

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

# | 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\*

\* 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 workdoad 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.

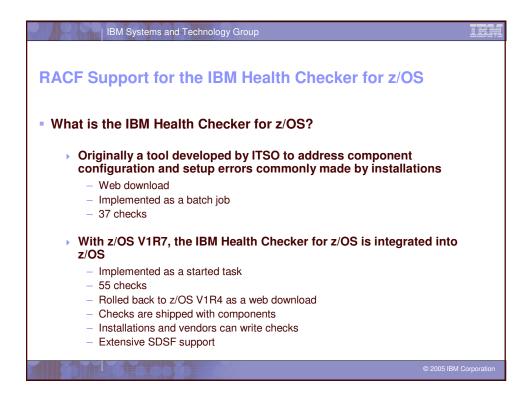
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations 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 their published announcements. IBM has not tested those products and cannot

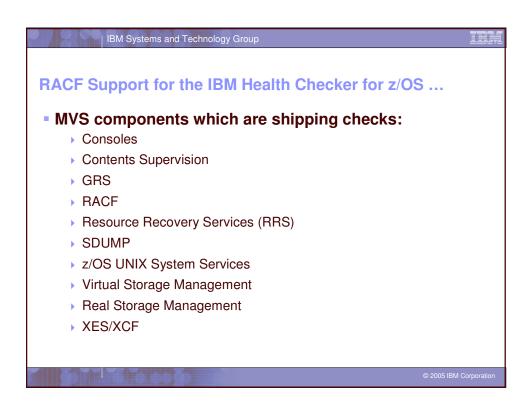
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products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

# 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 ... 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



IBM Systems and Technology Group

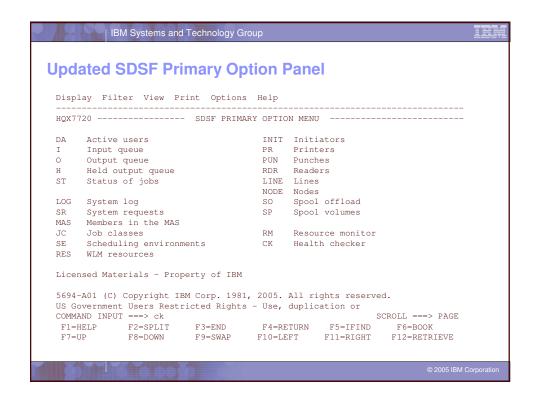
# RACF Support for the IBM Health Checker for z/OS ...

- 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

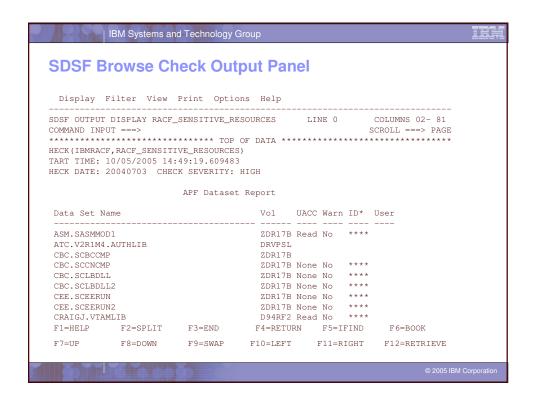
© 2005 IBM Corporation

# | IBM Systems and Technology Group 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 SERNL SYSZRACF SETROPTS E SYSZRACF SETROPTS SPEC E SYSZRAC2 IRRCRV05 SERNL SYSZRAC2 IRRCRV05 \* High severity Exception \* IRRH202E One or more RACF ENQ names were found in a GRS Resource Name List. 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. <code>IBMRACF</code> Reason: None of the RACF <code>ENQ</code> names should be in RNLs. Check parameters: $\ensuremath{\text{N/A}}$ 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
                                              _____ ZDR17 Read No **** >Read
 E SYS1.LINKLIB
   SYS1.SVCLIB
                                               ZDR17 None No None
 E ISPF350.ISPLOAD
                                               PRODAL Read No
                                                                **** >Read
                                                                **** >Read
 E ISPF350.ISPLPA
                                              PRODAL Read No
                                              PRODAL Read No **** > Read PRODAL Read No *** > Read PRODAL Read No *** > Read D94RF2 Updt Yes ****
 E ISPF350.ISRLPA
 E ISPF350.LPALIB
 E RACF0001.ADAU.LOAD
RACF317.MIGLIB
 V RACFTEST.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.
```

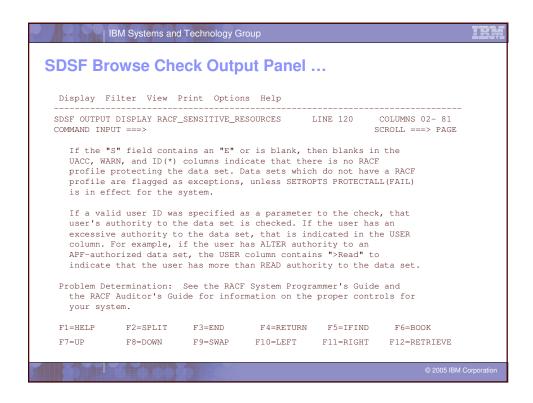


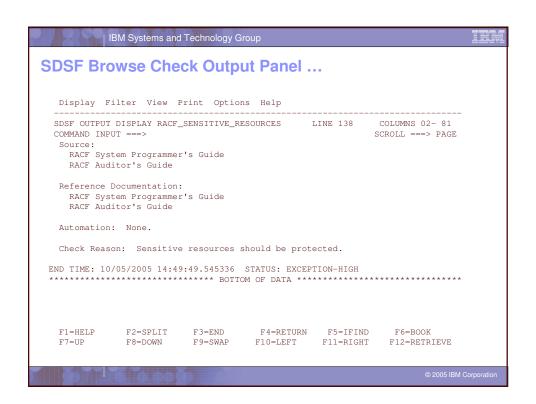
$\mathbf{D}_{\mathbf{v}}$	SF Check Selec	ction Pa	nel		
Dis	play Filter View F	rint Optic	ons Help		
 SDSF	HEALTH CHECKER DISPI	AY RACFR17	,	LINE 11-27 (50)	
NP	NAME		CheckOwner	State	Status
	CNZ_TASK_TABLE		IBMCNZ	ACTIVE (ENABLED)	SUCCES
	CSV_APF_EXISTS		IBMCSV	ACTIVE (ENABLED)	EXCEPT
	CSV_LNKLST_NEWEXTENT	'S	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_RESOU	RCES	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_ALLOCATIO	N	IBMSDUMP	ACTIVE (ENABLED)	EXCEPT
COMMAND INPUT ===>				SCROLL ==	==> PAGE
F1=	HELP F2=SPLIT	F3=END	F4=RETURN	F5=IFIND F6=B0	OOK
	UP F8=DOWN		F10=LEFT	F11=RIGHT F12=R	



# | IBM Systems and Technology Group 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 Vol UACC Warn ID\* User S Data Set Name RDB317 None No \*\*\*\* RACFDRVR.RACF317 \* 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 Operator Response: Report this problem to the system security administrator and the and the system auditor.

### | IBM Systems and Technology Group 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 ${\tt WARNING}$ mode. If there is no profile, then ${\tt PROTECTALL}\,\bar{\tt (FAIL)}$ 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 F7=UP F8=DOWN F9=SWAP F10=LEFT F11=RIGHT F12=RETRIEVE





```
***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
***SHASP003 SPECIFICATION
RACFR17 ***HASP6646 12.0000 PERCENT SPOOL UTILIZATION
RACFR17 HZS0001I CHECK (IBMCSV, CSV_APF_EXISTS):
CSVH0957E Some problem(s) were found with data set(s) in the APF list.
***RACFR17 ***HZS0003E CHECK (IBMCRCF, RACF_SENSITIVE_RESOURCES):
***IRRE204E THE RACF_SENSITIVE_RESOURCES sheek has found one or
***more potential errors in the security controls on this system.

00 RACFR17 ***SHASP003 RC=(52),
SHASP003 RC=(52), SHASP003 RC=(52), CC
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
***SHASP003 RC=(52), T1-999 - NO SELECTABLE EN
```

# | IBM Systems and Technology Group

# 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/zseris/zos/hchecker/

2005 IBM Corporation