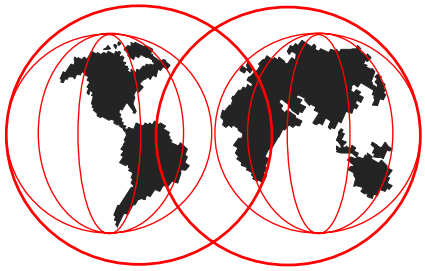
RACFICE overview
RACF reporting made easy

Paul de Graaff ITSO Poughkeepsie S/390 Security



Objectives

- At the end of this session, you will understand:
  - How DFSORT's ICETOOL utility can be used to assist in managing an OS/390 environment by analyzing the content of the RACF database and the SMF audit stream.
  - The DFSORT statements required to create customized reports from using the output of RACF's data base unload (IRRDBU00) and SMF unload (IRRADU00) utilities.
  - The sample reports that are shipped by RACF in SYS1.SAMPLIB(IRRICE)
  - How to use the RACFICE proc.

IBM Technical Support

- At the end of this session, you'll see the power of ICETOOL and the RACFICE reports!

Agenda

- The History of RACFICE
- Functions of ICETOOL used by RACFICE
  - SORT/COPY
  - DISPLAY
  - OCCURS
- RACFICE Installation
- RACFICE Contents
- Summary
- Questions

IBM Technical Support

- We'll begin our session with how and why the RACFICE reporting functions evolved.
-
- Next - though there are many pieces to DFSORT's ICETOOL utility RACFICE only uses a subset of the functions. Therefore we will concentrate only on the functions of the ICETOOL used by RACFICE. The functions that we will be looking at today are, SORT/COPY, DISPLAY and OCCURS
-
- Thirdly we will review the steps necessary to 'unpack' the various components of the RACFICE. They are shipped in SYS1.SAMPLIB(IRRICE). The process to 'unpack' this via IEBUPDTE is very straight forward.
-
- Fourth we will review the contents of the RACFICE product and touch on how the reports can be best configured for your installation.
-
- Last I will wrap up the presentation and also solicit questions that any of you may have.

The History of RACFICE

The History of RACFICE

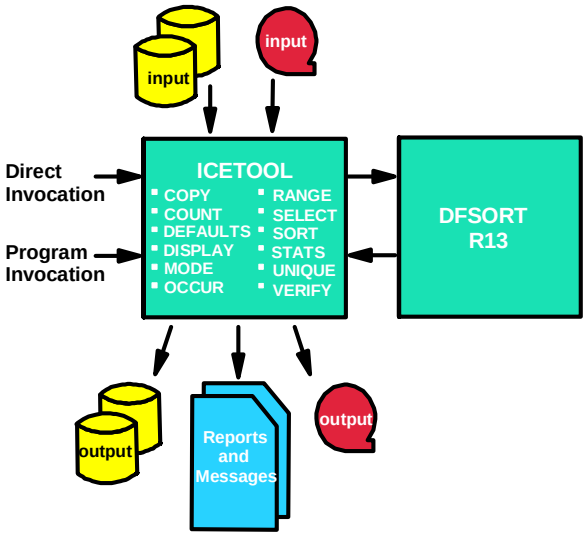
- RACF report writer functionally stabilized at the RACF 1.9.2 level, though it is still supported
- IRRDBU00 introduced in RACF 1.9.0
- IRRADU00 introduced in RACF 1.9.2
- Flexibility introduced Complexity
- RACFICE on the Web since 1994
  http://www.ibm.com/S390/racf
- RACFICE in SYS1.SAMPLIB(IRRICE) in OS/390 Security Server R2.8
- Assumes the use of DFSORT's ICETOOL

IBM Technical Support

- The main purpose of RACFICE is to provide a reporting tool that can be customized. With RACF 1.9.2, IBM functionally stabilized the RACF report writer. That means that it can still be used for pre-RACF 2.1 audit information, it does not report on any of the new event codes, such as those introduced with our OpenEdition (now UNIX System Services) support.
- Furthermore, the report writer offers little customization in how it presents data.
- Since RACF 1.9.0, RACF has provided a utility (IRRDBU00) to unload the RACF data base to a flat file, and since RACF 1.9.2 has done the same with its SMF audit data. This coupled with DFSORT's powerful ICETOOL reporting utility allows a unique opportunity to provide customers with a set of commonly-requested reports, which is exactly what we did in 1994 when we made the RACFICE report tool available on the web.
- Starting with OS/390 R2.8 the RACFICE control cards and JCL are shipped in SYS1.SAMPLIB. This provides a greater level of support from IBM. Since these samples are now officially part of the OS/390 Security Serve, IBM's full level 1 and level 2 support are available to resolve any issues with these samples.
- The assumption is that you are using DFSORT. These control cards are similar, but not exactly the same as some other popular sort/merge utilities. Therefore there are modifications needed to the ICETOOL control cards to allow RACFICE to run with other sort/merge products.

Functions of ICETOOL used by RACFICE

Functions of ICETOOL



IBM Technical Support

- ICETOOL utilizes DFSORT for functions such as record selection and provides a rich set of additional reporting and formatting functions.
-
- ICETOOL was introduced in Release 11 of DFSORT and enhanced in every subsequent Release of the product. ICETOOL works together with the basic DFSORT functions to provide a flexible report writer. ICETOOL uses DFSORT's sorting, copying, merging and record selection functions. Additionally, ICETOOL adds new features for reporting, formatting, statistics and dealing with duplicates. The end result is a quick method of generating reports.
-
- DFSORT Release 14 allows you to use symbol mappings for RACF records available from IBM. This will be discussed later in today's presentation.
-
- RACFICE uses - SORT, COPY, DISPLAY and OCCURS, the other 8 ICETOOL operators are COUNT, DEFAULTS, MODE, RANGE, SELECT, STATS, UNIQUE and VERIFY.

Functions of ICETOOL used by RACFICE

- ICETOOL introduced in R11 of DFSORT
- SORT/COPY
- DISPLAY
- OCCURS

IBM Technical Support

-
- RACFICE only uses a small subset of the functions available in DFSORT's ICETOOL. For a complete picture of what the ICETOOL can do, refer to the DFSORT Application Programming Guide for your release of DFSORT.
-
- SORT/COPY will copy selected records from one file to another and optionally order them.
-
- Display is used to generate the look of the report.
-
- Occurs is similar to Display except it also allows the use of 'count' values (HIGHER statement) to further select what you are interested in reporting.

RACFICE SORT/COPY

```
COPY    FROM(inddn) TO(outddn) USING(ddn+'CNTL')
              -or-
SORT    FROM(inddn) TO(outddn) USING(ddn+'CNTL')


COPY    FROM(ADUDATA) TO(TEMP0001) USING(RACF)
```

A typical RACFICE COPY/SORT statement.

IBM Technical Support

- This is the syntax of the SORT/COPY. This is typically the first statement in the Control cards. Depending upon the RACFICE report - it may be a COPY or it may be a SORT statement. The SYNTAX of the statements is nearly identical, and it obviously only directs whether or not the records in this report will be ordered or not.
- **INDDN** - The input DDNAME - typically either ADUDATA or DBUDATA (indicating which sort of input to expect.
- **OUTDDN** - The output DDNAME as found in the JCL for this step. This usually points to a TEMP file which becomes input for the DISPLAY or OCCURS portion of the ICETOOL report function.
- **DDN** - The DDNAME which points to the control cards to use for the Copy of Sort function. Notice that the ICETOOL assumes a suffix of CNTL. So all the RACFICE tool USING statements are USING(RACF). This means all the control cards for the Copy or Sort function are in the DDNAME pointed to by RACFCNTL within the JCL.
-
- This is the First control card encountered in the DFSORT ICETOOL logic path.
-

SORT/COPY continued

```
SORT    FIELDS=(start,length,type,sequence....)
INCLUDE COND=(start,length,type,eval,value,and|or,
              start,length,type......)
```

IBM Technical Support

- This is the syntax of the SORT/COPY statement for RACFICE this is usually the 'CNTL' suffixed members. These members further define the SORT or COPY as initialized by the statements discussed on the previous foils.
- The 'SORT' statement is used to order or sort the records based upon the criteria specified in the FIELDS portion of the SORT statement.
- The INCLUDE statement is used to Select or Include records based upon the criteria specified in the COND portion of the INCLUDE statement.
-
- **start** - is the starting position of the string
- **length -** is the length of the string
- **type** - is the description or 'type' of data - the 2 types of data you will find in the RACFICE tool is:
  - "CH" indicating character data
  - "SS" indicating a substring of data
- **sequence** - is the order or the sequence you wish the previously described data in (based upon the start, length and type)
  - "A" indicates ascending order
  - "D" indicates descending order
- **eval -** The type of the 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

SORT/COPY continued

```
SORT    FIELDS=(63,8,CH,A)
INCLUDE COND=(5,8,CH,EQ,C'ACCESS',AND,
              91,3,CH,EQ,C'YES')
OPTION   VLSHRT
```

NOTE: Sort includes the RDW in its calculation of the field location. Add 4 to the value found in *Macros and Interfaces* Manual to obtain field location for ICETOOL.

IBM Technical Support

- This is the sort control statements for the OPER RACFICE procedure. Based upon these statements we know the following.
-
- We are sorting the records in ascending sequence based upon the value in column 63. This value includes the record descriptor word (RDW). By referring to the *Macros and Interfaces* Manual - SC28-1914 you can see that the value in location **59** for a length of 8 is the USER ID associated with the Event. (Notice that 4 must be added to the value found in the *Macros and Interfaces* Manual).
-
- Additionally we are only looking for ACCESS events where the reason for the access being granted is because the ID has the OPERATIONS attribute.
-
- So - in column 1 (referring to the manual) the string ACCESS appears identifying this as an ACCESS event, plus in column 87 (based upon the manual again) we are looking for a YES for a length of 3 - the manual states that column 87 answers the question "Was operations authority checking a reason for access being allowed?" Yes - ...

RACFICE DISPLAY

```
DISPLAY FROM(indd) LIST(listdd) -
        PAGE -
        TITLE('string')-
        DATE(abcd) -
        TIME(abc)  -
        BLANK -
        ON(start,length,type)  HEADER('string') -
        ON(start,length,type)  HEADER('string') .....
```

IBM Technical Support

- The Display statement describes the 'Look' of the report. With the Display statement you define how you want things like the top of each page to look, you can format such things as the date and time the report was run, the title of the report and the data which is to appear in the report. The order you put the commands will influence the 'look' of the report.
-
- A description of the syntax follows
  - **INDD** - The input data set name as found in the JCL for this step
  - **LISTDD** - The output DDNAME for the Report (or List), as found in the JCL for this step
  - **STRING** - Any string of characters (1 to 50 long)
  - **ABCD** - Format of the date - any combination of M (month) D (day) Y (year) and 4 (4 digit year). Specify each only once (Y and 4 are mutually exclusive).
  - **ABC** - Format of the time - '12:' or '24:' are valid values. 12: means use 12 hour clock with a.m. or p.m. suffix, 24: means use 24 hour clock.
  - start, length and type have been discussed on the previous foil.
  - **BLANK** - Insert a blank line.
-
-

RACFICE DISPLAY continued

```
DISPLAY FROM(TEMP0001) LIST(PRINT) -
      PAGE -
      TITLE('VIOL: Access Violations')-
      DATE(YMD/) -
      TIME(12:)  -
      BLANK -
      ON(23,8,CH)   HEADER('Time') -
      ON(32,10,CH)  HEADER('Date') .... -
```

IBM Technical Support

- This is a portion of the VIOL control card which generates a the Access violation report.
-
- The TEMP001 is input and the report is going to a DDNAME called 'PRINT'. Strings have been defined for the Title 'Access Violations' and the 2 header columns we can see - 'Time' and 'Date'
-
- The Date on the first line will appear as YMD using a 2 character year. Reflecting the day the report was run.
-
- The Time on the first line of the report will be in a 12 hour clock format. Reflecting the time the report was run.

RACFICE DISPLAY continued

- 1 - VIOL: Access Violations 99/06/23 03:08:10 pm

Date	Time	Result	User ID	Resource Name
1999-06-15	13:47:56	INSAUTH	TSTBUDS	GRAAFF.IRRDBU00.CNTL
1999-06-15	13:48:17	INSAUTH	TSTBUDS	GRAAFF.RACFTOOL.CNTL

IBM Technical Support

- This gives a portion of the report produced by the control cards shown on the previous pages.
- You can see how the Display statement resolves into the contents of the report.
- This page shows that ID TSTBUDS attempted to access resource name(s) GRAAFF.IRRDBU00.CNTL and GRAAFF.RACFTOOL.CNTL, but did not have sufficient access. This example is only from the left most columns of the report. Further to the right (off this foil) is the profile name for the resource and the type of resource (dataset in this case).

RACFICE OCCURS

```
OCCURS  FROM(TEMP0001) LIST(PRINT) -
        PAGE -
        TITLE('User IDs With Incorrect Passwords')-
        DATE(YMD/) -
        TIME(12:)  -
        BLANK -
        ON(63,8,CH) HEADER('User ID') -
        ON(VALCNT)  HEADER('# of Incorrect Passwords')  -
        HIGHER(3)
```

IBM Technical Support

- The occurs statement has the same syntax as the Display statement but it adds an additional variable. The 'HIGHER' command used in conjunction with the VALCNT operand.
-
- The HIGHER statement provides a threshold for the events. The example shown here is from the LOGF report. The LOGF reports on the USERIDs who have more than '3' incorrect password attempts. Your installation can modify this number to an appropriate count - based upon your reporting needs.
-

RACFICE OCCURS continued

- 1 - LOGF: User IDs With Excessive Incorrect Passwords

User ID	Number of Incorrect Passwords
SLACKER	9
TEEDEE	5

IBM Technical Support

- This shows the results of the previous OCCURS statement.
-
- Notice that this report summarizes rather than listing every instance of the incorrect passwords. Additionally it uses the HIGHER statement to determine the threshold to show on this report.
-

RACFICE Installation

RACFICE Installation

- Allocate a PDS to contain the RACFICE report formats
  - Record Format: FB
  - LRECL : 80
  - Size : 10 tracks 3390
- Unload SYS1.SAMPLIB(IRRICE) into pre-Allocated PDS
  - JCL is in SYS1.SAMPLIB(RACJCL)
- Modify for your installation
  - JCL
  - Reports

- A PDS needs to be pre-allocated prior to running the IEBUPDTE JCL found in the RACJCL. The PDS needs to have an LRECL of 80 with a record format of Fixed Block (FB). The size of the PDS should be around 10 3390 tracks.
-
- Next using the JCL in SYS1.SAMPLIB(RACJCL) as a starting point (modify to your installations requirements) Run the RACJCL JCL to UNLOAD the SYS1.SAMPLIB(IRRICE) member into the pre-Allocated PDS just created.
-
- Finally you will need to modify the JCL and PROCs for use at your installation. For instance you will need to point to the location of your IRRDBU00 and IRRADU00 output. You need to modify the overrides to point to your newly created RACFICE PDS. Lastly you should determine if the reports as shipped are appropriate for your installation.
-
- During the discussion on the contents of the RACFICE tool the types of things which may need to change for your installation will be discussed.
-

RACFICE Installation notes

- Early R8 shipped RACJCL ICEUPDTE with
  - //SYSIN DD DSN=SYS1.PARMLIB(IRRICE),DISP=SHR
- Should be
  - //SYSIN DD DSN=SYS1.**SAMPLIB**(IRRICE),DISP=SHR

IBM Technical Support

- Some early version of RACFICE shipped with an incorrect DSN in the RACJCL ICEUPDTE. Note you should be pointing to SYS1.SAMPLIB(IRRICE)

RACFICE Contents

RACFICE Contents

- RACFICE Proc (member name RACFICE)
  - Probably no modifications needed
- RACFICE JCL (member name $$CNTL$$)
  - JOB Card
  - Input/Output Data sets
  - Comment Out unnecessary Reports (or add new ones?)
- RACFICE Control Cards
  - Pairs <report_name> and <report_name>CNTL
  - Any modifications, i.e. SELU selects IBMUSER as shipped
- Stand-alone Reports ($CFQG, $CHLQ and $ULAST90)

IBM Technical Support

- There are 4 types of members found in the RACFICE PDS.
-
- The RACFICE proc contained in member RACFICE. This proc probably needs no modifications. We will discuss it further on the next foil
-
- The RACFICE JCL contained in member $$CNTL$$. You will need to modify the JOB card to make it applicable to your site - the symbolics for the input/output datasets, the JCLLIB statement pointing to your PROCLIB (probably the PDS you've preallocated) the Symbolic for the PDS where your RACFICE control cards are located.
-
- The RACFICE control cards should be reviewed. For instance on the SELUCNTL card the events for user IBMUSER are selected. While that may be of some interest (especially if you find out it is being used) - typically you will be looking for reporting on a USER unique to your site.
-
- The stand-alone reports may also be of interest and should perhaps be reviewed for applicability to your installation.
-

RACFICE Contents/RACFICE proc

```
//RACFICE  PROC  REPORT=                Name of report
//RACFICE   EXEC PGM=ICETOOL
//TOOLMSG   DD DUMMY
//PRINT     DD SYSOUT=*
//DFSMSG    DD DUMMY
//ADUDATA   DD DISP=SHR,DSN=&ADUDATA
//DBUDATA   DD DISP=SHR,DSN=&DBUDATA
//TEMP0001  DD DISP=(NEW,DELETE,DELETE),SPACE=(CYL,(20,5,0))
//TEMP0002  DD DISP=(NEW,DELETE,DELETE),SPACE=(CYL,(20,5,0))
//TOOLIN    DD DISP=SHR,DSN=&ICECNTL(&REPORT)
//RACFCNTL  DD DISP=SHR,DSN=&ICECNTL(&REPORT.CNTL)
```

IBM Technical Support

- This is the RACFICE proc without the comments. As you can see there is probably nothing you need to change within this proc. The overrides from the JCL member $$CNTL$$ will take care of everything.
- However, this is a good time to discuss the flow of the various ICETOOL components. The DDNAMEs of PRINT/ADUDATA/DBUDATA/TEMP001 and RACFCNTL are all referenced in the control cards for the various reports. Also we'll discuss the variables present here. &ADUDATA/&DBUDATA/&ICECNTL and &REPORT.
- The PRINT DDNAME is where all the output for the various reports go - this may be something you would change if for instance you're going to route all your reports to disk or have a specific output class where these types of reports would go.
- ADUDATA is the output from your IRRADU00 program. This data originated as SMF data and after IRRADU00 has run only RACF 'events' are left in a format which is easily used by any report writer.... The format of the records is discussed in detail in the OS/390 Macros and Interfaces manual.
- DBUDATA is the output from your IRRDBU00 program. This data originated from your RACF data base. This file had all the various RACF records and extensions broken down into an easily readable format... Again as with the ADUDATA, The format of the records is discussed in detail in the OS/390 Macros and Interfaces manual.
- Often the TEMP001 is the out put from the 'sort' portion of each step, then used as input to the 'reporting' portion of each step

RACFICE Contents/$$CNTL$$ member

```
//  JCLLIB ORDER=USER01.RACFICE.CNTL    ICETOOL PROC
//  SET  ADUDATA=USER01.IRRADU00          IRRADU00 data
//  SET  DBUDATA=USER01.IRRDBU00          IRRDBU00 data
//  SET  ICECNTL=USER01.ICE.TOOL           ICETOOL  DATA

.........

//  SELU       EXEC  RACFICE,REPORT=SELU
```

IBM Technical Support

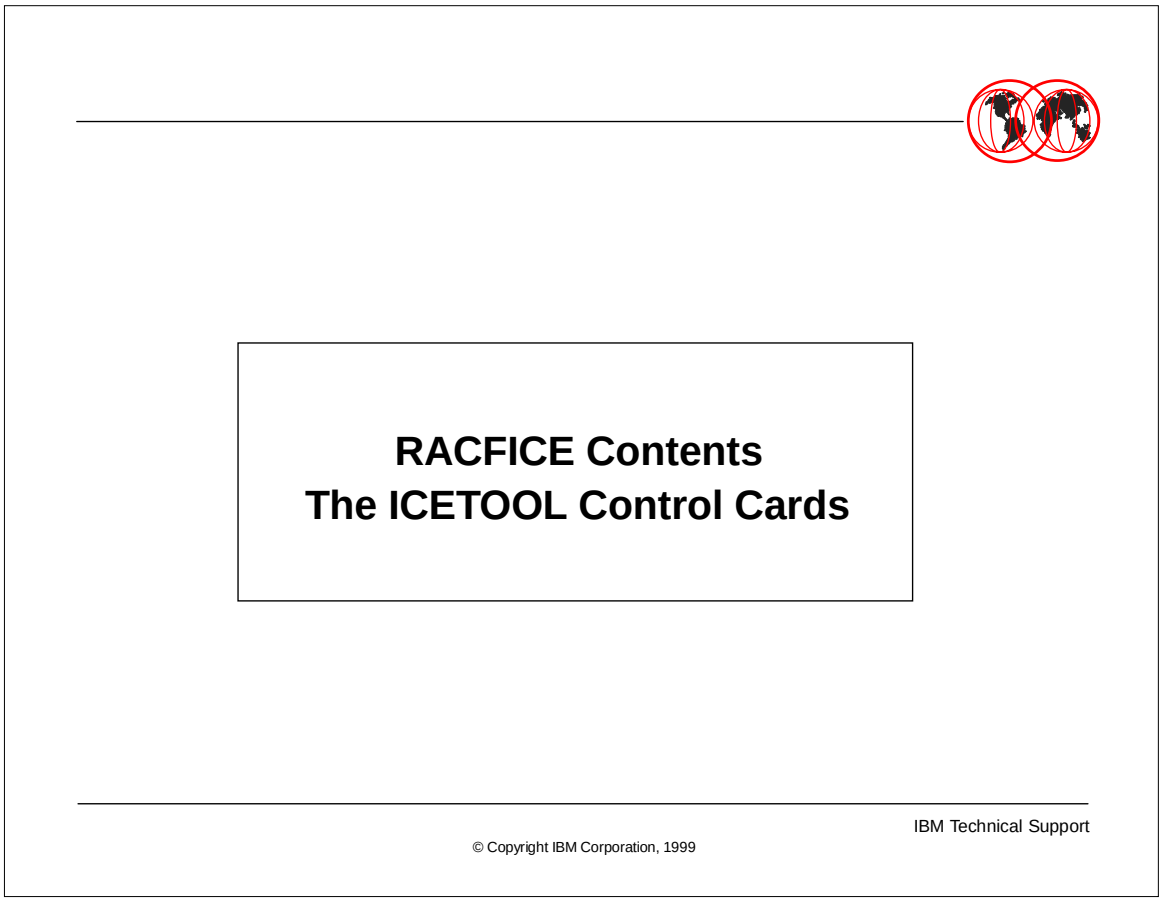
- The $$CNTL$$ member contains the JCL to run the ICETOOL
- Shown on this chart are the symbolic over rides you will need to modify.
- The JCLLIB order statement should point to the PDS file where your RACFICE proc is located
- The ADUDATA should point to the output from the IRRADU00 utility
- The DBUDATA should point to the output from the IRRDBU00 utility
- The ICECNTL should point to the PDS where you have all the RACFICE control cards located.
- You will probably also need to modify the JOB card to comply with the standards set at your installation.
- Something else to consider is whether you will really need to run all of the reports. For instance some of the reports have to do with RRSF. If you are not using RRSF you probably are not interested in running any of those reports. So comment out or delete the RRSF related steps. The RRSF related reports are ACD$, ECD$, PWD$ and RACL
- You can chose to split $$CNTL$$ into different sets of JCL to run... or comment out the reports that do not apply to your installation. The SELU step shown is the general format of all the reports. The step name matches the report name.

RACFICE Contents/Stand-Alone Members

- There are 3 Stand-alone members in the RACFICE PDS
  - $CFQG
  - $CHLQ
  - $ULAST90
- Possible Error in $CFQG and $CHLQ when running in a non-VIO environment
  - //DS$1 DD DISP=(NEW,PASS),DSN=&TEMP1
- Add a Space parameter for non-VIO on all DS$x DDNAMES
  - **//DS$1 DD DISP=(NEW,PASS),DSN=&TEMP1,SPACE=(TRK,(75,5))**

IBM Technical Support

-
- At this point in the discussion it is of interest that these three reports do not follow the previous mentioned pattern - the only rule is that there must always be an exception to the rule.
-
- These do not use RACFICE, nor any other RACFICE control cards, they are self contained reports.
-
- The JOB card must be modified as on the $$CNTL$$ member and the input data set must be modified. All 3 of these use output from the IRRDBU00 utility. (note that the comments shipped in SYS1.SAMPLIB are incorrect)
-
- Depending upon your environment you may need to add the Space parameter to all the DS$x (DS$1-DS$8) found in the $CFQG and $CHLQ members of the RACFICE PDS. If your temporary data sets use VIO, you should be OK, otherwise add a SPACE parameter.



-
- Next will give a quick overview of all the RACFICE reports that are shipped as samples.
-
- These are broken up into reports which are based on the output of IRRDBU00, and reports that are based upon the output of IRRADU00.
-
- These 'report' names correspond to the 'member pairs' found in the ICETOOL control cards. Remember the member pairs are in the format of <report_name> and <report_name>CNTL.
-
- The exception being the 3 stand-alone reports - which will be discussed after the other reports.
-
- Comments will also be made on reports where you may want to do some modifications for your installation.

Control Cards - IRRDBU00

- ALDS - Users with Alter authority to discrete data set profiles
- ASOC - Users with explicit RACF Remote Sharing Facility (RRSF) associations.
- BGGR - Discrete general resource profiles with generic characters.
- CCON - Count of Users connections, reporting on those with more than "n" connections (shipped with 20 - change if needed).
- CGEN - Count of general resource profiles.
- CPRO - Count of all profiles in the RACF database.
- CONN - Users with Group privileges above use.

IBM Technical Support

- ALDS - If there are large number of USERS who can delete and define discrete profile, you may want to consider some changes, either making the DSN profile a fully qualified generic or reducing the numbers of folks who could possibly move a discrete dataset.
-
- ASOC - if your not using RRSF, skip using this report. If IDs have password synchronization setup via a RACLINK definition for instance, you will see the link her
-
- BGGR - An excellent report to find any profiles which are in error (or find if a resource class has accidentally switched to NOGENERIC)
-
- CCON - Count of users connections, As shipped from IBM shows users with connections over 100. Use your best judgment as to what the proper threshold should be for your installation - then - change the HIGHER(100) to an appropriate value.
-
- CGEN - Count of General Resource Profiles, a nice statistic to know....
-
- CUGD - Count of all profiles - an indicator of the size of your data base.
-
- CONN - a list of users with Connects to a Group with other than USE.
-

Control Cards - IRRDBU00 continue

- IDSC - Data set conditional access list entries with an ID(*) entry of other than NONE
- IDSS - Data set standard access list entries with an ID(*) entry of other than NONE
- IGRC - General resource conditional access list entries with an ID(*) of other than NONE
- IGRS - General resource standard access list entries with an ID(*) of other than NONE
- OMVS - List of IDs which have a UNIX System Services (OMVS) segment
- SUPU - UNIX 'super users' (UID of Zero)

IBM Technical Support

-
- IDSC, IDSS, IGRC, IGRS are all looking for access lists which may be allowing any authenticate User too much access. This is certainly a good list to review periodically.
- Obviously some differences whether they are conditional access lists or not.
-
- Reports on OMVS (Unix Systems Services - USS) users
-
- SUPU, Audit the Super Users at your installation
-
-
-

Control Cards - IRRDBU00 continued

- UADS - Data set profiles with UACCs other than NONE
- UAGR - General Resource profiles with UACCs other than NONE
- UGLB - Users with extraordinary global authorities
- UGRP - Users with extraordinary RACF group authorities
- UIDS - UNIX Systems Services UIDs which are used more than once
- URVK - Users which are currently revoked
- WNDS - Dataset profiles in warning mode
- WNGR - General resource profiles in warning mode

IBM Technical Support

- UADS and UAGR, These reports are looking for any access which is globally allowed, even to IDs which are not authenticated.
-
- UGLB looking for GLOBAL SPECIAL, OPERATIONS AND AUDIT privileges.
-
- UIDS which USS uids are being used by multiple users?
-
- URVK reports on all the revoked users in the system.
-
- WNDS dataset profiles in warning mode. Certainly a good thing to monitor
-
- WNGR general resource profiles in warning mode are also good to keep an eye on.

Control Cards - IRRADU00

- ACD$ - users who are using automatic command direction
- CADU - total count of events by category
- CCMD - count of RACF commands issued by USER
- ECD$ - users who are directing commands explicitly
- LOGB - users who log on with LOGON BY
- LOGF - All users with excessive incorrect passwords, shipped with 3 as excessive
- OPER - Accesses allowed because the user has the OPERATIONS privilege
- PWD$ - Users who are using password synchronization

IBM Technical Support

- ACD$, ECD$, PWD$ and RACL are all related to RRSF. If you are not using RRSF you may not want to use these reports. NOTE: You must have UAUDIT turned on or be auditing RRSFDATA to gather information on PWD$, ACD$ and ECD$.
-
- CADU, Big Picture
-
- CCMD, Big picture of administration activity
-
- LOGB, relates to VM LOGON BY.. certainly a good thing to monitor
-
- LOGF, Your installation needs to determine what 'excessive' means. As shipped the LOGF considers more than three incorrect passwords from a specific ID to be excessive. The other variable to consider is the time-span covered by your SMF input data. For instance 4 incorrect passwords over a 30 day period would seem to be normal. Adjust this parameter according to your needs.
-
- OPER, This may indicate an access list should be changed.
-

Control Cards - IRRADU00 continued

- RACL - Show RACLINK audit records
- RINC - Class Statistics at IPL
- SELU - Identify all audit records for a specific user, shipped with IBMUSER.
- SPEC - Accesses allowed because the user has SPECIAL privilege
- TRMF - Excessive incorrect passwords from the same terminal, shipped with a HIGHER(3)
- VIOL - Report all access violations
- WARN - Access allowed because the resource is in WARNING mode

IBM Technical Support

- RACL, shows any RACLINK commands issued.
-
- RINC, shows if class are active you think should be and also shows if raclisted, generics and gencmd active for the class.
-
- SELU, selects all events where IBMUSER is the USER. Probably want to alter this for your installation.
-
- SPEC
-
- TRMF monitor an attempted breach from a specific terminal, for instance if someone was simply picking IDs but kept the invalid password count on each ID low enough not to revoke the ID you may want to monitor the 'source' where a number of invalid passwords are originating from. As shipped the HIGHER(3) may not be appropriate for your installation.
-
- VIOL Reports on all access violations
-
- Warn

Control Cards - Stand alone reports

- $CFQG HLQs with excessive fully qualified generic qualifiers as shipped HIGHER(100)
- $CHLQ HLQs with excessive generic profiles as shipped HIGHER(200)
- $ULAST90 USERS added to the RACF database in the last 90 days. This is a REXX exec the '90' is determined by a variable called user_age

IBM Technical Support

- For both $CFQG and $CHLQ you need to determine what value is 'excessive' for your environment. Performance of your entire system can be adversely affected if either fully qualified generics or generic profiles under the same HLQ become excessive.
- $ULAST90, reports on all USERS added within the last 90 days. Of interest is that this is a REXX exec which uses ICETOOL. The variable user_age may be changed to a value other than 90 as your installation may require.

Control Cards - Symbols

- DFSORT release 14 introduced the DFSORT SYMBOL
  - USBD_OPER could be used as a symbol for 44,1,CH
- RACFICE off the WEB **- only -** has 2 members which defines all the symbols for IRRADU00 and IRRDBU00 fields
  - ADUSYMBL for IRRADU00 fields
  - DBUSYMBL for IRRDBU00 fields
- Could change all SORT and INCLUDEs to use symbols.

IBM Technical Support

-
- If you are running release 14 of DFSORT you can use symbols rather than columns to run ICETOOL
-
- This is NOT shipping with the SAMPLIB version of ICETOOL. Only available of the RACF web page.
-
- There are 2 members which allow the use of the SYMBOLS. ADUSYMBL and DBUSYMBL

Symbols/RACFICE Modification

```
//RACFICE   PROC  REPORT=              Name of report
//RACFICE   EXEC PGM=ICETOOL
//TOOLMSG  DD DUMMY
//PRINT      DD SYSOUT=*
//DFSMSG     DD DUMMY
//ADUDATA  DD DISP=SHR,DSN=&ADUDATA
//DBUDATA   DD DISP=SHR,DSN=&DBUDATA
//TEMP0001   DD DISP=(NEW,DELETE,DELETE),SPACE=(CYL,(20,5,0))
//TEMP0002   DD DISP=(NEW,DELETE,DELETE),SPACE=(CYL,(20,5,0))
//TOOLIN     DD DISP=SHR,DSN=&ICECNTL(&REPORT)
//RACFCNTL  DD DISP=SHR,DSN=&ICECNTL(&REPORT.CNTL)
//SYMNAMES  DD DISP=SHR,DSN=&SYMBOLS(ADUSYMBL)
//                DD DISP=SHR,DSN=&SYMBOLS(DBUSYMBL)
```

IBM Technical Support

- You will need to make some modifications if you plan on using the SYMBOLs provided to you from the RACF home page.
-
- The SYMBOLS use a DDNAME called SYMNAMES. This shows a technique for adding the SYMNAME to your existing RACFICE proc. Also added is the symbolic &SYMBOLS.

Symbol/$$CNTL$$ changes

```
// JCLLIB ORDER=USER01.RACFICE.CNTL    ICETOOL PROC
// SET  ADUDATA=USER01.IRRADU00          IRRADU00 data
// SET  DBUDATA=USER01.IRRDBU00          IRRDBU00 data
// SET  ICECNTL=USER01.ICE.TOOL           ICETOOL  DATA
// SET  SYMBOLS=USER01.RACFICE.CNTL    SYMBOLS
.........

// OPRT       EXEC  RACFICE,REPORT=OPRT
```

IBM Technical Support

- Since new symbolics were added to the RACFICE proc the $$CNTL$$ member will need to change to reflect those modifications. A new 'SET' operand and the INPUT symbolic are shown here. The OPRT is to distinguish between the OPER report. Simply to distinquish it as a modified report. As always use the standards set by your installation.

SYMBOLS control cards

```
SORT    FIELDS=(63,8,CH,A)
INCLUDE COND=(5,8,CH,EQ,C'ACCESS',AND,
              91,3,CH,EQ,C'YES')
OPTION   VLSHRT

_____________________________________
SORT    FIELDS=(ACC_EVT_USER_ID,A)
INCLUDE
COND=(ACC_EVENT_TYPE,EQ,C'ACCESS',AND,
              ACC_AUTH_OPER,EQ,C'YES')
OPTION   VLSHRT
```

IBM Technical Support

- This shows the difference between using the DFSORT control statements with and without the use of symbols.
-
- Since the symbol has already defined the location, length and type of data, you simply need to refer to the symbol and do not need to concern your self with the esoterics of location, length and type of data.
-
-

SYMBOLS control cards

ACC_EVT_USER_ID,63,8,CH

.....

ACC_EVENT_TYPE,5,8,CH

.....

ACC_AUTH_OPER,91,1,CH

IBM Technical Support

- This shows the symbol statements which are contained in the symbol control cards.

RACFICE Summary

RACFICE Summary

- DFSORT's ICETOOL using IRRADU00 and IRRDBU00 data as input
  - Customize Report Formats
  - Change Selection Criteria to meet each installation's needs
- Using Samples as a starting point will reduce setup time for any Report Writing needs

IBM Technical Support

- The ICETOOL samples use IRRADU00 and IRRDBU00 as input. Samples of these utilities are available in SYS1.SAMPLIB(RACJCL).
- An installation can change the 'look' of a report, or chose to report on events or RACF database records beyond what is shipped in SYS1.SAMPLIB
- Regardless of your SORT/MERGE utility, using the samples as a starting point will greatly reduce the amount of time needed to set up reporting.

RACFICE Summary references

- "RACF and DFSORT Security Analysis Tools" by Frank Yaeger and Mark Nelson, Technical Communications, October 1996 http://www.naspa.net/PDF/T96100001.pdf
- Current ICETOOL and Documentation check the downloads http://www.ibm.com/s390/racf
- DFSORT Applications Programming Guide (SC33-4035)
- RACF Macros and Interfaces (SC28-1914)
- RACF Security Administrator's Guide (SC28-1915)
- RACF Auditor's Guide (SC28-1916)

-
- A full description of RACFICE was published in the National Association of Systems Programmer (NaSPA) magazine "Technical Communications".
-
- Source code is available now off the RACF homepage now
-
- Macros and Interfaces describes the record layouts for the IRRADU00 and IRRDBU00 utilities
-
- Security Administrators Guide and Auditors Guide for R8 will describe how security administrators and auditors can use RACFICE