RSH CONSULTING

RACF DSMON

KOIRUG - November 2014

Presentation Developers / Speakers

David Bell, Hartford Financial Services

David Bell is a Senior Compliance Specialist for Hartford Financial Services. He has worked with IBM mainframes since 1996 and in various operational and technical Information Security disciplines since 1988. Mr. Bell began working with RACF in 1996 when he joined Harford Financial Services. While there he was the technical lead for several RACF migrations/database merges related to acquisitions and internal consolidations and also was lead the implementation of user provisioning tools. In 2000 Mr. Bell worked for RSH Consulting for a brief period. While with RSH Consulting he assisted a major retailer implement enterprise wide user provisioning technology, conducted security reviews and assisted with RACF database consolidations. Mr. Bell returned to Hartford Financial Services in 2001 and continued working with RACF and user provisioning technologies until 2007, when he joined IBM Global Services as part of an outsourcing arrangement. Mr. Bell worked for IBM Global Services for three years where he provided RACF technical support and conducted RACF security reviews for several international companies. In 2010, Mr. Bell returned to Hartford Financial Services as a Compliance Specialist where he has focused on PII, PCI, RACF and SOX compliance.

Todd Grant, Navient

Todd Grant, CISSP is a Senior Information Security Analyst at Navient Corporation, located in the Indianapolis, Indiana area. He has worked in Information Technology since 1995; and has specialized in Information Security since 2006. Since joining his company's RACF team in 2010, Todd has earned both the GIAC Security Essentials (GSEC) as well as the prestigious Certified Information Systems Security Professional (CISSP) certifications. He currently attends Indiana Wesleyan University, where he will be graduating with a Bachelor of Science in Management degree in summer 2015. Prior to his technology career Todd served in the United States Navy for 10 years, as a Cryptologic Technician.

Robert S. Hansel, RSH Consulting

Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc., an IT security professional services firm he established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. He has worked with IBM mainframes since 1976 and in information systems security since 1981. Mr. Hansel began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. He has reviewed, implemented, and enhanced RACF controls for major insurance firms, financial institutions, utilities, payment card processors, universities, hospitals, and international retailers. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He has also created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON Introduction

- DSMON - RACF Data Security Monitor
- APF-authorized program - ICHDSM00
- Produces reports on the status of …
  - System and security environment
  - Certain RACF controls
- To execute, requires ...
  - Either …
    - EXECUTE or READ access to PROGRAM ICHDSM00
      - Define PROGRAM profile ICHDSM00 if backstop ** profile exists
    - System-level AUDITOR if program is not defined or not executing in a clean program environment
  - And …
    - READ access to FACILITY ICHDSM00.SYSCAT to list user catalogs with SYSCAT (allowed if not defined)
- Reference: RACF Auditor's Guide

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Batch JCL

```
//jobname  JOB (account),'username',CLASS=x,MSGCLASS=x
//DSMON    EXEC PGM=ICHDSM00
//SYSPRINT DD  SYSOUT=*                Status and error messages
//SYSUT2   DD  SYSOUT=*                DSMON report
//SYSIN    DD  *                       Input control statements
  -- control statements --
```

Control Statements

- LINECOUNT 0 | 40-99 | 55 — Lines per page of output
- FUNCTION *function* | ALL — Report to be generated
- USEROPT USRDSN | RACGRP — User specified dataset or group subtree

```
FUNCTION USRDSN
USEROPT USRDSN PROD.PAYROLL [ VOL=volser ]

FUNCTION RACGRP
USEROPT RACGRP ACCTDEPT

FUNCTION ALL
USEROPT USRDSN PROD.PAYROLL     Lists USRDSN with other selected datasets
USEROPT RACGRP ACCTDEPT         Shows only group subtree
```


© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Functions

- FUNCTIONs (in report generated sequence) run for each ...

SYSTEM	**System and RACF identification**	**Execution(1)**
SYSPPT	**Program Properties Table (PPT) entries**	**System**
RACAUT	**RACF Authorized Caller Table entries**	**System**
RACEXT	**RACF Exits**	**System**
RACUSR	**RACF User Attribute Summary Report**	**Database(2)**
RACSPT	**RACF STARTED Class and Started Task Table entries**	**System**
RACCDT	**RACF Class Descriptor Table entries and status**	**System**
RACGAC	**RACF Global Access Checking Table Report**	**Database**
RACGRP	**RACF Group Tree**	**Database(2)**
SYSAPF	**Selected Dataset Report - APF library protection**	**System**
SYSLNK	**Selected Dataset Report - Linklist library protection**	**System**
SYSSDS	**Selected Dataset Report - System dataset report**	**System**
SYSCAT	**Selected Dataset Report - Catalog dataset protection**	**System**
RACDST	**Selected Dataset Report - RACF database protection**	**System**

(1) Include SYSTEM with every execution to identify the system of origin

(2) Avoid running RACUSR and RACGRP during peak processing periods

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Function SYSTEM

```
S Y S T E M    R E P O R T
-------------------------------------------------------------------------------
CPU-ID                                  010188
CPU MODEL                               9672
OPERATING SYSTEM/LEVEL                  z/OS 1.12.0
SYSTEM RESIDENCE VOLUME                 SYSRS1
SMF-ID                                  SY0T
RACF (FMID HRF7770) IS ACTIVE
```

- System Resident (SYSRES) Volume matches VOLSER of ****** in PROGRAM profiles
- The SMF-ID is recorded in SMF records
- Supported releases:

  http://www-03.ibm.com/systems/z/os/zos/support/zos_eos_dates.html

- What's Important …..
  - The z/OS version should be a supported level
  - Correct SYSRES was used to IPL the system
  - RACF should be active

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Function SYSPPT

```
P R O G R A M     P R O P E R T I E S     T A B L E     R E P O R T
PROGRAM          BYPASS PASSWORD          SYSTEM
NAME             PROTECTION               KEY
-----------------------------------------------------------------------
IEDQTCAM              NO                  YES
ISTINM01              YES                 YES
IEEVMNT2              NO                  YES
HASJES20              YES                 YES
IATINTK               YES                 YES
INSTPGM1              YES                 YES
DFHSIP                YES                 YES
```

- NOPASS allows access to any dataset without RACF authorization checking
- KEY indicates the program has been assign a System Key (0-7) which related to storage protection and can execute privileged SVCs (e.g., MODESET) to bypass security
- PPT entries are defined in PARMLIB(SCHEDxx)
- Programs must be fetched from an APF-authorized library (need not be AC>0)
- Entries may not match any programs (e.g., JES3 program IATINTK)
- IBM entries are documented in manual z/OS MVS Initialization and Tuning Reference
- IBM entries need not, and should not, be changed or nullified

- What's Important …..
  - NOPASS and KEY should not be assigned to installation entries unless strictly justified
  - UPDATE access to APF-authorized libraries should be strictly controlled

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Function RACAUT

```
R A C F     A U T H O R I Z E D      C A L L E R      T A B L E      R E P O R T
MODULE                RACINIT        RACLIST
NAME                  AUTHORIZED     AUTHORIZED
-------------------------------------------------------------------------------
NO ENTRIES IN RACF AUTHORIZED CALLER TABLE
```

- Allow non-APF-authorized program to use RACROUTE REQUEST=LIST and/or REQUEST=VERIFY , but excluding certain VERIFY keywords

- What's Important …..
  - This table should be empty - IBM does not recommend it be used

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Function RACEXT

```
R A C F     E X I T S     R E P O R T
EXIT MODULE            MODULE
NAME                   LENGTH
-----------------------------------------------------------------------------
ICHDEX01                 232
ICHRCX02               4,248
```

- Only lists RACF exits, and not SAF or Callable Services exits
- For dynamic exits IRREVX01 and IRRVAF01, the length will be NA (not available)
- Some system products install pointers to other modules, often to allow dynamic exit changes; usually show a short length

- What's Important …..
  - IBM's weak proprietary password encryption algorithm should not still be active, which is usually indicated by the presence of ICHDEX01 with a length of 232
  - Exit logic should be efficient and does not introduce security exposures
  - Source code should match the live modules in the system (assemble/compare)

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Function RACUSR

```
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  --------  ----------- ASSOCIATIONS  --------
          SPECIAL  OPERATIONS  AUDITOR  REVOKE  NODE.USERID  PASSWORD  ASSOCIATION
                                                             SYNC      TYPE
-------------------------------------------------------------------------------------
AHILL03                                SYSTEM
AUDITJH                       SYSTEM
CICS01              SYSTEM
CSTARR4   GROUP
JSMITH1   GROUP     SYSTEM             GROUP
IBMUSER             SYSTEM
RHOMES1                                       PRDA.RHOMES2  YES      PEER
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                  2           4        3       1
GROUP                   2           0        0       1
```

- Limited information; does not indicate groups(s) where authority is held
- Can be lengthy if many REVOKED users
- What's Important …..
  - It should be appropriate for users to have the authorities assigned

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Started Task Report

```
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                 ASSOCIATED  ASSOCIATED
NAME                    USER        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          YES      NO
NETA.*                  -STDATA NOT SPECIFIED, ICHRIN03 WILL BE USED-
**                      DFLTSTC     STASKGP     NO          NO       YES
```

=MEMBER - assign ID matching PROC name
Report is not generated if STARTED is not active

```
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       ASSOCIATED      ASSOCIATED
NAME            USER            GROUP           PRIVILEGED     TRUSTED
-----------------------------------------------------------------------------
JES2            JES2                            YES            YES
CICSTOR         CICSPRD         CICSSYS         NO             NO
CICSAOR         CICSPRD         CICSSYS         NO             NO
NETA            $SNETA          NTWKSTC         NO             NO
NETB            $SNETB          NTWKSTC         NO             NO
RCVRY           SYSRCVRY                        YES            NO
*               =                               YES            NO
```

* - all PROCs not specified above
= - assign ID matching PROC name

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Function RACSPT

- STARTED profiles lacking an STDATA segment use ICHRIN03 to assign an ID
- If assigned ID does not exist or is not connected to the specified group, Started Task runs with no ID (undefined user)
- TRACE(YES) produces IRR812I system log message when profile is used

- What's important ...
  - Users and groups in STARTED profiles and ICHRIN03 should be defined to RACF
  - All STARTED profiles should have an STDATA segment
  - No entries should assign USER of IBMUSER
  - All entries should specify a GROUP, especially default entries
  - No Started Task should be assigned PRIVILEGED
  - TRUSTED should only assigned as recommended by IBM (1) Optional (2) When using z/OSMF ISPF

APSWPROx(1)	CATALOG	CEA(2)	DFHSM(1)	DFS(1)
DUMPSRV	GPMSERVE(1)	HIS	IEEVMPCR	IOSAS
IXGLOGR	JESn	JESXCF	JES3AUX	LLA
OMVS(1)	NFS	RACF	RMF	RMFGAT
SMF	SMS	SMSPDSE1	SMSVSAM(1)	TCPIP
VLF	VTAM	WLM	XCFAS	ZFS(1)

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Function RACCDT

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
ACCTNUM		ACTIVE	NO	NO	NONE	NO
APPL		ACTIVE	NO	NO	NONE	NO
DASDVOL		ACTIVE	YES	NO	ACEE	YES
RACFVARS		ACTIVE	NO	NO	NONE	NO
T@TESTRN	(D)	ACTIVE	NO	NO	NONE	NO
TCICSTRN		ACTIVE	NO	NO	NONE	NO
TERMINAL		ACTIVE	YES	YES	ACEE	NO
TESTAPP	(D)	INACTIVE	NO	NO	READ	YES

- (D) signifies installation class defined by CDT class profile

- What's important ...
  - Only pre-defined IBM classes should allow OPERATIONS
  - Installation classes should have a special character in their name
  - Installation classes should have Default UACC of NONE or ACEE
  - Class that should be active are active
  - No classes should be active for STATISTICS
  - All classes should be active for AUDIT

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Function RACGAC

```
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            ACCESS          ENTRY
NAME             LEVEL           NAME
-----------------------------------------------------------------------------
DATASET          ALTER           &RACUID.*
                 ALTER           CATLG.*
                 READ            ISP.*
                 READ            PROD.*.LIB
                 UPDATE          SYS1.BRODCAST
                 NONE            SYS1.RACF.*
                 READ            SYS1.*
DASDVOL          -- GLOBAL INACTIVE --
TERMINAL         -- NO ENTRIES --
FACILITY         READ            STGADMIN.ARC.ENDUSER.*
```

- Access Level of NONE causes RACF to skip the GAT and check the profile; it does <u>not</u> prevent access

- What's important ...
  - Entries should not allow greater access than the UACC of the underlying associated profile(s)
  - Classes are deactivated (NOGLOBAL) is no entries are defined
  - Appropriate entries are defined to enhance RACF performance

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Function RACGRP

```
R A C F     G R O U P     T R E E     R E P O R T
LEVEL   GROUP       (OWNER)
-----------------------------------------------------------------------------
1   SYS1        (SECADM02)
2   | PROD
3   | | PAY
3   | | ACCTG
2   | USERDPT
3   | | USRGRPA
3   | | USRGRPB   (SECADM02)
2   | TECHSPT
3   | | TECHSPT1
4   | | | DASDMGT   (RJONES2)
5   | | | | DASDTEST
2   | SYS2
```

- OWNER is only displayed if it a user; otherwise, it is the superior group
- What's important ...
  - Users should only own groups to administer them or break the scope-of-groups by design

© 2014 RSH Consulting, Inc. All Rights Reserved.

DSMON - Functions SYSAPF, SYSLNK, SYSDSD, SYSCAT, RACDST

```
S E L E C T E D     D A T A     S E T S     R E P O R T
                   VOLUME  SELECTION       RACF        RACF
DATA SET NAME      SERIAL  CRITERION       INDICATED   PROTECTION  UACC
-----------------------------------------------------------------------------
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

                           N.F.  - Not Found
                           N.C.  - Not Cataloged
                           N.M.  - VOLSER Not Mounted
```

- Datasets may not exist; could be prepositioned entries for future maintenance
- Access by ID(*) is not shown and could undermine protection
- Not all PARMLIBs and PROCLIBs are listed (could include with USRDSN)
- SYSAPF only lists libraries defined in PARMLIB IEAAPFxx or PROGxx or added by MVS SETPROG command; LPA, MLPA, and FLPA authorized libraries may not appear
- RACF-indicated means the VTOC RACF bit is on and a discrete profile may exist
- What's important ...
  - Datasets should be protected with an appropriate UACC

© 2014 RSH Consulting, Inc. All Rights Reserved.