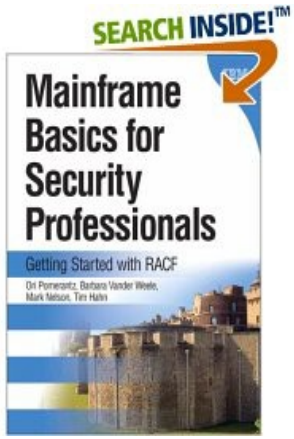
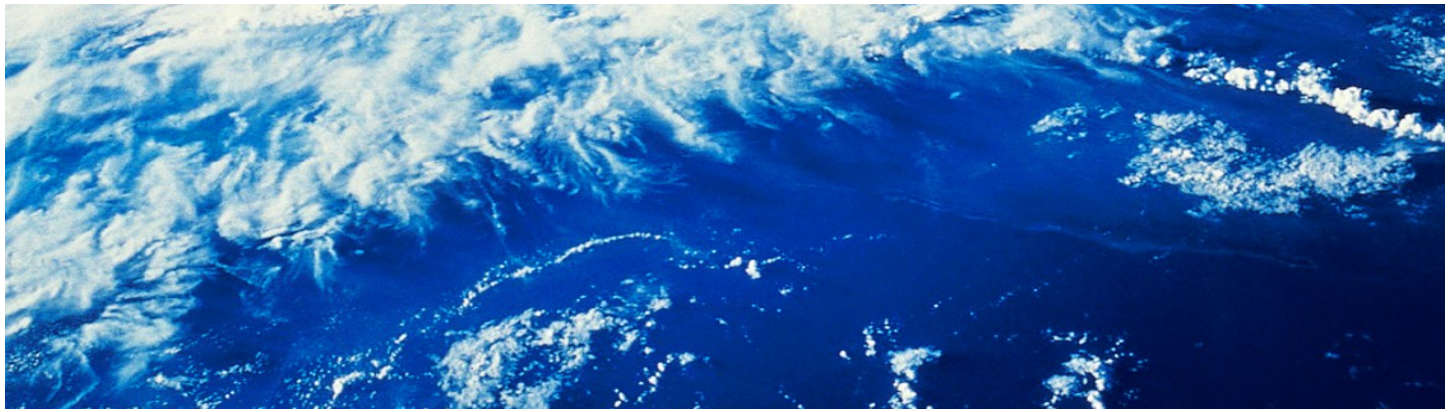
z/OS® V2.1 RACF® Update

Mark Nelson, CISSP®, CSSLP®
z/OS Security Development
IBM Poughkeepsie
markan@us.ibm.com

RACF Users Group of New England (RUG-One)
May 2014





Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AIX*
BladeCenter*
BookManager*
CICS*
DataPower*
DB2*
DFSMS
DFSMSdss
DFSMShsm
DFSMSrmm
DFSORT
Domino*
DS6000
DS8000*
FICON*
IBM*
IBM eServer
IBM logo*
IMS
InfinBand
Language Environment*
MVS
Parallel Sysplex*
ProductPac*
RACF*
Redbooks*
REXX
RMF
ServerPac*
SYSREXX
System Storage
System x*
System z
System z9
System z10
System z10 Business Class
Tivoli*
WebSphere*
z10
z10 BC
z10 EC
zEnterprise*
zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Windows Server and the Windows logo are trademarks of the Microsoft group of countries.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

* Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Agenda

What's new with z/OS V2.1 RACF?

- **Common Criteria Evaluation Update**
- **RRSF**
  - Support for TCP/IP V6
  - Comments in the RACF parameter library
  - TLS 1.2 cipher suite support
- **New and improved RACF Health Checks**
  - RACF_AIM_STAGE, RACF_UNIX_ID, RACF_CERTIFICATE_EXPIRATION, RACF_SENSITIVE_RESOURCES
- **Certificate issuer distinguished name, subject distinguished names and signature algorithms, in IRRDBU00 output**
- **RACDCERT Enhancements**
- **&RACUID in home directory path name**
- **Access controls for JES2/JES3 job classes**
- **PKI Services Enhancements**
- **Statement of Direction**

Common Criteria Update

Common Criteria Update

- **Recent Common Criteria Evaluations of Interest:**
  - z/OS V1.13, EAL4+, 12 September, 2012
  - z/OS V1.13/RACF, EAL5+, 27 February, 2013
  - z/VM Version 6 Release 1, EAL4+, 20 February, 2013
  - PR/SM on IBM Systems z196 GA2 z114 GA1, 1 March, 2012
  - PR/SM for IBM zEnterprise EC12 EAL5+, 19 February, 2013
  - PR/SM for IBM zEnterprise EC12 EAL5+, 19 February, 2014
- **http://www.ibm.com/security/standards/security_evaluations.html has the details**

RRSF

RRSF: Quick TCP/IP Review

- **Starting with z/OS V1.13, you can link RRSF nodes using TCP/IP instead of APPC! This means that you can now:**
  - Manage your RRSF network using the same skills as the rest of your TCP/IP network.
  - Ensure that the same network security policy (IDS, IPS, etc.) is in place for your RRSF network as in place for the rest of your z/OS TCP/IP network.
  - Utilize the encryption and peer-node authentication of AT-TLS
  - Convert a node from using APPC to TCP/IP without stopping communication
  - **Keep up with improvements in z/OS Communications Server Security.**

RRSF: IPv6 Support

- **Starting with z/OS V2.1, RRSF supports the use of TCP/IP V6 for communications between/among your RRSF nodes**
  - Once the z/OS Communications Server on your local note is configured for Ipv6:
    - IPv6-format addresses will be displayed
  - You do not have to migrate to IPv6 all at once: Some“remote” nodes can be IPv4 and some IPv6.

RRSF: IPv6 Addresses

Description	IPv4	IPv6
Address length	32 bits long (4 bytes)	128 bits long (16 bytes). 64 bits for network number, 64 bits for host numbe
Total addresses	4,294,967,296 (about 4.3 billion)	About 3.4 x 10^{38}
Address format in text	nnn.nnn.nnn.nnn Where 0<=nnn<=255	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx Where x is hex number. Double colon (::) designates any number of 0 bits
Example	9.127.42.144	`2001:0db8:85a3:0000:0000:8a2e:0370:7334`
Equivalent addresses	10.120.78.40	`::ffff:10.120.78.40` IPv4-mapped IPv6 address
Unspecified address	0.0.0.0	`::` (128 0 bits)

RRSF: TARGET LIST (V1.13)

```
NODE1  <target list node(node1)
NODE1  IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF LOCAL RRSF NODE NODE1:
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - APPC
                 LU NAME           - MF1AP001
                 TP PROFILE NAME   - IRRRACF
                 MODENAME          - <NOT SPECIFIED>
                 LISTENER STATUS   - ACTIVE
   PROTOCOL    - TCP
                 HOST ADDRESS      - 0.0.0.0
                 IP ADDRESS        - 9.57.1.243
                 LISTENER PORT     - 18136
                 LISTENER STATUS   - ACTIVE
   TIME OF LAST TRANSMISSION TO   - <NONE>
   TIME OF LAST TRANSMISSION FROM - <NONE>
   WORKSPACE FILE SPECIFICATION
         PREFIX                   - "NODE1.WORK"
         WDSQUAL                  - <NOT SPECIFIED>
         FILESIZE                 - 500
         VOLUME                   - TEMP01
         FILE USAGE
                "NODE1.WORK.NODE1.INMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
                "NODE1.WORK.NODE1.OUTMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
```

1st line indicates 'default' – not specified on TARGET.
2nd line is resolved address, if different than specified.

RRSF: TARGET LIST(V2.1)

```
NODE1  <target list node(node1)
NODE1  IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF LOCAL RRSF NODE NODE1:
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - APPC
                 LU NAME           - MF1AP001
                 TP PROFILE NAME   - IRRRACF
                 MODENAME          - <NOT SPECIFIED>
                 LISTENER STATUS   - ACTIVE
   PROTOCOL    - TCP
                 HOST ADDRESS      - ::                      <<< IPv6 default
                 IP ADDRESS        - ::FFFF:9.57.1.243       <<< IPv6 address
                 LISTENER PORT     - 18136
                 LISTENER STATUS   - ACTIVE
   TIME OF LAST TRANSMISSION TO    - <NONE>
   TIME OF LAST TRANSMISSION FROM  - <NONE>
   WORKSPACE FILE SPECIFICATION
         PREFIX                    - "NODE1.WORK"
         WDSQUAL                   - <NOT SPECIFIED>
         FILESIZE                  - 500
         VOLUME                    - TEMP01
         FILE USAGE
                 "NODE1.WORK.NODE1.INMSG"
                                   - CONTAINS 0 RECORD(S)
                                   - OCCUPIES 1 EXTENT(S)
                 "NODE1.WORK.NODE1.OUTMSG"
                                   - CONTAINS 0 RECORD(S)
                                   - OCCUPIES 1 EXTENT(S)
```

If IPv6 is enabled, addresses Are displayed in IPv6 format

RRSF: Comments in Parameter Library

- **Prior to z/OS V2.1, blank lines or whole-line comments would result in an IRRC003I (“COMMAND xxxxx IS NOT VALID”) error message**

- **With z/OS V2.1, blank lines and whole-line comments are allowed**
  - A whole-line comment begins with “//” in any column
    - Continuation characters at the end of a whole-line comment does not continue the comment
    - Whole-line comments or blank lines may not be placed within a continued command
    - Down-level systems will continue to flag whole-line and blank lines as errors
  - Examples of valid whole-line comments:
    - //This is a comment line
    - // This is a comment line
    - // define the local node with a socket listener

RRSF: TLS 1.2 Cipher Suite Support

- **RRSF uses Application Transparent Transport Layer Security (AT-TLS) to encrypt data between RRSF nodes**
  - AT-TLS supports more cryptography suites in z/OS V2.1
  - Certificates are used in AT-TLS to provide secure connections between RRSF systems using TCP/IP
  - In z/OS V2R1, ECC certificates with stronger encryption may be used
  - All cryptography suites in Transport Layer Security (TLS) Protocol Version 1.2 are supported

- **When a connection is established between 2 RRSF systems, here is an example of the informational message issued by RACF:**
  - `IRRI027I (>) RACF COMMUNICATION WITH TCP NODE NODE1 HAS BEEN SUCCESSFULLY ESTABLISHED USING CIPHER ALGORITHM C026 TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384.`

Health Check Updates

Health Checks: New and Updated Checks

- **There are three new RACF Health Checks in z/OS V2.1:**
  - RACF_AIM_STAGE
  - RACF_UNIX_ID
  - RACF_CERTIFICATE_EXPIRATION
- **RACF_AIM_STAGE and RACF_UNIX_ID are intended to assist you in migrating from BPX.DEFAULT.USER, which, as announced, is being withdrawn with z/OS V2.1**
  - These two checks rolled back to z/OS V1.12 and z/OS V1.13 with OA37164
- **Automatic start for the Health Checker address space at IPL time**

Health Checks: RACF_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**

Health Checks: RACF_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(IBMRACF,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 *********************************
```

Health Checks: RACF_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(IBMRACF,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
    IRRIRA00 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
```

Health Checks: RACF_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.

Health Checks: RACF_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(IBMRACF,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
```

Health Checks: RACF_UNIX_ID (OK)

```
******************************** TOP OF DATA ********************************
CHECK(IBMRACF,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 RACLISTed
  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
```

Health Checks: RACF_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(IBMRACF,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 RACLISTed
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:
```

Health Checks: RACF_UNIX_ID (Exception)

```
********************************* TOP OF DATA **********************************
CHECK(IBMRACF,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(IBMRACF,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

Health Checks: RACF_CERTIFICATE_EXPIRATION

- **The RACF_CERTIFICATE_EXPIRATION health check finds the certificates in the RACF database expired or about to expire**
  - Expiration window is an installation-defined value with a default of 60 days.
  - Valid expiration window values are 0-366 days
- **For each certificate, the check displays:**
  - The certificate “owner” ('SITE', 'CERTAUTH', or 'ID(*user_id*)')
  - The certificate label
  - The end date
  - The trust status
  - The number of rings to which the certificate is connected
- **The check only flags as exceptions those certificates which are TRUSTED.**

Health Checks: RACF_CERTIFICATE_EXPIRATION (OK)

```
CHECK(IBMRACF,RACF_CERTIFICATE_EXPIRATION)
START TIME: 01/23/2012 08:10:01.603497
CHECK DATE: 20111010  CHECK SEVERITY: MEDIUM


                    Certificates Expiring in 60 Days


S Cert Owner   Certificate Label                 End Date   Trust Rings
- ------------ -------------------------------- ---------- ----- -----


IRRH277I No exceptions are detected. Expired certificates that are not
trusted or are associated with only a virtual key ring are not
exceptions.


END TIME: 01/23/2012 08:10:01.643285  STATUS: SUCCESSFUL
```

Health Checks: RACF_CERTIFICATE_EXPIRATION (Exception)

```
CHECK(IBMRACF,RACF_CERTIFICATE_EXPIRATION)
START TIME: 02/28/2013 09:23:37.747549
CHECK DATE: 20111010  CHECK SEVERITY: MEDIUM

                  Certificates Expiring within 60 Days

S Cert Owner   Certificate Label                  End Date   Trust Rings
- ------------ -------------------------------- ---------- ----- -----
E CERTAUTH     VERISIGN CLASS 1 INDIVIDUAL      2008-05-12 Yes    0
E ID(MARKN)    MARK-001                         2012-11-11 Yes    0
E ID(MARKN)    MARK0001                         2012-11-05 Yes    0
  ID(CERTAUTH) START_OFF_M001__END_OFF_M001     2012-01-25 No     0
  ID(MARKN)    START_OFF_M001__END_OFF_M001     2012-01-25 No     0
  ID(SITE)     START_OFF_M001__END_OFF_M001     2012-01-25 No     0
  CERTAUTH     START_OFF_M365__END_OFF_M001     2012-01-25 No     0
  ID(CERTAUTH) START_OFF_M365__END_OFF_M001     2012-01-25 No     0
  CERTAUTH     ICP-Brasil CA                    2011-11-30 No     0
  CERTAUTH     MICROSOFT ROOT AUTHORITY - 01    2002-12-31 No     0
  CERTAUTH     VERISIGN CLASS 3 PUBLIC          2004-01-07 No     0
  CERTAUTH     VERISIGN CLASS 2 PUBLIC          2004-01-06 No     0

* Medium Severity Exception *

IRRH276E One or more certificates expired or are expiring within
the warning period.

  Explanation:  The RACF_CERTIFICATE_EXPIRATION check found one or more
    certificates that expired or are expiring within the warning period.
```

Health Checks: RACF_CERTIFICATE_EXPIRATION (Exception)

```
  The RACF_CERTIFICATE_EXPIRATION check lists each certificate that
  has an ending date prior to the current date or that has an ending
  date that is prior to the current date adjusted by the warning
  period that the installation has specified as a parameter to the
  RACF_CERTIFICATE_EXPIRATION check. If a parameter is not specified,
  a default warning period of 60 days is used.

  Only certificates that are marked as trusted result in exceptions.
  These certificates have an "E" in the "S" (Status) column. The trust
  status of the certificate is shown in the "Trust" column. The number
  of key rings to which the certificate is connected (other than the
  virtual key ring) is shown in the "Rings" column.

  Use the RACDCERT LIST command to list complete information about any
  certificate. The RACDCERT command syntax is:

          RACDCERT CERTAUTH     LIST(LABEL('label-name'))
                                 or
          RACDCERT SITE         LIST(LABEL('label-name'))
                                 or
          RACDCERT ID(user-id)  LIST(LABEL('label-name'))


  See z/OS Security Server RACF Security Administrator's Guide and the
  z/OS Security Server RACF Command Language Reference for more
  information about digital certificates.

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

Health Checks: RACF_SENSITIVE_RESOURCES

- **The RACF_SENSITIVE_RESOURCES check has been updated to check these new "static" resources names:**
  - BPX.DEBUG/FACILITY
  - BPX.WLMSERVER/FACILITY
  - IEAABD.DMPAKEY/FACILITY
  - MVS.SLIP/OPERCMDS
  - SUPERUSER.PROCESS.GETPSENT/UNIXPRIV
  - SUPERUSER.PROCESS.KILL/UNIXPRIV
  - SUPERUSER.PROCESS.PTRACE/UNIXPRIV

Health Checks: RACF_SENSITIVE_RESOURCES...

- **RACF is planning on updating the RACF_SENSITIVE_RESOURCES to check these new "dynamic" resources names:**
  - CSVAPF.*data_set_name*/FACILITY, excluding
    - CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC
  - CSVDYLPA.ADD.*module_name*/FACILITY
  - CSVDYNEX.*exit_name*.*function.modname*/FACILITY, *excluding*
    - *CSVDYNEX.LIST*
    - *CSVDYNEX.exit_name*.RECOVER
    - CSVDYNEX.exit_name.CALL
  - CSVDYNL.*lnklstname. Function*/FACILITY*excluding*
    - CSVDYNL.*lnklstname*.DEFINE CSVDYNL.*lnklstname.*UNDEFINE)
- **No validation is performed on the dynamic portion of these resource names (for example *data_set_ name, module_name,lnklstname*)**

Health Checks: RACF_SENSITIVE_RESOURCES...

Sensitive General Resources Report

S	Resource Name	Class	UACC	Warn	ID*	User
	<existing resources>					
	BPX.WLMSERVER	FACILITY	Updt	No	****	
	CSVAPF.RACFDEV.DISCRETE.NONE.LOAD	FACILITY	None	No	****	
	CSVAPF.RACFDEV.DISCRETE.READ.LOAD	FACILITY	Read	No	****	
E	CSVAPF.RACFDEV.DISCRETE.UPDATE.LOAD	FACILITY	Updt	No	****	
	CSVAPF.RACFDEV.**.NONE.LOAD	FACILITY	None	No	****	
	CSVAPF.RACFDEV.**.READ.LOAD	FACILITY	Read	No	****	
E	CSVAPF.RACFDEV.**.UPDATE.LOAD	FACILITY	Updt	No	****	
E	CSVDYLPA.ADD.MODULE001	FACILITY	Updt	No	****	
E	CSVDYLPA.DELETE.MODULE01	FACILITY	Updt	No	****	
E	CSVDYLPA.ADD.*	FACILITY	Updt	No	****	
E	CSVDYLPA.DELETE.*	FACILITY	Updt	No	****	
	CSVDYNEX.EXITNAME_READ.MODNAME01	FACILITY	Read	No	****	
E	CSVDYNEX.EXITNAME_UPDATE.DEFINE	FACILITY	Updt	No	****	
E	CSVDYNEX.EXITNAME_UPDATE.MODNAME01	FACILITY	Updt	No	****	
E	CSVDYNEX.*.DEFINE	FACILITY	Updt	No	****	
E	CSVDYNEX.*.MODNAME01	FACILITY	Updt	No	****	
E	CSVDYNEX.*	FACILITY	Updt	No	****	
E	IEAABD.DMPAKEY	FACILITY	Read	No	****	
E	IEAABD.DMPAUTH	FACILITY	Read	No	****	

Certificate Distinguished Names in IRRDBU00 Output

IRRDBU00: Additional Certificate Information

- **The RACF Database Unload Utility (IRRDBU00) unloads basic information about digital certificates into the 0560 (“General Resource Certificate Data Record”). This record contains:**
  - The record type (“0560”)
  - The name of the general resource profile which contains the certificate
  - The class (“DIGTCERT”)
  - The date and time from which the certificate is valid
  - The date and time from which the certificate is no longer valid
  - The type of key associated with the certificate
  - The key size
  - The last eight bytes of the last certificate signed with this key
  - A sequence number for certificates within a ring
- **What's missing? The issuer's distinguished name (IDN) and the subject's DN (SDN)of the certificate!**
  - This information is encoded within the certificate
  - Maps/mungs to the profile name, but given the profile name, you can't get the IDN or SDN

IRRDBU00: Additional Certificate Information...

- **A new record type (“1560”) is planned to contain:**
  - The issuer's distinguished name
  - The subject's distinguished name
  - The hashing algorithm used for the signing the certificate
- **The “1560” record links to the “0560” record using the profile name**
  - DFSORT's JOINKEY operator can be used when processing IRRDBU00 output
- **The Mapping of the1560 Record is:**

		Position		
Field Name	**Type**	**Start**	**End**	**Comments**
CERTN_RECORD_TYPE	Int	1	4	Record type of the certificate information record (1560).
CERTN_NAME	Char	6	251	General resource name as taken from the profile name.
CERTN_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
CERTN_ISSUER_DN	Char	262	1285	Issuer’s distinguished name. (1024 characters)
CERTN_SUBJECT_DN	Char	1287	2310	Subject’s distinguished name. (1024 characters)
CERTN_SIG_ALG	Char	2312	2327	Certificate signature algorithm. Valid values are md2RSA, md5RSA, sha1RSA, sha1DSA, sha256RSA, sha224RSA, sha384RSA, sha512RSA, sha1ECDSA, sha256ECDSA, sha224ECDSA, sha384ECDSA, sha512ECDSA, and UNKNOWN.

IRRDBU00: Additional Certificate Information

- **The RACF Database Unload Utility (IRRDBU00) unloads basic information about digital certificates into the 0560 (“General Resource Certificate Data Record”). This record contains:**
  - The record type (“0560”)
  - The name of the general resource profile which contains the certificate
  - The class (“DIGTCERT”)
  - The date and time from which the certificate is valid
  - The date and time from which the certificate is no longer valid
  - The type of key associated with the certificate
  - The key size
  - The last eight bytes of the last certificate signed with this key
  - A sequence number for certificates within a ring
- **What's missing? The issuer's distinguished name (IDN) and the subject's DN (SDN)of the certificate!**
  - This information is encoded within the certificate
  - Maps/mungs to the profile name, but given the profile name, you can't get the IDN or SDN

RACDCERT Enhancements

RACDCERT ADD Enhancement

- **Prior to z/OS V2.1, if you used RACDCERT ADD to add a PKCS#12 or PKCS#7 certificate chain using the RACDCERT ADD command, only the end entity certificate can be named using a specified label.**
  - RACDCERT generates labels for the rest of the certificates in the chain, but previously **did not display what labels** had been added.
- **Starting in V2R1, RACDCERT will display the generated labels of any certificates in the chain that were added.**

```
RACDCERT ID(COOPER) ADD('COOPER.CERTS.MYPKCS12') WITHLABEL('MyCert')

Certificate with label 'MyCert' is added under ID COOPER

Certificate with label 'LABEL00000002' is added under CERTAUTH

Certificate with label 'LABEL00000003' is added under CERTAUTH
```

RACDCERT LISTCHAIN Enhancement

- **Starting in V2R1 RACF is adding the ability to list a certificate chain with the introduction of the RACDCERT LISTCHAIN command.**

- **RACDCERT LISTCHAIN Syntax:**

  RACDCERT [ID(certificate-owner)| SITE | CERTAUTH]

  LISTCHAIN (LABEL('label-name'))

- Information provided:
  - Certificate details for the specified certificate
  - Details for each issuing certificate which is in RACF
  - Summary of the Chain:
    - Number of certificates in the chain
    - Whether RACF contains the complete chain
      - – chain is complete
      - – chain is incomplete
    - Indication of expired certificate(s), if any
      - – chain contains expired certificate(s)
    - List of rings that all certificates in chain share

RACDCERT LISTCHAIN Sample Output

```
RACDCERT LISTCHAIN(LABEL('samplecert'))



Certificate 1:
  Digital certificate information for user CHOI:
  Label: samplecert
  …
  Ring Associations:
    Ring Owner: COOPER
    Ring:
      >testring<

Certificate 2:
  Digital certificate information for CERTAUTH:
  Label: sampleCA
  …
  Ring Associations:
  Ring Owner: COOPER
  Ring:
   >testring<
```

```
Certificate 3:
  Digital certificate information for CERTAUTH:
  Label: MasterCA
  …
  Ring Associations:
  Ring Owner: COOPER
  Ring:
    >testring<

Chain information:
  Chain contains 3 certificate(s), chain is complete
  Chain contains ring in common: COOPER/testring
```

RACDCERT GENREQ Enhancement

- **Generating a Certificate Request (CSR) from RACDCERT GENREQ requires an existing certificate in RACF with a private key (usually a self signed certificate created with GENCERT).**

- **Don't delete that cert!**
  - A common issue encountered by RACDCERT users, is deleting the original certificate from RACF after the CSR has been generated... erroneously concluding that the certificate had no use.
  - If the original certificate is deleted from RACF after the CSR is created, the private key is also deleted, rendering any signed certificate based on this CSR useless (oops!).

- **Starting in V2R1 RACDCERT will prevent the deletion of a certificate that has been used for generating a request with GENREQ.**
  - Force override mechanism is provided to delete this certificate when needed

RACDCERT CHECKCERT Enhancement

- **RACDCERT CHECKCERT enhancement:**
  - LISTCHAIN is used to list certificates in RACF, while CHECKCERT is to list certificates in a dataset (which is going to be an input to the RACDCERT ADD)
  - Enhancements similar to LISTCHAIN were added to the display text of RACDCERT CHECKCERT, when displaying information on a certificate in a dataset.

RACDCERT Support for Secure TKDS

- Unlike the keys stored in the Public Key Data Set (PKDS), the keys stored in the Token Key Data Set (TKDS) are clear keys, not secure keys.
- "Secure Key" means that sensitive key material is always wrapped under a master key.
- In Web Deliverable #12, ICSF supports secure key in TKDS.
- To enable the applications to use the secure key in TKDS, RACF, PKI Services and System SSL need to be updated accordingly.

RACDCERT Support for Secure TKDS

- **RACDCERT can create a secure key on a specified PKCS#11 token on TKDS during certificate creation**
- **This new support allows RACDCERT to issue and use of certificates with hardware-protected keys in a PKCS#11 TKDS token.**
  - RACDCERT EXPORT can not export any secure key neither from PKDS nor TKDS
- **RACDCERT GENCERT / REKEY enhancements:**
  - New sub keyword TOKEN is added to indicate the generation of secure TKDS key. For example:
    - Generate a certificate with RSA key stored in a token called MY.PKCS11.TOKEN1 in TKDS
      - RACDCERT GENCERT SUB(CN('Company A')) WITHLABEL('New RSA cert') RSA**(TOKEN(MY.PKCS11.TOKEN1))**
    - Generate a certificate with NISTECC key stored in a token called MY.PKCS11.TOKEN2 in TKDS
      - RACDCERT GENCERT SUB(CN('Company A')) WITHLABEL('New ECC cert') NISTECC**(TOKEN(MY.PKCS11.TOKEN2))**

&RACUID and BPX.UNIQUE.USER

&RACUID in BPX.UNIQUE.USER

- **Clients who are using BPX.UNIQUE.USER to assign z/OS UNIX information to user IDs will be able to specify of &racuid in the home directory field of the model user's OMVS segment.**
  - `ALTUSER BPXMODEL OMVS(HOME(/u/&racuid))`
- **The appropriate user ID will be substituted for &racuid when a new OMVS segment is created for a user using BPX.UNIQUE.USER**
  - In upper case if “&RACUID” is specified
  - In lower case if any lower case characters are specified
- **Notes**
  - Only the first occurrence of &racuid is substituted
  - If the substitution would result in a path name exceeding the 1023 character maximum then substitution is not performed.
  - If sharing the RACF database with a downlevel system, substitution will not be performed on the downlevel system

JES2/JES3 SAF Check for Job Input Class

JES2/JES3: SAF Check for Job Input Class

- **JES2 and JES3 now perform a SAF check to verity a user's ability to use a job class**
  - Applies to both the “traditional” 36 single character classes as well as the planned up-to-eight character job classes
  - Does not apply to the “special” job classes STC and TSU
- **The resource name that is checked is:**
  - JESJOBS.*nodename.jobclass.jobname* in the JESJOBS class
- **Controlled by these profiles:**
  - JES.JOBCLASS.OWNER in the FACILITY class
    - If this profile is defined, then authorization checks are performed for job owners
  - JES.JOBCLASS.SUBMITTER in the FACILITY class
    - If this profile is defined, then authorization checks are performed for job submitters

PKI Services Enhancements

PKI Services Enhancements in z/OS V2.1

- Support for Extended Validation Certificates
- Granular Access Control
- Certificate Authority Path Length
- CRL Notification
- DB2 Custom Columns
- Secure TKDS Support

RACF Statement of Direction

z/OS V2.1 RACF Statement of General Direction

- **Enhanced RACF password encryption algorithm:**
  - In the future, an enhanced RACF password encryption algorithm is planned. This support will be designed to provide improved cryptographic strength in RACF password algorithm processing. This will be intended to help protect RACF password data in the event that a copy of a RACF database becomes inadvertently accessible.

Background: z/OS V1.13 Statement of Direction BPX.DEFAULT.USER

Statement of Direction

z/OS V1.13 is planned to be the last release to support BPX.DEFAULT.USER. IBM recommends that you either use the BPX.UNIQUE.USER support that was introduced in z/OS V1.11, or assign unique UIDs to users who need them and assign GIDs for their groups.

From *Preview: z/OS Version 1 Release 13 and z/OS Management Facility Version 1 Release 13 are planned to offer new availability, batch programming, and usability functions (*IBM United States Software Announcement 211-007, February 15, 2011)

z/OS V1.13 Statement of Direction …

- **Background: Assigning UID and GIDs**
  - **RACF 2.1 (1994):** Introduced OMVS segments for USERs and GROUPs.
    - Users with an OMVS segment could now use “Open MVS” (now z/OS UNIX System Services)
  - **OS/390 R2.4 (1997**): Introduced BPX.DEFAULT.USER FACILITY class profile
    - Allows assigning UIDs and GIDs to users and groups who do not have OMVS segments;

      One UID and one GID shared by all default users

z/OS V1.13 Statement of Direction …

- **Background: Assigning UID and GIDs…**
  - **z/OS V1.4 (2002):** Introduced AUTOUID/AUTOGID keyword on ADDUSER, ALTUSER, ADDGROUP, ALTGROUP
    - RACF could now find the next available UID or GID using the BPX.NEXT.USER profile in the FACILITY class
    - Required enabling RACF Alternate Index Mapping (“AIM”) to stage 2
      - Limitation of 129 eight-character users sharing one UID
      - Required running migration utility (“IRRIRA00”)
  - **z/OS V1.11 (2009):** Automatic generation of OMVS segment for USERs and groups
    - Built upon AUTOUID/AUTOGID
    - Requires AIM stage 3
    - Uses the BPX.UNIQUE.USER profile in the FACILITY class

z/OS V1.13 Statement of Direction (RACF) …

- **What this means to you:**
  - If you are using BPX.UNIQUE.USER then:
    - You are not using BPX.DEFAULT.USER (even if it is defined)
    - This SoD has no impact to you.
  - If you are already assigning UIDs and GIDs to all users using z/OS UNIX System Services by assigning OMVS segments to all necessary users and groups, then:
    - You must continue to assign all new users and groups OMVS segments
  - If you are already assigning UIDs and GIDS to all users using z/OS UNIX System Services by defining OMVS segments using AUTOUID/AUTOGID (which uses BPX.NEXT.USER) then:
    - You are already using AIM at a minimum of stage 2
    - You must continue to assign all new users and groups OMVS segments
  - If you are using only BPX.DEFAULT.USER
    - You must either move to the automatic generation of OMVS user and group segments or assign OMVS user and group segments to all necessary users and groups

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(IBMRACF,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

Helpful Publications

- SA23-2290 - z/OS Security Server RACF Callable Services
- SA23-2292 - z/OS Security Server RACF Command Language Reference
- GA32-0885 - z/OS Security Server RACF Data Areas
- SA23-2288 - z/OS Security Server RACF Macros and Interfaces
- SA23-2291 - z/OS Security Server RACF Messages and Codes
- SA23-2289 - z/OS Security Server RACF Security Administrator's Guide
- SA23-2287 - z/OS Security Server RACF System Programmer's Guide
- SA23-2294 - z/OS Security Server RACROUTE Macro Reference
- GA32-0886 - z/OS Security Server RACF Diagnosis Guide
- SA23-2286 - z/OS Cryptographic Services PKI Services Guide and Reference
- SC14-7495 - z/OS Cryptographic Services System Secure Sockets Layer Programming
- SA23-2231 - z/OS ICSF Writing PKCS #11 Applications
- SA23-2284 - z/OS UNIX System Services: Messages and Codes
- SA23-2281 - z/OS UNIX System Services Programming: Assembler Callable Services Reference
- SC27-3651 - z/OS Communication Server: IP Configuration Guide
- GC27-2652 - z/OS Communication Server: IP Diagnosis Guide
- SC27-3661 - z/OS Communication Server: IP System Administrator's Commands
- SA23-6843 - IBM Health Checker for z/OS User's Guide