

# **RACF MONITORING & REPORTING**

**SHARE - Winter 2007 - Session 1741 - February 2007**



**Robert S. Hansel**

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

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

# *TOPICS*

**Monitoring Basics**

**User Monitoring**

**Resource Monitoring**

**High Level Authority Monitoring**

**System Management Facilities (SMF)**

**Reporting Tools**

RACF, OS/390, z/OS, DB2, and CICS are Trademarks of the International Business Machines Corporation

# ***MONITORING BASICS***

## **RACF terminology - AUDITING**

### **Monitoring options can be specified in**

- **User profile**
- **Resource profile**
- **SETROPTS Options**
- **RACROUTE Macro LOG= parameter**

### **RACF auditing generates SMF records**

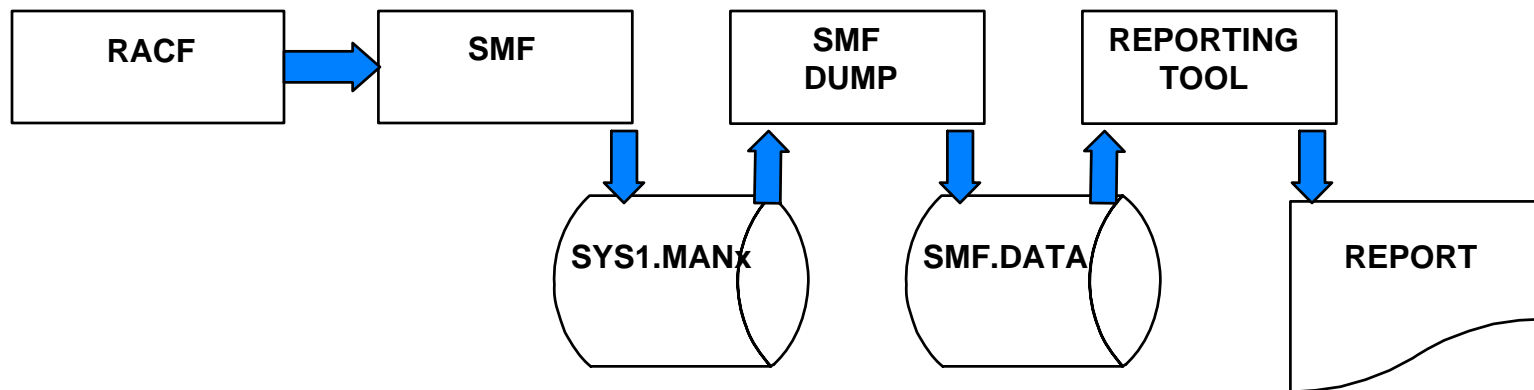
- **80 RACF Processing - Logged Events**
- **81 RACF Initialization - IPL**
- **83 RACF Audit Record for Data Sets (MLS)**

# 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



# ***USER MONITORING***

**Logon violations typically logged**

**SETROPTS AUDIT(USER) logs password changes at logon (z1.7)**

**SMF records used for TSO, Batch, and Started Task logon information**

- **20 Job Initiation (RACFRW only)**
- **30 Common Address Space Work (Job Initiation & Termination)**

**UAUDIT attribute on user profile**

- **All accesses logged - unless granted by Global Access Table or PRIVILEGED Started Task**
- **Some IDs may generate a substantial number of SMF records**
- **Used to analyze access activity in order to further restrict access**
- **Log selectively IDs of untrusted/external users & TRUSTED Started Tasks**

# RESOURCE MONITORING

## Dataset and General Resource Profile

### Audit settings

- **AUDIT( *option* ( *level* ))**
  - Set by Profile owner / SPECIAL
- **GLOBALAUDIT( *option* ( *level* ))**
  - Set by AUDITOR
- Used in combination

### Default settings

- **AUDIT(FAILURES(READ))**
- **GLOBALAUDIT(NONE)**

**Recommendation - log successes for sensitive resources**

### Auditing options

- **SUCCESS**
- **FAILURES**
- **ALL**
- **NONE**

### Auditing levels (at or above)

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

**Use profile LEVEL(##) to tag records for report selection**

# RESOURCE MONITORING

## LOGOPTIONS SETROPTS Options

- LOGOPTIONS( *level* ( *class* ) ) - set for each individual class
- Levels
  - DEFAULT Use resource profile log options
  - FAILURES Log all violations (*recommended for most*)
  - SUCCESSES Log all authorized access
  - NEVER Do not log
  - ALWAYS Log all access
- SUCCESSES and FAILURES augment profile audit settings
- ALWAYS and NEVER override profile audit settings
- ALWAYS level
  - Logs all accesses for a given resource class, even when no profile is defined to RACF - class must be active
  - Logs TRUSTED Started Tasks

# RESOURCE MONITORING

## LOGOPTIONS SETROPTS Options

- **Activates logging of Unix System Services (OMVS) events (FAILURES, SUCCESSES, & ALWAYS levels)**
  - **DIRSRCH**           Directory searches
  - **DIRACC**           Directory read/write access
  - **FSOBJ**             HFS object (e.g., file ) access
  - **FSSEC**            File system security changes (recommend ALWAYS)
  - **PROCESS**         Process uid or gid changes and privileged operations
  - **PROCACT**         Functions effecting other processes
  - **IPCOBJ**           Object access, uid or gid changes
  
- **LOGOPTIONS is ignored when access is granted by:**
  - **Global Access Table**
  - **RACROUTE FASTAUTH processing (use profile auditing (e.g., UNIXPRIV))**

# ***HIGH LEVEL AUTHORITY MONITORING***

## **SAUDIT SETROPTS Option**

- **Audit all RACF commands executed by SPECIAL user**
- **Audit all resource access using SPECIAL authority**

## **OPERAUDIT SETROPTS Option**

- **Audit all resource access using OPERATIONS authority**
- **Audit all ADDSDs using OPERATIONS authority**
- **Can generate massive amounts of SMF records if this authority is being relied on extensively**

## **CMDVIOL SETROPTS Option**

- **Audit all violations using RACF commands by anyone**
- **SEARCH and LIST-type command violations are not logged**
- **Rarely invoked - most command 'violations' are treated as 'errors'**

# PROFILE CHANGE MONITORING

## AUDIT( *resource-class* ) SETROPTS Option

- Audits all changes to RACF profiles in the associated resource class
- Captures administrative events not covered by SAUDIT and OPERAUDIT
- For certain classes, also logs:
  - DATASET creations and deletions of datasets
  - FSOBJ creations and deletions of USS file system objects
  - IPCOBJ creations and deletions of USS objects (e.g., semaphores)
  - PROCESS dubbing and undubbing of a process

# APPC & MLS AUDITING

## APPLAUDIT SETROPTS Option

- Allows user verification auditing at the beginning and ending of a user's transaction processing
- Must also specify **AUDIT(ALL)** or **GLOBALAUDIT(ALL)** on the APPL class profile associated with the APPC/MVS LU

## SETROPTS SECLEVELAUDIT( *seclevel* ) | NOSECLEVELAUDIT

- Activates auditing of all access attempts to resources at or above a specified security level
- Security level must be defined in SECDATA SECLEVEL profile

## SETROPTS SECLABELAUDIT | NOSECLABELAUDIT

- Specified that SECLABEL profile auditing options are to be used in addition to the resource profile auditing options in logging access

# ADDITIONAL MONITORING

## Real Time Notification

- NOTIFY( *userid* ) - Messages to *single* TSO user
- Security Console
  - Defined in PARMLIB(CONSOLxx) - MCS or SMCS
  - Route code 2, 9, and 11 messages
  - Recommend require logon if outside computer room

## SETROPTS STATISTICS( *class* )

- Access counts kept on Discrete profiles
- Counts not incremented for Global Access Table or RACLIST access
- Activated by class
- Little value and performance drag

# ***FACTORS EFFECTING MONITORING***

**LIST and SEARCH command usage is not logged**

**All SETROPTS command execution is automatically logged**

**PRIVILEGED Started Task access is never logged**

**Global Access Table (GAT) authorized access is never logged**

**RACF exits can expand or suppress auditing**

**Access granted during Failsoft is logged**

**RACF RACROUTE TYPE=AUDIT - generates log records**

# ***FACTORS EFFECTING MONITORING***

## **RACF RACROUTE Macro LOG= parameter**

- **Can expand or suppress auditing**
- **REQUEST=AUTH**
  - **NONE**      No logging or console operator messages
  - **NOSTAT**    Same as NONE and no profile statistics are updated
  - **NOFAIL**    Do not log violations - log successes per ASIS
  - **ASIS**      Log in accordance with profile & SETROPTS audit settings
- **REQUEST=FASTAUTH**
  - **NONE**      No logging or console operator messages
  - **NOFAIL**    Do not log violations - log successes per ASIS
  - **ASIS**      Log in accordance with profile & SETROPTS audit settings
- **REQUEST=VERIFY or VERIFYX**
  - **NONE**      No logging or console operator messages
  - **ASIS**      Log logon failures
  - **ALL**        Log all logon events

# ***SYSTEM MANAGEMENT FACILITIES (SMF)***

**Record Collection**

**Record Dumping**

**Monitoring**

# ***FACTORS EFFECTING SMF LOGGING***

## **SMF collects and saves log records**

- **SMF parameters can ignore record types**
- **SMF exits can suppress records**

## **SMF records are dumped for archive and for report processing**

- **SMF datasets must be dumped**
- **SMF dump utility and its exit can ignore records**
- **Datasets holding dumped archive SMF records can be manipulated or deleted**

# SMF - RECORD COLLECTION

**Parameters**      **PARMLIB(IEASYSxx)**  
**PARMLIB(SMFPRMxx)**

**Exits**

<b>IEFU83</b>	Receives control before record is written to the SMF dataset; can suppress record
<b>IEFU84</b>	Receives control when SMF Writer Routine is branch-entered and is <u>not</u> entered in cross-memory mode, before record is written to the SMF dataset; can suppress record
<b>IEFU85</b>	Receives control when SMF Writer Routine is branch-entered and is entered in cross-memory mode, before record is written to the SMF dataset; can suppress record

# SMF - RECORD COLLECTION - IEASYSxx

**SMF=xx**            **SMFPRMxx** member director

**OPI=YES | NO**    **IPL Operator Intervention**

To display current options via the console, issue command:

**DISPLAY SMF,O**

```
IEE967I 15.38.31 SMF PARAMETERS 373
      MEMBER = SMFPRMB1
      INTVAL(30) -- DEFAULT
      SUBSYS(STC,TYPE(0:98,100:255)) -- SYS
      SUBSYS(STC,NOINTERVAL) -- SYS
      SUBSYS(STC,NODETAIL) -- SYS
      SUBSYS(STC,EXITS(IEFUSO)) -- PARMLIB
      SUBSYS(STC,EXITS(IEFUJP)) -- PARMLIB
      SUBSYS(STC,EXITS(IEFU84)) -- PARMLIB
      SUBSYS(STC,EXITS(IEFU83)) -- PARMLIB
      SUBSYS(STC,EXITS(IEFU29)) -- PARMLIB
      SID(RSHB) -- PARMLIB
      JWT(0400) -- PARMLIB
      NOPROMPT -- PARMLIB
      DSNAME(SYS1.RSHB.MAN3) -- PARMLIB
      DSNAME(SYS1.RSHB.MAN2) -- PARMLIB
```

# **SMF - RECORD COLLECTION - SMFPRMxx**

<b>DSNAME(dsn)</b>	<b>SMF datasets (pre-MVS 5 - SYS1.MANx)</b>
<b>SID(sysid)</b>	<b>System Identifier (up to 4 characters)</b>
<b>PROMPT(ALL)</b>	<b>IPLR + LIST</b>
<b>PROMPT(LIST)</b>	<b>Change Options</b>
<b>PROMPT(IPLR)</b>	<b>IPL Reason Entry</b>
<b>NOPROMPT</b>	<b>No Intervention</b>
<b>SYS(options)</b>	<b>Global Options</b>
• <b>TYPE(0:255 #,#:#)</b>	<b>Type records collected</b>
• <b>NOTYPE(#,#:#)</b>	<b>Type records excluded</b>
• <b>EXITS(name,name)</b>	<b>Exits invoked</b>
<b>SUBSYS(name,options)</b>	<b>Subsystem options</b>
• <b>[Same as SYS]</b>	<b>Supersede SYS</b>

# ***SMF - RECORD DUMPING***

**Dump Exit**

**IEFU29**

**Automatic dump & switch**

**Dump Utility**

**IFASMFDP**

# SMF - RECORD DUMPING - IFASMFDP

```
//DUMPSMFR JOB (001),'HANSEL RS',CLASS=A,NOTIFY=&SYSUID
//STEP0001 EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//SYSMANDS DD DSN=SYS1.MAN1,DISP=SHR
//SMFMTHLY DD DSN=SMF.MONTHLY.DUMP.FEB,DISP=SHR
//RWDATA DD DSN=RSH.RACF.SMF.FEB,DISP=(NEW,CATLG,DELETE),UNIT=SYSDA,
// SPACE=(CYL,(100,10),RLSE),DCB=(LRECL=32767,RECFM=VBS)
//SYSIN DD *
        INDD(SYSMANDS,OPTIONS(DUMP))
        INDD(SMFMTHLY,OPTIONS(DUMP))
        OUTDD(RWDATA,TYPE(20,30,80,81,83))
        DATE(2006040,2006043) START(0800) END(1600)
        SID(MVSA)
        ABEND(NORETRY)
=====
        USER2(IRRADU00) USER3(IRRADU86) <<< SMF Unload
//ADUPRINT DD SYSOUT=*
//OUTDD DD DSN=RSH.SMF.UNLOAD,DISP=(NEW,CATLG,DELETE),
// SPACE=(CYL,(100,10),RLSE),UNIT=SYSDA,DCB=(LRECL=8192,RECFM=VB)
//XMLFORM DD DSN=RSH.SMF.XMLFORM,DISP=(NEW,CATLG,DELETE), <<< XML #1
// SPACE=(CYL,(100,10),RLSE),UNIT=SYSDA,DCB=(LRECL=8192,RECFM=VB)
//XMLOUT DD DSN=RSH.SMF.XMLOUT,DISP=(NEW,CATLG,DELETE), <<< XML #2
// SPACE=(CYL,(100,10),RLSE),UNIT=SYSDA,DCB=(LRECL=8192,RECFM=VB)
```

# SMF - MONITORING & INTEGRITY

## SMF Record Type

- 7 Lost Data
- 90 System Status

## SMFPRMxx

- NOBUFFS and LASTDS parameters - HALT option
- Can be used to prevent SMF record loss

**QUESTION:** For what length of time should SMF archives, either full or RACF-only extracts, be retained?

# **REPORTING TOOLS**

**RACF Report Writer**

**RACFRW**

**RACF SMF Unload**

**IRRADU00 & IRRADU86**

**DFSORT Utility Reports**

**ICETOOLS**

**Vendor Products**

**IBM (Consul) - zAdmin**

**Vanguard Integrity Prof. - Advisor**

**Allen Systems Group - ASG-Audit**

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

# REPORTING TOOLS

## RACFRW

- Creates reports from unformatted SMF data
- Limited report customization
  - Limited data selection criteria
  - Fixed report formats
  - Confusing detailed reports
- Requires no programming or database resources
- Stabilized RACF release 1.9.2

## SMF Unload

- Creates text and XML formatted data from unformatted SMF data
- Invoked through user exits in the SMF Dump Utility (IFASMFDP)
- DB2 table load SQL provided
- Text data can be browsed
- XML data can be viewed in an HTML browser
- Requires programming skills to generate reports
  - DB2 SQL queries
  - IBM RACFICE(DFSORT)
  - SAS, REXX, or other report writer

## Factors effecting reporting

- Reporting tool must be properly coded to select desired records for reporting
- Correct, comprehensive SMF archive datasets must be included for processing