IBM Systems

# RACF Health Check Updates for z/OS V1R10

NY RACF Users Group

October 2008

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





## Trademarks

- See http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

## Overview

- **RACF currently supports these checks:**
  - **RACF_SENSITIVE_RESOURCES**
    - RACF database, APF list, PARMLIB, the link list, system REXX data set, and selected general resources
  - **RACF_GRS_RNL**
    - Verifies that the scope of RACF ENQs are not changed
  - **RACF_<classname>_ACTIVE**
    - For the FACILITY, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, and UNIXPRIV classes






## Overview…

- **The current RACF checks examine key elements of the z/OS infrastructure, but:**
  - If you want to check your own resources, you were "on your own"
- **Solution:**
  - Let you define the resources that you want validated to RACF and let RACF and the IBM Health Checker for z/OS do the rest!
- **Benefit:**
  - Ability to verify a baseline set of protections for application data

## Overview…

- **With z/OS V1R10, RACF introduces:**

**1. The RACF_ICHAUTAB_NONLPA check**

- Raises an exception if your have a non-LPA ICHAUTAB module defined to your environment.
- This check is defined as SEV(MED) INTERVAL(24:00)

**2. Enhancements to the RACF_SENSITIVE_RESOURCES_CHECK**

- Raises an exception if an ICHAUTAB module is found in LPA
- Added these resources to the "Sensitive General Resources" report
  - BPX.FILEATTR.PROGCTL in the FACILITY class
  - SUPERUSER.FILESYS.MOUNT in the UNIXPRIV class

**3. The ability to define your own RACF check which validates the checks the access to the resources that you specify**






## The RACF_ICHAUTAB_NONLPA Check Output

```
CHECK(IBMRACF,RACF_ICHAUTAB_NONLPA)
START TIME: 02/27/2008 12:20:53.474044
CHECK DATE: 20070411  CHECK SEVERITY: MEDIUM

                 ICHAUTAB Non-LPA Report

S Module   REQUEST= REQUEST= Location
           VERIFY   LIST
- -------- -------- -------- --------

IRRH239I There are no ICHAUTAB programs on this system.

END TIME: 02/27/2008 12:20:53.624003  STATUS: SUCCESSFUL
```

- **Only non-LPA modules are listed**

## RACF_SENSITIVE_RESOURCES Check Output

```
                        ICHAUTAB Report

S Module   REQUEST= REQUEST= Location
           VERIFY   LIST
- -------- -------- -------- --------

IRRH239I There are no ICHAUTAB programs on this system.
```

- **Both LPA and non-LPA modules are listed**






## Installation Defined Resources

- **Defining your own resource takes these three steps:**

1. **Defining a RACF profile in the RACFHC class which contains the list of resources that you want t 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**

## Defining your Resources to RACF

- **The RACFHC class contains profiles which have the resources that 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.






## Defining your Resources to RACF…

- **In addition to defining resources in the ADDMEM value, you can specify a 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 apre-defined set of resources**

```
RDEFINE RACFHC MY_SYSTEM_STUFF
     ADDMEM(DATASET/SYS1.SAMPLIB//NONE
     IRR_APFLIST
     IRR_RACFDB)
```

## Defining your Check to the Health Checker

- **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 that you want checked**

```
ADD CHECK(USER01,MY_INSTALLATION_HEALTH_CHECK)
    CHECKROUTINE(IRRHCR00)
    MESSAGETABLE(IRRHCM00)
    ENTRYCODE(100)
    PARM('USER(USER01)  RESOURCELIST(MY_RESOURCE_LIST)')
    DATE(20070425)
    REASON('My sensitive resources')
    GLOBAL
    ACTIVE
    SEVERITY(HIGH)
    INTERVAL(08:00)
```






## Defining your Check to the Health Checker…

- **When defining your check, you must define a `PARM` value which contains:**
  - `RESOURCELIST(profileName)`, where profileName is the name of the RACFHC profile which defines the resources that you want checked
  - and optionally `USER(userID)`, which defines the user ID which is to be checked
- **When defining your check you can/must set:**
  - Check name and owner
  - INTERVAL
  - SEVERITY
  - Status (ACTIVE, INACTIVE)
  - DATE
  - REASON
  - Locale (GLOBAL, LOCAL)
- **You must specify these values for your check**
  - CHECKROUTINE(IRRHCR00)
  - MESSAGETABLE(IRRHCM00)
  - ENTRYCODE(100)

## Activating the Check

- **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_SMSPDSE1                   IBMPDSE          ACTIVE(ENABLED)    EXCEPT
     RACF_FACILITY_ACTIVE            IBMRACF          ACTIVE(ENABLED)    SUCCES
     RACF_GRS_RNL                    IBMRACF          ACTIVE(DISABLED)   ENV N/
```






## Output

```
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
V SEC.FILING.FORMS                 DATASET
V PUBLIC.REPORTS                   DATASET  REGVOL
  MY_RESOURCE_LIST                 RACFHC          None No   ****

* High Severity Exception *
```

## Session Summary

- **RACF's enhancements for z/OS V1R10 provide significant new security validation for your z/OS environment:**
  - Identification of ICHAUTAB entries in the RACF_ICHAUTAB_NONLPA check and in RACF_SENSITIVE_RESOURCES
  - Evaluation of new general resources in the RACF_SENSITIVE_RESOURCES check
  - The ability to define your own resources in your own RACF health checks!






## Appendix

- **Reference materials:**
  - IBM Health Checker for z/OS Users Guide
  - RACF Messages and Codes