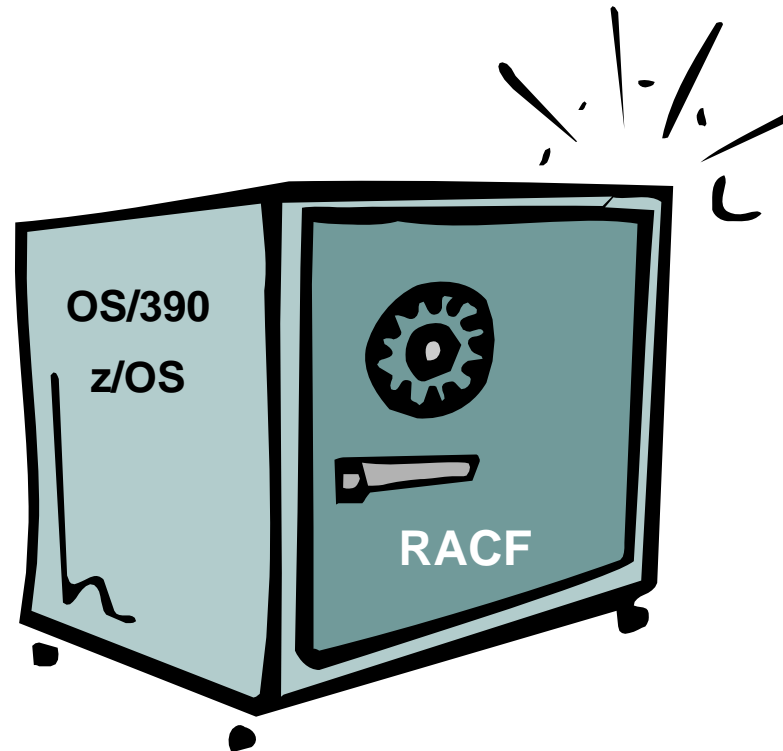


# ***RACF: AUDIT FOR RESULTS***

**ISACA NACACS Conference - Session 413 - April 2007**



**Robert S. Hansel**

**RACF Specialist - RSH Consulting, Inc.**

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

# **TOPICS**

**Concepts**

**Users**

**Groups**

**Resource Protection**

**Dataset Resources**

**General Resources**

**Monitoring**

**Administration**

**Audit Tools**

RACF, OS/390, and z/OS are Trademarks of the International Business Machines Corporation

# ***CONCEPTS***

**Introduction to RACF**

**RACF Functions**

**RACF'S Role & Authority**

**Profiles and Relationships**

**Initial Terms**

# ***INTRODUCTION TO RACF***

**Resource Access Control Facility (RACF)**

**IBM's Security Software Product for MVS, OS/390, & z/OS**

**First introduced in 1976**

**Component of IBM's z/OS Security Server**

**Comprised of:**

- **Software - Programs, Tables, Macros, TSO Commands, Utilities**
- **Database (Primary & Backup Pair)**
  - **SETROPTS Options**
  - **Profiles - Users, Groups, Datasets, General Resources**

# ***RACF FUNCTIONS***

**User Identification and Authentication**

**Resource Access Authorization**

**Monitor User Activity**

**Access Administration**

# RACF'S ROLE & AUTHORITY

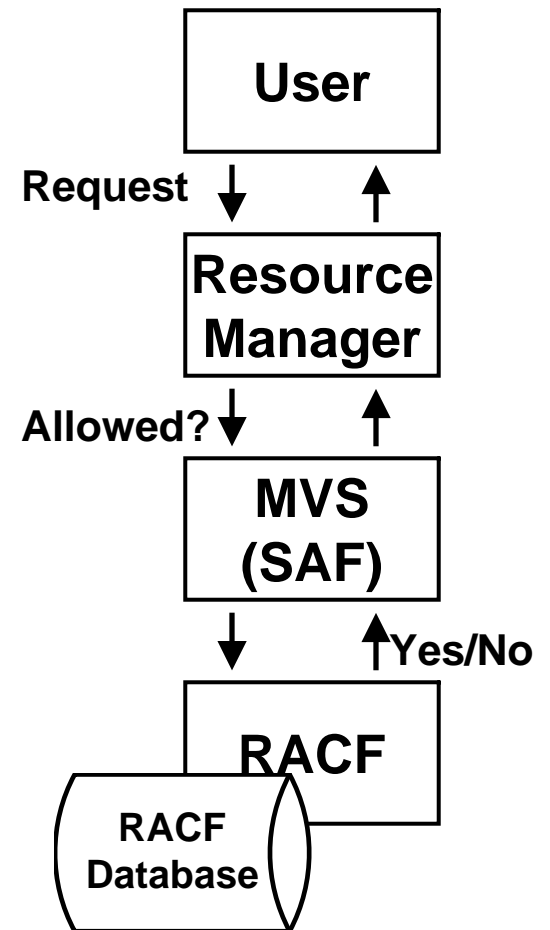
RACF is called by a system resource manager (e.g. CICS) whenever a user tries to logon or attempts to access a resource

RACF determines whether an action is authorized and *advises* the resource manager to allow or disallow the action

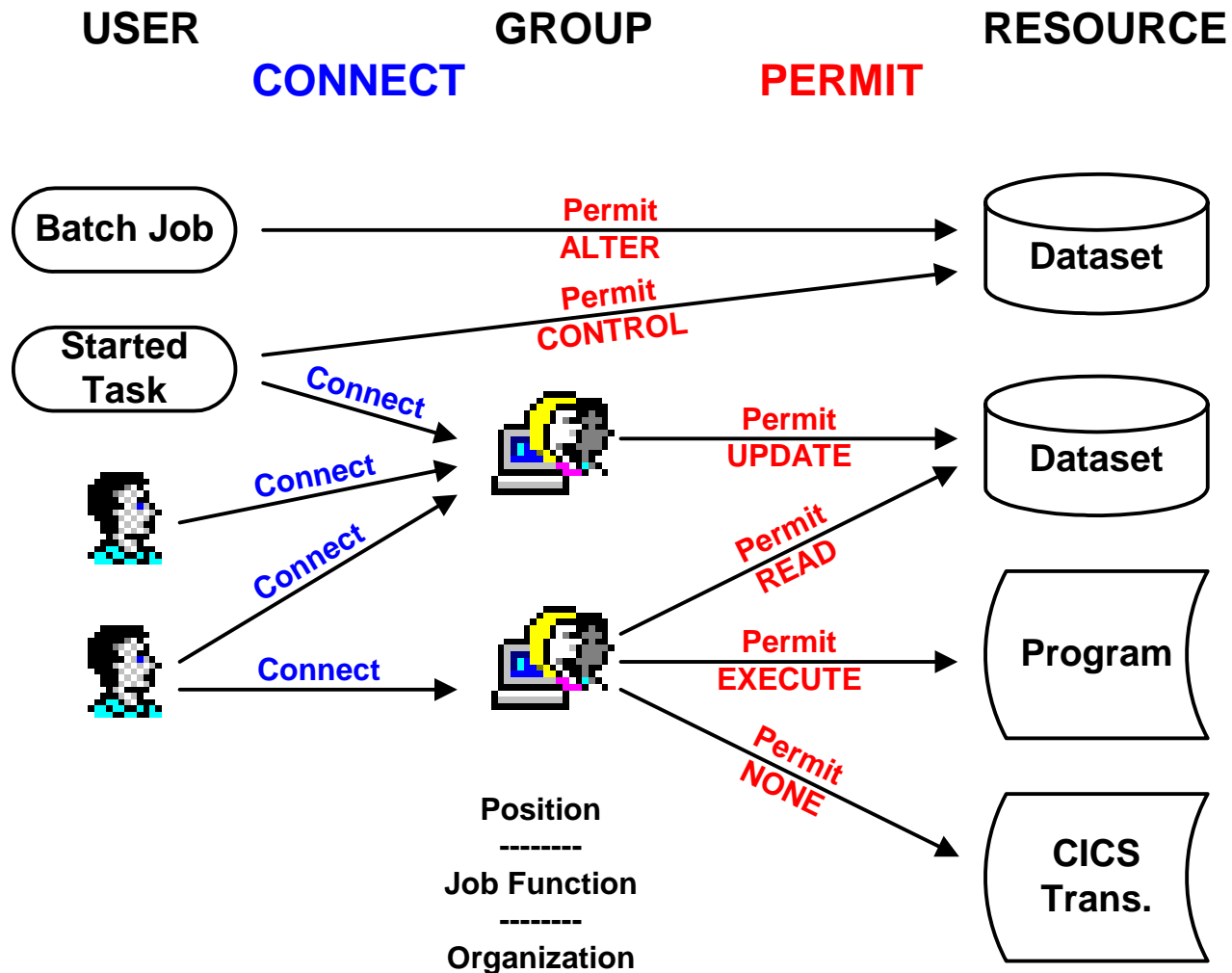
RACF uses the profiles defined in its database to make these determinations

The resource manager *decides* what action to take based on what RACF advises

**Common Audit Finding: Resource managers not configured to call RACF**



# PROFILES & RELATIONSHIPS



# ***INITIAL TERMS***

**RACF Commands** - TSO commands (i.e., programs) for administering RACF

**SETROPTS** - Set RACF Options - TSO command for setting & viewing RACF base options

**DSMON** - Data Security Monitor Utility - Generates various control status reports

**General Resource** - Any resource other than a dataset (e.g., terminals, CICS transactions, Operator Commands)

**General Resource Class** - RACF identifier for a specific General Resource type (e.g., TERMINAL, TCICSTRN, OPERCMDS)

# ***USERS***

**User Terms**

**RACF Identification and Authentication**

**USERID & Password**

**User Profile**

**Batch Jobs**

**Started Tasks**

# ***USER TERMS***

**User** - person or process accessing the system

**USERID** - identifier for a user - up to 8 characters in length

**Revoke/Resume** - deactivate/reactivate a USERID

**Password** - secret code for authenticating a user

**User Profile** - RACF database record for a USERID

**User Profile Segments** - profile extensions containing system software product-specific control information (e.g. TSO, OMVS)

**IBMUSER** - initial default ID provided with RACF - used to create initial administrator IDs and then disabled

# ***RACF IDENTIFICATION & AUTHENTICATION***

## **RACF checks at logon:**

- **Valid USERID**
- **USERID Not Revoked**
- **Valid Password**
- **Authorized for Time-of-Day and Day-of-Week**
- **Authorized to Use Terminal (TERMINAL) or JES Input Source (JESINPUT)**
- **Authorized to Logon to APPLID (APPL)**
- **Authorized to Use TSO (ACCTNUM, TSOPROC, TSOAUTH)**
- **Authorized to Submit Jobs from Remote Nodes (NODES)**

**Common Auditing Finding: System entry points not fully controlled**

# USERID

## RACF controls for USERID

- Time-of-Day, Day-of-Week logon limits
- Automatic revoke/resume dates
- Automatic revoke after prolonged inactivity (SETROPTS INACTIVE)
- Record last logon and password change (SETROPTS INITSTATS)
- PROTECTED attribute
  - Prevents use of the USERID as a logon ID
  - Intended for Batch and Started Task IDs

## Common Auditing Findings:

- IDs not revoked for inactivity
- PROTECTED attribute not used
- ID/Passwords are shared

# PASSWORD

One to eight alpha, numeric, and special characters - @ # \$

## RACF SETROPTS PASSWORD Options

- **INTERVAL** Frequency of mandatory periodic change
- **RULE** Minimum length and composition format
- **HISTORY** Prevent reuse of # prior passwords
- **REVOKE** Revoke ID after # attempts with bad password
- **MINCHANGE(#)** Minimum # days before next password change
- **MIXEDCASE** Enable use of mixed case passwords

## PASSPHRASE - 14-100 character text string authenticator

- Must not contain the USERID in uppercase or lowercase
- Must contain at least 2 alphabetic and 2 non-alphabetic characters
- Must not contain more than 2 consecutive identical characters

# PASSWORD

## USERID Password change options - PASSWORD Command

- **INTERVAL** Equal to or less than SETROPTS INTERVAL limit
- **NOINTERVAL** No password change required

## Password encryption

- **One-way encryption** - can change but cannot view
- **Algorithms**
  - IBM proprietary algorithm (RACF Exit - ICHDEX01)
  - DES

## Common Auditing Findings:

- **Password options are too liberal, especially syntax RULEs**
- **No password change required for Sensitive IDs**
- **Weak initial or reset passwords (e.g., common value)**

# USER PROFILE

```
LISTUSER JSMITH1 TSO
USER=JSMITH1  NAME=JOHN SMITH          OWNER=SECGRP1   CREATED=05.067
DEFAULT-GROUP=USRGRPA  PASSDATE=06.130  PASS-INTERVAL= 30
ATTRIBUTES=OPERATIONS
ATTRIBUTES=UAUDIT
REVOKE DATA=NONE      RESUME DATE=NONE
LAST-ACCESS=06.135/11:35:22
CLASS AUTHORIZATION=DASDVOL
INSTALLATION-DATA=SSN234-12-3990  TECHSPT DASD MANAGEMENT
NO-MODEL-NAME
LOGON ALLOWED      (DAYS)              (TIME)
-----
ANYDAY                                ANYTIME
GROUP=USRGRPA      AUTH=USE              CONNECT-OWNER=SECUSR02  CONNECT-DATE=05.067
CONNECTS= 3,234  UACC=NONE              LAST-CONNECT=06.135/11:35:22
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE      RESUME DATE=NONE
GROUP=TECHSPT1    AUTH=CONNECT      CONNECT-OWNER=RJONES2  CONNECT-DATE=05.070
CONNECTS=      00  UACC=READ              LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=OPERATIONS
REVOKE DATE=NONE      RESUME DATE=NONE
GROUP=SYS1        AUTH=CREATE      CONNECT-OWNER=SYS1     CONNECT-DATE=05.144
CONNECTS=      00  UACC=ALTER              LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE      RESUME DATE=NONE
GROUP=DASDMGT     AUTH=USE              CONNECT-OWNER=RJONES2  CONNECT-DATE=06.081
CONNECTS=      00  UACC=NONE              LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=SPECIAL
REVOKE DATE=02.030  RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
TSO INFORMATION
ACCTNUM= JJK001
HOLDCLASS= M
...
```

Groups listed in the order the user was connected to them

# **BATCH JOBS**

## **Batch job user identification**

- **USERID, Password, and Group Coded on JOB Card**
- **USERID propagation from logged on users**

## **Batch job control General Resource classes**

- **PROPCNTL**    **Prevent propagation**
- **SURROGAT**   **Allow users to submit jobs with other USERIDs**
- **NODES**        **Control NJE job submission and propagation**

## **Mandatory logon control - SETROPTS options**

- **Batch jobs without USERIDs may run as undefined users**
- **JES(BATCHALLRACF)**
- **JES(XBMALLRACF)**

# BATCH JOBS

## Surrogate USERID

- Allows a user to submit a batch job with another user's USERID without the password
- Primarily Intended for Started Tasks (e.g., Job Scheduler)
- SURROGAT Class
- Profile - *submitted-userid.SUBMIT* (e.g., RSH001.SUBMIT )
  - READ - Permits use of USERID
  - LOGOPTIONS(ALWAYS) recommended for all SURROGAT Class

## Common Auditing Findings:

- Mandatory batch logon not required
- Inappropriate SURROGAT authority
  - Profile such as \*\* or \*.SUBMIT cover large numbers of IDs
  - Users permitted to submit jobs with powerful IDs
  - Use of authority not adequately logged

# ***STARTED TASKS***

**System “Job” initiated by MVS 'START' Command**

**USERID obtained from either:**

- **STARTED Class profiles**
- **Started Task Table (ICHRIN03)**

**Profile/Table entries contain**

- **Procedure Name**
- **USERID**
- **RACF Group**
- **PRIVILEGED or TRUSTED authority**

**PRIVILEGED and TRUSTED grant unrestricted access to all resources & USS Superuser (uid 0); TRUSTED can be logged**

# STARTED TASKS

## Common Audit Findings:

- Started Tasks not uniquely identified for individual control - USERIDs shared by multiple Started Tasks
- Excessive assignment of PRIVILEGED or TRUSTED authority
- STARTED Class / Started Task Table entries, especially the default entry, do not associate Started Task IDs with a specific logon group

PROCEDURE NAME	ASSOCIATED USER	ASSOCIATED GROUP	PRIVILEGED	TRUSTED
-----	-----	-----	-----	-----
*	=		NO	NO

# ***GROUPS***

**Group Concept**

**Group Hierarchy**

**Group Functions**

**Group Profile**

# ***GROUP CONCEPT***

**A Group is a collection of users with similar access needs and common attributes**

**Groups simplify RACF administration; it is easier to manage 100 groups than 10,000 individual users**

**Users are "*connected*" (i.e., joined) to groups**

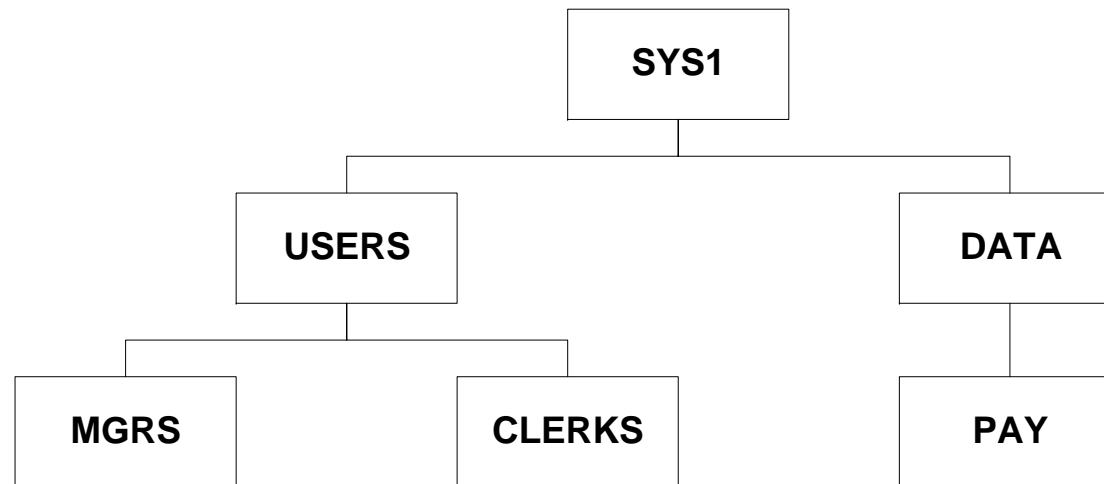
**A user can be connected to multiple groups**

**Every user must be connected to at least one group; this group is the user's default group**

**USERIDs are automatically removed from all groups upon deletion**

# **GROUP HIERARCHY**

**Groups are organized in a hierarchy with SYS1 at the top**



**Every group except SYS1 has a SUPGROUP (Superior Group)**

**RACF comes with 3 groups -- SYS1 VSAMDSET SYSCTLG**

**Group hierarchy does not affect access authority or the scope of group administrative authority (Profile Ownership determines administrative authority)**

# ***GROUP FUNCTIONS***

**Groups are the primary tool for organizing the RACF database**

**Groups can serve different purposes**

- **Organizational Groups**
- **User Holding Groups**
- **Access Authorizing Groups**
- **Dataset Holding Groups (HLQ)**
- **Resource Owning Groups**
- **Special/Administrative Groups**

**Naming conventions are often devised to distinguish between groups serving different purposes and the organizations responsible for them**

# GROUP PROFILE

```
LISTGRP DASDMGT OMVS
INFORMATION FOR GROUP DASDMGT
SUPERIOR GROUP=TECHSPT1          OWNER=RJONES2
INSTALLATION DATA=DASD MANAGEMENT SECTION
NO MODEL DATA SET
TERMUACC
SUBGROUP(S) = DASDTEST
USER(S) = ACCESS= ACCESS COUNT= UNIVERSAL ACCESS=
RJONES2 CREATE 000000 READ
CONNECT ATTRIBUTES=SPECIAL
REVOKE DATE=NONE
JSMITH1 USE 000000 NONE
CONNECT ATTRIBUTES=SPECIAL
REVOKE DATE=06.160 RESUME DATE=NONE
SREST03 CONNECT 000000 NONE
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE RESUME DATE=NONE
RHOMES1 USE 000000 NONE
CONNECT ATTRIBUTES=REVOKED
REVOKE DATE=NONE RESUME DATE=NONE
HWILLS2 USE 000000 NONE
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE RESUME DATE=NONE
JWINDS4 JOIN 000000 NONE
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE RESUME DATE=NONE
OMVS INFORMATION
GID = 0000000339
```

Users are listed in the order by which they were connected to the group

# GROUPS

## Common Audit Findings:

- **Group architecture and naming standards are not defined or adhered to**
- **Group architecture is disorganized**
- **Groups used for multiple purposes (e.g., grant access and own data)**
- **Different types of users (e.g., batch, started task, users) mixed together in same groups, especially those granting access**
- **Role-based groups not established**
- **Users connected to an excessive number of groups (> 10)**

# ***RESOURCE PROTECTION***

**Resource Protection Concepts**

**Resource Profiles**

**Generic Profiles**

**Access Permissions**

**Access Permissions For Groups**

**Conditional Access**

**OPERATIONS Authority**

**Mode**

**Global Access Table**

**Access Authorization Decision Logic**

# ***RESOURCE PROTECTION CONCEPTS***

**RACF determines whether a user is authorized to access a resource at the requested level of access (e.g., READ)**

**RACF makes this determination based on resource profiles defined in its database**

**Resource profiles specify:**

- **The logical name of the resource (e.g., the DSNAME)**
- **The type of resource or 'Class' (e.g., PROGRAM)**
- **How the resource is to be protected**

**RACF sends a Return Code (RC) back to the calling Resource Manager indicating the results of the authorization check**

- 0      Authorized**
- 4      Not-Protected**
- 8      Not-Authorized**

# ***RESOURCE PROFILES***

**RACF uses the name and class of the resource to locate the profile in its database**

## **Resource profile categories**

- **Dataset**
- **General resource (e.g., PROGRAM)**

## **Resource profiles contain**

- **Identifying information**
- **Control options**
- **Auditing specifications**
- **Access permissions**

# RESOURCE PROFILES

## Resource profile types

- Discrete - Full name match
- Generic - Partial name masking
- Grouping - Set of dissimilar full and masked names

**RACF uses the most specific profile (i.e., closest match) for determining access authorization**

- Discrete
- Generic with most match characters, from left to right

PAY.PROD.MASTER.EMPLOYEE

PAY.PROD.MASTER.\*

PAY.PROD.\*.EMPLOYEE

PAY.PROD.\*\*

PAY.\*\*

← PAY.PROD.MASTER.BKUP

← PAY.PROD.CHECKS.TAPE

# GENERIC PROFILES

Offer one-to-many relationship of profile to resource protected

Generally use masking characters to match multiple resources

Masking characters - in order of precedence

- % Single substitute character
- \* Any set of substitute characters
- \*\* Any set of substitute characters, multiple qualifiers

For Datasets, use of \*\* requires *Enhanced Generic Naming* option be activated

Use and behavior of the characters differs based on whether the profile is a Dataset or General Resource

# ACCESS PERMISSIONS

**Access permissions are specified in three ways**

- **Standard Access List**
- **Conditional Access List**
- **Universal Access (UACC) - default access granted to any user**

**Access can be permitted to**

- **USERID**
- **Group**
- **ID(\*)** - Grants access to all *RACF-Defined users*

**Each permission specifies an Access Level**

**RESTRICTED attribute - prevents access via UACC, ID(\*), and Global Access Table (intended for USS-default & external IDs)**

# ***ACCESS PERMISSIONS***

## **Access levels**

- **ALTER**
- **CONTROL**
- **UPDATE**
- **READ**
- **EXECUTE**
- **NONE**

**The meaning of an access level differs by the class of resource protected**

**Access level authorities are cumulative - each grants the combined authority of lower levels**

# CONDITIONAL ACCESS

Grants user access only when the condition is met

## Types of conditional access

- WHEN(JESINPUT(*device*))
- WHEN(PROGRAM(*program*))
- WHEN(TERMINAL(*terminal-id*))
- WHEN(SYSID(*smf-id*))
- WHEN(APPSPORT(*partner-lu-name*))
- WHEN(CONSOLE(*console-id*))

Most commonly used to grant access to JESSPOOL and OPERCMDS profiles WHEN(CONSOLE(SDSF))

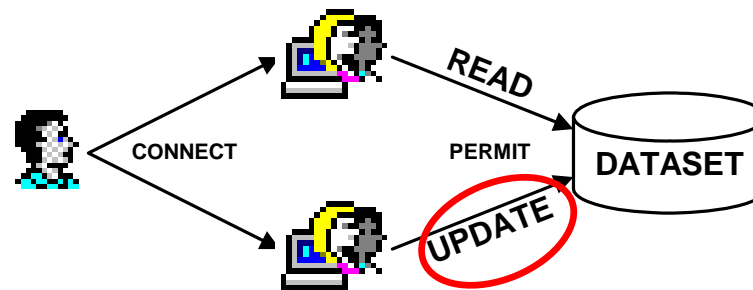
# ACCESS PERMISSIONS FOR GROUPS

Users who are connected to a Group are granted all the access the Group has been permitted (assuming the user's connection to the group is not revoked)

**SETROPTS option - List-of-Groups - Determines which of a user's connected groups are checked for access authorization**

- **NOGRPLIST** inactive - check only the user's current logon group
- **GRPLIST** active - include all the user's connected groups

If **GRPLIST** is active, RACF grants access based on the highest level of access allowed by any of the user's connected groups



# **ACCESS PERMISSIONS FOR GROUPS**

**Being connected to a Group with associated datasets (Group=HLQ, e.g. PAY) does not automatically grant access to those datasets**

**Being connected to a Group with subordinate groups does not grant a user any authority of the other groups - no cascading or inheritance of access authority**

## **Access administration considerations**

- **Profile access lists are not automatically updated when a USERID or Group is deleted**
- **Group connects are automatically removed when a USERID is deleted**
- **Best Practice - use Groups exclusively in granting end-user access**

# ***OPERATIONS AUTHORITY***

**User and Group-connect attribute**

**Grants ALTER level access to resources whose classes have been defined with OPER=YES in the Class Descriptor Table**

DATASET	DASDVOL/GDASDVOL	PSFMPL
TAPEVOL	VM Resources	RODMMGR
NETCMDS	NETSPAN	

**Grants access when user has not been permitted access**

**Can be restricted by specifically granting OPERATIONS user a lower level of access**

# ***MODE***

**MODE is a resource profile control option**

## **Mode options**

- **FAIL (default)**
- **WARN**

## **WARN Mode**

- **Predominantly used for testing new access permissions**
- **Intended to be temporary**
- **Resources are not protected**
- **Access violations are logged, but not prevented**
- **Warning message issued, except when creating a dataset**
- **Ignored for certain classes (PROGRAM, NODES)**

# ***GLOBAL ACCESS TABLE***

## **Performance enhancement tool**

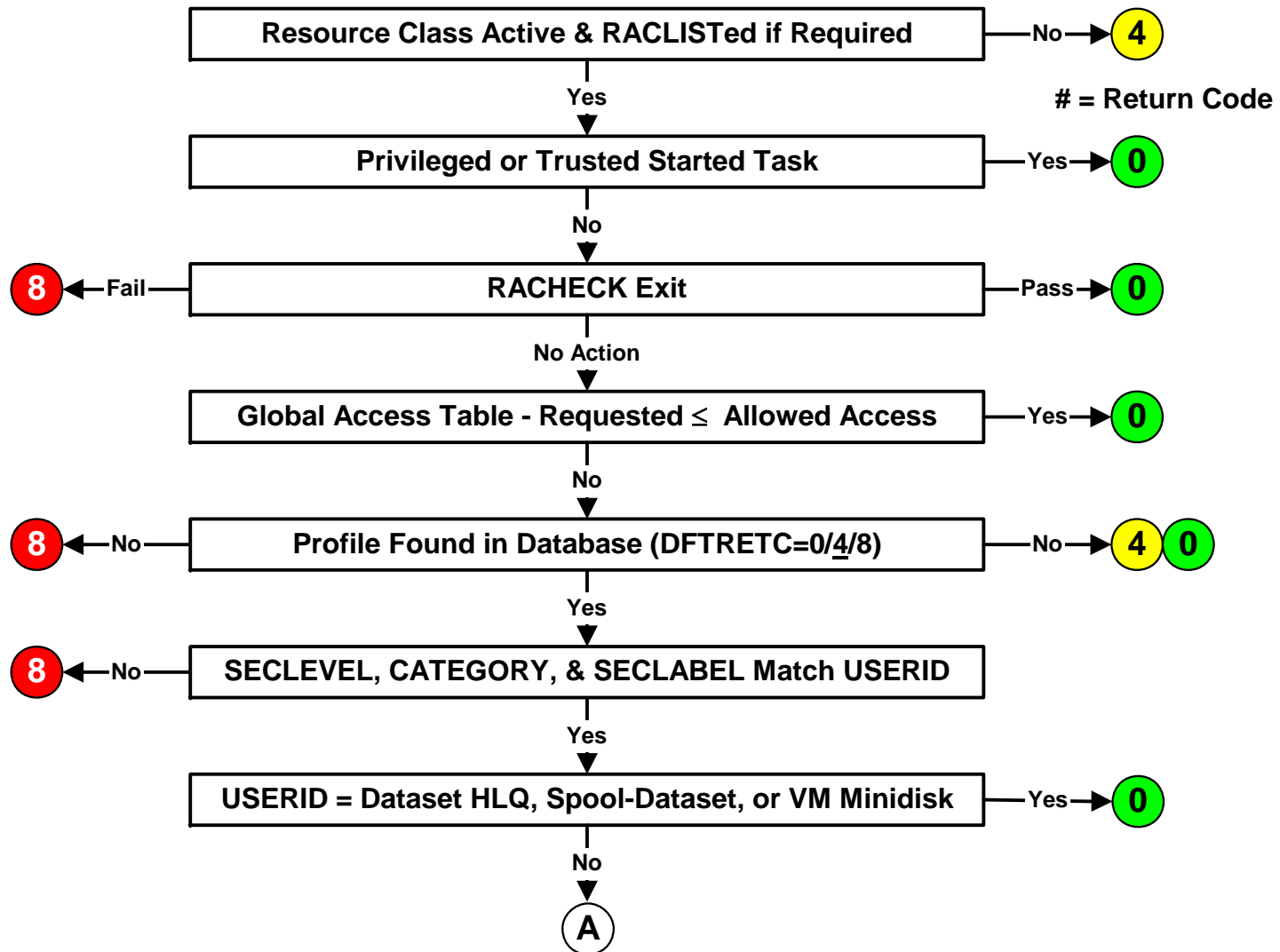
- **Grants immediate access without referring to the profile and without logging to improve performance**
- **Used to grant access to common shared resources**

## **GLOBAL Class - profiles are class names**

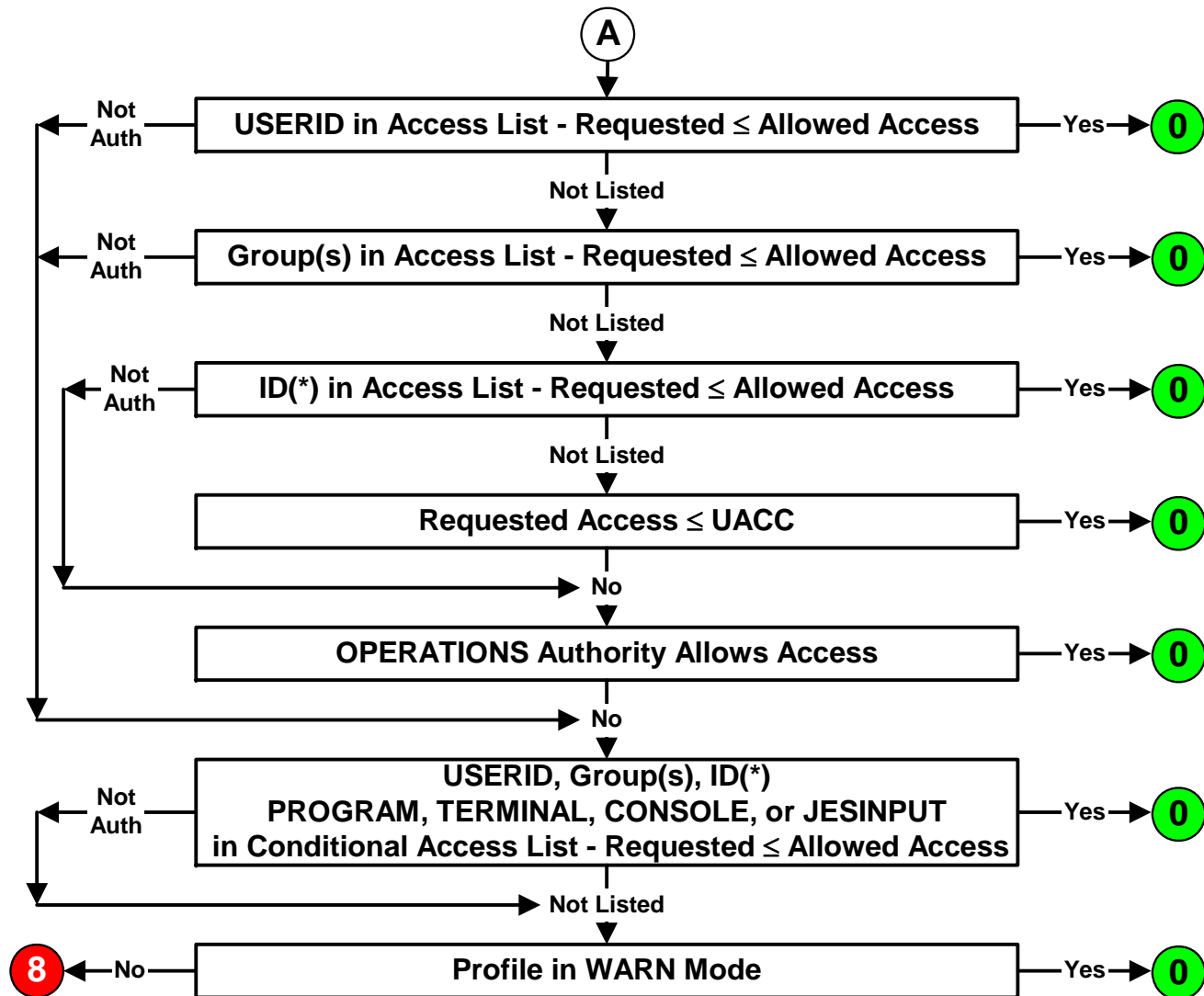
## **Sample DATASET profile entries (DSMON Report)**

<b>&amp;RACUID.**</b>	<b>ALTER</b>
<b>SYS1.BROADCAST</b>	<b>READ</b>
<b>CATALOG.MASTER</b>	<b>READ</b>
<b>CATALOG.USER</b>	<b>UPDATE</b>
<b>ISPF.LIBRARY</b>	<b>READ</b>
<b>SYS1.HELP</b>	<b>READ</b>

# ACCESS AUTHORIZATION DECISION LOGIC



# ACCESS AUTHORIZATION DECISION LOGIC



# RESOURCE PROTECTION

## Common Audit Findings:

- **UACCs set too high allowing inappropriate access**
  - **READ/UPDATE or above for datasets**
  - **READ or above for general resources**
  - **RESTRICTED attribute not set on external & Webserver default IDs**
- **Inappropriate access granted**
- **Access granted ID(\*) circumvents UACC(NONE) policy**
- **OPERATIONS attribute assigned extensively and used excessively**
- **WARN mode left on profiles for excessive length of time (and not monitored) or applied to high-power functions**
- **Global Access Table entry allows access prohibited by the resource profile**

<b>GAT Entry</b>	<b>SYS1.**</b>	<b>READ</b>
<b>Profile</b>	<b>SYS1.RACF.**</b>	<b>NONE</b>

# ***DATASET RESOURCE PROTECTION***

**Dataset Protection**

**Access Levels**

**Dataset Profiles**

**Protect-All**

**Storage Administration**

# ***DATASET PROTECTION***

**RACF protection is provide by Dataset Profiles**

## **Dataset Profile name**

- **Incorporates the name(s) of the dataset(s) it protects**
  - **Dataset**      **PAY.PROD.MASTER**
  - **Profile**      **PAY.PROD.\*\***
- **The HLQ must match an existing RACF identifier**
  - **Group**      **PAY**      **Group Datasets**
  - **USERID**      **USR11**      **User Datasets**

## **Dataset profile types**

- **Discrete**
- **Generic**

**Tape dataset protection - SETROPTS TAPEDSN**

# ***DATASET ACCESS LEVELS***

<b>ALTER</b>	Allows anything, to include creating, scratching (i.e., deleting), cataloging, uncataloging
<b>CONTROL</b>	For VSAM datasets, is comparable to the Control Password allowing use of improved control-interval processing (For non-VSAM datasets, is treated the same as UPDATE)
<b>UPDATE</b>	Allows writing and reading, but not creating and scratching
<b>READ</b>	Allows reading, to include copying
<b>EXECUTE</b>	Allows the execution of programs from a specified library, but will not allow reading, copying, or dumping of the programs
<b>NONE</b>	Denies all access

# DATASET PROFILE

LISTDS D DATASET('SYS1.LIBS\*') ALL  
INFORMATION FOR DATASET SYS1.LIBS\* (G)

<u>LEVEL</u>	<u>OWNER</u>	<u>UNIVERSAL ACCESS</u>	<u>WARNING</u>	<u>ERASE</u>
00	TECHSPT1	READ	NO	NO

AUDITING

-----

FAILURES(UPDATE)

NOTIFY

-----

NO USER TO BE NOTIFIED

<u>YOUR ACCESS</u>	<u>CREATION GROUP</u>	<u>DATASET TYPE</u>
READ	TECHSPT1	NON-VSAM

GLOBALAUDIT

-----

NONE

INSTALLATION DATA

-----

MVS LIBRARIES

SECURITY LEVEL

-----

NO SECURITY LEVEL

# DATASET PROFILE

## CATEGORIES

NO CATEGORIES

## SECLABEL

NO SECLABEL

CREATION DATE (DAY) (YEAR)	LAST REFERENCE DATE (DAY) (YEAR)	LAST CHANGE DATE (DAY) (YEAR)
270 02	NOT APPLICABLE FOR GENERIC PROFILE	

ALTER COUNT	CONTROL COUNT	UPDATE COUNT	READ COUNT
NOT APPLICABLE FOR GENERIC PROFILE			

ID	ACCESS
RJONES2	ALTER
TECHSPT1	UPDATE
DASDMGT	ALTER
JWILLS2	NONE

ID	ACCESS	CLASS	ENTITY NAME
APPPGMR	UPDATE	PROGRAM	PVAL01
APPPGMR	UPDATE	PROGRAM	PVAL04

# ***PROTECTALL***

## **SETROPTS Option**

**Requires datasets to be 'defined' to RACF; otherwise, access is denied**

**Only applies to datasets**

## **Implementation options**

- **WARN**
- **FAIL**

**Users with SPECIAL can access undefined data**

# **STORAGE ADMINISTRATION**

**Storage Admin involves managing data - archiving, relocating, compressing, backups/restores - but not accessing the data**

## **Storage Admin authorities**

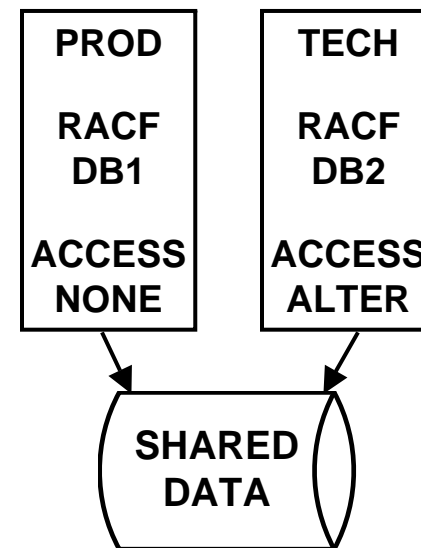
- **OPERATIONS authority - allows data access**
- **DASDVOL class - manage data on non-SMS-managed volumes**
- **FACILITY class STGADMIN profiles - manage all data & catalogs**
- **Catalog ALTER access - manage all catalog entries**

**Must be very strictly controlled**

# DATASET PROTECTION

## Common Audit Findings:

- Profiles do not comprehensively protect all data - HLQ.\*.\*\*
- TAPEDSN is inactive
- PROTECTALL is inactive
- Storage administration authorities either not used, not fully defined, or grant excessive authority
- Unnecessary or inappropriate access granted to system datasets (DSMON report)
  - MVS libraries and datasets
  - APF libraries
  - Linklist libraries
  - RACF datasets
  - Catalogs
- Inconsistent access controls protecting resources shared by multiple OS/390-z/OS images having separate RACF databases



# ***GENERAL RESOURCE PROTECTION***

**General Resources**

**General Resource Protection**

**General Resource Profile**

# GENERAL RESOURCES

**A General Resource is anything other than a dataset**

- Identified by their logical names (e.g., Program ICKDSF) within a specific class (e.g., PROGRAM)
- Format of the resource name is determined by the resource manager (e.g., ISFCMD.DSP.STATUS.JES2 for SDSF)

<u>RESOURCE-TYPE</u>	<u>CLASS / GROUPING-CLASS</u>	<u>RESOURCE-NAME</u>
Program	PROGRAM / PMBR	AMASPZAP
TSO Authority	TSOAUTH	OPER
DASD Volumes	DASDVOL / GDASDVOL	SYS001
CICS APPLID	APPL	CICSPRD1
Storage Admin	FACILITY	STGADMIN.ADR.DEFRAG
JES2 RJE Reader	JESINPUT	RMT0002.RD1
MVS Command	OPERCMDS	MVS.HALT.NET
CICS Transaction	TCICSTRN / GCICSTRN	CEMT

# **GENERAL RESOURCE PROTECTION**

Protection is provided by **General Resource Profiles**

**General Resource Profile names incorporate the class and name of the resource**

- **DASD Volume**                      **TSO003**
- **Class & Profile**                      **DASDVOL TSO\***

**General Resource classes are defined in two tables**

- **RACF Class Descriptor Table (CDT) or CDT Class Profiles (z1.6)**
- **RACF Router Table (RRT)**    [not required if using CDT profiles]

**Classes must be activated by SETROPTS Options**

- **ACTIVE(class)**
- **GENCMD(class)** - enables creation of generic profiles
- **GENERIC(class)** - activates generic profiles

# GENERAL RESOURCE PROTECTION

## General Resource Class types

- Member TCICSTRN
- Grouping (optional) GCICSTRN

## General Resource Profile types

- Discrete TCICSTRN CEMT
- Generic TCICSTRN C\*
- Grouping (members) GCICSTRN CICSCMD1 ADDMEM(CEDF)

## RACFVARS - Prefixed with an '&' (e.g., &RACLNDE )

- Variable text strings used in Generic profiles
- Ex: JES2.LOCAL.&PAYPRTR, where &PAYPRTR = PRT05 & PRT44

**Grouping Profiles allow dissimilar named resources (members) to be protected under a single profile (e.g., PAY1, RPAY, PY88)**

# ***GENERAL RESOURCE PROTECTION***

## **Access levels**

- ALTER
- CONTROL
- UPDATE
- READ (often equates to USE)
- EXECUTE
- NONE

**The meanings of the levels varies depending on the class of resources being protected.**

**OPERATIONS *may* grant ALTER access - CDT OPER parameter**

# GENERAL RESOURCE PROFILE

RLIST TCICSTRN CEMT ALL

CLASS NAME

-----

TCICSTRN CEMT

GROUP CLASS NAME

-----

GCICSTRN

RESOURCE GROUPS

-----

NONE

LEVEL	OWNER	UNIVERSAL ACCESS	YOUR ACCESS	WARNING
-------	-------	------------------	-------------	---------

-----	-----	-----	-----	-----
-------	-------	-------	-------	-------

00	CICSSPT	NONE	NONE	YES
----	---------	------	------	-----

INSTALLATION DATA

-----

NONE

APPLICATION DATA

-----

NONE

SECLEVEL

-----

NO SECLEVEL

CATEGORIES

-----

NO CATEGORIES

# GENERAL RESOURCE PROFILE

SECLABEL

-----  
NO SECLABEL

AUDITING

-----  
SUCCESSES (UPDATE) , FAILURES (READ)

NOTIFY

-----  
NO USER TO BE NOTIFIED

CREATION DATE (DAY) (YEAR)	LAST REFERENCE DATE (DAY) (YEAR)	LAST CHANGE DATE (DAY) (YEAR)
270 92	282 92	282 92

ALTER COUNT	CONTROL COUNT	UPDATE COUNT	READ COUNT
000000	000000	000000	000000

USER	ACCESS	ACCESS COUNT
RJONES2	ALTER	
CICSSPT	UPDATE	
DASDMGT	READ	
JWILLS2	NONE	

ID	ACCESS	ACCESS COUNT	CLASS	ENTITY NAME
NO ENTRIES IN CONDITIONAL ACCESS LIST				

# GENERAL RESOURCES

## Common Audit Findings:

- RACF resource classes are inactive
- RACF profiles do not comprehensively protect all resources - no catch-all \*\* profile (exclude FACILITY & PROPCNTL Classes)
- Resources are defined in multiple grouping profiles with conflicting protection
- No clear design, structure, or naming convention for grouping profiles

# ***MONITORING***

**Auditing**

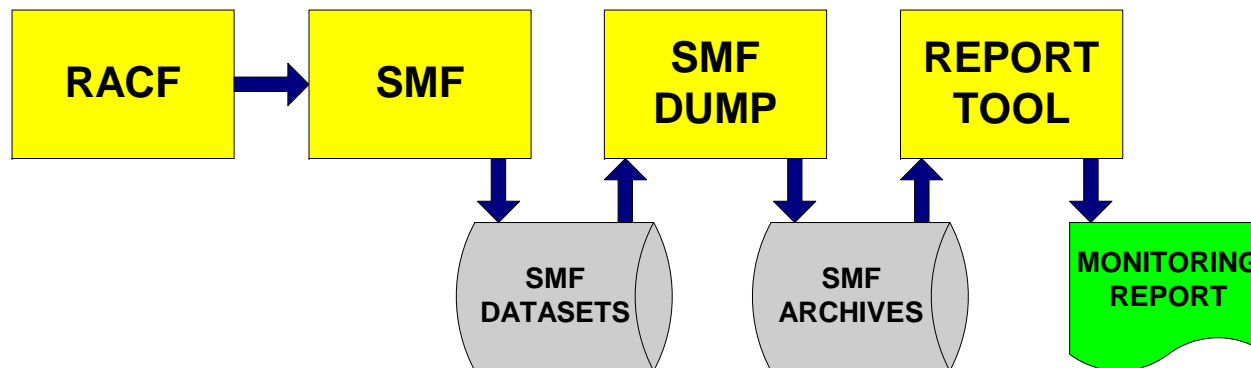
**Reporting Tools**

# AUDIT REPORT PROCESS

Reporting tools require comprehensive SMF data collection and retention to be effective

## Log collection & reporting process

- Resource Manager calls RACF for authorization check
- RACF Caller requires or does not suppress logging
- RACF Options Generate SMF Log Record
- SMF Collects and Saves Log Record
- SMF Record is Dumped for Report Processing
- RACF Tools Generate Reports from SMF Record



# AUDITING

## RACF auditing generates SMF records

- 20 Job Initiation
- 30 Common Address Space Work (Job Initiation & Termination)
- 80 RACF Processing - Logged Events
- 81 RACF Initialization - IPL
- 83 RACF Audit Record for Data Sets (MLS)

## User auditing

- Logons - automatically logged (by IBM products)
- User UAUDIT attribute

## Resource auditing

- **AUDIT(FAILURE(*access-level*),SUCCESS(*access-level*),ALL,NONE)**
- Default - FAILURE(READ)

# AUDITING

## SETROPTS Options

- SAUDIT - SPECIAL authority use
- OPERAUDIT - OPERATIONS authority use
- CMDVIOL - Command Violations
- AUDIT(*class*) - Profile changes
- LOGOPTIONS(*type(class)*) - DEFAULT(*all classes*) is default
  - Supersedes logging specified in profiles
  - Levels
    - ◆ Default
    - ◆ Failures (recommended for most classes)
    - ◆ Successes
    - ◆ Never
    - ◆ Always
  - Enables logging of TRUSTED Started Tasks
  - Enables logging of certain OMVS events  
FSSEC PROCESS PROCACT IPCOBJ

# **REPORTING TOOLS**

**RACF Report Writer**

**RACFRW**

**RACF SMF Unload**

**IRRADU00 & IRRADU86**

**DFSORT Utility Reports**

**ICETOOLS**

**Vendor Products**

**IBM (Consul) - zAudit**

**Vanguard Integrity Prof. - Advisor**

**Allen Systems Group - ASG-Audit**

**Software Eng. of Amer. - RA7**

# MONITORING

## Common Audit Findings:

- **Profile AUDIT options are not set to capture important events**
  - Resource profile AUDIT options do not record violations - FAILURES(READ)
  - Critical resource profile AUDIT options do not monitor access - SUCCESS(level)
  - Sensitive user profiles do not have UAUDIT attribute
- **SETROPTS monitoring options are not active**
  - OPERAUDIT not active
  - AUDIT(class) not set for all classes
  - LOGOPTIONS(FAILURES(class)) not set
- **Reporting tools not used effectively**
  - Incomplete SMF input data selected
  - Record selection criteria is not comprehensive
  - Reports on important types of activities not generated
  - Reports not organized for efficient review

# ***ADMINISTRATION***

**System and Group Attributes**

**Group Connect Authorities**

**Other Authorities**

# ***SYSTEM AND GROUP ATTRIBUTES***

## **Attributes**

- **SPECIAL** - Administer all profiles
- **AUDITOR** - Activate auditing options
- **OPERATIONS** - Access resources

## **Assignment of attributes and scope of authority**

- **USERID** - System
- **CONNECT** - Group - Limited to Scope-of-Groups

## **Scope-of-Groups**

- Includes profiles owned by the group or any of its subgroups
- Based on profile *ownership*, not group structure

# ***GROUP AUTHORITIES***

<b>USE</b>	<b>Use access granted to Group</b>
<b>CREATE</b>	<b>Create Group dataset profiles Create Group datasets</b>
<b>CONNECT</b>	<b>Connect/Remove users for Group Assign up to same authority</b>
<b>JOIN</b>	<b>Create users (with CLAUTH USER) Assign users up to same authority Create and delete subgroups</b>

**Authorities are cumulative**

**Scope-of-Groups does not extend authority**

# ***OTHER AUTHORITIES***

<b>Profile Owner</b>	<b>List, change, delete profile</b>
<b>Class Authorization - CLAUTH(class)</b>	<b>Create general resource class profiles without System-SPECIAL</b>
<b>FIELD Class profiles</b>	<b>List or update profile segment fields</b>
<b>ALTER Access in Discrete</b>	<b>List, change, delete profile</b>
<b>FACILITY Class profiles</b> - IRR.LISTUSER - IRR.PASSWORD.RESET	<b>List all USERIDs</b> <b>Change passwords for all non-admin users</b>
<b>Any User</b>	<b>Change own User profile Name, Default Group, Password, Password Interval</b> <b>List own User profile</b> <b>Create, change, delete own user dataset profiles</b>

# ADMINISTRATION

## Common Audit Findings:

- **Inappropriate assignment of User and Group authorities**
  - **Group CREATE, CONNECT, and JOIN authorities**
  - **Users own profiles (other than for their own TSO datasets)**
  - **AUDITOR attribute given to staff other than Audit or Security**
  - **CLAUTH(class) authority**
  - **FACILITY Class IRR.PASSWORD.RESET**
- **ALTER granted in Discrete profiles when not required for access**
- **IBMUSER not revoked and still in use**
- **Access lists contain entries for deleted USERIDs and Group**
- **RACF Database not backed up properly or checked regularly - requires IRRUT200 utility**
- **No formal OS/390-RACF security policy or standards exist**

# **AUDIT TOOLS**

**RACF USERID**

**AUDITOR attribute & TSO**

**RACF Options**

**SETROPTS LIST**

**DSMON**

**ICHDSM00**

**Database Unload Utility**

**IRRDBU00**

**Remove ID Utility**

**IRRRID00**

**Cross-Reference Utility**

**IRRUT100 (not useful)**

**Audit Plan**

**RACF Auditor's Guide**

# SETROPTS LIST

## SETROPTS LIST

```
ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) TERMINAL(READ) SAUDIT CMDVIOL OPERAUDIT
STATISTICS = DATASET TERMINAL
AUDIT CLASSES = DATASET USER GROUP DASDVOL GDASDVOL TERMINAL GTERMINL
ACTIVE CLASSES = DATASET USER GROUP DASDVOL GDASDVOL TERMINAL GTERMINL APPL
                  TCICSTRN GCICSTRN GLOBAL GMBR DSNR FACILITY SCDMBR SECDATA
                  FCICSFCT HCICSFCT JCICSJCT KCICSJCT DCICSDCT ECICSDCT SCICSTST
                  UCICSTST MCICSPPT NCICSPPT ACICSPCT BCICSPCT PMBR PROGRAM FIELD
                  TSOAUTH TSOPROC ACCTNUM PERFGRP $LMRKTMR T@TESTRN G@TESTRN
GENERIC PROFILE CLASSES = DATASET DASDVOL TERMINAL TCICSTRN FACILITY PROGRAM
GENERIC COMMAND CLASSES = DATASET DASDVOL TCICSTRN FACILITY PROGRAM FIELD
                          TSOAUTH TSOPROC ACCTNUM PERFGRP T@TESTRN
GENLIST CLASSES = NONE
GLOBAL CHECKING CLASSES = DATASET DASDVOL FACILITY
SETR RACLIST CLASSES = APPL DSNR FIELD TSOAUTH TSOPROC ACCTNUM PERFGRP
GLOBAL=YES RACLIST ONLY = TCICSTRN
LOGOPTIONS "ALWAYS" CLASSES = NONE
LOGOPTIONS "NEVER" CLASSES = NONE
LOGOPTIONS "SUCCESSES" CLASSES = NONE
LOGOPTIONS "FAILURES" CLASSES = NONE
LOGOPTIONS "DEFAULT" CLASSES = DATASET RVARSMBR RACFVARS DASDVOL GDASDVOL
                                ... G@TESTRN RMD$FORM
AUTOMATIC DATASET PROTECTION IS IN EFFECT
ENHANCED GENERIC NAMING IS IN EFFECT
REAL DATA SET NAMES OPTIONS IS INACTIVE
JES-BATCHALLRACF OPTION IS INACTIVE
JES-XBMALLRACF OPTION IS INACTIVE
JES-EARLYVERIFY OPTION IS INACTIVE
PROTECT-ALL OPTION IS NOT IN EFFECT
TAPE DATA SET PROTECTION IS INACTIVE
SECURITY RETENTION PERIOD IN EFFECT IS 9999 DAYS.
ERASE-ON-SCRATCH IS INACTIVE
SINGLE LEVEL NAME PREFIX IS LVL1X
LIST OF GROUPS ACCESS CHECKING IS ACTIVE.
INACTIVE USERIDS ARE NOT BEING AUTOMATICALLY REVOKED.
NO DATA SET MODELLING IS BEING DONE.
```

# SETROPTS LIST

## PASSWORD PROCESSING OPTIONS

PASSWORD CHANGE INTERVAL IS 45 DAYS.  
PASSWORD MINIMUM CHANGE INTERVAL IS 3  
MIXED CASE PASSWORDS IS NOT IN EFFECT  
10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.  
AFTER 4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,  
A USERID WILL BE REVOKED.

PASSWORD EXPIRATION WARNING LEVEL IS 5 DAYS.

INSTALLATION PASSWORD SYNTAX RULES:

RULE 1 LENGTH(5:8) \*\*\*\*\*  
RULE 2 LENGTH(6:8) LLLLLLLL

LEGEND:

A-ALPHA C-CONSONANT L-ALPHANUMERIC N-NUMERIC V-VOWEL W-NOVOWEL \*-ANYTHING  
c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL \$-NATIONAL

INSTALLATION DEFINED RVARV PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.

DEFAULT RVARV PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.

SECLEVELAUDIT IS INACTIVE

SECLABEL AUDIT IS NOT IN EFFECT

SECLABEL CONTROL IS NOT IN EFFECT

GENERIC OWNER ONLY IS NOT IN EFFECT

COMPATIBILITY MODE IS NOT IN EFFECT

MULTI-LEVEL QUIET IS NOT IN EFFECT

MULTI-LEVEL STABLE IS NOT IN EFFECT

NO WRITE-DOWN IS NOT IN EFFECT

MULTI-LEVEL ACTIVE IS NOT IN EFFECT

CATALOGUED DATA SETS ONLY, IS NOT IN EFFECT

USER-ID FOR JES NJEUSERID IS : ????????

USER-ID FOR JES UNDEFINEDUSER IS : +++++++

PARTNER LU-VERIFICATION SESSIONKEY INTERVAL DEFAULT IS 30 DAYS.

APPLAUDIT IS IN EFFECT

ADDCREATOR IS NOT IN EFFECT

KERBLVL = 0

MULTI-LEVEL FILE SYSTEM IS NOT IN EFFECT

MULTI-LEVEL INTERPROCESS COMMUNICATIONS IS NOT IN EFFECT

MULTI-LEVEL NAME HIDING IS NOT IN EFFECT

SECURITY LABEL BY SYSTEM IS NOT IN EFFECT

PRIMARY LANGUAGE DEFAULT : ENU / ENGLISH

SECONDARY LANGUAGE DEFAULT : ENU / ENGLISH



# DSMON

S E L E C T E D	U S E R	A T T R I B U T E		R E P O R T
USERID	----- ATTRIBUTE TYPE -----			
	SPECIAL	OPERATIONS	AUDITOR	REVOKE
-----				-----
AHILL03				SYSTEM
AUDITJH			SYSTEM	
CICS01		SYSTEM		
CSTARR4	GROUP			
JSMITH1	GROUP	SYSTEM		GROUP
IBMUSER		SYSTEM		
RHOMES1				GROUP
RJONES2	SYSTEM	SYSTEM	SYSTEM	
SECUSR02	SYSTEM		SYSTEM	

S E L E C T E D	U S E R	A T T R I B U T E			S U M M A R Y
-----					
TOTAL DEFINED USERS:					4,129
TOTAL SELECTED ATTRIBUTE USERS:					
ATTRIBUTE BASIS	SPECIAL	OPERATIONS	AUDITOR	REVOKE	
-----	-----	-----	-----	-----	
SYSTEM	3	3	3	1	
GROUP	2	0	0	2	

# DSMON

## R A C F S T A R T E D P R O C E D U R E S T A B L E R E P O R T

FROM PROFILES IN THE STARTED CLASS:

PROFILE NAME	ASSOCIATED USER	ASSOCIATED GROUP	PRIVILEGED	TRUSTED	TRACE
AUTOMAT1.AUTOMAT1	=MEMBER	STASKGP	NO	NO	NO
CICSP01.*	CICSPRD1	STASKGP	NO	NO	NO
CICST01.CICSTEST	=MEMBER	STCTEST	YES	NO	NO
DUMPSRV.*	MVSSYST	STASKGP	NO	NO	NO
NETA.*	-STDATA	NOT SPECIFIED,	ICHRIN03	WILL BE USED-	
**	DFLTSTC	STASKGP	NO	NO	YES

## R A C F S T A R T E D P R O C E D U R E S T A B L E R E P O R T

FROM THE STARTED PROCEDURES TABLE (ICHRIN03)

PROCEDURE NAME	ASSOCIATED USER	ASSOCIATED GROUP	PRIVILEGED	TRUSTED
JES2	JES2		YES	YES
CICSTOR	CICSPRD	CICSSYS	NO	NO
CICSAOR	CICSPRD	CICSSYS	NO	NO
NETA	\$NETA	NTWKSTC	NO	NO
NETB	\$NETB	NTWKSTC	NO	NO
RCVRY	SYSRCVRY		YES	NO
*	=		YES	NO

# DSMON

R A C F	C L A S S	D E S C R I P T O R		T A B L E	R E P O R T
CLASS NAME	STATUS	AUDITING	STATISTICS	DEFAULT UACC	OPERATIONS ALLOWED
RVARSMBR	INACTIVE	NO	NO	NONE	NO
DASDVOL	ACTIVE	YES	YES	ACEE	YES
TERMINAL	ACTIVE	YES	YES	ACEE	NO
TCICSTRN	ACTIVE	NO	NO	NONE	NO
\$LMRKTMR (D)	ACTIVE	NO	NO	NONE	YES
TESTAPP	INACTIVE	NO	NO	READ	YES

R A C F	G L O B A L	A C C E S S	T A B L E	R E P O R T
CLASS NAME	ACCESS LEVEL	ENTRY NAME		
DATASET	ALTER	&RACUID.*		
	READ	CATLG.*		
	READ	ISP.*		
	READ	PROD.*.LIB		
	UPDATE	SYS1.BROADCAST		
	NONE	SYS1.RACF.*		
	READ	SYS1.*		
DASDVOL	-- NO ENTRIES --			
TERMINAL	-- GLOBAL INACTIVE --			

# DSMON

## RACF GROUP TREE REPORT

```

1  SYS1          (SECADM02)
2  |
3  |   PROD
3  |   |   PAY
3  |   |   ACCTG
2  |   |   USERDPT
3  |   |   |   USRGRPA
3  |   |   |   USRGRPB (SECADM02)
2  |   |   |   TECHSPT
3  |   |   |   |   TECHSPT1
4  |   |   |   |   |   DASDMGT (RJONES2)
5  |   |   |   |   |   DASDTEST
2  |   |   |   |   |   |   SYS2
  
```

SELECTED	DATA	SETS	REPORT	RACF	UACC
DATA SET NAME	VOLUME SERIAL	SELECTION CRITERION	INDICATED	PROTECTION	
CA7.PROD.LOADLIB	DBD023	APF	NO	YES	READ
CATLG.MSTR	SYSCAT	MASTER CATALOG	NO	YES	READ
CATLG.USERA	SYSCAT	USER CATALOG	NO	YES	UPDATE
CICS.TEST.R33.LIB	TSTA02	APF	N.F.	YES	UPDATE
FDR.LOADLIB	SYS033	APF	YES	YES	READ
		LINKLST - APF			
PAY.PROD.LOADLIB	APP770	LNKLST - APF	NO	NO	
SYS1.IMAGELIB	SYS034	SYSTEM	NO	YES	READ
SYS1.PARMLIB	SYSRS1	SYSTEM	NO	YES	UPDATE
SYS1.RACF.V19.PRIM	SYS011	RACF PRIMARY	NO	YES	READ
TMS.LINKLIB	ALT222	APF	NO	YES	UPDATE
UCC7.PROD.LOADLIB	D11456	APF	N.M.	NO	