z/OS Security Server RACF®

Health Checker for z/OS® checks

APAR OA45608 (HRF7770, HRF7780, HRF7790)

September 2014

Table of Contents

1 Introduction

The PTFs for APAR OA45608 contain two new Health Checks for z/OS.

RACF_ENCRYPTION_ALGORITHM

RACF provides several options for protecting passwords in the RACF database. RACF can either mask the password, encrypt the password using the DES algorithm or allow the application to encrypt its own password. The ICHDEX01 installation exit controls the protection mechanism and returns one of several return codes.

For RACF protected passwords, DES encryption offers better security than masking.

The RACF_ENCRYPTION_ALGORITHM health check returns an exception when anything other than DES encryption algorithm is in use for password protection.

RACF_PASSWORD_CONTROLS

The RACF_PASSWORD_CONTROLS health check examines the client's RACF settings and raises an exception if either:

- RACF is not enabled for mixed-case passwords. Mixed-case passwords are necessary to extend the size of the key space.
- The invalid password revocation count is greater than three (3).
- The maximum number of days a user's password/passphrase is valid is less than 90 days.

Updated Publications List:
The IBM Health Checker for z/OS User's Guide (SA22-7994-xx, SC23-6843-xx)
z/OS Security Server RACF Messages and Codes (SA22-7686-xx, SA23-2291-xx)

2 The IBM Health Checker for z/OS User's Guide (SA22-7994-xx, SC23-6843-xx)

Part3, Chapter 13 IBM Health Checker for z/OS Checks, Section RACF checks (IBMRACF)

RACF_ENCRYPTION_ALGORITHM

Description: RACF provides several options for protecting passwords in the RACF database. RACF can either mask the password, encrypt the password using the DES algorithm or allow the application to encrypt its own password. The ICHDEX01 installation exit controls the protection mechanism and return one of several return codes.

For RACF protected passwords, DES encryption offers better security than masking.

The RACF_ENCRYPTION_ALGORITHM health check returns an exception when anything other than DES encryption algorithm is in use for password protection.

Reason for Check: IBM recommends the use of DES or stronger algorithms

z/OS releases the check applies to:
z/OS V1R12 and later.

Parameters accepted:
No

User override of IBM values:
The following shows keywords you can use to override check values on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command:

```
UPDATE CHECK(IBMRACF,RACF_ENCRYPTION_ALGORITHM)
DATE('date of the change')
SEVERITY(MED)
INTERVAL(08:00)
REASON('Health check interval change for RACF Encryption Algorithm')
```

Debug support:
No

Verbose support:
No

Reference:
See *z/OS Security Server RACF Security Administrator's Guide and*
z/OS Security Server RACF System Programmer's Guide

Messages:
This check issues the following exception messages:

- **IRRH295E**
- **IRRH298E**

See *z/OS Security Server RACF Messages and Codes.*

SECLABEL recommended for multilevel security users:
SYSLOW – see z/OS Planning for Multilevel Security and the Common Criteria for information on using SECLABELs.

Output:

RACF_ENCRYPTION_ALGORITHM REPORTS WITH EXCEPTIONS:

```
CHECK(IBMRACF,RACF_ENCRYPTION_ALGORITHM)
START TIME: 01/31/2014 09:44:29.892717
CHECK DATE: 20140131  CHECK SEVERITY: MEDIUM

IRRH295E  The RACF_ENCRYPTION_ALGORITHM check has detected an exception. ICHDEX01 is not in use on
this system. DES encryption falls back to RACF masking.

END TIME: 01/31/2014 09:44:29.893680  STATUS: EXCEPTION-MED
```

```
CHECK(IBMRACF,RACF_ENCRYPTION_ALGORITHM)
START TIME: 01/31/2014 09:44:29.892717
CHECK DATE: 20140131  CHECK SEVERITY: MEDIUM

IRRH296I  ICHDEX01 is in use on this system.

              ICHDEX01 Return Codes

Installation Mask    DES      Installation  DES then  Other
Only         Only    Only     Only          Mask
(RC=0)       (RC=04) (RC=08)  (RC=12)       (RC=16)   (RC=OTHER)
------------ ------- -------  ------------- --------- ----------
NO           NO      YES      NO            YES       NO

* Medium Severity Exception *

IRRH298E ICHDEX01 indicates an encryption algorithm other than DES is in use.

END TIME: 01/31/2014 09:44:29.893680  STATUS: EXCEPTION-MED
```

RACF_ENCRYPTION_ALGORITHM REPORT WITHOUT EXCEPTIONS:

```
CHECK(IBMRACF,RACF_ENCRYPTION_ALGORITHM)
START TIME: 01/31/2014 09:44:29.892717
CHECK DATE: 20140131  CHECK SEVERITY: MEDIUM

IRRH296I  ICHDEX01 is in use on this system.

              ICHDEX01 Return Codes

Installation Mask    DES      Installation  DES then  Other
Only         Only    Only     Only          Mask
(RC=0)       (RC=04) (RC=08)  (RC=12)       (RC=16)   (RC=OTHER)
------------ ------- -------  ------------- --------- ----------
NO           NO      YES      NO            NO        NO


IRRH297I ICHDEX01 indicates that only DES encryption is in use.

IRRH299I No exceptions are detected.

END TIME: 01/31/2014 09:44:29.893680  STATUS: SUCCESSFUL
```

Note: The RACF_ENCRYPTION_ALGORITHM only detects the encryption algorithm at the time the user logs on. If the check reports that ICHDEX01 has been installed and displays all of the 'ICHDEX01 Return Codes' as 'NO', then rerun the check.

RACF_PASSWORD_CONTROLS

Description:

The RACF_PASSWORD_CONTROLS health check examines the client's RACF settings and raises an exception if either:

- RACF is not enabled for mixed-case passwords. Mixed-case passwords are necessary to extend the size of the key space.
- The invalid password revocation count is greater than three (3).
- The maximum number of days a user's password/passphrase is valid is less than 90 days.

Reason for Check: Password control recommendations should be used.

z/OS releases the check applies to:
z/OS V1R12 and later.

Parameters accepted:

- MIXEDCASE(YES|NO)
- REVOKE(“nnn”) where “nnn” is between 0 and 255. A value of 0 indicates that the number of consecutive unsuccessful attempts is ignored.
- INTERVAL(“nnn”) where “nnn” is between 1 and 254.

User override of IBM values:

The following shows keywords you can use to override check values on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command:

```
UPDATE CHECK(IBMRACF,RACF_PASSWORD_CONTROLS)
DATE('date of the change')
SEVERITY(MED)
INTERVAL(24:00)
PARM('REVOKE(3),MIXEDCASE(YES),INTERVAL(90)')
REASON('Default values for RACF Password Controls')
```

Debug support:

No

Verbose support:

No

Reference:

See the *z/OS Security Server RACF System Programmer's Guide and the RACF Security Administrator's Guide.*

Messages:

This check issues the following exception messages:

- **IRRH283E**

See *z/OS Security Server RACF Messages and Codes.*

SECLABEL recommended for multilevel security users:

SYSLOW – see z/OS Planning for Multilevel Security and the Common Criteria for information on using SECLABELs.

Output:

RACF_PASSWORD_CONTROLS REPORT WITH EXCEPTION:

```
CHECK(IBMRACF,RACF_PASSWORD_CONTROLS)
SYSPLEX:    LOCAL     SYSTEM: RACFR22
START TIME: 02/03/2014 16:56:28.385841
CHECK DATE: 20140118  CHECK SEVERITY: MEDIUM
CHECK PARM: REVOKE(4)



                         RACF Password Controls
S Control                                            Value Target
- --------------------------------------------------- ----- ------
  Mixed case passwords are allowed                   YES   YES
E Maximum number of failed consecutive logon attempts None  003
  Maximum days a password/passphrase is valid         030   090
```

```
* Medium Severity Exception *


IRRH283E The RACF_PASSWORD_CONTROLS check found an exception
with one or more password control settings.


 Explanation:  The RACF_PASSWORD_CONTROLS check lists each password
    Control setting that is checked.  Only those password control
    Settings that do not meet the specified target result in an
    exception. The password control checks that result in an exception
    have an an "E" (Exception) in the "S" (Status) column.


    Use the SETROPTS LIST command to list the password control settings
    that are in effect. The SETROPTS command syntax is:


                             SETROPTS LIST


    Use the SETROPTS command to correct password control settings
    specifying the suboperands that need to be modified. For example,
    the syntax to specify the MIXEDCASE and REVOKE suboperands is:


               SETROPTS PASSWORD(MIXEDCASE REVOKE(3))

  See the z/OS Security Server RACF Security Administrator's Guide and
  the z/OS Security Server RACF Command Language Reference for more
  information about using the SETROPTS command to alter RACF password
  controls.

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:

Source:

Reference Documentation:

z/OS Security Server RACF Security Administrator's Guide
z/OS Security Server RACF Command Language Reference

Automation:  None.

Check Reason:  Password control recommendations should be used.


END TIME: 02/06/2014 12:23:15.999641  STATUS: EXCEPTION-MED
```

RACF_PASSWORD_CONTROLS REPORT WITHOUT EXCEPTIONS:

```
 CHECK(IBMRACF,RACF_PASSWORD_CONTROLS)
SYSPLEX:    LOCAL     SYSTEM: RACFR22
START TIME: 02/03/2014 16:54:07.628658
CHECK DATE: 20140118  CHECK SEVERITY: MEDIUM

                         RACF Password Controls
S Control                                            Value Target
- -------------------------------------------------- ----- ------
  Mixed case passwords are allowed                   YES   YES
  Maximum number of failed consecutive logon attempts 003   003
  Maximum days a password/passphrase is valid         030   090


IRRH284I No exceptions are detected.

END TIME: 02/03/2014 16:54:07.628918  STATUS: SUCCESSFUL
```

3 Z/OS Security Server RACF Messages and Codes (SA22-7686-xx, SA23-2291-xx)

Chapter 8. IBM health checker for z/OS and sysplex messages

The following are new messages:

IRRH295E The RACF_ENCRYPTION_ALGORITHM check has detected an exception. ICHDEX01 is not in use on this system. DES encryption falls back to RACF masking.

Explanation: The RACF_ENCRYPTION_ALGORITHM check verifies that only the KDFAES or DES encryption algorithm is used for password protection. The ICHDEX01 exit indicates the algorithm to use for password protection when KDFAES is not enabled. When the ICHDEX01 exit is not installed, RACF attempts to use the DES algorithm for password protection but falls back to RACF masking on failure. Since RACF masking could be in use, there is an exception.

See the z/OS Security Server RACF System Programmer's Guide for more information about the ICHDEX01 exit.

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:
Reference Documentation:
z/OS Security Server RACF System Programmer's Guide
Automation: None.

IRRH296I ICHDEX01 is in use on this system.

Explanation: The RACF_ENCRYPTION_ALGORITHM check verifies that only the KDFAES or DES encryption algorithm is used for password protection. The ICHDEX01 exit indicates the algorithm to use for password protection when KDFAES is not enabled.

See the z/OS Security Server RACF System Programmer's Guide for more information about the ICHDEX01 exit.

System Action: The check continues processing. There is no effect on the system.
Operator Response: None.
System Programmer Response: None.
Problem Determination:
Reference Documentation:
z/OS Security Server RACF System Programmer's Guide
Automation: None.

IRRH297I ICHDEX01 indicates that only DES encryption is in use.

Explanation: The RACF_ENCRYPTION_ALGORITHM check verifies that only the KDFAES or DES encryption algorithm is used for password protection. The ICHDEX01 exit indicates the algorithm to use for password protection when KDFAES is not enabled. ICHDEX01 has set a return code indicating the DES algorithm is always used.

See the z/OS Security Server RACF System Programmer's Guide for more information about the ICHDEX01 exit.

System Action: The check continues processing. There is no effect on the system.
Operator Response: None.
System Programmer Response: None.
Problem Determination:
Reference Documentation: z/OS Security Server RACF System Programmer's Guide
Automation: None.

IRRH298E ICHDEX01 indicates that an algorithm other than DES encryption is in use.

Explanation: The RACF_ENCRYPTION_ALGORITHM check verifies that only the KDFAES or DES encryption algorithm is used for password protection. The ICHDEX01 exit indicates the algorithm to use for password protection when KDFAES is not enabled. ICHDEX01 has set a return code indicating to use an algorithm other than DES which raises an exception.

See the z/OS Security Server RACF System Programmer's Guide for more information about the ICHDEX01 exit.

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:
Reference Documentation: z/OS Security Server RACF System Programmer's Guide
Automation: None.

IRRH299I No exceptions are detected.

Explanation: The RACF_ENCRYPTION_ALGORITHM check verifies that only the KDFAES or DES encryption algorithm is used for password protection. The ICHDEX01 exit indicates the algorithm to use for password protection when KDFAES is not enabled. Either ICHDEX01 is not installed or ICHDEX01 has set a return code indicating that only DES is in use for password protection.

See the z/OS Security Server RACF System Programmer's Guide for more information about the ICHDEX01 exit.

System Action: The check continues processing. There is no effect on the system.
Operator Response: None.
System Programmer Response: None.
Problem Determination:
Reference Documentation: z/OS Security Server RACF System Programmer's Guide
Automation: None.

IRRH283E The RACF_PASSWORD_CONTROLS check found an exception
with one or more password control settings.

Explanation: The RACF_PASSWORD_CONTROLS check lists each password control setting that is checked. Only those password control settings that do not meet the specified target result in an exception. The password control checks that result in an exception have an an "E" (Exception) in the "S" (Status) column.

Use the SETROPTS LIST command to list the password control settings that are in effect. The SETROPTS command syntax is:

```
SETROPTS LIST
```

Use the SETROPTS command to correct password control settings specifying the suboperands that need to be modified. For example, the syntax to specify the MIXEDCASE and REVOKE suboperands is:

```
SETROPTS PASSWORD(MIXEDCASE REVOKE(3))
```

See the z/OS Security Server RACF Security Administrator's Guide and the z/OS Security Server RACF Command Language Reference for more information about using the SETROPTS command to alter RACF password controls.

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:
Source:
Module: IRRHCR30
Routing code: N/A
Descriptor code: N/A
Automation: None.
Reference Documentation: See *z/OS Security Server RACF Security Administrator's Guide*.
See *z/OS Security Server RACF Command Language Reference*.

IRRH284I No exceptions are detected.

The RACF_PASSWORD_CONTROLS check lists each password control setting that is checked. Only those password control settings that do not meet the specified target result in an exception. The password control checks that result in an exception have an an "E" (Exception) in the "S" (Status) column.

Use the SETROPTS LIST command to list the password control settings that are in effect. The SETROPTS command syntax is:

```
SETROPTS LIST
```

Use the SETROPTS command to correct password control settings specifying the suboperands that need to be modified. For example, the syntax to specify the MIXEDCASE and REVOKE suboperands is:

```
SETROPTS PASSWORD(MIXEDCASE REVOKE(3))
```

See the z/OS Security Server RACF Security Administrator's Guide and the z/OS Security Server RACF Command Language Reference for more information about using the SETROPTS command to alter RACF password controls.

System Action: The check continues processing. There is no effect on the system.
Operator Response: None.
System Programmer Response: None.
Problem Determination: None.
Source:
Module: IRRHCR30
Automation: None.
Reference Documentation: See *z/OS Security Server RACF Security Administrator's Guide*.
See *z/OS Security Server RACF Command Language Reference*.