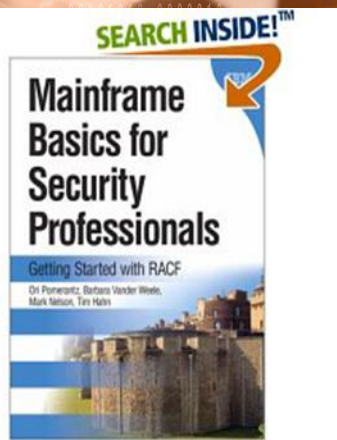


# VANGUARD

## SECURITY & COMPLIANCE CONFERENCE 2016

### Session BTB8 – RACF Utilities for Auditors® (and Friends!)



Mark Nelson, CISSP®, CISSLP®  
markn@us.ibm.com

IBM®

# 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)**
- **RACF Health Checks**
- **Summary**

# 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**
  
- **Does your security policy cover the proper configuration of the operating system?**

# Vanguard Integrity Professionals Critical Assessment Findings in Mainframe Environments

<b>%</b>	<b>Misconfiguration</b>	<b>Impact</b>
75%	Excessive Number of User ID's with no Password Interval	Severe
61%	Inappropriate Usage of z/OS UNIX Superuser Privilege, UID = 0	Severe
54%	Improper Use or Lack of UNIXPRIV Profiles	High
54%	Sensitive Data Sets with UACC Greater than NONE	High
54%	Critical Data Sets with UACC Greater than READ	Severe
53%	Started Task IDs are not Defined as PROTECTED IDs	High
47%	Excessive Access to the SMF Data Sets	High
46%	Excessive Access to APF Libraries	Severe
46%	Excessive Access to z/OS UNIX File System Data Sets	High
40%	RACF Database is not Adequately Protected	Severe

# RACF Utilities for Auditors

The RACF Cross Reference Utility  
(IRRUT100)

# 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.PUNCH.* (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 dataset profile USER01.RACFICE.* (G)
Owner of connect profile JAYMON/RACFWWW
Owner of connect profile GENEK/RACFWWW
Owner of connect profile DECKERC/RACFWWW
In access list of group WEBDEV
In access list of group RACFWWW
Owner of group RACFWWW
In access list of group BWVA
In access list of group $D09A
User entry exists
```



# Notes on Using IRRUT100

- **Note that IRRUT100:**

- ▶ 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

## 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
  
- **Authorization required**
  - ▶ **Pre z/OS V2.2: UPDATE to the input RACF database**
  - ▶ **z/OS V2.2 and later: READ if PARM=NOLOCKINPUT specified, UPDATE otherwise**

# 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

# IRRDBU00 Output

Rec Type	User ID	Created	Owner	ADSP	Spec	Oper	Rvkd	GRP- ACC	Pwd Int	Pwd Last Changed	...	...
-----1-----	-----2-----	-----3-----	-----4-----	-----5-----	-----6-----	-----7-----	-----8-----					
0200	irrcerta	1999-08-19	irrcerta	NO	NO	NO	YES	NO	000			
0200	irrmulti	2000-05-05	irrmulti	NO	NO	NO	YES	NO	000			
0200	irrsitec	1999-08-19	irrsitec	NO	NO	NO	YES	NO	000			
0200	IBMUSER	1994-11-04	IBMUSER	NO	YES	YES	NO	NO	030	2004-03-01		
0200	MARK	2003-10-11	MARKN	NO	YES	YES	NO	NO	030	2003-10-11		
0200	PUBLIC	1997-08-04	IBMUSER	NO	NO	NO	NO	NO	030			
0200	SMITH	1995-04-10	IBMUSER	NO	NO	NO	NO	NO	030			
0200	WOLENSKY	2002-08-12	IBMUSER	NO	YES	NO	NO	NO	030			
0200	SYSADM	1995-04-10	IBMUSER	NO	YES	NO	NO	NO	030			
0200	SYSADMN	2000-05-05	IBMUSER	NO	YES	NO	NO	NO	030			
0200	SYSLOGD	2000-02-16	IBMUSER	NO	YES	NO	NO	NO	030			
0200	TCPIP	2000-02-16	IBMUSER	NO	YES	NO	NO	NO	030			
0200	WEBADM	1997-08-04	IBMUSER	NO	NO	NO	NO	NO	030			
0200	WEBSRV	1997-08-04	IBMUSER	NO	NO	NO	NO	NO	030			
0200	XYZZY	2004-02-11	MARKN	NO	NO	NO	NO	NO	030			

# 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=UNLOCK, 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.

# RACF Utilities for Auditors

The RACF Remove ID Utility  
(IRRRID00)

## 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**

# 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
```

# IRRRID00 Output

```

/*****
/*
/* The RACF Remove ID Utility (IRRRID00) was executed on
/* 2007-03-15 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 Output

```
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                                */
/*****/
```

# 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**

# 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 Utilities for Auditors

The RACF SMF Unload Utility  
(IRRADU00)

# 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

## 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.

# Invoking IRRADU00

```
//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 (2004001,2004123)
      START (0800)
      END (1700)
      SID (SYS1)
/*
```



## Notes on Invoking IRRADU00

- **Invoked as exits to the SMF Dump Utility (IFASMFDP/IFASMFDL)**

- ▶ RACF SMF Data Unload modules invoked through the USER2 and USER3 exit points
- ▶ IFASMFDP/IFASMFDL 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

# IRRADU00 Output

Event Type	Event Qualifier	Time	Date	SMF SYSID	Viol	User Dfnd	Warn	User ID	Group ID	NRML Auth	SPEC Auth	...
----	1-----	2-----	3-----	4-----	5-----	6-----	7-----	8-----	9-----	10-----	11-----	12-----
JOBINIT	PWDEXPR	11:31:04	1994-11-28	IM13	YES	NO	NO	IBMUSER	SYS1	NO	NO	...
ACCESS	SUCCESS	15:48:52	1993-11-12	IM13	NO	NO	NO	IBMUSER	SYS1	NO	NO	...
ADDS	SUCCESS	15:12:48	1994-02-15	R190	NO	NO	NO	MARKN	SYS1	NO	YES	...
ADDGROUP	SUCCESS	14:06:48	1994-02-15	R190	NO	NO	NO	MARKN	SYS1	NO	YES	...
ADDUSER	SUCCESS	14:01:08	1994-02-15	R190	NO	NO	NO	MARKN	SYS1	NO	YES	...
ALTGROUP	INSAUTH	12:36:05	1994-05-04	IM13	NO	NO	NO	IBMUSER	SYS1	NO	YES	...
CONNECT	SUCCESS	14:15:38	1994-02-15	R190	NO	NO	NO	MARKN	SYS1	NO	YES	...
PASSWORD	SUCCESS	09:07:39	1994-06-02	R190	NO	NO	NO	MARKN	SYS1	NO	YES	...
REMOVE	INSAUTH	16:23:57	1994-05-13	IM13	NO	NO	NO	IBMUSER	SYS1	NO	YES	...
REMOVE	KEYWVIOL	16:23:57	1994-05-13	IM13	NO	NO	NO	IBMUSER	SYS1	NO	YES	...
GENERAL	008	19:50:10	1994-06-13	IM13	NO	NO	NO	TESTER1	SYS1	NO	NO	...
DIRSRCH	SUCCESS	22:06:25	1993-10-17	J80	NO	NO	NO	OMSIGGD	SYS1	YES	NO	...
CHAUDIT	NOTAUTHU	13:03:17	1994-02-11	IM13	YES	NO	NO	MEGA	KINGS	YES	NO	...
CHOWN	NOTAUTH	15:40:37	1993-09-29	3090	YES	NO	NO	IBMUSER	SYS1	YES	NO	...
UNLINK	SUCCESS	15:40:50	1993-09-29	3090	NO	NO	NO	IBMUSER	SYS1	YES	NO	...
CHKPRIV	NOTAUTH	14:20:24	1993-09-29	3090	YES	NO	NO	IBMUSER	SYS1	YES	NO	...
JOBINIT	INVPSWD	22:58:35	1993-11-30	R190	YES	NO	NO	MARKN	SYS1	NO	NO	...
ACCESS	WPROTALL	18:05:24	1993-12-01	R190	NO	NO	YES	MARKN	SYS1	NO	YES	...

## Notes on IRRADU00 Output

- **Base portion (columns 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.**

## 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 IRRDBU00 output**

# RACF Utilities for Auditors

Using The DFSORT ICETOOL Utility

## 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)'**



## 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**

# 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

## 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
```

# 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')
```

# 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 *  
    <sort keywords>  
/*
```

# RACF Utilities for Auditors

**The IBM Health Checker for z/OS**

- **Starting with z/OS V1R7 (rolled back to z/OS V1R4), IBM introduced the IBM Health Checker for z/OS, an infrastructure for IBM and vendor “health checks”**
- **RACF contains a number of checks that are of interest to auditors:**
  - ▶ RACF\_SENSITIVE\_RESOURCES
  - ▶ RACF\_<class-name>\_ACTIVE
    - FACILITY, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, UNIXPRIV, CSFSERV/CSFKEYS (OA44496 for V2.1), JESJOBS/JESSPOOL (OA48174 for V2.1 and V2.2)
  - ▶ RACF\_IBMUSER\_REVOKED
  - ▶ RACF\_ICHAUTAB\_NONLPA
  - ▶ ... starting with z/OS V1R10, you can define your own check that validates resources of your choice!
  - ▶ RACF\_ENCRYPTION\_ALGORITHM (OA45608 for V2.1)
  - ▶ RACF\_PASSWORD\_CONTROLS (OA45606 for V2.1)
  - ▶ RACF\_BATCHALL\_RACF (OA48714 for V2.1 and V2.2)
- **You can define your own check that validates resources of your choice merely by defining RACF profiles and making a simple change to PARMLIB member HZSPRMxx**
- **Output easily viewable from SDSF**

## RACF Support for the IBM Health Checker for z/OS

- **The RACF\_SENSITIVE\_RESOURCES check:**
  - ▶ Looks at the current APF data sets, PARMLIB data sets, SYSREXX data set (V1R9 and later), ICSF CKDS, PKDS and TKDS (with OA44496 for V2.1) and the RACF database data sets and flags those that are improperly protected:
    - Are not found on the indicated volume
    - Are protected by a profile with:
      - a UACC greater than READ(APF) or NONE(RACF DB)
      - ID(\*) greater than READ (APF) or NONE(RACF DB)
      - WARNING mode set
    - No RACF profile and PROTECTALL(FAIL) not in effect
    - (Optional): Specified user ID has UPDATE(APF) or READ(RACFDB) or greater access
  - ▶ Looks for ICHAUTAB modules



# Getting into the IBM Health Checker for z/OS (SDSF)

Display Filter View Print Options Help

HQX7750 ----- SDSF PRIMARY OPTION MENU -----

DA	Active users	INIT	Initiators
I	Input queue	PR	Printers
O	Output queue	PUN	Punches
H	Held output queue	RDR	Readers
ST	Status of jobs	LINE	Lines
		NODE	Nodes
LOG	System log	SO	Spool offload
SR	System requests	SP	Spool volumes
MAS	Members in the MAS		
JC	Job classes	RM	Resource monitor
SE	Scheduling environments	CK	Health checker
RES	WLM resources		

Licensed Materials - Property of IBM

COMMAND INPUT ==> CK	SCROLL ==> PAGE				
F1=HELP	F2=SPLIT	F3=END	F4=RETURN	F5=IFIND	F6=BOOK
F7=UP	F8=DOWN	F9=SWAP	F10=LEFT	F11=RIGHT	F12=RETRIEVE

# Getting into the IBM Health Checker for z/OS (SDSF)

Display Filter View Print Options Help

```

-----
SDSF HEALTH CHECKER DISPLAY RACFR1A LINE 38-52 (96)
NP NAME CheckOwner State Status
IXGLOGR_STRUCTUREFULL IBMIXGLOGR ACTIVE(DISABLED) ENV N/
PDSE_SMSPDSE1 IBMPDSE ACTIVE(ENABLED) EXCEPT
RACF_FACILITY_ACTIVE IBMRACF ACTIVE(ENABLED) SUCCES
RACF_GRS_RNL IBMRACF ACTIVE(DISABLED) ENV N/
RACF_IBMUSER_REVOKED IBMRACF ACTIVE(ENABLED) EXCEPT
RACF_ICHAUTAB_NONLPA IBMRACF ACTIVE(ENABLED) SUCCES
RACF_OPERCMDS_ACTIVE IBMRACF ACTIVE(ENABLED) EXCEPT
S RACF_SENSITIVE_RESOURCES IBMRACF ACTIVE(ENABLED) EXCEPT
RACF_TAPEVOL_ACTIVE IBMRACF ACTIVE(ENABLED) EXCEPT
RACF_TEMPDSN_ACTIVE IBMRACF ACTIVE(ENABLED) EXCEPT
RACF_TSOAUTH_ACTIVE IBMRACF ACTIVE(ENABLED) SUCCES
RACF_UNIXPRIV_ACTIVE IBMRACF ACTIVE(ENABLED) EXCEPT
RSM_AFQ IBMRSM ACTIVE(ENABLED) SUCCES
RSM_HVSHARE IBMRSM ACTIVE(ENABLED) SUCCES
RSM_MAXCADS IBMRSM ACTIVE(ENABLED) SUCCES
COMMAND INPUT ==> SCROLL ==> PAGE
F1=HELP F2=SPLIT F3=END F4=RETURN F5=IFIND F6=BOOK
F7=UP F8=DOWN F9=SWAP F10=LEFT F11=RIGHT F12=RETRIEVE

```

# RACF\_SENSITIVE\_RESOURCES Sample

START TIME: 01/08/2005 20:47:54.701509 IBMRACF,  
 RACF\_SENSITIVE\_RESOURCES  
 OWNER DATE: 20040703

## APF Dataset Report

S Data Set Name	Vol	UACC	Warn	ID*	User
E SYS1.LINKLIB	ZDR17B	Read	No	Ctrl	
SYS1.SVCLIB	ZDR17B	****	****	****	
ISPF350.ISPLOAD	PRODAL	Read	No	****	
ISPF350.ISPLPA	PRODAL	Read	No	****	
ISPF350.ISRLOAD	PRODAL	Read	No	****	
ISPF350.ISRLPA	PRODAL	Read	No	****	
ISPF350.LPALIB	PRODAL	Read	No	****	
FARRELL.TEST.TOOLS.LOAD	D94001	****	****	****	

## RACF Dataset Report

S Data Set Name	Vol	UACC	Warn	ID*	User
RACFDRVR.RACF317	RDB317	****	****	****	

\* High severity Exception \*

IRRH204E The RACF health check RACF\_SENSITIVE\_RESOURCES has found one or more potential errors in the security controls on this system.

### Explanation:

The RACF security configuration health check has found one or more potential errors with the system protection mechanisms.

## What's on the z/OS Console?

```
RACFR1A HZS0001I CHECK(IBM CNZ,CNZ_CONSOLE_ROUTCODE_11):
  CNZHF0005I One or more consoles are configured to receive messages
  intended only for programmers.
RACFR1A HZS0001I CHECK(IBM CSV,CSV_LNKLST_SPACE):
  CSVH0980E Some LNKLST sets include data set(s) allocated with
  secondary space defined.
RACFR1A HZS0001I CHECK(IBM CSV,CSV_APF_EXISTS):
  CSVH0957E Problem(s) were found with data sets in the APF list.
00 *RACFR1A *HZS0003E CHECK(IBM RACF,RACF_SENSITIVE_RESOURCES):
  *IRRH204E The RACF_SENSITIVE_RESOURCES check has found one or
  *more potential errors in the security controls on this system.
IEE612I CN=C3E0S1A  DEVNUM=03E0  SYS=RACFR1A

IEE163I MODE= RD
```

## 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
- **The IBM Health Checker for z/OS**
  - ▶ IBM Health Checker for z/OS User's Guide
- **DFSORT ICETOOL Utility**
  - ▶ DFSORT Application Programming Guide

# Summary

Utility	Authority Required	Comments
IRRUT100	<ul style="list-style-type: none"> <li>•None for own ID</li> <li>•SPECIAL/AUDITOR or GROUP-SPECIAL/AUDITOR for other IDs</li> </ul>	Have to know the ID your looking for Finds references, does not remove or create commands
IRRDBU00	Pre z/OS V2R2: UPDATE to the input RACF DB (may be a copy) z/OS V2R2: READ if PARM=NOLOCK, UPDATE otherwise	Easy input to report tools for tailored reports and complex analysis
IRRRID00	READ to the output of IRRDBU00	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
DFSORT ICETOOL	Read to its input (IRRDBU00 or IRRADU00)	Extremely flexible record selection, high performance
RACF Health Checks	READ to either XFACILIT resource - HZS.owner.checkname.MESSAGES or - HZS.owner.MESSAGES	The IBM Health Checker for z/OS should already be running at your installation

## Using these Tools to See if you have a “Top Ten” Issue

- **IRRUT100 is of limited value**
- **IRRDBU00 and IRRADU00 are of great value when used with DFSORT/ICETOOL or System REXX**
  - ▶ Users with no password interval
  - ▶ Started task users not defined as protected IDs (see [ftp://public.dhe.ibm.com/s390/zos/racf/pdf/share\\_2016\\_08\\_irrxut\\_il\\_health\\_check.pdf](ftp://public.dhe.ibm.com/s390/zos/racf/pdf/share_2016_08_irrxut_il_health_check.pdf) for a sample System REXX Health Check)
- **‘SYS1.SAMPLIB’ has a set of sample ICETOOL reports:**
  - ▶ SUPU: Users with UID(0) Assigned
  - ▶ UADS: Data sets with a UACC > NONE

## Using these Tools to See if you have a “Top Ten” Issue...

- **The IBM-shipped RACF\_SENSITIVE\_RESOURCE health checks is of immense value**
  - ▶ Excessive access to APF libraries
  - ▶ Excessive access to RACF data set(s)
  - ▶ Improper user or Lack of UNIXPRIV profiles
  
- **The Installation-Defined RACF Health Checks are of immense value**
  - ▶ Excessive access to SYS1 data sets
  - ▶ Excessive access to z/OS UNIX file system data sets

.... All that you have to do is define a few RACF profiles with the data set names and make a small change to PARMLIB member HZSPRMxx



# 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)**
- **RACF Health Checks**
- **Summary**

# Disclaimer

The information contained in this document is distributed on an "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.

# VANGUARD

## SECURITY & COMPLIANCE CONFERENCE 2016

Thank you!

