z/OS

APAR OA37164:
RACF HEALTH AND MIGRATION CHECKS

Preface

This information applies to APAR OA37164 which provides two new RACF health checks and a new RACF V2R1 migration check.

Software requirements

Support for APAR OA37164 requires one of the following software releases:

- z/OS Security Server RACF Version 1 Release 12 (FMID HRF7770)
- z/OS Security Server RACF Version 1 Release 13 (FMID HRF7780)

Chapter 1. z/OS checks

This information supplements *z/OS IBM Health Checker for z/OS: User's Guide*.

RACF_AIM_STAGE

Description:

The RACF_AIM_STAGE check examines the RACF database application identity mapping (AIM) to see whether it is at AIM stage 3, which is recommended. Your system programmer can convert your RACF database to AIM stage 3 using the IRRIRA00 conversion utility.

Reason for check:

AIM stage 3 allows RACF to more efficiently handle authentication and authorization requests from applications such as z/OS UNIX and is required to use some RACF function. You should assign a unique UNIX UID for each user and a unique GID for each group that needs access to z/OS UNIX functions and resources. Assigning unique IDs rather than shared IDs improves overall security and increases user accountability. However, if you have a large number of users without OMVS segments who need access to z/OS UNIX services, such as FTP, you might choose not to assign UNIX identities in advance of their need to use the services. In these cases, when your RACF database has been converted to AIM stage 3, you can enable RACF to automatically assign unique UNIX UIDs and GIDs at the time they are needed.

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_AIM_STAGE)
SEVERITY(MED),INTERVAL(24:00),DATE('date_of_the_change')
REASON('Your reason for making the update.')
```

Debug support:

No

Verbose support:

No

Reference:

- For information on running the IRRIRA00 conversion utility, see *z/OS Security Server RACF System Programmer's Guide*.
- For information about enabling RACF for automatic assignment of unique UNIX identities, see *z/OS Security Server RACF Security Administrator's Guide*.

Messages:

This check issues the following exception messages:

- IRRH501E

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:

- The following shows the output from a RACF_AIM_STAGE check that finds the system at stage 3:

```
CHECK(IBMRACF,RACF_AIM_STAGE)
START TIME: 05/06/2011 10:51:02.926675
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: 05/06/2011 10:51:02.927390  STATUS: SUCCESSFUL
```

- The following shows the output from an exception for RACF_AIM_STAGE:

```
CHECK(IBMRACF,RACF_AIM_STAGE)
START TIME: 05/06/2011 11:06:27.618944
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.

    Stage 3 of application identity mapping allows RACF to more
    efficiently handle authentication and authorization requests from
    applications such as z/OS UNIX and is required to use some RACF
    function. You should assign a unique UNIX UID for each user and a
    unique GID for each group that needs access to z/OS UNIX functions
    and resources. Assigning unique IDs rather than shared IDs improves
    overall security and increases user accountability. However, if you
    have a large number of users without OMVS segments who need access
    to z/OS UNIX services, such as FTP, you might choose not to assign
    UNIX identities in advance of their need to use the services. In
    these cases, when your RACF database has been converted to AIM stage
    3, you can enable RACF to automatically assign unique UNIX UIDs and
    GIDs at the time they are needed. See z/OS Security Server RACF
    Security Administrator's Guide for information about enabling RACF
    for automatic assignment of unique UNIX identities.

  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:  If you want to use RACF function such as
    support for automatically assigning unique UNIX UIDs and GIDs at the
    time that they are needed, run the IRRIRA00 utility to advance the
    RACF database to application identity mapping stage 3. For details
    about using the IRRIRA00 utility, see z/OS Security Server RACF
    System Programmer's Guide.

  Problem Determination:

  Source:
```

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

  Automation:  None.

  Check Reason:  AIM Stage 3 is suggested.

END TIME: 05/06/2011 11:06:27.620454  STATUS: EXCEPTION-MED
```

RACF_UNIX_ID

Description:

z/OS V1R13 is the last release that supports default UNIX identities implemented using using the BPX.DEFAULT.USER profile in the FACILITY class. To replace this function you can do one of the following:

- Use the replacement BPX.UNIQUE.USER profile function provided in z/OS R11 to enable RACF to automatically generate unique UIDs and GIDs.
- Define OMVS segments for all users and groups who require UNIX services.

The RACF_UNIX_ID check detects whether RACF is enabled to perform the best practice of automatically assigning unique UNIX identities when users without OMVS segments access the system to use UNIX services. This determination is based on whether the BPX.UNIQUE.USER and BPX.DEFAULT.USER profiles are defined in the FACILITY class. The following table summarizes the actions of the check:

Table 1. RACF_UNIX_ID check actions based on whether the BPX.UNIQUE.USER and BPX.DEFAULT.USER profiles are defined in the FACILITY class

BPX.UNIQUE.USER defined in Facility	BPX.DEFAULT.USER defined in Facility	Check action
No	No	RACF is not enabled to assign z/OS UNIX identities to users or groups who do not have OMVS segments. The check issues informational message IRRH504I (see "“RACF_UNIX_ID output” on page 4") and does not raise an exception, but you should use the best practice of assigning a unique UID and a unique GID to each user and group which needs access to z/OS UNIX functions and resources using either the BPX.UNIQUE.USER profile or by defining OMVS segments manually.
No	Yes	The presence of the BPX.DEFAULT.USER profile without the BPX.UNIQUE.USER profile indicates an intent to use default OMVS segment support, which is not recommended. The check raises a medium severity exception and issues error message IRRH505E. See "“RACF_UNIX_ID output” on page 4".
Yes	Yes or No	The presence of the BPX.UNIQUE.USER profile (with or without BPX.DEFAULT.USER) indicates an intent to have RACF automatically generate unique UNIX UIDs and GIDs, as is recommended. The check issues informational message IRRH502I and then verifies requirements for the automatic generation of unique UNIX IDs. IRRH502I includes a report showing whether all requirements have been met. See a sample of IRRH502I in "“RACF_UNIX_ID output” on page 4" The check's action then depends on whether it finds that requirements have been met or not: • If all requirements have been met, the check raises no exceptions and issues informational message IRRH506I. • If the check detects that not all requirements have been met, the check raises a medium severity exception and issues error message IRRH503E. Note that if both the BPX.UNIQUE.USER and BPX.DEFAULT.USER profiles are defined, RACF automatically assigns unique UNIX IDs. In this case, RACF does not use the BPX.DEFAULT.USER profile and, therefore does not do default OMVS segment processing.

Reason for check:

IBM recommends that a unique UNIX UID be assigned to each user and that a unique GID be assigned to each group that needs access to z/OS UNIX functions and resources. Assigning unique identities, rather than shared identities, improves overall security and increases user accountability.

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_UNIX_ID)
SEVERITY(MED),INTERVAL(24:00),DATE('date_of_the_change')
REASON('Your reason for making the update.')
```

Debug support:

No

Verbose support:

No

Reference:

z/OS Security Server RACF Security Administrator's Guide

Messages:

This check issues the following exception messages:

- IRRH503E
- IRRH505E

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:

- The following shows the output from a RACF_UNIX_ID check that finds neither the BPX.UNIQUE.USER or BPX.DEFAULT.USER profiles are defined:

```
CHECK(IBMRACF,RACF_UNIX_ID)
START TIME: 05/11/2011 10:26:01.195890
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: 05/11/2011 10:26:01.201875  STATUS: SUCCESSFUL
```

- The following shows the output from an exception for RACF_UNIX_ID when the presence of the BPX.DEFAULT.USER profile without the BPX.UNIQUE.USER profile indicates an intent to use default OMVS segment support, which is not recommended:

```
CHECK(IBMRACF,RACF_UNIX_ID)
START TIME: 05/10/2011 16:02:41.125401
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.

    On z/OS V1R13 and below, you have the option of enabling RACF to
    assign default z/OS UNIX identities, however it is not suggested.
    You should either define OMVS segments for user and group profiles,
    with unique UIDs and GIDs, or you should enable RACF to
    automatically assign unique z/OS UNIX identities when users without
    OMVS segments access the system to use certain UNIX services.
    Assigning unique identities rather than shared identities improves
    overall security and increases user accountability.

    See z/OS Security Server RACF Security Administrator's Guide for
    more information about how to assign a user identifier (UID) to a
    RACF user and how to assign a group identifier (GID) to a RACF
    group. z/OS Security Server RACF Security Administrator's Guide also
    contains information about how to enable RACF to automatically
    assign unique UNIX identities.

    Note: z/OS V1R13 is the last release that supports default UNIX
    identities. After z/OS V1R13, users and groups that need to access
    z/OS UNIX functions and resources must be assigned unique UNIX UIDs
    and unique GIDs in advance of their need to access these services,
    or you must enable RACF to automatically assign unique z/OS UNIX
    identities when users without OMVS segments access the system to use
    certain UNIX services. The FACILITY class BPX.DEFAULT.USER profile
    will no longer be used and can be deleted.

  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:

  Source:

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

  Automation:  None.

  Check Reason:  Unique UNIX identities are recommended.

END TIME: 05/10/2011 16:02:41.126280  STATUS: EXCEPTION-MED
```

- The following shows the output from a RACF_UNIX_ID check that finds that the requirements for the automatic generation of unique UNIX IDs have been met:

```
CHECK(IBMRACF,RACF_UNIX_ID)
START TIME: 05/11/2011 09:54:50.971115
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 = 1/0

IRRH506I The RACF UNIX identity check has detected no exceptions.

END TIME: 05/11/2011 09:54:50.972634  STATUS: SUCCESSFUL
```

- The following shows the output from a RACF_UNIX_ID check that finds that the requirements for the automatic generation of unique UNIX IDs have NOT been met and raises an exception:

```
CHECK(IBMRACF,RACF_UNIX_ID)
START TIME: 05/11/2011 09:44:58.682612
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
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:

    1. The RACF database is enabled for application identity mapping
    (AIM) stage 3.

    2. The UNIXPRIV class profile SHARED.IDS is defined and the UNIXPRIV
    class is active and RACLISTed.

    3. The FACILITY class profile BPX.NEXT.USER is defined and its
    APPLDATA field has valid ID values or ranges.

    4. The FACILITY class profile BPX.UNIQUE.USER is defined.

    See z/OS Security Server RACF Security Administrator's Guide for
    more information about enabling RACF for automatic assignment of
    unique UNIX identities.
  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:  The check produces a report listing the
    requirements. An "E" in the "S" (Status) column indicates that a
    requirement is not satisfied. For example, if the RACF database has
    not been enabled for AIM stage 3, this requirement is flagged as an
    exception. If the "S" field is blank, the requirement is satisfied.
    One or more requirements are not satisfied and have been flagged as
    an exception in the Status column.

  Source:

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

  Automation:  None.

  Check Reason:  Unique UNIX identities are recommended.

END TIME: 05/11/2011 09:44:58.740914  STATUS: EXCEPTION-MED
```

ZOSMIGV2R1_DEFAULT_UNIX_ID

Description:

This check determines whether a client is relying on RACF to assign default z/OS UNIX identities for users without OMVS segments who are accessing UNIX services. IBM recommends that a unique UNIX UID be assigned to each user and that a unique GID be assigned to each group that needs access to z/OS UNIX functions and resources.

Starting with z/OS V2R1, support for the default UNIX identity, implemented using the BPX.DEFAULT.USER profile in the FACILITY class, is no longer available, so a migration action may be required if you are using it. The need for a migration action is based on whether the BPX.UNIQUE.USER and BPX.DEFAULT.USER profiles are defined in the FACILITY class. The following table summarizes:

Table 2. ZOSMIGV2R1_DEFAULT_UNIX_ID check actions and migration actions

BPX.UNIQUE.USER defined in Facility	**BPX.DEFAULT.USER defined in Facility**	**Check action and migration action required:**
No	No	RACF is not enabled to assign z/OS UNIX identities to users or groups who do not have OMVS segments. The check issues informational message IRRH504I (see "“ZOSMIGV2R1_DEFAULT_UNIX_ID output” on page 9") and does not raise an exception, but you should use the best practice of assigning a unique UID and a unique GID to each user and group which needs access to z/OS UNIX functions and resources using either the BPX.UNIQUE.USER profile or by defining OMVS segments manually. **Migration action**: Not required; the installation continues to perform as before.

Table 2. ZOSMIGV2R1_DEFAULT_UNIX_ID check actions and migration actions (continued)

BPX.UNIQUE.USER defined in Facility	BPX.DEFAULT.USER defined in Facility	Check action and migration action required:
No	Yes	The presence of the BPX.DEFAULT.USER profile without the BPX.UNIQUE.USER profile indicates an intent to use default OMVS segment support, which is not recommended. The check raises a low severity exception and issues error message IRRH505E. See "“ZOSMIGV2R1_DEFAULT_UNIX_ID output” on page 9". **Migration action**: Required, because default OMVS segment support is not supported in z/OS V2R1 or later. Do one of the following: • Use the replacement BPX.UNIQUE.USER profile function provided in z/OS R11 to enable RACF to automatically generate unique UIDs and GIDs. • Define OMVS segments for all users and groups who require UNIX services.
Yes	Yes or No	The presence of the BPX.UNIQUE.USER profile (with or without BPX.DEFAULT.USER) indicates an intent to have RACF automatically generate unique UNIX UIDs and GIDs, as is recommended. The check issues informational message IRRH502I and then verifies requirements for the automatic generation of unique UNIX IDs. IRRH502I includes a report showing whether all requirements have been met. See a sample of IRRH502I in "“ZOSMIGV2R1_DEFAULT_UNIX_ID output” on page 9" The check's action then depends on whether it finds that requirements have been met or not: • If all requirements have been met, the check raises no exceptions and issues informational message IRRH506I. • If the check detects that not all requirements have been met, it issues informational message IRRH507I and does not raise an exception **Migration action**: Not required - requirements for the automatic generation of unique UNIX IDs are an issue of enablement rather than migration.

Reason for check:

Starting with z/OS V2R1, support for the default UNIX identity, implemented using the BPX.DEFAULT.USER profile in the FACILITY class, is no longer available, so a migration action may be required if you are using it

z/OS releases the check applies to:

z/OS V1R12 and z/OS V1R13

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,ZOSMIGV2R1_DEFAULT_UNIX_ID)
SEVERITY(LOW),INTERVAL(ONETIME),DATE('date_of_the_change')
REASON('Your reason for making the update.')
```

Debug support:

No

Verbose support:

No

Reference:

z/OS Security Server RACF Security Administrator's Guide

Messages:

This check issues the following exception messages:

- IRRH505E

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:

- The following shows the output from a ZOSMIGV2R1_DEFAULT_UNIX_ID check that finds neither the BPX.UNIQUE.USER or BPX.DEFAULT.USER profiles are defined:

```
CHECK(IBMRACF,ZOSMIGV2R1_DEFAULT_UNIX_ID)
START TIME: 05/11/2011 10:34:11.210824
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: 05/11/2011 10:34:11.211004  STATUS: SUCCESSFUL
```

- The following shows the output from an exception for ZOSMIGV2R1_DEFAULT_UNIX_ID when the presence of the BPX.DEFAULT.USER profile without the BPX.UNIQUE.USER profile indicates an intent to use default OMVS segment support, which is not recommended:

```
CHECK(IBMRACF,ZOSMIGV2R1_DEFAULT_UNIX_ID)
START TIME: 05/11/2011 10:36:31.611960
CHECK DATE: 20110101  CHECK SEVERITY: LOW

* Low 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.

    On z/OS V1R13 and below, you have the option of enabling RACF to
    assign default z/OS UNIX identities, however it is not suggested.
    You should either define OMVS segments for user and group profiles,
    with unique UIDs and GIDs, or you should enable RACF to
    automatically assign unique z/OS UNIX identities when users without
    OMVS segments access the system to use certain UNIX services.
    Assigning unique identities rather than shared identities improves
    overall security and increases user accountability.

    See z/OS Security Server RACF Security Administrator's Guide for
    more information about how to assign a user identifier (UID) to a
    RACF user and how to assign a group identifier (GID) to a RACF
    group. z/OS Security Server RACF Security Administrator's Guide also
    contains information about how to enable RACF to automatically
    assign unique UNIX identities.

    Note: z/OS V1R13 is the last release that supports default UNIX
    identities. After z/OS V1R13, users and groups that need to access
    z/OS UNIX functions and resources must be assigned unique UNIX UIDs
    and unique GIDs in advance of their need to access these services,
    or you must enable RACF to automatically assign unique z/OS UNIX
    identities when users without OMVS segments access the system to use
    certain UNIX services. The FACILITY class BPX.DEFAULT.USER profile
    will no longer be used and can be deleted.
  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:

  Source:

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

  Automation:  None.

  Check Reason:  Migration check for BPX.DEFAULT.USER removal.

END TIME: 05/11/2011 10:36:31.612823  STATUS: EXCEPTION-LOW
```

- The following shows the output from a ZOSMIGV2R1_DEFAULT_UNIX_ID check that finds that the requirements for the automatic generation of unique UNIX IDs have been met:

```
CHECK(IBMRACF,ZOSMIGV2R1_DEFAULT_UNIX_ID)
START TIME: 05/11/2011 11:02:39.632614
CHECK DATE: 20110101  CHECK SEVERITY: LOW

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 = 1/0

IRRH506I The RACF UNIX identity check has detected no exceptions.

END TIME: 05/11/2011 11:02:39.634310  STATUS: SUCCESSFUL
```

- The following shows the output from a ZOSMIGV2R1_DEFAULT_UNIX_ID check that finds that the requirements for the automatic generation of unique UNIX IDs have NOT been met and raises an exception:

```
CHECK(IBMRACF,ZOSMIGV2R1_DEFAULT_UNIX_ID)
START TIME: 05/11/2011 11:05:26.315471
CHECK DATE: 20110101  CHECK SEVERITY: LOW

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
E UNIXPRIV class is not active
  UNIXPRIV class is RACLISTed
  FACILITY class profile BPX.NEXT.USER is defined
  BPX.NEXT.USER profile APPLDATA is specified (not verified):
    APPLDATA = 1/0

IRRH507I 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.

END TIME: 05/11/2011 11:05:26.317215  STATUS: SUCCESSFUL
```

Chapter 2. RACF messages and code updates

This information supplements *z/OS Security Server RACF Messages and Codes*.

IRRH500I The RACF database is at the suggested stage of application identity mapping (AIM). The database is at AIM stage 03.

Explanation: The *RACF_AIM_STAGE* check has determined that the RACF database is at the suggested stage of application identity mapping (AIM).

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

Operator response: None.

System programmer response: None.

Problem Determination: None.

Source:

Reference Documentation: None.

Automation: None.

Detecting Module: IRRHCR00

Routing Code:

Descriptor Code:

IRRH501E The RACF database is not at the suggested stage of application identity mapping (AIM). The database is at AIM stage ***AIM-stage*****.**

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.

Stage 3 of application identity mapping allows RACF to more efficiently handle authentication and authorization requests from applications such as z/OS UNIX and is required to use some RACF function. You should assign a unique UNIX UID for each user and a unique GID for each group that needs access to z/OS UNIX functions and resources. Assigning unique IDs rather than shared IDs improves overall security and increases user accountability. However, if you have a large number of users without OMVS segments who need access to z/OS UNIX services, such as FTP, you might choose not to assign UNIX identities in advance of their need to use the services. In these cases, when your RACF database has been converted to AIM stage 3, you can enable RACF to automatically assign unique UNIX UIDs and GIDs at the time they are needed. See *z/OS Security Server RACF Security Administrator's Guide* for information about enabling RACF for automatic assignment of unique UNIX identities.

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: If you want to use RACF function such as support for automatically assigning unique UNIX UIDs and GIDs at the time that they are needed, run the IRRIRA00 utility to advance the RACF database to application identity mapping stage 3. For details about using the IRRIRA00 utility, see *z/OS Security Server RACF System Programmer's Guide*.

Problem Determination:

Source:

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

Automation: None.

Detecting Module: IRRHCR10

Routing Code:

Descriptor Code:

IRRH502I RACF attempts to assign unique 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 determined that you want RACF to assign unique UNIX IDs when users or groups without OMVS segments use certain z/OS UNIX services. Assigning unique UNIX identities rather than shared identities improves overall security and increases user accountability.

RACF automatically assigns unique UNIX identities for z/OS UNIX services when all of the following requirements are satisfied:

1. The RACF database is enabled for application identity mapping (AIM) stage 3.
2. The UNIXPRIV class profile SHARED.IDS is defined and the UNIXPRIV class is active and RACLISTed.

3. The FACILITY class profile BPX.NEXT.USER is defined and its APPLDATA field has valid ID values or ranges.
4. The FACILITY class profile BPX.UNIQUE.USER is defined.

See *z/OS Security Server RACF Security Administrator's Guide* for more information about enabling RACF for automatic assignment of unique UNIX identities.

The check produces a report listing the requirements for this support. An "E" in the "S" (Status) column indicates that a requirement is not satisfied. For example, if the RACF database has not been enabled for AIM stage 3, this requirement is flagged as an exception. If the "S" field is blank, the requirement is satisfied. If there are no exceptions indicated in the Status column, all requirements are satisfied.

Note: The check validates that the FACILITY class profile BPX.NEXT.USER APPLDATA field is present, not that it has valid ID values or ranges.

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

Operator response: None.

System programmer response: None.

Problem Determination:

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

Automation: None.

Detecting Module: IRRHCR10

Routing Code:

Descriptor Code:

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:

1. The RACF database is enabled for application identity mapping (AIM) stage 3.
2. The UNIXPRIV class profile SHARED.IDS is defined and the UNIXPRIV class is active and RACLISTed.
3. The FACILITY class profile BPX.NEXT.USER is defined and its APPLDATA field has valid ID values or ranges.
4. The FACILITY class profile BPX.UNIQUE.USER is defined.

See *z/OS Security Server RACF Security Administrator's Guide* for more information about enabling RACF for automatic assignment of unique UNIX identities.

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: The check produces a report listing the requirements. An "E" in the "S" (Status) column indicates that a requirement is not satisfied. For example, if the RACF database has not been enabled for AIM stage 3, this requirement is flagged as an exception. If the "S" field is blank, the requirement is satisfied. One or more requirements are not satisfied and have been flagged as an exception in the Status column.

Source:

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

Automation: None.

Detecting Module: IRRHCR10

Routing Code:

Descriptor Code:

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.

Explanation: The *RACF UNIX identity* check has determined that RACF is not enabled to assign UNIX IDs when users or groups that do not have OMVS segments use certain z/OS UNIX services. Users and groups that need to access z/OS UNIX functions and resources should be assigned unique UNIX UIDs and unique GIDs in advance of their need to access these services.

However, if you have a large number of users without OMVS segments that need access to z/OS UNIX services, such as FTP, you might choose not to assign UNIX identities in advance. In these cases, you can enable RACF to automatically assign unique UIDs and GIDs at the time they are needed-when users without OMVS segments access certain z/OS UNIX services.

RACF automatically assigns unique identities for z/OS

UNIX services when all of the following requirements are satisfied:

1. The RACF database is enabled for application identity mapping (AIM) stage 3.
2. The UNIXPRIV class profile SHARED.IDS is defined and the UNIXPRIV class is active and RACLISTed.
3. The FACILITY class profile BPX.NEXT.USER is defined and its APPLDATA field has valid ID values or ranges.
4. The FACILITY class profile BPX.UNIQUE.USER is defined.

However, the FACILITY class profile BPX.UNIQUE.USER is not defined, so RACF is not enabled to automatically assign unique UNIX identities for z/OS UNIX services. If you would like to use this support, see *z/OS Security Server RACF Security Administrator's Guide* for more information.

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

Operator response: None.

System programmer response: None.

Problem Determination:

Source:

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

Automation: None.

Detecting Module: IRRHCR10

Routing Code:

Descriptor Code:

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.

On z/OS V1R13 and below, you have the option of enabling RACF to assign default z/OS UNIX identities, however it is not suggested. You should either define OMVS segments for user and group profiles, with unique UIDs and GIDs, or you should enable RACF to automatically assign unique z/OS UNIX identities when users without OMVS segments access the system to use certain UNIX services. Assigning unique identities rather than shared identities improves overall security and increases user accountability.

See *z/OS Security Server RACF Security Administrator's Guide* for more information about how to assign a user identifier (UID) to a RACF user and how to assign a group identifier (GID) to a RACF group. *z/OS Security Server RACF Security Administrator's Guide* also contains information about how to enable RACF to automatically assign unique UNIX identities.

Note: z/OS V1R13 is the last release that supports default UNIX identities. After z/OS V1R13, users and groups that need to access z/OS UNIX functions and resources must be assigned unique UNIX UIDs and unique GIDs in advance of their need to access these services, or you must enable RACF to automatically assign unique z/OS UNIX identities when users without OMVS segments access the system to use certain UNIX services. The FACILITY class BPX.DEFAULT.USER profile is no longer used and can be deleted.

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:

Source:

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

Automation: None.

Detecting Module: IRRHCR10

Routing Code:

Descriptor Code:

IRRH506I The RACF UNIX identity check has detected no exceptions.

Explanation: The *RACF UNIX identity* check has examined the requirements for enabling RACF to assign unique UNIX IDs when users or groups without OMVS segments use certain z/OS UNIX services. No exceptions have been detected.

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

Operator response: None.

System programmer response: None.

Problem Determination:

Source:

Reference Documentation: None.

Automation: None.

Detecting Module: IRRHCR10

Routing Code:

Descriptor Code:

IRRH507I 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 migration 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 do this because one or more requirements are not satisfied.

No migration actions are required because enabling RACF to automatically assign unique z/OS UNIX identities is the recommended alternative to assigning unique UNIX UIDs and unique GIDs to users and groups in advance of their need to access z/OS UNIX functions. However, if you wish to use this support, you should examine the list of requirements and ensure that they are satisfied:

1. The RACF database is enabled for application identity mapping (AIM) stage 3.
2. The UNIXPRIV class profile SHARED.IDS is defined and the UNIXPRIV class is active and RACLISTed.
3. The FACILITY class profile BPX.NEXT.USER is defined and its APPLDATA field has valid ID values or ranges.
4. The FACILITY class profile BPX.UNIQUE.USER is defined.

See *z/OS Security Server RACF Security Administrator's Guide* or more information about enabling RACF for automatic assignment of unique UNIX identities.

The check produces a report listing the requirements. An "E" in the "S" (Status) column indicates that a requirement is not satisfied. For example, if the RACF database has not been enabled for AIM stage 3, this requirement is flagged as an exception. If the "S" field is blank, the requirement is satisfied. One or more requirements are not satisfied and have been flagged as an exception in the Status column.

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

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

System programmer response: None.

Problem Determination: None.

Source:

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

Automation: None.

Detecting Module: IRRHCR10

Routing Code:

Descriptor Code:

Trademarks

IBM®, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Other company, product, and service names may be trademarks or service marks of others.