z/OS ® V2.5 IBM Education Assistant

Solution Name: RACF® New Health Checks

Solution Element(s): RACF

Overview

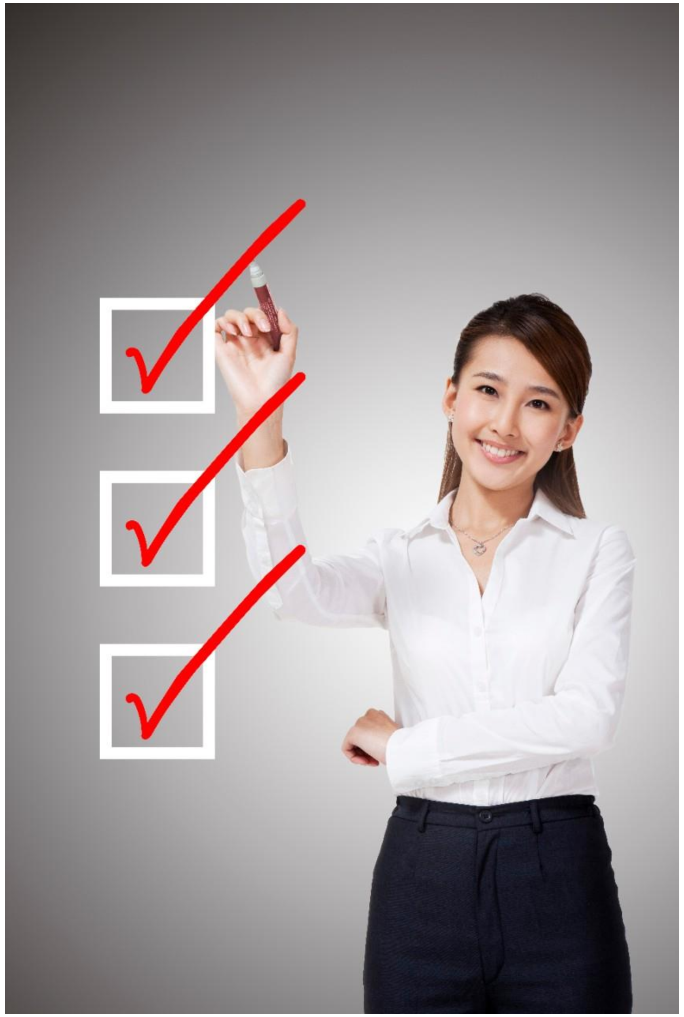
- **Who (Audience)**
  - z/OS systems programmers
  - z/OS security administrator
  - z/OS auditors

- **What (Solution)**
  - Five new RACF health checks

- **Wow (Benefit / Value, Need Addressed)**
  - To help you properly protect your z/OS environment

Usage & Invocation

- **With z/OS V2R5, RACF is introducing these five new health checks:**
  - **RACF_ADDRESS_SPACE,** which raises an exception if the RACF address space is not enabled
  - **RACF_ERASE_ON_SCRATCH**, which raises an exception if SETROPTS ERASE(ALL) is not in effect
  - **RACF_PROTECTALL_FAIL**, which raises an exception if SETROPTS PROTECTALL(FAIL) is not in effect
  - **RACF_PTKTDATA_CLASS**, which raises an exception if there are PassTicket profiles in the PTKTDATA class with keys that are not stored under the control of ICSF
  - **RACF_SYSPLEX_COMMUNICATION**, which raises an exception if RACF is not enabled for sysplex communication



]

Usage & Invocation: RACF_ADDRESS_SPACE

- **The RACF_ADDRESS_SPACE check raises an exception if the RACF address space is not active**
  - The RACF address space is required for the remote execution of RACF commands, issuing RACF commands from the MVS console, and RACF remote sharing. **It is not required for normal RACF authentication, authorization, or logging.**
  - Enabling RACF commands from a logged-on MVS console can be very useful in error recovery situations which prevent you from logging on to TSO to issue RACF commands.
  - By default, this check runs with a MEDIUM severity every 24 hours

Usage & Invocation: RACF_ADDRESS_SPACE…

- **RACF_ADDRESS_SPACE raising no exception results in this check output:**

```
CHECK(IBMRACF,RACF_ADDRESS_SPACE)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 02/27/2021 15:58:53.287534
CHECK DATE: 20200701  CHECK SEVERITY: MEDIUM

IRRH345I RACF address space is active.

END TIME: 02/27/2021 15:58:53.361367  STATUS: SUCCESSFUL
```

Usage & Invocation: RACF_ADDRESS_SPACE…

- **RACF_ADDRESS_SPACE raising an exception results in this check output:**

```
CHECK(IBMRACF,RACF_ADDRESS_SPACE)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 02/27/2021 02:15:48.549279
CHECK DATE: 20200701  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH344E RACF address space is inactive.

  Explanation:  The RACF_ADDRESS_SPACE check has determined that the
    RACF address space is inactive. IBM recommends that you configure
    the RACF address space. This allows you to issue RACF commands from
    a logged-on MVS console, without requiring JES or TSO.

  System Action:  The check continues processing. There is no effect on
    the system.
```

Usage & Invocation: RACF_ADDRESS_SPACE…

- **RACF_ADDRESS_SPACE exception (continued)**

```
  Operator Response:  Report this to the system programmer.

  System Programmer Response:  Configure the RACF Address Space.

  Problem Determination:  None.

  Source:  None.

  Reference Documentation:  z/OS Security Server RACF System
    Programmer's Guide

  Automation:  None.

  Check Reason:  IBM recommends starting the RACF address space.

END TIME: 02/27/2021 02:15:48.598538  STATUS: EXCEPTION-MED
```

Usage & Invocation: RACF_ERASE_ON_SCRATCH

- **The RACF_ERASE_ON_SCRATCH check raises an exception if SETROPTS ERASE(ALL) is not in effect.**
  - **SETROPTS ERASE(ALL)**
    - Instructs DFSMSdfp to erase all scratched data sets, *including temporary data sets*, regardless of the erasure indicator in the data set profile
  - **SETROPTS ERASE(seclevel-name)**
    - Instructs DFSMSdfp to erase all scratched data sets that have a security level equal to or greater than seclevel-name
  - **SETROPTS SETROPTS ERASE or ERASE(NOSECLEVEL)**
    - RACF instructs DFSMSdfp to erase a scratched data set if the erasure indicator in the data set profile is specified
  - **SETROPTS NOERASE**
    - No erase-on-scratch processing is to be performed, even if the data set erasure indicator is on in the data set profile

Usage & Invocation: RACF_ERASE_ON_SCRATCH

- **Caution**: While z/OS V2R1 and z/OS V2R2 provided improvements in erase on scratch processing time, do not enable ERASE(ALL) processing without testing for potential performance impact.

- **By default, this check runs with a MEDIUM severity every 24 hours**

Usage & Invocation: RACF_ERASE_ON_SCRATCH…

- **RACF_ERASE_ON_SCRATCH raising no exception results in the check output below. RCVTEOS, RCVTEOSL, and RCVTEOSA are flags in the RACF CVT (RCVT) that govern the RACF erase on scratch settings**

```
CHECK(IBMRACF,RACF_ERASE_ON_SCRATCH)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 02/26/2021 11:45:05.709913
CHECK DATE: 20190614  CHECK SEVERITY: MEDIUM

IRRH338I SETROPTS ERASE(ALL) is in effect.
RCVTEOS = 1 RCVTEOSL = 0 RCVTEOSA = 1

END TIME: 02/26/2021 11:45:05.710875  STATUS: SUCCESSFUL
```

Usage & Invocation: RACF_ERASE_ON_SCRATCH…

- **RACF_ERASE_ON_SCRATCH raising an exception results in this check output:**

```
CHECK(IBMRACF,RACF_ERASE_ON_SCRATCH)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 02/27/2021 01:38:56.255347
CHECK DATE: 20190614  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH335E SETROPTS NOERASE is in effect.

  Explanation:  The RACF_ERASE_ON_SCRATCH check has determined that
    SETROPTS NOERASE is in effect. IBM recommends that all data set
    space which is freed during a SCRATCH or RELEASE operation be
    erased. This prevents the inadvertent disclosure of this data and
    can be enabled with RACF's SETROPTS ERASE(ALL) command.
    RCVTEOS = 0 RCVTEOSL = 0 RCVTEOSA = 0
```

Usage & Invocation: RACF_ERASE_ON_SCRATCH…

- **RACF_ERASE_ON_SCRATCH exception (continued)**

```
    See the z/OS Security Server RACF Security Administrator's Guide for
    more information on SETROPTS ERASE. For more information on data set
    erasure, please see the Erasing DASD Data section in z/OS DFSMS
    Using Data Sets.

  System Action:  The check continues processing. There is no effect on
    the system.

  Operator Response:  Report this problem to the system security
    administrator. SETROPTS ERASE(ALL) should only be enabled after a
    careful evaluation of the potential performance impact of the data
    erasure.

  System Programmer Response:  None.
```

Usage & Invocation: RACF_ERASE_ON_SCRATCH…

- **RACF_ERASE_ON_SCRATCH exception (continued)**

```
Problem Determination:  None.

  Source:  None.

  Reference Documentation:
    z/OS Security Server RACF Security Administrator's Guide
    z/OS DFSMS Using Data Sets

  Automation:  None.

  Check Reason:  ERASE(ALL) should be enabled.

END TIME: 02/27/2021 01:38:56.259330  STATUS: EXCEPTION-MED
```

Usage & Invocation: RACF_PROTECTALL_FAIL

- **The RACF_PROTECTALL_FAIL check raises an exception if SETROPTS PROTECTALL(FAIL) is not in effect.**
  - **SETROPTS PROTECTALL(FAIL)**
    - Rejects any request to create or access a data set that is not RACF-protected (including tape data sets if TAPEDSN is in effect)
  - **SETROPTS PROTECTALL(WARN)**
    - Allows any request to create or access a data set that is not RACF-protected and logs the event and issues warning messages to the user and security administrator
  - **SETROPTS NOPROTECTALL**
    - Allows requests to create or access data sets that are not RACF-protected
- **By default, this check runs with a MEDIUM severity every 24 hours**

Usage & Invocation: RACF_PROTECTALL_FAIL…

- **RACF_PROTECTALL_FAIL raising no exception results in the check output below. RCVEOS, RCVTEOSL, and RCVTEOSA are flags in the RACF CVT (RCVT) that govern the RACF erase on scratch settings**

```
CHECK(IBMRACF,RACF_PROTECTALL_FAIL)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 02/27/2021 02:17:22.955643
CHECK DATE: 20190520  CHECK SEVERITY: MEDIUM

IRRH332I SETROPTS PROTECTALL(FAIL) is in effect.
RCVTPRO = 1 RCVTPROF = 0

END TIME: 02/27/2021 02:17:22.955846  STATUS: SUCCESSFUL
```

Usage & Invocation: RACF_PROTECTALL_FAIL…

- **RACF_PROTECTALL_FAIL raising an exception results in this check output:**

```
CHECK(IBMRACF,RACF_PROTECTALL_FAIL)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 02/27/2021 02:10:52.467428
CHECK DATE: 20190520  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH333E SETROPTS NOPROTECTALL is in effect.

  Explanation:  The RACF_PROTECTALL_FAIL check has determined that
    SETROPTS NOPROTECTALL is in effect.  This may allow unexpected
    access to data sets on this system. IBM recommends that the
    appropriate profiles be defined before enabling SETROPTS
    PROTECTALL(FAIL) to allow the appropriate access to data sets on
    this system.
    RCVTPRO = 0 RCVTPROF = 0
```

Usage & Invocation: RACF_PROTECTALL_FAIL…

- **RACF_PROTECTALL_FAIL exception (continued)**

```
     See the z/OS Security Server RACF Security Administrator's Guide for
    more information on SETROPTS PROTECTALL.

  System Action:  The check continues processing. There is no effect on
    the system.

  Operator Response:  Report this problem to the system security
    administrator. Do not enable SETROPTS PROTECTALL(FAIL) without
    defining the appropriate profiles.

  System Programmer Response:  None.

  Problem Determination:  None.

  Source:  None.

  Reference Documentation:
    z/OS Security Server RACF Security Administrator's Guide

  Automation:  None.

  Check Reason:  PROTECTALL(FAIL) should be enabled.

END TIME: 02/27/2021 02:10:52.493361  STATUS: EXCEPTION-MED
```

Usage & Invocation: RACF_PTKTDATA_CLASS

- **The RACF_PTKTDATA_CLASS check raises an exception if there are profiles in the PTKTDATA class which have keys which are not protected by ICSF.**

- **This check requires that the user ID associated with the Health Check address space has the RACF SPECIAL, AUDITOR, or ROAUDIT attribute.**

  - ROAUDIT is the recommendation

- **This check supports DEGUG=ON to display additional information on the user ID under which the check runs.**

- **By default, this check runs with a MEDIUM severity every 24 hours**

Usage & Invocation: RACF_PTKTDATA_CLASS…

- **RACF_PTKTDATA_CLASS raising no exception results in the check output below.**

```
CHECK(IBMRACF,RACF_PTKTDATA_CLASS)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 02/27/2021 02:10:53.629498
CHECK DATE: 20200701  CHECK SEVERITY: MEDIUM

                           RACF PassTicket Report

S Profile Name                     Key Label
- -------------------------------- -------------------------------------
  A                                SOMELABEL
  B                                IRR.SSIGNON.RACFR24.09112019.202528.0

IRRH340I No masked keys were found in the profiles in the PTKTDATA
class.

END TIME: 02/27/2021 02:10:59.081752  STATUS: SUCCESSFUL
```

Usage & Invocation: RACF_PTKTDATA_CLASS…

- **RACF_PTKTDATA_CLASS check raising an exception results in this check output:**

```
CHECK(IBMRACF,RACF_PTKTDATA_CLASS)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 02/27/2021 02:18:58.633273
CHECK DATE: 20200701  CHECK SEVERITY: MEDIUM

                           RACF PassTicket Report

S Profile Name                       Key Label
- -------------------------------- -------------------------------------
  A                                  SOMELABEL
  B                                  IRR.SSIGNON.RACFR24.09112019.202528.0
E TSOIM13                            *MASKED*

* Medium Severity Exception *

IRRH339E One or more PassTicket keys is stored masked in the RACF
database.

  Explanation:  The RACF_PTKTDATA_CLASS check has determined that one or
    more profiles in the PTKTDATA class have a masked key.
```

Usage & Invocation: RACF_PTKTDATA_CLASS…

- **RACF_PTKTDATA_CLASS exception (continued)**

```
   System Action:  The check continues processing. There is no effect on
     the system.

   Operator Response:  Report this problem to the system security
     administrator.

   System Programmer Response:  None.

   Problem Determination:  None.

   Source:  None.

   Reference Documentation:  z/OS Security Server RACF Security
     Administrator's Guide

   Automation:  None.

   Check Reason:  IBM recommends using ICSF to encrypt PassTicket keys.

END TIME: 02/27/2021 02:18:58.781457  STATUS: EXCEPTION-MED
```

Usage & Invocation: RACF_SYSPLEX_COMMUNICATION

- **The RACF_SYSPLEX_COMMUNICATION check raises an exception if RACF is not running in sysplex communication mode**

- **Sysplex communication mode provides:**
  - Consistent RACF data set usage (data set names table, data set range table, buffer definition) across the members of the sysplex
  - Propagation of certain RACF administrative commands (such as SETROPTS RACLIST(*classname*) REFRESH) across the systems sharing the RACF database
  - Improved RACF cache granularity for the deletion of cached data

- **By default, this check runs with a MEDIUM severity every 24 hours**

Usage & Invocation: RACF_SYSPLEX_COMMUNICATION…

- **RACF_SYSPLEX_COMMUNICATION raising no exception results in the check output below.**

```
CHECK(IBMRACF,RACF_SYSPLEX_COMMUNICATION)
SYSPLEX:    PLEX1     SYSTEM: SYSA
START TIME: 11/06/2019 18:21:46.884176
CHECK DATE: 20191008  CHECK SEVERITY: MEDIUM

IRRH343I Sysplex Communication is enabled.

END TIME: 11/06/2019 18:21:46.887243  STATUS: SUCCESSFUL
```

Usage & Invocation: RACF_SYSPLEX_COMMUNICATION…

- **RACF_SYSPLEX_COMMUNICATION check raising an exception results in this check output:**

```
CHECK(IBMRACF,RACF_SYSPLEX_COMMUNICATIONC)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 02/27/2021 02:10:52.466791
CHECK DATE: 20191008  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH342E RACF sysplex communication mode is not enabled.

  Explanation:  The RACF_SYSPLEX_COMMUNICATION check has determined that
    RACF sysplex communication mode is not enabled. IBM recommends RACF
    sysplex communication mode to be enabled to simplify security
    management.

    See z/OS Security Server RACF System Programmer's Guide for more
    information about RACF sysplex communication mode.

  System Action:  The check continues processing. There is no effect on
    the system.
```

Usage & Invocation: RACF_SYSPLEX_COMMUNICATION…

- **RACF_SYSPLEX_COMMUNICATION exception (continued)**

```
  Operator Response:  Report this problem to the system programmer.

  System Programmer Response:  None.

  Problem Determination:  None.

  Source:  None.

  Reference Documentation:
    z/OS Security Server RACF System Programmer's Guide
    z/OS Security Server RACF Security Administrator's Guide

  Automation:  None.

  Check Reason:  RACF sysplex communication mode should be enabled.

END TIME: 02/27/2021 02:10:52.496060  STATUS: EXCEPTION-MED
```

Interactions & Dependencies

- **Software Dependencies**
  - None

- **Hardware Dependencies**
  - None

- **Exploiters**
  - You!
    - ***Once you have validated that the check is appropriate for your environment.***

Upgrade & Coexistence Considerations

- **To exploit this solution, all systems in the Plex must be at the new z/OS level:**
  - No
- **List any toleration/coexistence APARs/PTFs:**
  - None
- **List anything that doesn't work the same anymore:**
  - Nothing

Installation & Configuration

- **These health checks are enabled by default. <u>Do not change a RACF system configuration setting without first testing the change.</u>**

  - If until the testing is performed or if the testing reveals that there is a setting which cannot be changed until some mitigation actions are taken, the check may be disabled with statements in the HZSPRMxx PARMLIB member:

```
ADDREPLACE POLICY(MY_OVERRIDE)
UPDATE
CHECK(IBMRACF,checkname)
INACTIVE
SEVERITY(MED)
INTERVAL(24:00)
DATE('20200703')
REASON('My installation does not want this check active.')

ACTIVATE POLICY(MY_OVERRIDE)
```

Summary

- **These five new RACF health checks can help you ensure the proper secure configuration of your z/OS environment**

Appendix

- **These checks will be documented in the IBM Health Checker for z/OS User’s Guide, SC23-6843.**