RSH CONSULTING

RACF
Custom Fields

June 2024

RSH Consulting – Robyn E. Gilchrist

RSH CONSULTING

RSH Consulting, Inc. is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050
- www.linkedin.com/company/rsh-consulting-inc.

Robyn E. Gilchrist is a Senior RACF and ACF2 Consultant. She assists clients with evaluation of their z/OS security posture and works with them to enhance their access controls. As a systems programmer and network engineer, Ms. Gilchrist has installed, configured, and maintained the z/OS Communications Server and WebSphere Application Server (WAS) for z/OS in Network Deployment (ND) mode with associated ACF2 and RACF controls. She has converted CPF-connected ACF2 databases to RRSF-connected RACF databases.

- 617-977-9090
- R.Gilchrist@rshconsulting.com
- www.linkedin.com/in/robyn-e-gilchrist/

Custom Fields

- Introduction
- CFIELD profiles
- CFDEF options
- Activation
- Assigning Values
- Considerations
- Administration

Custom Fields

- Provide a means to store installation-specific information in RACF
  - Augment installation DATA field (e.g. Employee Number, Active Directory ID, Department Code, Answers to password reset questions)
  - Do not require assembler programming, unlike USERDATA fields
  - Can be accessed and managed by ...
    - RACF commands
    - RACF ISPF panels
    - LDAP SDBM
    - R_admin
    - RACROUTE REQUEST=EXTRACT
    - ICHEINTY
    - Adjunct RACF administration products (e.g., zSecure Admin)
  - Available for USER and GROUP profiles, and as of z/OS 2.4, DATASET and GENERAL profiles
- Custom fields are defined as profiles in the CFIELD class
  - Custom field characteristics are defined CFDEF segments in CFIELD profiles
- Custom fields are assign values via CSDATA segments in USER, GROUP, DATASET, and GENERAL profiles

CFIELD Profile Sample

```
RDEFINE CFIELD USER.CSDATA.JOBTITLE  +
  CFDEF( TYPE(CHAR) FIRST(ANY) OTHER(ANY) MAXLENGTH(40) LISTHEAD('JOBTITLE =')    +
  MIXED(YES) HELP(' JOBTITLE = JOB TITLE. FREE FORM, 40 CHARACTERS ')
```

```
RLIST CFIELD USER.CSDATA.JOBTITLE CFDEF NORACF

CLASS      NAME
-----      ----
CFIELD     USER.CSDATA.JOBTITLE

CFDEF INFORMATION
-----------------
TYPE = CHAR
MAXLENGTH = 00000040
MAXVALUE = NONE
MINVALUE = NONE
FIRST = ANY
OTHER = ANY
MIXED = YES
HELP = JOBTITLE = JOB TITLE. FREE FORM, 40 CHARACTERS
LISTHEAD = JOBTITLE =
VALREXX = NONE
ACEE = NO
```

CFIELD Profile Sample

```
ALTUSER RSHTEST CSDATA( JOBTITLE( 'racf tester' ))
```

```
LISTUSER RSHTEST CSDATA NORACF

USER=RSHTEST

CSDATA INFORMATION
------------------
JOBTITLE = racf tester
```

CFIELD Class CDT Entry

- ID = 1
- POSIT = 588

- MAXLNTH = 26
- FIRST = ALPHA
- OTHER = ANY
- CASE = UPPER

- DFTRETC = 4
- DFTUACC = NONE
- OPER = NO

- GENLIST = DISALLOWED
- RACLIST = DISALLOWED
- RACLREQ = NO

Custom Fields - Profile

- CFIELD class profiles
  - USER.CSDATA.*field-name*
  - GROUP.CSDATA.*field-name*
  - DATASET.CSDATA.*field-name*
  - GENERAL.CSDATA.*field-name*
    - For General Resources, custom fields are not resource class specific
  - *Field-name* is installation chosen
    - Maximum length is 8 characters
    - Do not choose field names where one is the prefix of another (e.g., HOME and HOMEADDR, LOC and LOCPHONE) as RACF confuses the shorter name as an abbreviation of the longer
    - Do not use 'NO' as the prefix for a field name

Custom Fields - CFDEF

- CFDEF segment options
  - TYPE(CHAR | FLAG | HEX | NUM)
  - FIRST(ALPHA | ALPHANUM | ANY | NONATABC | NONATNUM | NUMERIC)
  - HELP('*help-text*')
  - LISTHEAD('*list-heading-text*' | *fieldname* =)
  - MAXLENGTH(*nnnn*)
  - MAXVALUE(*nnnnnnnnn*) | NOMAXVALUE
  - MINVALUE(*nnnnnnnnn*) | NOMINVALUE
  - MIXED(YES | NO)
  - OTHER(ALPHA | ALPHANUM | ANY | NONATABC | NONATNUM | NUMERIC)
  - VALREXX(system-rexx-exec-name)
  - ACEE(YES | NO) - New z/OS 3.1

Custom Fields - CFDEF

- CFDEF options and defaults depend on specified TYPE
  - TYPE(CHAR) - Character (text) field
    - Defaults: FIRST(ALPHA) MAXLENGTH(1100) MIXED(NO) OTHER(ALPHA)
    - To allow values specified as quoted strings, specify FIRST(ANY) OTHER(ANY)
    - Do not specify MAXVALUE or MINVALUE
  - TYPE(FLAG) - YES | NO flag
    - Fixed defaults: FIRST(NONATABC) OTHER(NONATABC) MAXLENGTH(3)
    - Do no specify any other attributes
  - TYPE(HEX) - Hexadecimal field
    - Defaults: MAXLENGTH(512)
    - Fixed defaults: FIRST(NONATNUM) OTHER(NONATNUM)
    - Do not specify FIRST, OTHER, MAXVALUE, MINVALUE, or MIXED
  - TYPE(NUM) - Numeric field
    - Defaults - MAXLENGTH(10) MINVALUE(0)
    - Fixed defaults - FIRST(NUMERIC) OTHER(NUMERIC)
    - Optionally specify MAXVALUE and MINVALUE
    - MAXVALUE is capped by MAXLENGTH [e.g., MAXLENGTH(4) - MAXVALUE(≤9999)]

Custom Fields - CFDEF

- Default value (*value*)
- Fixed value [*value*]
- Not applicable -

CSDEF FIELD	TYPE(CHAR)	TYPE(FLAG)	TYPE(HEX)	TYPE(NUM)
FIRST	(ALPHA)	[NONATABC]	[NONATNUM]	[NUMERIC]
MAXLENGTH	(1100)	[3]	(512)	(10)
MAXVALUE	-	-	-	(*maxlength)*
MINVALUE	-	-	-	(0)
MIXED	(NO)	-	-	-
OTHER	(ALPHA)	[NONATABC]	[NONATNUM]	[NUMERIC]

Custom Fields - CFDEF

- FIRST and OTHER options
  - ALPHA — A - Z and national characters (US: #, @, $)
  - ALPHANUM — A - Z, 0 - 9, and national characters
  - ANY — A - Z, 0 - 9, national characters, and any other character
    Specifying both FIRST(ANY) and OTHER(ANY) allows quoted strings
  - NONATABC — A-Z, but not 0-9 or national characters
  - NONATNUM — A - Z and 0 - 9, but not national characters
  - NUMERIC — 0 - 9
- HELP('*help-text*')
  - Text displayed when user presses the PF1 key
  - Length - 1-255 characters
  - Enclose in quotes if text contains parentheses, commas, or blanks
  - Use two abutting quotes for embedded quotes (e.g., 'USER''S NICKNAME')
  - Lower case alphabetic characters are translated into upper case
  - If omitted, defaults to the field name
  - Recommend including the field name in the help text

Custom Fields - CFDEF

- LISTHEAD('*list-heading-text*')
  - Text displayed when listing the CSDATA segment
  - Length - 1-40 characters
  - Use quotes as described for HELP
  - Ensure all fields have a unique LISTHEAD heading
  - If omitted, defaults to field name plus an equal '=' sign (e.g., DEPT =)
  - Recommend including the field name as an aid to changing the field
  - Recommend appending an end delimiter (e.g., = or :) to help distinguish between the field's header and the contents of the field
  - EX: LISTHEAD('EMPNO - EMPLOYEE NUMBER:')

- MAXLENGTH(*nnnn*)
  - Ranges determined by TYPE (default)
    - CHAR 1 - 1100
    - FLAG 3
    - HEX 1 - 512 - Recommend specifying in even numbers
    - NUM 1 - 10

Custom Fields - CFDEF

- MAXVALUE and MINVALUE
  - Range: 0 - 2,147,483,647
  - MINVALUE defaults to 0
  - MAXVALUE cannot be less than MINVALUE
  - If MAXLENGTH is specified but not MAXVALUE, MAXVALUE defaults to the highest value available based on MAXLENGTH
    - MAXLENGTH(3) - default MAXVALUE(999))
  - If both MAXLENGTH and MAXVALUE are specified, MAXVALUE cannot be higher that the highest value allowed by MAXLENGTH
- MIXED(YES | NO)
  - Enable use of mixed-case characters in custom field values
- VALREXX(*system-rexx-exec-name*)
  - Specifies name of a REXX EXEC called to perform validation of the assigned value
  - REXX exec must reside in the System REXX library concatenation
- ACEE(YES | NO) - New z/OS 3.1
  - Store field contents in ACEE for retrieval using the R_GetInfo service

CFIELD Profile - Creation

```
RDEFINE CFIELD USER.CSDATA.USERTYPE  +
  CFDEF( TYPE(CHAR) FIRST(ALPHA) MAXLENGTH(1)  LISTHEAD('USERTYPE:')   +
  HELP('USERTYPE - E-employee, C-contractor, S-system, X-terminated')
```

```
CLASS      NAME
-----      ----
CFIELD     USER.CSDATA.USERTYPE

CFDEF INFORMATION
-----------------
TYPE = CHAR
MAXLENGTH = 00000001
MAXVALUE = NONE
MINVALUE = NONE
FIRST = ALPHA
OTHER = ALPHA
MIXED = NO
HELP = USERTYPE - E-EMPLOYEE, C-CONTRACTOR, S-SYSTEM, X-TERMINATED
LISTHEAD = USERTYPE:
VALREXX = NONE
ACEE = NO
```

Custom Fields - Activation

- CFIELD class must be activated for profiles to take affect

  SETROPTS CLASSACT(CFIELD)

- For fields to be available for use, new or modified CFIELD profiles have to be loaded into the RACF Command Parsing Table via program IRRDPI00
  - IRRDPI00 can be executed as a TSO command or in batch
  - Run IRRDPI00 on all z/OS systems sharing the RACF database
  - Run IRRDPI00 on all z/OS systems in the RRSF network if CFIELD data is propagated
  - To execute IRRDPI00, the following RACF authority is required
    - If the PROGRAM class is active, READ access to program IRRDPI00 is required
      - IRRDPI00 resides in SYS1.LINKLIB
    - If the PROGRAM class is not active, READ access FACILITY resource IRRDPI00
    - If no FACILITY profile exists, user requires RACF SPECIAL authority

Custom Fields - Activation

- Validate CFIELD profiles before attempting to add them to the table

```
//xxxxxxxx JOB roex card fields
//STEP0010 EXEC PGM=IKJEFT01,REGION=0M,PARM='IRRDPI00 CHECK'
//SYSTSPRT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSUT1   DD  DSN=SYS1.SAMPLIB(IRRDPSDS),DISP=SHR
//SYSTSIN  DD  DUMMY
```

- Install CFIELD profiles if validation is successful

```
//xxxxxxxx JOB job card fields
//STEP0010 EXEC PGM=IKJEFT01,REGION=0M,PARM='IRRDPI00 UPDATE'
//SYSTSPRT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSUT1   DD  DSN=SYS1.SAMPLIB(IRRDPSDS),DISP=SHR
//SYSTSIN  DD  DUMMY
```

- Optionally list CFIELD definitions in the Command Parsing Table

```
//xxxxxxxx JOB job card fields
//STEP0010 EXEC PGM=IKJEFT01,REGION=0M,PARM='IRRDPI00 LIST (USER CSDATA)'
//SYSTSPRT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSUT1   DD  DSN=SYS1.SAMPLIB(IRRDPSDS),DISP=SHR
//SYSTSIN  DD  DUMMY
```

Custom Fields - Assigning Values

- Values assigned via add and alter commands (e.g., ADDUSER, ALTUSER)
- To add or change a value, specify CSDATA(*field-name*(*field-value*) ...)
  - Enclosed text values in 'quotes'
  - Maximum number of fields per command is 85

    ADDUSER USERBOB CSDATA(EMP#(12345) JOBTITLE('Dept Manager'))

    ALTGROUP RSHCORP CSDATA(DEPT#(A1))
- For TYPE(HEX)
  - Only values with characters 0-9 and A-F are allowed
  - Values must not be enclosed in quotes
  - A leading zero '0' is appended for values with an odd number of characters
- To remove a field from the CSDATA segment, specify CSDATA(NO*field-name*)

  ALTUSER USERBOB CSDATA(NOEMP#)
- To remove the CSDATA segment in its entirety, specify NOCSDATA

  ALTGROUP RSHCORP NOCSDATA
- To list a CSDATA segment, specify CSDATA with the list type command

  LISTUSER USERBOB CSDATA

Custom Fields - Considerations

- Cannot change TYPE or remove TYPE, MAXLENGTH, FIRST, OTHER, HELP, MIXED, or LISTHEAD from CFDEF segment
- A CSDATA segment has a maximum size of 64K bytes
  - Field name and 1-byte type are stored along with the field value
- Before changing a CFDEF segment, delete all related CSDATA segments who contents will not conform to the new characteristics
- Before deleting a CFIELD profile or a CFDEF segment, delete all related CSDATA fields
- Custom Field Validation Exit (IRRVAF01)
  - Can be used to validate entries
  - Pre-dates VALREXX - latter much easier to use

Custom Fields - Considerations

- CSDATA fields in a user's ACEE
  - Not available in z/OS 2.5 and before
  - Available on a field-by-field basis in z/OS 3.1 with CFIELD option ACEE(YES)

- RACF ISPF panels for updating custom fields use R_admin callable services, and to use them, users must be permitted READ access to the following FACILITY class resources depending on the class associated with the field
  - IRR.RADMIN.ADDUSER | ALTUSER | DELUSER | LISTUSER
  - IRR.RADMIN.ADDGROUP | ALTGROUP | DELGROUP | LISTGRP
  - IRR.RADMIN.ADDSD | ALTDSD | DELDSD | LISTDSD
  - IRR.RADMIN.RDEFINE | RALTER | RDELETE | RLIST

- RACF Database Unload contains CFIELD profiles and CSDATA segments for installation processing
  - Restrict access to the unload if CSDATA segments contain sensitive information

- CSDATA data will appear in SMF records generated for RACF commands that add or change the data - be mindful of this if the data is sensitive

Custom Fields - Use Case Examples

RSH RACF Survey - #15 - December 2012

What custom fields have you implemented?

USER	Count		GROUP	Count
National ID Number (e.g. SSN)	2		Access Level Granted	1
HR Employee Number	2		Group Owner Identity	1
Department Number	1		Application	1
Email Address	1		Usage (Production, Test, etc.)	1
Phone Number	1			
First Name	1			
Birthdate	2			
ID Creation Date	1			
Freeform Text	1			

Custom Fields - Administration - FIELD Class

- Delegate maintenance of custom field segments CFDEF and CSDATA

- General Resource
  - Class - FIELD RACLIST-REQUIRED
  - Profile - *profile-class.segment*.[*field*]
    - CFDEF CFIELD.CFDEF.*cfdef-field*
    - CSDATA USER | GROUP | DATASET | GENERAL .CSDATA.*custom-field*
      (e.g. USER.CSDATA.MANAGER)
  - Access Levels
    - READ - examine
    - UPDATE - change

- &RACUID can be used to permit users access to just their own USER segment(s) - usually to allow viewing (READ)

- UPDATE to resource *profile-class.segment.* (includes ending period) is required to create an empty segment or delete a segment

Custom Fields - Administration - FIELD Class

- CFIELD.CFDEF.*cfdef-field*

CFDEF Keyword	CFDEF FIELD Name
ACEE	CFACEE
TYPE	CFDTYPE
MAXLENGTH	CFMXLEN
MAXVALUE	CFMXVAL
MINVALUE	CFMNVAL
FIRST	CFFIRST
OTHER	CFOTHER
MIXED	CFMIXED
HELP	CFHELP
LISTHEAD	CFLIST
VALREXX	CFVALRX

Custom Fields - Administration - FIELD Class

- Use FIELD class profiles to allow viewing and administering CSDATA segments

```
RDEFINE FIELD USER.CSDATA.EMPNO
PERMIT USER.CSDATA.EMPNO CLASS(FIELD) ID(&RACUID) ACCESS(READ)
PERMIT USER.CSDATA.EMPNO CLASS(FIELD) ID(HRADMIN) ACCESS(UPDATE)

RDEFINE FIELD USER.CSDATA.HOMEADDR
PERMIT USER.CSDATA.HOMEADDR CLASS(FIELD) ID(&RACUID) ACCESS(READ)
PERMIT USER.CSDATA.HOMEADDR CLASS(FIELD) ID(HRADMIN) ACCESS(UPDATE)
PERMIT USER.CSDATA.HOMEADDR CLASS(FIELD) ID(HRBATCH) ACCESS(UPDATE)

RDEFINE FIELD USER.CSDATA.*
PERMIT USER.CSDATA.* CLASS(FIELD) ID(&RACUID) ACCESS(READ)
PERMIT USER.CSDATA.* CLASS(FIELD) ID(HRADMIN) ACCESS(READ)
```