

“Check, please!”

RACF and IBM Health Checker for z/OS

BY MARK NELSON

IBM Health Checker for z/OS provides a wonderful framework into which IBM components can plug their product specific checks. RACF® is just one of the many z/OS elements that are taking advantage of this framework to help ensure the proper configuration of your z/OS environment.

RACF now provides two checks for the IBM Health Checker for z/OS environment:

- RACF_GRS_RNL looks at the global resource serialization resource name list (RNL) that is in use to ensure that they won't affect RACF's serialization. This check is available with APAR OA11833 for z/OS V1R6 and later.
- RACF_SENSITIVE_RESOURCES examines the RACF definitions for your APF-authorized data sets and your RACF database for a proper baseline set of protections. This check is available with be APAR OA11833 for z/OS V1R4 and later.

RACF_GRS_RNL

When RACF accesses its database, it has to ensure that its data retrieval and update process is not affected by accesses to the RACF database from other systems that are sharing the database. RACF does this by serializing its database access using global resource serialization's RESERVE, ENQ, and DEQ services. Global resource serialization provides many facilities for installations to monitor, control, and even modify these serialization requests. For example, you can change the scope of an ENQ from one that is for all of the systems in your sysplex (SCOPE=SYSTEMS ENQ) to one that affects only the system on which the ENQ is issued (SCOPE=SYSTEM). You change the scope of an ENQ with an entry in an RNL.

RACF is critically dependent on the proper serialization of its activities. In many cases, changing the scope of an ENQ is a good thing to do, but you have to be careful when specifying an RNL because you may experience undesirable

results, such as a corruption of your RACF database. Database damage caused by improper serialization is often hard to debug because the symptoms of the corruptions depend on factors such as:

- What type of serialization was being used?
- What else was occurring on each of the systems that were sharing the RACF database?

The RACF_GRS_RNL check compares your RNLs to the ENQs that RACF performs. If the check finds an RNL entry that affects a RACF ENQ, the check raises a SEVERITY(HIGH) exception. The output of the check includes the major and minor name of the RACF ENQ, the type of serialization, and the QNAME, RNAME, and type of the RNL entry.

The check is marked as “not applicable” in a system running with GRS=NONE.

Figure 1 shows a sample output of the RACF_GRS_RNL check when the check has found an exception.

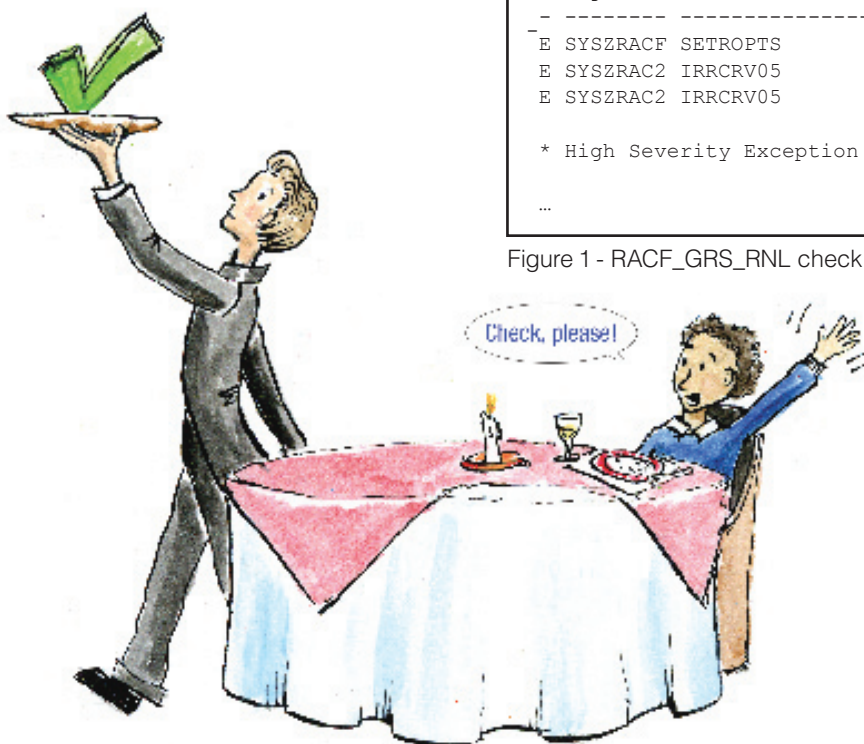
```
1CHECK (IBMRACF,RACF_GRS_RNL)
START TIME: 04/14/2005 08:53:27.899234
CHECK DATE: 20040703 CHECK SEVERITY: HIGH

                                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
E SYSZRAC2  IRRCRV05             SIRNL SYSZRAC2  IRRCRV05   SPEC

* High Severity Exception *
...
```

Figure 1 - RACF_GRS_RNL check output



RACF_SENSITIVE_RESOURCES

RACF_SENSITIVE_RESOURCES check examines your current APF libraries and the data sets that make up your RACF database. For each data set, the check will:

- Determine if the data set is on the expected volume
- Find the RACF profile covering the data set
- Examine the profile to see if it provides a minimal protection for the data set.

You can optionally supply a user ID to the check. If you do, the check tests the specified user's access to each data set.

The check indicates an exception by placing a "V" or "E" in the status ("S") column. An exception occurs if:

- The data set is not on the indicated volume (a "V" exception)
- There is no RACF profile protecting the resource and PROTECTALL(FAIL) is not in effect (an "E" exception)
- There is a RACF profile protecting the resource and one or more of the following is true:
 - UACC of the profile is greater than that which is recommended
 - The user ID "*" is on the access list with an access greater than what is recommended
 - The user ID that you specified has more access authority than what is recommended
 - The profile is in WARNING mode.

If the check finds an undefined or unprotected data set, the check raises a SEVERITY(HIGH) exception. Figure 2 shows the output of the check.

Activating the checks

During RACF initialization, RACF automatically registers these checks with IBM Health Checker for z/OS. These checks run when you start IBM Health Checker for z/OS. This is the time when you can change the SEVERITY, INTERVAL, and other check attributes using IBM Health Checker for z/OS parmlib or commands.

For further information on the RACF checks and on how to write a check, "check out" *IBM Health Checker for z/OS User's Guide*, SA22-7994.

```

CHECK (IBMRACF,RACF_SENSITIVE_RESOURCES)
START TIME: 06/30/2005 10:33:35.278967
CHECK DATE: 20040703 CHECK SEVERITY: HIGH
CHECK PARM: GENUSER

                                APF Dataset Report

S Data Set Name                    Vol      UACC Warn ID*  User
-----
ASM.SASMMOD1                       ZDR17
V CBC.SCBCCMP                       ZDR17
  CBC.SCCNCMP                       ZDR17  None No  ****
  CBC.SCLBDLL                       ZDR17  None No  ****
  CBC.SCLBDLL2                      ZDR17  None No  ****
  CEE.SCEERUN                       ZDR17  None No  ****
  CEE.SCEERUN2                     ZDR17  None No  ****
E CSF.SCSFMOD0                     ZDR17  None Yes ****  >Read
  EOY.SEOYLOAD                      ZDR17
E GDM.SADMMOD                      ZDR17  Updt No  ****  >Read
  GIM.SGIMLMD0                     ZDR17
  IOE.SIOELMOD                     ZDR17
  ISF.SISFLINK                      ZDR17  None No  ****
  ISF.SISFLOAD                      ZDR17  None No  ****
  ISP.SISPLoad                      ZDR17  None No  ****
  ISP.SISPLPA                       ZDR17  None No  ****
  ISP.SISPSASC                      ZDR17  None No  ****
E MARKN.DB2810.LOAD                D94RF1  None No  Updt  >Read
V MARKN.NOSUCH.VOLUME              TEMP99
  RACFDRVR.ATC.AUTHLIB              D79PK5  None No  ****
  RACFL2.LINKLIB                    D94RF1  None No  ****
  RACFTTEST.RRSF.LOAD               D94RF2
  RACF317.MIGLIB                    D97107
  SYS1.CMDLIB                       ZDR17  None No  ****
  SYS1.DFQLLIB                      ZDR17  None No  ****
  SYS1.DGTLIB                       ZDR17  None No  ****
  SYS1.LINKLIB                      ZDR17  None No  ****
  SYS1.SBDTLink                    ZDR17  None No  ****
  SYS1.SCBDHENU                    ZDR17  None No  ****
  SYS1.SERBLINK                    ZDR17  None No  ****
V SYS1.SHASLINK                    ZDR17
  SYS1.SHASLNKE                    ZDR17  None No  ****
  SYS1.SHASMIG                      ZDR17  None No  ****
  SYS1.SVCLIB                       ZDR17  None No  None
  SYS1.VTAMLIB                     ZDR17  None No  ****
  TCPIP.SEZADSIL                    ZDR17  Read No  ****
V TCPIP.SEZALINK                    ZDR17
  TCPIP.SEZALNK2                    ZDR17  Read No  ****
  TCPIP.SEZALOAD                    ZDR17  Read No  ****
  TCPIP.SEZATCP                     ZDR17  Read No  ****

                                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.

END TIME: 06/30/2005 10:33:58.588174 STATUS: EXCEPTION-HIGH

```

Figure 2 - RACF_SENSITIVE_RESOURCES check output