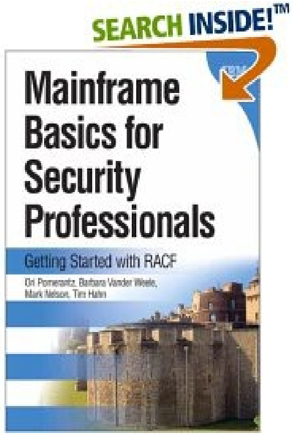
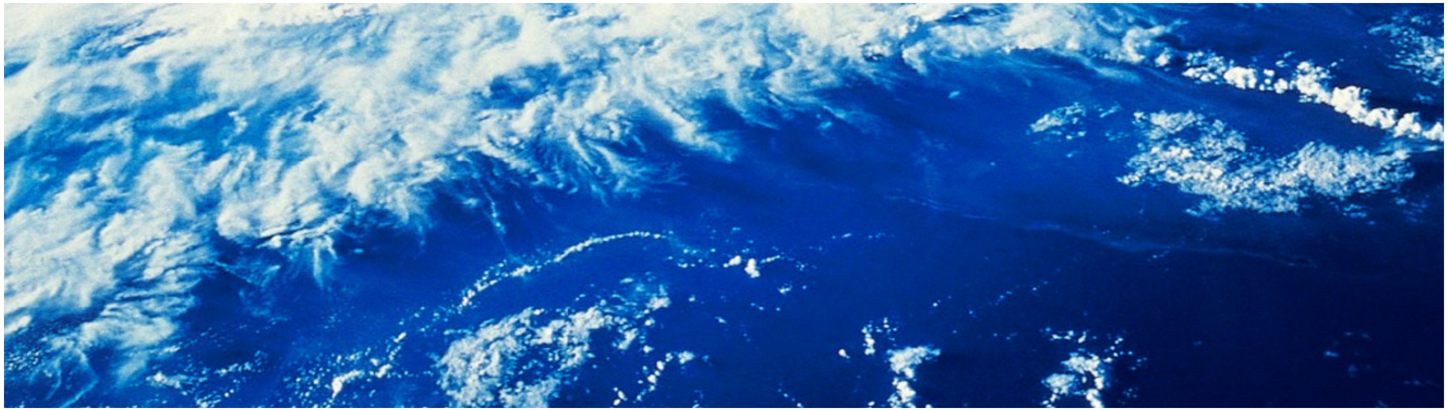
z/OS® V2.1 RACF® Update

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

Vanguard Security and Compliance (RACF 2!1"#
Session RAA02
June 2014


SEARCH INSIDE!™
Mainframe Basics for Security Professionals
Getting Started with RACF
Ori Pomerantz, Barbara Vander Weele, Mark Nelson, Tim Hahn



$rademar()

$%e &ollo ' ing are trademar() o& t%e *nternational +u)ine)) , ac%ine) Corporation in t%e United State) and/or ot%er countrie).

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

- %at.) ne ' ' it% z/OS V2.1 RACF /

- Common Criteria **01**aluation Update
- RRSF
  - Support for TCP/IP V6
  - Comments in the RACF parameter library
  - TLS 1.2 cipher suite support
- **2**e ' and impro**1**ed RACF **3**ealt% C%ec**()**
  - RACF_AIM_STAGE, RACF_UNIX_ID, RACF_CERTIFICATE_EXPIRATION, RACF_SENSITIVE_RESOURCES
- Certi&icate i**))**uer di**)**tingui**)**%ed name4 **)**u**5**6ect di**)**tingui**)**%ed name**)** and **)**ignature algorit%m**)**4 in *RR**7** **+**U**!!** output
- RAC**7**C**0**R**$** **0**n%ancement**)**
- **8**RACU***7** in %ome directory pat% name
- Acce**))** control**)** &or **90**S2/**90**S**:** 6o**5** cla**))**e**)**
- **;<*** Ser**1**ice**)** **0**n%ancement**)**
- Statement o& **7**irection

Common Criteria Update

Common Criteria Update

- Recent Common Criteria 01aluation) o& *ntere)t=
    - 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 GA1 EAL5+, 19 February, 2013
    - PR/SM for IBM zEnterprise EC12 GA2/BC12 GA1 EAL5+, 19 February, 2014

- %ttp=//' ' '.i5m.com/)ecurity/)tandard)/)ecurity>e1aluation).%tml %a) t%e detail)

RRSF

RRSF= ?uic($C;/*; Re1ie'

- Starting 'it% z/OS V1.1:4 you can lin(RRSF node) u)ing $C;/*; in)tead o& A;;C@ $%i) mean) t%at you can no'=
  - 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
  - <eep up 'it% impro1ement) in z/OS Communication) Ser1er Security.

RRSF= * ; 1A Support

- Starting ' it% z/OS V2.14 RRSF)upport) t%e u)e o& $C ; /* ; VA &or communication) 5et ' een/among your RRSF node)
  - 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=*;1A Addre))e)

7e)cription	*;1"	*;1A
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= $ARB0$ C*S$ (V1.1:#

```
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      - 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= $ARB0$ C*S$(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= Comment) in ;arameter Ci5rary

- ;rior to z/OS V2.14 5lan(line) or '%ole line comment) 'ould re)ult in an *RRC!!:* (DCO , , A27 EEEEE *S 2O$ VAC*7F# error me))age

- - it% z/OS V2.14 5lan(line) and '%ole line comment) are allo'ed
  - 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= $CS 1.2 Cip%er Suite Support

- RRSF u)e) Application $ran)parent $ran)port Cayer Security (A$ $CS# to encrypt data 5et'een RRSF node)
  - 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

- -%en a connection i) e)ta5li)%ed 5et'een 2 RRSF)y)tem)4 %ere i) an eEample o& t%e in&ormational me))age i))ued 5y RACF=

  -
    ```
    IRRI027I (>) RACF COMMUNICATION WITH TCP NODE NODE1 HAS
    BEEN SUCCESSFULLY ESTABLISHED USING CIPHER ALGORITHM C026
    TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384.
    ```

3ealt% C%ec(Update)

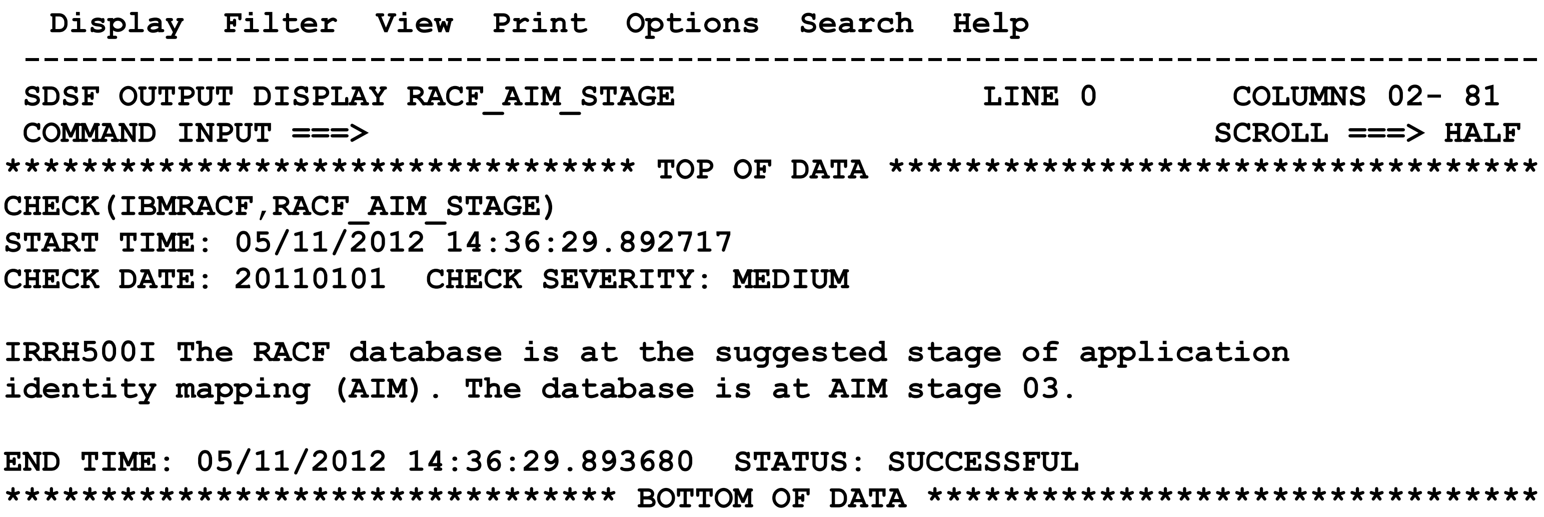
3ealt% C%ec()= 2e' and Updated C%ec()

- $%ere are t%ree ne' RACF 3ealt% C%ec() in z/OS V2.1=
  - RACF_AIM_STAGE
  - RACF_UNIX_ID
  - RACF_CERTIFICATE_EXPIRATION
- RACF>A*,>S$AB0 and RACF>U2*G>*7 are intended to a))i)t you in migrating &rom +;G.70FAUC$.US0R4 '%ic%4 a) announced4 i) 5eing 'it%dra'n 'it% z/OS V2.1
  - These two checks rolled back to z/OS V1.12 and z/OS V1.13 with OA37164
- Automatic)tart &or t%e 3ealt% C%ec(er addre)))pace at *;C time
- $'o ne' c%ec() and an update to RACF>S02S*$*V0>R0SOURC0S
  - RACF_CSFKEYS_ACTIVE
  - RACF_CSFSERV_ACTIVE
  - Inclusion of ICSF CKDS, PKDS, and TKDS data sets in RACF_SENSITIVE_RESOURCES

3ealt% C%ec()= RACF>A* , >S$AB0

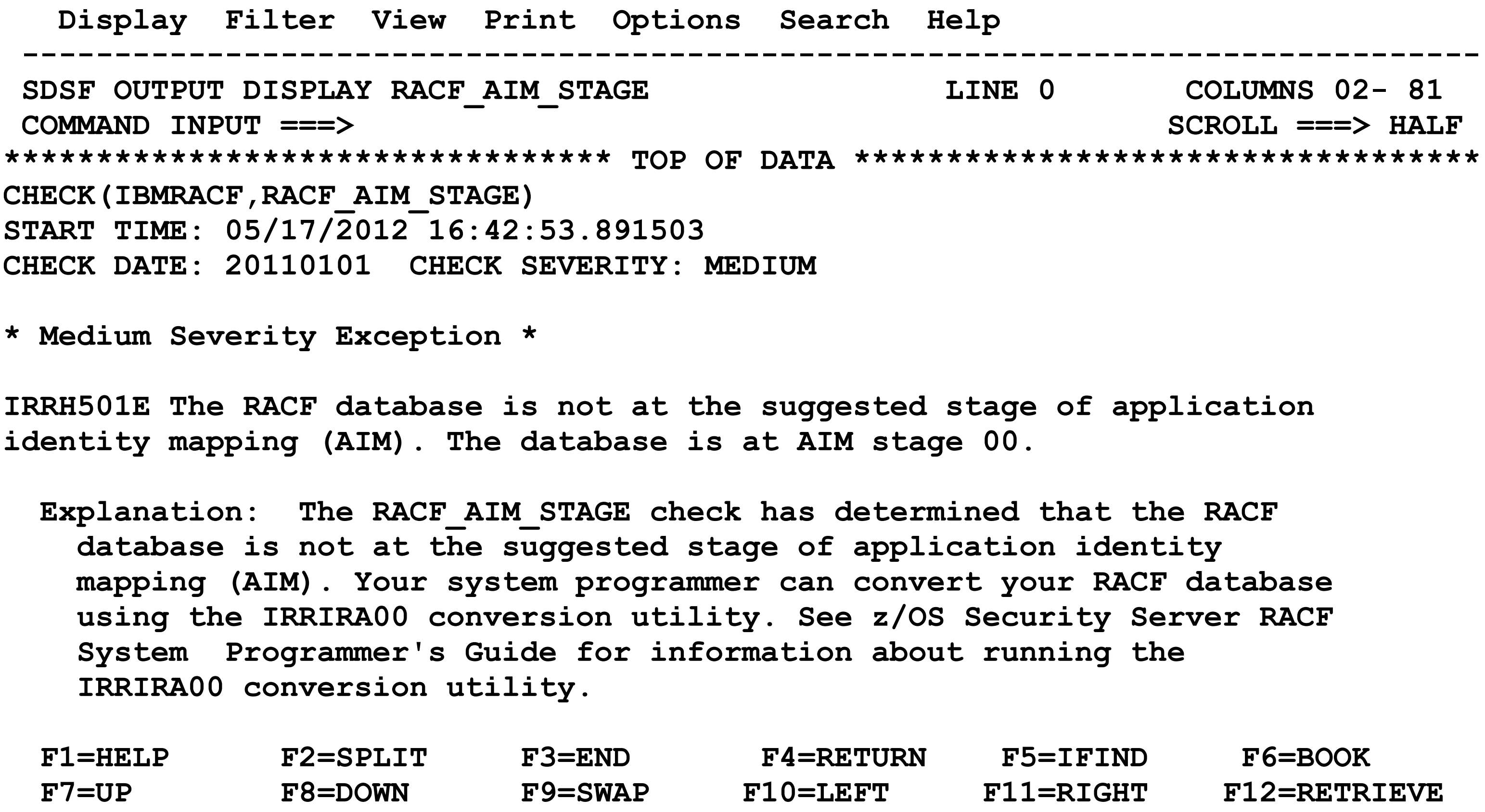
- $%e RACF>A* , >S$AB0 3ealt% C%ec(eEamine) your application identity mapping (A* , #)etting and &lag) a) an eEception i& you are at a)tage le)) t%an)tage :.
  - Stage 0: No AIM support; only mapping profiles are used
  - Stage 1: Mapping profiles are used; alternate index created and managed, but not used
  - Stage 2: Alternate index create, managed, and used; mapping profiles maintained.
  - Stage 3: Only alternate index maintained and used. Mapping profiles deleted.
- , o1ing &rom eac%)tage reHuire) t%e eEecution o& t%e *RR*RA! ! utility.
- A* ,)tage 2 or)tage : i) needed &or certain RACF &unction)

3ealt% C%ec()= RACF>A* , >S$AB0 (O<#



```
  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 ********************************
```

3ealt% C%ec()= RACF>A* , >S$AB0 (0Eception#

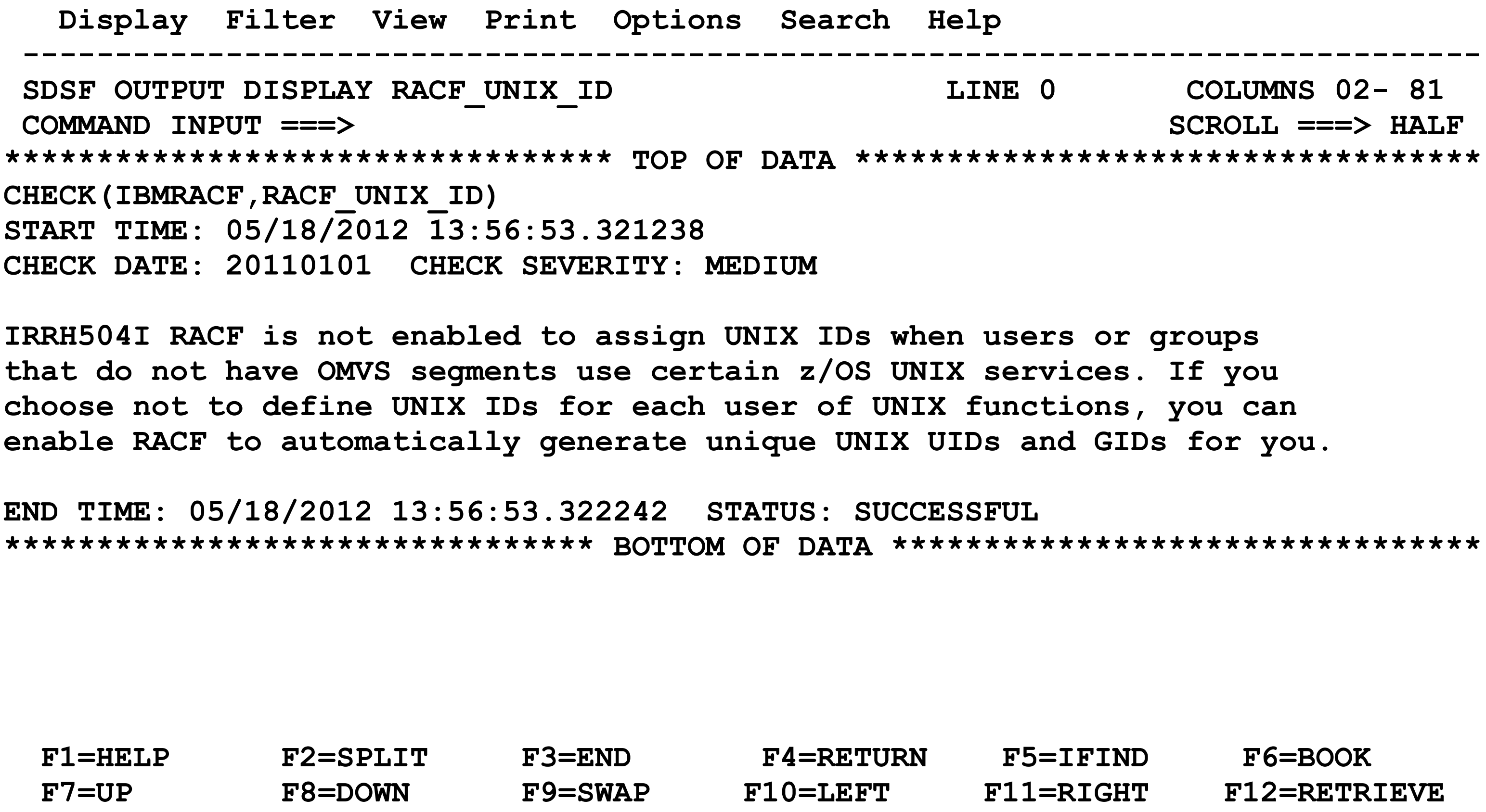


```
   Display  Filter  View  Print  Options  Search  Help
 -------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_AIM_STAGE                LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                              SCROLL ===> HALF
********************************* 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
```

3ealt% C%ec()= RACF>U2*G>*7

- $%e RACF>U2*G>*7 3ealt% C%ec(determine) '%et%er RACF 'ill automatically a))ign uniHue z/OS U2*G Sy)tem Ser1ice) identitie) '%en u)er) 'it%out O,VS)egment) u)e certain U2*G)er1ice)
  - 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.

3ealt% C%ec()= RACF>U2*G>*7 (O<#

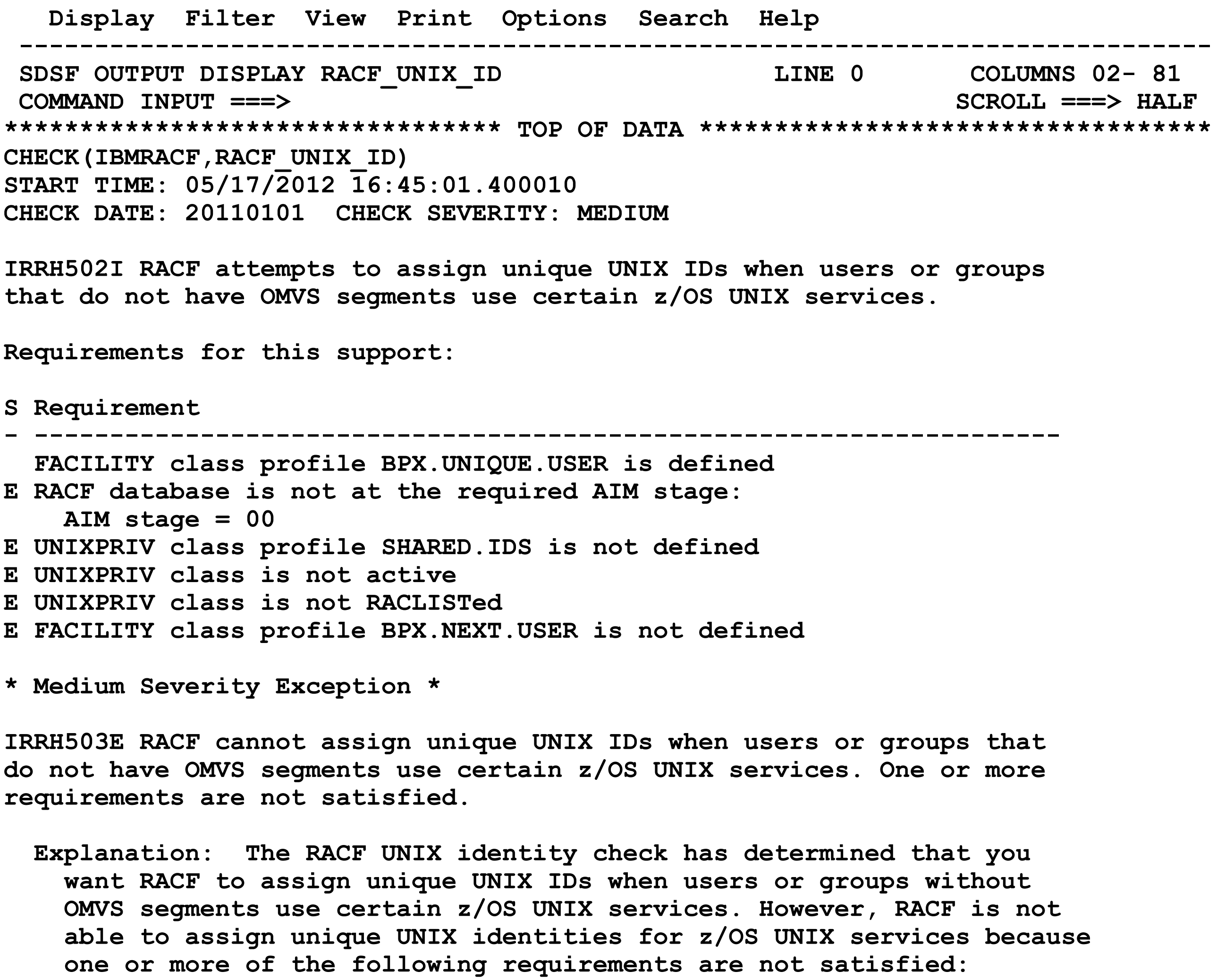


```
    Display  Filter  View  Print  Options  Search  Help
  -------------------------------------------------------------------------------
  SDSF OUTPUT DISPLAY RACF_UNIX_ID                 LINE 0       COLUMNS 02- 81
  COMMAND INPUT ===>                                           SCROLL ===> HALF
 ******************************** 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
```

3ealt% C%ec()= RACF>U2*G>*7 (O<#

```
********************************* 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
```

3ealt% C%ec()= RACF>U2*G>*7 (0Eception#

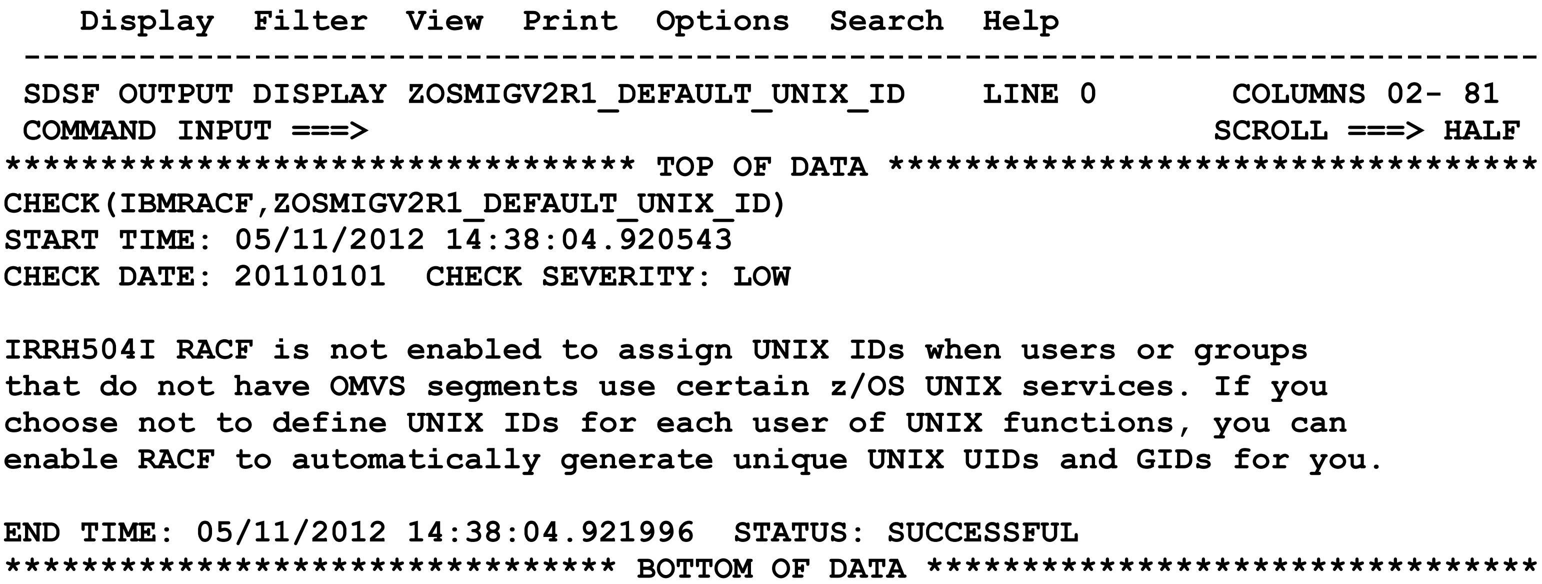


```
   Display  Filter  View  Print  Options  Search  Help
 -------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_UNIX_ID                       LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                                 SCROLL ===> 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:
```

3ealt% C%ec()= RACF>U2*G>*7 (0Eception#

```
********************************* 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 V1.1:= 3ealt% C%ec(I 7e&ault U2*G *7



```
     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 ********************************
```

- $%i) i) a migration c%ec(@
  - 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

3ealt% C%ec()= RACF>C0R$*F*CA$0>0G;*RA$*O2

- $%e RACF>C0R$*F*CA$0>0G;*RA$*O2 %ealt% c%ec(&ind) t%e certi&icate) in t%e RACF data5a)e eEpired or a5out to eEpire
  - Expiration window is an installation-defined value with a default of 60 days.
  - Valid expiration window values are 0-366 days
- For eac% certi&icate4 t%e c%ec(di)play)=
  - 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
- $%e c%ec(only &lag) a) eEception) t%o)e certi&icate) ' %ic% are RUS07.

3ealt% C%ec()= RACF>C0R$*F*CA$0>0G;*RA$*O2 (O<#

```
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
```

3ealt% C%ec()= RACF>C0R$*F*CA$0>0G;*RA$*O2 (0Eception#

```
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.
```

3ealt% C%ec()= RACF>C0R$*F*CA$0>0G;*RA$*O2 (0Eception#

```
    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.
```

3ealt% C%ec()= RACF>S02S*$*V0>R0SOURC0S

- $%e RACF>S02S*$*V0>R0SOURC0S c%ec(%a) 5een updated to c%ec(t%e)e ne' D)taticF re)ource) name)=
  - BPX.DEBUG/FACILITY
  - BPX.WLMSERVER/FACILITY
  - IEAABD.DMPAKEY/FACILITY
  - MVS.SLIP/OPERCMDS
  - SUPERUSER.PROCESS.GETPSENT/UNIXPRIV
  - SUPERUSER.PROCESS.KILL/UNIXPRIV
  - SUPERUSER.PROCESS.PTRACE/UNIXPRIV

3ealt% C%ec()= RACF>S02S*$*V0>R0SOURC0S...

- RACF i) updating t%e RACF>S02S*$*V0>R0SOURC0S to c%ec(t%e)e ne' DdynamicF re)ource) name)=
  - 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)
- 2o 1alidation i) per&ormed on t%e dynamic portion o& t%e)e re)ource name) (&or eEample ***data_set_ name, module_name,lnklstname***#

3ealt% C%ec()= RACF>S02S*$*V0>R0SOURC0S...

```
                      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   ****
```

3ealt% C%ec()= RACF>S02S*$*V0>R0SOURC0S...

- RACF i) updating t%e RACF>S02S*$*V0>R0SOURC0S to c%ec(&or t%e *CSF C<7S4 ;<7S4 and $<7S data)et).

- *& *CSF %a) not 5een)tarted4 in&ormational me))age D*RR32"2*= *CSF %a) not 5een)tarted on t%i))y)temF i) i))ued and t%e c%ec(continue) proce))ing.

```
                     System Rexx Dataset Report

S Data Set Name                           Vol    UACC Warn ID*  User
- --------------------------------------- ------ ---- ---- ---- ----
  SYS1.SAXREXEC                           ZDR22B Read No   ****

                          ICSF Dataset Report

S Data Set Name                           Vol    UACC Warn ID*  User
- --------------------------------------- ------ ---- ---- ---- ----
V RACFTEST.CLC.PKDS2
V RACFTEST.CLC.CKDS
```

Certi&icate 7i)tingui)%ed 2ame) in *RR7+U!! Output

*RR7+U!!= Additional Certi&icate *n&ormation

- $%e RACF 7ata5a)e Unload Utility (*RR7+U!!# unload) 5a)ic in&ormation a5out digital certi&icate) into t%e !JA! (DBeneral Re)ource Certi&icate 7ata RecordF#. $%i) record contain)=
  - 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
- -%atK) mi))ing/ $%e i))uerK) di)tingui)%ed name (*72# and t%e)u56ectK) 72 (S72#o& t%e certi&icate@
  - 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

*RR7+U!!= Additional Certi&icate *n&ormation...

- $%e ne' record type (D1JA!F# contain)=
  - The issuer's distinguished name
  - The subject's distinguished name
  - The hashing algorithm used for the signing the certificate
- $%e D1JA!F record lin() to t%e D!JA!F record u)ing t%e pro&ile name
  - DFSORT's JOINKEY operator can be used when processing IRRDBU00 output
- $%e ,apping o& t%e1JA! Record i)=

		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.

RAC7C0R$ 0n%ancement)

RAC7C0R$ A77 0n%ancement

- ;rior to z/OS V2.14 i& you u)ed RAC7C0R$ A77 to add a ;<CSL12 or ;<CSLM certi&icate c%ain u)ing t%e RAC7C0R$ A77 command4 only t%e end entity certi&icate can 5e named u)ing a)peci&ied la5el.
  - RACDCERT generates labels for the rest of the certificates in the chain, but previously did not di)play '%at la5el) had been added.

- Starting in V2R14 RAC7C0R$ 'ill di)play t%e generated la5el) o& any certi&icate) in t%e c%ain t%at 'ere 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
```

RAC7C0R$ C*S$C3A*2 0n%ancement

- Starting in V2R1 RACF i) adding t%e a5ility to li)t a certi&icate c%ain ' it% t%e introduction o& t%e RAC7C0R$ C*S$C3A*2 command.

- RAC7C0R$ C*S$C3A*2 SyntaE=

```
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

RAC7C0R$ C*S$C3A*2 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
```

RAC7C0R$ B02R0? 0n%ancement

- Benerating a Certi&icate ReHue)t (CSR# &rom RAC7C0R$ B02R0? reHuire) an eEi)ting certi&icate in RACF 'it% a pri1ate (ey (u)ually a)el&)igned certi&icate created 'it% B02C0R$#.

- 7onKt delete t%at 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 RAC7C0R$ 'ill pre1ent t%e deletion o& a certi&icate t%at %a) 5een u)ed &or generating a reHue)t 'it% B02R0?.
  - Force override mechanism is provided to delete this certificate when needed

RAC7C0R$ C30C<C0R$ 0n%ancement

- RAC7C0R$ C30C<C0R$ en%ancement=
  - 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.

RAC7C0R$ Support &or Secure $<7S

- Unli(e t%e (ey))tored in t%e ;u5lic <ey 7ata Set (;<7S#4 t%e (ey))tored in t%e $o(en <ey 7ata Set ($<7S# are clear (ey)4 not)ecure (ey).
- DSecure <eyF mean) t%at)en)iti1e (ey material i) al ' ay) ' rapped under a ma)ter (ey.
- *n - e5 7eli1era5le L124 *CSF)upport))ecure (ey in $<7S.
- $o ena5le t%e application) to u)e t%e)ecure (ey in $<7S4 RACF4 ;<* Ser1ice) and Sy)tem SSC need to 5e updated accordingly.

RAC7C0R$ Support &or Secure $<7S

- RAC7C0R$ can create a)ecure (ey on a)peci&ied ;<CSL11 to(en on $<7S during certi&icate creation
- $%i) ne')upport allo') RAC7C0R$ to i))ue and u)e o& certi&icate) 'it% %ard'are protected (ey) in a ;<CSL11 $<7S to(en.
  - RACDCERT EXPORT can not export any secure key neither from PKDS nor TKDS
- RAC7C0R$ B02C0R$ / R0<0N en%ancement)=
  - 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($O<02(, N. ; <CS11.$O<021##
    - 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($O<02(, N. ; <CS11.$O<022##

8RACU***7** and **+;G**.U**2*?**U**0**.US**0**R

8RACU*7 in +;G.U2*?U0.US0R

- Client) '%o are u)ing +;G.U2*?U0.US0R to a))ign z/OS U2*G in&ormation to u)er *7) 'ill 5e a5le to)peci&y o& 8racuid in t%e %ome directory &ield o& t%e model u)er() O,VS)egment.
  - `ALTUSER BPXMODEL OMVS(HOME(/u/&racuid))`
- $%e appropriate u)er *7 'ill 5e)u5)tituted &or 8racuid '%en a ne' O,VS)egment i) created &or a u)er u)ing +;G.U2*?U0.US0R
  - In upper case if “&RACUID” is specified
  - In lower case if any lower case characters are specified
- 2ote)
  - 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

90S2/90S: SAF C%ec(&or 9o5 *nput Cla))

90S2/90S:= SAF C%ec(&or 9o5 *nput Cla))

- 90S2 and 90S: no' per&orm a SAF c%ec(to 1erity a u)er') a5ility to u)e a 6o5 cla))
  - Applies to both the “traditional” 36 single character classes as well as theup-to-eight character job classes
  - Does not apply to the “special” job classes STC and TSU
- $%e re)ource name t%at i) c%ec(ed i)=
  - JOBCLASS.*nodename.jobclass.jobname* in the JESJOBS class
- Controlled 5y t%e)e pro&ile)=
  - 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

; <* Ser1ice) 0n%ancement)

; <* Ser1ice) 0n%ancement) in z/OS V2.1

- Support &or 0Etended Validation Certi&icate)
- Branular Acce)) Control
- Certi&icate Aut%ority ;at% Cengt%
- CRC 2oti&ication
- 7+2 Cu)tom Column)
- Secure $<7S Support

RACF Statement o& 7irection

z/OS V2.1 RACF Statement o& Beneral 7irection

- 0n%anced RACF pa))'ord encryption algorit%m=
  - 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.

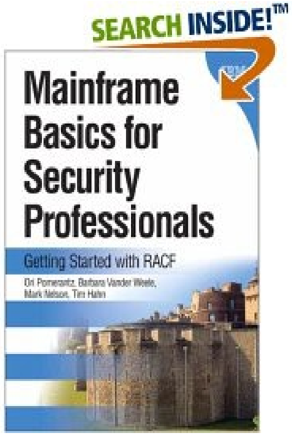
3elp&ul ;u5lication)

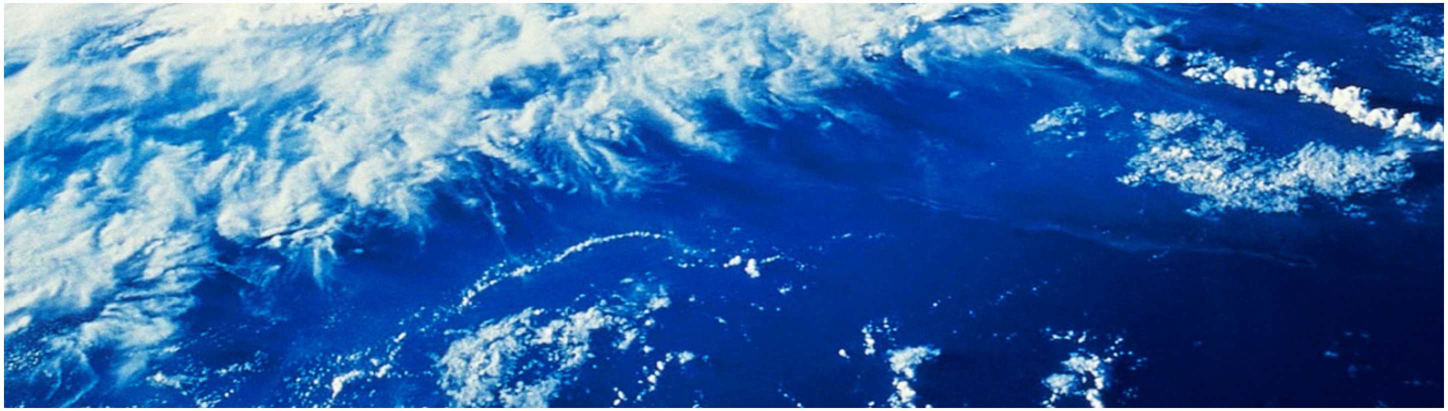
- SA2: 220! z/OS Security Ser1er RACF Calla5le Ser1ice)
- SA2: 2202 z/OS Security Ser1er RACF Command Canguage Re&erence
- BA:2 !PPJ z/OS Security Ser1er RACF 7ata Area)
- SA2: 22PP z/OS Security Ser1er RACF ,acro) and *nter&ace)
- SA2: 2201 z/OS Security Ser1er RACF ,e))age) and Code)
- SA2: 22P0 z/OS Security Ser1er RACF Security Admini)tratorK) Buide
- SA2: 22PM z/OS Security Ser1er RACF Sy)tem ;rogrammerK) Buide
- SA2: 220" z/OS Security Ser1er RACROU$0 ,acro Re&erence
- BA:2 !PPA z/OS Security Ser1er RACF 7iagno)i) Buide
- SA2: 22PA z/OS Cryptograp%ic Ser1ice) ;<* Ser1ice) Buide and Re&erence
- SC1" M"0J z/OS Cryptograp%ic Ser1ice) Sy)tem Secure Soc(et) Cayer ;rogramming
- SA2: 22:1 z/OS *CSF -riting ;<CS L11 Application)
- SA2: 22P" z/OS U2*G Sy)tem Ser1ice)= ,e))age) and Code)
- SA2: 22P1 z/OS U2*G Sy)tem Ser1ice) ;rogramming= A))em5ler Calla5le Ser1ice) Re&erence
- SC2M :AJ1 z/OS Communication Ser1er= *; Con&iguration Buide
- BC2M 2AJ2 z/OS Communication Ser1er= *; 7iagno)i) Buide
- SC2M :AA1 z/OS Communication Ser1er= *; Sy)tem Admini)tratorK) Command)
- SA2: AP": *+, 3ealt% C%ec(er &or z/OS U)erK) Buide

z/OS® V2.1 RACF® Update

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

Vanguard Security and Compliance (RACF 2!1"#
Session RAA02
June 2014


SEARCH INSIDE!™
Mainframe Basics for Security Professionals
Getting Started with RACF
Ori Pomerantz, Barbara Vander Weele, Mark Nelson, Tim Hahn



Statement o& 7irection

z/OS V1.1: i) planned to 5e t%e la)t relea)e to)upport +;G.70FAUC$.US0R. *+, recommend) t%at you eit%er u)e t%e +;G.U2*?U0.US0R)upport t%at 'a) introduced in z/OS V1.114 or a))ign uniHue U*7) to u)er) '%o need t%em and a))ign B*7) &or t%eir group).

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 V1.1: Statement o& 7irection Q

- +ac(ground= A))igning U*7 and B*7)
  - RACF 2.1 (100"#= Introduced OMVS segments for USERs and GROUPs.
    - Users with an OMVS segment could now use “Open MVS” (now z/OS UNIX System Services)
  - OS/:0! R2." (100M): 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

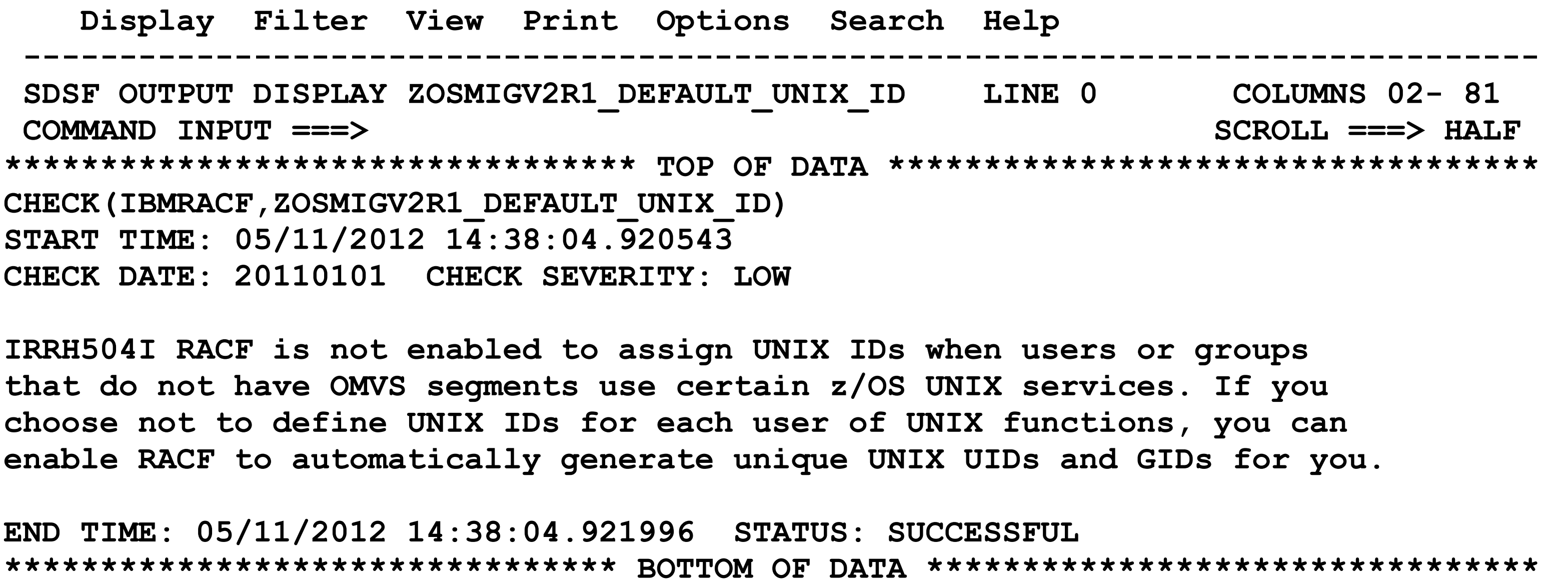
z/OS V1.1: Statement o& 7irection Q

- +ac(ground= A))igning U*7 and B*7)Q
  - z/OS V1." (2!!2#= 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 (2!!0#= 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 V1.1: Statement o& 7irection (RACF# Q

- - %at t%i) mean) 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 V1.1:= 3ealt% C%ec(I 7e&ault U2*G *7



```
   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 ********************************
```

- $%i) i) a migration c%ec(@
  - 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