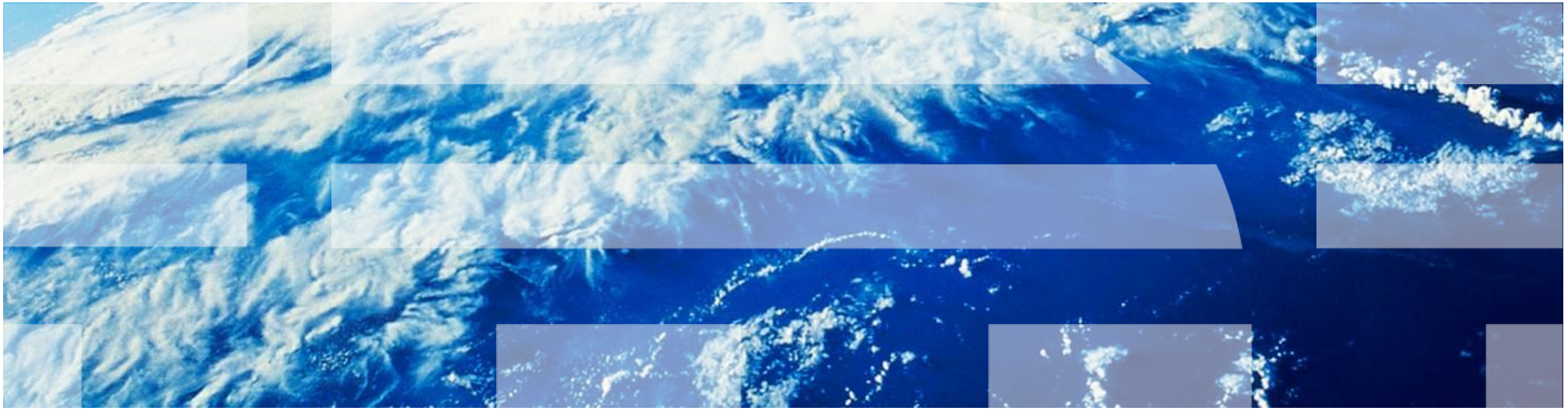
Removal of BPX.DEFAULT.USER Profile LI2914

LWard@us.ibm.com



Summary

What?

z/OS V1.13 is the last release to support FACILITY class profile BPX.DEFAULT.USER

Why?

When BPX.DEFAULT.USER support is used, many users of UNIX System Services can share a UID and GID

What do you need to do?

You must either:

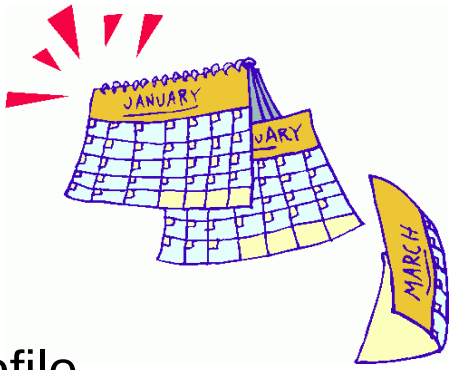
1) Assign a unique UID to each user and GID to each group

-or-

2) Use the BPX.UNIQUE.USER support to **automatically** assign a unique UID to each USS user and a unique GID for their group

A little history...

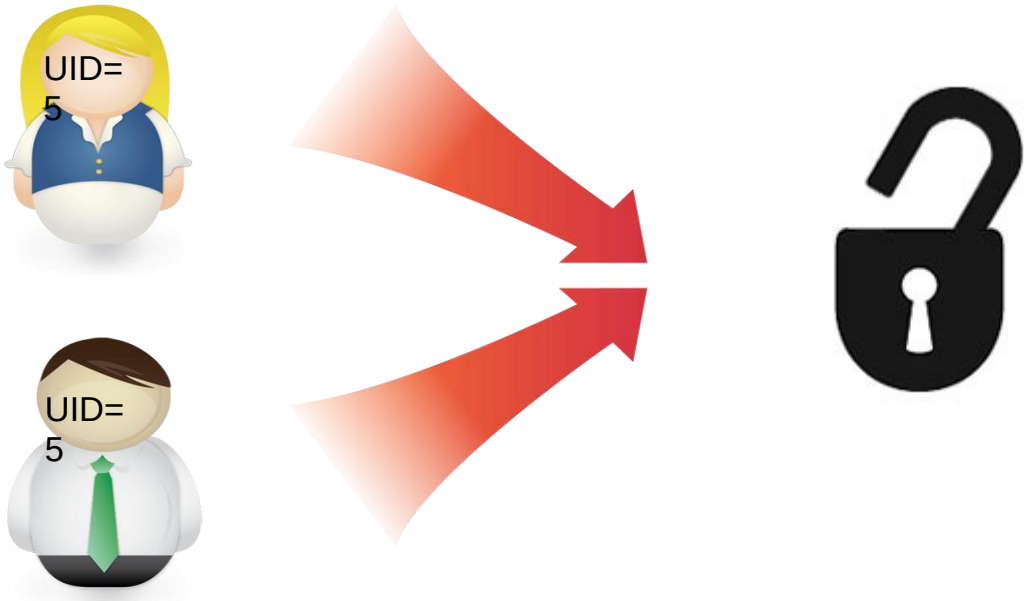
- OS/390 Release 4 (1997) introduced BPX.DEFAULT.USER profile
  - A way to allow an MVS user to use USS services **without a defined OMVS segment**.
  - Primary purpose was to enable use of UNIX sockets for every FTP user with minimal RACF administration
  - UID defined in the profile could be shared between many users
- z/OS V1R4 (2002) introduced AUTOUID keyword on ALTUSER command
  - Made it easier to generate 'next' unique UID
  - Requires Application Identity Mapping (AIM) Stage 2
- Years passed...
  - IBM encouraged use of unique UIDs assigned to each user
  - More and more Unix services were added
  - Default UIDs were still be used and misused



- z/OS V1R11 (2009) introduced BPX.UNIQUE.USER profile
  - Automatic “on-demand” generation of unique UIDs and GIDs
  - When a z/OS UNIX service is invoked by a user **without an OMVS segment**, a unique UID is permanently assigned
    - Requires Application Identity Mapping (AIM) Stage 3
- z/OS V1.13 (2011) is the last release to support BPX.DEFAULT.USER

What's wrong with using BPX.DEFAULT.USER?

- Shared UID produces audit non-conformances
  - No accountability for who did what, who owns what, etc.
- 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
- Certain Unix services are not allowed when user has default UID
  - kill(), sigqueue(), pidaffinity(), ptrace



How do I know if I am using BPX.DEFAULT.USER?

- Wait for OA37164
  - RACF Health and Migration checks for z/OS V1R12 and higher

- In the meantime, here are some other checks:
  - Does the FACILITY class profile BPX.UNIQUE.USER exist?
    - Yes → then you are not using BPX.DEFAULT.USER
    - No...continue
    - Does the FACILITY class profile BPX.DEFAULT.USER exist?

      Yes → then you are probably using it
  - Check your SMF records
    - Bit which “Indicates a default z/OS UNIX security environment is in effect” is in extended relocate section at location 317 (13D)
    - Event codes 28-58, 60-65
    - SMF unload fields xxxx_DFLT_PROCESS

      xxxx is the prefix to the SMF unload record, such as CMOD, COWN

How can I stop using BPX.DEFAULT.USER?

- Start using FACILITY profile BPX.UNIQUE.USER instead
  - Directions are in RACF Security Adminstrator's Guide
  - Requirements:
    - FACILITY profile BPX.UNIQUE.USER must exist
    - RACF database must be at AIM (Application Identity Mapping) stage 3

      Run utility IRRIRA00 to check
    - 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

- Or assign a UID to every user and a GID to every group
  - ALTUSER MARCY OMVS(AUTOUID))
  - ALTGROUP DEPT5 OMVS(AUTOGID))
  - Here is an easy way to assign a unique GID to all your groups
    - SEARCH CLASS(GROUP) NOLIST CLIST('ALTGROUP' ' OMVS(AUTOGID)')
    - EX EXEC.RACF.CLIST

What happens if I do nothing?

- In z/OS V1R13, nothing changes
- In next release, BPX.DEFAULT.USER profile will be ignored
  - You may get warning messages from the z/OS Health Checker
  - Users with no OMVS segment or no UID will not be able to run any Unix service

Summary

What?

z/OS V1.13 is the last release to support FACILITY class profile BPX.DEFAULT.USER

What do you need to do?

You must either:

1) Assign a unique UID to each user and GID to each group

-or-

2) Use the BPX.UNIQUE.USER support to **automatically** assign a unique UID to each USS user and a unique GID for their group

Additional Info

Publications

- *z/OS Security Server RACF Security Administrator's Guide*
- Section "*Automatically assigning unique IDs through UNIX services*"

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.