



CorreLog Agent for z/OS

Integrating z/OS Mainframe into
Enterprise SIEM



CorreLog Agent for z/OS

WHY A CORRELOG AGENT FOR z/OS?

Regulatory Requirements

- PCI DSS – the Payment Card Industry Data Security Standard
 - Applies to you if you process or store credit card data
 - Requires (among other things) a secure, archived log of privileged user access, invalid access attempts, creation and deletion of system level objects, ...
- HIPAA
 - Penalties for illegitimate access to patient data range up to \$50,000 per violation
- IRS Publication 1075
 - Applies to state agencies with whom IRS shares taxpayer data
 - Requires auditing of access and retention of audit data
- Sarbanes-Oxley
 - Requires the “security and preservation” of financial data
- Dodd-Frank, FISMA, etc.

Don't Find a Crew from *60 Minutes* Outside Your Office

- Bank of America Insider Theft
 - Employees sold customer information to prison-based identity theft gang
 - Cost Bank of America more than \$10 million
- Celebration, Florida Hospital Records Theft
 - Registration clerk searched 760,000 patient records for accident victims
 - Sold data to third party who solicited for chiropractic and legal services
- South Carolina Health and Human Services
 - Employee e-mailed himself 228,435 patient records, including ID numbers
- LSU Hospital Identity Theft
 - Billing clerk used database check images to create fake checks and IDs
 - 416 patients victimized
- South Carolina Department of Revenue Breach
 - 74 GB of tax return data including SSNs stolen with employee's credentials
 - Employee had fallen victim to phishing attack
- Texas Department of Health and Human Services
 - Worker used patient immunization records to obtain credit cards online



CorreLog Agent for z/OS

z/OS AGENT OVERVIEW

The CorreLog Agent for z/OS

- Standards-conformant Syslog Agent for z/OS
- Runs as z/OS started task
- Real-time monitoring of z/OS security events
- Flexible enough to accommodate any SIEM system
- Simple to configure and administer
- Minimal use of mainframe resources
- Reliable Syslog delivery via TCP/IP
- Optional state-of-the-art TLS encryption using z/OS Cryptographic Services

Syslog Agent?

- “Syslog” has two meanings
- z/OS SYSLOG: “a data set residing in the primary job entry subsystem's spool space ... used by application and system programmers to record communications about problem programs and system functions.”
 - *MVS Planning: Operations*

```
Display Filter View Print Options Search Help
50SP SYSLOG 5017.101 SYS0 SYS0 02/10/2012 TW 051,740 COLUMNS 02- 01
COMMAND INPUT
=====
N 4000000 SYSB 12041 17:40:00.09 STC06972 00000000 TMD0000071 - Connect Mgr
N 4000000 SYSB 12041 17:40:00.09 STC06972 00000000 TMD0000061 - Connect Mgr
N 4000000 SYSB 12041 17:40:08.13 STC06972 00000000 TMD0000071 - Connect Mgr
N 4000000 SYSB 12041 17:40:08.13 STC06972 00000000 TMD0000211 - Connect Mgr
N 4000000 SYSB 12041 17:40:08.13 STC06972 00000000 TMD0000231 - Connect Mgr
N 4000000 SYSB 12041 17:40:08.13 STC06972 00000000 TMD0000241 - Connect Mgr
N 0000000 SYSB 12041 17:40:00.14 000000200 IEA0091 SLIP TRAP ID=X13
N 4000000 SYSB 12041 17:40:10.41 STC06972 00000000 TMD0000271 - Connect Mgr
N 4000000 SYSB 12041 17:40:10.42 STC06972 00000000 TMD0000231 - Connect Mgr
N 4000000 SYSB 12041 17:40:10.42 STC06972 00000000 TMD0000241 - Connect Mgr
N 0000000 SYSB 12041 17:40:10.42 000000200 IEA0091 SLIP TRAP ID=X13
N 4000000 SYSB 12041 17:40:10.49 STC06972 00000000 TMD0000271 - Connect Mgr
N 4000000 SYSB 12041 17:40:12.86 STC07004 00000000 TMD0430511 - Module exit
N 4000000 SYSB 12041 17:40:12.86 STC07004 00000000 TMD0430571 - QMS Mgr DB2
N 4000000 SYSB 12041 17:40:12.87 STC07004 00000000 TMD0430991 ACT/SUPP DB2
N 4000000 SYSB 12041 17:40:12.87 STC07004 00000000 TMD0430511 - Module exit
N 4000000 SYSB 12041 17:40:12.87 STC07004 00000000 TMD0430991 FREE DSL buff
N 4000000 SYSB 12041 17:40:12.87 STC07004 00000000 TMD0430501 - DSL buf sta
N 4000000 SYSB 12041 17:40:12.87 STC07004 00000000 TMD0430511 - Module exit
N 4000000 SYSB 12041 17:40:16.51 STC07004 00000000 TMD0430991 FREE DSL buff
N 4000000 SYSB 12041 17:40:16.51 STC07004 00000000 TMD0430501 - DSL buf sta
N 4000000 SYSB 12041 17:40:18.92 STC07004 00000000 TMD0430511 - Module exit
N 4000000 SYSB 12041 17:40:18.92 STC07004 00000000 TMD0430991 ACT/SUPP DB2
N 4000000 SYSB 12041 17:40:18.92 STC07004 00000000 TMD0430511 - Module exit
N 0000000 SYSB 12041 17:40:26.42 IAS1TRM0 000002100 LOGIN
N 0200000 SYSB 12041 17:40:34.25 TSU07274 00000251 SHASP100 R00100 ON TSO
N 4000000 SYSB 12041 17:40:34.29 TSU07274 00000000 SHASP373 R00100 STARTE
N 0000000 SYSB 12041 17:40:34.29 TSU07274 00000000 IEF1251 R00100 - LOGGED
N 0000000 SYSB 12041 17:40:34.31 STC05926 00000200 CACLIEN004E CONNECT FAT
N 0000000 SYSB 12041 17:40:34.41 TSU07274 00000000 CC0246021 DSN: SYS1,DR
N 0000000 SYSB 12041 17:40:34.41 TSU07274 00000000 CC0246031 REJECT CMP
4200000 SYSC 14.01.24 STC06613 *3295 DF59961 *IMS READY* IM1A
0020000 PROD 09.51.17 STC09540 *2502 LMK065031 - GDC3PTMP REPLY: APPL=, BYP
4200000 EDUC 16.28.01 STC01203 *2967 DF59961 *IMS READY* I110
4200000 EDUC 16.27.44 STC01203 *2963 DF59961 *IMS READY* IM10
4000000 SYS0 12.40.47 STC00205 *2860 REPLY WITH REQUEST TO IDMS V1700
4120000 PROD 13.20.09 STC04470 *1347 EMS0990A EMSVRS01 READY FOR COMMANDS,
4000000 SYS0 09.23.37 STC09524 *2582 REPLY WITH REQUEST TO IDMS V1000
***** BOTTOM OF DATA *****
```

- That is not the “Syslog” I’m talking about



“Syslog” – The Security Meaning

- “The BSD syslog Protocol”
 - IETF RFC 3164 and follow-ons RFC 5424, 5425 and 5426
 - Almost free-format text (ASCII) messages
 - `<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8`
 - UDP or TCP/IP with optional SSL/TLS encryption
 - Generated by most routers, firewalls, UNIX systems, etc.
 - No native Syslog capability: Windows and z/OS

A pure mainframe, pure standards-based solution

z/OS Mainframe



CorreLog
CZAGENT

Real-Time SMF Data



CorreLog or any other Syslog Console



Agent and Syslog Console
plug together via RFC 3164
(UDP) or RFC 6587 (TCP/IP)

CorreLog Agent for z/OS

- Integrates your z/OS mainframe into your enterprise SIEM strategy
- Helps assure mainframe compliance with FISMA, PCI DSS, HIPAA, NERC, and Sarbanes-Oxley
- Forwards security, TCP/IP, job and database events to CorreLog or any Syslog console
- Highly configurable: get just the events and data you need
- Compatible with all current releases of z/OS: V1R11 through V2R1
- Installs in just a few hours
- Uses just a few seconds of CPU time per day





CorreLog Agent for z/OS

EVENT TYPES MONITORED

Event Types

SMF Record Type	Description of Events
15	Close of conventional datasets opened for output
18	Dataset renames
30	Job, Started Task, and TSO Session starts and ends. Captures TSO logons, job completions, and ABENDs
42	Modifications to libraries such as z/OS parmlibs
64	Close of VSAM datasets
80	RACF and Top Secret Security events, including successes. Captures invalid passwords, illegal resource access attempts, configuration changes, etc.
100, 101, 102	DB2 auditing. Captures administrative actions, invalid logical access attempts, etc.
110	CICS. Captures usage of audited transactions.
119	TCP/IP and FTP events. Captures incoming connections and FTP failures and successes
230	ACF2 events, including successes. Captures invalid passwords, illegal resource access attempts, configuration changes, etc.

dbDefender Audits DB2 Security in Real Time

- Monitors events required by PCI DSS, HIPAA, Sarbanes-Oxley, etc.
 - Actions by privileged users
 - Invalid logical access attempts
 - Creation and Deletion of System Level Objects
 - All accesses to specific tables
 - Up to 23 different types of events
- Designed for easy configuration and minimal impact on performance
 - Optionally starts required DB2 traces automatically
 - Optionally suppresses disk I/O for SMF trace records

DB2 Auditing in CorreLog Dashboard

#1: Z DB2 Administrative Actions

Administrative Actions

Sort: Span:

Value:	Count	Graph
EXECUTE	9	
USE	4	
LOAD	4	
DROP	4	
RUNSTATS UTILITY	2	
CREATE TABLE	2	
CREATE TABLESPACE	2	

#2: Z DB2 Invalid Logical Access

Access Violators

Sort: Span:

Value:	Count	Graph
RU018A	2	

1 Parsed Values.

[Related Info...](#)

#3: Z DB2 Audited Objects

Read and Write of Audited Objects

Sort: Span:

Value:	Count	Graph
RU018B	6	

1 Parsed Values.

#4: Z DB2 System Level Objects

Creation and Deletion of System Level Objects

Sort: Span:

Value:	Count	Graph
DELETE DA1LDB.DSNDBC.COR...	2	
DEFINE CL(NAME/DA1LDB.DS...	2	
DELETE DA1LDB.DSNDBC.COR...	2	
DEFINE CL(NAME/DA1LDB.DS...	2	

4 Parsed Values.

#5: Z DB2 DDF Identity Mapping

Remote IP Addresses Accessing DB2

Sort: Span:

Value:	Count	Graph
::ffff:10.2.1.126	3	

1 Parsed Values.

#6: Z DB2 SQL for Audited Objects

SQL for Audited Objects

Sort: Span:

Value:	Count	Graph
SELECT * FROM CORE1010.N...	1	

1 Parsed Values.



DB2 - Privileged User Monitoring

- Required by PCI DSS 10.2.2
- Message includes user ID, affected table, type of action (“SELECT”) and text of SQL or command
- Overhead: Very low

User ID

Type of Admin
Authority

Text of SQL or
command

```
DB2: Subsys: DA1L - IFCID: 361 - UserID: RU018B -  
AuthID: RU018B - CorrID: RU018BD3 - Auth: SYSADM -  
Priv: SELECT - ObjType: Table or view - Cmd: SELECT  
* FROM SYSIBM.SYSTABLES - SrcQual: SYSIBM - Src:  
SYSTABLES
```

DB2 Invalid Logical Access Attempts

- Required by PCI DSS 10.2.4
- Message includes user ID, submitter's node, and "Port of Entry" (terminal name, etc.)
- Overhead: Very low

Source of
Access Attempt

Attempted SQL

User ID

```
DB2: Subsys: DA1L - IFCID: 140 - UserID: RU018A - AuthID:  
RU018A - CorrID: RU018ADS - Priv: SELECT - ObjType: Table  
or view - SrcQual: CORE1010 - Src: NEWPHONE - ExitRet: -1  
- Lang1: Dynamic - Lang3: None - Node: JES2SYSB - Group:  
RESTRICT - POE: INTRDR - Sql: SELECT * FROM  
CORE1010.NEWPHONE
```


DB2 Reads or Writes of Audited Tables

- Required by PCI DSS 10.2
- Message includes Authorization ID, remote transaction program, workstation name
- Overhead: Moderate – one record per commit

Remote application
name

Remote
workstation

User ID

```
DB2: Subsys: DA1L - IFCID: 144 - UserID: RU018B - AuthID:  
RU018B - CorrID: 300_ODBC.exe - DBID: 265 - PSID: 4 -  
OBID: 18 - Plan: DISTSERV - OpID: RU018B - Trans:  
300_ODBC.exe - WrkSta: X201NOTEBOOK - Loc: NA01DA1L -  
NetID: GA020193 - LU: AFA2 - Conn: SERVER
```

Alert on Events by Text or E-Mail



[Advisory](#) | [Search](#) | [Query](#) | [More](#) | User: [admin](#)

Home | Dashboards | Messages/ | Correlation/ | **Alerts/** | Tickets/ | Reports/ | System/ | [Help](#)

Counters | Devices | Patterns | Custom | Config/

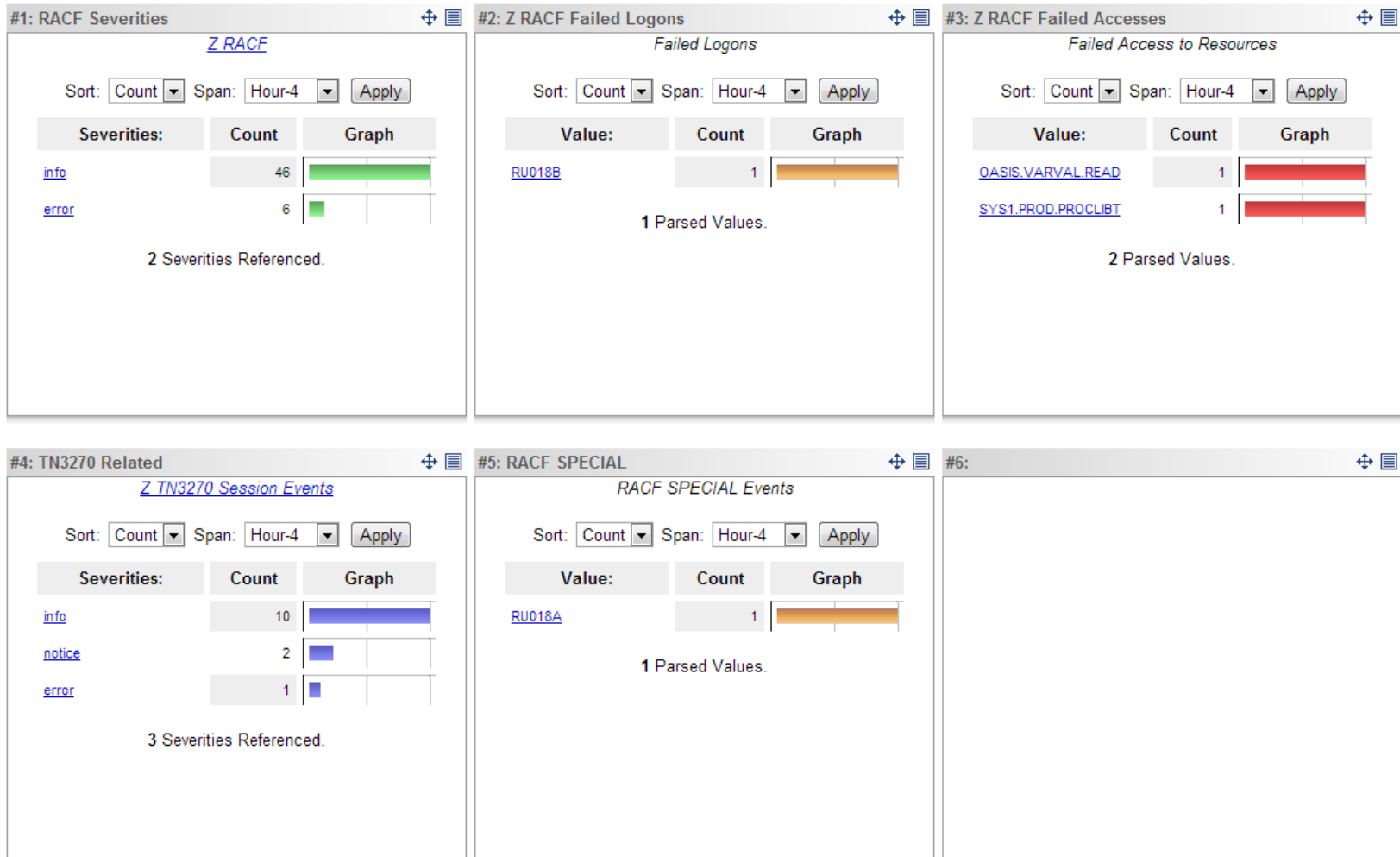
Sort By: State | List: Max-50 | Match: * | [Apply](#) | [AddNew >](#) | [Wizard >](#)

Edit:	State:	Threshold: Counts Per Interval	Now: Counts Per Interval	Alert Severity & Message:
# 01		GE 2 / 120 Secs	0	notice: More than 2 DB2 Invalid Logical Access attempts in past two minutes! Counter: Thread/ Z DB2 Invalid Logical Access Assigned To: admin
# 02		GE 1 / 120 Secs	0	notice: Thread/ Z FTP Requested File Action Not Taken - Too Many Messages Received - Problem Should Be Investigated Counter: Thread/ Z FTP Requested File Action Not Taken Assigned To: admin

[Audit Full Alert Configuration Data](#)



Security Events



Drill Down to RACF Event Detail

- Compatible with RACF and CA Top Secret
- Expired passwords, revoked user IDs, security configuration changes, unauthorized access attempts, and similar mainframe security events
- Example:

User Name
SYSB RACF: RESOURCE ACCESS: Insufficient Auth -
UserID: RU018B - Group: RESTRICT - Reas: AUDIT
option - Job: RU018BTR - Res:
SYS1.PROD.PROCLIBT - Req: READ - Allow: NONE -
Vol: SYS001 - Type: DATASET - Prof:
SYS1.PROD.PROCLIBT - Owner: DATASET - Name:
ROBERT SMITH - POE: INTRDR

Resource

Type of Event

ACF2 Security Events

- Logon ID Modification, Dataset & Program Security Journal, Invalid Password Authority, Resource Access Violation, Restricted Logon ID and similar mainframe security events

- Example:

User Name

User ID

Type of Event

```
mvssysb ACF2: EventDesc: Logonid  
modification - ChgDesc: Delete - JobNm:  
DECRO01 - UserID: DECRO01 - Pgm: ACF02ALT -  
Name: ROSS DECENT - Rel#: 140 - RdrTime:  
2012-07-03T16:19:43.880 - ASID: XE34 -  
DelTime: 2012-07-03T17:19:51.028 - UID:  
OMVSDGRPAAABDECRO01
```

Audits Failed TSO Logons

- Shows user ID, name, and terminal
- Use corresponding TCP/IP event to trace back to originating IP address

User Name

User ID

```
RACF: INIT/LOGON: Invalid Password - UserID: QAMLB2 -  
Group: TSOHOLD - Auth: 00 - Reas: VERIFY failure - Term:  
TCPA2959 - Name: MARIE BERGERON - POE: TCPA2959
```

Correlate TSO Access Back to IP Address

- Failed TSO Access:

```
RACF: INIT/LOGON: Invalid Password - UserID:  
QAMLB2 - Group: TSOHOLD - Auth: 00 - Reas: VERIFY  
failure - Term: TCPA2959 - Name: MARIE BERGERON -  
POE: TCPA2959
```



Full IPv6
Support



Optional ISO8601
Time Formatting

- TN3270 Session Initiation

```
TCP/IP: Subtype: Telnet SNA init - InitTime: 2012-  
05-14T21:38:15.150 - App:TN3270S - TermNm:  
TCPA2959 - RemtIP: ::ffff:10.90.0.90
```

File Integrity Monitoring

- Be alerted to modifications of critical system files

Terminal

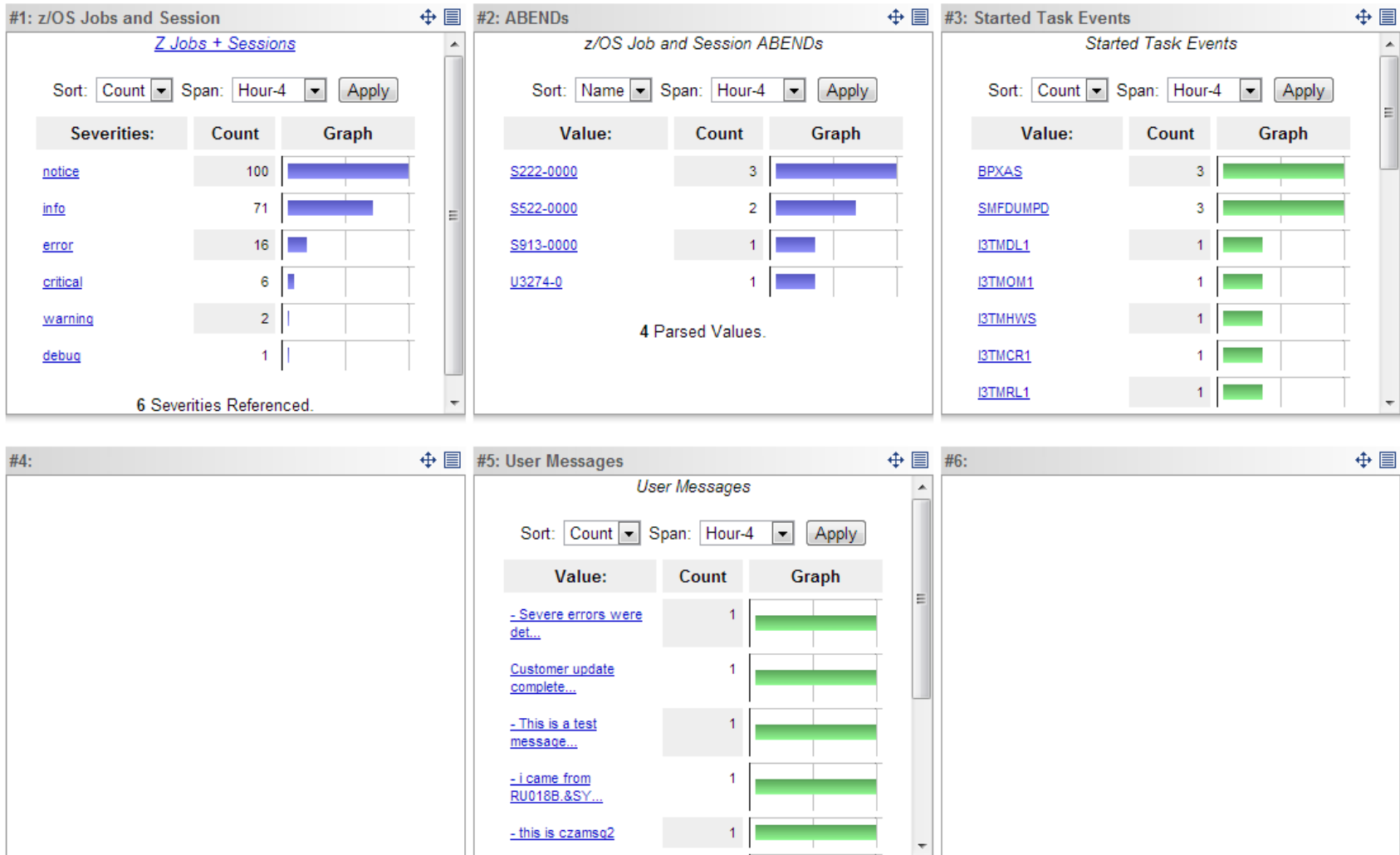
File Name

Type of Access

User Name

```
SYSB RACF: RESOURCE ACCESS: Successful  
Access - UserID: RU018B - Group: RESTRICT -  
Auth: Normal check - Reas: AUDIT option -  
Term: TCPA2953 - Job: RU018B - Res:  
RU018B.AUDITALL.TEST1 - Req: UPDATE - Allow:  
ALTER - Vol: LS0158 - Type: DATASET - Prof:  
RU018B.AUDITALL.* - Name: ROBERT SMITH
```


View Job and Started Task Events



Collects Job Events

- Notifies your Syslog console if mainframe jobs are failing
- Generates compliance audit trail of TSO logons
- Highly configurable: collect as much or as little information as you want
- Example:

System Task

ABEND Code

```
SMF: End - Work: STC - Sysname: SYSB - JobNm:  
MITDB41T - JobID: STC07802 - Step#: 1 - Group:  
DFLTSTC - UID: LSCSTC - RC: U0011-0
```

Monitors FTP and TN3270 Logons

#1: z/OS TCP/IP

Z TCP/IP

Sort: Span:

User Names:	Count	Graph
10.2.2.155	731	
Lscstc	518	
B42v310p	125	
127.0.0.1	34	
Nvpphub3	20	
Ru018b	14	
Mdrris22	11	

#2: TN3270

TN3270 Session Initiation and Termination

Sort: Span:

Value:	Count	Graph
10.10.8.155	1	
10.21.0.105	1	
10.2.1.126	1	
10.10.7.74	1	
10.2.1.110	1	

5 Parsed Values.

#3: TCP/IP Session Initiation by Country

Source Country of Session Initiation

Sort: Span:

Value:	Count	Graph
ZZ	5	

1 Parsed Values.

#4: FTP Client File Transfers

FTP Client File Transfers

Sort: Span:

Value:	Count	Graph
RU018B.DELETE.ME	4	
CUSTDUMP.S861259.SADDMP...	1	

2 Parsed Values.

#5: FTP Server File Transfers

FTP Server File Transfers

Sort: Span:

Value:	Count	Graph
RU018B.CORRELOG.CDSECT	2	

1 Parsed Values.

#6: FTP Login Failures

FTP Login Failures

Sort: Span:

Value:	Count	Graph
::ffff:10.2.8.52	1	

1 Parsed Values.



Collects FTP and Other TCP/IP Events

- Logs failed attempts to access FTP
- Audits Successful FTP usage: know who transferred what files and where
- Example:

```
TCP/IP: Subtype: FTP server complete - Stack:  
TCPIP - Op: Retrieve - FileType: SEQ - RemtDataIP:  
::ffff:10.31.0.209 - UserID: RX239JB - DStype: HFS  
- Start: 11037 22:32:45.21 - Dur: 0.78 - Bytes:  
56324 - SessID: FTPD100335 - DSN:  
/u/rx239jb/Source/Fields.C - Security: {Mech: None  
- CtlProt: None - DataProt: None - Login:  
Password}
```

FTP Download

User ID

File name

Collects Failed FTP Logons

- See who is trying to access your mainframe
- Trace back to originating IP address

User ID

See logon failures

Originating IP
Address

```
TCP/IP: Subtype: FTP server logon fail - Stack: TCPIP -  
AS: FTPD1 - UserID: DV174A - RemoteIP: ::ffff:10.10.8.66 -  
LogonUserID: DV174A - Reas: Password invalid - SessID:  
FTPD100026 - Security: {Mech: None - CtlProt: None -  
DataProt: Undefined - Login: Password}
```

Audits CICS Transactions

- Logs audited CICS transactions
- Know who ran critical transactions, and when

User ID

ISO 8601
Timestamp

CICS Transaction

```
SYSB CICS: - JobNm: QBCTS410 - Tran: DB2I  
- UserID: CICSUSER - Type: SD - Start:  
2012-05-14T18:21:02.573 - Stop: 2012-05-  
14T18:21:02.913 - Pgm: BMRKDB2I - Net:  
USTCS.QBCTS410 - ServCls: CICSDFLT -  
ReptCls: QDFLT
```

Built-In Support for ArcSight and Splunk

- One-parameter change to support ArcSight or Splunk:
 - **OPTIONS SIEM(RFC3164 | CEF | SPLUNK)**
- ArcSight- and Splunk-ready parameter files distributed with product



z/OS Events in ArcSight ESM

The screenshot displays the ArcSight Console interface. The title bar indicates the version is 6.0.0.1333.0 and it is a trial license. The main window shows the 'Correlog' viewer with the following details:

- Active Channel: Correlog [Modified]
- Total Events: 21,928
- Start Time: 14 Nov 2013 18:00:00 PST
- End Time: 1 Dec 2013 17:00:00 PST
- Filter: HotchPotter (Correlog)
- Inline Filter: Device Event Class ID = "RAC"

The 'Radar' section is currently empty. Below it, a table lists event details:

Manager Receipt Time	Name	Device ID	Device Type	Device Vendor	Device Product	Device ID	Device ID	End Time	Device Host Dev	Attacker Host	Attacker User Name	Attacker User	So	Dr
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF		CorreLog	Agent for z/OS	1		11/15 20:23:17	mvstsysb	TCPP0896		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF		CorreLog	Agent for z/OS	1		11/15 20:23:17	mvstsysb	TCPP0896		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF		CorreLog	Agent for z/OS	1		11/15 20:23:17	mvstsysb	TCPP0896		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF		CorreLog	Agent for z/OS	1		11/15 20:23:17	mvstsysb	TCPP0896		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF		CorreLog	Agent for z/OS	1		11/15 20:23:17	mvstsysb	TCPP0896		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF		CorreLog	Agent for z/OS	1		11/15 20:23:17	mvstsysb	TCPP0896		
15 Nov 2013 07:18:38 PST	INET.LOGON: Undefined User ID	RACF		CorreLog	Agent for z/OS	6		11/15 20:18:31	mvstsysb					
15 Nov 2013 07:18:38 PST	INET.LOGON: Successful Racint De...	RACF		CorreLog	Agent for z/OS	1		11/15 20:18:31	mvstsysb					
15 Nov 2013 07:13:18 PST	INET.LOGON: Undefined User ID	RACF		CorreLog	Agent for z/OS	6		11/15 20:13:13	mvstsysb					
15 Nov 2013 07:13:18 PST	INET.LOGON: Successful Racint De...	RACF		CorreLog	Agent for z/OS	1		11/15 20:13:13	mvstsysb					
15 Nov 2013 07:12:28 PST	INET.LOGON: Invalid Password	RACF		CorreLog	Agent for z/OS	6		11/15 20:12:24	mvstsysb					
15 Nov 2013 07:12:28 PST	INET.LOGON: Successful Racint De...	RACF		CorreLog	Agent for z/OS	1		11/15 20:12:24	mvstsysb					
15 Nov 2015 07:11:58 PST	INET.LOGON: Successful Racint Invt	RACF		CorreLog	Agent for z/OS	1		11/15 20:11:51	mvstsysb	TCPP0828		
15 Nov 2013 07:10:48 PST	INET.LOGON: Successful Racint De...	RACF		CorreLog	Agent for z/OS	1		11/15 20:10:44	mvstsysb	TCPP0828		
15 Nov 2013 07:09:58 PST	INET.LOGON: Password phrase is n...	RACF		CorreLog	Agent for z/OS	6		11/15 20:09:47	mvstsysb	TCPP0889		
15 Nov 2013 07:09:18 PST	INET.LOGON: Successful Racint Invt	RACF		CorreLog	Agent for z/OS	1		11/15 20:09:01	mvstsysb	TCPP0828		
15 Nov 2013 07:08:08 PST	INET.LOGON: Undefined User ID	RACF		CorreLog	Agent for z/OS	6		11/15 20:07:55	mvstsysb					
15 Nov 2013 07:08:08 PST	INET.LOGON: Successful Racint De...	RACF		CorreLog	Agent for z/OS	1		11/15 20:07:55	mvstsysb					
15 Nov 2013 07:07:28 PST	INET.LOGON: Successful Racint De...	RACF		CorreLog	Agent for z/OS	1		11/15 20:07:23	mvstsysb	TCPP0828		
15 Nov 2013 07:02:38 PST	INET.LOGON: Undefined User ID	RACF		CorreLog	Agent for z/OS	6		11/15 20:02:36	mvstsysb					
15 Nov 2013 07:02:38 PST	INET.LOGON: Successful Racint De...	RACF		CorreLog	Agent for z/OS	1		11/15 20:02:36	mvstsysb					
15 Nov 2013 06:57:18 PST	INET.LOGON: Undefined User ID	RACF		CorreLog	Agent for z/OS	6		11/15 9:57:17	mvstsysb					
15 Nov 2013 06:57:18 PST	INET.LOGON: Successful Racint De...	RACF		CorreLog	Agent for z/OS	1		11/15 9:57:17	mvstsysb					
15 Nov 2013 06:52:00 PST	INET.LOGON: Undefined User ID	RACF		CorreLog	Agent for z/OS	6		11/15 9:51:58	mvstsysb					
15 Nov 2013 06:52:00 PST	INET.LOGON: Successful Racint De...	RACF		CorreLog	Agent for z/OS	1		11/15 9:51:58	mvstsysb					

z/OS Events in Splunk

The screenshot shows the Splunk search interface. The search query is 'racf', and 412 events were found. The results are displayed in a table format. The table has columns for Time and Event. The events are sorted by time, showing a sequence of RACF events on December 13, 2013. The events include an invalid password attempt, a successful Racinit Init, and a successful Racinit Delete.

Time	Event
12/13/13 5:18:00.000 PM	<35>Dec 13 17:18:00 mvssysb RACF eventdesc="INIT/LOGON: Invalid Password" severity=Error userid=CUSFIW group=LSCOMV5 auth=None reas="VERIFY failure" termnm=TCPP0693 name="FRED WRIGHT" poe=TCPP0693 host = mvssysb source = tcp:1468 sourcetype = syslog termnm = TCPP0693
12/13/13 5:05:10.000 PM	<38>Dec 13 17:05:10 mvssysb RACF eventdesc="INIT/LOGON: Successful Racinit Init" severity=Informational userid=DV231B group=TSOHOLD auth=None reas=None termnm=DV231B jobnm=NVPTTC24 name="DAVID BROOKS" poe=DV231B host = mvssysb source = tcp:1468 sourcetype = syslog termnm = DV231B
12/13/13 4:20:53.000 PM	<38>Dec 13 16:20:53 mvssysb RACF eventdesc="INIT/LOGON: Successful Racinit Delete" severity=Informational userid=DVWGD group=TSOHOLD auth=None reas=None termnm=NVPTD002 jobnm=NVPTMVB name="BILL DICKEY" poe=NVPTD002 host = mvssysb source = tcp:1468 sourcetype = syslog termnm = NVPTD002
12/13/13 4:20:53.000 PM	<38>Dec 13 16:20:53 mvssysb RACF eventdesc="INIT/LOGON: Successful Racinit Init" severity=Informational userid=DVWGD group=TSOHOLD auth=None reas=None termnm=NVPTD002 jobnm=NVPTMVB name="BILL DICKEY" poe=NVPTD002 host = mvssysb source = tcp:1468 sourcetype = syslog termnm = NVPTD002
12/13/13 4:19:41.000 PM	<38>Dec 13 16:19:41 mvssysb RACF eventdesc="INIT/LOGON: Successful Racinit Delete" severity=Informational userid=DVWGD group=TSOHOLD auth=None reas=None termnm=NVPTD002 jobnm=NVPTMVB name="BILL DICKEY" poe=NVPTD002



CorreLog Agent for z/OS

CONFIGURATION

Configuration

- Configured with single, plain-text PDS member
- Configurable to support any Syslog collector
- Flexible “IDCAMS format” statement syntax
 - **VERB PARM1 PARM2 (operand operand)**
- Easy to get going
 - Configuration file provided with install
 - Typically only two quick edits needed
- Change configuration “on the fly” without restarting agent
- Clear error messages

Configuration Statements

Statement	Description
OPTIONS	Specifies global options that apply to entire agent such as field delimiters, format of field tags, etc.
SERVER	Specifies address and port of Syslog collector
LOCAL	May optionally be used to create a local (on the LPAR) copy of all messages sent
TIME	Specifies format of all message date and time fields
SMF nn	Parameters unique to formatting of specific event type, e.g., SMF 80 statement controls formatting of RACF events

Highly Configurable

Events to Ignore

```
SMF 30 TSO( START(NOTICE) END(SUPPRESS) ) +
      STC( START(SUPPRESS) +
          END( NOTICE RC4(WARN) RC8(ERROR) ABEND(CRIT) ) ) +
      JOB( START(SUPPRESS) +
          STEPEND(SUPPRESS) +
          END( SUPPRESS RC4(WARN) RC8(ERROR) ABEND(CRIT) ) ) +
      OTHER( START(NOTICE) +
            END( SUPPRESS ABEND(NOTICE) ) ) +
FIELDS(SMF30STPD+
      SMF30WID +
      SMF30JBN +
      SMF30PGM +
      SMF30STM +
      SMF30U1F +
      SMF30JNM +
      SMF30STN +
      SMF30USR +
      SMF30GRP +
      SMF30RUD +
      SMF30TID +
      SMF30TSN +
      SMF30PSN +
      SMF30CL8 +
      SMF30SSN +
      SMF30SCC )
```

Event Severities

"INVALID PARAMETER"

Like a report generator: Fields to Display and Order in which to Display Them

Excellent Diagnostic Messages

Supplementary
message displayed
for parameter errors

```
CZA0118S Field name 'SMF30U1F' not found in  
defined fields for SMF Type 30  
CZA0011I Above error detected in CZAPARMS  
line 31, near column 16
```

User Friendly – Locate Errors Instantly

```

SMF 30 TSO(  START(NOTICE)  END(SUPPRESS) )      +
        STC(  START(SUPPRESS)                                +
              END( NOTICE   RC4(WARN) RC8(ERROR) ABEND(CRIT) ) ) +
        JOB(  START(SUPPRESS)                                +
              STEPEND(SUPPRESS)                              +
              END( SUPPRESS  RC4(WARN) RC8(ERROR) ABEND(CRIT) ) ) +
        OTHER( START(NOTICE)                                +
               END( SUPPRESS ABEND(NOTICE) ) ) +
FIELDS(SMF30STPD+
        SMF30WID +
        SMF30JBN +
        SMF30PGM +
        SMF30STM +
        SMF30UIF +
        SMF30JNM +
        SMF30STN +
        SMF30USR +
        SMF30GRP +
        SMF30RUD +
        SMF30TID +
        SMF30TSN +
        SMF30PSN +
        SMF30CL8 +
        SMF30SSN +
        SMF30SCC )
    
```

TermNm	Terminal symbolic name.
SMF30UIF	Ident User-defined identification field (taken from common exit parameter area, not from USER=parameter on job statement).
Pgmr	Programmer's name

Line 31,
Column 16





CorreLog Agent for z/OS

QUESTIONS & ANSWERS

Customers

