# *RACF Utilities for Auditors*

**Mark Nelson, CISSP**

**z/OS Security Server (RACF) Design and Development**
**IBM Corporation**
**2455 South Road**
**Department BWVA Mail Station P388**
**Poughkeepsie, NY  12601**

**RACF- 2003**
**Session 84**
**July, 2003**

**Phone:  (845) 435-7758**
**Internet:  markan@us.ibm.com**

# RACF Utilities for Auditors

## Trademarks

- These terms are trademarks of the IBM Corporation in the United States, other countries, or both:
  - DB2
  - DFSORT
  - IBM
  - OS/390
  - RACF
  - SQL/DS
  - S/390
  - z/OS
- SAS is a trademark of the SAS Institute, Inc.
- UNIX is a registered trademark in the United States, other countries, or both and is licensed exclusively through X/Open Company Limited.

# RACF Utilities for Auditors

## Agenda

- What is Auditing?
- RACF Cross Reference Utility (IRRUT100)
- RACF Database Unload Utility (IRRDBU00)
- RACF Remove ID Utility (IRRRID00)
- RACF Report Writer (RACFRW)
- RACF SMF Data Unload Utility (IRRADU00)
- Summary
- Questions

# RACF Utilities for Auditors

## What is Auditing?

- **Verification of compliance with the Installation Security Policy, by examining:**
  - Procedures and policies
  - Access rules
  - Physical access
  - User identification
  - Event data
    - **Looking at both successful (allowed) and unsuccessful (denied) events, looking for patterns**
  - Etc.

## RACF Cross Reference Utility (IRRUT100)

- **Searches live RACF database looking for references to user IDs and group IDs that you specify**
  - Standard and conditional access lists
  - NOTIFY, OWNER
  - Data set high level qualifiers
- **Results are limited to your scope of authority**
  - System SPECIAL/AUDITOR sees all
  - Group-SPECIAL/AUDITOR yields those references that are within the scope of authority of the group
  - Users can see references to their own user profile
- **Uses**
  - Find references to a known ID
    - ID deletion
    - ID reassignment

# RACF Utilities for Auditors

## IRRUT100 Invocation

```
//JOBNAME  JOB  JOB CARD. . . . . .
//IRRUT100 EXEC PGM=IRRUT100
//SYSUT1   DD   UNIT=SYSDA,SPACE=(TRK,(5,1))
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
  MARKN
/*
```

# RACF Utilities for Auditors

## IRRUT100 Output

**Occurrence of IBMUSER**

**in standard access list of general resource profile TSOAUTH  TESTAUTH**
**In standard access list of general resource profile GTERMINL  TGROUP**
**In notify field of general resource profile TERMINAL TRM$NOTE**
**Owner of SECLABEL SYSNONE**
**Owner of SECLABEL SYSLOW**
**Owner of SECLABEL SYSHIGH**
**Owner of connect profile MARKN/SYS1**
**Owner of connect profile IBMUSER/VSAMDSET**
**Owner of connect profile IBMUSER/SYS1**
**Owner of connect profile IBMUSER/SYSCTLG**
**In access list of group VSAMDSET**
**Owner of group VSAMDSET**
**In access list of group SYS1**
**Owner of group SYS1**
**In access list of group SYSCTLG**
**Owner of user MARKN**
**Owner of user IBMUSER**
**User entry exists**

## IRRUT100 Notes

### Note that IRRRUT100:

- Works only with the current RACF database
- Reads each profile in the RACF database to find a reference causing record-level serialization
- Doesn't search resource names, other than data set HLQ

# RACF Utilities for Auditors

## When to Use IRRUT100

- When you know exactly what IDs you are interested in
- When you need to see the absolutely most current data
- When the impact of running the utility is small

# RACF Utilities for Auditors

## RACF Database Unload Utility (IRRDBU00)

- Decomposes a restructured RACF database into a set of "flat" records
- Suitable for up-loading to a relational data manager, such as DB2
- Uses either an active (primary or back-up) RACF database or a copy
- Requires UPDATE to the input RACF database to execute

## How is Database Unload Used?

- Output loaded to a data manager
- Query manager used to create reports

# RACF Utilities for Auditors

## IRRDBU00 Record Formats

- **Relational representation of the RACF database, suitable for a DBMS load utility**
- **Conventions used in unloading the data:**
  - All fields unloaded, with the exception of encrypted and "reserved for IBM" fields
  - Fields decoded and presented in a readable format
    - **Example: UACC is output as "READ," "UPDATE," "ALTER," or "CONTROL" rather than as a binary field**
  - One record type per segment and per repeat group
    - **Identified by a 4 byte record type**
  - Each record contains a "name" field which identifies the profile being described

# RACF Utilities for Auditors

## IRRDBU00 Record Formats: Example

- Records which define user IDs look like:

| Record ID | User ID | Created | Owner | ADSP | Special | Operations | Revoked | GRPACC | PWD INT |
|---|---|---|---|---|---|---|---|---|---|
| 0200 | MARKN | 1997-07-03 | SYSADMIN | NO | YES | YES | NO | NO | 030 ... |
| 0200 | SMITH | 1996-04-25 | IBMUSER | NO | YES | YES | YES | NO | 030 ... |
| 0200 | WOLENSKY | 1997-03-03 | MARKN | NO | NO | NO | NO | NO | 030 ... |

# RACF Utilities for Auditors

## IRRDBU00 Invocation

- If your database is split, can process all parts or each part separately
- Uses the enhanced generic naming (EGN) setting and class descriptor table (CDT) from the execution system.
- Sample JCL

```
//USERX      JOB  Job card. . .
//UNLOAD     EXEC PGM=IRRDBU00,PARM=NOLOCK
//INDD1      DD   DISP=SHR, DSN=SYS1.RACFDB.PART1.COPY
//OUTDD      DD   DISP=SHR, DSN=SYS1.RACFDB.FLATFILE
//SYSPRINT   DD   SYSOUT=*
```

# RACF Utilities for Auditors

## When to Use IRRDBU00

- When you want to create tailored reports on your RACF user, group, and access control definitions
- When you want to perform a detailed analysis of the contents of the RACF database
- When working with an off-loaded copy of the RACF data is OK

## RACF Remove ID Utility (IRRRID00)

- A RACF utility which finds references to IDs and creates the commands to remove those references
- Uses the output of the RACF Database Unload Utility (IRRDBU00) as input, not the RACF database
- You can supply a list of IDs to search for. If you don't, IRRRID00 searches for all "residual" IDs
- Created commands must be reviewed and edited if necessary
- Requires READ authority to the IRRDBU00 output to create commands
- Normal RACF authorities required to execute the commands that are created

# RACF Utilities for Auditors

## IRRRID00 Invocation

```
//JOBNAME    JOB   Job  Card.....
//STEP1      EXEC  PGM=IRRRID00
//SYSPRINT   DD    SYSOUT=*
//SYSOUT     DD    SYSOUT=*
//SORTOUT    DD    UNIT=SYSALLDA,SPACE=(CYL,(5,5))
//SYSUT1     DD    UNIT=SYSALLDA,SPACE=(CYL,(3,5))
//INDD       DD    DISP=OLD,DSN=USER01.IRRDBU00.DATA
//OUTDD      DD    DISP=OLD,DSN=USER01.IRRRID00.CLIST
//SYSIN      DD    DUMMY No SYSIN data requests a residual search
```

# RACF Utilities for Auditors

## IRRRID00 Command Output

```
/*********************************************************************/
/*                                                                   */
/* The RACF Remove ID Utility (IRRRID00) was executed on             */
/* 2003-03-15 at 09:00:01.                                           */
/*                                                                   */
/* This file contains RACF commands that can be used to              */
/* identify references to user IDs and group IDs.  Residual          */
/* references on an access list are deleted with the PERMIT          */
/* command.  For all other references, commands are created to       */
/* change the reference to another value.  The default value         */
/* is ?id.  This allows all references to a particular ID to         */
/* be easily changed to another value using a text editor.           */
/*                                                                   */
/*********************************************************************/


/*********************************************************************/
/*                                                                   */
/* The INDD data set has been scanned for all names that do          */
/* not have a user or group id defined for them in INDD.  This       */
/* list of names has been formatted and sorted into the              */
/* SORTOUT data set.                                                 */
/*********************************************************************/
```

## IRRRID00 Command Output (Continued)

```
 CONNECT BILL     GROUP(RACFDEV )     OWNER(?MARKN   )
 ALTDSD 'DASDDEF.VCE313S'   GENERIC   OWNER(?MARKN   )
 PERMIT      D12*     CLASS(DASDVOL )  ID(MARKN   ) DELETE
 PERMIT      111111   CLASS(DASDVOL  )  ID(MARKN   ) DELETE
 PERMIT      22222    CLASS(DASDVOL  )  ID(BRUCE   ) DELETE
/*********************************************************************/
/*  The following commands delete profiles.  You must review         */
/*  these commands, editing them if necessary, and then remove       */
/*  the EXIT statement to allow the execution of the commands.       */
/*********************************************************************/

 EXIT
 DELDSD 'D69A.BRUCE.TEXT'  VOLUME(TS0018)  NOSET
 DELDSD 'D69A.MARKN.*'
/*********************************************************************/
/*  IRRRID00 has successfully completed                              */
/*********************************************************************/
```

# RACF Utilities for Auditors

## IRRRID00 SYSPRINT

```
IRR680011 No IDs were found in the SYSIN data set.  A search for all
residual references is being performed.
IRR68019I IRRRID00 has searched 10000 records and processed 0 records.
IRR68019I IRRRID00 has searched 20000 records and processed 0 records.
IRR68019I IRRRID00 has searched 30000 records and processed 0 records.
IRR68019I IRRRID00 has searched 40000 records and processed 0 records.
IRR68019I IRRRID00 has searched 50000 records and processed 0 records.
IRR68019I IRRRID00 has searched 60000 records and processed 0 records.
IRR68019I IRRRID00 has searched 70000 records and processed 0 records.
IRR68019I IRRRID00 has searched 80000 records and processed 0 records.
IRR68019I IRRRID00 has searched 84907 records and processed 0 records.
IRR68019I IRRRID00 has searched 84907 records and processed 10000 records.
IRR68019I IRRRID00 has searched 84907 records and processed 20000 records.
IRR68019I IRRRID00 has searched 84907 records and processed 30000 records.
IRR68019I IRRRID00 has searched 84907 records and processed 40000 records.
IRR68019I IRRRID00 has searched 84907 records and processed 50000 records.
IRR68019I IRRRID00 has searched 84907 records and processed 60000 records.
IRR68019I IRRRID00 has searched 84907 records and processed 70000 records.
IRR68019I IRRRID00 has searched 84907 records and processed 80000 records.
IRR68019I IRRRID00 has searched 84907 records and processed 84907 records.
IRR68004I IRRRID00 found 3734 references
IRR68011I The utility has successfully completed.
```

# RACF Utilities for Auditors

## When to Use IRRRID00

- When you want to "clean-up" your RACF database and remove residual authorities
- When you want to find and remove the authorities of an ID
- When you want to change the ownership of RACF profiles

# RACF Utilities for Auditors

## Agenda

- What is Auditing?
- RACF Cross Reference Utility (IRRUT100)
- RACF Data Base Unload Utility (IRRDBU00)
- RACF Remove ID Utility (IRRRID00)
- **RACF Report Writer (RACFRW)**
- RACF SMF Data Unload Utility (IRRADU00)
- Summary
- Questions

## RACF Report Writer (RACFRW)

- **Create reports and summary statistics from the security-relevant SMF data**
- **Three phase process:**
  1. Command and subcommand processing
  2. Record selection
  3. Report generation
- **Process SMF type 20 (job initiation) type 30 (common address work data) type 80 (access events) type 81 (RACF initialization) type 83 (data sets affected by SECLABEL)**
- **Requires READ authority to the SMF data**
- **Functionally stabilized at the RACF 1.9.2 level**

## When to Use RACFRW

- When you want to look at single events
- When your selection criteria is simple (time, User ID, Group ID, system name, event type)

# RACF SMF Data Unload Utility (IRRADU00)

## What is the SMF Data Unload Utility?

- **A RACF utility that translates the security relevant audit information into a set of records that can be imported to a relational data base management system, such as SQL/DS, DB2 or SAS.**
  - One record type per event type
  - Processes SMF type 30, 80, 81, and 83 records
- **Primary users are the system auditor and security administrator**
- **Requires READ authority to the SMF data**

# RACF Utilities for Auditors

## What is the Rationale Behind SMF Data Unload?

- **Auditors traditionally focus on "failure" events; The majority of data fraud is done by people authorized to the data and functions that are the targets of the fraud**
- **Analysis of security audit data is a semi-structured problem; Auditors require advanced data analysis tools.**
- **Existing reporting tools are insufficient key problems:**
  - Lack of record selectivity
  - Lack of tailor-ability of report format
  - Non-standard nature of analysis commands
- **Customers are writing their own SMF extract utilities**
- **Existing inquiry/analysis/reporting tools enjoy wide acceptance**
- **Every installation has at least one report generation/inquiry tool.**

## How is the Utility Invoked?

- **Invoked as exits to the SMF Dump Utility (IFASMFDP)**
  - RACF SMF Data Unload modules invoked through the **USER2** and **USER3** exit points
  - IFASMFDP can be used to provide data, time, system ID, and record type selection

```
//USERX    JOB   Job Card...
//UNLOAD   EXEC  PGM=IFASMFDP
//DUMPIN   DD    DISP=SHR,DSN=USER01.SMFDATA
//DUMPOUT  DD    DUMMY
//OUTDD    DD    DISP=SHR,DSN=USER01.SMFDATA.IRRRID00
//SYSPRINT DD    SYSOUT=*
//ADUPRINT DD    SYSOUT=*
//SYSIN    DD    *
     USER2(IRRADU00)  USER3(IRRADU86)
     DATE (99001,99123)
     START (0800)
     END(1700)
     SID(SYS1)
/*
```

# RACF Utilities for Auditors

## What Does the Utility Produce?

- **Relational representation of the security relevant audit data, suitable for export to a relation data base management system (RDBMS) or browsing**
- **One record type per event code**

| | |
|---|---|
| **ACCESS** | Resource access |
| **ADDSD** | ADDSD command |
| **ADDUSER** | ADDUSER Command |
| **CONNECT** | Connect a user to a group |
| **DELRES** | Delete resource |
| **DELVOL** | Delete volume |
| **DEFINE** | Define resource |
| **JOBINIT** | Job initiation |
| **RENAMEDS** | Rename dataset |
| **.....** | Etc. |

## What Does the Utility Produce (Continued)?

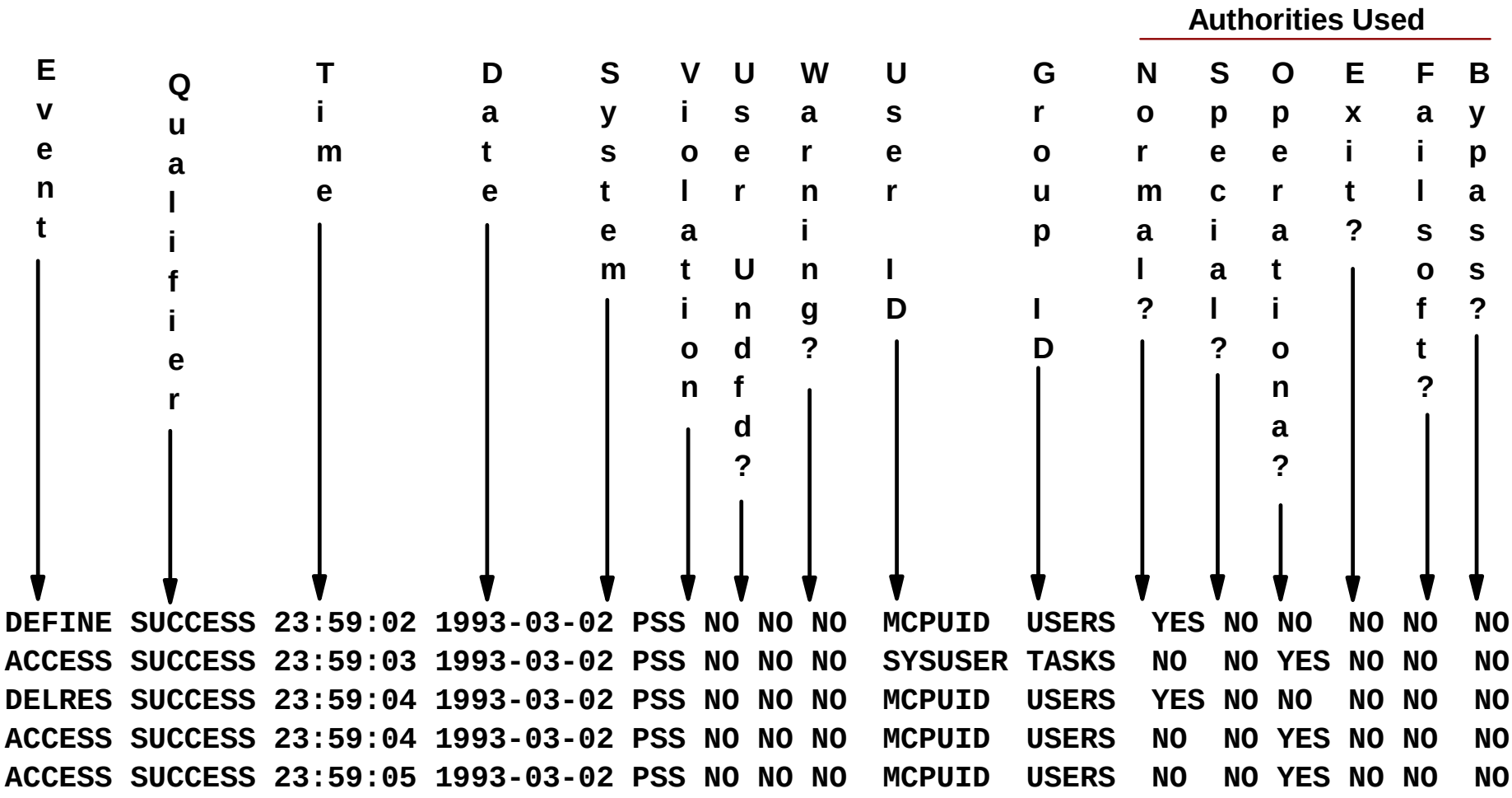
- All data decoded
- Commands translated into command text format
- Event code qualifiers decoded into meaningful eight byte values

| | |
|---|---|
| **INVPSWD** | Not valid password |
| **INVTERM** | Not valid terminal |
| **NASECL** | Not authorized to SECLABEL |
| **NJENAUTH** | NJE job not authorized |
| **.....** | Etc. |

# RACF Utilities for Auditors

## Record Formats

- All records of a specific event code are identical
- Base portion of all Type 80-based records are identical



# RACF Utilities for Auditors

## A Sample Query

- Find all of the data set accesses made to data sets whose name begins with "PAYROLL." that were made before 8:00 AM and after 4:59 PM. Ignore all of the requests made by the user OPERBKUP.

```
SELECT
     *
FROM
     USER01.ACCESS
WHERE
     (HOUR(SMF80_TIME_WRITTEN)<8 OR HOUR(SMF80_TIME_WRITTEN)>16)
     AND
     SMF80_EVT_USER_ID^= 'OPERBKUP'
     AND
     ACC_RES_NAME LIKE 'PAYROLL.%'
     ;
```

# When to Use IRRADU00

- When you have complex selection criteria
- When you want to create tailored reports
- When you want to look at trends of events

## What Samples are Shipped With RACF?

- **Sample JCL for:**
  - IRRDBU00
  - IRRADU00
  - IRRRID00
- **Sample SQL create tablespace and create table statements for IRRDBU00 and IRRADU00**
- **DBMS Load Utility control statements for DB2 Load Utility for IRRDBU00 and IRRADU00**
- **Sample queries for IRRADU00 and IRRDBU00 output**

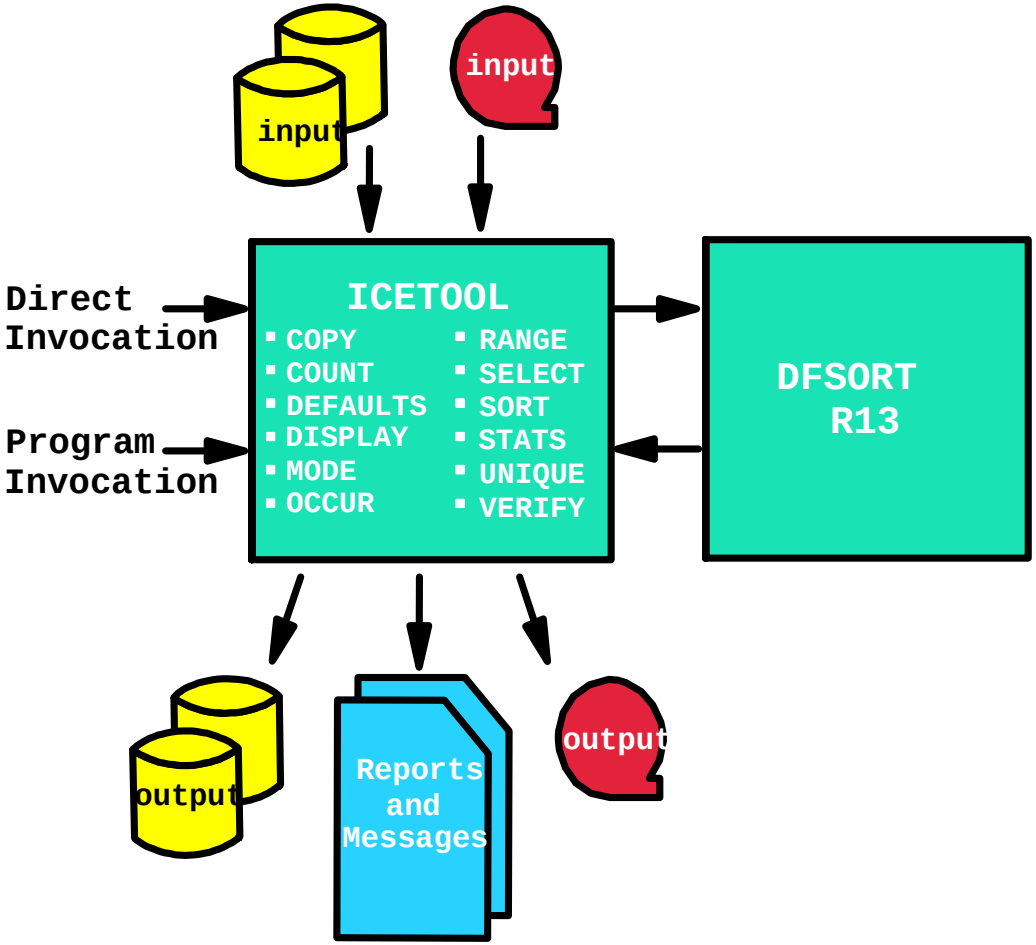
# RACF Utilities for Auditors

## Using the DFSORT™ ICETOOL Utility

- IBM's DFSORT product contains a simple yet powerful report generation tool, ICETOOL
- ICETOOL adds an easy-to-use reporting facility to DFSORT's powerful record selection and ordering capabilities
- ICETOOL can easily be used with RACF's SMF unload utility (IRRADU00) and database unload utility (IRRDBU00) output
- 30+ sample reports are shipped in 'SYS1.SAMPLIB(IRRICE)'
- May of these reports are available from in RACFICE package, which can be found on the RACF web page (http://www.ibm.com/servers/eserver/zseries/zos/racf/)

# RACF Utilities for Auditors

## DFSORT's ICETOOL Utility



## RACFICE and ICETOOL

- **All of the RACFICE Reports are created using only 3 of the 15 ICETOOL operators:**
  - **SORT/COPY**
    - Record ordering and selection
  - **DISPLAY**
    - Select input fields, create report and column headers, and specify output report format
  - **OCCURS**
    - Counts occurrences of values
    - Can be used to report counts over a specified threshold value

## Selecting Records Using DFSORT

- **Records are included in a report using DFSORT's INCLUDE statement:**

```
INCLUDE COND=((start,length,type,eval,value,AND|OR,
              start,length,type....)
```

  - `start` is the starting position
  - `length` is the length of the string being compared
  - `type` describes the data type
    - "CH" indicates character
    - "SS" indicates substring
  - `eval` is the type of comparison
    - "EQ" is equal
    - "NE" is not equal
    - "LT" is less than
    - "LE" is less than or equal to
    - "GT is greater than
    - "GE is greater than or equal to

## Sample RACFICE Report: SORT Keywords

```
SORT FIELDS=(10,8,CH,A)
INCLUDE COND=((44,1,CH,EQ,C'Y',OR,
               49,1,CH,EQ,C'Y',OR,
               390,1,CH,EQ,C'Y'),AND,
               5,4,CH,EQ,C'0200')
OPTION   VLSHRT
```

# RACF Utilities for Auditors

## Sample RACFICE Report: ICETOOL Keywords

```
*************************************************************************
* Name: UGLB                                                            *
*                                                                       *
* Find all of the user IDs which have extraordinary RACF privileges,    *
* such as SPECIAL, OPERATIONS, and AUDITOR at the global level.         *
*************************************************************************
 SORT    FROM(DBUDATA) TO(TEMP0001) USING(RACF)
 DISPLAY FROM(TEMP0001) LIST(PRINT) -
        PAGE -
        TITLE('User IDs With Extraordinary Global Authorities') -
        DATE(YMD/) -
        TIME(12:)  -
        BLANK -
        ON(10,8,CH)  HEADER('User ID') -
        ON(79,20,CH) HEADER('User Name') -
        ON(44,4,CH)  HEADER('Special') -
        ON(49,4,CH)  HEADER('Operations') -
        ON(390,4,CH) HEADER('Auditor')
```

# RACF Utilities for Auditors

## Sample RACFICE Report : JCL

```
//MARKNICE JOB 'M.NELSON P385',NOTIFY=&SYSUID,CLASS=A,
//         REGION=0M,MSGCLASS=H
//*-------------------------------------------------------------
//UNLOAD    EXEC PGM=IRRDBU00,PARM=NOLOCKINPUT
//SYSPRINT  DD SYSOUT=*
//INDD1     DD DISP=SHR,DSN=RACFDRVR.RACF260
//OUTDD     DD DISP=(NEW,PASS),SPACE=(CYL,(5,1)),UNIT=SYSALLDA,
//          LRECL=5096,RECFM=VB,BLKSIZE=0,DSN=USER01.IRRDBU00
//*-------------------------------------------------------------
//REPORT    EXEC PGM=ICETOOL
//TOOLMSG   DD DUMMY
//PRINT     DD SYSOUT=*
//DFSMSG    DD DUMMY
//DBUDATA   DD DISP=(SHR,DELETE),DSN=USER01.IRRDBU00
//TEMP0001  DD DISP=(NEW,DELETE),SPACE=(CYL,(5,1,0)),UNIT=SYSALLDA
//TOOLIN    DD *
 <icetool control statements>
//RACFCNTL  DD *
 <sort keywords>
```

# RACF Utilities for Auditors

## Sample RACFICE Report : Output

```
- 1 -          User IDs With Extraordinary Global Authorities          98/12/29

User ID    User Name                 Special   Operations   Auditor
--------   ----------------------    -------   ----------   -------
GLBAUDIT   ######################    NO        NO           YES
GLBOPER    ######################    NO        YES          NO
GLBSPEC    ######################    YES       NO           NO
IBMUSER                              YES       YES          YES
MARKN      ######################    YES       YES          YES
SPECUSR    ######################    YES       YES          YES
UAUDR$Y    AUDITOR                   NO        NO           YES
UOPER$Y    OPERATIONS                NO        YES          NO
USPEC$Y    SPECIAL                   YES       NO           NO
```

## Using the "substring" Conditional Test

- **DFSORT release 13 introduced the substring ("SS") comparison test, which indicates that a record is included if the selected value appears anywhere within the specified field**

```
INCLUDE COND=(10,44,CH,SS,"*")
```

  - selects any record in which the character "*" appears within columns 10 to 53

- **Consider this example:**

```
INCLUDE COND=(5,4,CH,EQ,C'0500',AND,
              266,4,CH,EQ,C'NO  ',AND,
                 (10,249,SS,EQ,C'*',OR,
                  10,249,SS,EQ,C'%',OR,
                  10,249,SS,EQ,C'&'))
```

  - Which finds all general resource profiles (record type '0500') which are not generic (record offset 266 contains 'NO') but have a generic character in the name (the "SS" operands)

## Using DFSORT Symbols

- DFSORT release 14 introduced the DFSORT SYMBOL, which can be used to replace fields (and constants) in DFSORT and ICETOOL statements with easy-to-read labels
  - USBD_OPER could be used as a symbol for 44,1,CH
- RACFICE contains DFSORT symbols for all of the IRRADU00 and IRRDBU00 fields.
- Using these symbols, you could specify these DFSORT statements:

```
SORT FIELDS=(USBD_NAME,A)
INCLUDE COND=(GRBD_RECORD_TYPE,EQ,C'0500',AND,
              GRBD_GENERIC,EQ,C'NO  ',AND,
                (GRBD_NAME,SS,EQ,C'*',OR,
                  GRBD_NAME,SS,EQ,C'%',OR,
                  GRBD_NAME,SS,EQ,C'&'))
```

# RACF Utilities for Auditors

## What Reports does RACFICE Contain?

- Users who have extraordinary global/goup RACF attributes
- Discrete data set/general resource profiles which contain generic characters
- Users who have more than 20 group connections
- Count of user/group/data set/general resource (by class) profiles
- User IDs with group privileges above USE
- Data set standard and general resources with a UACC of other than NONE
- Data set standard and conditional access lists with ID(*) of other than NONE
- General resource standard and conditional access lists with ID(*) of other than NONE
- Users who have explicit RRSF associations defined
- User IDs with an OMVS segment
- OS/390 UNIX super users (UID of zero)
- OS/390 UNIX UIDs which are used more than once
- HLQs with excessive generic profiles
- HLQs with excessive fully-qualified generic profiles
- User profiles defined in the past 90 days

# RACF Utilities for Auditors

## What Reports does RACFICE Contain?...

- Events associated with a specific user
- User IDs with excessive incorrect passwords
- Terminals with excessive incorrect passwords
- Accesses allowed due to WARNING mode profiles
- Accesses allowed because the user has OPERATIONS
- Users who are using Automatic Command Direction
- Users who are directing command explicitly
- User who log on with LOGON BY
- RACLINK audit records
- Users who are using password synchronization
- Access violations

# RACF Utilities for Auditors

## Where are These Utilities Documented?

- **RACF Cross Reference Utility (IRRUT100)**
  - RACF Security Administrator's Guide
- **RACF Database Unload Utility (IRRDBU00)**
  - RACF Security Administrator's Guide
  - RACF Macros and Interfaces
- **RACF Remove ID Utility (IRRRID00)**
  - RACF Security Administrator's Guide
- **RACF Data Security Monitor (DSMON)**
  - RACF Auditor's Guide
- **RACF Report Writer (RACFRW)**
  - RACF Auditor's Guide
- **RACF SMF Data Unload Utility (IRRADU00)**
  - RACF Auditor's Guide and RACF Macros and Interfaces
- **DFSORT  ICETOOL Utility**
  - DFSORT Application Programming Guide

# RACF Utilities for Auditors

## Summary

| Utility | Authority Required | Comments |
|---|---|---|
| IRRUT100 | • None, for own ID<br>• SPECIAL/AUDITOR or GROUP-SPECIAL/AUDITOR for other IDs | • Have to know the ID you're looking for<br>• Finds references, does not remove or create commands |
| IRRDBU00 | • UPDATE to the input RACF DB (may be a copy) | • Easy input to reporting tools for tailored reports and complex analysis |
| IRRRID00 | • READ to the IRRDBU00 output<br>• Authority to issue RACF commands | • Must review output prior before executing the generated commands |
| IRRADU00 | • READ to the SMF data | • Easy input to reporting tools for customized reports and complex analysis |

# RACF Utilities for Auditors

## Agenda

- What is Auditing?
- RACF Cross Reference Utility (IRRUT100)
- RACF Data Base Unload Utility (IRRDBU00)
- RACF Remove ID Utility (IRRRID00)
- RACF Report Writer (RACFRW)
- RACF SMF Data Unload Utility (IRRADU00)
- Summary
- **Questions**

# RACF Utilities for Auditors

## Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.