



IBM Systems and Technology Group

RACF Support for the IBM Health Checker for z/OS

New York RACF Users Group
October, 2005

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

© 2005 IBM Corporation

IBM Systems and Technology Group



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

DB2®
e-business logo
IBM®
IBM eServer
IBM logo®
OS/390®
RACF®
z/OS®

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
UNIX is a registered trademark of The Open Group in the United States and other countries.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

© 2005 IBM Corporation

Agenda

- **What is the IBM Health Checker for z/OS?**
 - ▶ History
 - ▶ Structure
 - ▶ Existing checks
 - ▶ What's new for z/OS V1R4-V1R7
 - ▶ Tailoring checks
 - ▶ MVS components which are shipping checks
- **RACF support for the IBM Health Checker for z/OS**
 - ▶ Two new general resource classes (XFACILIT/GXFACILI)
 - ▶ Two new RACF checks:
 - RACF_GRS_RNL
 - RACF_SENSITIVE_RESOURCES
 - ▶ Demo?

RACF Support for the IBM Health Checker for z/OS

- **What is the IBM Health Checker for z/OS?**
 - ▶ **Originally a tool developed by ITSO to address component configuration and setup errors commonly made by installations**
 - Web download
 - Implemented as a batch job
 - 37 checks
 - ▶ **With z/OS V1R7, the IBM Health Checker for z/OS is integrated into z/OS**
 - Implemented as a started task
 - 55 checks
 - Rolled back to z/OS V1R4 as a web download
 - Checks are shipped with components
 - Installations and vendors can write checks
 - Extensive SDSF support

RACF Support for the IBM Health Checker for z/OS ...

- **A check is identified by its name (1-32 characters) and owner (1-16 characters)**
- **Each check has:**
 - ▶ An execution interval (one time or timer interval)
 - ▶ A default severity (low, medium, or high)
 - ▶ A scope (LOCAL or GLOBAL)
 - ▶ Activity status (ACTIVE or INACTIVE)
- **Check defaults can be overridden by the installation**
- **Checks can be manually started**

RACF Support for the IBM Health Checker for z/OS ...

- **MVS components which are shipping checks:**
 - ▶ Consoles
 - ▶ Contents Supervision
 - ▶ GRS
 - ▶ RACF
 - ▶ Resource Recovery Services (RRS)
 - ▶ SDUMP
 - ▶ z/OS UNIX System Services
 - ▶ Virtual Storage Management
 - ▶ Real Storage Management
 - ▶ XES/XCF

RACF Support for the IBM Health Checker for z/OS ...

- **RACF Support for the IBM Health Checker for z/OS:**
 - ▶ **New general resource classes: XFACILIT/GXFACILI**
 - The eXtended FACILITy class
 - Resource name of up to 246 characters
 - Shared POSIT value with the FACILITY class
 - Shipped in APAR OA10774, back to z/OS V1R4
 - ▶ **Two RACF checks (owner: IBMRACF)**
 - **RACF_GRS_RNL (rolled back to z/OS V1R6 with APAR OA11833)**
 - Checks to see if any of the RACF ENQ names are on a GRS resource name exclusion list which changes the scope of the RACF ENQ
 - **RACF_SENSITIVE_RESOURCES (rolled back to z/OS V1R4 with APAR OA11833)**
 - Looks at the current APF data sets and the RACF database data sets and flags those that are improperly protected
 - Are not found on the indicated volume
 - Are improperly protected

RACF_GRS_RNL Output

START TIME: 11/10/2004 10:13:10.341622 IBMRACF, RACF_GRS_RNL
OWNER DATE: 20040703

RACF_GRS_RNL Report

S	Major	Minor	Type	QName	Rname	Type
E	SYSZRACF	SETROPTS	SERNL	SYSZRACF	SETROPTS	SPEC
E	SYSZRAC2	IRRCRV05	SERNL	SYSZRAC2	IRRCRV05	SPEC

* High severity Exception *

IRRH202E One or more RACF ENQ names were found in a GRS Resource Name List.

Explanation:

The RACF RACF_GRS_RNL check has detected that a RACF resource is covered by an entry in the specified GRS resource name list (RNL). RACF resource names should not be in either the system inclusion RNL (SIRNL) or the system exclusion RNL (SERNL).


System Action:

The check continues processing. There is no effect on the system.

...

IBMRACF Reason: None of the RACF ENQ names should be in RNLs.
Check parameters: N/A

END TIME: 01/08/2005 20:47:54.819710

IBM Systems and Technology Group 

RACF_SENSITIVE_RESOURCES Output

START TIME: 01/08/2005 20:47:54.701509 IBMRACF,
 CHECK (IBMRACF,RACF_SENSITIVE_RESOURCES)
 START TIME: 04/14/2005 11:07:25.901856
 CHECK DATE: 20040703 CHECK SEVERITY: HIGH
 CHECK PARM: MARKN

APF Dataset Report

S Data Set Name	Vol	UACC	Warn	ID*	User
E SYS1.LINKLIB	ZDR17	Read	No	****	>Read
SYS1.SVCLIB	ZDR17	None	No	None	
E ISPF350.ISPLOAD	PRODAL	Read	No	****	>Read
E ISPF350.ISPLPA	PRODAL	Read	No	****	>Read
E ISPF350.ISRLPA	PRODAL	Read	No	****	>Read
E ISPF350.LPALIB	PRODAL	Read	No	****	>Read
E RACF0001.ADAU.LOAD	D94RF2	Updt	Yes	****	
RACF317.MIGLIB	D97107	****	****	****	
V RACFTTEST.RRSF.LOAD	D94RF2				


RACF Dataset Report

S Data Set Name	Vol	UACC	Warn	ID*	User
RACFDRVR.RACF317	RDB317				

* High severity Exception *

IRRH204E The RACF health check RACF_SENSITIVE_RESOURCES has found one or more potential errors in the security controls on this system.

© 2005 IBM Corporation

IBM Systems and Technology Group 

Updated SDSF Primary Option Panel

Display Filter View Print Options Help

HQX7720 ----- SDSF PRIMARY OPTION MENU -----

DA	Active users	INIT	Initiators
I	Input queue	PR	Printers
O	Output queue	PUN	Punches
H	Held output queue	RDR	Readers
ST	Status of jobs	LINE	Lines
		NODE	Nodes
LOG	System log	SO	Spool offload
SR	System requests	SP	Spool volumes
MAS	Members in the MAS		
JC	Job classes	RM	Resource monitor
SE	Scheduling environments	CK	Health checker
RES	WLM resources		

Licensed Materials - Property of IBM

5694-A01 (C) Copyright IBM Corp. 1981, 2005. All rights reserved.
 US Government Users Restricted Rights - Use, duplication or
 COMMAND INPUT ==> ck SCROLL ==> PAGE

F1=HELP	F2=SPLIT	F3=END	F4=RETURN	F5=IFIND	F6=BOOK
F7=UP	F8=DOWN	F9=SWAP	F10=LEFT	F11=RIGHT	F12=RETRIEVE

© 2005 IBM Corporation



SDSF Check Selection Panel

Display Filter View Print Options Help

```

SDSF HEALTH CHECKER DISPLAY RACFR17 LINE 11-27 (50)
NP NAME CheckOwner State Status
CNZ_TASK_TABLE IBMCNZ ACTIVE (ENABLED) SUCCES
CSV_APF_EXISTS IBMCSV ACTIVE (ENABLED) EXCEPT
CSV_LNKLST_NEWEXTENTS IBMCSV ACTIVE (ENABLED) SUCCES
CSV_LNKLST_SPACE IBMCSV ACTIVE (ENABLED) EXCEPT
GRS_CONVERT_RESERVES IBMGRS ACTIVE (DISABLED) ENV N/
GRS_EXIT_PERFORMANCE IBMGRS ACTIVE (ENABLED) SUCCES
GRS_MODE IBMGRS ACTIVE (DISABLED) ENV N/
GRS_SYNCHRES IBMGRS ACTIVE (ENABLED) SUCCES
RACF_GRS_RNL IBMRACF ACTIVE (DISABLED) ENV N/
S RACF_SENSITIVE_RESOURCES IBMRACF ACTIVE (ENABLED) EXCEPT
RSM_AFQ IBMRSM ACTIVE (ENABLED) SUCCES
RSM_HVSHARE IBMRSM ACTIVE (ENABLED) SUCCES
RSM_MAXCADS IBMRSM ACTIVE (ENABLED) SUCCES
RSM_MEMLIMIT IBMRSM ACTIVE (ENABLED) EXCEPT
RSM_REAL IBMRSM ACTIVE (ENABLED) EXCEPT
RSM_RSU IBMRSM ACTIVE (ENABLED) SUCCES
SDUMP_AUTO_ALLOCATION IBMSDUMP ACTIVE (ENABLED) EXCEPT
COMMAND INPUT ==> SCROLL ==> PAGE
F1=HELP F2=SPLIT F3=END F4=RETURN F5=IFIND F6=BOOK
F7=UP F8=DOWN F9=SWAP F10=LEFT F11=RIGHT F12=RETRIEVE
    
```



SDSF Browse Check Output Panel

Display Filter View Print Options Help

```

SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES LINE 0 COLUMNS 02- 81
COMMAND INPUT ==> SCROLL ==> PAGE
***** TOP OF DATA *****
HECK (IBMRACF,RACF_SENSITIVE_RESOURCES)
TART TIME: 10/05/2005 14:49:19.609483
HECK DATE: 20040703 CHECK SEVERITY: HIGH

APF Dataset Report

Data Set Name Vol UACC Warn ID* User
-----
ASM.SASMMOD1 ZDR17B Read No ****
ATC.V2R1M4.AUTHLIB DRVPSL
CBC.SCBCCMP ZDR17B
CBC.SCCNCMP ZDR17B None No ****
CBC.SCLBDLL ZDR17B None No ****
CBC.SCLBDLL2 ZDR17B None No ****
CEE.SCEERUN ZDR17B None No ****
CEE.SCEERUN2 ZDR17B None No ****
CRAIGJ.VTAMLIB D94RF2 Read No ****
F1=HELP F2=SPLIT F3=END F4=RETURN F5=IFIND F6=BOOK
F7=UP F8=DOWN F9=SWAP F10=LEFT F11=RIGHT F12=RETRIEVE
    
```

SDSF Browse Check Output Panel ...

Display Filter View Print Options Help

 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES LINE 87 COLUMNS 02- 81
 COMMAND INPUT ==> SCROLL ==> PAGE

RACF Dataset Report

S	Data Set Name	Vol	UACC	Warn	ID*	User
	RACFDRVR.RACF317	RDB317	None	No	***	

* High Severity Exception *

IRRH204E The RACF_SENSITIVE_RESOURCES check has found one or more potential errors in the security controls on this system.

Explanation: The RACF security configuration check has found one or more potential errors with the system protection mechanisms.

System Action: The check continues processing. There is no effect on the system.

Operator Response: Report this problem to the system security administrator and the and the system auditor.

SDSF Browse Check Output Panel ...

Display Filter View Print Options Help


 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES LINE 105 COLUMNS 02- 81
 COMMAND INPUT ==> SCROLL ==> PAGE

System Programmer Response: Examine the report that was produced by the RACF check. Any data set which has an "E" in the "S" (Status) column has excessive authority allowed to the data set. That authority may come from a universal access (UACC) or ID(*) access list entry which is too permissive, or if the profile is in WARNING mode. If there is no profile, then PROTECTALL(FAIL) is not in effect. Any data set which has a "V" in the "S" (Status) field is not on the indicated volume. Remove these data sets from the list or allocate the data sets on the volume. Any data set which has an "M" in the "S" (Status) field has been migrated.

The APF_LIBS check provides additional analysis of the non-RACF aspects of your APF list.

If the "S" field contains an "E" or is blank, then blanks in the UACC, WARN, and ID(*) columns indicate that there is no RACF

F1=HELP F2=SPLIT F3=END F4=RETURN F5=IFIND F6=BOOK
 F7=UP F8=DOWN F9=SWAP F10=LEFT F11=RIGHT F12=RETRIEVE

IBM Systems and Technology Group 

SDSF Browse Check Output Panel ...

Display Filter View Print Options Help

SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES LINE 120 COLUMNS 02- 81
 COMMAND INPUT ==> SCROLL ==> PAGE


If the "S" field contains an "E" or is blank, then blanks in the UACC, WARN, and ID(*) columns indicate that there is no RACF profile protecting the data set. Data sets which do not have a RACF profile are flagged as exceptions, unless SETROPTS PROTECTALL(FAIL) is in effect for the system.

If a valid user ID was specified as a parameter to the check, that user's authority to the data set is checked. If the user has an excessive authority to the data set, that is indicated in the USER column. For example, if the user has ALTER authority to an APF-authorized data set, the USER column contains ">Read" to indicate that the user has more than READ authority to the data set.

Problem Determination: See the RACF System Programmer's Guide and the RACF Auditor's Guide for information on the proper controls for your system.

F1=HELP	F2=SPLIT	F3=END	F4=RETURN	F5=IFIND	F6=BOOK
F7=UP	F8=DOWN	F9=SWAP	F10=LEFT	F11=RIGHT	F12=RETRIEVE

© 2005 IBM Corporation

IBM Systems and Technology Group 

SDSF Browse Check Output Panel ...

Display Filter View Print Options Help

SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES LINE 138 COLUMNS 02- 81
 COMMAND INPUT ==> SCROLL ==> PAGE

Source:
 RACF System Programmer's Guide
 RACF Auditor's Guide

Reference Documentation:
 RACF System Programmer's Guide
 RACF Auditor's Guide

Automation: None.

Check Reason: Sensitive resources should be protected.

END TIME: 10/05/2005 14:49:49.545336 STATUS: EXCEPTION-HIGH
 ***** BOTTOM OF DATA *****

F1=HELP	F2=SPLIT	F3=END	F4=RETURN	F5=IFIND	F6=BOOK
F7=UP	F8=DOWN	F9=SWAP	F10=LEFT	F11=RIGHT	F12=RETRIEVE

© 2005 IBM Corporation

z/OS Console Messages from Health Checks

```

*RACFR17 *HZS0015E PROBLEM WITH HZSPDATA DATA SET:
*DD NOT DEFINED
*RACFR17 *10 HZS0013A SPECIFY THE NAME OF AN EMPTY HZSPDATA DATA SET
$HASP003 SPECIFICATION
RACFR17 $HASP646 12.0000 PERCENT SPOOL UTILIZATION
RACFR17 HZS0001I CHECK (IBMCSV,CSV_APP_EXISTS):
CSVH0957E Some problem(s) were found with data set(s) in the APF list.
*RACFR17 *HZS0003E CHECK (IBMRACF,RACF_SENSITIVE_RESOURCES):
*IRRH204E The RACF_SENSITIVE_RESOURCES check has found one or
*more potential errors in the security controls on this system.
00 RACFR17 $HASP003 RC=(52), C
$HASP003 RC=(52),S1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
$HASP003 SPECIFICATION C
RACFR17 $HASP003 RC=(52),
$HASP003 RC=(52),T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
$HASP003 SPECIFICATION
RACFR17 $HASP650 Q,Q=W INVALID OPERAND OR MISPLACED OPERAND
RACFR17 $HASP893 VOLUME (SPOOL1) C
$HASP893 VOLUME (SPOOL1) STATUS=ACTIVE, SYSAFF=(ANY), TGNUM=175,
$HASP893 TGINUSE=21, TRKPERTGB=3, PERCENT=12
RACFR17 $HASP646 12.0000 PERCENT SPOOL UTILIZATION

IEE612I CN=C3E0S17 DEVNUM=03E0 SYS=RACFR17

```

References

- **z/OS V1R7**
 - ▶ <http://www3.ibm.com/servers/eserver/zseries/zos/bkserv/>
- **IBM Health Checker for z/OS**
 - ▶ *“An apple a day.... keeps the PMRs away! An overview of the IBM Health Checker for z/OS”*
 - z/OS Hot Topics, Issue 13, August 2005, available at http://www.ibm.com/servers/eserver/zseries/zos/bkserv/hot_topics.html
 - ▶ *“RACF and the IBM Health Checker for z/OS”*
 - ibid
 - ▶ IBM Health Checker for z/OS User’s Guide (SA22-7994)
 - <http://www.ibm.com/servers/eserver/zseries/zos/hchecker/>