www.SecureMyi.com

Forensic Analysis - Using QAUDJRN

Dan Riehl
dan.riehl@SecureMyi.com

IT Security and Compliance Group, LLC

Cilasoft Security Solutions – US Operations

Agenda

- **Examine the current auditing configuration**
- **Determining the availability of audit data**
- **Methods for QAUDJRN extraction - Pros & Cons**
- **Research Examples**
  - Reporting on the use of Sensitive CL Commands
  - Reporting Access to Sensitive Files
  - Reporting System Related Events
  - Reporting for Special Cases

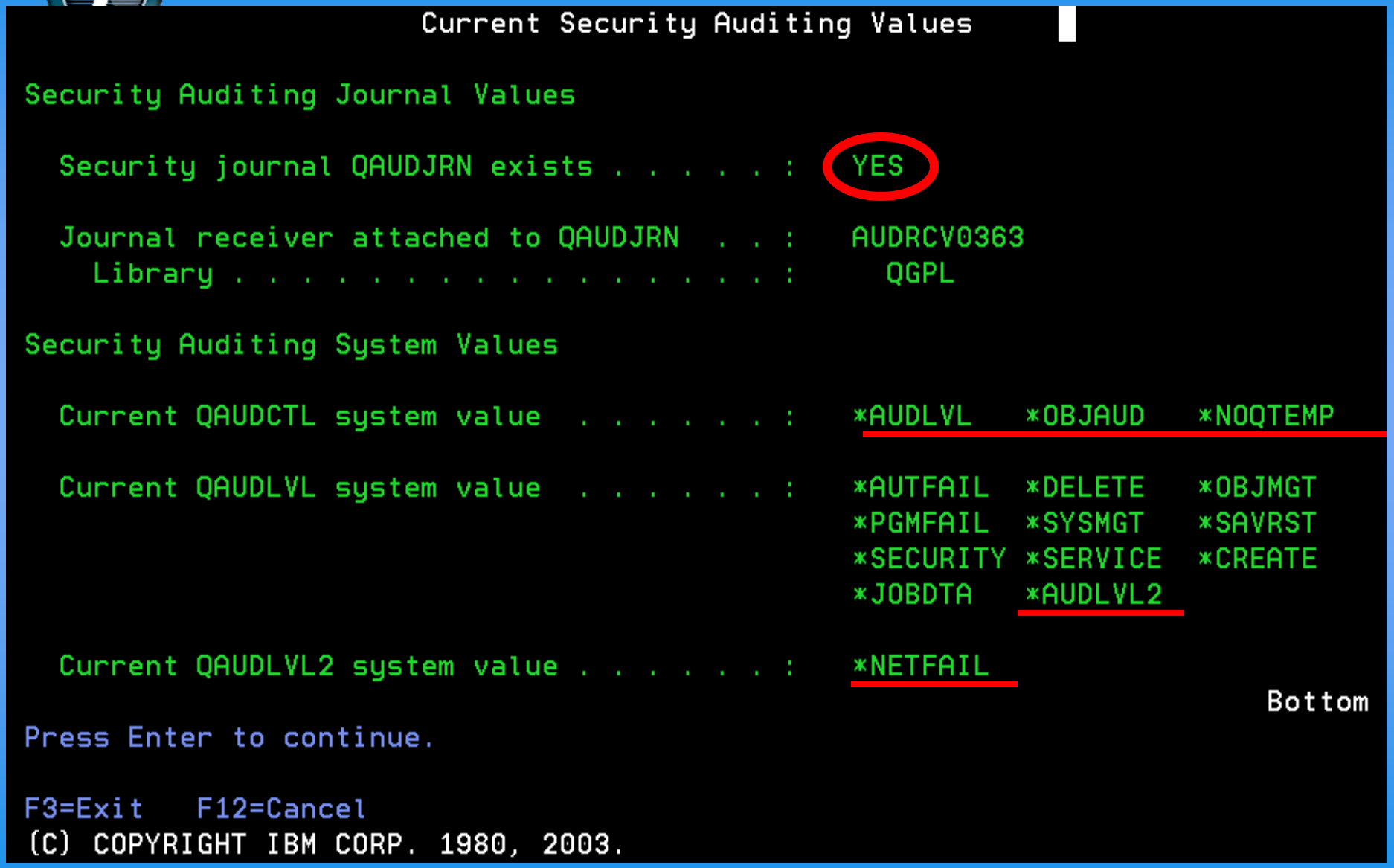
Security Auditing Check-Up

- If you want to inquire into your current security auditing setup, Use the command

DSPSECAUD (Display Security Auditing)

- You must have *ALLOBJ and *AUDIT special authority to run the command.

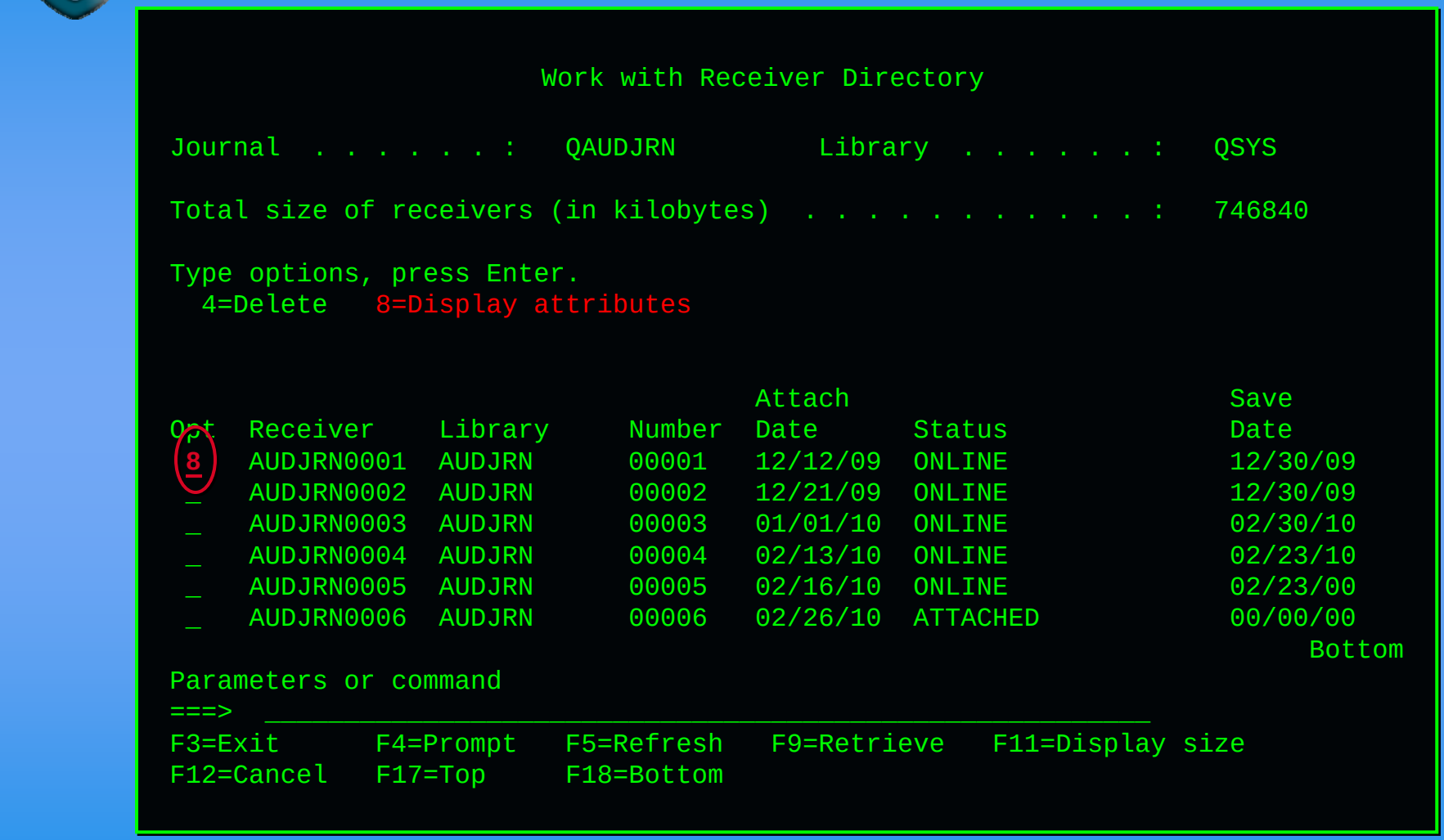
DSPSECAUD Command Display



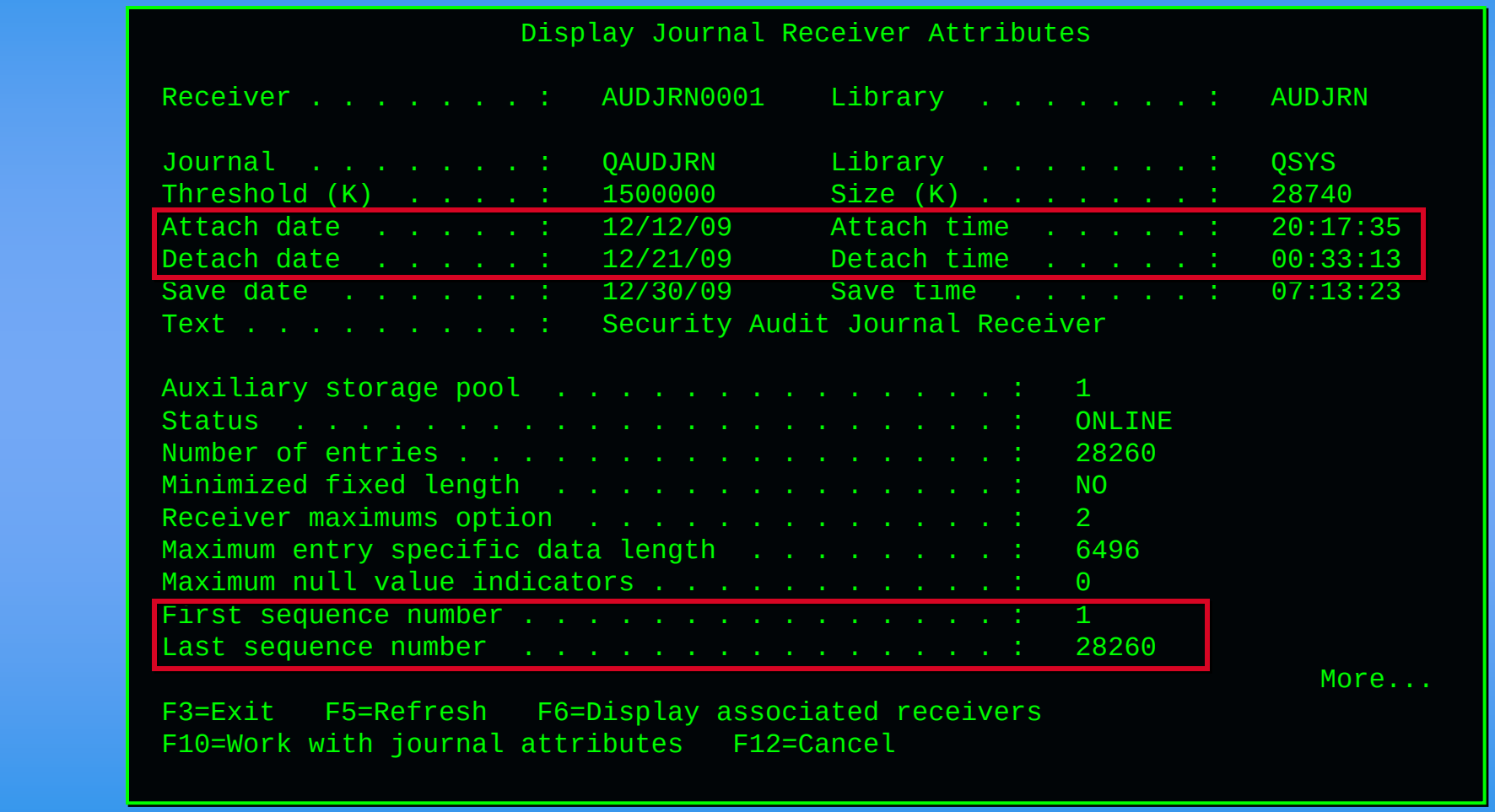
Determining the Availability of Audit Data
Use command WRKJRNA QAUDJRN

```
                        Work with Journal Attributes

Journal  . . . . . :   QAUDJRN         Library  . . . . . :   QSYS

Attached receiver  . :   AUDJRN0006    Library  . . . . . :   AUDJRN

Text . . . . . :   Security Audit Journal

ASP  . . . . . :   1                   Journaled objects:
Message queue  . . . :   QSYSOPR          Current  . . . . . :         6
  Library  . . . . . :     *LIBL          Maximum  . . . . . :    250000
Manage receivers . . :   *SYSTEM        Recovery count . . . :   *SYSDFT
Delete receivers . . :   *NO            Receiver size options:   *RMVINTENT
Journal cache  . . . :   *NO                                     *MAXOPT2
Manage delay . . . . :   10
Delete delay . . . . :   10
Journal type . . . . :   *LOCAL
Journal state  . . . :   *ACTIVE
Minimize entry data  :   *NONE

                                                                    More...
F13=Display journaled files        F14=Display journaled access paths
F15=Work with receiver directory   F24=More keys
```

QAUDJRN Receiver Directory



Attach/Detach Date/Time and Sequence



QAUDJRN Extraction Methods Pros & Cons

- **DSPAUDJRNE (Display Audit Journal Entries)**
  - Quick and Easy
  - Output only to Display or Print
  - No longer updated for new journal entry types
- **CPYAUDJRNE (Copy Audit Journal Entries)**
  - Newer command, but limited selection criteria
  - Output to a fully formatted *OUTFILE
- **DSPJRN (Display Journal)**
  - Maximum Selection Criteria
  - Optional output to a fully formatted *OUTFILE

DSPAUDJRNE (Display Audit Journal Entries)

```
DSPAUDJRNE  ENTTYP(AF)        +
            USRPRF(QSECOFR)   +
            JRNRCV(*CURCHAIN) +
            FROMTIME('04/20/2010' '02:00:00') +
            TOTIME('04/25/2010' '23:59:59')   +
            OUTPUT(*PRINT)
```

"The command does not support all security audit record types, and the command does not list all the fields for the records it does support." (IBM V5R3 Security Reference)

CPYAUDJRNE (Copy Audit Journal Entries)

```
CPYAUDJRNE ENTTYP(AF)
           OUTFILE(MYLIB/OUTFILE) +
           USRPRF(QSECOFR)        +
           JRNRCV(*CURCHAIN)      +
           FROMTIME('04/20/2010' '02:00:00') +
           TOTIME('04/25/2010' '23:59:59')
```

Limited Selection Criteria

Behind the scenes, it uses CRTDUPOBJ and DSPJRN

DSPJRN (Display Journal) *OUTFILE

CRTDUPOBJ OBJ(QASYCDJ5) FROMLIB(QSYS) OBJTYPE(*FILE)
TOLIB(MYWORK) NEWOBJ(CD_MODEL)

```
DSPJRN     JRN(QAUDJRN)      +
           RCVRNG(*CURCHAIN)    +
           FROMENT(*FIRST) TOENT(*LAST)  +
           FROMTIME('04/20/2010' '02:00:00')   +
           TOTIME('04/25/2010' '23:59:59')       +
           JRNCDE((T))      +
           ENTTYP(CD)      +
           JOB(QZDASOINIT)     +
           PGM(QZDASOINIT)    +
           USRPRF(QSECOFR)   +
           OUTPUT(*OUTFILE)    +
           OUTFILFMT(*TYPE5)   +
           OUTFILE(MYWORK/CD_MODEL)    (This File already exists!)
```

Allows for maximum selection criteria
Output to fully formatted *OUTFILE

QASYCDJ5 – Common Entry Data

Field Text	Field Name	Type	Length	Dec	Loc
Length of entry	CDENTL	S	5	0	1
Sequence number	CDSEQN	A	20		6
Journal code	CDCODE	A	1		26
Entry type	CDENTT	A	2		27
Timestamp of entry	CDTSTP	Z	26		29
Name of job	CDJOB	A	10		55
Name of user	CDUSER	A	10		65
Number of job	CDNBR	S	6	0	75
Name of program	CDPGM	A	10		81
Program library	CDPGMLIB	A	10		91
Program Asp device	CDPGMDEV	A	10		101
Program Asp number	CDPGMASP	S	5	0	111
Not used	CDRES1	A	71		116
User profile	CDUSPF	A	10		187
System name	CDSYNM	A	8		197
Not used	CDRES2	A	16		205
System sequence	CDSYSSEQ	A	20		221
Receiver	CDRCV	A	10		241
Receiver Library	CDRCVLIB	A	10		251
Receiver Asp device	CDRCVDEV	A	10		261
Receiver Asp number	CDRCVASP	S	5	0	271
Arm number	CDARM	S	5	0	276
Thread identifier	CDTHREAD	A	8		281
Thread Id hex	CDTHRDHX	A	16		289
Address family	CDADF	A	1		305
Remote port	CDRPORT	S	5	0	306
Remote address (IP Address)	CDRADR	A	46		311
Not used	CDRESA	A	249		357
Length of specific data	CDESDL	B	10	0	606

QASYCDJ5 – Formatted Entry Specific Data

Field Text	Field Name	Type	Length	Dec	Loc
Type of entry	CDETYP	A	1		610
Command name	CDONAM	A	10		611
Command Library name	CDOLIB	A	10		621
Object type	CDOTYP	A	8		631
Y - Command run from CL Pgm?	CDCLP	A	1		639
Entire Command string	CDCMDS	A	6000		640
Asp name for command library	CDASP	A	10		6640
Asp number for command library	CDASPN	A	5		6650

Standard method used – Avoid this method

```
DSPJRN JRN(QAUDJRN) RCVRNG(*CURRENT)
       JRNCDE((T)) ENTTYP(CD) OUTPUT(*OUTFILE)
       OUTFILFMT(*TYPE5)
       OUTFILE(MYLIB/CDENTRIES)
       OUTMBR(*FIRST *REPLACE)
```

- In this example the Output file CDENTRIES is created as an *OUTFILE by the DSPJRN command. It does not exist prior to DSPJRN command execution.
- Gives Common Header fields, but then gives unformatted field JOESD(Entry Specific Data)

Forensic Analysis - Research Examples

- **Reporting on the the use of Sensitive CL Commands**
  - All CL Commands Run by QSECOFR
  - Every use of the CRTLIB Command
- **Reporting access to Sensitive Files**
  - All IT access to the sensitive CREDITCARD file (Read /Update)
  - All access to sensitive files via ODBC (Read / Update)
- **Reporting System Related Events**
  - Changes to System Values
  - Reporting On Deleted Objects (Who? When? Where? How?)
- **Reporting for Special cases**
  - Changes made to the i/OS Job Scheduler
  - Changes made to the i/OS Exit Program Registry (WRKREGINF)

Auditing Sensitive CL Commands

- **Start auditing every CL command run by QSECOFR**
  - To begin auditing CL command usage by a particular user, you use the CHGUSRAUD (Change User Auditing) command.

```
CHGUSRAUD  USRPRF(QSECOFR) AUDLVL(*CMD)
```

- **Start auditing all use of the Command CRTLIB(Create Library)**
  - When you want to audit the usage of a particular CL command, use the command CHGOBJAUD (Change Object Auditing).

```
CHGOBJAUD OBJ(QSYS/CRTLIB) OBJTYPE(*CMD) OBJAUD(*ALL)
```

- **When an audited command is used, a journal entry type CD is written to QAUDJRN**

Extracting Command Usage from QAUDJRN

- 1) Create a duplicate of the IBM supplied *TYPE5 model *OUTFILE for CD entries, use the command.

```
CRTDUPOBJ  OBJ(QASYCDJ5) FROMLIB(QSYS) OBJTYPE(*FILE)
           TOLIB(MYLIB) NEWOBJ(CD_MODEL)
```

- 2) Run the DSPJRN command, and specify *TYPE5 and the name of your copy of the IBM model *OUTFILE.

```
DSPJRN JRN(QAUDJRN) RCVRNG(*CURRENT) JRNCDE((T)) ENTTYP(CD)
       USRPRF(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE5)
       OUTFILE(MYLIB/CD_MODEL) OUTMBR(*FIRST *REPLACE)
```

- When you are using the IBM supplied model outfile QASYCDJ5, all the data fields are already parsed out for you from the JOESD, so your reporting facility does not have to do the parsing work.

QASYCDJ5 – Common Entry Data

Field Text	Field Name	Type	Length	Dec	Loc
Length of entry	CDENTL	S	5	0	1
Sequence number	CDSEQN	A	20		6
Journal code	CDCODE	A	1		26
Entry type	CDENTT	A	2		27
Timestamp of entry	CDTSTP	Z	26		29
Name of job	CDJOB	A	10		55
Name of user	CDUSER	A	10		65
Number of job	CDNBR	S	6	0	75
Name of program	CDPGM	A	10		81
Program library	CDPGMLIB	A	10		91
Program Asp device	CDPGMDEV	A	10		101
Program Asp number	CDPGMASP	S	5	0	111
Not used	CDRES1	A	71		116
User profile	CDUSPF	A	10		187
System name	CDSYNM	A	8		197
Not used	CDRES2	A	16		205
System sequence	CDSYSSEQ	A	20		221
Receiver	CDRCV	A	10		241
Receiver Library	CDRCVLIB	A	10		251
Receiver Asp device	CDRCVDEV	A	10		261
Receiver Asp number	CDRCVASP	S	5	0	271
Arm number	CDARM	S	5	0	276
Thread identifier	CDTHREAD	A	8		281
Thread Id hex	CDTHRDHX	A	16		289
Address family	CDADF	A	1		305
Remote port	CDRPORT	S	5	0	306
Remote address	CDRADR	A	46		311
Not used	CDRESA	A	249		357
Length of specific data	CDESDL	B	10	0	606

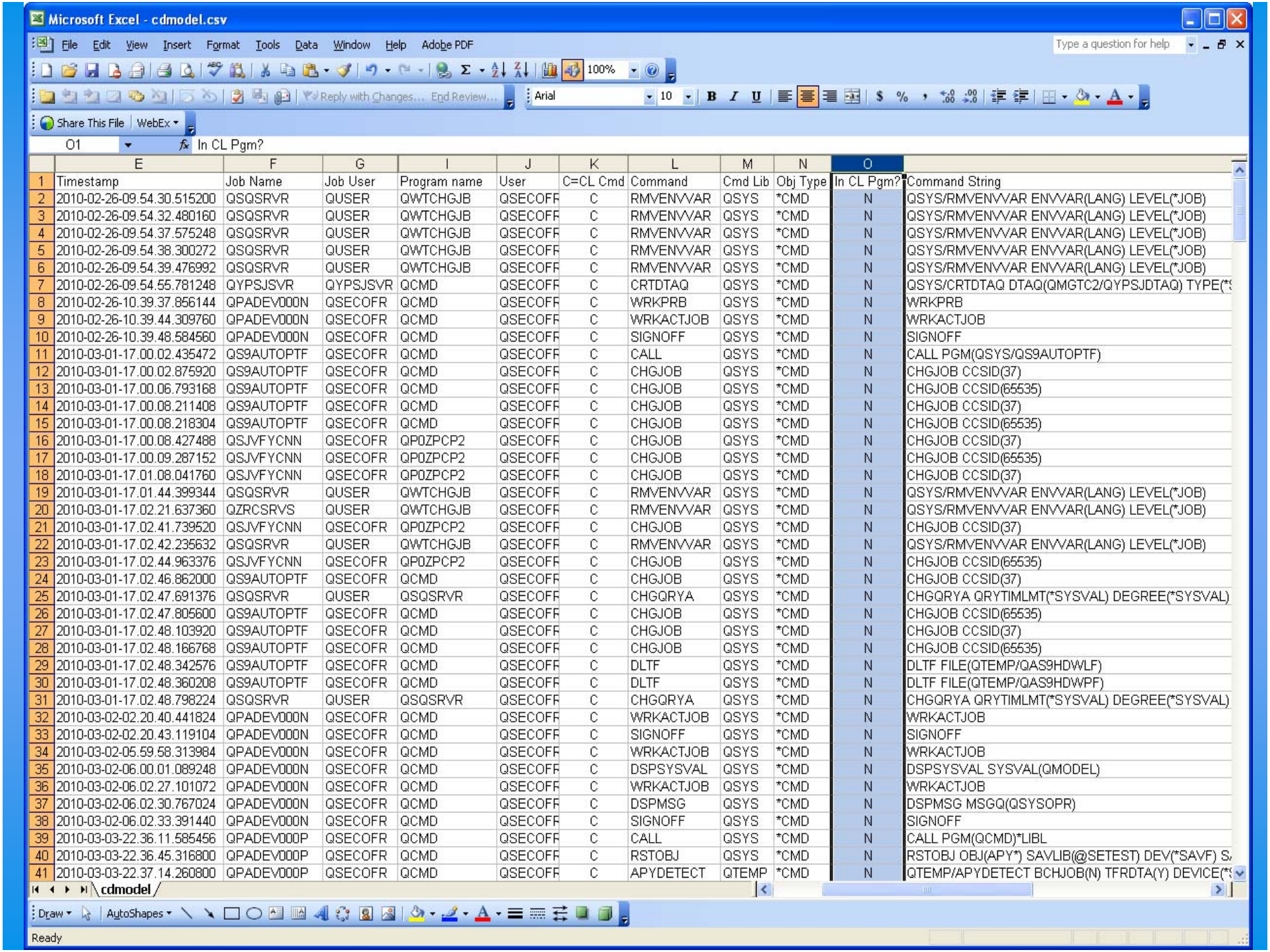
This is the Common Header for all Entry Types, But the Prefix changes from CD

QASYCDJ5 – Entry Specific Data

Field Text	Field Name	Type	Length	Dec	Loc
Type of entry	CDETYP	A	1		610
Value Meaning C CL Command run L OCL statement O Operator control command P S/36 procedure S Command run after command substitution took place U Utility Control Statement					
Command name (Always Here)	CDONAM	A	10		611
Command Library name	CDOLIB	A	10		621
Object type	CDOTYP	A	8		631
Y - Command run from CL Pgm?	CDCLP	A	1		639
Value Meaning Y Command run from CL Program N Command NOT run from CL Program (Command line/QCMDEXC, etc)					
Entire Command string	CDCMDS	A	6000		640
This field will not be available when the command is run from a program that specifies RTVCLSRC(*NO), or does not have observability intact.					
Asp name for command library	CDASP	A	10		6640
Asp number for command library	CDASPN	A	5		6650

Now that I have my *OUTFILE, What next?

- Use Query (Select records, format output)
- Use SQL Select
- Download to Excel (Slice and Dice)



	E	F	G	I	J	K	L	M	N	O	
1	Timestamp	Job Name	Job User	Program name	User	C=CL Cmd	Command	Cmd Lib	Obj Type	In CL Pgm?	Command String
2	2010-02-26-09.54.30.515200	QSQSRVR	QUSER	QWTCHGJB	QSECOFR	C	RMVENVVAR	QSYS	*CMD	N	QSYS/RMVENVVAR ENVVAR(LANG) LEVEL(*JOB)
3	2010-02-26-09.54.32.480160	QSQSRVR	QUSER	QWTCHGJB	QSECOFR	C	RMVENVVAR	QSYS	*CMD	N	QSYS/RMVENVVAR ENVVAR(LANG) LEVEL(*JOB)
4	2010-02-26-09.54.37.575248	QSQSRVR	QUSER	QWTCHGJB	QSECOFR	C	RMVENVVAR	QSYS	*CMD	N	QSYS/RMVENVVAR ENVVAR(LANG) LEVEL(*JOB)
5	2010-02-26-09.54.38.300272	QSQSRVR	QUSER	QWTCHGJB	QSECOFR	C	RMVENVVAR	QSYS	*CMD	N	QSYS/RMVENVVAR ENVVAR(LANG) LEVEL(*JOB)
6	2010-02-26-09.54.39.476992	QSQSRVR	QUSER	QWTCHGJB	QSECOFR	C	RMVENVVAR	QSYS	*CMD	N	QSYS/RMVENVVAR ENVVAR(LANG) LEVEL(*JOB)
7	2010-02-26-09.54.55.781248	QYPSJSVR	QYPSJSVR	QCMD	QSECOFR	C	CRTDTAQ	QSYS	*CMD	N	QSYS/CRTDTAQ DTAQ(QMGTC2/QYPSJDTAQ) TYPE(*S
8	2010-02-26-10.39.37.856144	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	WRKPRB	QSYS	*CMD	N	WRKPRB
9	2010-02-26-10.39.44.309760	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	WRKACTJOB	QSYS	*CMD	N	WRKACTJOB
10	2010-02-26-10.39.48.584560	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	SIGNOFF	QSYS	*CMD	N	SIGNOFF
11	2010-03-01-17.00.02.435472	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	CALL	QSYS	*CMD	N	CALL PGM(QSYS/QS9AUTOPTF)
12	2010-03-01-17.00.02.875920	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(37)
13	2010-03-01-17.00.06.793168	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(65535)
14	2010-03-01-17.00.08.211408	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(37)
15	2010-03-01-17.00.08.218304	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(65535)
16	2010-03-01-17.00.08.427488	QSJVFYCNN	QSECOFR	QP0ZPCP2	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(37)
17	2010-03-01-17.00.09.287152	QSJVFYCNN	QSECOFR	QP0ZPCP2	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(65535)
18	2010-03-01-17.01.08.041760	QSJVFYCNN	QSECOFR	QP0ZPCP2	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(37)
19	2010-03-01-17.01.44.399344	QSQSRVR	QUSER	QWTCHGJB	QSECOFR	C	RMVENVVAR	QSYS	*CMD	N	QSYS/RMVENVVAR ENVVAR(LANG) LEVEL(*JOB)
20	2010-03-01-17.02.21.637360	QZRCSRVS	QUSER	QWTCHGJB	QSECOFR	C	RMVENVVAR	QSYS	*CMD	N	QSYS/RMVENVVAR ENVVAR(LANG) LEVEL(*JOB)
21	2010-03-01-17.02.41.739520	QSJVFYCNN	QSECOFR	QP0ZPCP2	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(37)
22	2010-03-01-17.02.42.235632	QSQSRVR	QUSER	QWTCHGJB	QSECOFR	C	RMVENVVAR	QSYS	*CMD	N	QSYS/RMVENVVAR ENVVAR(LANG) LEVEL(*JOB)
23	2010-03-01-17.02.44.963376	QSJVFYCNN	QSECOFR	QP0ZPCP2	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(65535)
24	2010-03-01-17.02.46.862000	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(37)
25	2010-03-01-17.02.47.691376	QSQSRVR	QUSER	QSQSRVR	QSECOFR	C	CHGQRYA	QSYS	*CMD	N	CHGQRYA QRYTIMLMT(*SYSVAL) DEGREE(*SYSVAL)
26	2010-03-01-17.02.47.805600	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(65535)
27	2010-03-01-17.02.48.103920	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(37)
28	2010-03-01-17.02.48.166768	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	CHGJOB	QSYS	*CMD	N	CHGJOB CCSID(65535)
29	2010-03-01-17.02.48.342576	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	DLTF	QSYS	*CMD	N	DLTF FILE(QTEMP/QAS9HDWLF)
30	2010-03-01-17.02.48.360208	QS9AUTOPTF	QSECOFR	QCMD	QSECOFR	C	DLTF	QSYS	*CMD	N	DLTF FILE(QTEMP/QAS9HDWPF)
31	2010-03-01-17.02.48.798224	QSQSRVR	QUSER	QSQSRVR	QSECOFR	C	CHGQRYA	QSYS	*CMD	N	CHGQRYA QRYTIMLMT(*SYSVAL) DEGREE(*SYSVAL)
32	2010-03-02-02.20.40.441824	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	WRKACTJOB	QSYS	*CMD	N	WRKACTJOB
33	2010-03-02-02.20.43.119104	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	SIGNOFF	QSYS	*CMD	N	SIGNOFF
34	2010-03-02-05.59.58.313984	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	WRKACTJOB	QSYS	*CMD	N	WRKACTJOB
35	2010-03-02-06.00.01.089248	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	DSPSYSVAL	QSYS	*CMD	N	DSPSYSVAL SYSVAL(QMODEL)
36	2010-03-02-06.02.27.101072	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	WRKACTJOB	QSYS	*CMD	N	WRKACTJOB
37	2010-03-02-06.02.30.767024	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	DSPMSG	QSYS	*CMD	N	DSPMSG MSGQ(QSYSOPR)
38	2010-03-02-06.02.33.391440	QPADEV000N	QSECOFR	QCMD	QSECOFR	C	SIGNOFF	QSYS	*CMD	N	SIGNOFF
39	2010-03-03-22.36.11.585456	QPADEV000P	QSECOFR	QCMD	QSECOFR	C	CALL	QSYS	*CMD	N	CALL PGM(QCMD)*LIBL
40	2010-03-03-22.36.45.316800	QPADEV000P	QSECOFR	QCMD	QSECOFR	C	RSTOBJ	QSYS	*CMD	N	RSTOBJ OBJ(APY*) SAVLIB(@SETEST) DEV(*SAVF) S/
41	2010-03-03-22.37.14.260800	QPADEV000P	QSECOFR	QCMD	QSECOFR	C	APYDETECT	QTEMP	*CMD	N	QTEMP/APYDETECT BCHJOB(N) TFRDTA(Y) DEVICE(*S

Reporting Access to Sensitive Files?

- Operations for File (*FILE): (PF-DTA and LF)
  - Access or Open for Input operation (Entry Type **ZR)**
  - Access or Open for Update operation (Entry Type **ZC**)

  - **To record All access to a Sensitive File (ZR and ZC)**

```
CHGOBJAUD OBJ(SECLIB/CREDITCARD) OBJTYPE(*FILE) OBJAUD(*ALL)
```

  - **To record only Update Access to a Sensitive File (ZC Only)**

```
CHGOBJAUD OBJ(SECLIB/CREDITCARD) OBJTYPE(*FILE) OBJAUD(*CHANGE)
```

QAUDCTL System Value must include *OBJAUD

Extracting Read-Only Access to CREDITCARD File

- 1) Create a duplicate of the IBM supplied model *OUTFILE for ZR entries, use the command.

```
CRTDUPOBJ  OBJ(QASYZRJ5) FROMLIB(QSYS) OBJTYPE(*FILE)
           TOLIB(MYLIB) NEWOBJ(ZR_MODEL)
```

- 2) Run the DSPJRN command, and specify *TYPE5 and the name of your copy of the IBM model *outfile.

```
DSPJRN JRN(QAUDJRN) RCVRNG(*CURRENT) JRNCDE((T))
       ENTTYP(ZR) USRPRF(*ALL) OUTPUT(*OUTFILE)
       OUTFILFMT(*TYPE5)
       OUTFILE(MYLIB/ZR_MODEL) OUTMBR(*FIRST *REPLACE)
```

- Cannot specifically limit to CREDITCARD file, Selection required.

Extracting Update Access to CREDITCARD File

- 1) Create a duplicate of the IBM supplied model *outfile for ZC entries, use the command.

```
CRTDUPOBJ  OBJ(QASYZCJ5) FROMLIB(QSYS) OBJTYPE(*FILE)
           TOLIB(MYLIB) NEWOBJ(ZC_MODEL)
```

- 2) Run the DSPJRN command, and specify *TYPE5 and the name of your copy of the IBM model *outfile.

```
DSPJRN JRN(QAUDJRN) RCVRNG(*CURRENT) JRNCDE((T))
       ENTTYP(ZC) USRPRF(*ALL) OUTPUT(*OUTFILE)
       OUTFILFMT(*TYPE5)
       OUTFILE(MYLIB/ZC_MODEL) OUTMBR(*FIRST *REPLACE)
```

- Cannot specifically limit to CREDITCARD file, Selection required.

Fields of Interest for ZC and ZR entries

- ZR/ZCONAM - The File/Object name that was accessed
- ZR/ZCOLIB - The Library name which contains the object
- ZR/ZCOTYP - The Object type that was accessed (*FILE)
- ZR/ZCOPGM - The program used to access the object
- ZR/ZCOPGMLIB - The library of the program used
- ZR/ZCJOB - The Job Name that accessed the object
- ZR/ZCUSPF - The current user profile used to access the object

To report access by just the IT group,
You need to perform record selection,
or join the *OUTFILE to a file of selected
IT user names.

Join using the column ZR/ZCUSPF, NOT the Job User.

Selected Entry Specific Data for ZR and ZC Entries

ZRONAM/ZCONAM	CHAR		10	10	611	Both	Object Name
ZROLIB/ZCOLIB	CHAR		10	10	621	Both	Library Name
ZROTYP/ZCOTYP	CHAR		8	8	631	Both	Object Type
ZRACTP/ZCACTP	PACKED	5	0	3	639	Both	Access Type

- Access Type Codes

Code	Access type
1	Add
2	Activate Program
3	Analyze
4	Apply
5	Call or TFRCTL
6	Configure
7	Change
8	Check
9	Close
10	Clear
11	Compare
12	Cancel
13	Copy
14	Create
15	Convert
16	Debug
17	Delete
18	Dump
19	Display
20	Edit
21	End
22	File
23	Grant
24	Hold
25	Initialize
26	Load
27	List
28	Move
29	Merge
30	Open
31	Print
32	Query
33	Reclaim
34	Receive
35	Read
36	Reorganize
37	Release
38	Remove
39	Rename
40	Replace
41	Resume
42	Restore
43	Retrieve
44	Run
45	Revoke
46	Save
47	Save with Storage Free
48	Save and Delete
49	Submit
50	Set
51	Send
52	Start
53	Transfer
54	Trace
55	Verify
56	Vary
57	Work
58	Read/Change DLO Attribute
59	Read/Change DLO Security
60	Read/Change DLO Content
61	Read/Change DLO all parts
62	Add Constraint
63	Change Constraint
64	Remove Constraint
65	Start Procedure
66	Get Access on **OOPOOL
67	Sign object
68	Remove all signatures
69	Clear a signed object
70	MOUNT
71	Unload
72	End Rollback

Reporting ZC and ZR for CREDITCARD

- **Query/SQL/Excel**

Select *
where ZCONAM = CREDITCARD

Then subset as needed,
or slice and dice in Excel

Select *
where ZRONAM = CREDITCARD

Then subset as needed,
or slice and dice in Excel

Extracting ODBC Update Access

- 1) Create a duplicate of the IBM supplied model *OUTFILE for ZC entries, use the command.

```
CRTDUPOBJ  OBJ(QASYZCJ5) FROMLIB(QSYS) OBJTYPE(*FILE)
           TOLIB(MYLIB) NEWOBJ(ZC_MODEL)
```

- 2) Run the DSPJRN command, and specify *TYPE5 and the name of your copy of the IBM model *OUTFILE.

```
DSPJRN JRN(QAUDJRN) RCVRNG(*CURRENT) JRNCDE((T))
       ENTTYP(ZC) JOB(QZDASOINIT) OUTPUT(*OUTFILE)
       OUTFILFMT(*TYPE5) OUTFILE(MYLIB/ZC_MODEL)
       OUTMBR(*FIRST *REPLACE)
```

- The QZDASOINIT job is specified. The main ODBC server job.
- Cannot make the JOB selection using CPYAUDJRNE command.

Don’t Forget to Start Auditing the Objects

- When reporting ZC and ZR entry types Only audited objects can be reported.
- The OBJECT is in charge of its Auditing!

```
CHGOBJAUD OBJ(SECLIB/MYFILE) OBJTYPE(*FILE) OBJAUD(*ALL)
```

```
CHGOBJAUD OBJ(SECLIB/MYFILE) OBJTYPE(*FILE) OBJAUD(*CHANGE)
```

Reporting Changes To System Values

- QAUDCTL System Value must include *AUDLVL
- QAUDLVL System Value must include *SECURITY

- A change to a System value, or Service Attribute will generate a QAUDJRN Journal entry with entry type **SV**

The Model Outfile used in extraction is QASY<u>SV</u>J5

Extracting Changes to System Values

- 1) Create a duplicate of the IBM supplied model *OUTFILE for SV entries, use the command.

```
CRTDUPOBJ  OBJ(QASYSVJ5) FROMLIB(QSYS) OBJTYPE(*FILE)
           TOLIB(MYLIB) NEWOBJ(SV_MODEL)
```

- 2) Run the DSPJRN command, and specify *TYPE5 and the name of your copy of the IBM model *OUTFILE.

```
DSPJRN JRN(QAUDJRN) RCVRNG(*CURRENT) JRNCDE((T))
       ENTTYP(SV)  OUTPUT(*OUTFILE)
       OUTFILFMT(*TYPE5) OUTFILE(MYLIB/SV_MODEL)
       OUTMBR(*FIRST *REPLACE)
```

Always specify any known selection criteria on DSPJRN command.

e.g. Dates, Times, Sequence Numbers, User, Job, Receiver Range.

System Value Entry Specific Data

SVETYP		CHAR	1	1	610	Both	Entry Type
Values	A	A system value was changed					
	B	A service attribute was changed					
	C	The System clock was changed					
SVSYSV		CHAR	10	10	611	Both	System Value Name
SVNVAL		CHAR	250	250	621	Both	New Value
SVOVAL		CHAR	250	250	871	Both	Old Value
SVNCVL		CHAR	250	250	1121	Both	New Value Continued
SVOCVL		CHAR	250	250	1371	Both	Old value Continued

Other Fields of interest

SVTSTP	TIMESTAMP
SVJOB	Job Name – Workstation name for Interactive jobs
SVUSER	Job User
SVNBR	Job Number
SVPGM	Program used to make the change
SVPGMLIB	Library of Program used to make the change
SVUSPF	Current User Profile (Who made Change)
SVRADR	Client/Host IP Address used in making the change

Reporting Deleted Objects

- QAUDCTL System Value must include *AUDLVL
- QAUDLVL System Value must include *DELETE

- When an object is deleted, the event will generate a QAUDJRN Journal entry with entry type **DO**

The Model Outfile used in retrieval is QASY<u>DO</u>J5

Extracting Information on Deleted Objects

- 1) Create a duplicate of the IBM supplied model *OUTFILE for DO entries, use the command.

```
CRTDUPOBJ  OBJ(QASYDOJ5) FROMLIB(QSYS) OBJTYPE(*FILE)
           TOLIB(MYLIB) NEWOBJ(DO_MODEL)
```

- 2) Run the DSPJRN command, and specify *TYPE5 and the name of your copy of the IBM model *OUTFILE.

```
DSPJRN JRN(QAUDJRN) RCVRNG(*CURRENT) JRNCDE((T))
       ENTTYP(DO)  OUTPUT(*OUTFILE)
       OUTFILFMT(*TYPE5) OUTFILE(MYLIB/DO_MODEL)
       OUTMBR(*FIRST *REPLACE)
```

AGAIN: Always specify any known selection criteria on DSPJRN command.

e.g. Dates, Times, Sequence Numbers, User, Job, Receiver Range.

DO – Entry Specific Data

DOETYP	CHAR	1	1	610	Both	Entry type
Values:	A Object was deleted (not under commitment control)					
	C A pending object delete was committed					
	D A pending object create was rolled back					
	P Object delete pending (the delete was performed under commitment control)					
	R A pending object delete was rolled back					
DOONAM	CHAR	10	10	611	Both	Object name
DOOLIB	CHAR	10	10	621	Both	Library name
DOOTYP	CHAR	8	8	631	Both	Object type
DOOUSR	CHAR	10	10	659	Both	Office user
DOODLO	CHAR	12	12	669	Both	DLO name
DOOFLR	CHAR	63	63	689	Both	Folder path
DOOBUS	CHAR	10	10	752	Both	Behalf of user
DOOLEN	BINARY	4 0	2	780	Both	Object name length
DOCCID	BINARY	5 0	4	782	Both	Object name CCSID
DOCNTY	CHAR	2	2	786	Both	Object name region
DOLANG	CHAR	3	3	788	Both	Object name language
DOPFID	CHAR	16	16	794	Both	Parent file ID
DOOFID	CHAR	16	16	810	Both	Object file ID
DOOBJN	CHAR	512	512	826	Both	Object name
DOOID	CHAR	16	16	1338	Both	Object file ID
DOASP	CHAR	10	10	1354	Both	ASP name
DOASPN	CHAR	5	5	1364	Both	ASP number
DOPCCI	BINARY	5 0	4	1369	Both	Path name CCSID
DOPCNT	CHAR	2	2	1373	Both	Path name region
DOPLAN	CHAR	3	3	1375	Both	Path name language
DOPNLN	BINARY	4 0	2	1378	Both	Path name length
DOAPIN	CHAR	1	1	1380	Both	Absolute path indic
Values	Y Path Name field contains complete absolute path name for the object					
	N Path Name field does not contain an absolute path name for the object					
DORPFI	CHAR	16	16	1381	Both	Relative file ID
DOPNM	CHAR	5000	5002	1397	Both	Path name

Reporting Changes Made to the Job Scheduler

- QAUDCTL System Value must include *OBJAUD

- Audit the actual Job Schedule Object for Changes

CHGOBJAUD (QUSRSYS/QDFTJOBSCD) OBJTYPE(*JOBSCD) OBJAUD(*CHANGE)

  - **Extract the ZC entries, Report on only the QDFTJOBSCD object OR the type *JOBSCD.**

- Audit the commands used to manipulate the Job Scheduler

CHGOBJAUD (QSYS/ADDJOBSCDE) OBJTYPE(*CMD) OBJAUD(*ALL)
CHGOBJAUD (QSYS/CHGJOBSCDE) OBJTYPE(*CMD) OBJAUD(*ALL)
CHGOBJAUD (QSYS/RMVJOBSCDE) OBJTYPE(*CMD) OBJAUD(*ALL)

  - **Extract the CD entries, Report on Only these commands.**

- Audit additional commands that update the Job Scheduler
  - Example: The **ANZPRFACT** command adds the entry QSECIDL1.

CHGOBJAUD (QSYS/ANZPRFACT) OBJTYPE(*CMD) OBJAUD(*ALL)

  - **Extract the CD entries, Report on Only these commands.**

Reporting Changes Made to the Exit Program Registry (WRKREGINF, ADDEXITPGM, etc.. Options 1 and 2)

- **1) QAUDCTL System Value must include *OBJAUD**
- Audit the actual Exit program Registry object for Changes

CHGOBJAUD OBJ(QUSRSYS/QUSEXRGOBJ) OBJTYPE(*EXITRG) OBJAUD(*CHANGE)

  - Extract the **ZC** entries, Report Only the object name and/or type.

- **2) QAUDCTL System Value must include *AUDLVL**
  - **QAUDLVL** System value must include ***SECURITY** or ***SECCFG**

- When the exit point registry is manipulated by any process, a Journal Entry type **GR** is written. **GR** is Generic, as of 6.1 all **GR** entries are related to the Exit Program Registry.
  - Extract the **GR** entries, Report all instances.

- The model Outfile for **GR** entries is QASY**GR**J5.

Journal Entry Types by *AUDLVL values

Layout of All Journal Entry OUTFILES

- **See Attached Appendices from the IBM Security Reference**

www.SecureMyi.com

Thank you!

Any Questions?

Dan Riehl
dan.riehl@SecureMyi.com

www.Cilasoft.com