG_PGMNAME	First program name Originating Network Unit-of-Work ID
dproc		SMFSTSSI	Sub-System Identification
start		DFHCICS_START	Task start time
end		DFHCICS_STOP	Task stop time
suid		DFHCICS_USRID	User identification

SMF 119 Fields

SMF 119 Fields Common to All Type 119 Record Subtypes

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
cat		SMF119CAT	Constant “TCP/IP”
deviceExternalID		SMF119TI_SYSName	System name from SYSNAME in IEASYSxx
deviceProcessName		SMF119TI_Comp	TCP/IP subcomponent: FTPC FTP client; FTPS FTP server; IKE IKE daemon; IP IP layer; STACK Entire TCP/IP stack; TCP TCP layer; TN3270C TN3270 client; TN3270S TN3270 server; UDP UDP layer.

[3] Most of these descriptions are taken directly from “CICS Transaction Server for z/OS Version 4 Release 2 Data Areas” © Copyright IBM Corporation 1977, 2011.

[4] Most of these descriptions are taken directly from “z/OS Communications Server IP Configuration Reference” © Copyright International Business Machines Corporation 2000, 2008.

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
dproc		SMF119TI_ASName	Started task qualifier or address space name of address space that writes this SMF record

SMF 119 Fields of the Connection Initiation Record (Subtype 1)

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
c6a2	RemtIP	SMF119AP_TIRIP	Remote IPv6 address at time of connection open
c6a3	LocIP	SMF119AP_TILIP	Local IPv6 address at time of connection open
dpt		SMF119AP_TILPort	Local port number at time of connection open
dst		SMF119AP_TILIP_V4	Local IP address at time of connection open, formatted as an IPv4 address or 255.255.255.255
spt		SMF119AP_TIRPort	Remote port number at time of connection open
src		SMF119AP_TIRIP_V4	Remote IP address at time of connection open, formatted as an IPv4 address or 255.255.255.255

SMF 119 Fields of the Connection Termination Record (Subtype 2)

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
c6a2	RemtIP	SMF119AP_TTRIP	Remote IPv6 address at time of connection open
c6a3	LocIP	SMF119AP_TTLIP	Local IPv6 address at time of connection open
dpt		SMF119AP_TTLPort	Local port number at time of connection open
dst		SMF119AP_TTLIP_V4	Local IP address at time of connection open, formatted as an IPv4 address or 255.255.255.255
in		SMF119AP_TTInBytes	Inbound byte count
out		SMF119AP_TTOutBytes	Outbound byte count
spt		SMF119AP_TTRPort	Remote port number at time of connection open
src		SMF119AP_TTRIP_V4	Remote IP address at time of connection open, formatted as an IPv4 address or 255.255.255.255

SMF 119 Fields of the FTP Client Completion Record (Subtype 3)

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
c6a2	RemtCtlIP	SMF119FT_FCCRIP	Remote IPv6 address (control connection)
c6a3	LocCtlIP	SMF119FT_FCCLIP	Local IPv6 address (control connection)
cs1	SubCmd	SMF119FT_FCCmd	FTP subcommand (according to RFC 959)
cs3	DStype	SMF119FT_FCDSType	Data set type: SEQ, PDS, or HFS
cs4	RemtUserID	SMF119FT_FCUserID	User name or user ID used to log into the FTP server.
cs5	Security	SMF119FT_FCScty	See SMF 119 Fields of the Type 119 Security Sections above
dpt		SMF119FT_FCCLPort	Local port number (control connection)
dst		SMF119FT_FCCLIP_V4	Local IP address (control connection) , formatted as an IPv4 address or 255.255.255.255
duid		SMF119FT_FCLUser	Local User ID
end		SMF119FT_FCETime	Transmission end date and time of day
filePath		SMF119FT_FCFileName	MVS or z/OS UNIX Data Set Name associated with the Rename file transfer operation. Use the ″Data Set Type″ field information in the FTP client transfer completion section to determine the type of filename represented here.
fileType		SMF119FT_FCFType	Local file type (SEQ, JES, or SQL)
fname		SMF119FT_FCM1	PDS member name
in		SMF119FT_FCBytes	Transmission byte count; 64-bit integer
reason		SMF119FT_FCLReply	Last server reply (3-digit RFC 959 code, left justified)
shost		SMF119FT_FCHostname	Host name
spt		SMF119FT_FCCRPort	Remote port number (control connection)
src		SMF119FT_FCCRIP_V4	Remote IP address (control connection) , formatted as an IPv4 address or 255.255.255.255
start		SMF119FT_FCSTime	Transmission start date and time of day
suid		SMF119FT_FCRUser	User ID (login name) on server

SMF 119 Fields of the TN3270E SNA Session Initiation Record (Subtype 20)

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
c6a2	RemtIP	SMF119TN_NIRIP	Remote IPv6 address
c6a3	LocIP	SMF119TN_NILIP	Local IPv6 address

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
cn1	DevNo	SMF119TN_NILdev	Telnet server internal logical device number
dpt		SMF119TN_NILPort	Local port number
dst		SMF119TN_NILIP_V4	Local IP address, formatted as an IPv4 address or 255.255.255.255
shost		SMF119TN_NILU	Telnet LU name
spt		SMF119TN_NIRPort	Remote (client) port number
src		SMF119TN_NIRIP_V4	Remote IP address, formatted as an IPv4 address or 255.255.255.255
start		SMF119TN_NITime	Date and time of day of session initiation

SMF 119 Fields of the TN3270E SNA Session Termination Record (Subtype 21)

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
c6a2	RemtIP	SMF119TN_NTRIP	Remote IPv6 address
c6a3	LocIP	SMF119TN_NTLIP	Local IPv6 address
cn1	DevNo	SMF119TN_NTLdev	Telnet server internal logical device number
cs2	Devt	SMF119TN_NTDevt	Telnet device type
dpt		SMF119TN_NTLPort	Local port number
dst		SMF119TN_NTLIP_V4	Local IP address, formatted as an IPv4 address or 255.255.255.255
end		SMF119TN_NTtTime	Date and time of day of session termination
in		SMF119TN_NTInByte	Inbound byte count[Error! Bookmark not defined.]
out		SMF119TN_NTOutByte	Outbound byte count[Error! Bookmark not defined.]
reason		SMF119TN_NTRCode	Session termination reason code. The values in this field are the same as those displayed in message EZZ6034I as value for the object variable.
shost		SMF119TN_NTLU	Telnet LU name
spt		SMF119TN_NTRPort	Remote (client) port number
src		SMF119TN_NTRIP_V4	Remote IP address, formatted as an IPv4 address or 255.255.255.255
start		SMF119TN_NTiTime	Date and time of day of session initiation

SMF 119 Fields of the FTP Server Completion Record (Subtype 70)

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
c6a2	RemtCtlIP	SMF119FT_FSCRIP	Remote IPv6 address (control connection)

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
c6a3	LocCtlIP	SMF119FT_FSCLIP	Local IPv6 address (control connection)
cs1	SubCmd	SMF119FT_FSCmd	FTP command (according to RFC 959+)
cs3	DStype	SMF119FT_FSDSType	Data set type: SEQ, PDS, or HFS
cs5	Security	SMF119FT_FSScty	See SMF 119 Fields of the Type 119 Security Sections above.
dpt		SMF119FT_FSCLPort	Local port number (control connection - server)
dst		SMF119FT_FSCLIP_V4	Local IP address (control connection) , formatted as an IPv4 address or 255.255.255.255
end		SMF119FT_FSETime	Transmission end date and time of day
filePath		SMF119FT_FSFileName2	Second MVS or z/OS UNIX file name associated with a rename. This is the new file or data set name.
fileType		SMF119FT_FSFType	File type (SEQ, JES, or SQL)
fname		SMF119FT_FSM2	Second PDS member name (if rename operation)
in		SMF119FT_FSBytes	Transmission byte count; 64-bit integer**Error! Bookmark not defined.**
oldFileName		SMF119FT_FSM1	PDS Member name
oldFilePath		SMF119FT_FSFileName1	Server MVS or z/OS UNIX file name associated with the file transfer or rename operation. When the operation is a rename, this is the file or data set original name.
reason		SMF119FT_FSLReply	Last reply to client (3-digit RFC 959 code, right justified)
shost		SMF119FT_FSHostname	Host Name
spt		SMF119FT_FSCRPort	Remote port number (control connection - client)
src		SMF119FT_FSCRIP_V4	Remote IP address (control connection) , formatted as an IPv4 address or 255.255.255.255
start		SMF119FT_FSSTime	Transmission start date and time of day
suid		SMF119FT_FSSUser	Client User ID on server

SMF 119 Fields of the FTP Server Logon Failure Record (Subtype 72)

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
c6a2	RemtIP	SMF119FT_FFRIP	Remote IPv6 address
c6a3	LocIP	SMF119FT_FFLIP	Local IPv6 address

CEF Name	CEF Label	CZAGENT Field Name	Description[4]
cs5	Security	SMF119FT_FFScty	See SMF 119 Fields of the Type 119 Security Sections above.
dpt		SMF119FT_FFLPort	Local port number (Server)
dst		SMF119FT_FFLIP_V4	Local IP address, formatted as an IPv4 address or 255.255.255.255
reason		SMF119FT_FFReason	Login failure reason: Password invalid, Password expired, User ID revoked, No user server access, FTCHKPWD reject, Excessive bad passwords, Group ID failed, User ID unknown, Certificate not valid, or Client name certificate or ticket user name mis-match
spt		SMF119FT_FFRPort	Remote port number (Client)
src		SMF119FT_FFRIP_V4	Remote IP address, formatted as an IPv4 address or 255.255.255.255
suid		SMF119FT_FFSUser	Client User ID received by server

SMF ACF2 Fields

SMF ACF2 Fields Common to All Type ACF2 Record Subtypes

CEF Name	CEF Label	CZAGENT Field Name	Description[5]
cat		SMFACF2CAT	Constant “ACF2”
deviceExternalId		ACSMFIDE	SMFID of sys where event occurred
deviceProcessName		ACSMFMOD	Name of module that journalled this record
duser		ACSMFNAM	ACF2 user name
end		ACSMFTOD	Time of delete TOD stamp (Logon ID/rule/info)
reason		ACSMFERR	Error message number for E/L/R records logging failed change attempts.
sproc		ACSMFJOB	Job name
start		ACSMFRTM	Job time stamp from reader
suid		ACSMFLID	ACF2 user Logon ID string

SMF ACF2 Fields of the ACRECD (Dataset & Program Security Journal) Record Subtype

CEF Name	CEF Label	CZAGENT Field Name	Description[5]
cs2	DD	A$SSPDDN	DD name used for access

[5] Most of these descriptions are taken directly from ACFSMF and associated CA MACROs, Copyright © 2000, 2008 CA Inc.

CEF Name	CEF Label	CZAGENT Field Name	Description[5]
cs3	JobID	A$SSJES#	JES job Id number
cs5	StepNm	A$SSSTEP	Current stepname
fileID		A$SSPVOL	Volume on which dataset resides
filePath		A$SSPDSN	Dataset accessed
fname		A$SSPMEM	Member name for PDS, if any
oldFileId		A$SSOVOL	Original volume for DSN
oldFilePath		A$SSODSN	Original/unmodified DSN
spid		A$SSPID1	Security Module Issuing Svc expressed as an integer code
spid		A$SSPID1D	Security Module Issuing Svc expressed as text
spriv		A$SLTFLG	User's privileges expressed as an integer
spriv		A$SLTFLGD	User's privileges expressed as text
suser		A$SSNAME	Users name

SMF ACF2 Fields of the ACRECL (Logon ID Modification) Record Subtype

CEF Name	CEF Label	CZAGENT Field Name	Description[5]
cs4	LIDname	LIDNAME	Name of user
cs5	LogonID	LIDLID	Logon ID - index for this record
cs6	LIDuser	LIDTFLAG	User type flags

SMF ACF2 Fields of the ACRECU (RACROUTE REQUEST=DIRAUTH) Record Subtype

CEF Name	CEF Label	CZAGENT Field Name	Description[5]
fileType		ACUMF_F2	Flag for TYPE keyword expressed as an integer
fileType		ACUMF_F2D	Flag for TYPE keyword expressed as text
outcome		ACUMF_SAFRC	SAF return code

SMF ACF2 Fields of the ACRECV (Resource Access Violation/Log) Record Subtype

CEF Name	CEF Label	CZAGENT Field Name	Description[5]
cs1	SubFunc	ACVMFSFN	Input sub-function
fileType		ACVMFLRT	Logical resource type

SMF DB2 Fields

SMF DB2 Fields Common to All DB2 IFCIDs

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs3	Work	QWHSLWID	Logical unit of work ID
cs4	Loc	QWHSLOCN	Local location name
cs5	NetID	QWHSNID	Network ID
cs6	CorrID	QWHCCV	Correlation ID
dproc		SM100SSI	DB2 Subsystem ID
duid		QWHCAID	Correlation authorization ID
shost		QWHCEUWN	The end user's workstation name
sproc		QWHCPLAN	Plan name
suid		QWHCEUID	The end user's user ID at the user's workstation

SMF DB2 Fields of IFCIDs 23, 24 and 25

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cn1	DBID	QW002XDB	Database ID (DBID)
cn3	PSID	QW002XPD	Pagespace ID
deviceProcessName		QW002XNM	Utility name
filePath		QW002XNA	Database name
fname		QW002XPN	Object name
sproc		QW002XJN	Job name. IFCIDs 24 and 25 only.

SMF DB2 Fields of IFCID 53

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cfp1	SQLerrd4	QW0053_SQLERRD4	Generally, contains timerons, a short floating-point value that indicates a rough relative estimate of resources required. It does not reflect an estimate of the time required. For a particular statement, this number can vary with changes to the statistics in the catalog. It is also subject to change between releases of DB2 for z/OS.
cs4	Loc	QW0053LN	Location name

[6] Most of these descriptions are taken directly from one of the following sources: “DB2 Version 9.1 for z/OS Performance Monitoring and Tuning Guide” © Copyright International Business Machines Corporation 1982, 2009; “DB2 10 for z/OS SQL Reference” © Copyright IBM Corporation 1982, 2011; the IBM macro DSNA10.ADSNMACS(DSNDQWSP) Copyright 1982, 2010 IBM Corp.; or “z/OS Security Server RACF Data Areas” © Copyright International Business Machines Corporation 1994, 2008.

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
outcome		QW0053_SQLCODE	Contains the SQL return code. 0 Successful execution (though there might have been warning messages). Positive Successful execution, but with a warning condition or other information. Negative Error condition. For the specific meanings of SQL return codes, see the IBM manual "DB2 10 for z/OS DB2 Codes."
sourceServiceName		QW0053PN	Program name

SMF DB2 Fields of IFCID 58

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cfp1	SQLerrd4	QW0058_SQLERRD4	Generally, contains timerons, a short floating-point value that indicates a rough relative estimate of resources required. It does not reflect an estimate of the time required. For a particular statement, this number can vary with changes to the statistics in the catalog. It is also subject to change between releases of DB2 for z/OS.
cs4	Loc	QW0058LN	Location name
outcome		QW0058_SQLCODE	Contains the SQL return code. 0 Successful execution (though there might have been warning messages). Positive Successful execution, but with a warning condition or other information. Negative Error condition. For the specific meanings of SQL return codes, see the IBM manual "DB2 10 for z/OS DB2 Codes."
sourceServiceName		QW0058PN	Program name

SMF DB2 Fields of IFCID 59

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs4	Loc	QW0059LN	Location name
sourceServiceName		QW0059PN	Program name

SMF DB2 Fields of IFCID 60

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs4	Loc	QW0060LN	Location name
sourceServiceName		QW0060PN	Program name

SMF DB2 Fields of IFCID 61

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs4	Loc	QW0061LN	Location name
sourceServiceName		QW0061PN	Program name

SMF DB2 Fields of IFCID 62

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
fileType		QW0062OT	Object type, expressed as a one-byte code such as T or I
fileType		QW0062OTD	Object type, expressed as a name such as Table or Index
fname		QW0062ON	Object name

SMF DB2 Fields of IFCID 63

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs1	Sql	QW0063ST_1023	Statement requested to be parsed, truncated to 1023 bytes. Host variables in SQL statements are represented as ": H". The SQL statement is truncated after 5000 bytes.

SMF DB2 Fields of IFCID 64

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs4	Loc	QW0064LN	Location name
sourceServiceName		QW0064PN	Program name

SMF DB2 Fields of IFCID 65

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs4	Loc	QW0065LN	Location name
sourceServiceName		QW0065PN	Program name

SMF DB2 Fields of IFCID 66

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs4	Loc	QW0066LN	Location name
sourceServiceName		QW0066PN	Program name

SMF DB2 Fields of IFCID 90

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs1	Cmd	QW0090CT	Command Text

SMF DB2 Fields of IFCID 91

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
outcome		QW0091RC	Command completion return code
reason		QW0091RS	Command completion reason code

SMF DB2 Fields of IFCID 92

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs1	Cmd	QW0092	Access Method Services command (160 bytes maximum)

SMF DB2 Fields of IFCID 97

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs1	Cmd	QW0097P1	Access Method Services command (160 bytes maximum)
outcome		QW0097RC	Command completion return code

SMF DB2 Fields of IFCID 107

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cn1	DBID	QW0107DB	Database ID (DBID)
cn3	PSID	QW0107OB	Pageset OBID
filePath		QW0107DN	Data base name
fileType		QW0107T	Type of request expressed as a one-byte code: C for Close or O for Open
fileType		QW0107TD	Type of request expressed as “Close” or “Open”
fname		QW0107TN	Table space name

SMF DB2 Fields of IFCID 140

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs1	Sql	QW0140TX_1023	SQL text, truncated to 1023 bytes.
cs2	AuthIDType	QW0140AT	Authorization ID type, expressed as a one-byte code of blank for primary or secondary authorization ID, and L for a role
cs2	AuthIDType	QW0140ATD	Authorization ID type, expressed as “AuthID” or “Role”

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
filePath		QW0140TC	Target Object Owner: Qualifier of the object being defined. This field is valid for the CREATE INDEX and CREATE TABLE privileges. It is also valid for the CREATE VIEW authorization check which is a set of checks against the following privileges: CREATE VIEW (when creating view for another), SELECT, INSERT, DELETE and UPDATE.
fileType		QW0140OB	Object type, expressed as a one byte code such as B or C
fileType		QW0140OBD	Object type, expressed as a textual description such as Bufferpool or Collection
fname		QW0140TN	Target object name: Name of the object being defined. This field is valid only in the same cases for which QW0140TC is valid.
outcome		QW0140RC	Return code from access control authorization exit routine: -1 - exit was not called; 4 - perform db2 authorization check; 8 - not authorized; 12 - unable to service request, do not call again
reason		QW0140RS	User defined reason code from the access control authorization exit routine
spriv		QW0140UT_SGRP	ACEE UToken submitting GROUPNAME

SMF DB2 Fields of IFCID 141

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs1	Sql	QW0141TX_1023	GRANT or REVOKE SQL statement, truncated to 1023 bytes
cs2	AuthIDType	QW0141OT	Authorization ID type, expressed as a one-byte code of blank for primary or secondary authorization ID, and L for a role
cs2	AuthIDType	QW0141OTD	Authorization ID type, expressed as “AuthID” or “Role”
dpriv		QW0141RE	Authority type, represented as a one-character code such as B or C
dpriv		QW0141RED	Authority type, represented as a textual description such as System DBADM, DBCTRL, etc.
fileType		QW0141OB	Object type, as a one byte code such as B or C
fileType		QW0141OBD	Object type, expressed as a textual description such as Bufferpool or

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
			Collection
outcome		QW0141CO	SQL return code. 0 = Successful execution (though there might have been warning messages); positive = Successful execution, but with a warning condition or other information; negative = Error condition.
reason		QW0141AC	Access granted or revoked, expressed as a one-character code G or R
reason		QW0141ACD	Access granted or revoked, expressed as text Grant or Revoke

SMF DB2 Fields of IFCID 142

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cn1	DBID	QW0142DB	Database ID
cn2	OBID	QW0142OB	Object ID
cs1	Sql	QW0142TX_1023	SQL text, truncated to 1023 bytes.
cs2	AuthIDType	QW0142OR	Authorization ID type, expressed as a one-byte code of blank for primary or secondary authorization ID, and L for a role
cs2	AuthIDType	QW0142ORD	Authorization ID type, expressed as “AuthID” or “Role”
filePath		QW0142OW	Table owner, same as qualifier
fname		QW0142TN	Table name
reason		QW0142AC	Statement type (CREATE, DROP or ALTER) expressed as a one-character code
reason		QW0142ACD	Statement type (CREATE, DROP or ALTER) expressed as a text

SMF DB2 Fields of IFCID 143 and 144

Note: these field names are all common to IFCID 143 and 144.

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cn1	DBID	QW0143DB	Database ID (DBID)
cn2	OBID	QW0143OB	Record OBID
cn3	PSID	QW0143PS	Pageset OBID

SMF DB2 Fields of IFCID 145

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs1	Sql	QW0145RT_1023	SQL statement text truncated to 1023 bytes. Additional statement text is written in subsequent records until the entire SQL statement text is written. *The DB2 Version 9.1 IFCID record refers to the SQL statement text as QW0145TX. dbDefender uses the field name QW0145RT_1023 for all supported versions of DB2.*
outcome		QW0145SC	SQL return code. 0 = Successful execution (though there might have been warning messages; probably does not occur for IFCID145); positive = Successful execution, but with a warning condition or other information; negative = Error condition.
sourceServiceName		QW0145PN	Program name

SMF DB2 Fields of IFCID 233

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs4	Loc	QW0233LN	Location name
fileType		QW0233TY	Type of statement, represented as an integer
fileType		QW0233TYD	Type of statement, represented as “OPEN”, “FETCH” etc.
outcome		QW0233EX	Action expressed as a code: 00 The agent is entering a routine; 01 The agent has returned from a routine
outcome		QW0233EXD	Action expressed as text: Entry or Exit
sourceServiceName		QW0233PN	Program name
suser		QW0233PR	Routine specific name

SMF DB2 Fields of IFCID 247

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs4	Loc	QW0247LN	Location name
fileType		QW0247TY	Data type of this entry, expressed as an integer (see the IBM manual “DB2 for z/OS SQL Reference”)
sourceServiceName		QW0247PN	Program name

SMF DB2 Fields of IFCID 319

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
c6a2	ReqIP	QW0319RI_IPv6	IPv6 Address, if TCP/IP
deviceProcessName		QW0319CP	Client product ID
src		QW0319RI_IPv4	IPv6 Address, if TCP/IP, formatted as an IPv4 address, or 255.255.255.255
suid		QW0319US	Derived userid
suser		QW0319D1	Requesting Kerberos principal name, if applicable.

SMF DB2 Fields of IFCID 361

Note: IFCID 361 is not available in DB2 Version 9.

CEF Name	CEF Label	CZAGENT Field Name	Description[6]
cs1	Cmd	QW0361TX_1023	SQL statement or command, truncated at 1023 bytes if required
cs2	AuthIDType	QW0361IT	Authorization ID type, expressed as a one-byte code of blank for primary or secondary authorization ID, and L for a role
cs2	AuthIDType	QW0361ITD	Authorization ID type, expressed as “AuthID” or “Role”
dpriv		QW0361AT	Authority type, represented as a one-character code such as B or C
dpriv		QW0361ATD	Authority type, represented as a textual description such as System DBADM, DBCTRL, etc.
filePath		QW0361TC	Target object qualifier/owner
fileType		QW0361OT	Object type, expressed as a one-byte code such as B or C
fileType		QW0361OTD	Object type, expressed as a name such as Bufferpool or Collection
fname		QW0361TN	Target object name
spriv		QW0361PR	Privilege checked, expressed as an integer
spriv		QW0361PRD	Privilege checked, expressed as a textual description such as “Display profile” or “Start profile”.

SMF DIAG Fields

CEF Name	CEF Label	CZAGENT Field Name	Description
cat	Cmd	SMFDIAGCAT	Constant “Diag”

Trademarks

dbDefender is a trademark and CorreLog® is a registered trademark of CorreLog, Inc.

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

DB2®
IBM®
MVS
RACF
z/OS®

ACF2® and Top Secret® are registered trademarks of CA Inc.