CORRELOG

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.

CORRELOG

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

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

CORRELOG

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*

- That is <u>not</u> the "Syslog" I'm talking about

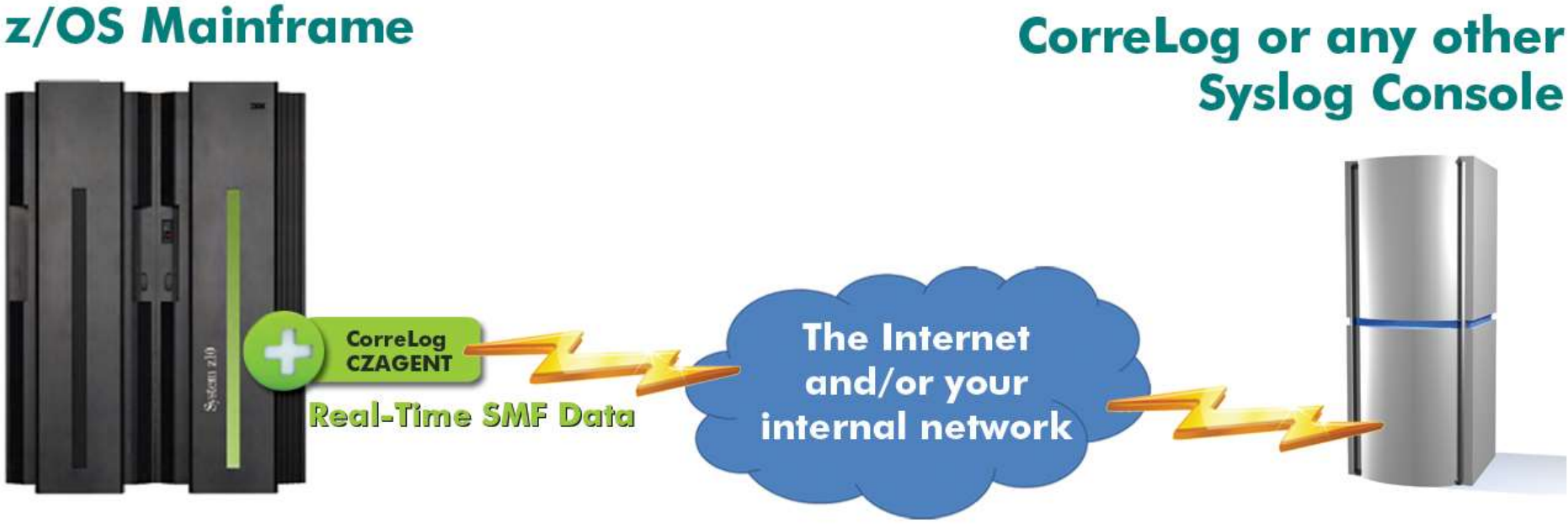
CORRELOG

“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

CORRELOG

A pure mainframe, pure standards-based solution



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

CORRELOG

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

CorreLog Agent for z/OS

EVENT TYPES MONITORED

Event Types

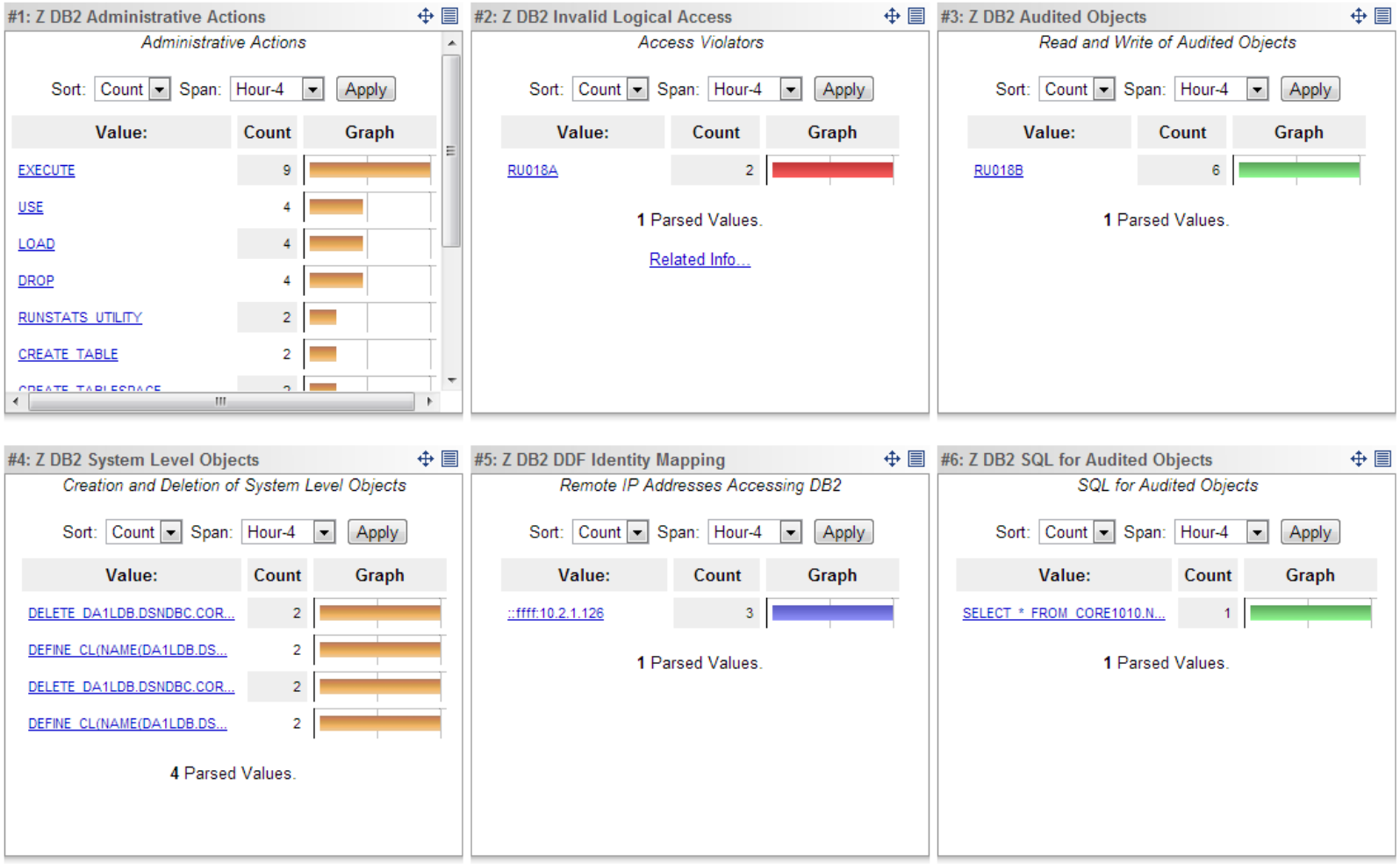
SMF Record Type	Description of Events
15	Close of conventional datasets opened for output
18	Dataset renames
30	Job, Started Task, and TSO Session starts and ends. Captures TSO logons, job completions, and ABENDs
42	Modifications to libraries such as z/OS parmlibs
64	Close of VSAM datasets
80	RACF and 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

CORRELOG

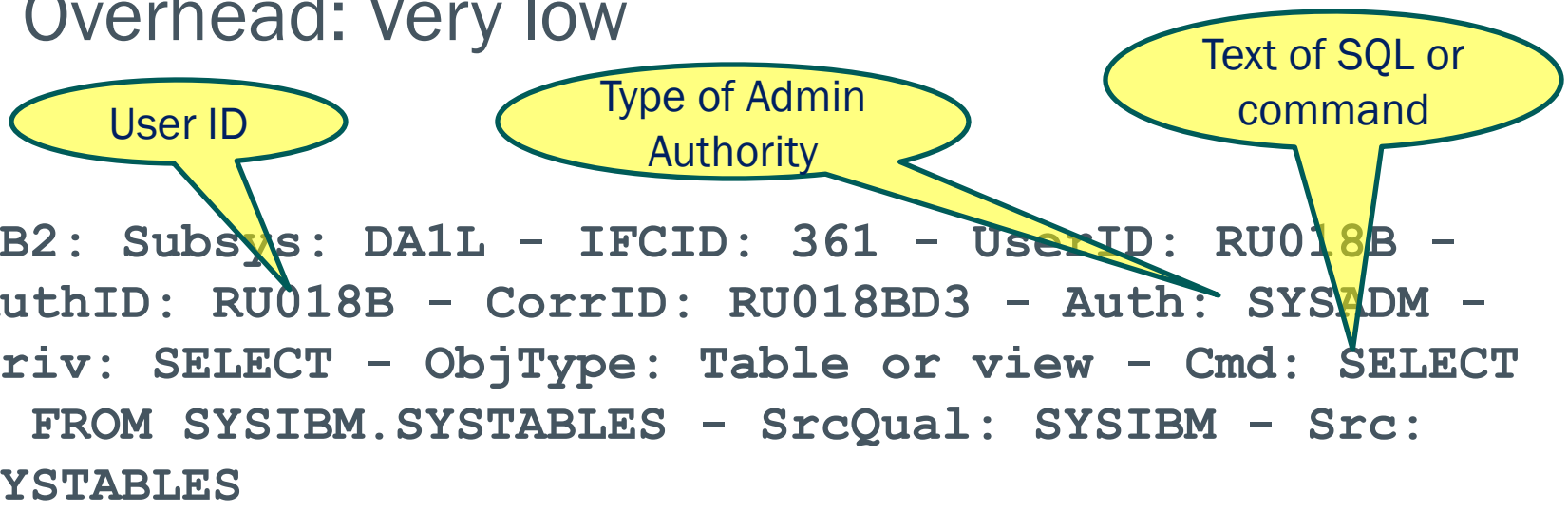
DB2 Auditing in CorreLog Dashboard



CORRELOG

DB2 - Privileged User Monitoring

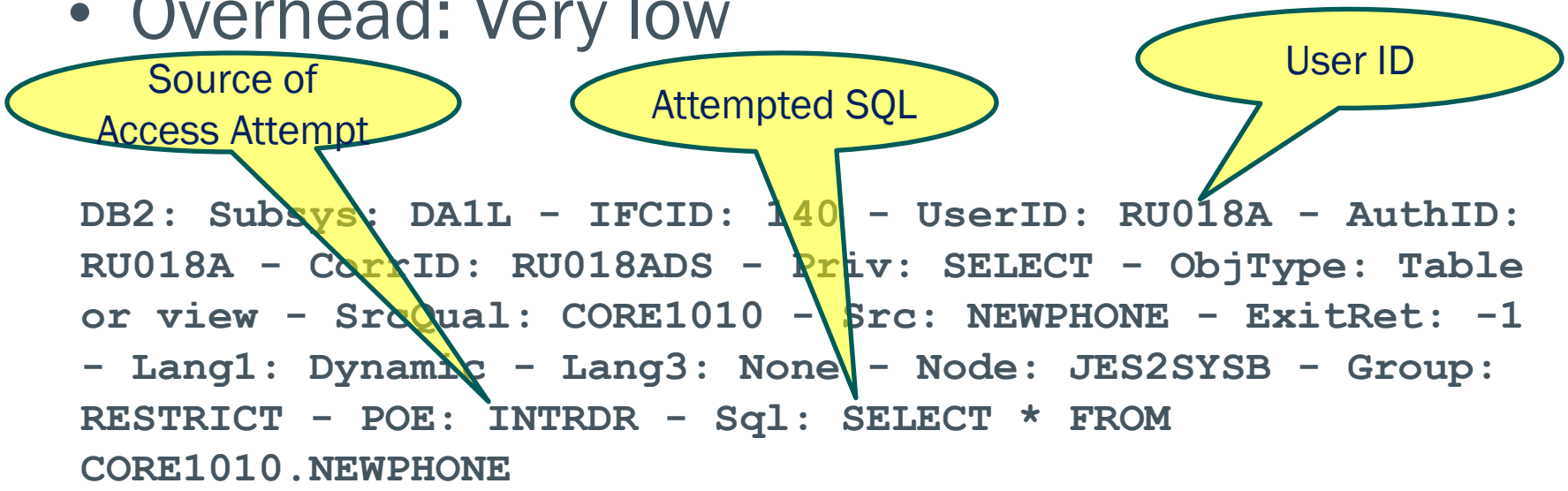
- Required by PCI DSS 10.2.2
- Message includes user ID, affected table, type of action (“SELECT”) and text of SQL or command
- Overhead: Very low



CORRELOG

DB2 Invalid Logical Access Attempts

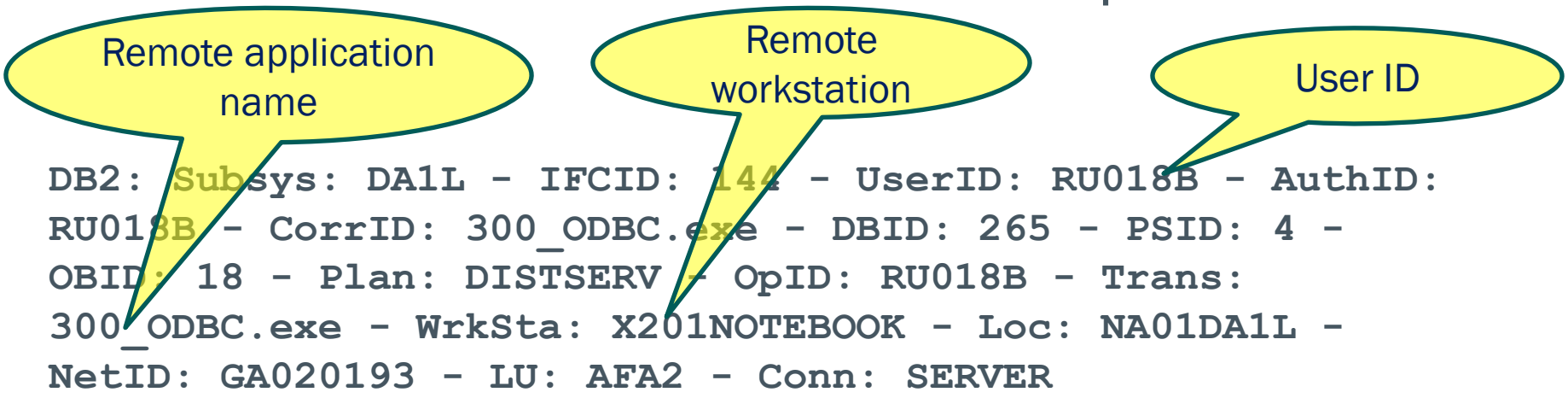
- Required by PCI DSS 10.2.4
- Message includes user ID, submitter's node, and "Port of Entry" (terminal name, etc.)
- Overhead: Very low



CORRELOG

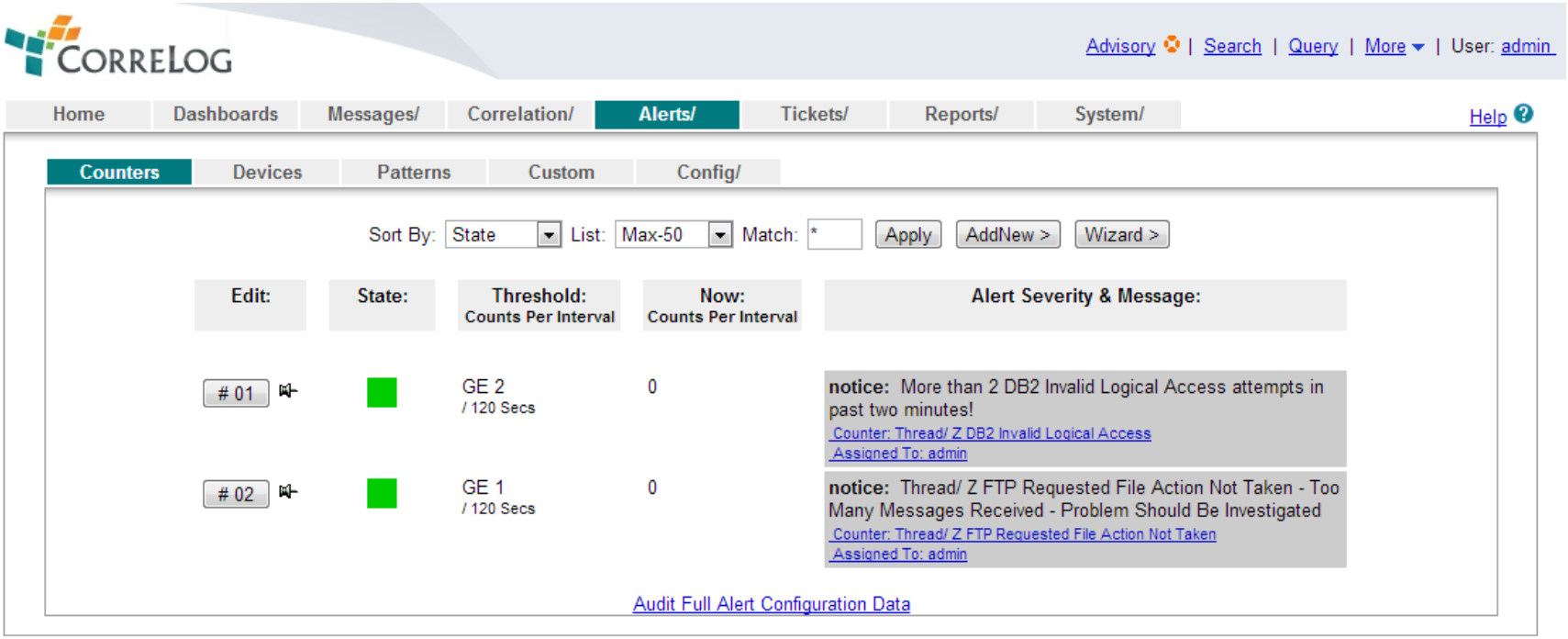
DB2 Reads or Writes of Audited Tables

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



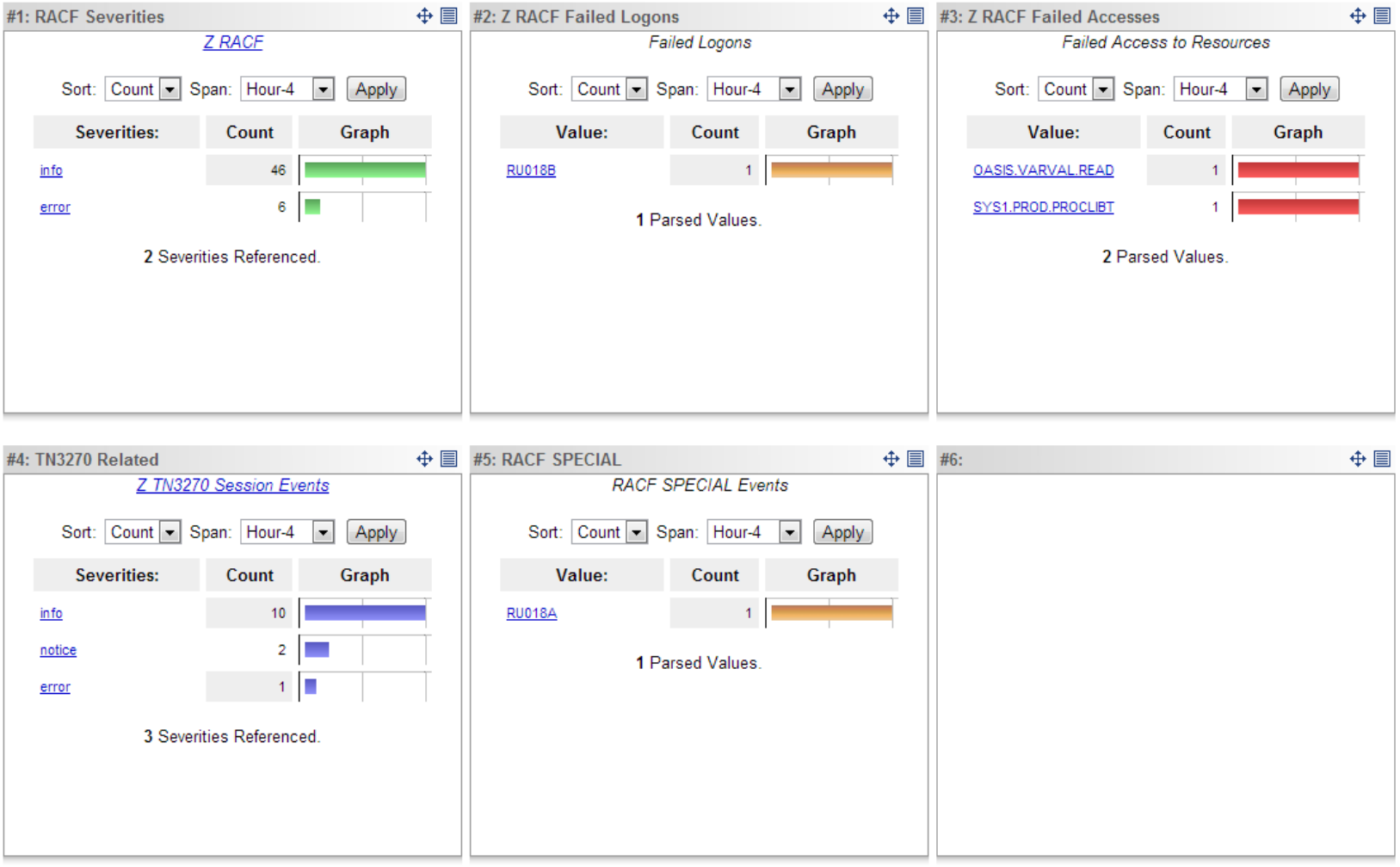
CORRELOG

Alert onEvents by Text or E-Mail



CORRELOG

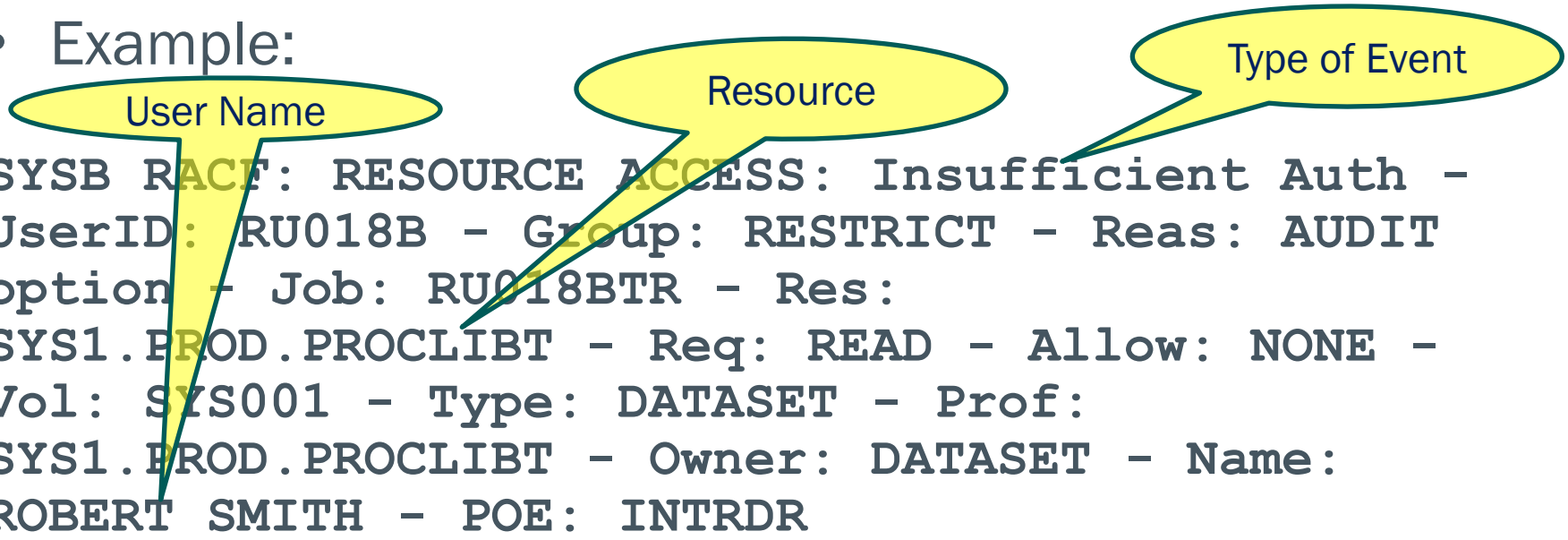
Security Events



CORRELOG

Drill Down to RACF Event Detail

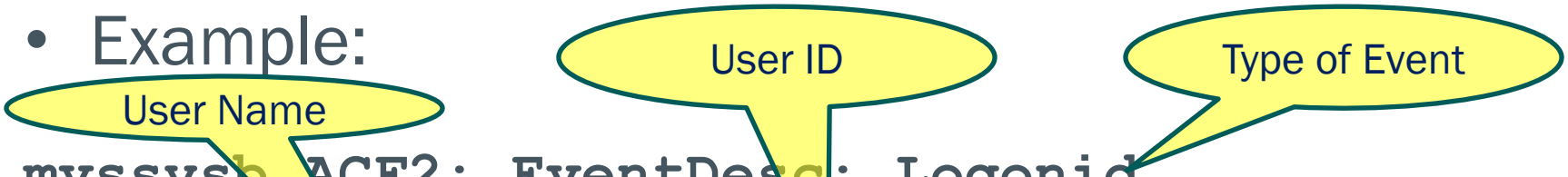
- Compatible with RACF and CA Top Secret
- Expired passwords, revoked user IDs, security configuration changes, unauthorized access attempts, and similar mainframe security events
- Example:



CORRELOG

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:

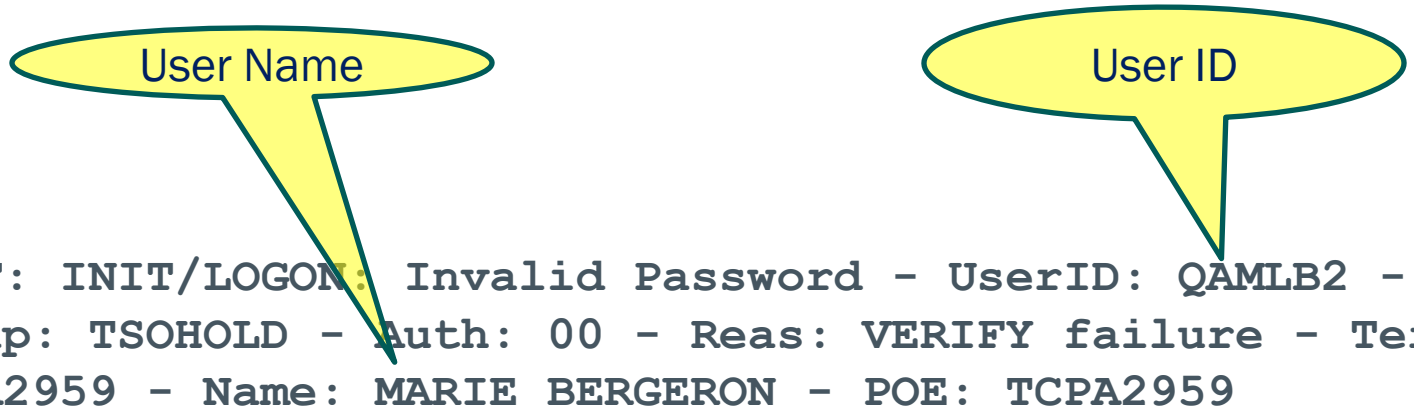



```
mvssysb ACF2: EventDesc: Logonid
modification - ChgDesc: Delete - JobNm:
DECRO01 - UserID: DECRO01 - Pgm: ACF02ALT -
Name: ROSS DECENT - Rel#: 140 - RdrTime:
2012-07-03T16:19:43.880 - ASID: XE34 -
DelTime: 2012-07-03T17:19:51.028 - UID:
OMVSDGRPAAABDECRO01
```

CORRELOG

Audits Failed TSO Logons

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



CORRELOG

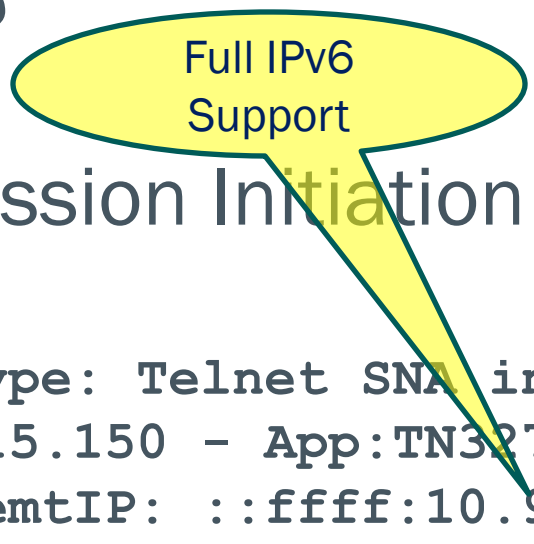
Correlate TSO Access Back to IP Address

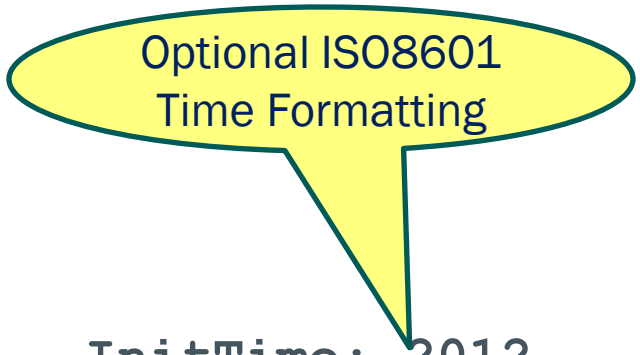
- Failed TSO Access:

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

- 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
```

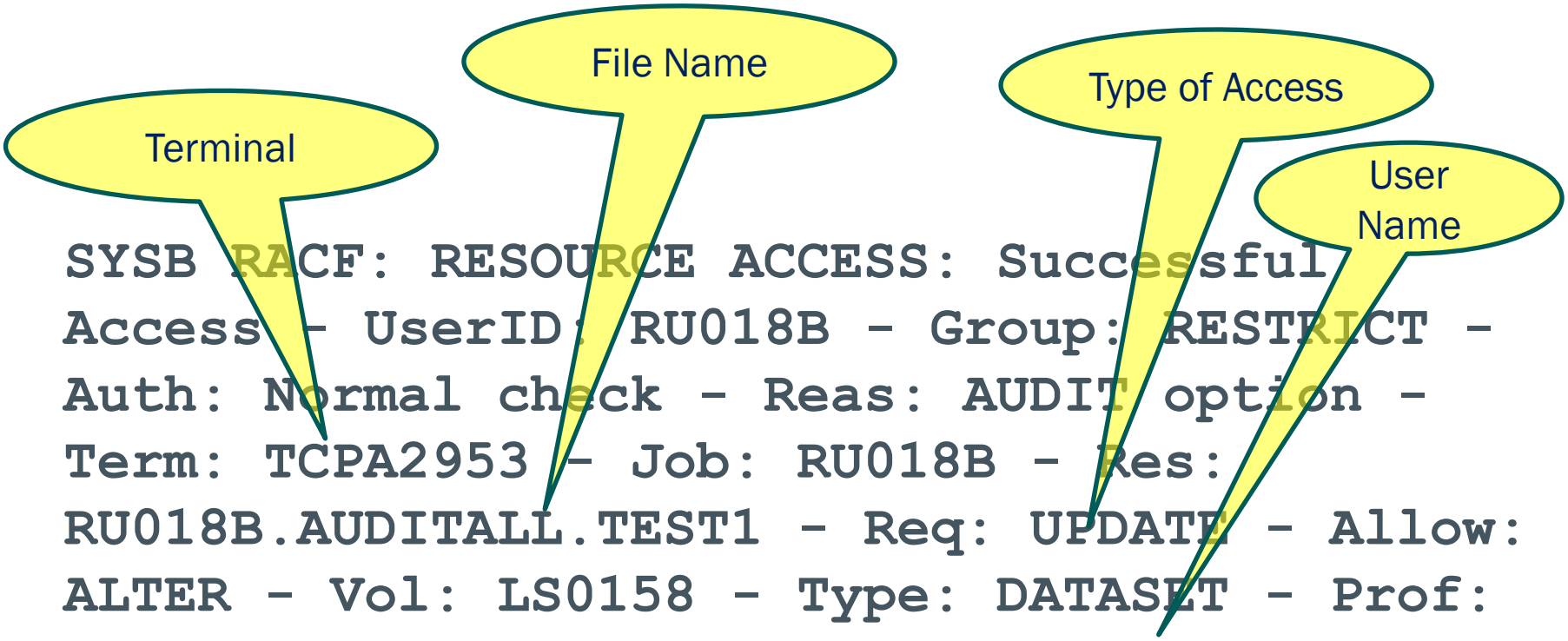




CORRELOG

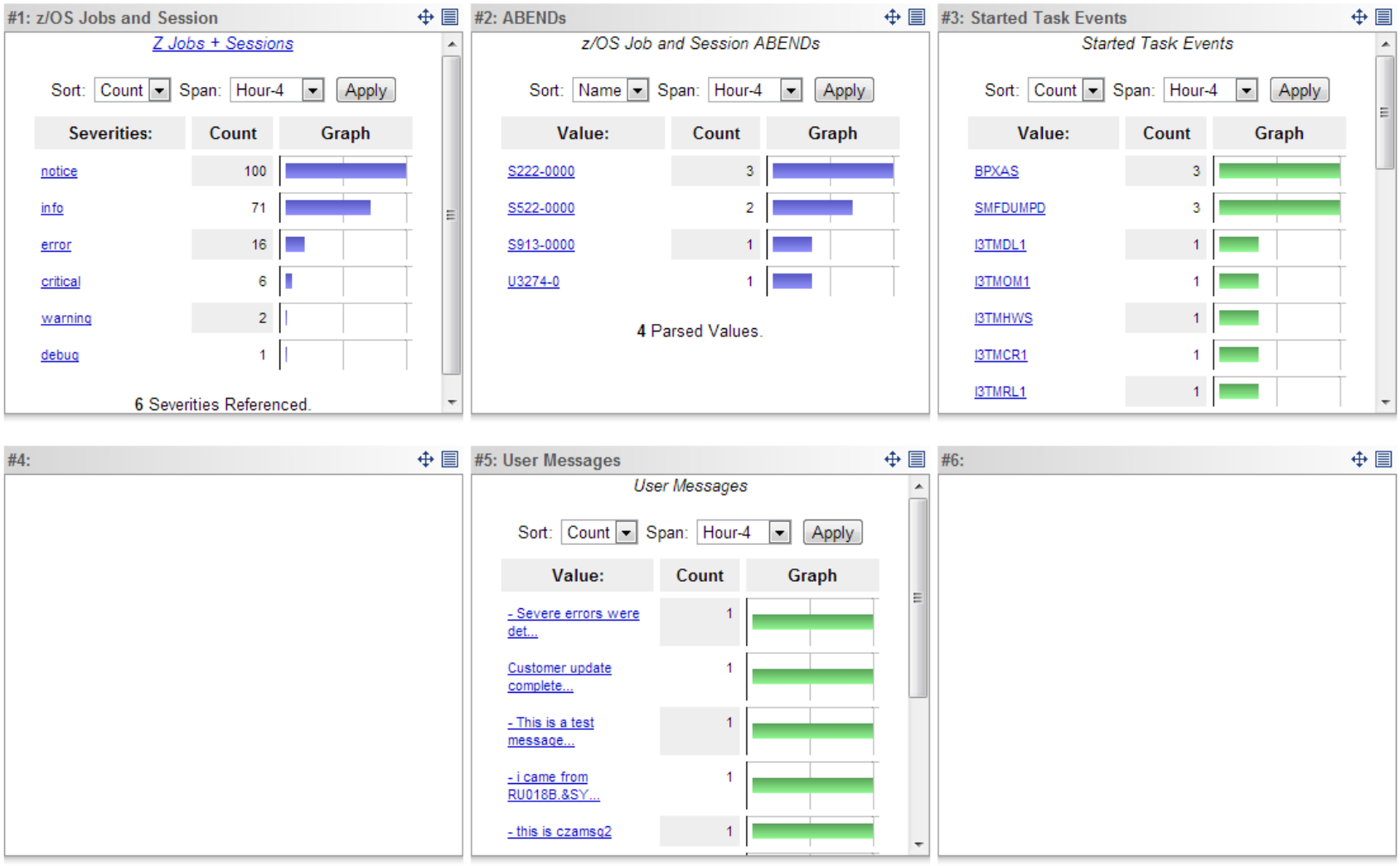
File Integrity Monitoring

- Be alerted to modifications of critical system files



CORRELOG

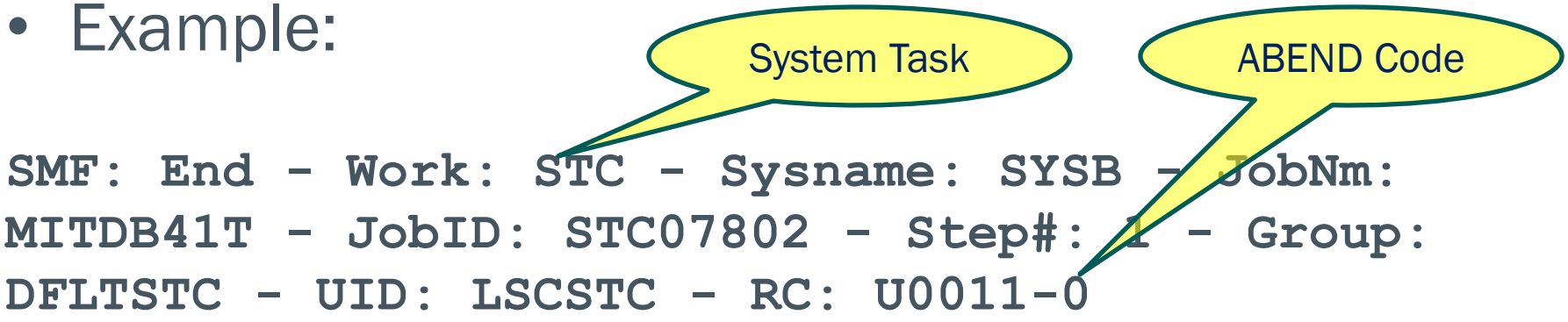
View Job and Started Task Events



CORRELOG

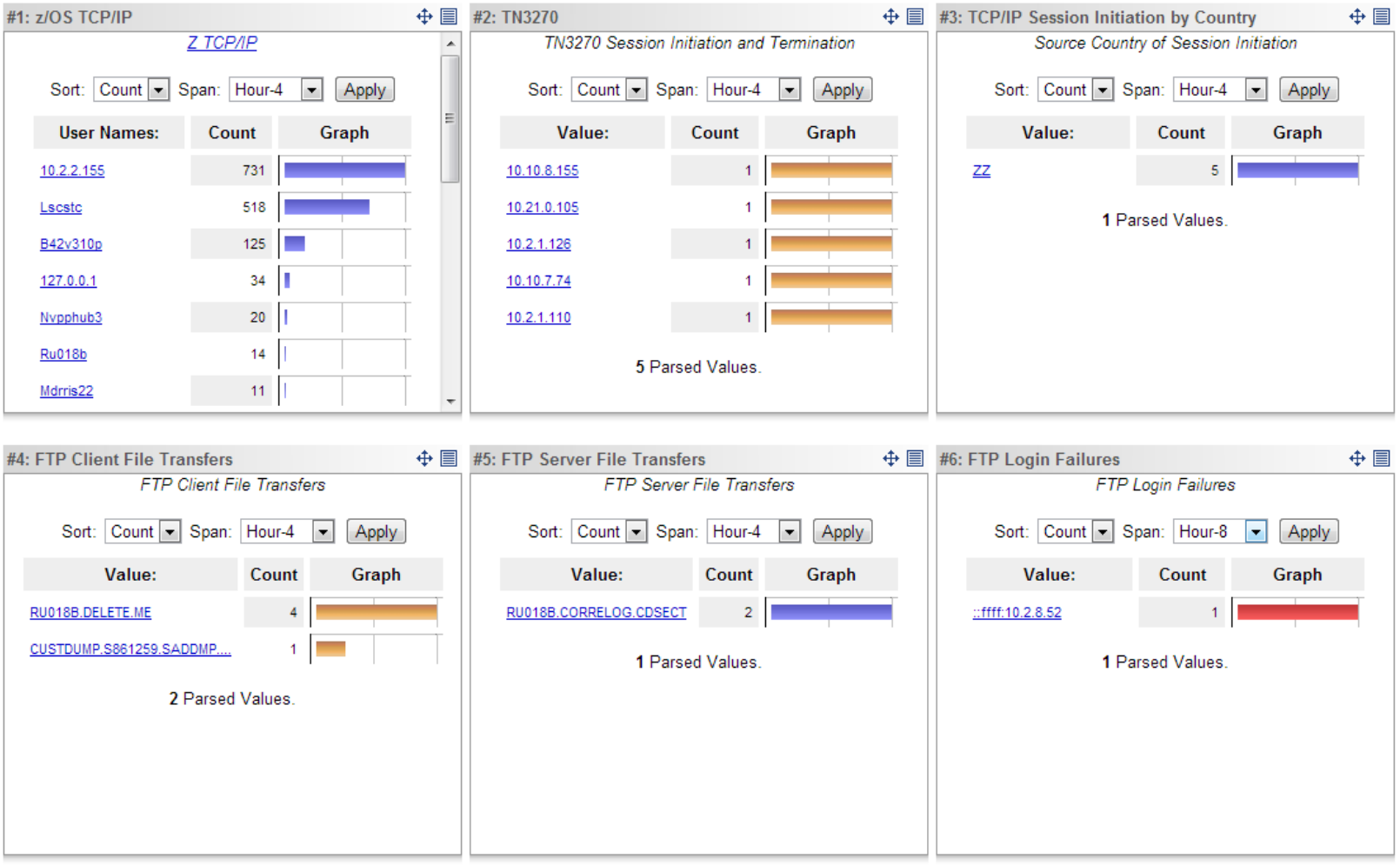
Collects Job Events

- 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:



CORRELOG

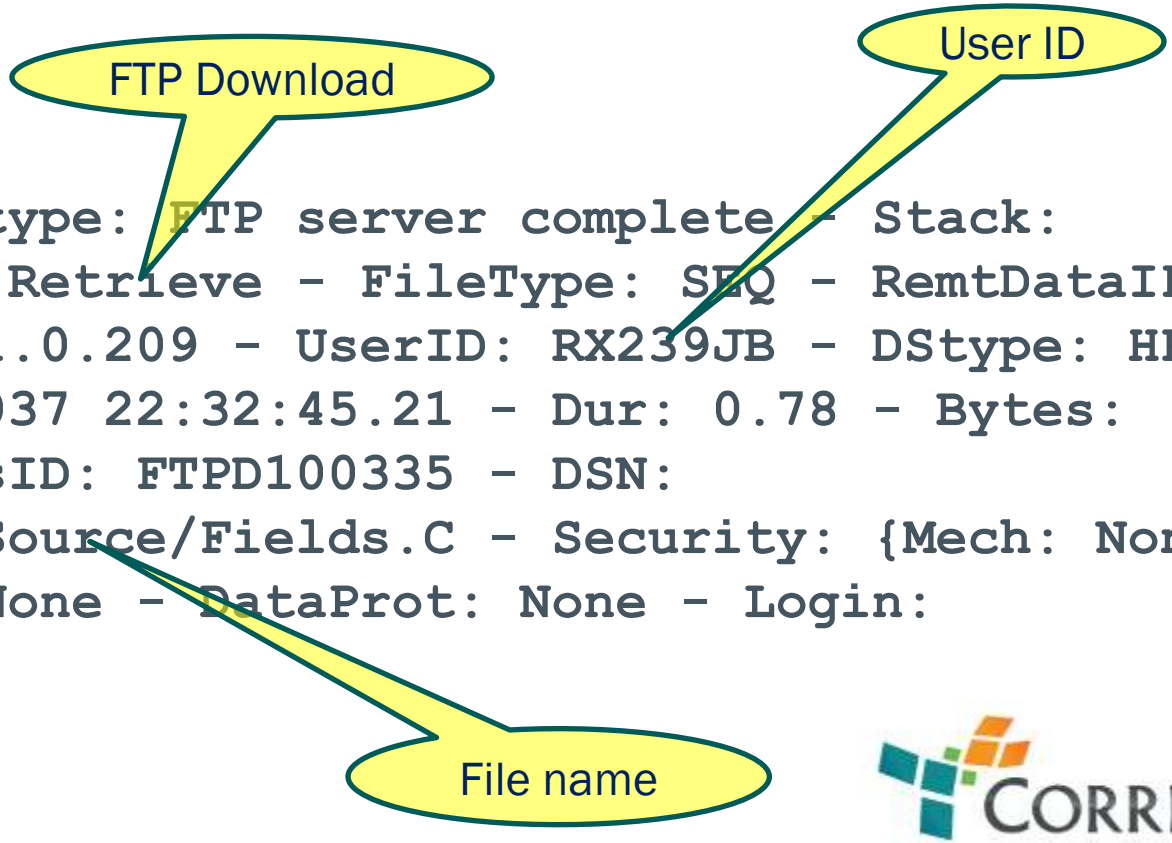
Monitors FTP and TN3270 Logons



CORRELOG

Collects FTP and Other TCP/IP Events

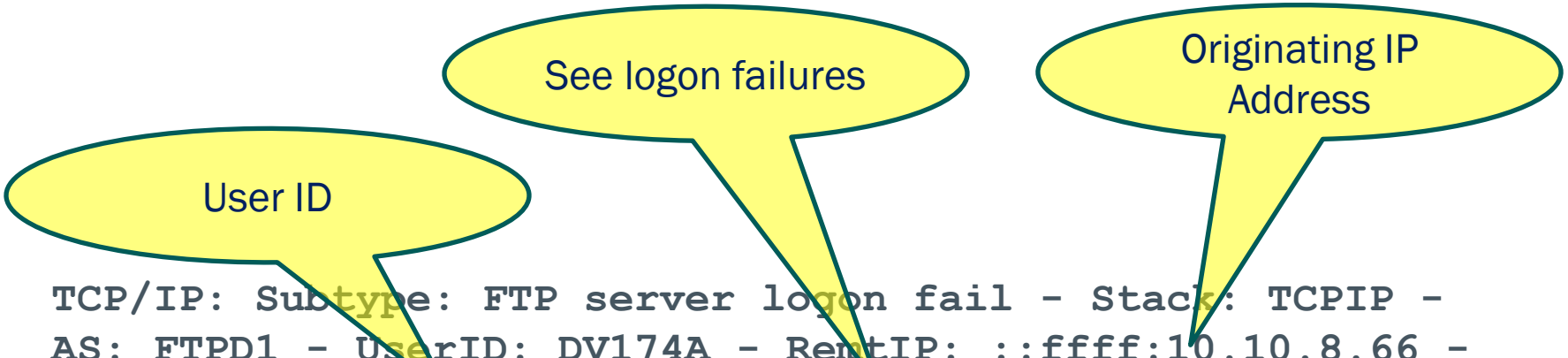
- Logs failed attempts to access FTP
- Audits Successful FTP usage: know who transferred what files and where
- Example:



CORRELOG

Collects Failed FTP Logons

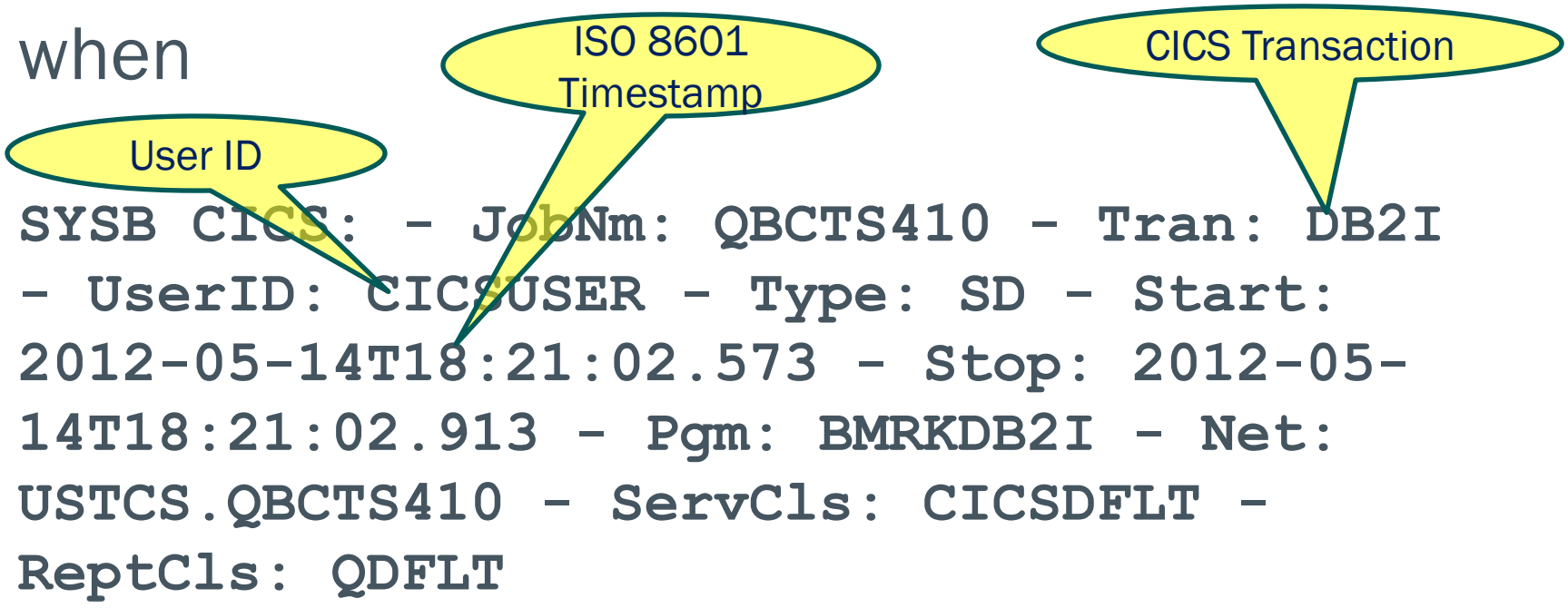
- See who is trying to access your mainframe
- Trace back to originating IP address



CORRELOG

Audits CICS Transactions

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



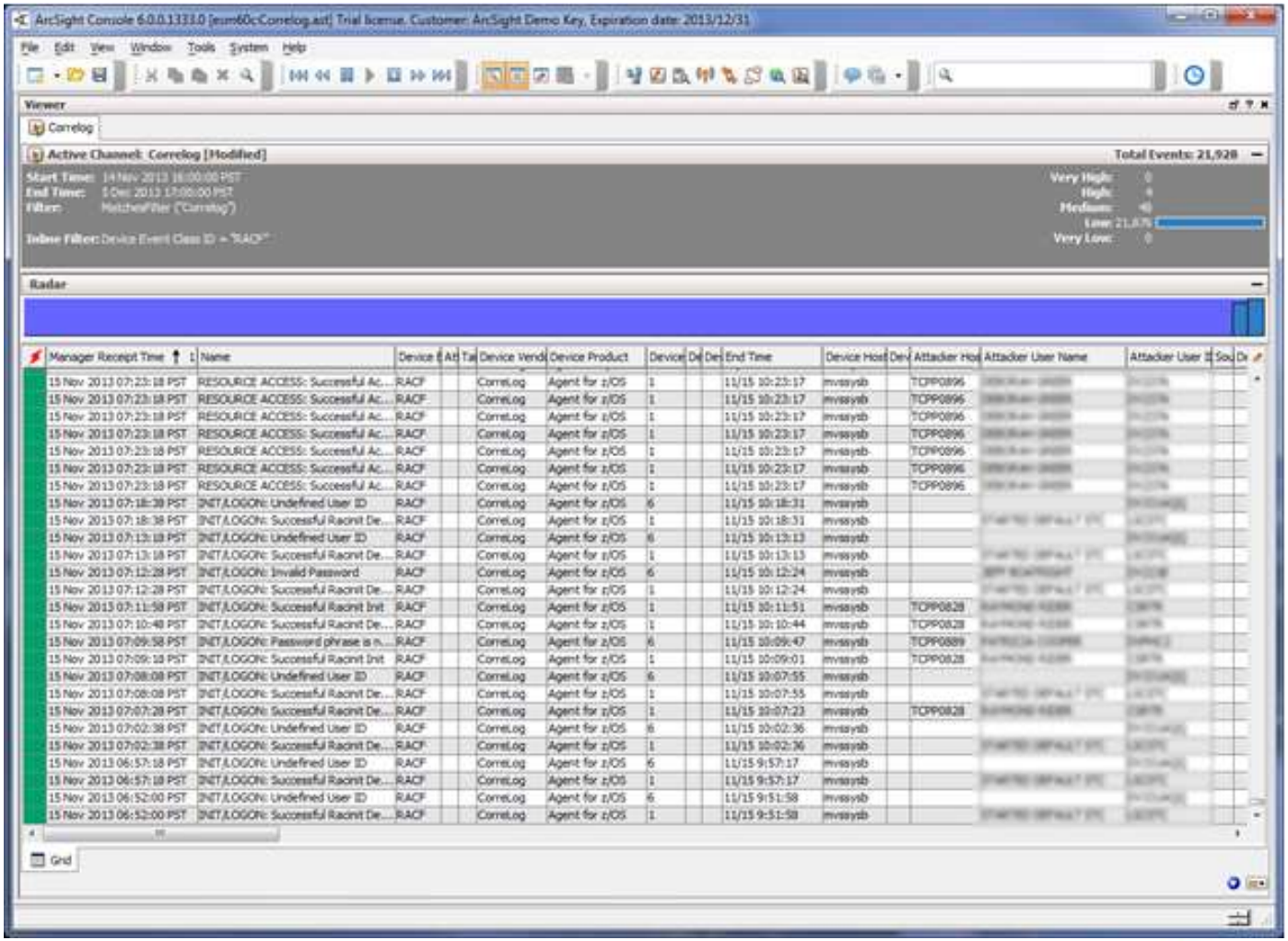
CORRELOG

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

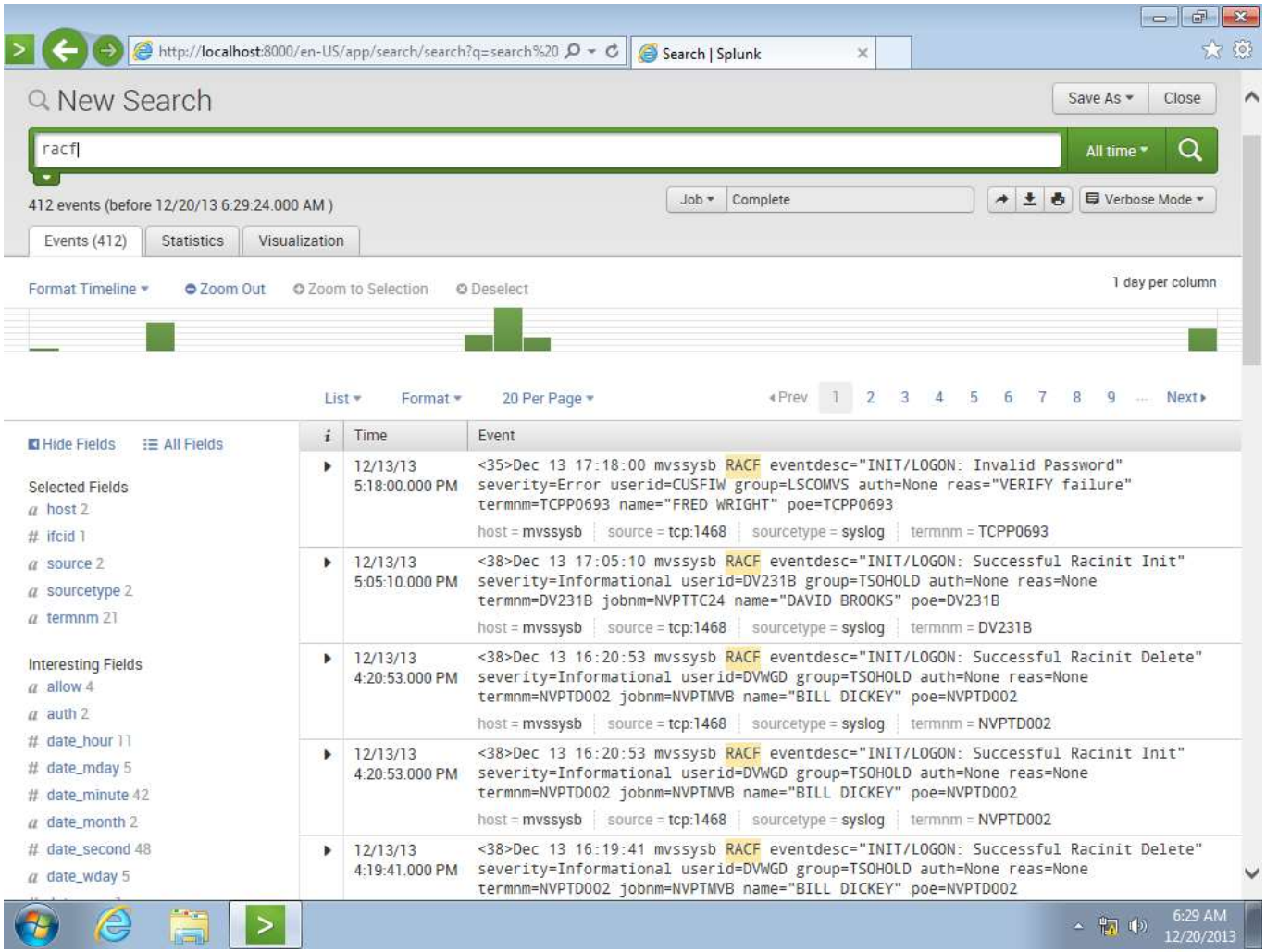
CORRELOG

z/OS Events in ArcSight ESM



CORRELOG

z/OS Events in Splunk



CORRELOG

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

CORRELOG

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

Event Severities

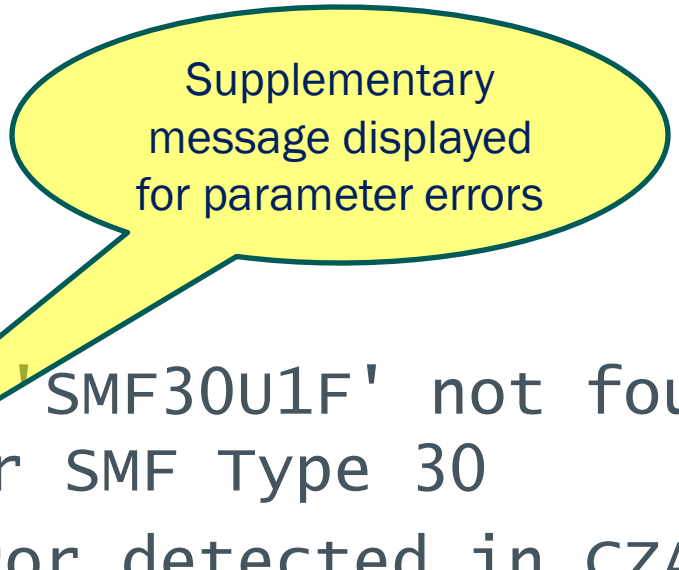
```
SMF 30  TSO(    START(NOTICE)    END(SUPPRESS) )                          +
        STC(    START(SUPPRESS)                                           +
                END( NOTICE      RC4(WARN) RC8(ERROR) ABEND(CRIT) ) )     +
        JOB(    START(SUPPRESS)                                           +
                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 )
```

"INVALID PARAMETER"

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

CORRELOG

Excellent Diagnostic Messages




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

CORRELOG

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

CorreLog Agent for z/OS

QUESTIONS & ANSWERS

Customers


PMA COMPANIES


WHSmith


GLOBAL PROCESSING SYSTEMS


BankServ
International


KDRS
RZRS


Deloitte.


BANK OF THE WEST
BNP PARIBAS GROUP


W&W


UNIVERSAL


MTS allstream


Teneo


National Science Foundation
WHERE DISCOVERIES BEGIN


Ohio.gov
DODD


ROAM DATA™
IMPROVING COMMERCE, IMPROVING LIVES


CITY OF FORT MYERS
2200 SECOND STREET (239) 321-7000
F L O R I D A


BOSTON BALLET
MIKKO NISSINEN ARTISTIC DIRECTOR


Collier County
FLORIDA