



IBM Systems Group

An Introduction to DSMON

RACF-2004
Session D11
June 2004

Mark Nelson, CISSP
z/OS Security Server (RACF) Design and Development
IBM Poughkeepsie
markan@us.ibm.com

Trademarks

- **These terms are trademarks of the IBM Corporation in the United States, other countries, or both:**
 - ▶ **CICS**
 - ▶ **IBM**
 - ▶ **IMS**
 - ▶ **MVS**
 - ▶ **OS/390**
 - ▶ **RACF**
 - ▶ **z/OS**
- **UNIX is a registered trademark in the United States, other countries, or both and is licensed exclusively through the X/Open Company Limited.**

Agenda

- **What is DSMON?**
- **How is DSMON invoked?**
- **Who can invoke DSMON?**
- **What do the reports show?**
- **What should you look for?**

What is DSMON?

- **DSMON is a RACF-supplied program which produces reports on:**
 - ▶ Your OS/390 or z/OS security environment
 - ▶ Selected key system resources

- **Interpretation of DSMON output is the responsibility of the user of the report**

How is DSMON Invoked?

- **Traditionally invoked as a batch job**

```
//JOBNAME   JOB.....  
//          EXEC PGM=ICHDSM00  
//SYSUT2    DD     SYSOUT=*  
//SYSPRINT  DD     SYSOUT=*  
//SYSIN     DD     *  
    <DSMON control cards>  
/*
```

- **SYSPRINT is the destination for messages**
- **SYSUT2 is the destination for the reports**
- **SYSIN is for control statements**

How is DSMON Invoked?...

- **The `SYSDN` control statements that you can specify are:**
 - ▶ `FUNCTION <function-name>`
 - ▶ Default: All reports
 - ▶ `LINECOUNT <lines-per-page>`
 - ▶ `USEROPT USRDSN <data-set> VOL=<vol>`
 - ▶ `USEROPT RACGRP <group-name>`

Who Can Run DSMON?

- **...anyone with the AUDITOR attribute**
- **...anyone who has at least EXECUTE authority to the ICHDSM00 program**
 - ▶ Defining a PROGRAM * profile for SYS1.LINKLIB with a UACC of other than NONE may allow more people to run DSMON than you intend!
 - ▶ Create a PROGRAM profile for ICHDSM00 with the correct access list
 - ▶ DO NOT CREATE A PROGRAM PROFILE OF * WITH UACC(NONE)!

DSMON Reports

Report Name	Description
SYSTEM	Basic information about the system
RACGRP	Group tree hierarchy
SYPPT	Program properties table
RACAUT	RACF authorized caller table
RACCDT	RACF class descriptor table
RACEXT	RACF exits
RACGAC	RACF global access table
RACSPT	RACF started procedures table
RACUSR	RACF Selected user attribute report
SYSLNK	LNKLSTxx data sets
SYSAPF	APF-authorized data sets
SYSCAT	System catalog and user catalogs
RACDST	RACF databases
SYSSDS	Selected system data sets
USRDSN	User-specified data sets

System Report

- **Identifies your system**
 - ▶ Operating system and RACF level
 - ▶ SMF system ID
 - ▶ SYSRES volume

- **What to look for:**
 - ▶ Correct system?
 - ▶ Correct operating system/RACF level?
 - ▶ Correct SYSRES?

Program Properties Table Report

DATE: 01/18/02 TIME: 18:50:52 PAGE: 2
PROGRAM PROPERTIES TABLE REPORT
PROGRAM BYPASS PASSWORD SYSTEM
NAME PROTECTION KEY

IEDQTCAM	NO	YES
ISTINM01	YES	YES
IKTCAS00	NO	YES
AHLGTF	NO	YES
HHLGTF	NO	YES
IHLGTF	NO	YES
IEFLIC	NO	YES
IEEMB860	YES	YES
IEVMNT2	NO	YES
IASXWR00	NO	YES
CSVVFCRE	NO	YES
HASJES20	NO	YES
DFSMVRC0	NO	YES
IATINTK	NO	NO
DXRRLM00	NO	YES
APSPPIEP	NO	YES
AKPCSI EP	NO	YES
IATINTKF	NO	NO
DSNYASCP	NO	YES
DSNUTILB	NO	YES
IEAVTDSV	YES	YES
IFASMF	NO	YES
CSVLLCRE	YES	YES
AVFMNBLD	NO	

Program Property Table Report

- **Identifies programs (load modules) which execute with special privileges**
 - ▶ Bypass password protection
 - ▶ Execution key

- **What to look for:**
 - ▶ Are modules in the list the correct ones? Are there any "extras"?
 - ▶ Are vendor recommendations being followed?
 - ▶ See "z/OS MVS Initialization and Tuning" or "OS/390 MVS Initialization and Tuning" for IBM defaults

Authorized Caller Table Report

RACF DATA SECURITY MONITOR DATE: 01/18/02 TIME: 18:50:52 PAGE: 6

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

Authorized Caller Table Report

- **Identifies non-authorized programs which can invoke privileged RACF functions RACINIT and RACLIST**

- **What to look for:**
 - ▶ Should be empty!

Exits Reports

RACF DATA SECURITY MONITOR DATE: 01/18/02 TIME: 18:50:52 PAGE: 7

R A C F E X I T S R E P O R T

EXIT MODULE NAME	MODULE LENGTH
---------------------	------------------

ICHRIX01	240
----------	-----

Exits Reports...

- **Shows the names and lengths of RACF exits**
 - ▶ Does not show the SAF Router Exits (ICHRTX00, ICHRTX01) or Callable Service Router Exit (IRRSTX00)

- **What to look for:**
 - ▶ Are there any extra exits listed?
 - ▶ Are the lengths of the exits correct?
 - ▶ Are there any error messages?

Selected User Attribute Report

RACF DATA SECURITY MONITOR DATE: 01/18/02 TIME: 18:50:52 PAGE: 26

USERID	-----	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	-----	ASSOCIATIONS	-----
		ATTRIBUTE	TYPE				PASSWORD	ASSOCIATION
				REVOKE	NODE.USERID		SYNC	TYPE
GRAND					SYSTEM			
GREAN	GROUP							
GREET					SYSTEM			
HUFFL	GROUP							
IBMUSER					SYSTEM			

Select User Attribute Report...

RACF DATA SECURITY MONITOR DATE: 01/18/02 TIME: 18:50:52 PAGE: 49
 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 R E P O R T

TOTAL DEFINED USERS:		20,549			
TOTAL SELECTED ATTRIBUTE USERS:					
ATTRIBUTE BASIS	SPECIAL	OPERATIONS	AUDITOR	REVOKE	
SYSTEM	23	47	14	782	
GROUP	64	6	2	2	

Selected User Attribute Report

- **Shows user IDs which:**

- ▶ Have the SPECIAL, OPERATIONS, or AUDITOR (at system or group level)
- ▶ Are revoked
- ▶ Have RRSF associations

- **What to look for:**

- ▶ Is IBMUSER revoked?
- ▶ Do you have a proper separation of duties?
- ▶ Unexpected IDs? Number of IDs?
- ▶ Are the associations to user IDs with administrative authority?

Started Procedures Table – STARTED Class Report

RACF DATA SECURITY MONITOR DATE: 01/18/02 TIME: 18:50:52 PAGE: 50
 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
BPXOINIT.* (G)	OMVSKERN	OMVSGRP	NO	NO	NO
EREPDALY.* (G)	EREP		NO	NO	NO
HSM.* (G)	HSM		NO	YES	NO
INIT.* (G)	STCBYP		NO	NO	NO
IOSAS.* (G)	IOSAS		NO	YES	NO
JES2.* (G)	JES2		NO	YES	NO
LLA.* (G)	STCBYP		NO	NO	NO
MMS.* (G)	STCBYP		NO	YES	NO
NET.* (G)	NET		NO	YES	NO
TSO.* (G)	TSOSTC		NO	NO	NO
VLFF.* (G)	STCBYP		NO	NO	NO
XCFAS.* (G)	XCFAS		NO	YES	NO
** (G)	=MEMBER	STCGRP	NO	NO	YES

Started Procedures Table - ICHRIN03 Report

RACF DATA SECURITY MONITOR DATE: 01/18/02 TIME: 18:50:52 PAGE: 52
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
HSM	HSM		NO	YES
INIT	STCBYP		NO	NO
IOSAS	IOSAS		NO	YES
JES2	JES2		NO	YES
LLA	STCBYP		NO	NO
NET	NET		NO	YES
TSO	TSOSTC		NO	NO
VLF	STCBYP		NO	NO
XCFAS	XCFAS		NO	YES
*	=	STCGRP	NO	NO

Started Procedures Table Report

- **Shows the user ID/group ID that will be associated with a started task along with the "trusted" or "privileged" status**

- **Two versions of the report:**
 - ▶ STARTED class (created only if STARTED class is active)
 - ▶ ICHRIN03

Started Procedures Table Report...

■ **What to look for:**

- ▶ ICHRIN03 should contain entries which allow the startup and recovery of your system (e.g. VTAM, JES, TSO)
- ▶ Default entry maps to a user ID with a specified group name
- ▶ No "*" = entries with no group specified
- ▶ "Privileged" and "trusted" attributes are assigned correctly
- ▶ "Trusted" is preferred as it may be logged
- ▶ TRACE on default STARTED class entry

Class Descriptor Table Report

DATE: 01/18/02 TIME: 18:50:52

PAGE: 54

CLASS NAME	R A C F STATUS	C L A S S AUDITING	D E S C R I P T O R STATISTICS	T A B L E DEFAULT UACC	R E P O R T OPERATIONS ALLOWED
RVARSMBR	ACTIVE	YES	NO	NONE	NO
RACFVARS	ACTIVE	YES	NO	NONE	NO
SECLABEL	INACTIVE	YES	NO	NONE	NO
DASDVOL	ACTIVE	YES	NO	ACEE	YES
GDASDVOL	ACTIVE	YES	NO	ACEE	YES
TAPEVOL	ACTIVE	YES	NO	ACEE	YES
TERMINAL	ACTIVE	YES	NO	ACEE	NO
GTERMINL	ACTIVE	YES	NO	ACEE	NO
APPL	ACTIVE	YES	NO	NONE	NO
TIMS	INACTIVE	YES	NO	NONE	NO
GIMS	INACTIVE	YES	NO	NONE	NO
AIMS	INACTIVE	YES	NO	NONE	NO
TCICSTRN	ACTIVE	YES	NO	NONE	NO
GCICSTRN	ACTIVE	YES	NO	NONE	NO
PCICSPSB	ACTIVE	YES	NO	NONE	NO
QCICSPSB	ACTIVE	YES	NO	NONE	NO
GLOBAL	ACTIVE	YES	NO	NONE	NO
GMBR	ACTIVE	YES	NO	NONE	NO
DSNR	ACTIVE	YES	NO	ACEE	NO
FACILITY	ACTIVE	YES	NO	NONE	NO

Class Descriptor Table Report...

- **For each RACF general resource class, shows:**
 - ▶ Status: ACTIVE or INACTIVE
 - ▶ Is "AUDITING" (logging is a better word) enabled for the class?
 - ▶ Does having the OPERATIONS attribute allow you to access resources in this class?
 - ▶ What is the default UACC?
 - NONE
 - Taken from ACEE
 - ▶ Are statistics being recorded?

Class Descriptor Table Report...

- **What to look for:**

- ▶ Are the expected classes defined?
- ▶ Are the expected classes active?
- ▶ Are the right classes being logged (audited)?

Global Access Table Report

RACF DATA SECURITY MONITOR DATE: 01/18/02 TIME: 18:50:52 PAGE: 63

CLASS ACCESS GLOBAL ACCESS TABLE REPORT
 NAME LEVEL ENTRY NAME

```

-----
DATASET          ALTER          &RACUID.**
                  ALTER          RA.P.&RACUID.**
                  ALTER          RA.T.&RACUID.**
                  UPDATE        SYS1.BROADCAST
RVARSMBR         -- GLOBAL INACTIVE --
SECLABEL         -- GLOBAL INACTIVE --
DASDVOL          -- GLOBAL INACTIVE --
TAPEVOL          -- GLOBAL INACTIVE --
TERMINAL         -- GLOBAL INACTIVE --
APPL             -- GLOBAL INACTIVE --
TIMS             -- GLOBAL INACTIVE --
AIMS             -- GLOBAL INACTIVE --
TCICSTRN        -- GLOBAL INACTIVE --
PCICSPSB        -- GLOBAL INACTIVE --
GMBR            -- GLOBAL INACTIVE --
DSNR            -- GLOBAL INACTIVE --
FACILITY        -- NO ENTRIES --
  
```

Global Access Table Report,,,

- **For each RACF general resource class, shows:**
 - ▶ The global access entities which are in effect
 - ▶ The access that is granted (remember that the global access table can only grant access; If access is not granted by the global access table, processing continued with profiles in the RACF database)

Global Access Table Report...

■ What to look for:

- ▶ Are the expected global access entries in place?
- ▶ Do the global access rules match what is in the RACF database for the target class?
- ▶ Is a more restrictive and specific global table entry overridden by a more generic entry?
 - 'SYS1.**'/READ
 - 'SYS1.RACFPRIM'/NONE
- ▶ Do you really want to have 'SYS1.**'/READ'?

Selected Data Sets Report...

- **For each selected data set, shows:**
 - ▶ Volume
 - ▶ Why the data set was selected for reporting
 - Linklist
 - APF
 - Catalog
 - RACF database
 - ▶ RACF indicated
 - ▶ RACF protected
 - ▶ UACC

Selected Data Sets Report...

- **What to look for:**

- ▶ APF data sets which are "N.F." (not found)
- ▶ Data sets which are "N.M." (not mounted)
- ▶ Excessive UACC
- ▶ Not "RACF Protected"
 - Note that being RACF protected doesn't mean that it is properly protected!

Group Tree Report

```
          R A C F      G R O U P      T R E E      R E P O R T
LEVEL  GROUP          (OWNER)
-----
1  SYS1              (IBMUSER )
2  |  PROD            (PRODMGT )
3  |  |  PRODP1
3  |  |  PRODP2
3  |  |  PRODP3
3  |  |  PRODP4
3  |  |  PRODP5
2  |  SYSCTLG        (IBMUSER )
2  |  TEST           (TESTADM )
3  |  |  TESTP1      (MARKN  )
4  |  |  |  TESTPZ1
4  |  |  |  TESTPZ2
4  |  |  |  TESTPZ3
4  |  |  |  TESTPZ4
4  |  |  |  TESTPZ5
3  |  |  TESTP2
3  |  |  TESTP3
3  |  |  TESTP4
3  |  |  TESTP5
2  |  VSAMDSET      (IBMUSER )
```

Group Tree Report...

- **Shows the hierarchy of groups**
- **Identifies the ownership chain**
- **What to look for:**
 - ▶ Are your naming conventions being followed?
 - ▶ How does group-level SPECIAL, OPERATIONS, and AUDITOR work with your group tree?
 - ▶ Are there obsolete groups?

Is That All There Is?

- **Now that you are done with DSMON review, are you done?**

- **Other sources to be reviewed:**
 - ▶ SETROPTS options
 - ▶ SMF data
 - ▶ Key resources (e.g. OPERCMDS, TSOAUTH)
 - ▶ UNIX System Services resources (e.g. BPX.SUPERUSER)

Disclaimer (The Legal Stuff)

- The information contained in this document is distributed on an "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.
- In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.
- It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.
- IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.