

### **RACF Utilities for Auditors**

RACF-2006 Session I8 July 2006

Mark Nelson, CISSP® z/OS® Security Server (RACF®) Design and Development IBM® Poughkeepsie markan@us.ibm.com

© 2005 IBM Corporation

### | IBM Systems and Technology Group

### **Trademarks**

- These terms are trademarks of the IBM Corporation in the United States, other countries, or both:
  - DB2
  - DFSORT
  - ▶ IBM
  - MVS
  - ▶ OS/390
  - **RACF**
  - > z/OS
- CISSP is a registered certification mark of the International Information Systems Security Certification Consortium, Inc.
- SAS is a trademark of the SAS Institute
- UNIX is a registered trademark in the United States, other countries, or both and is licensed exclusively through the X/Open Company Limited.

Agenda

What is Auditing?

RACF Cross Reference Utility (IRRUT100)

RACF Database Unload Utility (IRRDBU00)

RACF Remove ID Utility (IRRRID00)

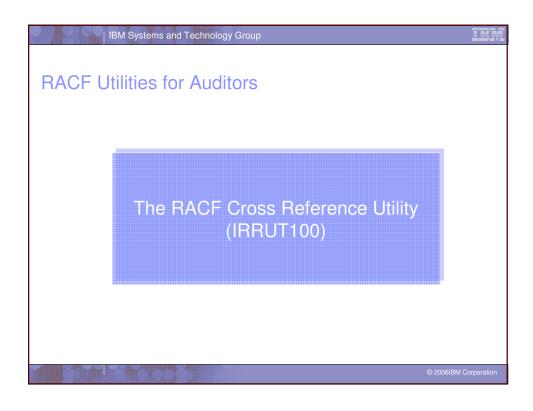
RACF Report Writer (RACFRW)

RACF SMF Data Unload Utility (IRRADU00)

Summary

Questions

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



### IBM Systems and Technology Group 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

```
IRRUT100 Invocation

//JOBNAME JOB JOB CARD.....

//IRRUT100 EXEC PGM=IRRUT100

//SYSUT1 DD UNIT=SYSDA, SPACE=(TRK, (5,1))

//SYSPRINT DD SYSOUT=*

//SYSIN DD *

MARKN

/*
```

```
IRRUT100 Output

Occurrences of MARKN

In standard access list of general resource profile SDSF ISFCMD.ODSP.READER.* (G) In standard access list of general resource profile SDSF ISFCMD.ODSP.PRINTER.* (G) In notify field of general resource profile JESSPOOL &RACLNDE.MARKN.** (G) Owner of JESSPOOL &RACLNDE.MARKN.** (G) In standard access list of general resource profile ACCTNUM 263680 In standard access list of general resource profile ACCTNUM 263680 In standard access list of dataset profile USER01.RACFICE.* (G) Owner of connect profile GENEK/RACFWWW Owner of connect profile GENEK/RACFWWW Owner of connect profile DECKERC/RACFWWW Owner of group RACFWWW Owner of group RACFWWW Owner of group RACFWWW In access list of group BWDA In access list of group $D09A User entry exists
```

### Notes on Using IRRUT100 Note that IRRUT100: Note that IRRUT100: Note that IRRUT100: Reads each profile in the 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

# When to Use IRRUT100 • When should you 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

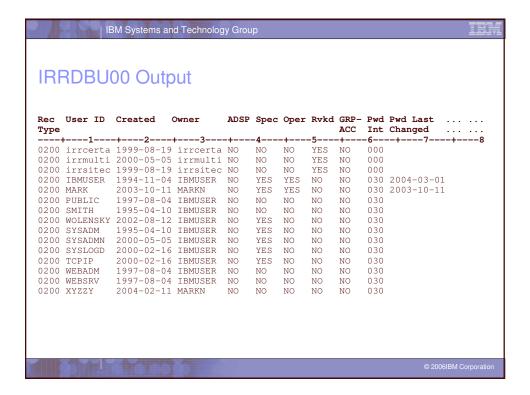
# RACF Utilities for Auditors The RACF Database Unload Utility (IRRDBU00)

## RACF Database Unload Utility (IRRDBU00) What does the RACF Database Unload Utility do? Decomposes a restructured RACF database into a set of "flat" records Suitable for viewing using an editor, reporting using DFSORT or equivalent, or up-loading to a relational data manager, such as DB2 Uses either an active (primary or back-up) RACF database or a copy IRRDBU00 requires UPDATE to the input RACF database

### **IRRDBU00** Record Format

- 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

© 2006IBM Corporation



7

```
IRRDBU00 Invocation

//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=*
```

### **IRRDBU00 Notes**

- The RACF Certificate 'anchor IDs' are unloaded.
- If you are processing your data using DFSORT or DB2, you must add the length of the record descriptor word (4) to each of the field offsets.
- 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.
- IRRDBU00 does not interpret the data in the data base.
- Three PARM= values are supported:
  - > PARM=LOCK, which locks the input database until the utility finishes unloading
  - PARM=UNLOAD, which unlocks the input database and does not unload any records
  - > PARM=NOLOCK, which unloads the input database without locking

### When to Use IRRDBU00 • Use IRRDBU00 when: • You want to create tailored reports on your RACF user, group, and access control definitions, • You want to perform a detailed analysis of the contents of the RACF database, or when • Working with an off-loaded copy of the RACF data is OK.



### The 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

© 2006IBM Corporation

IBM Systems and Technology Group

IIM

### **IRRRID00** Invocation

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

```
| IBM Systems and Technology Group
IRRRID00 Output
                GROUP (RACFDEV )
                                  OWNER (?MARKN
        'DASDDEF.VCE313S' GENERIC OWNER(?MARKN
ALTDSD
                   CLASS (DASDVOL ) ID (MARKN ) DELETE
                                           ) DELETE
 PERMIT
           111111 CLASS (DASDVOL ) ID (MARKN
 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.
DELDSD 'D69A.BRUCE.TEXT' VOLUME (TS0018) NOSET
DELDSD 'D69A MARKN *'
/* IRRRID00 has successfully completed
```

```
IBM Systems and Technology Group
IRRRID00 Messages to 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
```

## When to Use IRRRID00? When should you 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

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

### IBM Systems and Technology Group The RACF Report Writer (RACFRW) What is the RACF Report Writer? A RACF utility which creates reports and summary statistics from the security-relevant SMF data Three phase process: Command and subcommand processing Record selection 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 Only 'basic information is presented for UNIX Systems Services events

# When to use the RACF Report Writer • When should you use the RACF Report Writer? • 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 RACF 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

© 2006IBM Corporation

IBM Systems and Technology Group



### Rationale for IRRADU00

- 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 are:
  - 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.

### What does IRRADU00 Produce?

- "Flat file" 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
- All data is decoded
- Commands are translated into command format
- Event codes and event code qualifiers have meaningful values:
  - ACCESS for resource access, JOBINIT for logon, job initiation, ADDUSER, ALTUSER, DELUSER, etc. for the RACF commands
  - SUCCESS for success, INVPSWD for incorrect password, etc.

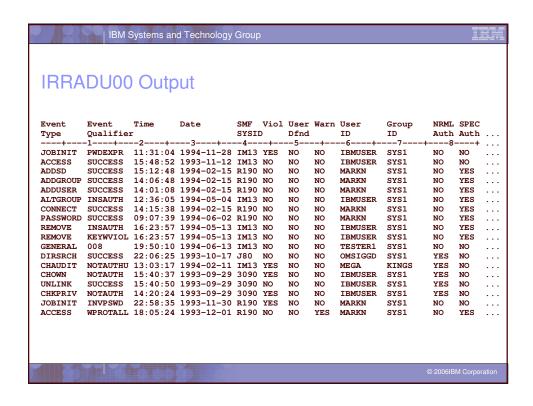
```
IBM Systems and Technology Group
Invoking IRRADU00
     //USERX
                 JOB
                       Job Card...
     //UNLOAD EXEC PGM=IFASMFDP
//DUMPIN DD DISP=SHR,DSN
//DUMPOUT DD DUMMY
                        DISP=SHR, DSN=USER01.SMFDATA
     //OUTDD DD DISP=SHR, DSN=USER01.SMFDATA.IRRRID00
     //SYSPRINT DD
                       SYSOUT=*
                        SYSOUT=*
     //ADUPRINT DD
     //SYSIN
                        DD
       USER2 (IRRADU00)
                           USER3 (IRRADU86)
       DATE (2004001, 2004123)
       START (0800)
       END (1700)
       SID (SYS1)
```

### IBI

### Notes on Invoking IRRADU00

- 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
  - Can be executed against off-line copies of your SMF data or your live SMF data set
    - Note that SMF buffers records before writing them

© 2006IBM Corporation



17

### Notes on IRRADU00 Output

- Base portion (colums 1-282) are the same for all RACF type 80 records.
- If you are processing your data using DFSORT or DB2, you must add the length of the record descriptor word (4) to each of the field offsets.
- "Unknown" event code and event code qualifiers are unloaded as numeric values.

© 2006IBM Corporation

IBM Systems and Technology Group

### IEM

### Using DB2 to Process IRRADU00 Data

- Loading IRRADU00 data to DB2 provides a robust data mining environment for your log data.
- Example: 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 should you 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 DFSORT's ICETOOL 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 IRRADU00 Sample queries for IRRADU00 and IRRADU00



### 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 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

© 2006IBM Corporation

### | IBM Systems and Technology Group

### Selecting Records Using ICETOOL

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

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

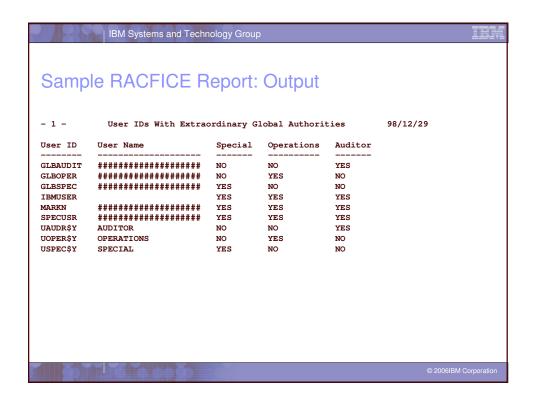
```
Sample RACFICE Report: SORT Keywords

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
```

```
| IBM Systems and Technology Group
Sample RACFICE Report: ICETOOL Keywords
* Name: UGLB
\star Find all of the user IDs which have extraordinary RACF privileges,
* such as SPECIAL, OPERATIONS, and AUDITOR at the global level.
        FROM (DBUDATA) TO (TEMP0001) USING (RACF)
 SORT
 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')
```

```
IBM Systems and Technology Group
Sample RACFICE Report: JCL Keywords
//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 *
```



### Using the DFSORT 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:

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)

© 2006IBM Corporation

IBM Systems and Technology Group

### 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 can specify:

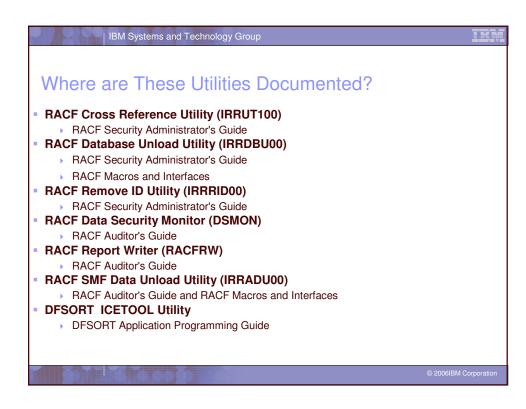
```
SORT FIELDS=(USBD_NAME, A)

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'&'))
```

### IBM Systems and Technology Group What RACF DB Reports Are in RACFICE? 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 **UNIX System Services super users (UID of zero)** UNIX Systen Services 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

### What SMF RACFICE Reports are in RACFICE? 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

IBM Systems and Technology Group



Jtility	Authority Required	Comments
RRUT100	None for own ID SPECIAL/AUDITOR or GROUP- SPECIAL/AUDITOR for other IDs	Have to know the ID your looking for Finds references, does not remove or create commands
IRRDBU00	Update to the input RACF DB (may be a copy)	Easy input to report tools for tailored reports and complex analysis
IRRRID00	Read input to	Must review output before executing the generated commands
IRRADU00	Read to the input SMF data	Easy input to report tools for tailored reports and complex analysis

### 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

© 2006IBM Corporation

IBM Systems and Technology Group



### 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.