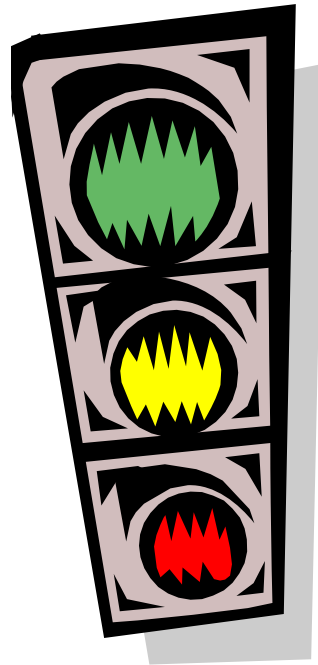


RACF AUTHORIZATION LOGIC

RACF Users Group of the Northeast (RUGONE) - April 2011



Robert S. Hansel

Lead RACF Specialist - RSH Consulting, Inc.

R.Hansel@rshconsulting.com - 617-969-9050 - www.rshconsulting.com

TOPICS

Step-by-Step review of RACF authorization logic

Does not cover Multi-Level Security (MLS), SECLABEL, or SECLEVEL processing steps

RACF and z/OS are Trademarks of the International Business Machines Corporation

RACF AUTHORIZATION FACTORS

RACROUTE REQUEST= AUTH | FASTAUTH | VERIFY(X)

RACHECK | FRACHECK | RACINIT

RESTRICTED

OPERATIONS

System-SPECIAL

RACLIST

Return Code (RC) = 0 | 4 | 8

RACF Callable Services

SAF

SAF - System Authorization Facility

Called by RACROUTE

Issues a SAF RC to accompany the RACF RC

RACHECK / FRACHECK - skip to Step 6

1. SAF EXITS

ICHRTX01 - Pre-MSI (Master Scheduler Initialization)

ICHRTX00 - Post-MSI (Master Scheduler Initialization)

Not invoked for UNIXPRIV class authorization checks which are made as part of RACF callable service checks

Can optionally set RC and bypass further checking

Can optionally modify the RACROUTE parameters before further checking is performed

2. RACF ROUTER TABLE

Controls the action taken by the RACF router module ICHFR00 when invoked by the RACROUTE macro

ICHFR01 module

- **Installation-defined router entries**
- **Entries made using ICHRFRTB macro**
- **Entries specify CLASS and optionally REQSTOR and SUBSYS**

SAF stops further processing and returns RC=4 if either:

- **Entry with matching CLASS, and if specified matching REQSTOR and SUBSYS, has parameter ACTION=NONE**
- **RACROUTE macro specifies operands DECOUPL=NO, REQSTOR=, and SUBSYS=, but does not provide values for these parameters**

3. - 4. - 5. RACF & CLASS ACTIVE

SAF sets RC=4 and stops further processing if ...

3. RACF is not active

4. For general resources, the class is not active

5. Class is defined as RACLIST required, but is not RACLISTed

- ICHERCDE macro - RACLREQ=YES
- CDT class profile - CDTINFO segment - RACLIST(REQUIRED)

APPCSERV	APPCTP	CRYPTOZ	CSFKEYS	CSFSERV	DEVICES
DIGTCIRT	DIGTNMAP	FIELD	IDIDMAP	NODES	OPERCMDS
PROPCNTL	PSFMPL	PTKTDATA	RACFHC	RACFVARS	RDATA LIB
SECLABEL	SERVAUTH	STARTED	SYSMVIEW	UNIXPRIV	VTAMAPPL

SAF processing effectively ends - checking passes to RACF

6. PRIVILEGED OR TRUSTED

Applies to Started Tasks

Grants unrestricted access to all resources

If either is true, set RC=0 and bypass all further checking

TRUSTED can be logged (UAUDIT or LOGOPTIONS)

As of z/OS 1.11, also checked in FASTAUTH

Does not apply if CSA or PRIVATE is specified in the RACROUTE ENTITY= or ENTITYX= parameter

7. NAMING CONVENTIONS TABLE

Only applies to DATASET class

Module ICHNCV00 - macro ICHNCONV

Can deny access - set RC=8

[*label*] ICHNCONV DEFINE,NAME=*convention name*

[*label*] ICHNCONV SELECT,COND=(*condition/compound condition*)

[*label*] ICHNCONV END,NEXT=**'ERROR'**

If exit ICHRCX01 exists, continue processing, else skip to Step 24

8. PRE-PROCESSING EXITS

REQUEST=AUTH | RACHECK

- **ICHRCX01**

REQUEST=FASTAUTH | FRACHECK

- **ICHRFX01 - non-cross-memory calls**
- **ICHRFX03 - cross-memory calls and UNIXPRIV checks**
- **Do not get invoked for PROGRAM authorization checks**

Can optionally set RC and ...

- **For AUTH / RACHECK, skip to Step 24**
- **For FASTAUTH / FRACHECK, end further processing**

Can optionally modify the RACROUTE parameters

9. DEFAULT USER TOKEN

If requesting user has a default user token, set RC=8 and skip to step 24

Default user token created by SAF in response to a RACROUTE REQUEST=VERIFYX when RACF is not yet available

10. UTOKEN MATCHES RTOKEN

Security Tokens are created by SAF at the request of JES

UTOKEN - User Token

- **Assigned to a job or session upon entry to the system**
- **Contains Execution USERID, Group, Session-type (e.g., batch), Port-of-Entry (POE), STOKEN (Submitter Token)**

RTOKEN - Resource Token

- **Assigned to job resources - SYSIN, SYSOUT**
- **Contains information similar to UTOKEN**

Step performed when Resource Manager specifies UTOKEN and RTOKEN in REQUEST=AUTH

If USERIDs in Tokens match, set RC=0 and skip to Step 23

- **TSO CANCEL for own job**
- **JESSPOOL resources for own job depending on resource manager**

11. GLOBAL ACCESS TABLE

RACF checks the table if the class is active for global checking

- SETROPTS GLOBAL(*class-name*)

If a matching entry for the resource exists with sufficient access, set RC=0 and skip to Step 23

DATASET	&RACUID.**	ALTER
DATASET	CATALOG.MASTER	READ
DATASET	CATALOG.USER	UPDATE
DATASET	ISPF.LIBRARY	READ
FACILITY	STGADMIN.ARC.ENDUSER.**	READ
JESSPOOL	*.&RACUID.**	ALTER

Global Access Table is not checked for ...

- RESTRICTED users
- FASTAUTH / FRACHECK processing
- VERIFY / RACINIT processing for APPL, TERMINAL, JESINPUT, CONSOLE, APPCPORT, or SERVAUTH class resources
- RACROUTE requests where CSA or PRIVATE is specified in the ENTITY= or ENTITYX= parameter

12. PROFILE NOT FOUND

If a profile cannot be found in storage or in the database, set default RC and skip to Step 23

RACF does not search the database if profiles for the class are in a dataspace or in the user's address space

Profiles in Grouping classes are ignored if the class is not RACLISTed (e.g., GDASDVOL, GTERMINL)

For TERMINAL, skip to Step 17

12. PROFILE NOT FOUND - DEFAULT RC

For DATASET, default RC is 4

For General Resources, default RC is specified for the class

- ICHERCDE macro - DFTRETC= 0 | 4 | 8
- CDT class profile - CDTINFO segment - DEFAULTRC(0 | 4 | 8)

DFTRETC=8 Classes

(* - includes grouping class)

APPCSERV	APPCTP	CBIND	CONSOLE	DCEUUIDS
DIRACC	DIRAUTH	DIRECTRY	DIRSRCH	FILE
FSOBJ	FSSEC	IPCOBJ	JESINPUT	JESJOBS
JESSPOOL	KEYSMSTR	MQADMIN*	MQCHAN*	MQCMDS
MQCONN	MQNLIST*	MQPROC*	MQQUEUE*	MXADMN*
MXNLIST*	MXPROC	MXQUEUE*	MXTOPIC*	PROCACT
PROCESS	PSFMPL	RACFHC	ROLE	SECLABEL
SFSCMD	SERVER	SOMDOBJ*	TEMPDSN	TMEADMIN
WRITER	XCSFKEY	XFACILITY*		

13. USER OWNS RESOURCE

If the user owns the resource, set RC=0 and skip to Step 23

- **Dataset HLQ matches the USERID**
- **USERID and Node of creator (UTOKEN) matches USERID and Node of JESSPOOL resource (RTOKEN)**

Does not apply when JESSPOOL resources are accessed via FTP with option JESINTERFACELEVEL=2

PROGRESS SUMMARY

SAF exit did not halt processing

RACF is active

Class is active

Class is RACLISTed if required

User is not PRIVILEGED or TRUSTED

Naming Convention Table did not halt processing

Pre-Processing Exits did not halt processing

User did not have default token

User UTOKEN did not match resource RTOKEN

Global Access Table did not grant access

RACF found a profile

User was not the owner of the resource

14. USERID IN ACCESS LIST

RACF looks for the USERID in the access list

If found ...

- **With sufficient permission, set RC=0 and skip to Step 23**
- **With insufficient permission, skip to Step 19**

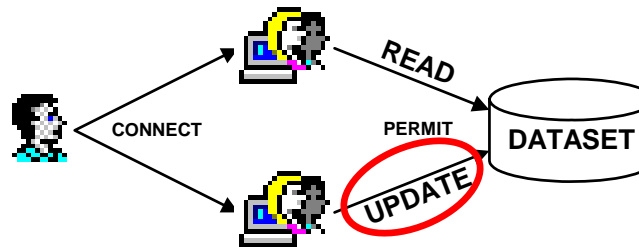
15. GROUP IN ACCESS LIST

RACF looks for the user's group(s) in the access list

- If List-of-Groups not active (SETROPTS NOGRPLIST), only looks for user's current connect group
- If List-of-Groups active (SETROPTS GRPLIST), looks for all of user's connect groups (ignores those with CONNECT attribute of REVOKE)

If found ...

- With List-of-Groups, uses the highest access permitted of all the user's groups



- With sufficient permission, set RC=0 and skip to Step 23
- With insufficient permission, skip to Step 19

16. ID * IN ACCESS LIST

If the user has logged on with a RACF-authenticated USERID, RACF looks for * in the access list

If found ...

- **With sufficient permission, set RC=0 and skip to Step 23**
- **With insufficient permission, skip to Step 18**

Bypassed for RESTRICTED users

17. UNIVERSAL ACCESS (UACC)

If the UACC provides sufficient permission, set RC=0 and skip to Step 23

Bypassed for RESTRICTED users

For TERMINAL authorization ...

- **The UACC for undefined terminals is determined by SETROPTS option `TERMINAL(READ | NONE)`**
- **The UACC is ignored if the user's current connect group has `NOTERMUACC` - treated as if `UACC(NONE)`**

PROGRESS SUMMARY

User's USERID was not in the standard access list

User's Groups were not in the standard access list

ID(*) did not grant access

UACC did not grant access

18. OPERATIONS ATTRIBUTE

Set RC=0 and skip to Step 23 if ...

- The resource class honors OPERATIONS authority, and
- The user has either ...
 - System-OPERATIONS, or
 - Group-OPERATIONS and the resource is within the scope-of-groups

Class attribute determines if OPERATIONS is honored

- ICHERCDE macro - OPER=YES | NO
- CDT class profile - CDTINFO segment - OPERATIONS(YES | NO)

IBM default classes that honor OPERATIONS

DATASET	DASDVOL/GDASDVOL	PSFMPL
TAPEVOL	VM Resources	RODMMGR
NETCMDS	NETSPAN	

CONDITIONAL ACCESS

REQUEST=AUTH

- WHEN(JESINPUT(*device*))
- WHEN(TERMINAL(*terminal-id*))
- WHEN(SYSID(*smf-id*)) - for PROGRAM class resources only
- WHEN(APPCPORT(*partner-lu-name*))
- WHEN(SERVAUTH(*servauth-profile*))
- WHEN(SQLROLE(*db2-role-name*))
- WHEN(CONSOLE(*console-id*))
- WHEN(PROGRAM(*program*)) - checked after other conditional checks

REQUEST=FASTAUTH - additional checks

- WHEN(CRITERIA(*criteria-value*))
- WHEN(PROGRAM(*program*)) for SERVAUTH class resources

Resource named in WHEN permission must be defined to RACF in its associated class (except for SYSID)

19. - 20. - 21. CONDITIONAL ACCESS

19. USERID + Condition in the access list

20. Group(s) + Condition in the access list

21. ID(*) + Condition in the access list ... if ...

- **User logged on with RACF-authenticated USERID**
- **USERID not RESTRICTED**

If USERID or Group found ...

- **With sufficient permission, set RC=0 and skip to Step 23**
- **With insufficient permission, skip to Step 22**

22. WARNING

If the profile WARNING flag is ...

- **ON, set RC=0**
- **OFF, set RC=8 and skip to Step 24**

WARNING does not apply to profiles in classes ...

- **NODES**
- **PROGRAM**
... treated as if flag set to OFF

23. CATDSNS(FAILURES)

Only applies to DATASET class

Required datasets to be cataloged

If SETROPTS CATDSNS(FAILURES) is in effect, set RC=8 unless one of the following is true:

- The dataset is newly created in this job or is a system temporary dataset
- The dataset is on tape, and the request is for UPDATE access
- The dataset is protected by a discrete profile
- The dataset is cataloged in the master catalog
- The user has READ access to FACILITY class resource ICHUNCAT.*dsname* (truncated to 39 characters, if necessary)
- The user has System-SPECIAL

24. POST-PROCESSING EXITS

REQUEST=AUTH | RACHECK

- **ICHRCX02**

REQUEST=FASTAUTH | FRACHECK

- **ICHRFX02 - non-cross-memory calls**
 - **If the class is RACLISTed or defined in the CDT class, call ICHRFX04 and then ICHRFX02**
- **ICHRFX04 - cross-memory calls and UNIXPRIV checks**
- **Do not get invoked for PROGRAM authorization checks**

Can optionally set the RC to another value

Post-processing exits execute before logging and can change logging specifications

25. PROTECTALL(FAILURES)

Only applies to DATASET class where ...

- **No profile was found, and**
- **Exits have not set the RC to 0 or 8**

If SETROPTS PROTECTALL(FAILURES) is in effect ...

- **If user has System-SPECIAL, set RC=4**
- **Otherwise, set RC=8**

If FAILURES not in effect, set RC=4

RC SENT BACK TO CALLER

0



4

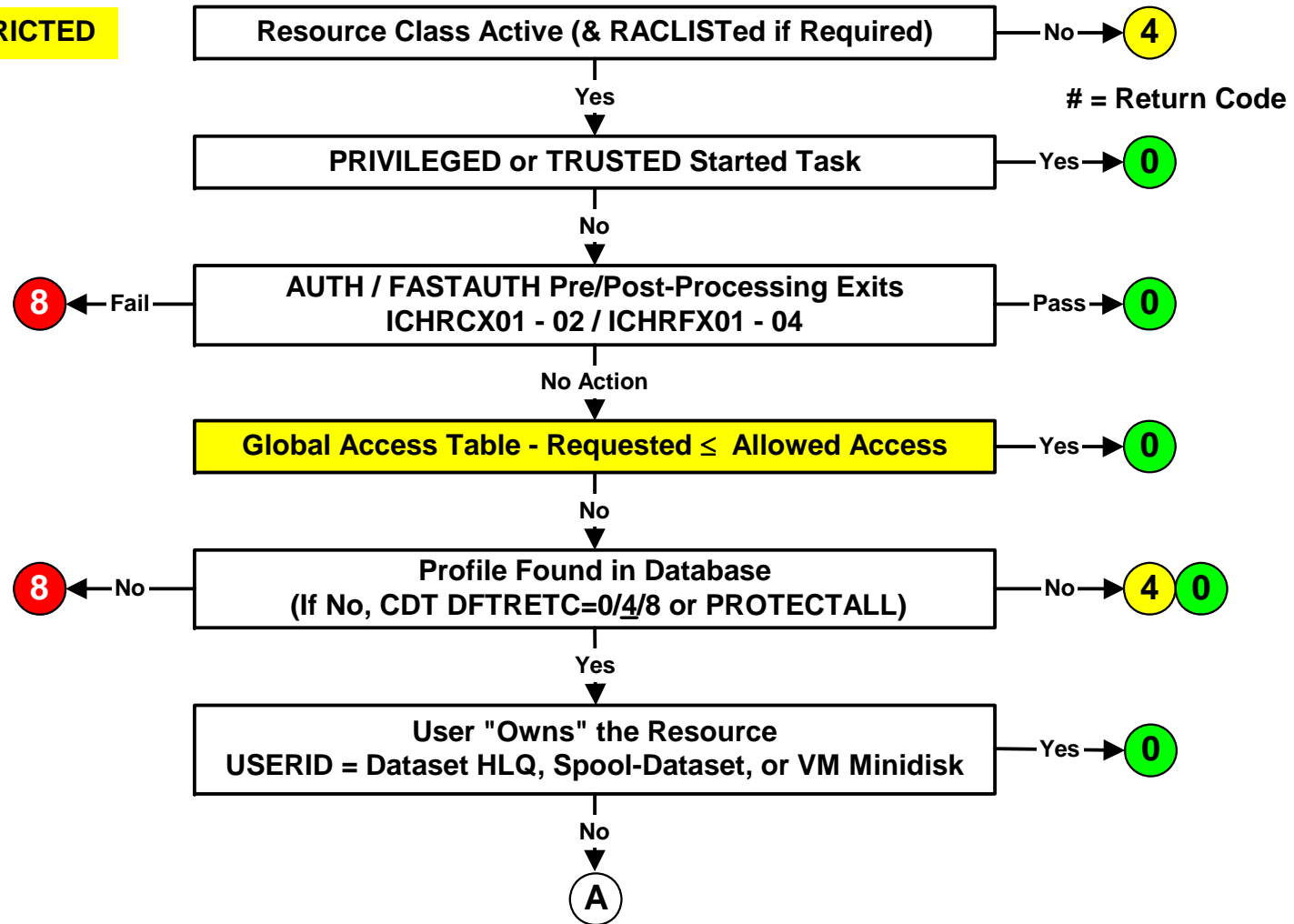


8



ACCESS AUTHORIZATION FLOWCHART

Not RESTRICTED



ACCESS AUTHORIZATION FLOWCHART

