

The IBM® Health Checker for z/OS®

RACF-2009 Jacksonville, FL

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

8 8 8 8 8 8 8 8

© 2009 IBM Corporation

IBM Systems and Technology Group



Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Agenda History of the IBM Health Checker for z/OS Structure The Health Check The RACF Health Checks

- Check "Philosophy"
- Check Output
- Installation-Defined RACF Checks
- References

© 2009 IBM Corporation

The IBM Health Checker for z/OS • What is the IBM Health Checker for z/OS? • Originally a tool developed by IBM International Technical Support Organization (ITSO) to address common configuration and setup errors • 15-20% of system outages attributed to setup and configuration • Implemented as a batch job, with 37 checks in 2003 • Delivered as a web download • With z/OS V1R7, the IBM Health Checker for z/OS is integrated into z/OS • Implemented as a started task • 55 checks with z/OS V1R1; with z/OS V1R10 130+ 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

Structure of the IBM Health Checker for z/OS

The IBM Health Checker for z/OS consists of:

IBM Systems and Technology Group

- A managing address space (the "backbone")
- ▶ The Health Checks
 - Written by individual components (such as RACF, UNIX® System Services)
 - ISVs and Installations can write their own checks
 - Can be written in System REXX, stating with z/OS V1R9
- A utility (HZSPRINT) for collecting check output
- A check is identified by a:
 - ▶ 1-32 character check name, examples of which are:
 - CSV APF EXISTS
 - GRS_CONVERT_RESERVES
 - RACF_IBMUSER_REVOKED
 - ▶ 1-16 character check owner
 - The owner for an IBM-supplied check begins with IBM, for example:
 - · IBMCSV, IBMGRS, and IBMRACF

© 2009 IBM Corporation

IBM Systems and Technology Group

The Health Check

- Each check (usually) represents a single "best practice", which comes from:
 - Product documentation
 - ▶ The z/OS System Test organization
 - ▶ The z/OS Service Team
 - The Parallel Sysplex Availability Checklist
 - ▶ ITSO Redbooks
 - Washington System Center Flashes
- When migrating to z/OS V1R10, you can use the IBM migration checks to help you analyze your system and identify activities to complete when migrating.

IBM Systems and Technology Group

iri

The Health Check...

- Associated with each check is information about its execution:
 - Execution state:
 - ACTIVE or INACTIVE
 - How often the check runs
 - ONETIME, hh:mm
 - The severity of the check, which influences how check output is issued
 - HIGH, MEDIUM, LOW, NONE
 - ▶ WTOTYPE
 - CRITICAL, EVENTUAL, INFORMATIONAL, HARDCOPY, NONE
- Some checks accept parameters which direct the processing of the check or set thresholds
- Check information is set by the check writer, but can be changed by the installation by:
 - Policy statements in the HZSPRMxx member of PARMLIB
 - MVS MODIFY Command (F HC)

© 2009 IBM Corporation

| IBM Systems and Technology Group



Health Checks...

- The IBM Health Checker for z/OS is dynamic. That is, health checks:
 - Are separately packaged and shipped
 - Do not have to be predefined
 - Check writers must merely register with the HZSADDCHECK MVS dynamic exit point
 - ▶ Can be added after the startup of the Health Checker "backbone"
 - Can have their characteristics changed by either MVS command or PARMLIB
 - Do not execute if the IBM Health Checker for z/OS is not active
- IBM is adding new checks in new releases and in the service stream
 - To get the most recent checks, use the Enhanced Preventative Service Planning (PLP) tool

Health Checks... • MVS components have shipped over 130 checks: • Consoles • Contents Supervision • GRS • RACF • Resource Recovery Services (RRS) • SDUMP • z/OS UNIX System Services • Virtual Storage Management • Real Storage Management • XES/XCF

The RACF Health Checks... RACF ships these Health Checks: RACF_GRS_RNL 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 Defaults: Severity(High) Interval(08:00) RACF_SENSITIVE_RESOURCES Looks at the current APF data sets, PARMLIB, the System REXX data sets, LINKLIST, and the RACF database data sets and flags those that are improperly protected Are not found on the indicated volume Are improperly protected Examines key system general resources Severity(High) Interval(08:00)

IBM Systems and Technology Group

ier

The RACF Health Checks...

- Checks introduced with z/OS V1R8
 - **▶ RACF_IBMUSER_REVOKED**
 - Verifies that the user ID IBMUSER is revoked
 - Defaults: Severity(Medium), Interval(24:00)
 - RACF_<class-name>_ACTIVE
 - Verifies that the class <class-name> is active
 - Check is performed for FACILITY, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, UNIXPRIV
 - Defaults: Severity(Medium), Interval(24:00)

© 2009 IBM Corporation

IBM Systems and Technology Group



The RACF Health Checks...

- Checks introduced with z/OS V1R10:
 - **▶ ICHAUTAB checks:**
 - For over 20 years, IBM has recommended not using the RACF Authorized Caller Table (ICHAUTAB)
 - RACF introduces a new check to verify that ICHAUTAB is not being used
 - RACF_ICHAUTAB_NONLPA raises a SEV(MED) exception if a non-LPA resident ICHAUTAB is found
 - Severity(Medium), Interval(24:00)
 - The existing RACF_SENSITIVE_RESOURCES raises a SEV(HIGH) exception if an LPA-resident ICHAUTAB is found
 - The "installation-defined resource" check which allows you to define the resources that you want to check



Check Output

- The output of a check consists of:
 - Write to Operator messages (WTO)s, which are written with the routing codes and descriptor codes associated with the check
 - Messages written to the Health Check message buffer, which can be:
 - Kept in storage (most recent check invocation only)
 - Written to a log stream
- Check output can be processed with:
 - SDSF, using the "CK" panels
 - Using the HZSPRINT utility

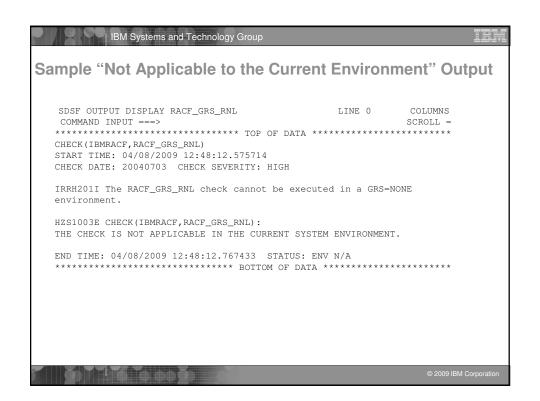
© 2009 IBM Corporation

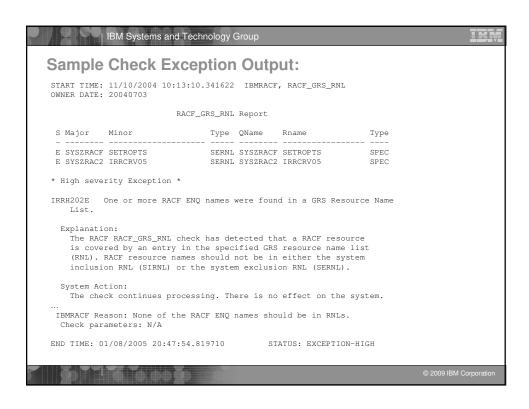
IBM Systems and Technology Group



Check "Philosophy"

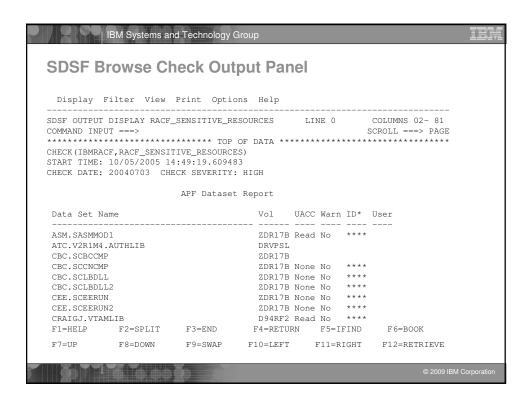
- Checks which are not applicable to the current environment place themselves in a "not applicable" status and will not run unless triggered.
- Health Checks raise exceptions and make recommendations, <u>but they do not automatically take</u> any actions
 - You must review the recommendation and ensure that it is appropriate for your environment
- When an exception is found, Health Checks present the entire message information, including the "explanation", "systems programmer response", etc., along with pointers to relevant documentation.
- Checks which find no exception clearly state that no exception was found.



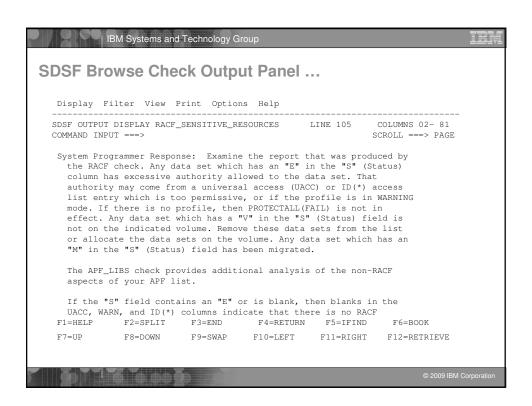


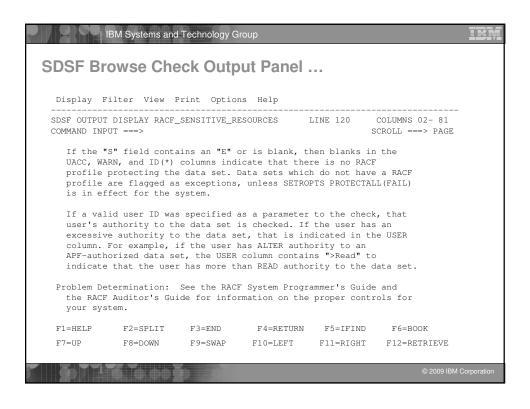
HQX7	720 SDSF PR	IMARY OPTIC	N MENU	
DA	Active users	INIT	Initiators	
I	Input queue	PR	Printers	
	Output queue	PUN	Punches	
	Held output queue	RDR	Readers	
ST	Status of jobs	LINE	Lines	
	3	NODE	Nodes	
LOG	System log	SO	Spool offload	
SR	2	SP	Spool volumes	
MAS	Members in the MAS		1	
JC	Job classes	RM	Resource monitor	
SE	Scheduling environments	CK	Health checker	
	WLM resources			
Lice	nsed Materials - Property of II		All rights reserved.	

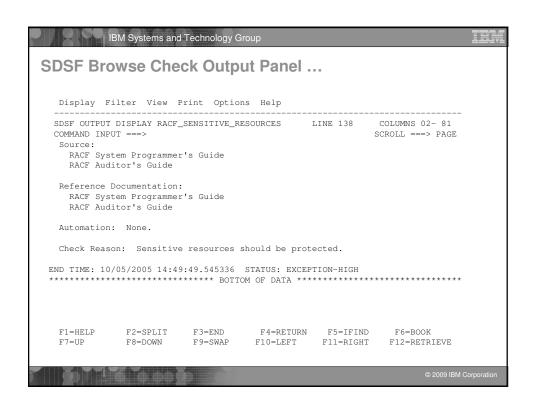
DS	SF Ch	eck Sele	ction Pa	nel			
Dis	play F	ilter View	Print Optio	ons Help			
 SDSF	HEALTH	CHECKER DISP	LAY RACFR1	 7	LINE 11-	 27 (50)	
NP	NAME		CheckOwner	State		Status	
	CNZ_TA	SK_TABLE		IBMCNZ	ACTIVE (ENABLED)		SUCCES
	CSV_APF_EXISTS				ACTIVE (ENABLED)		EXCEPT
	CSV_LNKLST_NEWEXTENTS			IBMCSV	ACTIVE (ENABLED)		SUCCES
	CSV_LN	KLST_SPACE		IBMCSV	ACTIVE (ENABLED)		
	GRS_CONVERT_RESERVES		IBMGRS	ACTIVE (DISABLED)			
	GRS_EXIT_PERFORMANCE		IBMGRS	ACTIVE (EN	ABLED)	SUCCES	
	GRS_MODE			IBMGRS	ACTIVE (DISABLED)		ENV N/
	GRS_SYNCHRES			IBMGRS	ACTIVE (ENABLED)		
	RACF_G	RS_RNL		IBMRACF	ACTIVE (DI	SABLED)	ENV N/
S	RACF_SENSITIVE_RESOURCES			IBMRACF	ACTIVE (EN		
	RSM_AFQ			IBMRSM	ACTIVE (EN		
	RSM_HVSHARE			IBMRSM	ACTIVE (ENABLED)		
	RSM_MAXCADS			IBMRSM	ACTIVE (ENABLED)		
	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	
COMM	AND INP	UT ===>			S	CROLL ==	=> PAGE
F1=	HELP	F2=SPLIT	F3=END	F4=RETURN	F5=IFIND	F6=BO	OK
F7=	UP	F8=DOWN	F9=SWAP	F10=LEFT	F11=RIGHT	F12=RE	TRIEVE



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 S Data Set Name Vol UACC Warn ID* User 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 the system. Operator Response: Report this problem to the system security administrator and the and the system auditor.







```
IBM Systems and Technology Group
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 HZS00011 CHECK(IBMCSV,CSV_APF_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),
$HASP003 RC=(52),$1-999 - NO SELECTABLE ENTRIES FOUND MATCHING
        $HASP003
                              SPECIFICATION
        SHASPOUS OFFICE COLUMN SHASPOOR RC=(52), SHASPOOR RC=(52), T1-999 - NO SELECTABLE ENTRIES FOUND MATCHING SHASPOOR SPECIFICATION
        SHASPOOD NO (C2.,)

SHASPOOD SPECIFICATION
RACFR17 SHASP650 Q,Q=W INVALID OPERAND OR MISPLACED OPERAN
RACFR17 SHASP893 VOLUME(SPOOL1)

SHASP893 VOLUME(SPOOL1) STATUS=ACTIVE,SYSAFF=(ANY),TGNUM=175,
TGINUSE=21,TRKPERTGB=3,PERCENT=12
                                            INVALID OPERAND OR MISPLACED OPERAND
        RACFR17 $HASP646 12.0000 PERCENT SPOOL UTILIZATION
   IEE612I CN=C3E0S17 DEVNUM=03E0 SYS=RACFR17
```

| IBM Systems and Technology Group

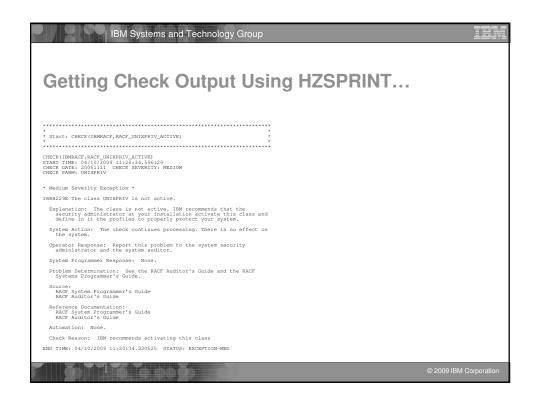
Getting Check Output Using HZSPRINT

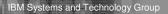
- The HZSPRNT utility extracts check output from either the in-storage buffers or the logstream
 - PARM= allows filtering based on check owner and check name:

```
//MARKNHC3 JOB 'D5202P,?','M.NELSON',MSGLEVEL=(1,1),NOTIFY=&SYSUID,
// CLASS=A,MSGCLASS=H,REGION=19M
//RACFCKS EXEC PGM=HZSPRNT,PARM='CHECK(IBMRACF,*)'
//SYSOUT DD SYSOUT=*,DCB=LRECL=256
```

... shows all of the checks which have "IBMRACF" as the owner

IBM Systems and Technology Group		IBM
Getting Check Output Usin	na H7SPRINT	
dotting oncon output con	19 11201 111111111	
***************************************	*****	
* HZSPRINT (HBB7730-06024) 2009/04/10 11:23	*	
* HZSU001I Check messages * Sysplex: LOCAL System: SY1	*	
* * Filter: CHECK(IBMRACF,*)	*	
* ************************************	*	
***************************************	*****	
* Start: CHECK(IBMRACF,ZOSMIGV1R9_RACF_PASSWRD_ENVELOPE)	*	
***************************************	*****	
***************************************	*****	
* No messages exist	*	
*************************************	*****	
***************************************	*****	
* End: CHECK(IBMRACF,ZOSMIGV1R9_RACF_PASSWRD_ENVELOPE)	*	
***************************************	*****	
		© 2009 IBM Corporation







Authorization Checking

- The IBM Health Checker for z/OS performs authorization checks in the XFACILIT class
 - The eXtended FACILITy class
 - Member class for the GXFACILI class
 - Resource name of up to 246 characters
 - Shared POSIT value with the FACILITY class
 - The resource names that are checked, depending on the type of output which is being accessed are:
 - READ authority to HZS.sysname.QUERY
 - READ authority to HZS.sysname.check-owner.QUERY
 - READ authority to HZS.sysname.check-owner.MESSAGES
 - READ authority to HZS.sysname.check-owner.check-name.MESSAGES
 - See "Setting up security for the HZSPRNT utility" in the "IBM Health Checher for z/OS User's Guide" for details.

© 2009 IBM Corporation

IBM Systems and Technology Group



Installation

- The steps for installing the IBM Health Checker for z/OS are:
 - 1. Allocate the HZSPDATA data set
 - HZSPDATA is used to save data between executions of a check
 - 2. Create the RACF definitions
 - Assign the Health Checker started task a user ID which has UID(0), HOME('/') and PROGRAM('bin/sh')
 - Give the user ID above UPDATE authority to the HZSPDATA data set and READ authority to the PARMLIB data sets
 - If you are using a log stream for the check output define the LOGSTRM resources required to allow the Health Checker to connect and write to the log stream.
 - 3. Start the Health Checker address

IBM Systems and Technology Group

Installation-Defined RACF Health Checks in z/OS V1R10

- The current RACF checks examine key elements of the z/OS infrastructure, but:
 - The checks look at the resources IBM thinks are important
 - Unless you wrote your own check you can't examine the protection of your data resources
- With z/OS V1R10, you can check the protection of the resources you want simply by defining profiles and registering your check with the IBM Health Checker for z/OS

© 2009 IBM Corporation

| IBM Systems and Technology Group



Installation-Defined RACF Health Checks...

- Defining your own resource check takes these three steps:
 - Defining a RACF profile in the new RACFHC general resource class. This profile contains the list of resources that you want to check
 - 2. Define a PARMLIB entry that defines your check using the IBM Health Checker for z/OS Dynamic Registration
 - 3. Activate your PARMLIB entry

Installation-Defined RACF Health Checks...

IBM Systems and Technology Group

The RACFHC class contains profiles which have the resources you want to check. The RDEFINE command to add a profile is:

RDEFINE RACFHC MY_RESOURCE_LIST

ADDMEM (DATASET/PROD.VALUABLE.DATA/ZDR17B/NONE

DATASET/SEC.FILING.FORMS//NONE

RACFHC/MY RESOURCE LIST//NONE)

The ADDMEM field defines the resources that you want checked. The format is:

className/resourceName/volume/maximumPublicAccess

- className is any valid RACF class
- resourceName is a resources name within the class
- Volume is the volume serial for a DATASET resource, otherwise no value should be specified
- maximumPublicAccess is the access level which if exceeded results in an exception. Valid values are NONE, READ, UPDATE, and CONTROL.

© 2009 IBM Corporation

IBM Systems and Technology Group

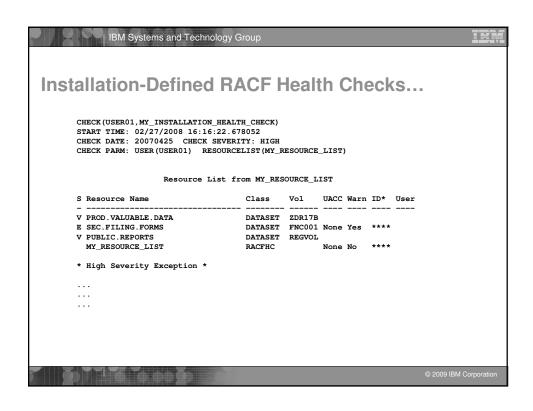
Installation-Defined RACF Health Checks...

- In addition to defining resources in the ADDMEM value, you can specify one or more IBM-defined report sets. These report sets are:
 - ▶ IRR_APFLIST: APF data set list
 - ▶ IRR LINKLIST: Current link list data set list
 - ▶ IRR_PARMLIB: Current PARMLIB data set list
 - ▶ IRR_RACFDB: Data sets which comprise the RACF data base
 - ▶ IRR_SYSREXX: System REXX data set
 - ▶ IRR_ICHAUTAB: ICHAUTAB entries
- Sample profile definition for a pre-defined set of resources

RDEFINE RACFHC MY_SYSTEM_STUFF
ADDMEM(DATASET/SYS1.SAMPLIB//READ
IRR_APFLIST
IRR_RACFDB)

IBM Systems and Technology Group Installation-Defined RACF Health Checks... A Health Checker PARMLIB statement is used to define your check, set its characteristics (such as the interval, severity), and associate the check with the RACFHC profile which contains the resources you want checked ADD CHECK (USER01, MY_INSTALLATION_HEALTH_CHECK) CHECKROUTINE (IRRHCR00) MESSAGETABLE (IRRHCM00) ENTRYCODE (100) PARM('USER(USER01) RESOURCELIST(MY_RESOURCE_LIST)') DATE (yyyymmdd) REASON ('My sensitive resources') GLOBAL ACTIVE SEVERITY (HIGH) **INTERVAL (**08:00)

IBM Systems and Technology Group Installation-Defined RACF Health Checks... The final step is to activate your check. After adding it to a member (HZSPRMMN in this example) activate the PARMLIB entry using the MVS modify command for the Health Checker address space: F HC, ADD, PARMLIB=MN Your check is now registered with the IBM Health Checker for z/OS! Display Filter View Print Options Help SDSF HEALTH CHECKER DISPLAY RACFR1B LINE 38-53 (92) CheckOwner State Status MY_INSTALLATION_HEALTH_CHECK USER01 ACTIVE (ENABLED) PDSE SMSPDSE1 TRMPDSE ACTIVE (ENABLED) EXCEPT RACF FACILITY ACTIVE IBMRACF ACTIVE (ENABLED) SUCCES RACF_GRS_RNL IBMRACF ACTIVE (DISABLED) ENV N/



IBM Systems and Technology Group References IBM Health Checker for z/OS User's Guide (SA22-7994) http://www.ibm.com/servers/eserver/zseris/zos/hchecker/ IBM Education Assistant http://www-01.ibm.com/software/info/education/assistant/ The IBM Health Checker for z/OS web site http://www.ibm.com/systems/z/os/zos/hchecker/ A list of all of the IBM-supplied checks can be foun at: http://wwwibm.com/systems/z/os/zos/hchecker/check_table.html "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" "Personalize your RACF Checking with the IBM Health Checker for z/OS" z/OS Hot Topics, Issue 19, August 2008, available at http://www.ibm.com/servers/eserver/zseries/zos/bkserv/hot_topics.html