IBM Education Assistance for z/OS V2R1

Item: Remove BPX.DEFAULT.USER Support
Element/Component: RACF

Material is current as of April 2013

Agenda

- Trademarks
- Overview
- Usage & Invocation
- Migration & Coexistence Considerations
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Overview

- Problem Statement / Need Addressed
  - When BPX.DEFAULT.USER support is used, many users of UNIX System Services can share a UID and GID
    - Shared UIDs produce audit non-conformances
    - If a Unix service creates a resource while running with a shared UID, that resource is available to all users running with that shared UID
    - Some Unix services are disallowed -- kill(), sigqueue(), pidaffinity(), ptrace
- Solution
  - z/OS V1.13 is the last release to support FACILITY class profile BPX.DEFAULT.USER. In z/OS V2.1, you must either:
    - Assign a unique UID to each user and GID to each group, **or**
    - Use BPX.UNIQUE.USER support to automatically assign a unique UID to each USS user and a unique GID for their group
- Benefit / Value
  - Improved security and accountability

Usage & Invocation

- Two RACF health checks will help with this transition:
  1) The RACF_UNIX_ID check will determine 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 will inform you that you must assign USS identities before needed
     - If you are relying on BPX.DEFAULT.USER support, the check will issue an error message
     - If you are relying on BPX.UNIQUE.USER support, the check will verify requirements and indicate if any exceptions are found, such as
       - **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**

Usage & Invocation

2)The RACF_AIM_STAGE check will determine whether the RACF database has been upgraded to application identity mapping (AIM) level 3 as recommended

- AIM stage 3 allows RACF to more efficiently handle authentication and authorization requests from applications such as z/OS UNIX System Services
- AIM stage 3 is required to use some RACF function, such as BPX.UNIQUE.USER support

Usage & Invocation

- In addition, we are enhancing BPX.UNIQUE.USER to allow specification of &racuid in the home directory field of the model user's OMVS segment.
  - ALTUSER BPXMODEL OMVS(HOME(/u/&racuid))
- Will substitute user ID 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
- When using automount, this eliminates all manual intervention
- Notes
  - Only the first occurrence of &racuid is substituted
  - If the substitution would result in a path name exceeding 1023 characters (the max), then substitution is not performed.
  - If sharing the RACF database with a downlevel system, substitution will not be performed on the downlevel system

Migration & Coexistence Considerations

- The two health checks (RACF_UNIX_ID and RACF_AIM_STAGE) are available for z/OS V1.12 and z/OS V1.13 with the PTFs for APAR OA37164
- A migration check (ZOSMIGV2R1_DEFAULT_UNIX_ID) is also available for z/OS V1.12 and z/OS V1.13 with the PTFs for APAR OA37164
  - ZOSMIGV2R1_DEFAULT_UNIX_ID can be enabled by customers planning to migrate to z/OS V2.1
  - Similar to the RACF_UNIX_ID check, it will issue an error message if you are relying on BPX.DEFAULT.USER support
- See also
  - z/OS Hot Topics article: "Nobody's deFault but mine"
    - http://publibfp.dhe.ibm.com/epubs/pdf/eoz2n1e0.pdf
  - BPXCHECK REXX exec on RACF web site
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/downloads/bpxcheck.html

Appendix

- Publications
  - z/OS V2R1.0 Security Server RACF Security Administrator’s Guide (SA23-2289)
    - Section “*Automatically assigning unique IDs through UNIX services*” describes how to enable BPX.UNIQUE.USER support
  - IBM Health Checker for z/OS V2R1 User's Guide (SC23-6843)
  - z/OS V2R1.0 Security Server RACF Messages and Codes (SA23-2291)
    - Provide information about the new checks and messages

Appendix

- Statement of Direction
  - 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 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.”**