SHARE in Orlando 2015

Solving IMS Security "Gotchas"

Session 17761

Maida Snapper, IBM

maidalee@us.ibm.com

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence**.

Disclaimer

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS AND/OR SOFTWARE.

Areas We Will Explore

- Security Activation
- RACF resource class and profile
- User ID
- Exits
- Dependent region security (RAS)
- References

Areas We Will Explore

- **Security Activation:** Are the windows locked?
  - RACF resource class and profile
  - User ID
  - Exits
  - Dependent region security (RAS)
  - References

The IMS House with all its doors and windows.

Think of each window as a way of accessing IMS: SNA, OTMA, APPC, MSC, etc.

Security Activation Concepts (cont)

How is the message trying to get in?

There's a lock for that.

Each window has its own lock and key.

The “windows”	The “locks”	Where to find the “locks”
3270 terminal	RCF	DFSPB
TCO script	RCF and TCORACF	DFSPB
OTMA	OTMASE	DFSPB
ODBA	ODBASE or ISIS	DFSPB
APPC / LU 6.2	APPCSE	DFSPB
MSC	MSCSEC	DFSDC
Operations Manager (OM)	CMDSEC	CSLOI DFSCG (or DFSDF)
MCS or E-MCS	CMDMCS	DFSPB
DBRC	CMDAUTH	RECON
AOI type 1	AOI1	DFSPB
AOI type 2	AOIS	DFSPB
Dependent region	ISIS	DFSPB

8

Reference chart of “windows”, locks/keys and where you specify the lock/key value.

Security Activation Concepts (cont)

CMDSEC in CSLOIxxx for Operations Manager

- Tells OM what security to perform for **all** commands (type 1 and type 2)
- OM only uses the OPERCMDS class
  - Define type 1 commands using OPERCMDS profile format
    - Example to protect /DIS DB command RDEF OPERCMDS IMS.*plxname*.DIS.DB UACC(NONE)
  - OM does not use CIMS class

CMDSEC in DFSCGxxx or DFSDFxxx for IMS

- Tells IMS what security to perform for type 1 commands passed to IMS from OM
  - IMS does not perform security for type 2 commands
- IMS only uses the CIMS class
  - Define type 1 commands using CIMS profile format
    - Example to protect /DIS command RDEF CIMS DIS UACC(NONE)
  - IMS does not use OPERCMDS class

If you don't define a type 1 command in the OPERCMDS class, then RACF returns a 4 (undefined) and Operations Manager passes the command to IMS.

By defining type 1 commands in the OPERCMDS class you can let Operations Manager do all the security checking and IMS won't have to make RACF calls for type 1 commands that come from OM. In that case do not specify CMDSEC in DFSCGxxx. If you do not define type 1 commands in the OPERCMDS class format, then you should also specify CMDSEC in DFSCGxxx so that IMS can authorize type 1 commands in the CIMS class.

Solving Security Activation Problems

Now let's solve some problems.

Real problems reported by

real people.

Solving Security Activation Problems (cont)

I set RCF=Y but some things are not being protected.

- Because RCF=Y only locks the ETO terminal "window"

OK, I changed RCF from Y to A but that didn't make any difference.

- Because you have to cold start for RCF changes to take effect

RCF= N do not call RACF

Y call RACF to authorize transactions and commands from ETO terminals

C call RACF to authorize commands from ETO terminals

S call RACF to authorize commands from both static and ETO terminals

T call RACF to authorize transactions from both static and ETO terminals

A call RACF to authorize transactions and commands from both static and ETO terminals

Solving Security Activation Problems (cont)

I turned off all security in my test system but I'm still getting security violations when I do some IMS commands.

DFS3662W 17:20:17 COMMAND REJECTED BY DEFAULT COMMAND SECURITY

- Because turning off all security gives you default security which protects some type 1 commands.

The default subset of commands allowed for each source is documented in IMS Command Reference

Commands allowed by default for

LU6.2: /BROADCAST,/LOCK,/LOG,/RDISPLAY,/RMLIST

OTMA: /LOCK, /LOG, /RDISPLAY

ETO: /BROADCAST /CANCEL /DIAGNOSE /END /EXCLUSIVE /EXIT /FORMAT /HOLD /IAM /LOCK /LOG /LOOPTEST

/RCLDST /RCOMPT /RDISPLAY /RELEASE /RESET /RMLIST /SET /SIGN /TEST /UNLOCK

Solving Security Activation Problems (cont)

I gave DIS a UACC(READ) so everyone would be authorized but some people can't do /DIS

DFS3662W 17:20:17 COMMAND REJECTED BY DEFAULT COMMAND SECURITY

- Because if you didn't lock one of the windows, commands entered through that window get default security.
- Default security for that window might not allow /DIS

The default subset of commands allowed for each source is documented in IMS Command Reference. The commands allowed by default are different for each "window".

Solving Security Activation Problems (cont)

I turned off AOI security but programs are still getting CD status codes.

- Because even if you aren't using AOI security, you still need to code a value for AOI on the TRANSACT macro in order to allow the transaction to issue DLI CMD calls.

AOI=YES/TRAN/CMD specifies what user ID to authorize against if you do activate security using the AOI1 parameter. You don't have to activate any security but you do have to specify a value for AOI.

Solving Security Activation Problems (cont)

I set RACF=Y in IMS Connect but unauthorized users are able to do transactions.

- Because IMS Connect can verify a user ID but does not do transaction authorization.
- IMS OTMA does transaction authorization
  - You need to set OTMASE to get transaction authorization for transactions from IMS Connect

The RACF calls made by the IMS Connect region are not related to the OTMA security level (OTMASE). IMS Connect does not call RACF to authorize access to the transaction code. IMS Connect just does authentication of the user itself. Whether or not IMS Connect calls RACF to authenticate the user in each transaction message is controlled by the RACF keyword in the HWS statement within the IMS Connect configuration member. IMS Connect will call RACF to authenticate the user ID and password in each transaction message only if RACF=Y is specified.

Whether or not you want IMS Connect to authenticate users will depend on the kind of TCP/IP clients which are able to open sockets with it. If all the clients opening sockets with IMS Connect are trusted servers which have already authenticated the users, then there is no need for IMS Connect to do the authentication. If it is possible for non-trusted clients to open sockets with IMS Connect then it needs to authenticate the user of all incoming messages. If you do need to do authentication in IMS Connect then one thing that can save on the overhead of calls to the RACF database is the IMS Connect Extensions for z/OS. This program product is an extension to IMS Connect, and one of its features saves the ACEE control blocks in a cache for use in authenticating subsequent transactions issued by the same user.

.

Solving Security Activation Problems (cont)

Why isn't Operations Manager calling RACF for type 1 commands?

- OM ***is*** calling RACF for type 1 commands. You did not define type 1 commands in the OPERCMDS class. RACF did not find profiles and gave OM return code 04 ("unprotected"). OM passed the commands to IMS.
- When IMS got the commands from OM, IMS did not call RACF because CMDSEC was not specified in DFSCGxxx or DFSDFxxx.

Solving Security Activation Problems (cont)

Remember:

- Each “window” is locked independently of the rest
- If a “window” is not locked
  - Default security is in effect for type 1 commands entered through that “window”
  - The commands allowed by default are different depending on the “window”
  - If the Command Authorization Exit (DFSCCMD0) is in RESLIB, default security is deactivated
- Locks can be changed with a warm start
  - Exception: RCF requires a cold start to change

If you don’t implement IMS command security, IMS automatically provides a type of command security commonly referred to as 'default' security to limit the commands users may enter.

Default security applies to type 1 IMS commands. Default security does not affect other IMS resources such as transactions, databases, terminals, programs, etc.

Default security allows only a subset of the IMS commands to be entered. The subset of commands allowed when default security is active depends on where the command is entered (the “window”). For example, the subset of IMS commands that may be entered from an ETO terminal is different than the subset of IMS commands that may be entered from OTMA.

Default security for a given source is deactivated by specifying another form of command security for that source. Default security is deactivated if you have the DFSCCMD0 exit in RESLIB.

The default subset of commands allowed for each source is documented in IMS Command Reference.

Areas We Will Explore

- Security Activation
- **RACF resource class and profile:** **How does IMS talk to RACF?**
- User ID
- Exits
- Dependent region security (RAS)
- References

Class and Profile Concepts (cont)

If you ask for RACF security, then at IMS initialization
IMS calls RACF to load resource profiles into RACF dataspace
RACROUTE REQUEST=LIST,GLOBAL=YES

If this fails:

U0166

19

When an application like IMS RACLISTs a class using RACROUTE REQUEST=LIST,GLOBAL=YES, the RACLISTed profiles are stored in a data space. The data space can be shared by many applications. Applications that issue a subsequent RACROUTE REQUEST=LIST,GLOBAL=YES for the same class simply access the data space built by the first application. When all applications have relinquished their access to the data space by issuing a RACROUTE REQUEST=LIST,ENVIR=DELETE request, the data space can be deleted by issuing a SETROPTS NORACLIST(classname) command. The SETROPTS NORACLIST command processes not only the class specified by classname, but also all valid classes that share the same POSIT value as classname. If you issue a SETROPTS RACLIST for that class, RACF rebuilds the data space from the RACF database profiles and replaces the existing data space.

Class and Profile Concepts (cont)

Some of the default resource classes that come with RACF:

TIMS

CIMS

IIMS

LIMS

These are some of the default IMS classes that come already defined from IBM.

Class and Profile Concepts (cont)

Default IMS resource classes

- These resource classes may be required for IMS to come up
  - Depends on your security parameters

CIMS | DIMS	Commands (first 3 characters of command)
TIMS | GIMS	Transactions (trancode)
IIMS | JIMS	Program Specification Blocks (PSBs)
LIMS | MIMS	Logical terminals (LTERM)
AIMS	APSB (Allocate PSB) for CPIC-PSB and ODBA

The RACF default IMS resource classes on this slide are used exclusively by IMS. The default classes are defined and provided by IBM but have to be activated when you are ready to use them. Note that the AIMS and RIMS classes do not have a grouping class associated with them.

Prior to IMS10, the AIMS class was used for "AGN" security. AGN security was replaced by RAS in IMS10. Now the AIMS class is used to authorize "allocate PSB" calls. Programs that make these calls are APPC programs using CPIC and, optionally, programs that access IMS through ODBA. The resources in the AIMS class are PSBs.

Class and Profile Concepts (cont)

Default IMS resource classes

- These resource classes are not required for IMS to come up
  - Certain function will not be available

RIMS	Asynchronoushold queues for RESUME TPIPE call
FIMS | HIMS	Database fields (for AUTH calls)
SIMS | UIMS	Database segments (for AUTH calls)
OIMS | WIMS	Other (information in RACF for AUTH calls)
PIMS | QIMS	Databases (for AUTH call)

22

The PIMS, SIMS, FIMS and OIMS resource classes are only used by IMS in response to an application program issuing an AUTH call.

They allow applications to use RACF to control access to the application data at a finer level of granularity. IMS passes the RACF return code back

to the application and the application must decide what to do. The application should remember to code for a possible A4 status code if the class was not activated.

Class and Profile Concepts(cont)

IMS also shares some resource classes with other products

TERMINAL | GTERMINL

APPL

VTAMAPPL

APPCPORT

APPCLU

APPCTP

DATASET

FACILITY

OPERCMDS

STARTED

In addition to the RACF classes used exclusively for IMS resource security definitions, a number of other RACF classes are also used to secure access to IMS resources. The other classes may be used by other subsystems, such as CICS, TSO, and other MVS subsystems.

Class and Profile Concepts (cont)

In a single, shared RACF database you can have different security rules for the same resource

- RACF resource is defined by Class + Name
  - Example: TIMS + ADDINV
- You can define a new class
  - Example: TIMSTEST + ADDINV
- You can point IMS to its own set of RACF rules using RCLASS
  - Example: RCLASS=IMSTEST

You may want to give a user different authorization to the same resource name (an IMS command, for example).

You may want to allow access in a test IMS but deny access in a production IMS.

If test and production share the same RACF database you need to find a way to differentiate the resource

when it is accessed in test versus production.

If the resource cannot be differentiated by its name (an IMS command, for example),

then you can differentiate it by its class. You can create installation-defined classes.

IMS points to its own set of RACF rules using the RCLASS parameter defined in PROCLIB.

RCLASS=position 2-8 of the RACF class name.

IMS General Resource Profiles

IMS resource	Resource class singular/grouping	Resource name
Transaction	T*IMS* / G*IMS*	transaction code
Command (type 1)	C*IMS* / D*IMS*	first 3 characters of command
DBRC command	FACILITY	*safhlq*.command_verb.qualifier.modifier
Command (type 2)	OPERCMDS	IMS.*plxname*.command_verb.command_keyword
Program (PSB)	I*IMS* / J*IMS*	program name
Logical terminal	L*IMS* / M*IMS*	logical terminal name (lterm)
CF structure	FACILITY	CQSSTR.*structure_name* or IXLSTR.*structure_name*
IMS Control Region	APPL	*Imsid and sapplid*
IMSPlex (CSL)	FACILITY	CSL.*imsplexname*
XCF group (Client bid)	FACILITY	IMSXCF.groupname.*membername*
Dataset	DATASET	*dataset name*

The portion of a resource class or name that is shown in blue italics on this chart is the part you can change to make a resource unique.

Member class profile names must conform to the rules shown in this chart.

Grouping class profile names can be any 1-8 alphanumeric characters you choose.

Notice that there are 2 kinds of IMS commands: type 1 and type 2. Type 2 commands are newer and can only be entered through the Operations Manager address space.

They are sometimes called plex commands.

Class and Profile Concepts (cont)

Example of some installation-defined resource classes when RCLASS=IMSTEST

T*IMSTEST*

C*IMSTEST*

I*IMSTEST*

L*IMSTEST*

There are two ways to define new resource classes: static or dynamic.

Define them in the dynamic class descriptor table (CDT), using RDEFINE and RALTER commands.

For information on how to do this, see z/OS Security Server RACF Security Administrator's Guide.

You can also define them in the static class descriptor table, using the ICHERCDE macro where each installation-defined class entry becomes a CSECT in load module ICHRRCDE.

Recommendation: Define your classes in the dynamic class descriptor table, to avoid the need to IPL.

Sample IMS Resource Class Description for Transactions

TIMS

POSIT=4
OTHER=ALPHANUM
MAXLNTH=8
DFTRETC=4
DFTUACC=NONE
GROUP=GIMS
OPER=NO
ID=9
FIRST=ALPHANUM

GIMS

POSIT=4
OTHER=ALPHANUM
MAXLNTH=8
DFTRETC=4
DFTUACC=NONE
MEMBER=TIMS
OPER=NO
ID=10
FIRST=ALPHA

The TIMS and GIMS definitions on this chart were copied from z/OS Security Server RACF Macros and Interfaces Appendix C

IMS resource classes have a default return code of 4.

Class and Profile Concepts (cont)

To have different security rules for different IMS systems you can define your own classes

- Class name 1-8 alphanumerics
  - First character must match corresponding default class
    - C, D, T, G, I, J, L, M, A, R, etc
  - Model new classes on the corresponding default class
    - Length must be the same as default class (8)
    - Optionally change the POSIT value
  - Activate the new classes
    - SETR CLASSACT(*classname)*
  - Point IMS to the new classes
    - Specify RCLASS in DFSPBxxx (default is IMS)
    - RCLASS= position 2-8 of class name

28

You can define your own IMS resource classes so that different IMS systems can have their own RACF rules.

Things to know:

1) New classes can be defined statically with an IPL or dynamically (no IPL required). It is recommended to define new classes dynamically.

2) The singular and grouping class are a pair and both must exist. If you are adding a new installation-defined class, be sure you also add its grouping class.

3) There is a maximum of 1024 classes. IBM provides 256 classes, you can define 768 new ones.

4) Classes are loaded at IPL by merging static, then dynamic class descriptors. A dynamic entry will replace static of the same name. If the merge reaches 1024, RACF warns entries are being ignored

5) Updating the RACF Router Table for new resource classes is not required because ACTION=RACF is the default.

6) Supplied CDT entries are documented in the z/OS Security Server RACF Macros and Interfaces

Class and Profile Concepts (cont)

- POSIT value
  - an arbitrary number that ties classes together for operations like activate/deactivate/refresh
  - You can specify POSIT values 19–56 and 128–527.
    - POSIT 0–18, 57–127, and 528–1023 are reserved for IBM

29

An important attribute of every class is its POSIT value. There are 1024 possible numeric POSIT values. You can specify POSIT values 19–56 and 128–527. POSIT values 0–18, 57–127, and 528–1023 are reserved for IBM use and should not be used for your dynamic class entries **unless you intend to share SETROPTS options with an IBM supplied class.** If you use a reserved POSIT number that is not currently used for an IBM supplied class, be aware that in the future IBM might create a supplied class with this POSIT number. If this conflict occurs, processing results for your class will be unpredictable.. Use a unique POSIT value when you want to administer a class separately from any other class.

When a POSIT value is shared between two or more classes, certain RACF processing options are controlled in the same manner (simultaneously) for all classes with the shared POSIT value.

Any of the following SETROPTS affect the resources or profiles with shared POSIT value:

CLASSACT, AUDIT, STATISTICS, GENERIC, GENCMD, GLOBAL, LOGOPTIONS, RACLIST and ALTUSER *userid* CLAUTH

Therefore, if you deactivate a class using SETROPTS NOCLASSACT, RACF deactivates all classes in the class descriptor table that have the same POSIT value as the class you specify.

For example, the classes TIMS, GIMS, and AIMS all have a POSIT value of 4 in their respective class descriptor table entries.

If you deactivate any one of these classes, you deactivate all of them.

Solving Class and Profile Problems

Now let's solve some problems

Real problems reported by

real people.

Solving Class and Profile Problems (cont)

The most commonly reported problem in IMS security:

Why did IMS abend U0166 at initialization?

- A **required** resource class not active
  - Default classes also need to be activated
  - Deactivated by mistake
    - Maybe class with same POSIT was deactivated
- A **required** resource class not defined
  - Maybe RACF ignored it if >1024 classes defined
- Wrong class specified
  - IMS 13: Maybe RCLASS was not specified in PROCLIB
- SAF product not available
  - Maybe not updated to support a new IMS release

31

Things to know:

1) IMS decides which classes will be required based on your security specifications. If a class is required to satisfy a specification, then it must be defined and active even if it does not contain any profiles.

2) SETROPTS NOCLASSACT(classname) acts on all classes with the same POSIT value. You may accidentally deactivate a class if it shares a POSIT value with a class you deactivated.

3) When you migrate to IMS13, the SECURITY macro goes away so you must specify RCLASS in PROCLIB (DFSPBxxx). If you forget to do this, RCLASS defaults to “IMS” which may not be the class you expect or want.

4)When you migrate to a new release of IMS you may need to update your SAF product (ACF2 for example) to support the new IMS release.

In the U0166 dump register 15 indicates cause of failure:

X'04‘ Unable to perform the requested function

X'08‘ Class specified not defined to RACF

X'0C‘ RACLIST processing error

X'10‘ RACF not active or class not active

X'14‘ RACLIST installation exit routine error

X'18‘ Parameter list error

X'1C‘ RACF not installed or insufficient level of RACF

And register 5 indicates the class: 4=CIMS, 5=TIMS, 6=IIMS, 7= LIMS

Solving Class and Profile Problems (cont)

Why did I start getting this message?

DFS3187W RACF NOT ACTIVE FOR RESUME TPIPE CLASS=RIMS

- Because RACF could not load profiles for RIMS class
  - RIMS secures retrieval of OTMA asynchronous output messages
- IMS functions normally but without security for RESUME TPIPE
  - Any user ID could RESUME TPIPE and retrieve the message

DFS3187W RACF NOT ACTIVE FOR RESUME TPIPE CLASS= RIMS RC=xx RACF EXIT RC=yy REASON CODE=zz.

IMS restart continues. The warning is only applicable for IMS Connect clients who use RESUME TPIPE commands to retrieve asynchronous output messages from the

IMS queues. If the Rxxxxxxx class does not exist or is inactive, there will be no RACF OTMA RESUME TPIPE security.

The DFS3187W message was added in IMS V11 by APAR PM33686.

Solving Class and Profile Problems (cont)

Should I worry about this?

DFS2466I AUTHORIZATION RACLIST FAILED, RACROUTE= 04, 04, 04, 04 RACLIST= 08, 08, 08, 08
REASON= 00, 00, 00, 00 . IMSA

- RACF could not load profiles for the following classes:
  - FIMS,HIMS,SIMS,UIMS,OIMS,WIMS,PIMS,QIMS
- IMS functions normally but application AUTH calls get A4 status code

DFS2466I message issued if one or more of the classes used for application AUTH calls is not defined or not active. IMS doesn't know in advance if an application program will issue an AUTH call so initialization continues. Then, if an application program issues an AUTH call, IMS will return an A4 status code.

Solving Class and Profile Problems (cont)

Why didn't my RACF changes take effect when I recycled IMS?

- Because recycling IMS has no effect on the RACF dataspace
  - Exception: if you activate a new IMS class, recycle IMS to load it into the RACF dataspace
- Updating a RACF resource profile updates the RACF ***database***.
- You must REFRESH the online RACF ***dataspace***
- Issue REFRESH on all systems sharing the RACF database
  - unless RACF is enabled for sysplex communication
- All classes with the same POSIT value will be refreshed

SETROPTS RACLIST(classname) REFRESH causes RACF to reload resource profiles from the database into the data space.

The scope of a RACLIST REFRESH command is the class named on the command plus any other classes sharing the same POSIT value. See z/OS Security Server RACF Security Administrator's Guide for further information.

If your installation has two or more systems sharing a RACF database, you must issue the REFRESH on all systems to have the results effective on all systems, unless RACF is enabled for sysplex communication. However, if you do not perform a refresh on a system sharing a RACF database and that system needs to re-IPL, a fresh copy of the RACLISTed profiles is read from the database at IPL time.

When RACF is enabled for sysplex communication, it propagates the REFRESH command to each of the systems in the data sharing group.

For the DATASET class: RACF caches a list of generic profiles which begin with the HLQ of a data set for which an authorization check has been done.

For example, if you open 'IMSP1.RECON1' then RACF loads the names of all the generic profiles which begin with IMSP1

To refresh the list: SETR GENERIC(DATASET) REFRESH. This purges all of the data set profiles that were cached by RACF.

There are 2 rare cases when IMS has to be recycled for certain RACF changes to take effect:

1) For DATASET resource: if new access is given to a GROUP and IMS was not

previously connected to that GROUP you have to recycle IMS.

2) For general resource: if you activate a new IMS class you have to recycle IMS to get it loaded into a RACF dataspace

Solving Class and Profile Problems (cont)

HELP! My RECONs are dropping like flies!

- Because a user was not authorized to all 3 RECON datasets, VSAM got a RACF violation and told IMS the RECON could not be opened. IMS thought it was an I/O error and discarded it.
- Make sure authorized users are in the access list with an appropriate level of access for all 3 RECON datasets.

When IMS resources like the RECON are protected by RACF, then the user ID of DBRC needs access. Users who run batch DBRC jobs also need access.

If you protect the RECONs in RACF, be sure users have authorization to all 3 RECON datasets.

If the VSAM open for a RECON fails because of a RACF security violation, VSAM tell IMS the RECON could not be opened and IMS interprets the VSAM open failure as an I/O error.

IMS discards that RECON dataset. If the RECON is being accessed READONLY, the user's job will fail and the RECON will not be discarded.

IMS V10 added READONLY support for the RECONs. This is invoked with PARM(READONLY) on the EXEC statement for the DBRC utility (DSPURX00) or by specifying the new READONLY=YES parameter on the DBRC API FUNC=STARTDBRC macro. When READONLY is specified, the RECONs are opened for read. This means that only READ authority is required in SAF (RACF).

As of IMS10, CONTROL is no longer required for users who update the RECONs. Only UPDATE authority is required.

ALTER is still required to DELETE and DEFINE the data sets.

If you invoke the DBRC utility from your program you may use the DSPURXRT entry point. You can specify READONLY through a parameter passed to the entry point in the first word of the argument list

Solving Class and Profile Problems (cont)

Remember:

- Bigger is not better
  - Define new classes the same MAXLNTH as the IMS default classes (8)
  - Changing MAXLNTH gives unpredictable results including 0C4
- Be careful if sharing POSIT value
- RACF allows conflicting profiles and will use these rules
  - the most *specific* (best match)
  - the most *restrictive* UACC
  - the most *permissive* ACCESS

36

Be careful when specifying MAXLNTH. IMS passes up to an 8 character resource class name in the call to RACF and RACF reads MAXLNTH number of characters.

If you tell RACF that MAXLNTH is greater than 8, RACF may pick up “garbage” for part of resource class name and results will be unpredictable

For conflicting profile rules: see z/OS: Security Server RACF Security Administrator's Guide: Resolving Conflicts among Multiple Profiles

Solving Profile Problems (cont)

- Undefined usually means Unprotected
  - RACF return code is 04 for a resource with no profile
  - IMS allows access
  - DBRC does not allow access
    - Do RACF work before activating DBRC Command Authorization (CMDAUTH)

- Beware of using Discrete profiles for datasets
  - Discrete profiles are deleted when the dataset is deleted
  - Avoid this problem by using Fully Qualified Generic profiles or generic profiles.

Areas We Will Explore

- Security Activation
- RACF resource class and profile
- **User ID:** It's not always a person
- Exits
- Dependent region security (RAS)
- References

User ID Concepts

An IMS user ID is not always a person sitting at a terminal…….

An IMS user ID can be for:

- Job, Started Task (BMP, utility, etc.)
- Transaction
- Command
- Logical terminal (LTERM)
- Program (PSB)
- TCO (Time Controlled Operations) script
- IMS Master terminal or system console WTOR

The IMS systems programmer sometimes has to ask the security administrator to create a user ID that does
For example, to allow an IMS program to issue IMS commands you can view the program as though it were

User ID Concepts (cont)

- All IMS regions should have a user ID.
  - Can use RACF STARTED class to assign user ID
  - RACF builds ACEE when region starts
    - This is the “security environment” for that region

40

the RACF user ID will be in the security segment of the x'01' log record. Macro DFSQMSGS in SDFSMAC describes the security segment.

IMS requires all ETO terminals to sign on.

Static terminals are not required to sign on unless specified by IMS parameters (SIGNON parameter in DFSDCxxx member of PROCLIB).

If AUTOSIGN is specified on the TERMINAL or TYPE macro, the terminal will automatically be signed on at logon time, using the LTERM name as the user ID. IMS will issue this sign on to RACF with a request to bypass password checking (PASSCHK=NO in the VERIFY request).

The LTERM user IDs can be defined to RACF.

The IMS Master Terminal and the Console (WTOR) both have unrestricted access to IMS commands and are not forced to SIGN ON. They do need to sign on to issue transactions. They can also be signed on automatically using the DFSDCxxx parameters MTOUSID and WTORUSID.

User ID Concepts (cont)

- If possible, require all users to sign on.
  - ETO users are required to sign on
  - Static terminal users can be forced to sign on
    - SIGNON=ALL
- You can automatically assign a user ID (no password) for
  - Static terminals with AUTOSIGN=
  - System console with WTORUSID=
  - IMS Master with MTOUSID=
  - TCO script with SIGNTCO=

41

the RACF user ID will be in the security segment of the x'01' log record. Macro DFSQMSGS in SDFSMAC describes the security segment.

IMS requires all ETO terminals to sign on.

Static terminals are not required to sign on unless specified by IMS parameters (SIGNON parameter in DFSDCxxx member of PROCLIB).

If AUTOSIGN is specified on the TERMINAL or TYPE macro, the terminal will automatically be signed on at logon time, using the LTERM name as the user ID. IMS will issue this sign on to RACF with a request to bypass password checking (PASSCHK=NO in the VERIFY request).

The LTERM user IDs can be defined to RACF.

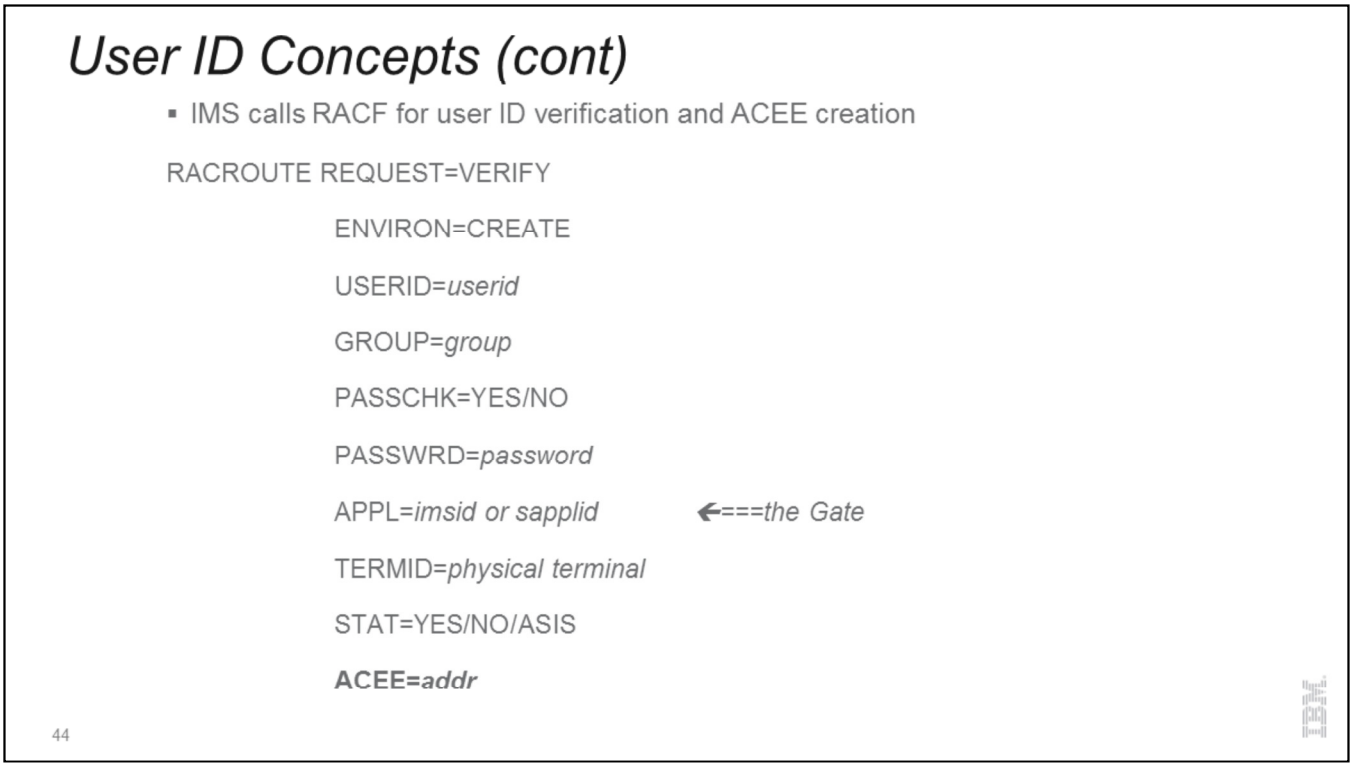
The IMS Master Terminal and the Console (WTOR) both have unrestricted access to IMS commands and are not forced to SIGN ON. They do need to sign on to issue transactions. They can also be signed on automatically using the DFSDCxxx parameters MTOUSID and WTORUSID.


United Kingdom of Great Britain and Northern Ireland
Passport Passeport
Type/Type
P
State
GBR
Passport No/Passeport No
023477812
Surname/Nom
BEAN
Given name/Prenom
MR
Nationality/Nationalite
BRITISH CITIZEN
Date of birth/Date de naissance
6 JAN/JAN 55
Children/Enfants
0
Sex/Sexe
M
Place of birth/lieu de naissance
ENFIELD
Date of issue/Date de delivrance
20 SEP/SEP 96
Authority/Autorite
UNITED KINGDOM
PASSPORT AGENCY
Date of expiry/Date d'expiration
20 SEP/SEP 06
Observations-page/Observation-page
P<GB<MR<BEAN<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
023477812GBR8111063M0004422<<<<<<<<<<<<<<<<06
42

The APPL Gate

Think of this as the APPL gate. Users go through the SAPPLID door in the middle. JOBS and APPC attach requests go through the side IMSID doors.

SAPPLID is an 8 character value you can specify in DFSDCxxx. It defaults to IMSID.



RACF verifies user ID, group, physical terminal, **application**
If PASSCHK=YES, RACF verifies password
RACF builds ACEE
RACF returns ACEE address and SAF return code to IMS
IMS logs x'16'

Reference: z/OS Security Server RACF RACROUTE Macro Reference

•*STAT determines whether RACF will update the user's profile with date/time of last access*

TERMID is the physical terminal being used. If it is protected in the RACF TERMINAL/GTERMNL class, then the user must be authorized in the access list.

APPL is the application the user is accessing. When applications like IMS, TSO, CICS, etc. are protected in the RACF APPL class, the user must be authorized in the access list.

If IMS RAS security is activated (ISIS=R|A), all dependent region user IDs must also be authorized in the access list of the *imsid* in the APPL class.

User ID Concepts (cont)

When the user signs off

- IMS calls RACF to delete the user's ACEE
  RACROUTE REQUEST=VERIFY,ENVIR=DELETE,ACEE=addr…
- IMS logs x'16'

An accessor environment element (ACEE) is a control block that represents the security environment for the user.

An ACEE is constructed for IMS users when IMS calls RACF to VERIFY a user ID. It provides a description of the current user, including userid, current connect group, user attributes, and group authorities.

Each user in a group requires a level of group authority for that group. If a user is connected to several groups, the user has a level of group authority for each group.

Basically, a user's authority to access a resource while operating in a RACF-protected system at any time is determined by a combination of user's identity,

user's attributes, user's group authorities, security classification of the user and the resource profile, and access authority specified in the resource profile.

IMS keeps track of user/ACEE relationships and passes the appropriate ACEE pointer to RACROUTE REQUEST=AUTH and RACROUTE REQUEST=VERIFY (CHANGE or DELETE).

User ID Concepts (cont)

Messages from SNA terminal

- ETO user must /SIGN ON

- If static terminal sign on is not required
  - User can /SIGN ON
  - IMS can specify AUTOSIGN
  - If user does not sign on
    - No VERIFY call to RACF, no ACEE is built
    - RACF uses “security environment” (ACEE) of caller (IMS CTL)
    - IMS puts the LTERM in the user ID field of the message

IMS puts a user ID in the security segment of the x'01' log record. Macro DFSQMSGS in SDFSMAC describ
IMS requires all ETO terminals to sign on.
Static terminals are not required to sign on unless specified by IMS parameters (SIGNON parameter in DF
If AUTOSIGN is specified on the TERMINAL or TYPE macro, the terminal will automatically be signed on at
The LTERM user IDs can be defined to RACF.
The IMS Master Terminal and the Console (WTOR) both have unrestricted access to IMS commands and a

User ID Concepts (cont)

MSC

- Messages from many different IMS users flow across the physical link
- It is a 'pooled connection‘
- IMS includes original user ID from the original msg (from SNA terminal, APPC or OTMA message, etc) in the IMS control data of the message
- Back end IMS can rebuild an ACEE for that user ID and use it for authorization
  - If further authorization is required on the back end

APPC

- User ID is in a control section of the input message

IMS puts a user ID in the security segment of the x'01' log record. Macro DFSQMSGS in SDFSMAC describ
IMS requires all ETO terminals to sign on.
Static terminals are not required to sign on unless specified by IMS parameters (SIGNON parameter in DF
If AUTOSIGN is specified on the TERMINAL or TYPE macro, the terminal will automatically be signed on at
The LTERM user IDs can be defined to RACF.
The IMS Master Terminal and the Console (WTOR) both have unrestricted access to IMS commands and a

User ID Concepts (cont)

CICS (ISC)

- "Pooled connection": messages from many users flow across the link
  - Unlike MSC, does not include control information for the user ID.
  - IMS treats it as a legacy terminal that signs on once with one user ID
- CICS itself can issue /SIGN ON
- CICS can define a default user ID
  - DFLTUSER
- If no sign on and no default user ID
  - dynamic links
    - USER ID=SUBPOOL name
  - static links
    - RACF uses IMS CTL user ID for transaction authorization
    - IMS puts LTERM name in user ID field of message

To signon a static ISC link either CICS must issue a /SIGN ON command after the session is established or AUTOSIGN must be specified in IMS for this link. For AUTOSIGN IMS will automatically signon the session to RACF using the USER/SUBPOOL name as the userid. For a static ISC link that has not signed on to IMS, RACF will use the IMS CTL region user ID for transaction authorization and the input message (01 log record) will be queued with the ISC LTERM name as the user ID. This user ID will be used for dependent region CHNG and AUTH call security. For dynamic ISC links RACF signon is performed at logon using the USER/SUBPOOL as the userid (same as AUTOSIGN for static).

User ID Concepts (cont)

Messages from IMS Connect client => IMS Connect

- IMS Connect or IMS Connect client can do user ID verification
- RACF=Y/N in HWSCFG
  - RACF=Y ICON calls RACF to verify user ID and password
  - RACF=N ICON does not call RACF directly
- ICON User Message Exit
  - can do RACF user verification
  - can set “Trusted User” flag

Trusted User support bypasses the security check for messages from 'trusted' users even if IMS Connect sp
Trusted User support is provided by HWSSMPL0/HWSSMPL1 user message exits
To implement trusted user support define and provide logic in both the client (indicator in the IRM) and the IM
HWSSMPL0/HWSSMPL1 or your own user message exit to detect the indicator in the IRM and bypasses se

User ID Concepts (cont)

From IMS Connect client => IMS Connect

- User ID and password or passticket in the message
  - Entered by IMS Connect client
  - Set by the IMS Connect User Message Exit
- APPLname is optional
  - Entered by IMS Connect client
  - Set by IMS Connect User Message Exit
  - Defaulted to on DATASTORE control cards

Passticket support provides an encrypted alternative to sending a password. A passticket is a one-time-only password that removes the need to send passwords across the network in clear text. It is generated/interpreted by an algorithm using:

User ID,Application identifier (APPLID), Timestamp, Secured signon key for encryption.

The client environment generates the PassTicket and IMS Connect calls RACF to interpret/validate the PassTicket

Uses APPLID value coded on DATASTORE statement or value passed in the IRM header

RACF uses the PTKTDATA resource class profile definition for APPLID name.

User ID Concepts (cont)

From IMS Connect => IMS OTMA

- ICON passes message with user ID or UTOKEN to IMS OTMA
  - ICON does not send password to IMS OTMA
- If OTMA security is active, OTMA calls RACF to build ACEE
  - OTMASE=C/F
  - OTMASE=P use the security specified in the message
- If RACF cannot build ACEE, message is rejected
- ACEE is cached by OTMA and can be “aged off” or “refreshed”

51

A cache, or hash table, is used to store previously verified user IDs. Each OTMA client (IMS Connect, WebSphere MQ for z/OS®, or others) has a hash table created in the IMS control region after a successful client bid. Use of the hash table minimizes the number of calls to RACF to VERIFY user IDs. This way, if the same user ID enters multiple messages destined for IMS/OTMA, IMS can check the hash table for a valid entry for the user ID and might be able to avoid the VERIFY call to RACF. The entry for the user ID in the hash table contains a pointer to the accessor environment element (ACEE) for the user ID. The ACEE that is pointed to can be used for resource (command and transaction) FASTAUTH calls to RACF.

IMS calls RACF to VERIFY that the user ID in the incoming message is a valid user ID (one that has been defined to RACF).If the OTMA client (IMS Connect or WebSphere MQ for z/OS) supplied a UTOKEN in the incoming message, IMS supplies the address of the UTOKEN on the VERIFY call to RACF and RACF returns an ACEE security control block to IMS for verified user IDs.

IMS calls RACFto verify that the user ID in the incoming message is authorized to the IMS transaction code set as the destination on a DL/I CHNG or AUTH call. A cached ACEE is used for these calls, which eliminates performance concerns for application programs that issue many CHNG or AUTH calls.

User ID Concepts (cont)

- If NMD BMP inserts a message
  - BMPUSID specifies what should be placed in user ID field of inserted message
    - BMPUSID=USERID is value of USER= on JOB statement
    - BMPUSID=PSBNAME
  - If BMPUSID is not specified the PSB is placed in the user ID field of the inserted message
  - Specify BMPUSID on the DFSDCxxx member of PROCLIB

- Message-driven BMP
  - Authorization is against the user ID associated with each transaction message
  - BMPUSID is ignored

BMPUSID is only for NMD BMPs. For message-driven BMPs, authorization is against the user ID associated with each transaction message, regardless of the BMPUSID setting.

BMPUSID=PSBNAME | USERID

Specifies the value to be placed in the user ID field of the message prefix for a message generated by a non-message driven BMP and the value to be used for the userid for CHNG and AUTH calls made by a non-message-driven BMP.

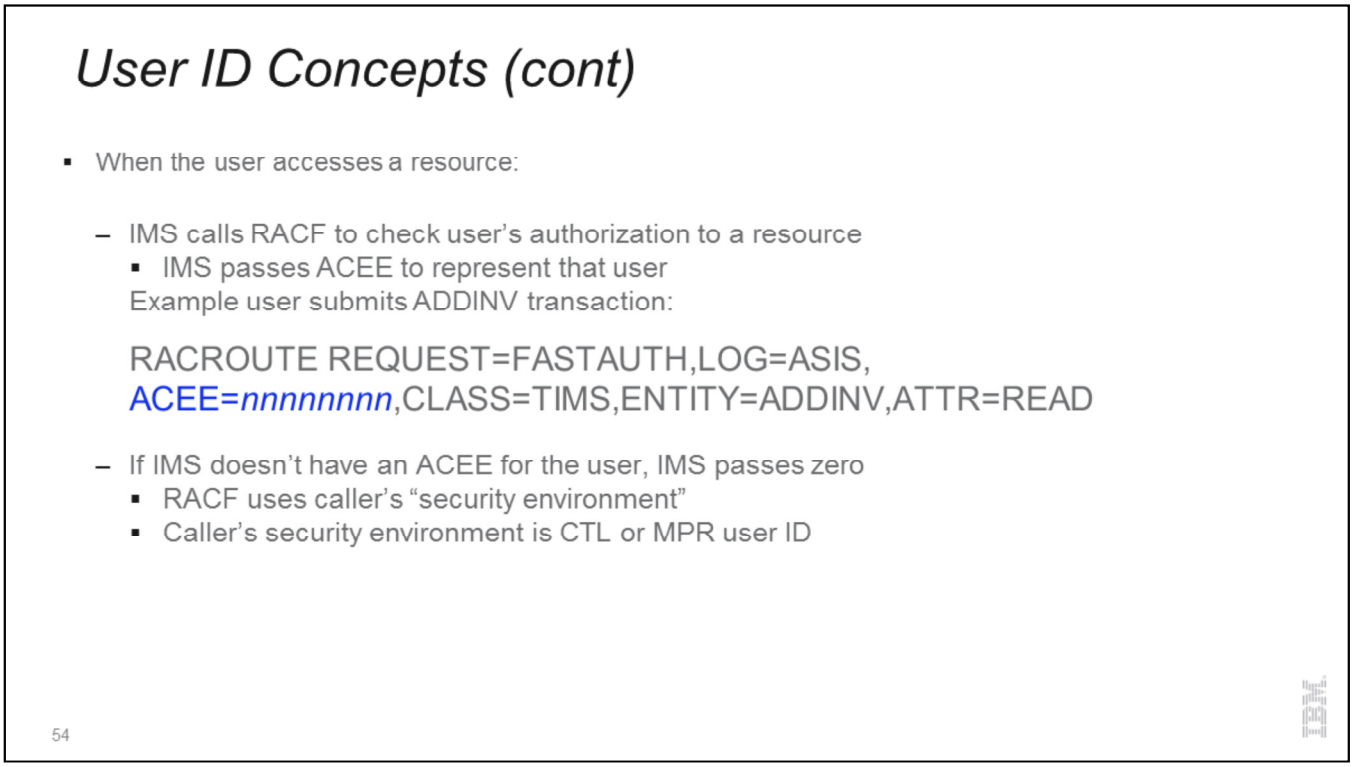
If BMPUSID=USERID is specified, the value from the USER= keyword on the JOB statement is used.

If USER= is not specified on the JOB statement, the program's PSB name is used.

If BMPUSID=PSBNAME is specified, or if BMPUSID= is not specified at all, the program's PSB name is used.

User ID Concepts (cont)

- User ID is valid. But what is the user authorized to do?



If there is no ACEE to represent the user, then the user ID of the address space making the call (CTL or MPR) will be used whenever IMS calls RACF to check the user's authorization to a resource.

In the example, IMS is calling RACF to see if the user can do /DIS protected in the CIMS class. IMS has no ACEE to pass so RACF will use IMS CTL user ID. If the IMS control region user ID has read access to the Display command, then the user will be allowed to issue that command.

Be careful about giving IMS CTL access to resources it does not need.

LOG= describes the auditing options

ASIS RACF records the event in the manner specified in the profile that protects the resource, or by other methods such as a SETROPTS option.

For FASTAUTH, IMS (as of version 10) always specifies LOG=ASIS

ASIS - RACF performs auditing if its authorization check results in success (RC=0) or failure (RC=8), and determines whether auditing is necessary based on the following conditions:

The user's UAUDIT setting

The AUDIT, GLOBALAUDIT, and WARNING options in effect for the resource

If SETR SECLABELAUDIT is in effect, then the AUDIT options in the resource SECLABEL profile

The pre- or postprocessing installation exit's indication of whether or not to do auditing.

NOFAIL - If the authorization check fails, the attempt is not recorded. If the authorization check succeeds, the attempt is recorded as in ASIS.

NONE - The attempt is not recorded. LOG=NONE suppresses both messages and SMF records regardless of MSGSUPP=NO.

User ID Concepts (cont)

- Once a transaction is scheduled and running in MPR, what happens if it accesses another resource?
  - Issues CHNG call
  - Issues AUTH call
  - Does a deferred conversational program-program switch
  - Calls external subsystem (DB2, MQ)
  - Issues a command (AOI)
    - IMS commands are always processed in CTL
    - TRANSACT macro must specify AOI parameter

An ACEE control block representing a user is built in the IMS control region when the user signs on and deleted when the user signs off.

Once a transaction is authorized and scheduled into a dependent region, it may do things that require additional resource authorizations. For example, it may do a message switch to spawn a new transaction. The dependent region will have to call RACF to see if the user ID is authorized to do the new transaction. It may issue an AUTH call to see if the user ID is authorized to a database, field or segment. If it calls DB2, DB2 can use the ACEE to authorize the use of DB2 resources by that user.

User ID Concepts (cont)

- Program does CHNG call, AUTH call, deferred conversational pgm switch
  - For non-OTMA, IMS dynamically builds a temporary ACEE in MPR
  - OTMA can access cached ACEE (no build necessary)
- Dynamically built ACEE does not change the MPR "security environment"

A dynamic build of ACEE in MPR is not necessary for OTMA messages because OTMA can access the cached ACEEs.

User ID Concepts (cont)

To avoid dynamic build

- DFSBSEX0 R15=04 builds ACEE in MPR when msg scheduled
- APPCSE=F builds ACEE in MPR when msg scheduled
- OTMASE=F builds ACEE in MPR when msg scheduled
- This changes the MPR "security environment"
  - MPR security environment is now end user ACEE

With OTMA or APPC security set to FULL, the user's ACEE will be built in both the dependent region and the IMS control region when the message is scheduled. Since OTMA can now access the cached ACEEs from the MPR OTMA=F is not necessary unless the application does external subsystem calls.

DFSBSEX0 set to condition code 4 tells IMS to build an ACEE for the user in both the dependent region and the control region when the message is scheduled.

If an ACEE is built for the end user in the MPR using FULL or DFSBSEX0 04, that ACEE because the MPR's "security environment" while that transaction is running. The user's ACEE will be used for all calls to RACF for the life of that message. Therefore the user's ID might need access to resources like JESSPOOL and LOGSTRM for example.

If you do not enforce sign on and there is no user ID signed on, then with DFSBSEX0 RC04 the user's LTERM name is used as user ID.

DFSBSEX0 can also be used to bypass security checks.

User ID Concepts (cont)

Be aware:

- If dynamic build fails
  - ACEE of caller's "security environment" is used
    - MPR user ID
    - CTL user ID

If RACF cannot build the dynamic ACEE, the subsequent authorization call will be made with ACEE of zero and RACF uses the caller's security environment (CTL or MPR) for authorization. For example, if a NMD BMP inserted a message with PSB as user ID. Then the new transaction issues a CHNG call and RACF cannot build an ACEE for the PSB because the PSB is not defined as a user ID in RACF. Then IMS calls RACF for authorization with ACEE 0 and the resource on the CHNG call will be authorized against the MPR user ID. If the MPR does not have a user ID, the CTL user ID will be used.

User ID Concepts (cont)

If the application program calls DB2

- IMS can pass user ID and group to DB2 Signon Exit
  - DB2 can do RACF VERIFY call
  - User ID passed is from original input message
    - Signed on user ID
    - LTERM if user not signed on
    - PSB or USER= if NMD BMP

or

- DB2 can access ACEE of MPR "security environment" directly
  - Enhancement PM27835

Security for the ESS interface can be provided by the DB2 Signon Exit routine. The Signon Exit Routine informs the external subsystem (ESS) of the userid associated with the transaction input message. IMS can pass the userid and group name in an EPL to the Signon Exit. The userid that is passed is extracted from the original input message prefix and can be the:

Inputting LTERM name (if the terminal user is not signed on)

RACF userid of a non-message driven BMP

PSB name (or USER= specification from the JOB card) of a non-message driven BMP

The Signon Exit is created by the external subsystem. IMS passes it (the Signon Exit) security information in the extended parameter list (EPL) in the form of a userid and group name.

When a connection is initially established, the Signon Exit Routine is activated before a thread is created by the Create Thread exit routine. All subsequent requests result in the exit routine being activated after a thread is created. For example, Signon is activated for each message processed during a single scheduling, whether or not the messages are separated by commit processing.

User ID Concepts (cont)

- DB2 can access ACEE of MPR "security environment" directly
  - MPR "security environment" is ACEE of MPR user ID
  - To set MPR security environment to ACEE of end user:
    - OTMASE=F
    - APPCSE=F
    - For non-OTMA non-APPC code DFSBSEX0 R15=04

DB2 enhancement PM27835 (RSU1112) gives DB2 direct access to the ACEE if IMS has been configured to use APPC/OTMA security full or the DFSBSEX0 security exit has been configured to return RC04 in register15 to tell IMS to create the ACEE in the dependent region.

User ID Concepts (cont)

Be aware:

- DFSBSEX0 Reg15=04 or OTMASE=F or APPCSE=F
  - Sets security environment of MPR = ACEE of user who submitted the message
  - **All** RACF calls for the message will use end user's ACEE
    - End user *may* need access to other resources like dump datasets, etc.

When IMS regions are started, an ACEE is built for the region user ID. This is a "security environment" at the address space level (ASXBSENV) and all calls to RACF from that address space would use that environment.

When a program does the GU, you can use OTMA FULL or DFSBSEX0 04 to set a TCB-level security environment (TCBSENV) that points to the ACEE of the user who submitted the message. Keep in mind this also means, any resources that are accessed from the dependent region must be authorized to the user ID of the person who submitted the message.

Solving User ID Problems

Now let's solve some problems

Real problems reported by
real people.

Solving User ID Problems

Why does an active IMS user keep getting his user ID deleted from RACF?

- Last Access Date is not being updated.
- Only a VERIFY call will update the Last Access Date.
- For example: with MSC, if VERIFY call is done on the front end and the back end IMS uses a different RACF database, the user ID can look inactive on the back end RACF database.

The last accessed date only gets updated when a RACROUTE REQUEST=VERIFY is issued to authenticate the user.

It does not get updated by a RACROUTE REQUEST=AUTH for authorizing access to a resource.

In this example, the user had an MSC network. The front end and back end IMS systems had 2 different RACF databases. Although the user was defined in each RACF database, he rarely signed onto the back end IMS. Even though his transactions often ran on the back end IMS, his user ID profile was not updated there unless a VERIFY call was done. He usually signed onto the front end IMS and the VERIFY call was done there.

.

Solving User ID Problems

Why are we seeing such high I/O to the RACF database coming from IMS?

- Do not always blame IMS.
- For example, if your DB2 Signon Exit specifies STAT=YES on the VERIFY, then every time DB2 does a VERIFY call, the user's profile is updated in the RACF database. You can specify STAT=NO or you can specify you only want stats updated once a day, or DB2 can access the existing ACEE that IMS has already verified.

Solving User ID Problems (cont)

My automation product is getting a security violation shutting down a WFI BMP.

- Your automation is using the WTOR to issue a transaction that tells the BMP to stop.
- RACF is called to authorize the transaction and a user ID is required.
- You can use WTORUSID to assign a user ID to the WTOR, define that user ID to RACF and give it authority to issue the transaction.
- Commands can be entered through WTOR without a sign on because RACF is not called for commands from WTOR.

Solving User ID Problems (cont)

Why did IMS Connect allow an unauthorized user to access a transaction even though I have RACF=Y?

- Because IMS Connect never does transaction authorization. RACF=Y tells IMS Connect to do user ID verification.
- IMS (not IMS Connect) does transaction authorization if you specify OTMASE=C/F/P

Solving User ID Problems (cont)

Why is DB2 returning -922 for users who should be authorized?

- Because when the transaction calls DB2, DB2 is directly accessing the ACEE of the MPR's "security environment".
- The MPR "security environment" is the MPR user ID and the MPR user ID is not authorized to the resources.

- You can change the "security environment" in the MPR by setting OTMASE=F for OTMA messages, APPCSE=F for APPC messages and DFSBSEX0 code 04 for all other messages.

Solving User ID Problems (cont)

We set OTMASE=F so DB2 can get the right user ID. Why is the MPR now getting security violations for LOGSTRM and JESSPOOL? The MPR is authorized to those resources.

- Because OTMASE=F tells IMS to build an ACEE for the end user in the MPR. This changes the "security environment" of the MPR to point to the end user's ID instead of the MPR's user ID. All RACF authorization calls while that user's transaction is processing will be made with that end user's ACEE.

It's not that common for the MPR to need access to other resources so OTMASE=F may not cause this issue in your environment.

Areas We Will Explore

- Security Activation
- RACF resource class and profile
- User ID
- **Exits:** Don't pick up hitch-hikers
- Dependent region security (RAS)
- References

Exit Concepts (cont)

- Can be used alone or with RACF
- May provide more granularity than the RACF profile
- Most exits can now be refreshed dynamically
- Can override the RACF result
  - Called after RACF

Some IMS security-related exits:

Sign on/off verification: DFSCSGN0, DFSSGNX0, DFSSGFX0

Transaction authorization: DFSCTRN0, DFSCTSE0 (reverify), DFSBSEX0 (build security env)

Command authorization: DFSCCMD0, DSPDCAX0 (DBRC), OM user exits

RAS (dependent region/thread): DFSRAS00

Other: DFSYRTUX (OTMA), DFSTCNT0 (TCO), DFSCMPX0 (encryption), DFSFLGE0 (log edit),

DFSMSCE0 (MSC), HWSAUTH0 (ODBM), IMSLSECX (IMS Connect)

Exit Concepts (cont)

- If an exit cannot be explicitly specified, IMS will invoke it if it exists
  - The IVP may install sample exits into RESLIB if you specify RACF on IVP panel
- If an exit is explicitly specified, IMS will not come up if it does not exist
  - U0718 on initialization

IMS will abend during initialization with U718 if you specify the use of an exit and the exit does not exist.

If an exit cannot be explicitly specified IMS will invoke it if it exists. For example, the RCF parameter offers no value to specify the Command Authorization Exit. Therefore DFSCCMD0 will be invoked after RACF if it exists.

Some parameters, like CMDMCS for example, do provide values to explicitly specify the use of the Command Authorization Exit.

Exit Concepts (cont)

- The Command Authorization Exit (DFSCCMD0) is not invoked by Operations Manager (OM)
  - OM invokes its own user exits
- The Transaction Authorization Exit (DFSCTRN0) is never invoked if the RACF return code is greater than 4.
- The Transaction Reverification Exit (DFSCTSE0) is invoked if the RACF return code is greater than 4

Prior to IMS13, you had to specify TRANEXIT and SIGNEXIT on the SECURITY macro in order for those exits to be invoked. IMS13 makes them standalone exits in RESLIB similar to DFSCCMD0 and they will be invoked if they exist.

Exit Concepts (cont)

- The Build Security Environment (DFSBSEX0) is invoked before the message is given to the application program
  - Not initially called for messages from OTMA, APPC, NMD BMP
- DFSBSEX0 is always invoked for CHNG and AUTH calls no matter where the original message came from
- DFSBSEX0 is called when the security environment does not exist
  - For example: CHNG call on back-end SMQ or MSC

DFSBSEX0 is a standalone module in STEPLIB. It receives control before the input message is given to an IMS application program.

IMS invokes the Build Security Environment exit routine before the first or next input message is given to an IMS application program, where the input message is not from OTMA, APPC or a NMD BMP. However, the exit is called for all AUTH and CHNG calls, regardless of the origin device of the input transaction.

Prior to passing the message for TRANX to PGMX for processing, IMS checks to see if the Build Security Environment Exit Routine (DFSBSEX0) has been included in the system. If DFSBSEX0 has been included, it is called to determine whether or not the ACEE used to authorize the user's access to TRANX should be copied to the dependent region and, if copied, when it should be copied. DFSBSEX0 may be customized to determine:

•Whether or not the ACEE should be built at all, and if so, whether it is built now before giving the message to the program (PGMX) …

• Or later when the application requests a transaction by issuing a CHNG call, AUTH call, or deferred conversational program-to-program switch

•The security facilities to call to perform authorization checking

Prior to returning to IMS, the exit sets the contents of register 15. The register 15 contents informs IMS what to do next.

If you do not enforce sign on and there is no user ID signed on, then with RC04 the user's LTERM name would be used.

the exit gets program name, transaction code, userid, transaction class, etc.

The DFSBSEX0 exit is called when the security environment for the user has to be created because it does not exist on the environment

where the user signed on. Here are some examples:

a) SMQ, user not signed on to back-end IMS (SMQ or MSC) and program issues

CHNG call

b) user signed on, submitted a transaction, and signed off and program issues CHNG Summarizing this question:

Exit Concepts (cont)

- With IMS13, these exits no longer linked into Nucleus:
  - Sign On DFSCSGN0
  - Transaction Authorization (DFSCTRN0)
  - Transaction Reverification (DFSCTSE0)
- With IMS13, these exits are:
  - standalone members of RESLIB
  - invoked if they exist
  - loaded dynamically
    - use of VCONs to reference other modules or ctl blks will no longer work
- New initialization call (R0=4) added for DFSCSGN0
  - verify your DFSCSGN0 exits will function correctly with this new entry vector

74

Prior to IMS13, exits DFSCSGN0, DFSCTRN0, DFSCTSE0 were only invoked if specified on the SECURITY macro (SIGNEXIT, TRANEXIT) and linked into the IMS Nucleus.

Solving Exit Problems

Now let's solve some problems

Real problems reported by
real people.

Solving Exit Problems (cont)

RACF rejected the command but IMS did it anyway!

```
15:36:21.32 STC00761 00000281  ICH408I USER(IMSUSRA  ) GROUP(IMSOPRL  ) NAME(#####
              785 00000281    ASS CL(CIMS    )
              785 00000281    INSUFFICIENT ACCESS AUTHORITY
              785 00000281    ACCESS INTENT(READ    ) ACCESS ALLOWED(NONE    )

DFS058I 15:36:21 ASSIGN COMMAND COMPLETED
```

Command Authorization Exit (DFSCCMD0) allowed the command.

RACF rejected the command but IMS did it anyway.

RACF issued the ICH408I message because IMS called RACF with LOG=ASIS. (Prior to IMS10 you would not have seen the ICH408I message because prior to IMS10, the FASTAUTH option did not log the message. To get the ICH408I message prior to IMS10, IMS issued a second AUTH call to RACF to log the message.)

Solving Exit Problems (cont)

Results when DFSCCMD0 was removed from RESLIB:

```
15:36:21.32 STC00761 00000281  ICH408I USER(IMSUSRA  ) GROUP(IMSOPRL  ) NAME(#####
            785 00000281    ASS CL(CIMS     )
            785 00000281    INSUFFICIENT ACCESS AUTHORITY
            785 00000281    ACCESS INTENT(READ    ) ACCESS ALLOWED(NONE    )

DFS3662W 16:23:58 COMMAND REJECTED BY RACF; USER NOT AUTH   ; RC= 0008
```


Solving Exit Problems (cont)

I removed the sample DFSCCMD0 exit from RESLIB and now IMS won't come up.

- Because any of these parameters cause IMS to load DFSCCMD0
  - CMDSEC=E or A
  - AOI1=A or C
  - AOIS=A or C
  - CMDMCS=B or C

- **Any** exit you explicitly specify must exist or IMS will abend.
  - U0718

Solving Exit Problems (cont)

After migrating to IMS13, we started getting sign on security violations

- Because there was an old version of DFSCSGN0 exit in RESLIB
- Prior to IMS13, DFSCSGN0 was not invoked
  - if SECURITY macro specified NOSIGNEXIT
- IMS13 invokes DFSCSGN0
  - if it is in RESLIB

SIGNEXIT on the SECURITY macro (prior to IMS13) specifies the use of the older signon exit, DFSCSGN0.

The newer signon exit, DFSSGNX0, is included in the system when you specify ETO=Y.

Solving Exit Problems (cont)

- Be careful not to accidentally pick up an exit.
  - Are there exits in your RESLIB?
  - Should they be there?
  - Are they obsolete?
  - Do you want them?

- When IMS comes up, look for
  DFS1937I USER EXIT DFSxxxx0 LOADED

Areas We Will Explore

- Security Activation
- RACF resource class and profile
- User ID
- Exits
- **Dependent region security (RAS)**
- References

The APPL Gate

Think of this as the APPL gate. Users go through the SAPPLID door in the middle. JOBS and APPC attach requests go through the side IMSID doors.

SAPPLID is a 4 character value you can specify in DFSDCxxx. It defaults to IMSID.

RAS Concepts (cont)

RACF APPL class

- Restrict terminal users' access to applications (TSO, IMS, CICS, etc.)
  - Define a RACF profile for *sapplid* in APPL class
  - Specify *sapplid* in DFSDCxxx
  - *sapplid* defaults to *imsid*
- Control ATTACH requests
  - Protect conversations between partner LUs
- Control whether a dependent region can connect to IMS
  - **This check is only made if IMS RAS security is active (ISIS=R|A)**
  - Examples of dependent regions: BMP, CICS, DB2 stored procedure
  - Define a RACF profile for *imsid* in the APPL class

You can restrict online access to IMS using the APPL class in RACF to protect the imsid.

When the user attempts to sign on, IMS uses RACF to verify the user's identity and his authority to access the specific IMS control region. IMS passes the application identifier for IMS on the RACROUTE REQUEST=VERIFY macro using the APPL= parameter.

RACF does an authorization check to determine the user's authorization to the IMS identified by the APPL= parameter on the RACROUTE request.

You can also use the APPL resource class to protect conversations between partner LUs. This support provides the ability to grant or deny access on the basis of the identity of both the user and the logical unit (LU) from which the user's request originated.

When RAS security is activated (ISIS), you can use the APPL class to control access to IMS by dependent regions such as MPP,BMP,CICS,JBP,JMP,IFP,DB2 stored procedures, etc.

RAS Concepts (cont)

With RAS enabled (ISIS in DFSPBxxx):

- First RAS check: getting through the gate
  - Is the dependent region allowed to connect to IMS
  - Protect imsid in RACF APPL class
  - If RAS security is activated ***all*** authorized dependent regions need access
    - PERMIT IMSP CLASS(APPL) ID(MPP1,BMP1,CICS1,etc.) ACCESS(READ)
  - The RAS exit DFSRAS00 can specify exclusions from this check.

RAS Concepts (cont)

With RAS enabled (ISIS)

- Second check: getting in the house
  - Is the dependent region allowed to access PSB, TRAN, LTERM?
  - Define resources you want to protect
    - IIMS/JIMS for PSB
    - TIMS/GIMS for TRAN
    - LIMS/MIMS for LTERM
  - If RAS security is activated ***all*** authorized dependent regions need access to the resources
  - The RAS exit (DFSRAS00) can define exclusions from these checks

Solving RAS Problems

Now let's solve some RAS problems

Solving RAS Problems (cont)

An unauthorized user updated a production database!

- Because the user submitted a BMP and ISIS=N
- Without RAS security
  - Any user can submit a BMP from TSO for any PSB with no security checks
- Some customers use alternative controls for job submission
  - RACF Program Control
  - job scheduling product
  - z/OS exit

Programmer submitted a BMP from TSO and accidentally specified production IMS in his JCL. The BMP ran with the programmer's TSO ID.

Although the programmer himself could not have signed on to IMS because his ID was not authorized to the production imsid in the RACF APPL class, ("user not authorized to application"), the BMP does not go through that APPL check unless IMS RAS security is activated.

As for the user having no access to production databases, in the online environment it is DL/I that needs access to the databases, not the user.

Note that some shops use alternatives to protect the production system from unauthorized jobs. For example: some use a z/OS exit to allow only certain user IDs to run on the production LPAR, some use a feature of their job scheduling system.

The important thing is to make sure you have something in place to control what jobs can run in production.

Solving RAS Problems (cont)

I activated RAS and now my MPRs won't come up.

DFS2854A …. FAILED SECURITY CHECK

- Because with RAS active, all dependent regions need access to the imsid and any protected resources accessed in that region
  - The user ID of the MPR must be authorized to imsid
  - The user ID of the MPR must be authorized to transactions
  - DFSRAS00 exit can be used to bypass the MPR security check

Solving RAS Problems (cont)

I added a new transaction and gave the users access to it. Why are they getting RACF violations?

- The message region is getting the violation, not the user. RAS is active and you did not give the MPR access to the transaction.
  - You will see that the user ID specified in the ICH408I message is the MPR, not the user who submitted the transaction.
- The user ID of the MPR must be authorized to transactions
- DFSRAS00 exit can be used to bypass some checking

When you get a security violation, the user ID that is failing authorization appears in the RACF message. In this example, the user ID belonged to the dependent region.

Solving RAS Problems (cont)

- You can use the RAS exit (DFSRAS00) to bypass security checks for certain regions, resources, region types, etc.
  - For example you could activate RAS only for BMPs

Solving RAS Problems (cont)

It's too much work to protect the imsid because I will have to define all the online users in the RACF access list for the imsid.

- You can define a value for SAPPLID that is different from the imsid and leave that access open.
  - RACF VERIFY for online users is always done against SAPPLID
  - RACF VERIFY for dependent regions is always done against IMSID
  - SAPPLID (in DFSDCxxx) defaults to IMSID
- Using SAPPLID also allows you to separate access
  - For example: let a user sign onto IMS but not submit BMPs

Access to IMS can be controlled at a high level using the RACF APPL class.

When a user signs on, the IMS passes the value of SAPPLID to RACF and RACF checks that the user has READ access.

If you do not specify a value for SAPPLID, it defaults to IMSID.

This check is always made.

When a dependent region tries to connect to IMS, RACF does the same check but against IMSID, not SAPPLID

This check is only made if you enable Resource Access Security (RAS). It is made for every region (MPP,BMP,CICS,DB2 stored procedure, etc.). You can use the RAS exit DFSRAS00 to exclude some region types from this security check.

REFERENCES

References

- IMS Home Page

  www.ibm.com/ims contains links to

  - Upcoming Webcasts, Roadshows and other events
  - Samples submitted by IBM and customers (IMS Examples Exchange)
  - Presentations/papers
  - Library
  - IMS Tools and the Tools library
  - Information Center
  - IMS Newsletters
  - And more

References (cont)

User Groups and Forums

IMS Regional User Groups
www.ims-ug.org

IMS-L
http://imslistserv.bmc.com/

Virtual IMS Connection
http://www.virtualims.com

References (cont)

New 3-volume Redbook set for Security on the IBM Mainframe

Volume 1 published December 2014. Volume 2 and 3 in the future.

Security on the IBM Mainframe, Vol. 1 A Holistic Approach by Reducing Risk and Improving Security SG24-7803-01

Vol 1: Overall introduction of mainframe security architecture and best practices

Vol 2: Networking and communications server security architecture and best practices

Vol 3: Security architecture and best practices for software products like DB2, CICS, IMS

References (cont)

IBM strongly suggests that all System z customers be subscribed to the IBM System z Security Portal to receive the latest critical System z security and system integrity service. If you are not subscribed, see the instructions on the System z Security web site

http://www-03.ibm.com/systems/z/advantages/security/integrity_sub.html

Security and system integrity APARs and associated fixes will be posted to this portal. IBM suggests reviewing the CVSS scores and applying all security or integrity fixes as soon as possible to minimize any potential risk.

The “windows”	The keys	Where to find the keys
3270 terminal	RCF	DFSPB
TCO script	RCF and TCORACF	DFSPB
OTMA	OTMASE	DFSPB
ODBA	ODBASE or ISIS	DFSPB
APPC / LU 6.2	APPCSE	DFSPB
MSC	MSCSEC	DFSDC
Operations Manager (OM)	CMDSEC	CSLOI DFSCG or DFSDF
MCS or E-MCS	CMDMCS	DFSPB
DBRC	CMDAUTH	RECON
AOI type 1	AOI1	DFSPB
AOI type 2	AOIS	DFSPB
Dependent region	ISIS	DFSPB

97

Reference chart of “windows”, locks/keys and where you specify the lock/key value.

IMS General Resource Profiles

IMS resource	Resource class singular/grouping	Resource name
Transaction	T*IMS* / G*IMS*	transaction code
Command (type 1)	C*IMS* / D*IMS*	first 3 characters of command
DBRC command	FACILITY	*safhlq*.command_verb.qualifier.modifier
Command (type 2)	OPERCMDS	IMS.*plxname*.command_verb.command_keyword
Program (PSB)	I*IMS* / J*IMS*	program name
Logical terminal	L*IMS* / M*IMS*	logical terminal name (lterm)
CF structure	FACILITY	CQSSTR.*structure_name* or IXLSTR.*structure_name*
IMS Control Region	APPL	*imsid*
IMSPlex (CSL)	FACILITY	CSL.*imsplexname*
XCF group (Client bid)	FACILITY	IMSXCF.groupname.*membername*
Dataset	DATASET	*dataset name*

The portion of a resource class or name that is shown in blue italics on this chart is the part you can change to make a resource unique.

Member class profile names must conform to the rules shown in this chart.

Grouping class profile names can be any 1-8 alphanumeric characters you choose.

Notice that there are 2 kinds of IMS commands: type 1 and type 2. Type 2 commands are newer and can only be entered through the Operations Manager address space.

They are sometimes called plex commands.

Write to me!

Maida Snapper

maidalee@us.ibm.com