RSH CONSULTING

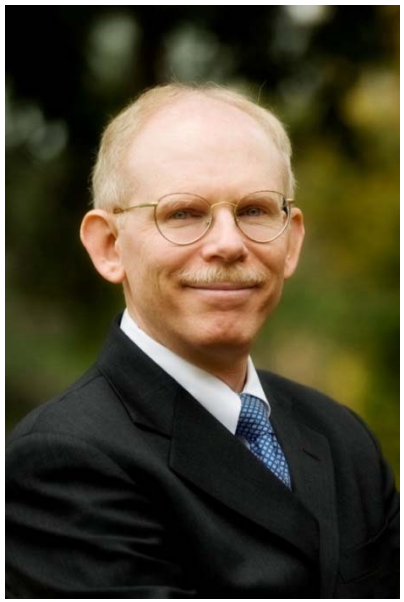
RACF Utilities

KOIRUG - April 2016

RSH Consulting - Robert S. Hansel

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



Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc. He began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He is a leading expert in securing z/OS Unix using RACF. Mr. Hansel has created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel
- http://twitter.com/RSH_RACF

RACF Utilities

- Programs providing extended services within the RACF environment
  - Manage and maintain the RACF database and profiles
  - Load the command parsing table
  - Report on security status
  - Unload RACF profiles and SMF access events

- Information provided for each utility
  - Description and function
  - Sample JCL and execution options
  - Usage considerations and recommendations
  - References

- As a general rule, if multiple systems share a RACF database and are at different z/OS release levels, use the utilities from the highest level system
  - This is mandatory for IRRMIN00 and IRRUT400

RACF Utilities

- IRRMIN00 RACF Initialization Utility
- IRRIRA00 RACF Internal Reorganize Alias Utility
- IRRDPI00 RACF Dynamic Parse Initialization
- IRRUT100 RACF Cross Reference Utility
- IRRUT200 RACF Database Verification Utility
- BLKUPD RACF Block Update Utility (a.k.a. IRRUT300)
- IRRUT400 RACF Database Split/Merge/Extend Utility
- ICHDSM00 RACF Data Security Monitor (DSMON)
- IRRDBU00 RACF Database Unload Utility
- IRRRID00 RACF Remove ID Utility
- IRRADU00 RACF SMF Data Unload Utility
- RACFRW RACF Report Writer (not covered)
- Unsupported RACF utilities

IRRMIN00 - RACF Database Initialization Utility

- Initializes new databases and updates templates in existing databases
- PARM=
  - NEW - Initializes new RACF database
  - UPDATE - Installs new templates in existing RACF database
  - ACTIVATE - Activates new templates by loading them into storage
- Sample JCL

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//UPDATE   EXEC PGM=IRRMIN00,PARM=UPDATE
//STEPLIB  DD DSN=SYS1.LINKLIB,DISP=SHR,       <- Library with newest IRRMIN00
//    UNIT=unit,VOL=SER=volser
//SYSPRINT DD SYSOUT=*
//SYSRACF  DD DSN=racf.database,DISP=SHR
```

- Considerations
  - PARM=NEW will not overwrite a RACF database in use on the system where executed
  - Templates must be updated in all primary and backup database datasets
  - Requires ALTER (for NEW) or UPDATE (for UPDATE) access authority to the target database
  - If using RACF sysplex data sharing, execute on a system in the sysplex group
- Use operator command SET LIST to display current template level
- Reference: RACF Systems Programmer's Guide

IRRIRA00 - RACF Internal Reorganize Aliases Utility

- Converts a RACF database to use the Application Identity Mapping (AIM) structure
  - Adds alias index structure for identity mapping
  - Replaces use of pre-existing identity mapping profiles in classes UNIXMAP (z/OS Unix), NOTELINK (Lotus Notes) and NDSLINK (Novell Directory Services)
- Reasons for converting
  - More efficient lookup of application identities (VLF caching with IRRUMAP and IRRGMAP for z/OS Unix is still needed)
  - Enables use of SEARCH on UID and GID
  - Alias index requires less space than mapping profiles in both the RACF database and the IRRDBU00 unload
  - Required to implement ...
    - UNIXPRIV SHARED.IDS Stage 2
    - FACILITY BPX.NEXT.USER Stage 2
    - FACILITY BPX.UNIQUE.USER Stage 3
- Reference: RACF Systems Programmer's Guide

IRRIRA00 - RACF Internal Reorganize Aliases Utility

- AIM conversion stages (indicator set in ICB record and RCVT):
  - 0 = Pre-conversion, uses mapping profiles for lookups if mapping class is active
  - 1 = Builds and maintains alias index but uses mapping profiles for lookups
  - 2 = Uses alias index and mapping profiles for lookups
  - 3 = Uses alias index for lookups and deletes mapping profiles

- Sample JCL

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//STEP     EXEC PGM=IRRIRA00,PARM=STAGE(1)
//SYSPRINT DD  SYSOUT=*
```

- PARM=
  - No parms specified: displays current stage
  - STAGE(1 | 2 | 3): upgrade by one level to the level specified

- Must pass through all stages, converting from one stage to the next, one stage at a time, until reaching stage 3; cannot retreat to a previous stage

IRRIRA00 - RACF Internal Reorganize Aliases Utility

- Requires UPDATE access authority to the live RACF database (primary and backup)
  - Runs only against the live database
- Considerations
  - Ensure IRRMIN00 PARM=UPDATE was run and system was IPLed before going to stage 1
  - Verfy the database has sufficient free space for the new index before converting
  - Maximum of 129 8-character IDs can share an identity (e.g., UID(0))
    - Identify and reduce excessive sharing before conversion
  - IRRIRA00 assumes UNIXMAP profiles are accurate and builds the index from them
    - Either identify and fix UNIXMAP profile / OMVS segment mismatch errors before the conversion or run IRRUT400 immediately afterwards to rebuild the index
  - If using RACF sysplex data sharing, execute on a system in the sysplex group
  - Before attempting each stage, make an IRRUT200 backup
    - Check for integrity errors before proceeding
  - IRRIRA00 obtains exclusive use of the database during execution
    - Run during non-peak periods and suspend RACF administrative work
    - Stage 1 conversion may take a long time if there are many mapping profiles
    - To expedite, deactivate backup and create a new backup from the converted primary when done
  - Do the entire conversion (0-to-1, 1-to-2, 2-to-3) in a single session
  - Deactive mapping classes upon reaching stage 3

IRRDPI00 - RACF Dynamic Parse Initialization Utility

- TSO command to build RACF profile segment parsing table

- Should be run …
  - At IPL - by a Started Task or the RACF subsystem
  - After activating new templates (IRRMIN00 with ACTIVATE) if instructed by PTF documentation
  - After creating or modifying Custom Field CFIELD class profile CFDEF segments

- Executed by either …
  - Started Task - typically IRRDPTAB
  - RACF subsystem (preferred method at IPL)

```
//RACF      PROC
//RACF      EXEC PGM=IRRSSM00,REGION=0M,PARM='OPT=xx'
//RACFPARM DD DSN=racf.parm.library,DISP=SHR
```

    Member IRROPTxx in RACFPARM library contains command IRRDPI00
  - TSO user at READY prompt
    - Requires program IRRDPI00 to be APF-authorized via PARMLIB member IKJTSOxx

IRRDPI00 - RACF Dynamic Parse Initialization Utility

- To execute, requires ...
  - Either …
    - READ access to PROGRAM class profile IRRDPI00
      - Define PROGRAM profile IRRDPI00 if backstop * or ** profile exists
    - READ access to FACILITY class profile IRRDPI00 if ...
      - PROGRAM not protected, and
      - Executing in TSO
    - RACF SPECIAL if neither profile is defined
    - Recommendation: Define profile IRRDPI00 in both the PROGRAM and FACILITY class and permit the same IDs to both
  - And …
    - READ access to table source code referenced in DD SYSUT1 - usually SYS1.SAMPLIB(IRRDPSDS)

- IRRDPI00 options
  - CHECK - Verifies syntax of CFDEF defintions - run before UPDATE
  - UPDATE - Verifies syntax of CFDEF defintions and updates the table
  - LIST [(profile-type [segment-name [keyword-name]])] - List entries

IRRDPI00 - RACF Dynamic Parse Initialization Utility

- Executed in batch (for Started Task, replace JOB with PROC card)

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//STEP0001 EXEC PGM=IKJEFT01,REGION=2M,
//    PARM='IRRDPI00 UPDATE'
//SYSTSPRT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSUT1   DD DSN=SYS1.SAMPLIB(IRRDPSDS),DISP=SHR
//SYSTSIN DD DUMMY
```

- Executed as a TSO command or by RACF subsystem

```
ALLOCATE FILE(SYSUT1) DATASET('SYS1.SAMPLIB(IRRDPSDS)') SHR
IRRDPI00 UPDATE
FREE FILE(SYSUT1)
```

- SYS1.SAMPLIB(IRRDPSDS) contains the parsing table entries included with RACF

- Reference: RACF Systems Programmer's Guide

IRRUT100 - RACF Cross Reference Utility

- Lists all references to specified USERIDs and/or groups in the RACF database in …
  - Standard and Conditional access lists
  - NOTIFY and OWNER fields
  - Group memberships for users
  - Dataset profiles with matching High Level Qualifier (HLQ)
- Does not list instances where …
  - ID is embedded in qualifiers in general resource profiles
  - ID is embedded in dataset profile qualifiers except the HLQ
  - ID is in APPLDATA field (e.g., BPX.DEFAULT.USER)
- Authority to execute
  - System-level SPECIAL / AUDITOR / ROAUDIT - can report on any ID or group
  - Group-level SPECIAL / AUDITOR can report on IDs and groups within their scope
  - Users can generate a report on their own USERID
- Usage Notes
  - Works only with the current (active) RACF database
  - Serializes on one profile at a time - reads every profile
  - Can list up to 1,000 IDs and/or groups

IRRUT100 - RACF Cross Reference Utility

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//IRRUT100 EXEC PGM=IRRUT100
//SYSUT1   DD   UNIT=SYSDA,SPACE=(CYL,(10,1))              <<< Work dataset
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
JSMITH1  DJONES
/END                                                      <<< Optional
```

SYSPRINT output

```
OCCURRENCES OF JSMITH1

IN STANDARD ACCESS LIST OF DATASET PROFILE SYSTEST.FDR.OBJLIB
IN STANDARD ACCESS LIST OF DATASET PROFILE SYS1.DASDUTIL.LIB (G)
IN ACCESS LIST OF GROUP USERGRPA
OWNER OF PROFILE HSM.BACKUP.WEEKLY (G)
IN STANDARD ACCESS LIST OF PROGRAM PROFILE AMASPZAP
FIRST QUALIFIER OF PROFILE JSMITH1.TEST.* (G)
USER ENTRY EXISTS

(G) - ENTITY NAME IS GENERIC
```

- Recommendation: Use sparingly if at all
- Reference: RACF Security Administrator's Guide

IRRUT200 - RACF Database Verification Utility

- Identifies inconsistencies in the internal organization of a RACF database
  - Identifies problems with the index-block chains
  - Verifies index entries point to the correct profile
  - Validates and reports errors found in Relative Byte Addresses (RBAs) of all profile segments
  - Reports inconsistencies in the block segments of the database that are actually in use as compared to the block segments listed as allocated in Block Availability Mask (BAM) blocks
  - Validates the database format
  - Issues return codes to indicate validation errors
- Makes an exact, block-by-block, copy of the RACF database
- Optionally creates a formatted index report displaying the 255-byte profile name and profile type information
- Reference: RACF System Programmer's Guide

IRRUT200 - RACF Database Verification Utility

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//STEP     EXEC PGM=IRRUT200
//SYSRACF  DD  DSN=SYS1.RACF,DISP=SHR                    <- Input RACF Database
//SYSUT1   DD  DSN=INFOSEC.RACF.COPY,                    <- Output copy or temp file
//             UNIT=SYSDA,SPACE=(CYL,(10),,CONTIG),
//             DCB=(LRECL=4096,RECFM=F)
//SYSUT2   DD  SYSOUT=*                                  <- Output messages
//SYSPRINT DD  SYSOUT=*                                  <- Output report
//SYSIN    DD  *                                         <- Control statements
INDEX FORMAT
MAP ALL
END
```

- SYSIN control statements
  - INDEX [FORMAT] Performs index scan function; FORMAT adds a report of all index blocks
  - MAP [ALL] Maps BAM/allocation; ALL adds an encoded map for each BAM block
  - END Terminates the utility
- To obtain an abbreviated summary listing of just the database status, its percentage full, and number of profiles by class, simply specify:

  MAP

  END

IRRUT200 - RACF Database Verification Utility

- Sample Output (Index Block Verification)

```
TOTAL NUMBER OF NAMES IN RACF DATA SET 00016699
TOTAL NUMBER OF INDEX BLOCKS IN RACF DATA SET 00000313
AVERAGE NUMBER OF NAMES PER INDEX BLOCK 053
AVERAGE NAME LENGTH 007
AVERAGE NUMBER OF UNUSED BYTES PER INDEX BLOCK 2277
TOTAL NUMBER OF LEVEL 01 BLOCKS IN RACF DATA SET 00000305
```

- Sample Output (BAM Block Verification)

```
NUMBER OF BAM BLOCKS DEFINED 006
LAST BAM THAT DEFINES USED SPACE - RBA 00000000D000
RACF DATA SET IS  24 PERCENT FULL.
TOTAL NUMBER OF INDEX BLOCKS IN RACF DATA SET 00000313
TOTAL NUMBER OF LEVEL 01 BLOCKS IN RACF DATA SET 00000305
NUMBER OF GROUP    ENTRIES - 0002174
NUMBER OF USER     ENTRIES - 0003862
NUMBER OF DATASET  ENTRIES - 0004500
NUMBER OF $CHGMAN  ENTRIES - 0000108
NUMBER OF $OMEGCIC ENTRIES - 0000003
NUMBER OF $OMEGDB2 ENTRIES - 0000003
NUMBER OF $OMEGMVS ENTRIES - 0000021
NUMBER OF ACCTNUM  ENTRIES - 0000002
NUMBER OF CDT      ENTRIES - 0000022
```

IRRUT200 - RACF Database Verification Utility

- Requires READ authority to the RACF database being verified
- Considerations and Recommendations
  - Has exclusive use of the database during the copy phase - avoid executing during peak work periods
  - If merely analyzing an active database, always specify a work dataset on the SYSUT1 DD to make a temporary copy for analysis to avoid holding a RESERVE on the database throughout the entire analysis phase
  - If using RACF sysplex data sharing, execute on a system in the sysplex group
  - Device, space, and DCB parameters on SYSUT1 should be exactly the same as input RACF database; use SPACE=(type(n),,CONTIG)
  - SYSUT1 must not be allocated in the extended addressing area of a DASD volume (EATTR)
  - With optional PARM=ACTIVATE, can copy the in-use active primary to the in-use but inactive backup and then automatically RVARY ACTIVE the backup - avoids losing any updates
    - If sharing the database and not using RACF Sysplex Communications, RVARY ACTIVE must be executed on the other systems to activate the backup
  - Regularly review the percentage full to avoid running out of space
- IRRUT200 is the only way to make a valid RACF database backup - it suspends updates during the copy process
  - If split database, each database dataset must be backed up individually

BLKUPD - RACF Database Block Update Command

- The BLKUPD TSO command
  - Modifies blocks in a RACF database
  - Enables correction of inconsistencies found by IRRUT200 in the RACF database
- Requires UPDATE access to the RACF database being fixed
- Use with extreme caution and only after other commands fail
  - Before using, make a backup of the database in case of a mistake
  - Test the fix on a copy of the data base, vary the fixed copy active, confirm the fix was correct, then fix the “active” data base
- Reference: RACF Diagnosis Guide

IRRUT400 - RACF Database Split/Merge/Extend Utility

- Copies a RACF database to a larger or smaller sized database
- Copies a database to a different device type
- Redistributes data amongst split RACF database datasets
- Identifies inconsistencies (e.g., duplicate profiles)
- Physically reorganizes the database
  - Reduces fragmentation by bringing all segments of a profile together and, optionally, kept within a block boundary
  - Compresses index
  - Rebuilds all index blocks - profile and AIM (corrects errors)
  - Rebuilds Block Availability Mask (BAM) blocks (corrects errors)

IRRUT400 - RACF Database Split/Merge/Extend Utility

- PARM=
  - LOCKINPUT | NOLOCKINPUT | UNLOCKINPUT
    - (no default - one must be specified)
    - LOCKINPUT - Locks the input data set to prevent updates; remains locked after execution ends
    - NOLOCKINPUT - Does not change the status of the database
      - If the live database is used for input, changes made during execution could result in a corrupted copy
    - UNLOCKINPUT - Unlocks database that was previously locked
  - TABLE(table-name) | NOTABLE
    - TABLE(table-name) - user written range table will be used; table-name is the dataset range table load module to be used for splitting the database
    - NOTABLE - forces selection of OUTDD1 for all profiles
  - FREESPACE(nn) | NOFREESPACE
    - FREESPACE(nn) - specifies percentage of freespace to be left within the index blocks to accommodate future growth; 'nn' is 0 to 50 - recommended with at least 10
    - NOFREESPACE - is equivalent to FREESPACE(0)

IRRUT400 - RACF Database Split/Merge/Extend Utility

- PARM= (continued)
  - ALIGN | NOALIGN
    - ALIGN - forces profiles and segments that occupy multiple 256-byte slots to be placed so they do not span 4096 physical blocks so retrieval requires less I/O - recommended
    - NOALIGN - causes no special alignment
  - DUPDATASETS | NODUPDATASETS
    - DUPDATASETS - all duplicate dataset profiles are allowed and processed
    - NODUPDATASETS - if duplicate dataset profiles are found on multiple input databases when merging databases, only the profile from the lowest numbered input database, identified by INDDxx, is retained

IRRUT400 - RACF Database Split/Merge/Extend Utility

- Copying a Database

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//COPYDB   EXEC PGM=IRRUT400,PARM='NOLOCKINPUT,FREESPACE(20)'
//SYSPRINT DD  SYSOUT=*
//INDD1    DD  DSN=SYS1.RACF.COPY,DISP=OLD
//OUTDD1   DD  DSN=SYS2.RACF5,DISP=(,KEEP),VOL=SER=RACVL2,
//             SPACE=(CYL,10,,CONTIG),DCB=DSORG=PSU,UNIT=SYSDA
```

- Splitting a Database

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//SPLITDB  EXEC PGM=IRRUT400,PARM='NOLOCKINPUT,TABLE(NEWRNG)'
//SYSPRINT DD  SYSOUT=*
//INDD1    DD  DSN=SYS1.RACF.COPY,DISP=OLD
//OUTDD1   DD  DSN=SYS2.RACF1,DISP=(,KEEP),
//             UNIT=SYSDA,VOL=SER=VOL1,DCB=DSORG=PSU,
//             SPACE=(CYL,5,,CONTIG)
//OUTDD2   DD  DSN=SYS2.RACF2,DISP=(,KEEP),
//             UNIT=SYSDA,VOL=SER=VOL2,DCB=DSORG=PSU,
//             SPACE=(CYL,20,,CONTIG)
//OUTDD3   DD  DSN=SYS2.RACF3,DISP=(,KEEP),
//             UNIT=SYSDA,VOL=SER=VOL3,DCB=DSORG=PSU,
//             SPACE=(CYL,5,,CONTIG)
//STEPLIB  DD  DSN=INSTALL.LINKLIB,DISP=SHR
```

IRRUT400 - RACF Database Split/Merge/Extend Utility

- Merging a Database (first run)

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//MERGEDB  EXEC PGM=IRRUT400,PARM='NOLOCKINPUT,DUPDATASETS'
//SYSPRINT DD  SYSOUT=*
//INDD1    DD  DSN=SYS1.RACF1.COPY,DISP=OLD
//INDD2    DD  DSN=SYS1.RACF2.COPY,DISP=OLD
```

  - First make a test run to identify any possible inconsistencies
  - Dataset entries with identical names, but from different RACF databases, are allowed
  - Correct any inconsistencies and continue with the merge

- Merging a Database (second run)

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//DBMERGE  EXEC PGM=IRRUT400,
//            PARM='NOLOCKINPUT,NODUPDATASETS,FREESPACE(10),ALIGN'
//SYSPRINT DD SYSOUT=*
//INDD1    DD DSN=SYS1.RACF1.COPY,DISP=OLD
//INDD2    DD DSN=SYS1.RACF2.COPY,DISP=OLD
//OUTDD1   DD DSN=SYS2.RACF,DISP=(,KEEP),UNIT=SYSDA,VOL=SER=VOL001,
//            DCB=DSORG=PSU,SPACE=(CYL,10,,CONTIG)
```

IRRUT400 - RACF Database Split/Merge/Extend Utility

- Copying to a Larger Database (Extend)

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//EXTEND   EXEC PGM=IRRUT400,PARM='LOCKINPUT,FREESPACE(10),ALIGN'
//SYSPRINT DD  SYSOUT=*
//INDD1    DD  DSN=SYS1.RACF,DISP=OLD
//OUTDD1   DD  DSN=SYS2.RACF,DISP=(,KEEP),UNIT=SYSDA,VOL=SER=VOL1,
//             DCB=DSORG=PSU,SPACE=(CYL,15,,CONTIG)
```

- Unlocking the Database

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//UNLOCK   EXEC PGM=IRRUT400,PARM='UNLOCKINPUT'
//SYSPRINT DD  SYSOUT=*
//INDD1    DD  DSN=SYS1.RACF,DISP=OLD
```

  - Does not make a copy - simply unlocks the database

IRRUT400 - RACF Database Split/Merge/Extend Utility

- Not intended to merge RACF databases from different systems
- Output database cannot be the active RACF database
- OUTDD must not be allocated in the extended addressing area of a DASD volume (EATTR)
- Recommendations
  - Run at a time when updates are not likely to be made to the RACF database
  - Process sequence
    - Copy the database using IRRUT200 and verify integrity
    - Reorganize using this copy
    - RVARY the reorganized copy online to become the active primary, then use IRRUT200 PARM=ACTIVATE to copy the reorganized primary to the backup
- Requires UPDATE access to the input RACF database
- Reference: RACF System Programmer's Guide

ICHDSM00 - RACF Data Security Monitor (DSMON)

- Produces reports on the status of …
  - System and security environment
  - Certain RACF controls

- Requires
  - Either …
    - READ access to PROGRAM profile ICHDSM00
      - Define PROGRAM profile ICHDSM00 if backstop * or ** profile exists
    - System-level AUDITOR if program is not defined
  - And …
    - READ access to FACILITY ICHDSM00.SYSCAT to list user catalogs with SYSCAT (allowed if not defined)

- Run on every system to collect system-specific configuration information

- Reference: RACF Auditor's Guide

ICHDSM00 - RACF Data Security Monitor (DSMON)

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//DSMON    EXEC PGM=ICHDSM00
//SYSPRINT DD  SYSOUT=*                                    <- DSMON report
//SYSUT2   DD  SYSOUT=*                                    <- Messages
//SYSIN    DD  *
  FUNCTION option
  LINECOUNT 55 | 0 | 40 - 99          0 = page break only at beginning of each report
  USEROPT USRDSN dsname(s) [VOL=volser(s)]
  USEROPT RACGRP SYS1 | group
```

- Function options (in report generated sequence)

SYSTEM	System and RACF identification	[Recommendation - specify with every execution]
SYSPPT	Program Properties Table (PPT) entries	
RACAUT	RACF Authorized Caller Table entries	
RACEXT	RACF Exits	
RACUSR	RACF User Attribute Summary Report	
RACSPT	RACF STARTED Class and Started Task Table entries	
RACCDT	RACF Class Descriptor Table entries and status	
RACGAC	RACF Global Access Checking Table Report	
RACGRP	RACF Group Tree	
SYSAPF	APF library protection	
SYSLNK	Linklist library protection	
SYSSDS	System dataset report	
SYSCAT	Catalog dataset protection	
RACDST	RACF database protection	
ALL	Produces all reports listed above	

IRRDBU00 - RACF Database Unload Utility

- Unloads the RACF database into a sequential text dataset where the output can be used to extract information by …
  - Browsing directly as is
  - Processing by installation-developed programs, such as ...
    - REXX
    - SAS
    - DFSORT and ICETOOL (see SYS1.SAMPLIB(IRRICE))
  - Loading to a database manager such as DB2 for SQL queries
- Performs diagnostic checks down to the field level - run periodically just to check for data errors
- Input to the utility can be from …
  - A copy of a RACF Database (preferred)
    - May fail if the copy is not allocated as contiguous (CONTIG)
  - The active backup RACF Database
  - The active primary RACF Database

IRRDBU00 - RACF Database Unload Utility

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//UNLOAD   EXEC PGM=IRRDBU00,PARM=NOLOCKINPUT
//INDD1    DD  DSN=input.racf.database,DISP=SHR            <- Input RACF database
//OUTDD    DD  DSN=output.racf.unload,UNIT=DISK,           <- Output RACF unload
//             DISP=(NEW,CATLG,DELETE),DCB=(RECFM=VB,LRECL=4096),
//             SPACE=(CYL,(100,50),RLSE),
//SYSPRINT DD  SYSOUT=*
```

- PARM= (no default - one must be specified)
  - LOCKINPUT - Locks the input data set to prevent updates; remains locked after execution ends
  - NOLOCKINPUT - Does not change the status of the database
  - UNLOCKINPUT - Unlocks database that was previously locked

- If split RACF database, can specify multiple input datasets with INDDn statements to create a combined unload file OUTDD; however, ...
  - The datasets must be listed in the same order as is specified in the dataset name table (ICHRDSNT)
  - The range table (ICHRRNG) on the system where IRRDBU00 is executed must be identical to that used in creating the split database; otherwise, each dataset must be unloaded separately

IRRDBU00 - RACF Database Unload Utility

- Results are affected by the system where IRRDBU00 is executed
  - Uses Enhanced Generic Naming (EGN) setting on the system where it executes
  - Uses Class Descriptor Table (CDT) of the system where it executes
    - Can result in missing profiles for classes not defined on execution system
  - If the database templates on the system where it executes are downlevel, new profile fields will not be unloaded
- To execute, requires access to source RACF database ...
  - Pre-z/OS 2.2 - UPDATE
  - z/OS 2.2 - UPDATE if using LOCKINPUT or UNLOCKINPUT
    - READ if using NOLOCKINPUT
- Recommendation: Create a copy of the RACF database with the IRRUT200 utility and use as input to the IRRDBU00 utility
  - Prevents interference if LOCKINPUT used on active database
  - Prevents integrity errors if NOLOCKINPUT used on active database
- Reference: RACF Security Administrator's Guide

IRRDBU00 - RACF Database Unload Utility

- Unload records
  - All fields are unloaded with two exceptions
    - Encrypted fields
    - RESERVED fields
  - Fields are decoded into a readable format
    - UACC is output as “READ”, “UPDATE”, “CONTROL”, “ALTER” rather than a bit mask
  - One record type per segment per repeat group, identified by a 4-byte record type
    - 0100 series - groups
    - 0200 series - users
    - 0400 series - datasets
    - 0500 series - general resources

```
0200 HANSELR  1998-06-18  SYSADMIN NO YES YES NO 030 …
0200 ONORATO  1998-06-18  SYSADMIN NO YES YES NO 030 …
```

  - Record Layout Reference: Security Server Macros and Interfaces Guide

IRRRID00 - RACF Remove ID Utility

- Helps keep the RACF database current by …
  - Either …
    - Finding all references to any USERIDs and groups that no longer exist
    - Finding all references to select USERIDs and groups slated for deletion
  - And building commands to remove all references to them

- IRRRID00 looks for references to USERIDs and groups in …
  - Profile qualifiers in DATASET, FACILITY, and most general resource classes
  - Standard and conditional access lists
  - OWNER and NOTIFY fields
  - Superior groups, subordinate groups, default groups, connections
  - APPLDATA field of certain general resource profiles
  - STDATA segment of STARTED class profiles

- IRRRID00 will not build commands to remove key RACF entities (e.g., IBMUSER, SYS1, irrcerta)

IRRRID00 - RACF Remove ID Utility

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//STEP0001 EXEC PGM=IRRRID00,REGION=25M
//SYSPRINT DD  SYSOUT=*                                    <- Status report
//SYSOUT   DD  SYSOUT=*                                    <- Messages
//INDD     DD  DSN=racf.database.unload.file,DISP=SHR      <- IRRDBU00 output file
//SORTOUT  DD  SPACE=(CYL,(200,20),RLSE)                   <- Work dataset
//SYSUT1   DD  SPACE=(CYL,(200,20),RLSE)                   <- Work dataset
//OUTDD    DD  DSN=racf.remove.commands.clist.file,        <- Output commands
//             DISP=(NEW,CATLG,DELETE),
//             UNIT=DISK,
//             SPACE=(CYL,(10,5),RLSE),
//             DCB=(RECFM=VB,LRECL=259)
   - either -
//SYSIN    DD  DUMMY           <- Look for obsolete entries
   - or -
//SYSIN    DD  *               <- List of USERIDs and groups to be deleted
USERAB1
GRP002
USERNM  USERBB                 <- second ID is replacement (e.g., OWNER)
```

IRRRID00 - RACF Remove ID Utility

- Sample Output

```
CONNECT MBOM17 GROUP(REVOKE) OWNER(?MBOMB17)
PERMIT  'AP.DS.I.FTP.**' GENERIC  ID(SLAU97V ) DELETE
PERMIT  'BD.DS.M.ISPF.**' GENERIC  ID(BTAY51V ) DELETE
PERMIT  'SYS2.DB2.**' GENERIC  ID(DSNDBC  ) DELETE
RALTER  STARTED  BACKUPV.* STDATA( USER(?BACKUPV ))
CONNECT ?SYSKBMD  GROUP(SYST     )

EXIT

RDELETE SURROGAT SLAU97V.SUBMIT
DELDSD  'DB2T.DSNDBC.*.**' GENERIC
DELDSD  'TSS.BTAY51V.BOSGET.*.**' GENERIC
```

- Failsafes
  - ? - Are embedded within operands and commands fail if run without modification
  - EXIT statement - is inserted before the delete commands – preventing accidental “fall through” execution

IRRRID00 - RACF Remove ID Utility

- Types of commands generated
  - PERMIT DELETE
    - Remove access list entries; can usually be executed unchanged
  - ALTDSD / RALTER NONOTIFY
    - Can optionally be modified to specify new NOTIFY(userid)
  - ALTUSER / ALTGROUP / ALTDSD / RALTER / CONNECT OWNER(?owner)
    - Replacement group or USERID must be entered for the ?owner
    - If replacement ID was specified via SYSIN, commands have new ID instead of ?owner
  - RALTER STARTED STDATA(USER(?user)) | GROUP(?group))

    CONNECT ?userid GROUP(group) - USER was not found

    CONNECT userid GROUP(?group) - GROUP was not found
    - Replacement started task USERID or group must be selected, or STARTED profile is obsolete and should be removed
    - If former STARTED STDATA(USER or GROUP) has since been recreated as the other type of ID (e.g., was an ID, now a group), PERMIT DELETEs and DELUSER / DELGROUP are still created for original ID
  - DELDSD / RDELETE / RALTER DELMEM(member)
    - Member or profile assumed to be obsolete if ID matches the member or a qualifier
  - DELUSER / DELGROUP
    - Commands related to IDs specified for deletion via SYSIN

IRRRID00 - RACF Remove ID Utility

- Recommendations
  - If RACF database is split, ensure IRRDBU00 was created using all database datasets
  - Run with no SYSIN on a regular basis to keep database free of obsolete residual entries
  - Run with SYSIN IDs as standard procedure for deletion, especially for UNIVERSAL groups
  - Archive output from both the IRRDBU00 run and the IRRRID00 utility for future reference and recovery
  - Carefully review profile and member deletions - some may not be desirable
  - Consider removing 05xx STARTED class records from input unload file when running initial execution to check for obsolete IDs

- Reference: RACF Security Administrator's Guide

IRRADU00 - RACF SMF Data Unload Utility

- Reads SMF data and produces sequential text dataset where the output can be used to extract information by …
  - Browsing directly as is
  - Processing by installation-developed reporting programs
  - Loading to a database manager such as DB2 for SQL queries
  - Viewing with a web browser (XML formatted output)

- SMF data types processed:
  - 30 Common A.S. Work: Subtypes 1 (Initiation) and 5 (Termination)
  - 80 RACF processing
  - 81 RACF initialization
  - 83 RACF Audit - Subtypes 1 (Dataset SECLABEL), 2 (EIM), 3 (LDAP), 4 (R-auditx), 5 (WebSphere), 6 (TKLM)

- Executed as user exits to the SMF dump programs IFASMFDP and IFASMFDL

- Reference: RACF Auditor's Guide

IRRADU00 - RACF SMF Data Unload Utility

```
//SMFUNLD  JOB (001),'HANSEL RS',CLASS=A,NOTIFY=&SYSUID
//STEP0001 EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//DUMPIN   DD DSN=SMF.MONTHLY.RACF.DUMP.ARCHIVE,DISP=SHR            <- Input SMF data
//DUMPOUT  DD DUMMY
//ADUPRINT DD SYSOUT=*                                             <- Messages
//XMLFORM  DD DSN=RSH.SMF.XMLFORM,DISP=(NEW,CATLG,DELETE),         <- XML #1
//            SPACE=(CYL,(100,10),RLSE),UNIT=SYSDA,DCB=(LRECL=12288,RECFM=VB)
//XMLOUT   DD DSN=RSH.SMF.XMLOUT,DISP=(NEW,CATLG,DELETE),          <- XML #2
//            SPACE=(CYL,(100,10),RLSE),UNIT=SYSDA,DCB=(LRECL=12288,RECFM=VB)
//OUTDD    DD DSN=RSH.SMF.UNLOAD,DISP=(NEW,CATLG,DELETE),          <- Text
//            SPACE=(CYL,(100,10),RLSE),UNIT=SYSDA,DCB=(LRECL=12288,RECFM=VB)
//SYSIN    DD *
   ABEND(NORETRY)
   USER2(IRRADU00)                                                 <- SMF Unload
   USER3(IRRADU86)                                                 <- SMF Unload
```

- Only one form of SMF unload output will be generated
- Output DDs are processed in sequence: (1) XMLFORM, (2) XMLOUT, (3) OUTDD
- First DD found in above sequence will be the output type generated
- Unloads the entire DUMPIN dataset - no selection criteria

IRRADU00 - RACF SMF Data Unload Utility

- Unload records
  - Commands and events are translated into text format, example:
    - ACCESS - Resource access
    - ADDUSER - ADDUSER command
  - Event Codes are decoded into 8-character strings, examples:
    - INVPSWD - Invalid password
    - REVKUSER - User has been revoked
  - XML format - includes <> tags for each field
    - XMLOUT - One line per event
    - XMLFORM - One line per tagged element

```
ACCESS  SUCCESS 16:43:00 1999-06-24 SYSA NO  NO  NO ONORATO SYSP  YES …
ACCESS  SUCCESS 16:43:01 1999-06-24 SYSA NO  NO  NO ONORATO SYSP  YES …
ACCESS  SUCCESS 16:43:01 1999-06-24 SYSA NO  NO  NO ONORATO SYSP  YES …
ACCESS  SUCCESS 16:43:01 1999-06-24 SYSA NO  NO  NO ONORATO SYSP  YES …
ACCESS  SUCCESS 16:43:02 1999-06-24 SYSA NO  NO  NO ONORATO SYSP  YES …
```

- Record Layout Reference: RACF Macros and Interfaces Guide

Unsupported Utilities

- Various programs provided “as is” with no formal support
- Available via the 'Downloads' link in the 'Resources' tab on the RACF webpage at www.ibm.com/racf
- Examples:
  - CDT2DYN - Convert installation ICHRRCDE defined classes to Dynamic CDT profiles
  - CUTPWHIS - Remove old password history entries (Obsolete with APAR AO43999)
  - DBSYNC - Builds RACF commands to synchronize databases
  - irrhsfu - C program to unload HFS FSPs, like IRRDBU00
  - IRRXUTIL - REXX programs using the IRRXUTIL R_admin callable service interface
  - PWDCOPY - Copy cyphered passwords between RACF data bases
  - RACFDB2 - Migrate DB2 access controls to RACF profiles
  - RACKILL - Unconditionally deletes profiles
- Detailed instructions included with each utility on website