

IBM Systems and Technology Group

IBM

The RACF® Checks for the IBM® Health Checker for z/OS®

RACF-2012
Session AST14
June 2012

SEARCH INSIDE!™

Mainframe Basics for Security Professionals
Getting Started with RACF
Dr. Premraj, Suresh Kumar Shrivastava, Mark Nelson, Teri Yule

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

© 2012 IBM Corporation

IBM Systems and Technology Group

IBM

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.

© 2012 IBM Corporation

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
- New RACF Checks
- References

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 was 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:**
 - ▶ 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, starting 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

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 a new release of z/OS, you can use the IBM migration checks to help you analyze your system and identify activities to complete when migrating.**

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)

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)

The RACF Health Checks...

- **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)

The RACF Health Checks...

- **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**

- **New checks with V1.13:**
 - ▶ RACF_AIM_STAGE
 - ▶ RACF_UNIX_ID
 - ▶ ZOSMIGV2R1_DEFAULT_UNIX_ID

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

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, *but they do not automatically take 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.**

Sample “No Exception” Output

```

SDSF OUTPUT DISPLAY RACF_OPERCMDS_ACTIVE          LINE 0
COMMAND INPUT ==>
***** TOP OF DATA *****
CHECK(IBMRAF,RACF_OPERCMDS_ACTIVE)
START TIME: 04/08/2009 12:48:12.764702
CHECK DATE: 20051111  CHECK SEVERITY: MEDIUM
CHECK PARM: OPERCMDS

IRRH228I The class OPERCMDS is active.

END TIME: 04/08/2009 12:48:12.767783  STATUS: SUCCESSFUL
***** BOTTOM OF DATA *****

```

Sample “Not Applicable to the Current Environment” Output

```

SDSF OUTPUT DISPLAY RACF_GRS_RNL                  LINE 0          COLUMNS
COMMAND INPUT ==>                                SCROLL =
***** TOP OF DATA *****
CHECK(IBMRAF,RACF_GRS_RNL)
START TIME: 04/08/2009 12:48:12.575714
CHECK DATE: 20040703  CHECK SEVERITY: HIGH

IRRH201I The RACF_GRS_RNL check cannot be executed in a GRS=NONE
environment.

HZS1003E CHECK(IBMRAF,RACF_GRS_RNL):
THE CHECK IS NOT APPLICABLE IN THE CURRENT SYSTEM ENVIRONMENT.

END TIME: 04/08/2009 12:48:12.767433  STATUS: ENV N/A
***** BOTTOM OF DATA *****

```


Sample Check Exception 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	IRRRCRV05	SERNL	SYSZRAC2	IRRRCRV05	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 STATUS: EXCEPTION-HIGH

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

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_APPF_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 *****
CHECK (IBMRACF,RACF_SENSITIVE_RESOURCES)
START TIME: 10/05/2005 14:49:19.609483
CHECK 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

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

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

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 APP list.
*RACFR17 *HZS0003E CHECK(IBMRAF,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 C
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

```

Getting Check Output Using HZSPRINT

- **The HZSPRINT 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=HZSPRINT,PARM='CHECK(IBMRAF,*)'
//SYSOUT DD SYSOUT=*,DCB=LRECL=256

```

- ▶ ... shows all of the checks which have "IBMRAF" as the owner

Getting Check Output Using HZSPRINT...

```

*****
* HZSPRINT (HBB7730-06024) 2009/04/10 11:23
*
* HZSU001I Check messages
* Sysplex: LOCAL System: SY1
* Filter: CHECK(IBMRAF,*)
*****

*****
* Start: CHECK(IBMRAF,ZOSMIGVIR9_RACF_PASSWRD_ENVELOPE)
*****

*****
* No messages exist
*****

*****
* End: CHECK(IBMRAF,ZOSMIGVIR9_RACF_PASSWRD_ENVELOPE)
*****

```

Getting Check Output Using HZSPRINT...

```

*****
* Start: CHECK(IBMRAF,RACF_UNIXPRIV_ACTIVE)
*****

CHECK(IBMRAF,RACF_UNIXPRIV_ACTIVE)
START TIME: 04/10/2009 11:20:34.596129
CHECK DATE: 20051111 CHECK SEVERITY: MEDIUM
CHECK PARM: UNIXPRIV

* Medium Severity Exception *
IRRH229E The class UNIXPRIV is not active.

Explanation: The class is not active. IBM recommends that the
security administrator at your installation activate this class and
define in it the profiles to properly protect your system.

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 system auditor.

System Programmer Response: None.

Problem Determination: See the RACF Auditor's Guide and the RACF
Systems Programmer's Guide.

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: IBM recommends activating this class
END TIME: 04/10/2009 11:20:34.930525 STATUS: EXCEPTION-MED

```

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 Checker for z/OS User’s Guide” for details.

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')
 - With z/OS V1R12, you can use BPX.SUPERUSER instead of UID(0)
 - 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 space

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**

Installation-Defined RACF Health Checks...

- **Defining your own resource check takes these three steps:**
 1. 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...

- 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.

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)
```

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)
```

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)
NP NAME CheckOwner State Status
MY_INSTALLATION_HEALTH_CHECK USER01 ACTIVE(ENABLED) EXCEPT
PDSE_SMPDSE1 IBMPDSE ACTIVE(ENABLED) EXCEPT
RACF_FACILITY_ACTIVE IBMRACF ACTIVE(ENABLED) SUCCES
RACF_GRS_RNL IBMRACF ACTIVE(DISABLED) ENV N/
```

Installation-Defined RACF Health Checks...

```
CHECK(USER01,MY_INSTALLATION_HEALTH_CHECK)
START TIME: 02/27/2008 16:16:22.678052
CHECK DATE: 20070425 CHECK SEVERITY: HIGH
CHECK PARM: USER(USER01) RESOURCELIST(MY_RESOURCE_LIST)
```

Resource List from MY_RESOURCE_LIST

S	Resource Name	Class	Vol	UACC	Warn	ID*	User
V	PROD.VALUABLE.DATA	DATASET	ZDR17B				
E	SEC.FILING.FORMS	DATASET	FNC001	None	Yes	****	
V	PUBLIC.REPORTS	DATASET	REGVOL				
	MY_RESOURCE_LIST	RACFHC		None	No	****	

* High Severity Exception *

...
...
...

z/OS V1.13: Health Check – AIM Stage

- **The RACF_AIM_STAGE Health Check examines your application identity mapping (AIM) setting and flags as an exception if you are at a stage less than stage 3.**
 - Stage 0: No AIM support; only mapping profiles are used
 - Stage 1: Mapping profiles are used; alternate index created and managed, but not used
 - Stage 2: Alternate index create, managed, and used; mapping profiles maintained.
 - Stage 3: Only alternate index maintained and used. Mapping profiles deleted.
- **Moving from each stage requires the execution of the IRRIRA00 utility.**
- **AIM stage 2 or stage 3 is needed for certain RACF functions**

z/OS V1.13: Health Check – AIM Stage (OK)

```

Display Filter View Print Options Search Help
-----
SDSF OUTPUT DISPLAY RACF_AIM_STAGE          LINE 0          COLUMNS 02- 81
COMMAND INPUT ==>                          SCROLL ==> HALF
***** TOP OF DATA *****
CHECK(IBMRAF,RACF_AIM_STAGE)
START TIME: 05/11/2012 14:36:29.892717
CHECK DATE: 20110101 CHECK SEVERITY: MEDIUM

IRRH500I The RACF database is at the suggested stage of application
identity mapping (AIM). The database is at AIM stage 03.

END TIME: 05/11/2012 14:36:29.893680 STATUS: SUCCESSFUL
***** BOTTOM OF DATA *****

```

z/OS V1.13: Health Check – AIM Stage (Exception)

```

Display Filter View Print Options Search Help
-----
SDSF OUTPUT DISPLAY RACF_AIM_STAGE          LINE 0          COLUMNS 02- 81
COMMAND INPUT ==>                          SCROLL ==> HALF
***** TOP OF DATA *****
CHECK(IBMRAF,RACF_AIM_STAGE)
START TIME: 05/17/2012 16:42:53.891503
CHECK DATE: 20110101 CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH501E The RACF database is not at the suggested stage of application
identity mapping (AIM). The database is at AIM stage 00.

Explanation: The RACF_AIM_STAGE check has determined that the RACF
database is not at the suggested stage of application identity
mapping (AIM). Your system programmer can convert your RACF database
using the IRRIRA00 conversion utility. See z/OS Security Server RACF
System Programmer's Guide for information about running the
IRRA00 conversion utility.

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

```

z/OS V1.13: Health Check – UNIX ID

- **The RACF_UNIX_ID Health Check determines whether RACF will automatically assign unique z/OS UNIX System Services identities when users without OMVS segments use certain UNIX services**
 - If you are not relying on RACF to assign UIDs and GIDs, the check informs you that you must continue to assign z/OS UNIX identities
 - If you are relying on the BPX.DEFAULT.USER support, the check issues an exception
 - If you are relying on the BPX.UNIQUE.USER support, the check will verify requirements and indicate if any exceptions are found
 - FACILITY class profile BPX.UNIQUE.USER must exist
 - RACF database must be at Application Identity Mapping (AIM) stage 3
 - UNIXPRIV class profile SHARED.IDS must be defined
 - UNIXPRIV class must be active and RACLISTed
 - FACILITY class profile BPX.NEXT.USER must be defined and its APPLDATA field must contain valid ID values or ranges
 - Note: The check only lists the APPLDATA content, it does not validate it.

z/OS V1.13: Health Check – UNIX ID (OK)

```

Display Filter View Print Options Search Help
-----
SDSF OUTPUT DISPLAY RACF_UNIX_ID          LINE 0          COLUMNS 02- 81
COMMAND INPUT ==>                          SCROLL ==> HALF
***** TOP OF DATA *****
CHECK(IBMRA CF,RACF_UNIX_ID)
START TIME: 05/18/2012 13:56:53.321238
CHECK DATE: 20110101 CHECK SEVERITY: MEDIUM

IRRH504I RACF is not enabled to assign UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services. If you
choose not to define UNIX IDs for each user of UNIX functions, you can
enable RACF to automatically generate unique UNIX UIDs and GIDs for you.

END TIME: 05/18/2012 13:56:53.322242 STATUS: SUCCESSFUL
***** 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

```

z/OS V1.13: Health Check – UNIX ID (OK)

```
***** TOP OF DATA *****
CHECK(IBMRA CF,RACF_UNIX_ID)
START TIME: 05/18/2012 14:12:18.914396
CHECK DATE: 20110101 CHECK SEVERITY: MEDIUM

IRRH502I RACF attempts to assign unique UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services.

Requirements for this support:

S Requirement
-----
FACILITY class profile BPX.UNIQUE.USER is defined
RACF database is at the required AIM stage:
  AIM stage = 03
UNIXPRIV class profile SHARED.IDS is defined
UNIXPRIV class is active
UNIXPRIV class is RACLIS T ed
FACILITY class profile BPX.NEXT.USER is defined
BPX.NEXT.USER profile APPLDATA is specified (not verified):
  APPLDATA = 1000/100

IRRH506I The RACF UNIX identity check has detected no exceptions.

END TIME: 05/18/2012 14:12:18.921241 STATUS: SUCCESSFUL
```

z/OS V1.13: Health Check – UNIX ID (Exception)

```
Display Filter View Print Options Search Help
-----
SDSF OUTPUT DISPLAY RACF_UNIX_ID LINE 0 COLUMNS 02- 81
COMMAND INPUT ==> SCROLL ==> HALF
***** TOP OF DATA *****
CHECK(IBMRA CF,RACF_UNIX_ID)
START TIME: 05/17/2012 16:45:01.400010
CHECK DATE: 20110101 CHECK SEVERITY: MEDIUM

IRRH502I RACF attempts to assign unique UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services.

Requirements for this support:

S Requirement
-----
FACILITY class profile BPX.UNIQUE.USER is defined
E RACF database is not at the required AIM stage:
  AIM stage = 00
E UNIXPRIV class profile SHARED.IDS is not defined
E UNIXPRIV class is not active
E UNIXPRIV class is not RACLIS T ed
E FACILITY class profile BPX.NEXT.USER is not defined

* Medium Severity Exception *

IRRH503E RACF cannot assign unique UNIX IDs when users or groups that
do not have OMVS segments use certain z/OS UNIX services. One or more
requirements are not satisfied.

Explanation: The RACF UNIX identity check has determined that you
want RACF to assign unique UNIX IDs when users or groups without
OMVS segments use certain z/OS UNIX services. However, RACF is not
able to assign unique UNIX identities for z/OS UNIX services because
one or more of the following requirements are not satisfied:
```

z/OS V1.13: Health Check – UNIX ID (Exception)

```
***** TOP OF DATA *****
CHECK(IBMRAF,RACF_UNIX_ID)
START TIME: 05/18/2012 14:22:52.066301
CHECK DATE: 20110101 CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH505E The BPX.DEFAULT.USER profile in the FACILITY class
indicates that you want RACF to assign shared default UNIX
IDs when users or groups that do not have OMVS segments use
certain z/OS UNIX services.

Explanation: The RACF UNIX identity check has found the
BPX.DEFAULT.USER profile in the FACILITY class. The presence of this
profile indicates an intent to have RACF assign shared default UNIX
UIDs and GIDs when users without OMVS segments access the system to
use certain UNIX services.
Reference Documentation:
z/OS Security Server RACF Security Administrator's Guide

Automation: None.

Check Reason: Unique UNIX identities are recommended.

END TIME: 05/18/2012 14:22:52.067783 STATUS: EXCEPTION-MED
```

z/OS V1.13: Health Check – Default UNIX ID

```
Display Filter View Print Options Search Help
-----
SDSF OUTPUT DISPLAY ZOSMIGV2R1_DEFAULT_UNIX_ID LINE 0 COLUMNS 02- 81
COMMAND INPUT ==> SCROLL ==> HALF
***** TOP OF DATA *****
CHECK(IBMRAF,ZOSMIGV2R1_DEFAULT_UNIX_ID)
START TIME: 05/11/2012 14:38:04.920543
CHECK DATE: 20110101 CHECK SEVERITY: LOW

IRRH504I RACF is not enabled to assign UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services. If you
choose not to define UNIX IDs for each user of UNIX functions, you can
enable RACF to automatically generate unique UNIX UIDs and GIDs for you.

END TIME: 05/11/2012 14:38:04.921996 STATUS: SUCCESSFUL
***** BOTTOM OF DATA *****
```

- **This is a migration check!**
 - Note the name: ZOSMIGV2R1.....This check is to prepare you to identify issues when you migrate to z/OS V2.1
 - Shipped INACTIVE; you activate when you start your V2.1 migration planning

z/OS V1.13: Health Checks

- **These three new health checks (two “best practice” and one “migration”) are shipped in APAR OA37164**
 - ▶ V1.12: PTF UA64936
 - ▶ V1.13: PTF UA64937

References

- **IBM Health Checker for z/OS User's Guide (SA22-7994)**
 - ▶ <http://www.ibm.com/servers/eserver/zseries/zos/hchecker/>
- **Exploiting the IBM Health Checker for z/OS Infrastructure**
 - ▶ <http://www.redbooks.ibm.com/abstracts/redp4590.html?Open>
- **IBM Education Assistant**
 - ▶ <http://www.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 found at:
 - ▶ http://www.ibm.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”***
 - ▶ *ibid*
- ***“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