RRE™ - RACF 'RULES' ENFORCER

Purpose:

- To verify all RACF profiles against a HR/CD/ID system and vice versa.
- To verify all RACF profiles against a set of user defined 'rules'.
- To enforce naming conventions in a RACF environment without having to have any exits.
- To simplify future audits.
- To reduce the immense costs of any future RACF audits.
- To keep HR/CD and RACF information in sync based on installation standards.
- To have a better control over all RACF profiles.
- To be able to manage multiple clients.
- To verify SETROPTS settings.

Most RACF installations do no longer know why certain user-Ids are connected to various RACF Group-Ids. Even when installations utilize a corporate directory (ID or CD or HR) it never matches the RACF environment 100%. Ownership of profiles may not be up-to-date either.

Especially large corporations with many decentralized RACF administrators face the immense problem to enforce standards.
Manually controlling such RACF environments is almost impossible.

This batch facility helps every RACF installation to verify corporate directories versus RACF. It lists all inconsistencies and generates the necessary RACF commands to alter/delete RACF profile information.

RRE consists of two parts:

- CD/ID/HR verification against RACF and vice versa
- Rules checking for RACF group-, user- (incl. connects), dataset- and general resource profiles

Installation:

- upload the XMIT members (LINKLIB, SAMPLIB, COMMANDS) to the host and issue the TSO RECEIVE command to unpack the XMIT members.
- Define the LINKLIB in the APF list
- Run IRRDBU00 from IBM to have an off-loaded RACF DB file available, which in turn will be needed as input by the JCL members found in the supplied SAMPLIB
- Tailor the SAMPLIB JCL members according to your installation standards

Problems:

- Please send an email to racfra2@bluewin.ch with the necessary JCL and output attached.

Copyrights :

- The copyrights of RRE and software ownership remain with Alain Steffen(ALS). RRE has been written by Eugene Vogt.

Disclaimer :

There are no warranties, either expressed, or implied on any the programs contained within. The authors try to test as much as is reasonable, but it is ultimately the responsibility of the user to ensure that the programs will not compromise the integrity of their environment. In other words, these programs are 'Use at your own Risk'.

Note:

- The IBM API IRRSEQ00 processing has multiple errors. Make sure to obtain the latest IBM APARS.
- None of the supplied RRE programs make any changes to your RACF DB.

DEB$SW1H - CD/HR VS RACF VERIFICATION

Purpose:

- Verify the HR/CD (corporate directory) against RACF and vice versa.

Note: It is the responsibility of each user to verify any generated RACF commands before executing them e.g. to alter or delete any user-Ids.

JCL required to run DEB$SW1H

Run the following JCL (refer to the YOURE.RRE.SAMPLIB member DEB$SW1H) to create the verification reports:

```
//RREVERIF   EXEC PGM=DEB$SW1H
//STEPLIB    DD   DISP=SHR,DSN=YOURE.RRE.LINKLIB
//*
//* INPUT FILES
//*
//IRRI0200   DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0200.VB(0)
//HRSI0200   DD   DISP=SHR,DSN=YOUR.MYCORP.HRS
//*
//* HRS RELATED INFORMATION (ALL HR IDS AND THEIR MISSING IDS IN RACF)
//*
//VERHRLST   DD SYSOUT=*    * HR HRSI0200 USERIDS LISTED "ASIS"
//VERHRMIS   DD SYSOUT=*    * HR USERIDS NOT FOUND IN RACF
//*
//* RACF RELATED INFORMATION (ALL RACF UIDS AND THEIR MISSING HR UIDS)
//*
//VERPRINT   DD SYSOUT=*    * PRINT +VERIFY CONTROL STATEMENTS
//VERRALST   DD SYSOUT=*    * RACF IRRI0200 USERIDS LISTED "ASIS"
//VERRAMIS   DD SYSOUT=*    * RACF LIST ALL MISSING USERIDS IN "HR"
//VERRANEV   DD SYSOUT=*    * RACF LIST ALL USERIDS NEVER USER "ASIS"
//VERRAREV   DD SYSOUT=*    * RACF LIST ALL REVOKED USERIDS
//VERRAOPR   DD SYSOUT=*    * RACF LIST ALL OPER/SPECIAL USERIDS  "ASIS"
//VERRAPRO   DD SYSOUT=*    * RACF LIST ALL PROTECTED USERIDS "ASIS"
//VERRCDEL   DD SYSOUT=*    * RACF DELETE ALL USERIDS NOT FOUND IN "HR"
//VERRCREV   DD SYSOUT=*    * RACF REVOKE ALL USERIDS NOT FOUND IN "HR"
//VERRCALT   DD SYSOUT=*    * RACF ALU    ALL USERIDS NOT FOUND IN "HR"
//VERINPUT   DD *           * FILTER CRITERIA FOR "HR" AND "RACF"
*
*OPTIONS HEADING=YES,PROTECTED=YES,REVOKE=YES,
*SPECIAL=YES,OPERATIONS=YES
+OPTIONS HEADING=YES
+VERIFY_INCLUDE USERID=@*,DFLTGRP=*,OWNER=STD*
*VERIFY_EXCLUDE USERID=*,DFLTGRP=*,OWNER=RACF*
```

How to build your own //HRSI0200 file?

RRE does not know any of your HR/CD/ID systems as they reside not on the IBM Host. You can build via REXX and LDAP searches the //HRSI0200 input file.

The //HRSI0200 file must have the same record format as the IRRDBU00 from IBM: RECFM=VB, LRECL=4096.
The record layout for the first two fields (record type and user-ID) has the same as the IBM IRRDBU00 user record type 0200.

Extract from your HR(human resources system)/CD(corporate directory)/ID(identity management) the user-Ids, which must have a RACF user-ID. Use REXX/LDAP or FTP the data to the host and modify the Host file to have the following format:

Pos. 1 – 4	record type	0200	Fix value
Pos. 6 – 13	User-ID	e.g. IBMUSER	
Pos. 15 – 22	Status	ENABLED or DISABLED	DISABLED=REVOKED inactive ENABLED=active

REXX/LDAP sample on how to build your own //HRSI0200 file?

RRE does not know any of your HR/CD/ID system(S), as they reside not the IBM Host. You can build via REXX and LDAP searches the //HRSI0200 input file

e.g. use an LDAP search to obtain your data:

REXX LDAP sample:

```
/* REXX */

HOST = 'XXX.CH.SWISSCOM.COM'
PORTID = 389

LDAP_O = "CN=RACF,CN=TARGETSYSTEMS,CN=INTRANET",
         "CN=* OBJECTCLASS=* DXRSTATE DXRTSSTATE"
/*                                                          */
/* -D BINDDN     BIND DN                                    */
/* -W PASSWD     BIND PASSWD                                */
/* -S SCOPE      ONE OF BASE, ONE, OR SUB (SEARCH SCOPE)    */
/*                                                          */
'GLDSRCH / -H 'HOST '-P 'PORTID' -L 120 -S SUB',
 '-D CN=XRZP001,CN=USERS,CN=INTRANET -W [PASSWORD] -B 'LDAP_O' >DD:HRSI0200'
IF RC /= 0 THEN DO
   SAY 'GLDSRCH ENDED WITH RETURN CODE = 'RC
END
EXIT RC
```

Filter Control Statements (//VERINPUT DD)

HR/CD verification against RACF and vice versa

Following control statements can be utilized to obtain the necessary HR versus RACF verification reports:

DDname	Verbs	Keywords	Comment	Default
//VERINPUT	*	N/A	Comment line	N/A
	+OPTIONS Note: only one statement allowed	HEADING=YES or NO	Print headings (title lines)	YES
		PROTECTED=YES or NO or blank. The keyword is not required.	Select only “RACF” user-Ids from //IRRI0200 DD DSN= marked as protected. This keyword is ignored by the selection process for //HRSI0200 records.	N/A
		REVOKE=YES or NO or blank. The keyword is not required.	Select only “RACF” user-Ids from //IRRI0200 DD DSN= marked as revoked. This keyword is ignored by the selection process for //HRSI0200 records.	N/A
		SPECIAL=YES or NO or blank. The keyword is not required.	Select only “RACF” user-Ids from //IRRI0200 DD DSN= marked as special This keyword is ignored by the selection process for //HRSI0200 records.	N/A
		OPERATIONS=YES or NO or blank. The keyword is not required.	Select only “RACF” user-Ids from //IRRI0200 DD DSN= marked as operations This keyword is ignored by the selection process for //HRSI0200 records.	N/A
	+VERIFY_INCLUDE Note: you can define as many +VERIFY_ statements as required. Make sure the region size is set to e.g. REGION=0M	USERID=	Select a user-ID. Generic Ids are supported incl. The ‘?’ as substitution character. Only the user-ID will be compared against the //HRSI0200 input file.	Blanks=all
		DFLTGRP=	Select a default group-ID. Generic Ids are supported incl. The ‘?’ as substitution character.	Blanks=all

		OWNER=	Select a default owner-ID. Generic Ids are supported incl. The '?' as substitution character.	Blanks=all
	+VERIFY_EXCLUDE	Note: the same rules apply like for +VERIFY_INCLUDE verb.		
	Note: 1. All records matching a "+VERIFY_" will be included or excluded. Input to the verification process are //HRSI0200 and //IRRI0200 (RACF offloaded file in IBM's IRRDBU00 format). Only record type 0200 will be processed. The include process will be performed first. An exclude of USERID=* will be ignored for the all //HRSI0200 records. 2. A compare will be done with all keywords except for the //HRSI0200 file. This file must have the same format as the IRRI0200 (IRRDBU00), whereby the tool checks only for record type 0200 at position 1-4 and at position 6-13 for the user-id. 3. The file //HRSI0200 must be build by the customer due to the fact that each customer has his own HR or CD system in place. Currently we are checking only the first 13 positions (record type and user-ID).			

Sample:

```
//VERINPUT   DD *
*
+OPTIONS HEADING=YES
+VERIFY_INCLUDE USERID=@*,DFLTGRP=*,OWNER=MIX*
+VERIFY_INCLUDE USERID=$*,DFLTGRP=*,OWNER=MAX*
*
+VERIFY_EXCLUDE USERID=*,DFLTGRP=*,OWNER=RACF*
+VERIFY_EXCLUDE USERID=*,DFLTGRP=HKROC,OWNER=TEST*
```

DDNAMES related to the HR/CD and RACF verification process

DDNAME	Description
VERINPUT	Input file - Control statments
VERPRINT	Print file – lists all //VERINPUT control statements. If an error occurred please review this output.
VERHRLST	Print file – lists unfiltered all //HRSI0200 records "AS IS".
VERHRMIS	Print file – lists all user-Ids from the //HRSI0200 file, which could not be found in RACF. This means you have defined user-Ids in your HR or CD, which do simply not exist in RACF or your +VERIFY_ verbs have excluded these IDS.
VERRALST	Print file – lists unfiltered all //IRRI0200 records "AS IS".
VERRAMIS	Print file – lists all user-Ids from the //IRRI0200 file, which could not be found in HR/CD. This means you have defined user-Ids in your RACF, which do simply not exist in the HR/CD or your +VERIFY_ verbs have excluded these IDS.
VERRANEV	Print file – lists unfiltered all RACF user-Ids, which 'never' logged on (= never used).
VERRAREV	Print file – lists unfiltered all RACF user-Ids, which have the status 'revoked'.
VERRAOPR	Print file – lists unfiltered all RACF user-Ids, which have the attribute 'operations and/or special'.
VERRAPRO	Print file – lists unfiltered all RACF user-Ids, which have the attribute 'protected'.
VERRCDEL	RACF command file (DCB=(RECFM=FB,LRECL=80)) – contains RACF delete user-ID commands for user-Ids not found in //HRSI0200. It is up to each installation to decide on what they want to do with user-Ids not found in the HR/CD system.
VERRCREV	RACF command file (DCB=(RECFM=FB,LRECL=80)) – contains RACF ALTUSER REVOKE user-ID commands for user-Ids not found in //HRSI0200. It is up to each installation to decide on what they want to do with user-Ids not found in the HR/CD system.
VERRCALT	RACF command file (DCB=(RECFM=FB,LRECL=80)) – contains RACF ALTUSER OWNER(new_ID) DFLTGRP(new_ID) REVOKE user-ID commands for user-Ids not found in //HRSI0200. It is up to each installation to decide on what they want to do with user-Ids not found in the HR/CD system. The user must modify the generated control statements accordingly.

Output Samples:

//VERHRLST lists all HR/CD entries ‘as is’:

```
******************************** TOP OF DATA ***************************************************************************
DEB$SW15-10 HR USER-IDS ENTRIES AS IS (ALL)             ALS(C) RRE340 07/03/05 12.33  RACF VERS 2608               PAGE:         1
                                                                                                                     DATE:2005-07-06
            JOBNAME :XRZP001S STEPNAME:RA2VERIF PROCNAME:                                                            TIME:   8:10:01
USERID   INFORMATION (ERROR MESSAGES ETC.)
-------- -------------------------------------------
VOGEL
TRXUMO

DEB$SW15-10 HR USER-IDS ENTRIES AS IS (ALL)             ALS(C) RRE340 07/03/05 12.33  RACF VERS 2608               PAGE:       213
                                                                                                                     DATE:2005-07-06
            JOBNAME :XRZP001S STEPNAME:RA2VERIF PROCNAME:                                                            TIME:   8:10:01
USERID   INFORMATION (ERROR MESSAGES ETC.)
-------- -------------------------------------------


===> TOTAL NUMBER OF USER-IDS READ     :         10.553
```

//VERHRMIS lists all HR/CD entries missing in RACF based on filter criteria’s:

```
******************************** TOP OF DATA ***************************************************************************
DEB$SW17-10 HR USER-IDS MISSING IN THE "RACF" SYSTEM(S)  ALS(C) RRE340 07/03/05 12.34  RACF VERS 2608               PAGE:         1
                                                                                                                     DATE:2005-07-06
            JOBNAME :XRZP001S STEPNAME:RA2VERIF PROCNAME:                                                            TIME:   8:14:17
USERID   INFORMATION (ERROR MESSAGES ETC.)
-------- -------------------------------------------
ARM3SE
ART3SS

DEB$SW17-10 HR USER-IDS MISSING IN THE "RACF" SYSTEM(S)  ALS(C) RRE340 07/03/05 12.34  RACF VERS 2608               PAGE:         2
                                                                                                                     DATE:2005-07-06
            JOBNAME :XRZP001S STEPNAME:RA2VERIF PROCNAME:                                                            TIME:   8:14:17
USERID   INFORMATION (ERROR MESSAGES ETC.)
-------- -------------------------------------------


===> TOTAL NUMBER OF USER-IDS VERIFIED :         10.552

===> TOTAL NUMBER OF USER-IDS MISSING  :             23
```

//VERPRINT lists all filter statements:

```
VERPRINT-10 CONTROL STATEMENTS (COMPARE HR:RACF AND RACF:HR)       ALS(C) RRE340 07/03/05 12.40   RACF VER:2608      PAGE:         1
                                                                                                                     DATE:2005-07-06
            JOBNAME :XRZP001S STEPNAME:RA2VERIF PROCNAME:                                                            TIME:   8:10:01

CONTROL CARD(S) READ VIA //VERINPUT                                  ERROR MESSAGE
-------------------------------------------------------------------- ------------------------------------------------

*
*OPTIONS HEADING=YES,PROTECTED=YES,REVOKE=YES,
*SPECIAL=YES,OPERATIONS=YES
+OPTIONS HEADING=YES
+VERIFY_INCLUDE USERID=@*,DFLTGRP=*,OWNER=STD*
+VERIFY_EXCLUDE USERID=*,DFLTGRP=RACFTUID,OWNER=*
                                                                      >-- EXCLUDE OF "*" OR "**" FOR USERID=  WILL BE IGNORED.
                                                                       THIS RESTRICTION APPLIES ONLY TO "HR" DATA
```

//VERRALST lists all RACF user-IDS ‘as is’:

```
DEB$SW14-10 RACF IRRDBU00 TYPE 0200 USER RECORDS (ALL)   ALS(C) RRE340 07/03/05 12.33  RACF VERS 2608               PAGE:         1
                                                                                                                     DATE:2005-07-06
            JOBNAME :XRZP001S STEPNAME:RA2VERIF PROCNAME:                                                            TIME:   8:10:01
USERID   USER NAME            AUTHDATE   OWNER    P S O R G ATTR DFLTGRP. LAST-LOGON TIME     INSTALLATION DATA
-------- -------------------- ---------- -------- - - - - - ---- -------- ---------- -------- ----------------------------------------
FIATFIAT  Intercept           2000-07-17 MERCURY  N N N Y N      RACFCICS 2000-07-17 14:17:46 JDBC-access
Etc.

DEB$SW14-10 RACF IRRDBU00 TYPE 0200 USER RECORDS (ALL)   ALS(C) RRE340 07/03/05 12.33  RACF VERS 2608               PAGE:       284
                                                                                                                     DATE:2005-07-06
            JOBNAME :XRZP001S STEPNAME:RA2VERIF PROCNAME:                                                            TIME:   8:10:01
USERID   USER NAME            AUTHDATE   OWNER    P S O R G ATTR DFLTGRP. LAST-LOGON TIME     INSTALLATION DATA
-------- -------------------- ---------- -------- - - - - - ---- -------- ---------- -------- ----------------------------------------


===> TOTAL NUMBER OF USER-IDS READ      :        14.138

===> TOTAL NUMBER OF USER-IDS PROTECTED :           820

===> TOTAL NUMBER OF USER-IDS SPECIAL   :            10

===> TOTAL NUMBER OF USER-IDS OPERATIONS:             3

===> TOTAL NUMBER OF USER-IDS REVOKED   :         1.377

===> TOTAL NUMBER OF USER-IDS NEVER USED:           931
```

//VERRAMIS lists all RACF user-IDS missing in HR/CD (HRSI0200) based on filter criteria's:

```
DEB$SW16-10 RACF USER-IDS MISSING IN THE "HR" SYSTEM(S)  ALS(C) RRE340 07/03/05 12.34  RACF VERS 2608               PAGE:         1
                                                                                                                  DATE:2005-07-06
            JOBNAME :XRZP001S STEPNAME:RA2VERIF PROCNAME:                                                         TIME:   8:14:16
USERID   USER NAME            AUTHDATE   OWNER    P S O R G ATTR DFLTGRP. LAST-LOGON TIME     INFORMATION (ERROR MESSAGES ETC.)
-------- -------------------- ---------- -------- - - - - - ---- -------- ---------- -------- ----------------------------------------
AGR100   Mike Norton          2005-05-20 TETRAPAK N N N N N      TETRAPAK                    ? NO DESCRIPTION
                                                                                             USER NEVER LOGGED ON
MILE07   LEADS Bill          2005-05-24 TETRAPAK N N N N N      TETRAPAK                    ? NO DESCRIPTION

                                                                                             PROTECTED USER
DEB$SW16-10 RACF USER-IDS MISSING IN THE "HR" SYSTEM(S)  ALS(C) RRE340 07/03/05 12.34  RACF VERS 2608               PAGE:        43
                                                                                                                  DATE:2005-07-06
            JOBNAME :XRZP001S STEPNAME:RA2VERIF PROCNAME:                                                         TIME:   8:14:16
USERID   USER NAME            AUTHDATE   OWNER    P S O R G ATTR DFLTGRP. LAST-LOGON TIME     INFORMATION (ERROR MESSAGES ETC.)
-------- -------------------- ---------- -------- - - - - - ---- -------- ---------- -------- ----------------------------------------


===> TOTAL NUMBER OF USER-IDS VERIFIED  :       12.287

===> TOTAL NUMBER OF USER-IDS MISSING   :        1.754

===> TOTAL NUMBER OF USER-IDS PROTECTED :           20

===> TOTAL NUMBER OF USER-IDS SPECIAL   :           10

===> TOTAL NUMBER OF USER-IDS OPERATIONS:            0

===> TOTAL NUMBER OF USER-IDS REVOKED   :        1.166
```

Sample creating a PDF to Email it:

The XMITIP program is public domain (refer to www.cbttape.org) to create a PDF and is not included on the product CD/TAPE:

```
//GETUSER   EXEC PGM=IKJEFT1B,DYNAMNBR=200
//SYSEXEC   DD   DISP=SHR,DSN=FERRARI.REXX.LIB
//SYSTSPRT  DD   SYSOUT=*
//HRSI0200  DD   DISP=(,PASS),DSN=&&TEMP,LRECL=80,RECFM=FB
//SYSTSIN   DD   *
%CDSEARCH
/*
```

```
//*
//* FILTER THE USERS (ONLY ENABLED ONES) AND OUTPUT '0200' RECORDS
//*
//FILTER    EXEC PGM=IKJEFT1B,COND=(0,LT),DYNAMNBR=200
//SYSEXEC   DD   DISP=SHR,DSN=FERRARI.REXX.LIB
//HRSI0200  DD   DISP=(,PASS),DSN=&&TEMP2,LRECL=4096,RECFM=VB
//INPUT     DD   DSN=&&TEMP,DISP=(OLD,DELETE,DELETE)
//SYSTSPRT  DD   SYSOUT=*
//SYSTSIN   DD   *
%CDFILTER
/*
```

```
//RA2VERIF  EXEC PGM=DEB$SW1H,COND=(0,LT)
//STEPLIB   DD   DISP=SHR,DSN=RA2002.LINKLIB
//*
//* INPUT FILES
//*
//IRRI0200  DD   DISP=SHR,DSN=RA2.IRRDBU.IRRI0200.VB(-0)
//HRSI0200  DD   DSN=&&TEMP2,DISP=(OLD,DELETE,DELETE)
//*
//* HRS RELATED INFORMATION (ALL HR IDS AND THEIR MISSING IDS IN RACF)
//*
//VERHRLST  DD   SYSOUT=*   * HR HRSI0200 USERIDS LISTED "ASIS"
//VERHRMIS  DD   DISP=(,PASS),DSN=&&VERHRMIS
//*
//* RACF RELATED INFORMATION (ALL RACF UIDS AND THEIR MISSING HR UIDS)
//*
//VERINPUT  DD DISP=SHR,DSN=YOURE.RRE.RULEDATA(R001VER)
//VERPRINT  DD   SYSOUT=*   * PRINT +VERIFY CONTROL STATEMENTS
//VERRALST  DD   SYSOUT=*   * RACF IRRI0200 USERIDS LISTED "ASIS"
//VERRAMIS  DD   DISP=(,PASS),DSN=&&VERRAMIS
//VERRANEV  DD   SYSOUT=*   * RACF LIST ALL USERIDS NEVER USER "ASIS"
//VERRAOPR  DD   SYSOUT=*   * RACF LIST ALL OPER/SPECIAL USERIDS "ASIS"
//VERRAPRO  DD   SYSOUT=*   * RACF LIST ALL PROTECTED USERIDS "ASIS"
//VERRAPRO  DD   SYSOUT=*   * RACF LIST ALL REVOKED USERIDS "ASIS"
//*
//* USER RACF COMMANDS BASED ON VERIFICATION PROCESSING
//* - AN INSTALLATION MUST DECIDE WHAT TO DO WITH USERIDS NOT FOUND
//*   IN THE "HR" (HRSI0200) FILE.
//* - EITHER YOU DELETE, REVOKE AND OR ALTER THE USERIDS
//* - YOU MIGHT AS WELL CHANGE THE +VERIFIY STATEMENTS TO EXCLUDE
//*   CERTAIN USERIDS
//*
//VERRCDEL  DD   SYSOUT=*   * RACF DELETE ALL USERIDS NOT FOUND IN "HR"
//VERRCREV  DD   SYSOUT=*   * RACF REVOKE ALL USERIDS NOT FOUND IN "HR"
//VERRCALT  DD   SYSOUT=*   * RACF ALU ALL USERIDS NOT FOUND IN "HR"
```

```
//* EMAIL ACCOUNTS THAT ARE IN CD (WITH RACF ROLE) BUT NOT IN RACF
//*
//EMAIL1    EXEC BATCHTMP
//TEMPDD    DD   DISP=(OLD,DELETE),DSN=&&VERHRMIS
//SYSIN     DD   *
 XMITIP MARCEL_SCHMIDT@SWISSCOM.COM +
   SUBJECT 'CD TO RACF VERIFICATION - MISSING ACCOUNTS IN RACF' +
   FROM MARCEL_SCHMIDT@SWISSCOM.COM +
   MSGDS 'FERRARI.XMITIP.LIB(IVPMSG)' +
   FILEDD TEMPDD +
   FORMAT PDF/DS:'FERRARI.XMITIP.LIB(CDCFG)'
/*
```

Config for PDF:

```
* TXT2PDF CONFIGURATION FILE CREATED ON 8 OCT 2002 06:51:28 BY %TXT2PDFI
CC YES
COMPRESS 9
ENCRYPT ST/FERRARI/CDTEAM/128/NE/NC
ORIENT  LANDSCAPE
PAPER A4/GREENBAR/HOLED
CONFIRM YES
OUTLINE RC/0/3/5



THIS E-MAIL, INCLUDING ATTACHMENTS, IS INTENDED FOR THE PERSON(S) OR
COMPANY NAMED AND MAY CONTAIN CONFIDENTIAL AND/OR LEGALLY PRIVILEGED
INFORMATION. UNAUTHORIZED DISCLOSURE, COPYING OR USE OF THIS INFORMATION
MAY BE UNLAWFUL AND IS PROHIBITED. IF YOU ARE NOT THE INTENDED RECIPIENT,
PLEASE DELETE THIS MESSAGE AND NOTIFY THE SENDER
```

DEB$SW1R - RACF RULES VERIFICATION (RRV)

Purpose:

- Verify the RACF based on installation defined 'rules' without having to utilize any exits at all.
- An installation can specify rules for all RACF base segments (groups, users, connects, datasets and general resource profiles.
- The intention of this utility is to simplify audits and profile verification.

Especially if you have one or more RACF environments, which have been maintained by a number of people over the last 10-20 years, it is most difficult to find out "what is what" and if all the rules (if any) are properly used. RACF Exits are for most companies not a feasible option due to the ever-changing security environment.

To execute this batch program an 'off-loaded' RACF DB is required. To set-up all the rules will take a considerable amount of time, especially in case no proper naming standards have been implemented.
RA/2 (search and tag facility under option 3.100, 200, 205, 400 and 500) can be utilized to generate the majority of the rules you may required, saving an installation a lot of time and money.

JCL required to run DEB$SW1R

Run the following JCL (refer to the YOURE.RRE.SAMPLIB member DEB$SW1R) to create the reports:

```
//RA2VERIF   EXEC PGM=DEB$SW1R
//STEPLIB    DD   DISP=SHR,DSN=YOUR.YOURE.RRE.LINKLIB
//*
//* COMMAND/TEMPLATE FILE
//*
//COMMANDS   DD   DISP=SHR,DSN=YOUR.COMMANDS.PDS.FILE
//*
//* INPUT FILES
//*

//IRRI0100   DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0100.VB(0)
```

```
//IRRI0200   DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0200.VB(0)
```

```
//IRRI0205   DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0205.VB(0)
```

```
//IRRI0400   DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0400.VB(0)
//           DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0401.VB(0)
//           DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0402.VB(0)
//           DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0403.VB(0)
//           DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0404.VB(0)
//           DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0405.VB(0)
//           DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0410.VB(0)
//           DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0420.VB(0)
//           DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0421.VB(0)
```

```
//IRRI0500   DD   DISP=SHR,DSN=YOUR.IRRDBU.IRRI0500.VB(0)
```

```
//SYSPRINT     DD   SYSOUT=*
//SYSOUT       DD   SYSOUT=*
//SORTWK01     DD   UNIT=SYSDA,SPACE=(CYL,(9,9))
//SORTWK02     DD   UNIT=SYSDA,SPACE=(CYL,(9,9))
//SORTWK03     DD   UNIT=SYSDA,SPACE=(CYL,(9,9))
//SORTWK04     DD   UNIT=SYSDA,SPACE=(CYL,(9,9))
//$ORTPARM DD *
NORC16
//SORTCNTL DD *
 DEBUG         NOABEND
 OPTION        VLSHRT
```

DDnames:

- //IRRIxxxx must be RECFM=VB as outlined by the IBM RACF IRRDBU00 offload program. These files are used as input to the program. In case the files are not split by record type then define on all //IRRIxxxx the offloaded RACF database flat file.
  - xxxx = IRRDBU00 record type.
- //COMMANDS must be RECFM=FB, LRECH=80, DSORG=PO. This file contains the product-supplied commands and the user defined commands. The first letter '$' is reserved for product supplied commands.
- //SORTxxxxx DDNAMES are required when the option VERIFY=YES is set.
- //SYSOUT is required by the SORT program
- //???Cxxxx must be RECFM=FB, LRECH=80, DSORG=PS.
  - ??? = USR, GRP, CON, DSN or RES
  - xxxx = IRRDBU00 record type

Note:

Control cards generated by this program must reside in separate flat files and not e.g. in one common PDS, otherwise you will encounter the following ABEND:
IEC143I 213-30,IFG0194D,MYJOBID,RA2VERIF,DSNC0400. This is due to the fact that multiple files are open at the same time to generate control cards.

JCL pertaining to group profiles (record type 0100)

```
//*
//* GROUP RULES RELATED DDNAMES
//* - RACF COMMANDS AND LISTINGS ARE BASED ON GROUPID-RULE PROCESSING
//*
//GRPPRINT   DD SYSOUT=*    * PRINT GROUPID_RULE  CONTROL STATEMENTS
//GRPRULEX   DD SYSOUT=*    * RACF GROUPIDS WITHOUT ANY RULE
//GRPRULEG   DD SYSOUT=*    * RACF GROUPIDS WITH A MATCHING RULE
//GRPRULEF   DD SYSOUT=*    * RACF GROUPIDS WHICH FAILED RULES CHECKS
//GRPRULES   DD *           * RACF BASE GROUPID RULES
*
* DEFINE RULES FOR GROUP PROFILES RECORD TYPE 0100
* +OPTIONS SPECIFIES THE DEFAULT VALUES TO BE ASSIGNED IF
*  NO RULE DOES MATCH
*
+OPTIONS     SET_OWNER=JAMES,SET_SUPGROUP=TEST
+GROUP_RULE  NAME='RULEA   ',GROUPID=T*
*
+GROUPID_RULE NAME='RULEB   ',GROUPID=T*,
              OWNER=TEST*,SUPGROUP=SYS1,
              SET_OWNER=T*USR,SET_SUPGROUP=SYS1SUP
*
+GROUPID_RULE NAME='Z GROUP',GROUPID=Z*,
              OWNER=TEST*,SUPGROUP=SYS1,
              SET_OWNER=Z*USR,SET_SUPGROUP=SYS1SUP
*
```

JCL pertaining to user-Id profiles (record type 0200)

```
//*
//* USER RULES RELATED DDNAMES
//* - RACF COMMANDS AND LISTINGS ARE BASED ON USERID-RULE PROCESSING
//*
//USRPRINT   DD SYSOUT=*    * PRINT USERID_RULE  CONTROL STATEMENTS
//USRRULEF   DD SYSOUT=*    * RACF USER-IDS WHICH FAILED RULES CHECKS
//USRRULEG   DD SYSOUT=*    * RACF USER-IDS WHICH PASSED RULES CHECKS
//USRRULEX   DD SYSOUT=*    * RACF USER-IDS WHICH HAVE NO RULES
//USRC0200   DD DSN=        * GENERATED CONTROL CARDS IF REQUESTED
//USRRULES   DD *           * RACF BASE USERID RULES
*
* DEFINE RULES FOR USER PROFILES RECORD TYPE 0200
* +OPTIONS SPECIFIES THE DEFAULT VALUES TO BE ASSIGNED IF
*  NO RULE DOES MATCH
*  YOU CAN SET THE OWNER, DEFAULT GROUP
*
+OPTIONS     SET_OWNER=USROWN01,SET_DFLTGRP=USRGRP01
*
+USERID_RULE NAME='TECH ',USERID=TEC*,
             OWNER=USRTECH,DFLTGRP=USRTECH
+USERID_RULE NAME='MODEL',USERID=?#??????,
             OWNER=USRMOD01,DFLTGRP=USRMOD01,
             SET_OWNER=USRMOD01,SET_DFLTGRP=USRMOD01
```

JCL pertaining to connect profiles (part of user-Id profiles record type 0205)

```
//*
//* CONNCT RULES RELATED DDNAMES
//* - RACF COMMANDS AND LISTINGS ARE BASED ON CONNECT-RULE PROCESSING
//*
//CONPRINT   DD SYSOUT=*    * PRINT CONNECT_RULE  CONTROL STATEMENTS
//CONRULEX   DD SYSOUT=*    * RACF CONNECTS WITHOUT ANY RULE
//CONRULEG   DD SYSOUT=*    * RACF CONNECTS WITH A MATCHING RULE
//CONRULEF   DD SYSOUT=*    * RACF CONNECTS WHICH FAILED RULES CHECKS
//CONC0205   DD DSN=        * GENERATED CONTROL CARDS IF REQUESTED
//CONRULES   DD *           * RACF BASE CONNECT USERID RULES
*
* DEFINE RULES FOR CONNECT PROFILES RECORD TYPE 0205
* +OPTIONS SPECIFIES THE DEFAULT VALUES TO BE ASSIGNED IF
*  NO RULE DOES MATCH
*
+OPTIONS     SET_OWNER=CONWON,SET_GROUPID=SETGRPID
+CONNECT_RULE NAME='THIS IS A CONNECT TEST',
             OWNER=FCT*,GROUPID=SYS1,
             REVOKE=YES,
             SET_OWNER=SETOWNER,SET_GROUPID=SETGRPG
+CONNECT_RULE NAME='TEST ON $KIINC',
             OWNER=$KIINC,GROUPID=$KIINC,
             SET_OWNER=$KINCC,SET_GROUPID=SETKINCC
+CONNECT_RULE NAME='TEST ON REVOKED',
             REVOKE=YES,
             SET_OWNER=$REVCC,SET_GROUPID=REVKINCC
```

JCL pertaining to group profiles (record type 0400)

```
//*
//* DATASET RULES RELATED DDNAMES
//* - RACF COMMANDS AND LISTINGS ARE BASED ON DATASET-RULE PROCESSING
//*
//DSNPRINT   DD SYSOUT=*    * PRINT DATASETT_RULE CONTROL STATEMENTS
//DSNRULEX   DD SYSOUT=*    * RACF DATASETS WITHOUT ANY RULE
//DSNRULEG   DD SYSOUT=*    * RACF DATASETS WITH A MATCHING RULE
//DSNRULEF   DD SYSOUT=*    * RACF DATASETS WHICH FAILED RULES CHECKS
//DSNC04OW   DD SYSOUT=B    * RACF DATASETS WHERE OWNER NE HLQ
//DSNCLEAN   DD SYSOUT=B    * RACF DATASETS WHICH FAILED VERFIFY=YES
//DSNVERIF   DD SYSOUT=*    * RACF DATASETS WHICH FAILED VERFIFY=YES
//DSNRULES   DD *           * RACF BASE USERID RULES
*
* DEFINE RULES FOR GROUP PROFILES RECORD TYPE 0400
* +OPTIONS SPECIFIES THE DEFAULT VALUES TO BE ASSIGNED IF
*  NO RULE DOES MATCH
*
+OPTIONS     SET_OWNER=SETOWN,SET_UACC=SETNONE,HLQ=TSO
+DATASET_RULE NAME='THIS IS A DATASET TEST1',
             DATASET=SYS1.**,OWNER=*,
             SET_OWNER=SETOWNER,SET_UACC=READ
+DATASET_RULE NAME='THIS IS A DATASET TEST2',
             FDATASET=IBMUSER.*.**,OWNER=*,
             SET_OWNER=AMEXT011,SET_UACC=ALTER
```

JCL pertaining to general resources profiles (record type 0500)

```
//*
//* GEN.RES RULES RELATED DDNAMES
//*
//RESPRINT   DD SYSOUT=*    * PRINT RESNAME_RULE CONTROL STATEMENTS
//RESRULEX   DD SYSOUT=*    * RACF RESOURCE WITHOUT ANY RULE
//RESRULEG   DD SYSOUT=*    * RACF RESOURCE WITH A MATCHING RULE
//RESRULEF   DD SYSOUT=*    * RACF RESOURCE WHICH FAILED RULES CHECKS
//RESRULES   DD *           * RACF BASE USERID RULES
*
* DEFINE RULES FOR GEN.RES. PROFILES RECORD TYPE 0500
* +OPTIONS SPECIFIES THE DEFAULT VALUES TO BE ASSIGNED IF
*  NO RULE DOES MATCH
*
+OPTIONS     SET_OWNER=SGRESOWN,SET_UACC=RESUACC
+RESNAME_RULE NAME='RA2002 FIXED RULE     ',
             CLASS=FACILITY,FRESNAME=RA2002.DEC$CG10,OWNER=ALAIN,
             SET_OWNER=SETGOWNR,SET_UACC=READ
```

Group-ID Rules (Filter) Control Statements (//GRPRULES DD *)

Following control statements can be utilized to perform the RACF group-ID verification:

DDname	Verbs	Keywords	Comment	Default
//GRPRULES	*****	N/A	Comment line	N/A
	+OPTIONS Note: only one statement allowed	SET_OWNER=	Assign new default owner if all rules fail. The global variable name &SGOWNER can be used in the command member for the failing rule.	N/A
		SET_SUPGROUP=	Assign new superior group if all rules fail. The global variable name &SGSUPGRP can be used in the command member for the failing rule.	N/A
		Note: all generated RACF control statements must be reviewed prior executing them. This utility does not automatically update the RACF DB.		
	+GROUPID_RULE **or** +GROUP_RULE or +GRP_RULE or +GR Note: you can define as many rule	NAME=	Specifies a rule name, which can be up to 32 characters. This rule name will appear on the generated listings as a reference. We recommend assigning for each rule a meaningful name.	N/A

	statements as required. Make sure the region size is set to e.g. REGION=0M	GROUPID=	Specifies a RACF group-ID to be verified.	N/A
		OWNER=	Specifies a RACF Owner-ID to be verified.	N/A
		SUPGROUP=	Specifies a RACF superior-group-ID to be verified.	N/A
		DATA=YES or NO	Specifies that installation data must be present.	N/A
		AUTHDATE=(yyyy-mm-dd,??) or AUTH_DATE=(yyyy-mm-dd,??)	AUTHDATE= allows to restrict a rule to a given date range. The compare will be done in the length of the supplied date e.g. AUTHDATE=(2000,GE) will only compare the first 4 digits. ??= EQ, GE, GT, LE or LT. AUTHDATE is the date when a profile was 'defined' to RACF.	N/A
		SET_OWNER=	Assign new default owner if this rule fails. The global variable name &SOWNER can be used in the command member for the failing rule.	N/A
		SET_SUPGROUP=	Assign new default superior group if this rule fails. The global variable name &SSUPGRP can be used in the command member for the failing rule.	N/A
	Note: • The key fields for rule checking support generic filtering. A key field can also contain the substitution character '?' e.g. IBM?A* • If all supplied rules fail, the program will create the necessary reports and RACF control cards to alter the profiles.			

Sample: Failing Group-IDs

```
DEB$SW50-10 RACF GROUP-IDS WHICH FAILED RULES CHECKING   ALS(C) RRE340 10/26/05 14.05  RACF VERS 2608               PAGE:         1
                                                                                                                    DATE:2005-10-27
            JOBNAME :XRZP001A STEPNAME:RA2RULES PROCNAME:                                                           TIME:   9:37:07
GROUPID  SUPGROUP AUTHDATE   OWNER    UACC     DATA (INSTALLATION DATA)                                FAILING RULE NAME(S)
-------- -------- ---------- -------- -------- ------------------------------------------------------- -----------------------------

$$$$TEST SYS1     2005-11-09 IBMUSER  NONE     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA '$  DATA'
$$DB2    SYS1     2005-04-10 SYS1     NONE     DB2      STC FUNC                                       '$  DATA'
$$FUNC   SYS1     2005-04-10 SYS1     NONE     GROUP FOR SYSTEM FUNCTIONS                             '$  DATA'
$$STC    SYS1     2005-04-10 SYS1     NONE     GROUP FOR STARTED TASKS                                '$  DATA'
```

Command generation

For each failing rule it is possible to generate any kind of commands. Below are the variable names listed which can be used in a command member (DDname //COMMANDS). Each time a rule fails and the keyword COMMAND=member name has been specified, the member will be read from //COMMANDS PDS file and all variables replaced. The output will be written to //GRPC0100. This facility works similar to the ISPF FTINCL function, however it does not support e.g.)SEL,)IM logic.

Variable names filled in by the IRRI0100 record:

The following variables can be used to generate commands related to group-Ids:

RACF IRRDBU00 NAME	RA/2 VARIABLE	FORMAT	SAMPLE DATA
NAME	&R10NAME		$$WEBPUB
SUPGRP_ID	&R10SUPG		$$WEB
CREATE_DATE	&R10AUTHD	YYYY-MM-DD	
OWNER_ID	&R10OWNER		
UACC	&R10UACC		NONE
NOTERMUACC	&R10TUACC	Y OR N (?)	
INSTALL_DATA	&R10DATA		
MODEL	&R10MODEL		

Variable names filled in by the failing rule:

OPTIONS KEYWORD	OPTIONS VARIABLE	FORMAT
SET_SUPGROUP=NAME	&SGSUPGRP	MAX. 8 CHAR
SET_OWNER=NAME	&SGOWNER	MAX. 8 CHAR

RULE KEYWORD	RULE VARIABLE	FORMAT
SET_SUPGROUP=NAME	&SSUPGRP	MAX. 8 CHAR
SET_OWNER=NAME	&SOWNER	MAX. 8 CHAR

User-ID Rules (Filter) Control Statements (//USRRULES DD *)

Following control statements can be utilized to perform the RACF user-ID verification:

DDname	Verbs	Keywords	Comment	Default
//USRRULES	*	N/A	Comment line	N/A
	+OPTIONS Note: only one statement allowed	SET_OWNER=	Assign new default owner if all rules fail. Variable name &SUOWNER will be set.	N/A
		SET_DFLTGRP=	Assign new default group if all rules fail. Variable name &SUDFLTGRP will be set.	N/A
		Note: all generated RACF control statements must be reviewed prior executing them. This utility does not automatically update the RACF DB.		
	+USERID_RULE or +USER_RULE +USR_RULE +UR Note: you can define as many rule statements as required. Make sure the region size is set to e.g. REGION=0M	NAME=	Specifies a rule name, which can be up to 32 characters. This rule name will appear on the generated listings as a reference. We recommend assigning for each rule a meaningful name.	N/A
		USERID=	Specifies a RACF user-ID to be verified.	N/A
		OWNER=	Specifies a RACF Owner-ID to be verified.	N/A
		DFLTGRP=	Specifies a RACF default-group-ID to be verified.	N/A
		DATA=YES or NO	Specifies that installation data must be present.	N/A
		PROTECTED=YES or NO	Specifies that the user-ID must be protected ('Y') or not.	N/A

		REVOKE=YES or NO	Specifies that the user-ID must be revoked ('Y') or not.	N/A
		SPECIAL=YES or NO	Specifies that the user-ID must have the special attribute ('Y') or not.	N/A
		OPERATIONS=YES or NO	Specifies that the user-ID must have the operations attribute ('Y') or not.	N/A
		ATTRIBUTE=	Other user attributes (RSTD for users with RESTRICTED attribute).	N/A
		LJDATE=YES or NO	Specifies that a logon date must be present ('Y') or not.	N/A
		AUTHDATE=(yyyy-mm-dd,??) or AUTH_DATE=(yyyy-mm-dd,??)	AUTHDATE= allows to restrict a rule to a given date range. The compare will be done in the length of the supplied date e.g. AUTHDATE=(2000,GE) will only compare the first 4 digits. ??= EQ, GE, GT, LE or LT. AUTHDATE is the date when a profile was 'defined' to RACF.	N/A
		INITDATE=(yyyy-mm-dd,??) or INIT_DATE=(yyyy-mm-dd,??)	INITDATE= allows to restrict a rule to a given date range. The compare will be done in the length of the supplied date e.g. INITDATE=(2000,LT) will only compare the first 4 digits. ??= EQ, GE, GT, LE or LT. INITDATE is the date when a profile was last used e.g. LOGON (=JOBINIT). To find userids, which have NO logon date (never used) you can specify e.g. INITDATE=(1,LT).	N/A
		SET_OWNER=	Assign new default owner if this rule fails. Variable name &SOWNER will be set.	N/A
		SET_DFLTGRP=	Assign new default group if this rule fails. Variable name &SDFLTGRP will be set.	N/A
		COMMAND=	Invoke command member from //COMMANDS if a rule fails. Command members can be used to fix problems. Command members are only invoked if a rule fails..	N/A
	Note: • The key fields for rule checking support generic filtering. A key field can also contain the substitution character '?' e.g. IBM?A* • If all supplied rules fail, the program will create the necessary reports and RACF control cards to alter the profiles.			

Sample: User-IDs which failed the rules checking

```
DEB$SW51-10 RACF USER-IDS WHICH FAILED RULES CHECKING    ALS(C) V3R4M1 11/30/05 00.45  RACF VERS 2608              PAGE:         1
                                                                                                              DATE:2005-11-30
            JOBNAME :XRZP0017 STEPNAME:RA2RULES PROCNAME:                                                     TIME:   0:46:00
USERID   USER NAME            AUTHDATE   OWNER    P S O R G ATTR DFLTGRP. LAST-LOGON TIME             RULE NAMES / COMMENT
-------- -------------------- ---------- -------- - - - - - ---- -------- ---------- --------         ----------------------------
TECTRAMM  PERFORMANCE TEST    2006-07-10 MAXTECH  N N N Y N      UMAXTECH 2006-03-11 19:07:25         'TECH USERIDS'
                                                                                                       'LJDATE      '
```

Sample: User-IDs for which a matching rule was found

```
DEB$SW51-20 RACF USER-IDS WHERE A DEFINED RULE MATCHED   ALS(C) V3R4M1 11/30/05 00.45  RACF VERS                    PAGE:        1
                                                                                                                   DATE:2005-11-30
           JOBNAME :XRZP0017 STEPNAME:RA2RULES PROCNAME:                                                           TIME:   0:46:00
USERID   USER NAME            AUTHDATE   OWNER    P S O R G ATTR DFLTGRP. LAST-LOGON TIME             RULE NAMES / COMMENT
-------- -------------------- ---------- -------- - - - - - ---- -------- ---------- --------         ----------------------------

$START   ################### 2001-09-04 MAXFTUID N N N N Y      MAXFTUID 2005-11-23 00:36:15          'LJDATE      '
```

Command generation

For each failing rule it is possible to generate any kind of commands. Below are the variable names listed which can be used in a command member (DDname //COMMANDS). Each time a rule fails and the keyword COMMAND=member_name has been specified, the member will be read from //COMMANDS PDS file and all variables replaced. The output will be written to //USRC0200. This facility works similar to the ISPF FTINCL function, however it does not support e.g.)SEL,)IM logic.

Variable names filled in by the IRRI0200 record:

The following variables can be used to generate commands related to user-Ids:

RACF IRRDBU00 NAME	RA/2 VARIABLE	FORMAT
NAME	&R20NAME	
CREATE_DATE	&R20AUTHD	YYYY-MM-DD
OWNER_ID	&R20OWNER	
ADSP	&R20ADSP	Y OR N (?)
SPECIAL	&R20SPEC	Y OR N (?)
OPER	&R20OPER	Y OR N (?)
REVOKE	&R20REV	Y OR N (?)
GRPACC	&R20GRPA	Y OR N (?)
PWD_INTERVAL	&R20PWI	
PWD_DATE	&R20PWL	YYYY-MM-DD
PROGRAMMER	&R20PGMN	
DEFGRP_ID	&R20DEFGR	
LASTJOB_TIME	&R20TIME	HH:MM:SS
LASTJOB_DATE	&R20DATE	YYYY-MM-DD
INSTALL_DATA	&R20DATA	
UAUDIT	&R20UAUD	Y OR N (?)
AUDITOR	&R20AUDIT	Y OR N (?)
NOPWD	&R20PWREQ	Y OR N (?)
OIDCARD	&R20IODC	Y OR N (?)
PWD_GEN	&R20GENPW	
REVOKE_CNT	&R20FAIL	
MODEL	&R20MODEL	
SECLEVEL	&R20SECL	
REVOKE_DATE	&R20REVD	YYYY-MM-DD
RESUME_DATE	&R20RESD	YYYY-MM-DD
ACCESS_SUN	&R20WDSUN	Y OR N (?)
ACCESS_MON	&R20WDMON	Y OR N (?)
ACCESS_TUE	&R20WDTUE	Y OR N (?)
ACCESS_WED	&R20WDWED	Y OR N (?)
ACCESS_THU	&R20WDTHU	Y OR N (?)
ACCESS_FRI	&R20WDFRI	Y OR N (?)
ACCESS_SAT	&R20WDSAT	Y OR N (?)
START_TIME	&R20WTSTR	HH:MM:SS
END_TIME	&R20WTEND	HH:MM:SS
SECLABEL	&R20SECLA	
STARTHH_TIME	&R20TIHHS	HH:MM:SS
ENDHH_TIME	&R20TIHHE	HH:MM:SS

Variable names filled in by the failing rule:

```
OPTIONS KEYWORD              OPTIONS VARIABLE   FORMAT
-----------------            ----------------   ----------
SET_DFLTGRP=NAME             &SUDFLTGRP         MAX. 8 CHAR
SET_OWNER=NAME               &SUOWNER           MAX. 8 CHAR
```

```
RULE KEYWORD                 RULE VARIABLE      FORMAT
-----------------            -------------      ----------
SET_DFLTGRP=NAME             &SDFLTGRP          MAX. 8 CHAR
SET_OWNER=NAME               &SOWNER            MAX. 8 CHAR
```

Sample: Command member

```
/* THIS IS A TEST MEMBER TO SHOW HOW COMMANDS WILL WORK */
 ALTUSER  (&R20NAME)           +
          NAME('&R20PGMN ')    +
          DFLTGRP(&R20DEFGR)   +
          SPECIAL              +
          OPERATIONS           +
          NOPASSWORD NOOIDCARD +
          RESTRICTED           +
          OWNER(&R20OWNER)
 PASSWORD INTERVAL(&R20PWI) USER(&R20NAME)
/*                                                    */
 SDFLTGRP    &SDFLTGRP
 SOWNER      &SOWNER
 SUDFLTGRP   &SUDFLTGRP
 SUOWNER     &SUOWNER
```

Connect-ID Rules (Filter) Control Statements (//CONRULES DD *)

Following control statements can be utilized to perform the RACF connect-user-ID verification:

DDname	Verbs	Keywords	Comment	Default
//CONRULES	*	N/A	Comment line	N/A
	+OPTIONS Note: only one statement allowed	SET_OWNER=	Assign new default owner if all rules fail. Assign new group-ID if all rules fail. The global variable name &SCOWNER can be used in the command member for the failing rule.	N/A
		SET_GROUPID=	Assign new group-ID if all rules fail. The global variable name &SCGROUP can be used in the command member for the failing rule.	N/A
		Note: all generated RACF control statements must be reviewed prior executing them. This utility does not automatically update the RACF DB.		
	+CONNECTID_RULE **or** +CONNECT_RULE or +CON_RULE or +CR Note: you can define as many rule statements as required. Make sure	NAME=	Specifies a rule name, which can be up to 32 characters. This rule name will appear on the generated listings as a reference. We recommend assigning for each rule a meaningful name.	N/A
		USERID=	Specifies a RACF user-ID to be verified.	N/A

	the region size is set to e.g. REGION=0M	OWNER=	Specifies a RACF Owner-ID to be verified.	N/A
		GROUPID=	Specifies a RACF connect-group-ID to be verified.	N/A
		REVOKE=YES or NO	Specifies that the connect-user-ID must be revoked ('Y') or not.	N/A
		SPECIAL=YES or NO	Specifies that the connect-user-ID must have the special attribute ('Y') or not.	N/A
		OPERATIONS=YES or NO	Specifies that the connect-user-ID must have the operations attribute ('Y') or not.	N/A
		UACC=	Specifies default universal access authority for all new resources the user defines while connected to the specified group. Valid values are NONE, READ, UPDATE, CONTROL, and ALTER.	N/A
		AUTHDATE=(yyyy-mm-dd,??) or AUTH_DATE=(yyyy-mm-dd,??)	AUTHDATE= allows to restrict a rule to a given date range. The compare will be done in the length of the supplied date e.g. AUTHDATE=(2000,GE) will only compare the first 4 digits. ??= EQ, GE, GT, LE or LT. AUTHDATE is the date when a profile was 'defined' to RACF.	N/A
		SET_OWNER=	Assign new connect-owner if this rule fails. The variable name &SOWNER can be used in the command member for the failing rule.	N/A
		SET_GROUPID=	Assign new connect-group if this rule fails. The variable name &SGROUP can be used in the command member for the failing rule.	N/A
	Note: • The key fields for rule checking support generic filtering. A key field can also contain the substitution character '?' e.g. IBM?A* • If all supplied rules fail, the program will create the necessary reports and RACF control cards to alter the profiles.			

Sample: Failing Connect-IDs

```
DEB$SW52-10 RACF CONNECT-IDS WHICH FAILED RULES CHECKING ALS(C) RRE340 10/26/05 14.18  RACF VERS 2608              PAGE:         1
                                                                                                               DATE:2005-10-27
            JOBNAME :XRZP001A STEPNAME:RA2RULES PROCNAME:                                                      TIME:   9:37:07
USERID   GROUP-ID AUTHDATE   T OWNER    S O R CON.-DATE  TIME                                  FAILING RULE NAME(S)
-------- -------- ---------- - -------- - - - ---------- --------                              -------------------------

$$$$USER $$$$TEST 2001-11-09 G $$$$TEST N N N                                                  -> ALL RULES FAILED
A        $$$$TEST 2005-05-22 U XRZP001  N N N                                                  -> ALL RULES FAILED
A        SYS1     2005-05-22 U AAAUSER  N N N                                                  'THIS IS A CONNECT TEST'
AOF01    SYS1     2004-09-18 U AAAUSER  N N N                                                  'THIS IS A CONNECT TEST'
```

Command generation

For each failing rule it is possible to generate any kind of commands. Below are the variable names listed which can be used in a command member (DDname //COMMANDS). Each time a rule fails and the keyword COMMAND=member_name has been specified, the member will be read from //COMMANDS PDS file and all variables replaced. The output will be written to

//CONC0205. This facility works similar to the ISPF FTINCL function, however it does not support e.g.)SEL,)IM logic.

Variable names filled in by the IRRI0205 record:

The following variables can be used to generate commands related to connect user-Ids:

RACF IRRDBU00 NAME	RA/2 VARIABLE	FORMAT	SAMPLE DATA
NAME	&R30NAME		A
GRP_ID	&R30GROUP		
CONNECT_DATE	&R30AUTHD	YYYY-MM-DD	
OWNER_ID	&R30OWNER		
LASTCON_TIME	&R30TIME	HH:MM:SS	
LASTCON_DATE	&R30DATE	YYYY-MM-DD	
UACC	&R30UACC		NONE
INIT_CNT	&R30INIT		
GRP_ADSP	&R30FLAG1	Y OR N (?)	
GRP_SPECIAL	&R30FLAG2	Y OR N (?)	
GRP_OPER	&R30FLAG3	Y OR N (?)	
REVOKE	&R30FLAG4	Y OR N (?)	
GRP_ACC	&R30FLAG5	Y OR N (?)	
NOTERMUACC	&R30TRM	Y OR N (?)	
GRP_AUDIT	&R30GRPAU	Y OR N (?)	
REVOKE_DATE	&R30REVD	YYYY-MM-DD	
RESUME_DATE	&R30RESD	YYYY-MM-DD	

Variable names filled in by the failing rule:

OPTIONS KEYWORD	OPTIONS VARIABLE	FORMAT
SET_GROUP=NAME	&SCGROUP	MAX. 8 CHAR
SET_OWNER=NAME	&SCOWNER	MAX. 8 CHAR

RULE KEYWORD	RULE VARIABLE	FORMAT
SET_GROUP=NAME	&SGROUP	MAX. 8 CHAR
SET_OWNER=NAME	&SOWNER	MAX. 8 CHAR

Dataset Rules (Filter) Control Statements (//DSNRULES DD *)

Following control statements can be utilized to perform the RACF dataset verification:

DDname	Verbs	Keywords	Comment	Default
//DSNRULES	*	N/A	Comment line	N/A
	+OPTIONS Note: only one statement allowed	SET_OWNER=	Assign new default owner if all rules fail. Variable name which can be used in the command members is: &SDOWNER	N/A
		SET_UACC=	Assign new UACC if all rules fail. Variable name which can be used in the command members is: &SDUACC	N/A
		SET_NOTIFY=	Assign new NOTIFY if all rules fail. Variable name which can be used in the command members is: &SDNOTIFY	N/A

		HLQ=TSO or USERID or OWNER	Verify that a user dataset profile has as owner the high level qualifier of the RACF profile (HQL = OWNER). Group dataset profiles will be ignored. For non-matching items, the relevant ALTDSD commands will be generated to change the owner to the HLQ. If the owner for a user dataset is 'SYS1', the verification will be skipped. The commands will be written to the Ddname //DSNC04OW, which must be of RECFM=FB, LRECL=80.	N/A
		UDSN or USERID_DATASET=NO or YES	Do not process dataset profiles where the high level qualifier is a user-ID. Record type 0200 will be checked = //IRRI0200 DD DSN=	YES
		GDSN or GROUPID_DATASET=NO or YES	Do not process dataset profiles where the high level qualifier is a group-ID. Record type 0100 will be checked = //IRRI0100 DD DSN=	YES
		CAT=YES or NO	Verify if for the RACF profile name datasets do exists on the system. If dataset names have been found the "T" column will be marked with a "+" (e.g. "+U" or "+G". The "T" column indicates if the HLQ is a group or user dataset.	NO
		USERID_UACC=NO or YES	If set to "NO", the UACC for all user dataset profiles will be ignored. UACC= checking is normally only required for group dataset profiles e.g. UACC=NONE.	YES
		GROUPID_UACC=NO or YES	If set to "NO", the UACC for all group dataset profiles will be ignored.	YES
		VERIFY=YER or NO	Independent of any dataset RULES defined: If the VERIFY option is set to 'YES', then in addition the OWNER, NOTIFY, ACCESS list(s) and the catalog (CAT=YES must be set too) will be checked. For dataset profiles, where the HLQ appears as the second qualifier again e.g. IBMUSER.IBMUSER.** a DELDSD command will be generated. Each failing entry will be reported on //DSNVERIF. Pre-defined ALTDSD and PE xxx DEL commands will be written to the file //DSNCLEAN. The pre-defined commands will be invoked from the PDS file //COMMANDS. All supplied (pre-defined) command members start with $04xxyzz and should not be altered.	NO

		Note: all generated RACF control statements must be reviewed prior executing them. This utility does not automatically update the RACF DB.		
	+DATASET_RULE or +DSNAME_RULE or +DSN_RULE or +DR Note: you can define as many rule statements as required. Make sure the region size is set to e.g. REGION=0M	NAME=	Specifies a rule name, which can be up to 32 characters. This rule name will appear on the generated listings as a reference. We recommend assigning for each rule a meaningful name.	N/A
		DATASET=	Generic profile checking: Specifies a RACF dataset to be verified. To check fixed names refer to FDATASET selection.	N/A
		FDATASET=	NON-Generic profile checking: Specifies a RACF dataset to be verified. The supplied profile name will be checked in its entire length of 44 bytes.	N/A
		OWNER=	Specifies a RACF Owner-ID to be verified.	N/A
		UACC=	Specifies universal access of this data set. Valid values are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER or blank.	N/A
		DATA=YES or NO	Specifies that installation data must be present.	N/A
		AUDIT_OKQUAL=	Specifies the successful access audit qualifier to be verified. This is set to blanks if AUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.	N/A
		AUDIT_FAQUAL=	Specifies the failing access audit qualifier to be verified. This is set to blanks if AUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.	N/A
		GAUDIT_OKQUAL=	Specifies the auditor-specified successful access audit qualifier to be verified. This is set to blanks if GAUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.	N/A
		GAUDIT_FAQUAL=	Specifies the auditor-specified failing access audit qualifier to be verified. This is set to blanks if GAUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.	N/A

		AUDIT_LEVEL=	Specifies the audit level to be verified. This indicates the level of resource-owner-specified auditing that is performed. Valid values are ALL, SUCCESS, FAIL, and NONE.	N/A
		GAUDIT_LEVEL=	Specifies the global audit level to be verified. This indicates the level of auditor-specified auditing that is performed. Valid values are ALL, SUCCESS, FAIL, and NONE.	N/A
		AUTHDATE=(yyyy-mm-dd,??) or AUTH_DATE=(yyyy-mm-dd,??)	AUTHDATE= allows to restrict a rule to a given date range. The compare will be done in the length of the supplied date e.g. AUTHDATE=(2000,GE) will only compare the first 4 digits. ??= EQ, GE, GT, LE or LT. AUTHDATE is the date when a profile was 'defined' to RACF.	N/A
		SET_OWNER=	Assign new dataset-owner if this rule fails. Variable name which can be used in the command members is: &SOWNER	N/A
		SET_UACC=	Assign new UACC if this rule fails. Variable name which can be used in the command members is: &SUACC	N/A
		SET_NOTIFY=	Assign new NOTIFY if this rule fails. Variable name which can be used in the command members is: &SNOTIFY	N/A
		SET_AUDIT_OKQUAL=	Assign new audit attributes if this rule fails. Variable name which can be used in the command members is: &SAUDIT_OKQUAL	N/A
		SET_AUDIT_FAQUAL=	Assign new audit if this rule fails. Variable name which can be used in the command members is: &SAUDIT_FAQUAL	N/A
		SET_GAUDIT_OKQUAL=	Assign new global audit if this rule fails. Variable name which can be used in the command members is: &SGAUDIT_OKQUAL	N/A
		SET_GAUDIT_FAQUAL=	Assign new global audit if this rule fails. Variable name which can be used in the command members is: &SGAUDIT_FAQUAL	N/A
		SET_AUDIT_LEVEL=	Assign new audit level if this rule fails. Variable name which can be used in the command members is: &SAUDIT_LEVEL	N/A

		SET_GAUDIT_LEVEL=	Assign new global audit level if this rule fails. Variable name which can be used in the command members is: &SGAUDIT_LEVEL	N/A
		COMMAND=	Invoke command member from //COMMANDS if a rule fails. Command members can be used to fix problems. Command members are only invoked if a rule fails.	N/A
	Note: • The key fields for rule checking support generic filtering. A key field can also contain the substitution character '?' e.g. DATASET=IBM?A*.** . • To check 'as is' on a complete profile name use the keyword FDATASET. • If all supplied rules fail, the program will create the necessary reports and RACF control cards to alter the profiles. • If CAT=YES is specified, care should be taken to review the reports where RACF profiles are listed indicating that there are no 'real' datasets present. IGGCSI000 from IBM does not always return all datasets (check for any open IBM APARS).			

Sample: Failing Dataset profiles

```
DEB$SW53-10 DATASETS WHICH FAILED RULES CHECKING        ALS(C) V3R4M1 12/14/05 11.48  RACF VERS 2608              PAGE:         1
                                                                                                                  DATE:2005-12-14
           JOBNAME :XRZP001C STEPNAME:RA2RULES PROCNAME:                                                          TIME:  11:48:34
DATASET NAME                           T AUTHDATE   O OWNER    U ASFASF W E INSTDATA                    RULE NAME(S)/COMMENT
---------------------------------------- - ---------- - -------- - ------ - - -------------------------- -------------------------

A.*                                     U 2003-06-27 U A        N F RN   N N                          'BAD OWNER AND OR  UACC'
A.**                                   +U 2003-06-27 U A        N F RN   N N                          'BAD OWNER AND OR  UACC'
ACFNCP.**                               G 2001-04-10 G ACFNCP   N F RN   N N ACF/SSP INSTALLATION      'BAD OWNER AND OR  UACC'
ADSM.*.**                               G 1997-06-10 G SYS1     R F RN   N N                          'BAD OWNER AND OR  UACC'
ANF.*.**                                G 1997-06-10 G SYS1     R F RN   N N                          'BAD OWNER AND OR  UACC'
```

Field names

Field name	Explanation	Comments
T	U = user dataset name G = group dataset name. A "+" in front indicates if any catalogued datasets exists for a given RACF profile name.	
U	UACC	Defines the universal access authority to be associated with the data sets. The universal access authorities are A=ALTER, C=CONTROL, R=READ, U=UPDATE, E=EXECUTE, and N=NONE.
O	Owner is a group- or user-Id. U = user; G = group	
ASF (first)	Audit attributes A = audit level S = success F= failures	The first character of the attribute will be shown as for the UACC.
ASF (second)	Global audit attributes A = audit level	The first character of the attribute will be shown as

	S = success F= failures	for the UACC.
W	Warning attribute	
E	Erase on scratch attribute	
Rule name	Specifies the rule name, which matched.	

Command generation

For each failing rule it is possible to generate any kind of commands. Below are the variable names listed which can be used in a command member (DDname //COMMANDS). Each time a rule fails and the keyword COMMAND=member_name has been specified, the member will be read from //COMMANDS PDS file and all variables replaced. The output will be written to //DSNC0400. This facility works similar to the ISPF FTINCL function, however it does not support e.g.)SEL,)IM logic.

Variable names filled in by the IRRI0400 record:

The following variables can be used to generate commands related to dataset profiles:

RACF IRRDBU00 NAME	RA/2 VARIABLE	FORMAT	SAMPLE DATA
NAME	&R40NAME		BBO.**
VOL	&R40VOL		
GENERIC	&R40GEND	Y OR N (?)	Y
CREATE_DATE	&R40AUTHD	YYYY-MM-DD	
OWNER_ID	&R40OWNER		
LASTREF_DATE	&R40LREF	YYYY-MM-DD	*
LASTCHG_DATE	&R40CREF	YYYY-MM-DD	*
ALTER_CNT	&R40ALTR		
CONTROL_CNT	&R40CNTL		
UPDATE_CNT	&R40UPDT		
READ_CNT	&R40READ		
UACC	&R40UACC		NONE
GRPDS	&R40FLAG1	Y OR N (?)	
AUDIT_LEVEL	&R40AUDIT		
GRP_ID	&R40GRPN		*
DS_TYPE	&R40DSTYP		
LEVEL	&R40DSLVL		
DEVICE_NAME	&R40DTYPX		
GAUDIT_LEVEL	&R40GAUD		*
INSTALL_DATA	&R40DATA		
AUDIT_OKQUAL	&R40AQS		*
AUDIT_FAQUAL	&R40AQF		*
GAUDIT_OKQUAL	&R40GQS		*
GAUDIT_FAQUAL	&R40GQF		*
WARNING	&R40WARN	Y OR N (?)	N
SECLEVEL	&R40SECL		*
NOTIFY_ID	&R40NOTIF		
RETENTION	&R40RETPD		
ERASE	&R40ERASE	Y OR N (?)	
SECLABEL	&R40SECLA		*

Variable names filled in by the failing rule:

OPTIONS KEYWORD	OPTIONS VARIABLE	FORMAT
SET_UACC=VALUE	&SDUACC	MAX. 8 CHAR
SET_OWNER=NAME	&SDOWNER	MAX. 8 CHAR
SET_NOTIFY=NAME	&SDNOTIFY	MAX. 8 CHAR

RULE KEYWORD	RULE VARIABLE	FORMAT
SET_UACC=VALUE	&SUACC	MAX. 8 CHAR
SET_OWNER=NAME	&SOWNER	MAX. 8 CHAR
SET_NOTIFY=NAME	&SNOTIFY	MAX. 8 CHAR

General Resource Rules (Filter) Control Statements (//RESRULES DD *)

Following control statements can be utilized to perform the RACF general resource verification:

DDname	Verbs	Keywords	Comment	Default
//RESRULES	*	N/A	Comment line	N/A
	+OPTIONS Note: only one statement allowed	SET_OWNER=	Assign new default owner if all rules fail. Variable name which can be used in the command members is: &SROWNER	N/A
		SET_UACC=	Assign new UACC if all rules fail. Variable name which can be used in the command members is: &SRUACC	N/A
		SET_NOTIFY=	Assign new NOTIFY if all rules fail. Variable name which can be used in the command members is: &SRNOTIFY	N/A
		Note: all generated RACF control statements must be reviewed prior executing them. This utility does not automatically update the RACF DB.		
	+RESNAME_RULE or +RESOURCE_RULE or +RES_RULE or +RR or Note: you can define as many rule statements as required. Make sure the region size is set to e.g. REGION=0M	NAME=	Specifies a rule name, which can be up to 32 characters. This rule name will appear on the generated listings as a reference. We recommend assigning for each rule a meaningful name.	N/A
		CLASS=	Specifies a RACF class to be verified.	N/A
		RESOURCE=	Generic profile checking: Specifies a RACF general resource to be verified. To check fixed names refer to FRESOURCE selection.	N/A
		FRESOURCE=	NON-Generic profile checking: Specifies a RACF general resource to be verified. The supplied profile name will be checked in its entire length of 246 bytes.	N/A
		OWNER=	Specifies a RACF Owner-ID to be verified.	N/A

		UACC=	Specifies universal access of this data set. Valid values are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER or blank.	N/A
		DATA=YES or NO	Specifies that installation data must be present.	N/A
		AUDIT_OKQUAL=	Specifies the successful access audit qualifier to be verified. This is set to blanks if AUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.	N/A
		AUDIT_FAQUAL=	Specifies the failing access audit qualifier to be verified. This is set to blanks if AUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.	N/A
		GAUDIT_OKQUAL=	Specifies the auditor-specified successful access audit qualifier to be verified. This is set to blanks if GAUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.	N/A
		GAUDIT_FAQUAL=	Specifies the auditor-specified failing access audit qualifier to be verified. This is set to blanks if GAUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.	N/A
		AUDIT_LEVEL=	Specifies the audit level to be verified. This indicates the level of resource-owner-specified auditing that is performed. Valid values are ALL, SUCCESS, FAIL, and NONE.	N/A
		GAUDIT_LEVEL=	Specifies the global audit level to be verified. This indicates the level of auditor-specified auditing that is performed. Valid values are ALL, SUCCESS, FAIL, and NONE.	N/A
		AUTHDATE=(yyyy-mm-dd,??) or AUTH_DATE=(yyyy-mm-dd,??)	AUTHDATE= allows to restrict a rule to a given date range. The compare will be done in the length of the supplied date e.g. AUTHDATE=(2000,GE) will only compare the first 4 digits. ??= EQ, GE, GT, LE or LT. AUTHDATE is the date when a profile was 'defined' to RACF.	N/A

		SET_OWNER=	Assign new dataset-owner if this rule fails. Variable name which can be used in the command members is: &SOWNER	N/A
		SET_UACC=	Assign new UACC if this rule fails. Variable name which can be used in the command members is: &SUACC	N/A
		SET_NOTIFY=	Assign new NOTIFY if this rule fails. Variable name which can be used in the command members is: &SNOTIFY	N/A
		SET_AUDIT_OKQUAL=	Assign new audit attributes if this rule fails. Variable name which can be used in the command members is: &SAUDIT_OKQUAL	N/A
		SET_AUDIT_FAQUAL=	Assign new audit if this rule fails. Variable name which can be used in the command members is: &SAUDIT_FAQUAL	N/A
		SET_GAUDIT_OKQUAL=	Assign new global audit if this rule fails. Variable name which can be used in the command members is: &SGAUDIT_OKQUAL	N/A
		SET_GAUDIT_FAQUAL=	Assign new global audit if this rule fails. Variable name which can be used in the command members is: &SGAUDIT_FAQUAL	N/A
		SET_AUDIT_LEVEL=	Assign new audit level if this rule fails. Variable name which can be used in the command members is: &SAUDIT_LEVEL	N/A
	Note: • The key fields for rule checking support generic filtering. A key field can also contain the substitution character '?' e.g. RESOURCE=IBM?A*.** . • To check 'as is' on a complete profile name use the keyword FRESOURCE. • If all supplied rules fail, the program will create the necessary reports and RACF control cards to alter the profiles.			

Sample: Failing general resources

```
DEB$SW54-10 RESOURCES WHICH FAILED RULES CHECKING       ALS(C) V3R4M1 12/13/05 21.50  RACF VERS 2608               PAGE:         1
                                                                                                                  DATE:2005-12-14
           JOBNAME :XRZP001C STEPNAME:RA2RULES PROCNAME:                                                          TIME:  11:48:34
CLASS    GENERAL RESOURCE NAME                     AUTHDATE   T OWNER    U ASFASF W INSTDATA             RULE NAME(S)/COMMENT
-------- ----------------------------------------- ---------- - -------- - ------ - -------------------- -------------------------

FACILITY RA2002.DEC$CG10                           2001-10-13 U XRZP001  N F RN   N                      'RA2002 FIXED RULE     '


DEB$SW54-10 RESOURCES WHICH FAILED RULES CHECKING       ALS(C) V3R4M1 12/13/05 21.50  RACF VERS 2608               PAGE:         2
                                                                                                                  DATE:2005-12-14
           JOBNAME :XRZP001C STEPNAME:RA2RULES PROCNAME:                                                          TIME:  11:48:34
CLASS    GENERAL RESOURCE NAME                     AUTHDATE   T OWNER    U ASFASF W INSTDATA             RULE NAME(S)/COMMENT
-------- ----------------------------------------- ---------- - -------- - ------ - -------------------- -------------------------


===> TOTAL NUMBER OF RESOURCES  READ   :         11.873


===> TOTAL NUMBER OF RULES      FAILED :             1


===> TOTAL NUMBER OF RULES      MATCHED:            48
```

Field names

Field	Explanation	Comments

name		
U	UACC	Defines the universal access authority to be associated with the datasets. The universal access authorities are A=ALTER, C=CONTROL, R=READ, U=UPDATE, E=EXECUTE, and N=NONE or NOTRUST (class=DIGICERT), T=TRUST.
O	Owner is a group- or user-Id. U = user; G = group	
ASF (first)	Audit attributes A = audit level S = success F= failures	The first character of the attribute will be shown as for the UACC.
ASF (second)	Global audit attributes A = audit level S = success F= failures	The first character of the attribute will be shown as for the UACC.
W	Warning attribute (Y or N)	
Rule name	Specifies the rule name, which matched.	

Command generation

For each failing rule it is possible to generate any kind of commands. Below are the variable names listed which can be used in a command member (DDname //COMMANDS). Each time a rule fails and the keyword COMMAND=member_name has been specified, the member will be read from //COMMANDS PDS file and all variables replaced. The output will be written to //RESC0500. This facility works similar to the ISPF FTINCL function, however it does not support e.g.)SEL,)IM logic.

Variable names filled in by the IRRI0500 record:

The following variables can be used to generate commands related to general resource profiles:

RACF IRRDBU00 NAME	RA/2 VARIABLE	FORMAT	SAMPLE DATA
NAME	&R50NAME		**
CLASS_NAME	&R50CLASS		
GENERIC	&R50GEND	Y OR N (?)	N
CLASS	&R50CDT		041
CREATE_DATE	&R50AUTHD	YYYY-MM-DD	
OWNER_ID	&R50OWNER		
LASTREF_DATE	&R50LREF	YYYY-MM-DD	2003-01-15
LASTCHG_DATE	&R50CREF	YYYY-MM-DD	2003-01-15
ALTER_CNT	&R50ALTR		00000
CONTROL_CNT	&R50CNTL		00000
UPDATE_CNT	&R50UPDT		00000
READ_CNT	&R50READ		00000
UACC	&R50UACC		READ
AUDIT_LEVEL	&R50AUDIT		
LEVEL	&R50DSLVL		
GAUDIT_LEVEL	&R50GAUD		NONE
INSTALL_DATA	&R50DATA		
AUDIT_OKQUAL	&R50AQS		
AUDIT_FAQUAL	&R50AQF		READ
GAUDIT_OKQUAL	&R50GQS		
GAUDIT_FAQUAL	&R50GQF		
WARNING	&R50WARN	Y OR N (?)	N
SINGLEDS	&R50RESFL	Y OR N (?)	
AUTO	&R50AUTO	Y OR N (?)	
TVTOC	&R50TVTOC	Y OR N (?)	
NOTIFY_ID	&R50NOTIF		
ACCESS_SUN	&R50WDSUN	Y OR N (?)	
ACCESS_MON	&R50WDMON	Y OR N (?)	
ACCESS_TUE	&R50WDTUE	Y OR N (?)	
ACCESS_WED	&R50WDWED	Y OR N (?)	
ACCESS_THU	&R50WDTHU	Y OR N (?)	
ACCESS_FRI	&R50WDFRI	Y OR N (?)	
ACCESS_SAT	&R50WDSAT	Y OR N (?)	
START_TIME	&R50TIMES	HH:MM:SS	
END_TIME	&R50TIMEE	HH:MM:SS	
ZONE_OFFSET	&R50ZONEO		
ZONE_DIRECT	&R50ZONED	Y OR N (?)	
SECLEVEL	&R50SECL		000
APPL_DATA	&R50APPL		
SECLABEL	&R50SECLA		000
STARTHH_TIME	&R50TIHHS	HH:MM:SS	
ENDHH_TIME	&R50TIHHE	HH:MM:SS	

Variable names filled in by the failing rule:

OPTIONS KEYWORD	OPTIONS VARIABLE	FORMAT
SET_UACC=VALUE	&SRUACC	MAX. 8 CHAR
SET_OWNER=NAME	&SROWNER	MAX. 8 CHAR
SET_NOTIFY=NAME	&SRNOTIFY	MAX. 8 CHAR

RULE KEYWORD	RULE VARIABLE	FORMAT
SET_UACC=VALUE	&SUACC	MAX. 8 CHAR
SET_OWNER=NAME	&SOWNER	MAX. 8 CHAR
SET_NOTIFY=NAME	&SNOTIFY	MAX. 8 CHAR

DEB$SWO1 - RACF SETROPTS VERIFICATION

Purpose:

- Verify the RACF SETROPTS settings. This feature allows an installation to detect any changes made to e.g. the classes, options. This program makes no modification to the RACF database. Make sure the latest IBM APARs for IRRSEQ00 from 28.2.2006 have been applied, otherwise this program will not work under RACF 7709 or higher.

JCL required to run DEB$SWO1

Run the following JCL (refer to the YOURE.RRE.SAMPLIB member DEB$SWO1) to create the verification reports:

```
//EXECSETR EXEC PGM=DEB$SWO1
//STEPLIB  DD   DISP=SHR,DSN=YOUR.YOURE.RRE.LINKLIB
//VERPRINT DD   SYSOUT=*
//SETROPTS DD   SYSOUT=*
//SETERROR DD   SYSOUT=*
//SETMATCH DD   SYSOUT=*
//VERINPUT DD   *
*-- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
*   VERIFY INSTALLATION STANDARDS
*-- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
+SETROPTS   CLASSACT=(,
```

DDnames:

- //VERPRINT lists the control cards (rules) to perform the verfication based on the defined field names. The field names utilized by this program are the same as documented by IBM under the callable function r_admin (setropts).
- //SETROPTS contains a standard SETROPTS LIST output.
- //SETERROR lists all the rules, which failed the verification process.
- //SETMATCH lists all the rules, which passed the verification process.

Note:

Each +SETROPTS statement is considered as one rule. You can specify as many rules as required. Only the specified verbs will be compared against the SETROPTS settings.

Verification Rules (Filter) Control Statements (//VERINPUT DD *)

Following control statements can be utilized to perform the RACF SETROPTS verification:

DDname	Verbs	Keywords	Comment	Default
//VERINPUT	*	N/A	Comment line	N/A
	+OPTIONS	HEADING=YES or NO	Print headings (title lines)	YES
	+SETROPTS			
		ADDCREAT=	YES or NO	N/A
		ADSP=	YES or NO	N/A
		APPLAUDT=	YES or NO	N/A
		AUDIT=	(classname, ...)	N/A
		CATDSNS	(YES,'value') or NO	N/A
		CLASSACT=	(classname, ...)	N/A

		CLASSTAT=	(classname, ...)	N/A
		CMDVIOL=	YES or NO	N/A
		COMPMODE=	YES or NO	N/A
		EGN=	YES or NO	N/A
		ERASE=	YES or NO	N/A
		ERASEALL=	YES or NO	N/A
		ERASESEC=	(YES,'value') or NO	N/A
		GENCMD=	(classname, ...)	N/A
		GENERIC=	(classname, ...)	N/A
		GENLIST=	(classname, ...)	N/A
		GENOWNER=	YES or NO	N/A
		GLOBAL=	(classname, ...)	N/A
		GRPLIST=	YES or NO	N/A
		HISTORY=	(YES,value) or NO	N/A
		INACTIVE=	(classname, ...)	N/A
		INITSTAT=	(classname, ...)	N/A
		INTERVAL=	(YES,value) or NO	N/A
		JESBATCH=	YES or NO	N/A
		JESEARLY=	YES or NO	N/A
		JESNJE=	(YES,'value') or NO	N/A
		JESUNDEF=	(YES,'value') or NO	N/A
		JESXBM=	YES or NO	N/A
		KERBLVL=	(YES,value) or NO	N/A
		LOGALWYS=	(classname, ...)	N/A
		LOGDEFLT=	(classname, ...)	N/A
		LOGFAIL=	(classname, ...)	N/A
		LOGNEVER=	(classname, ...)	N/A
		LOGSUCC=	(classname, ...)	N/A
		MINCHANG=	(YES,value) or NO	N/A
		MIXDCASE=	YES or NO	N/A
		MLACTIVE=	(YES,'value') or NO	N/A
		MLFS=	(YES,'value') or NO	N/A
		MLIPC=	(YES,'value') or NO	N/A
		MLNAMES=	YES or NO	N/A
		MLQUIET=	YES or NO	N/A
		MLS=	(YES,'value') or NO	N/A
		MLSTABLE=	YES or NO	N/A
		MODEL=	YES or NO	N/A
		MODGDG=	YES or NO	N/A
		MODGROUP=	YES or NO	N/A
		MODUSER=	YES or NO	N/A
		OPERAUDT=	YES or NO	N/A
		PREFIX=	(YES,'value') or NO	N/A
		PRIMLANG=	(YES,'value') or NO	N/A
		PROTALL=	(YES,'value') or NO	N/A
		RACLIST=	(classname, ...)	N/A
		REALDSN=	YES or NO	N/A
		RETPD=	(YES,'value') or NO	N/A
		REVOKE=	(YES,value) or NO	N/A

		RULE1=	(YES,'value') or NO	N/A
		RULE2=	(YES,'value') or NO	N/A
		RULE3=	(YES,'value') or NO	N/A
		RULE4=	(YES,'value') or NO	N/A
		RULE5=	(YES,'value') or NO	N/A
		RULE6=	(YES,'value') or NO	N/A
		RULE7=	(YES,'value') or NO	N/A
		RULE8=	(YES,'value') or NO	N/A
		RVARSTPW=	(YES,'value') or NO Note: the value must be defined as 7 characters e.g. (YES,'INSTLN ') until IBM fixes the problem and returns the correct length of this field.	N/A
		RVARSWPW =	(YES,'value') or NO Note: the value must be defined as 7 characters e.g. (YES,'INSTLN ') until IBM fixes the problem and returns the correct length of this field.	N/A
		SAUDIT=	YES or NO	N/A
		SECLABCT=	YES or NO	N/A
		SECLANG=	(YES,'value') or NO	N/A
		SESSINT=	(YES,'value') or NO	N/A
		SLABAUDT=	YES or NO	N/A
		SLBYSYS=	YES or NO	N/A
		SLEVAUDT=	(classname, ...)	N/A
		TAPEDSN=	YES or NO	N/A
		TERMINAL=	(YES,value) or NO	N/A
		WARNING=	(YES,value) or NO	N/A
		WHENPROG=	YES or NO	N/A

		NOTE: When specifying the 'Y' flag, the data supplied in the RULEn field consists of a length field and a character sequence, separated by a blank. The length field can be either a single numeric value, or two numeric values separated by a colon (:) to denote a minimum and maximum length. The character sequence conforms to the format of the output of the SETROPTS LIST command. It is a string of 1 to 8 characters, where each position of the string contains a character that indicates the valid characters that can occupy that position: A - Alphabetic ; C - Consonant ; c - Mixed consonant ; L - Alphanumeric ; m - Mixed numeric ; N - Numeric ; V - Vowel ; v - Mixed vowel ; W - Non-vowel ; * - Any character ; $ - National For example: RULE1 field is specified with field data of RULE1=(YES,'3:6 A*NV*A'). Field names which have not been verified will be listed as well in the output file //SETERROR. This has been implemented to make sure "ALL" existing field names obtained from RACF are examined.

Sample: control card (rules) input //VERINPUT

```
1VERPRINT-10 CONTROL STATEMENTS (VALIDATE SECURITY OPTIONS)        ALS(C) V3R4M1 02/28/06 04.08   RACF VER:7709      PAGE:         1
                                                                                                                     DATE:2006-02-28
            JOBNAME :XRZP001C STEPNAME:EXECSETR PROCNAME:                                                            TIME:  14:55:58

 CONTROL CARD(S) READ VIA //VERINPUT                                    ERROR MESSAGE
 ------------------------------------------------------------------------ ------------------------------------------------

 *-- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
 *   VERIFY INSTALLATION STANDARDS
 *-- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
 +SETROPTS   CLASSACT=(,
 DATASET,USER,GROUP,$$EQQ3,ACCTNUM,ACICSPCT,APPL,BCICSPCT,
 Etc. . . . ),
  CLASSTAT=,
  GENCMD=(,
 DATASET,ACCTNUM,ACICSPCT,AIMS,ALCSAUTH,APPCLU,
 APPCPORT,APPCSERV,APPCSI,APPCTP,APPL,CACHECLS,
 CBIND,CCICSCMD,CIMS,CONSOLE,CPSMOBJ,CPSMXMP, etc……
 ADDCREAT=YES,
  ADSP=NO,
  CATDSN=YES,
  COMPMODE=NO,
  EGN=YES,
  GENOWNER=YES,
  GRPLIST=YES,
  MLACTIVE=NO,
  MLQUIET=NO,
  MLS=NO,
  MLSTABLE=NO,
  MLNAMES=YES,
  SLBSYS=YES,
  MLIPC=(YES,INACTIVE),
  MLFS=(YES,INACTIVE),
  PREFIX=NO,
  PROTALL=(YES,WARNING),
  REALDSN=NO,
  RETPD=(YES,00000),
  RVARSWPW=(YES,'INSTLN '),
  RVARSTPW=(YES,'INSTLN '),
  SECLABCT=NO,
  SESSINT=(YES,00012),
  TAPEDSN=NO,
  WHENPROG=YES,
  MODGDG=NO,
  MODGROUP=NO,
  MODUSER=NO,
  MODEL=YES,
  ERASE=YES,
  ERASEALL=YES,
  ERASESEC=YES,
  PRIMLANG=(YES,ENU),
  SECLANG=(YES,ENU),
  JESBATCH=YES,
  JESEARLY=NO,
  JESXBM=YES,
  JESNJE=(YES,A???????),
  JESUNDEF=(YES,B+++++++)
```

Sample: failing rules //SETERROR

```
1SETERROR-10 DEFINED RULES WHICH DO NOT MATCH "SETROPTS" SETTINGS   ALS(C) V3R4M1 02/28/06 04.10   RACF VER:7709      PAGE:         1
                                                                                                                    DATE:2006-02-28
            JOBNAME :XRZP001C STEPNAME:EXECSETR PROCNAME:                                                           TIME:  14:55:58

 FIELD NAME REQUESTED  VALUE               SETROPTS   CURRENT VALUE(S)     COMMENT/ACTIONS
 ---------- ---------- -------------------- ---------- -------------------- --------------------------------

 GENCMD     VMNODE     * NOT FOUND
            VMPOSIX    * NOT FOUND

            XFACILIT   * NOT FOUND

 GENERIC    VMNODE     * NOT FOUND
            VMPOSIX    * NOT FOUND

            WRITER     * NOT FOUND
            XFACILIT   * NOT FOUND

 GLOBAL     NODES      * NOT FOUND
            SECLABEL   * NOT FOUND

            VXMBR      * NOT FOUND

 AUDIT      VMNODE     * NOT FOUND
            VMPOSIX    * NOT FOUND

            XFACILIT   * NOT FOUND

 LOGDEFLT   VMNODE     * NOT FOUND
            VMPOSIX    * NOT FOUND
            VMRDR      * NOT FOUND


 SESSINT    YES        00012               Y          00030               * ITEM(S) DID NOT MATCH
1SETERROR-10 DEFINED RULES WHICH DO NOT MATCH "SETROPTS" SETTINGS   ALS(C) V3R4M1 02/28/06 04.10   RACF VER:7709      PAGE:         2
                                                                                                                    DATE:2006-02-28
            JOBNAME :XRZP001C STEPNAME:EXECSETR PROCNAME:                                                           TIME:  14:55:58

 FIELD NAME REQUESTED  VALUE               SETROPTS   CURRENT VALUE(S)     COMMENT/ACTIONS
 ---------- ---------- -------------------- ---------- -------------------- --------------------------------

 JESNJE     YES        A???????            Y          ????????            * ITEM(S) DID NOT MATCH
 JESUNDEF   YES        B+++++++            Y          ++++++++            * ITEM(S) DID NOT MATCH
```

Sample: SETROPTS Standard list //SETROPTS

```
1SETROPTS-10 STANDARD "SETROPTS" SETTINGS                          ALS(C) V3R4M1 02/28/06 04.10   RACF VER:7709      PAGE:         1
                                                                                                                    DATE:2006-02-28
            JOBNAME :XRZP001C STEPNAME:EXECSETR PROCNAME:                                                           TIME:  14:55:58

 SETROPTS LIST
 ----------------------------------------------------------------------------------------------------------------------------------

 ATTRIBUTES = INITSTATS WHEN(PROGRAM -- ENHANCED WARNING) SAUDIT CMDVIOL OPERAUDIT
 STATISTICS = NONE
 AUDIT CLASSES = DATASET USER GROUP ACCTNUM ACICSPCT AIMS ALCSAUTH APPCLU
                 APPCPORT APPCSERV APPCSI APPCTP APPL BCICSPCT CACHECLS
                 CBIND CCICSCMD CDT CIMS CONSOLE CPSMOBJ CPSMXMP CSFKEYS
                 CSFSERV DASDVOL DBNFORM DCEUUIDS DCICSDCT DEVICES DIGTCERT
                 DIGTCRIT DIGTNMAP DIGTRING DIMS DIRACC DIRAUTH DIRECTRY
etc
```

Sample: matching rules //SETMATCH

```
1SETMATCH-10 RULES WHICH MATCH SETROPTS SETTINGS                  ALS(C) V3R4M1 02/28/06 04.10   RACF VER:7709      PAGE:         1
                                                                                                                      DATE:2006-02-28
            JOBNAME :XRZP001C STEPNAME:EXECSETR PROCNAME:                                                             TIME:  14:55:58

 FIELD NAME REQUESTED  VALUE               SETROPTS   CURRENT VALUE(S)     COMMENT/ACTIONS
 ---------- ---------- -------------------- ---------- -------------------- --------------------------------

 CLASSACT                                                                   * ALL ITEMS MATCHED
 RACLIST                                                                    * ALL ITEMS MATCHED
 TERMINAL   YES        READ                 Y          READ                 * ITEM MATCHED
 CMDVIOL    YES                             Y                               * ITEM MATCHED
 OPERAUDT   YES                             Y                               * ITEM MATCHED
 SAUDIT     YES                             Y                               * ITEM MATCHED
 APPLAUDT   NO                              N                               * ITEM MATCHED
 SLABAUDT   NO                              N                               * ITEM MATCHED
 KERBLVL    YES        001                  Y          001                  * ITEM MATCHED
 LOGALWYS                                                                   * ALL ITEMS MATCHED
 LOGNEVER                                                                   * ALL ITEMS MATCHED
 HISTORY    YES        012                  Y          012                  * ITEM MATCHED
 INTERVAL   YES        090                  Y          090                  * ITEM MATCHED
 WARNING    YES        005                  Y          005                  * ITEM MATCHED
 REVOKE     YES        006                  Y          006                  * ITEM MATCHED
 RULE1      YES        6:8 ALLLLLLL         Y          6:8 ALLLLLLL         * ITEM MATCHED
 RULE2      NO                              N                               * ITEM MATCHED
 RULE3      NO                              N                               * ITEM MATCHED
 RULE4      NO                              N                               * ITEM MATCHED
 RULE5      NO                              N                               * ITEM MATCHED
 RULE6      NO                              N                               * ITEM MATCHED
 RULE7      NO                              N                               * ITEM MATCHED
 RULE8      NO                              N                               * ITEM MATCHED
 ADDCREAT   YES                             Y                               * ITEM MATCHED
 ADSP       NO                              N                               * ITEM MATCHED
 COMPMODE   NO                              N                               * ITEM MATCHED
 EGN        YES                             Y                               * ITEM MATCHED
 GENOWNER   YES                             Y                               * ITEM MATCHED
 GRPLIST    YES                             Y                               * ITEM MATCHED
 MLACTIVE   NO                              N                               * ITEM MATCHED
 MLQUIET    NO                              N                               * ITEM MATCHED
 MLS        NO                              N                               * ITEM MATCHED
 MLSTABLE   NO                              N                               * ITEM MATCHED
 MLIPC      YES        INACTIVE             Y          INACTIVE             * ITEM MATCHED
 MLFS       YES        INACTIVE             Y          INACTIVE             * ITEM MATCHED
 PREFIX     NO                              N                               * ITEM MATCHED
 PROTALL    YES        WARNING              Y          WARNING              * ITEM MATCHED
 REALDSN    NO                              N                               * ITEM MATCHED
 RETPD      YES        00000                Y          00000                * ITEM MATCHED
 RVARSWPW   YES        INSTLN               Y          INSTLN               * ITEM MATCHED
 RVARSTPW   YES        INSTLN               Y          INSTLN               * ITEM MATCHED
 SECLABCT   NO                              N                               * ITEM MATCHED
 TAPEDSN    NO                              N                               * ITEM MATCHED
 WHENPROG   YES                             Y                               * ITEM MATCHED
 MODGDG     NO                              N                               * ITEM MATCHED
 MODGROUP   NO                              N                               * ITEM MATCHED
 MODUSER    NO                              N                               * ITEM MATCHED
 ERASEALL   YES                             Y                               * ITEM MATCHED
 PRIMLANG   YES        ENU                  Y          ENU                  * ITEM MATCHED
```