RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 6
Issue 2

April
2012

Replacing BPX.DEFAULT.USER

If you read "*Demise of BPX.DEFAULT.USER*" in the April 2011 edition of this newsletter, you are aware of IBM's intention to remove support for this profile beginning with Release 2.1 of z/OS. That article discussed possible replacement profiles. Our work helping clients replace BPX.DEFAULT.USER has identified other tasks you may need to complete, including:

- Establish standards for UID numbering. Define different number ranges for process IDs (e.g., Started Tasks) and for end users. Perhaps incorporate your HR system's Employee Number into the UID.
- Create standards for GID numbering. Define different number ranges for logon default groups and for role-based groups used for granting access to UNIX file objects.
- Before commencing widespread assignment of UIDs and GIDs, review your Hierarchical File System to find and replace orphaned OWNER UIDs and GROUP GIDs (those no longer matching an existing RACF ID).
- Set standards for user OMVS segment HOME and PROGRAM fields, especially for users who will not be accessing UNIX files.

To dispel a common myth, implementation of the Application Identity Mapping (AIM) database structure is not a prerequisite for addressing this issue. However, it is required to use the new FACILITY profiles to automate replacement of BPX.DEFAULT.USER. AIM is also needed to improve UID mapping performance and implement UNIXPRIV profile SHARED.IDS. We strongly encourage you to implement AIM.

Additional GLOBAL Entries

Our presentation on RACF Performance Tuning, available via our website, lists suggested entries for the Global Access Table. Here are a few more GLOBAL profiles and entries suggested by Elardus Engelbrecht of South Africa's State Information Technology Agency (SITA).

SDSF	ISFCMD.DSP.ACTIVE.*/READ
SDSF	ISFCMD.DSP.HELD.*/READ
SDSF	ISFCMD.DSP.OUTPUT.*/READ
FACILITY	ERBDSB.*/READ
OPERCMDS	MVS.DISPLAY.*/READ

Temporary Dataset Protection

Batch jobs create temporary datasets during execution to hold data for later processing within the same job. Their dataset names are prefixed with SYS*yyddd*.T*hhmmss*.RA000.*jobname*. These datasets are inaccessible to other users while the job is executing and are automatically deleted when the job terminates.

On rare occasions, a system failure may interrupt execution of a job in a way that leaves its temporary datasets undeleted. z/OS does not restrict access to these datasets. Any user can read them. This is cause for concern because such datasets may contain sensitive information.

Fortunately, orphaned temporary datasets can be protected simply by activating the TEMPDSN class. When class TEMPDSN is active, RACF prevents users from accessing a temporary dataset created by another process. A user with OPERATIONS authority can delete orphaned temporary datasets but cannot read them.

In the past, activation of TEMPDSN was not an easy task because it caused currently running processes (e.g., Started Tasks) to immediately lose access to their pre-existing temporary datasets. Since this could severely disrupt system operations, TEMPDSN could only be activated immediately prior to an all-way SysPlex IPL. Such IPLs are rare. As a result, our February 2012 survey indicated that fewer than 50% of installations had activated TEMPDSN.

When the survey results were announced on RACF-L, Lennie Dymoke-Bradshaw of IBM

posted a reply informing everyone that beginning with z/OS 1.13 the activation of TEMPDSN will no longer interfere with currently running processes. If all systems sharing a RACF database are at z/OS 1.13, it is now safe to activate TEMPDSN without waiting for an IPL. See Lennie's RACF-L email posting of February 27, 2012 for more details.

Auditors: Review Tape BLP Authority

Most tapes at your installation, even the virtual tapes, are formatted as Standard Label (SL). Labels are 80-byte records. The volume label is first and has the tape's volume-serial (VOLSER) number. Each dataset is preceded by two header labels giving its characteristics. When a user attempts to access a tape dataset, z/OS checks the volume and header labels to ensure the correct tape is mounted. If your system is configured to protect tape datasets (see "*Auditors: Verify Tape Data Protection is Active*" in the July 2009 newsletter), RACF verifies the user is permitted to access to the dataset.

A user can request z/OS ignore these labels when accessing the tape. This is known as Bypass Label Processing (BLP). To utilize this feature, the user specifies "BLP" in the LABEL parameter of the DD statement for the tape dataset. When BLP is invoked, dataset access permissions are **not** checked.

You can control the use of BLP by restricting access to resource ICHBLP in the FACILITY class. Access to ICHBLP is only checked when either (a) the TAPEVOL class is active or (b) the TAPEAUTHDSN parameter in PARMLIB member DEVSUPxx is set to YES. IBM's tape management product DFSMS/rmm relies on ICHBLP to control the use of BLP.

Many third-party tape management products provide their own resources to control BLP use. These controls can be used in lieu of or in addition to the use of ICHBLP. Like ICHBLP, READ permission is typically needed to read a tape and UPDATE is needed to write to a tape.

The class and resource names differ for each tape management product. Here are two of the more common ones.

CA - CA 1 Tape Management
CA@APE Class (parameter FUNC=YES | EXT)
BLPRES[.V*volser*.UCB*nnnn*] [with EXT]
BLPNORES[.V*volser*.UCB*nnnn*] [with EXT]
BLPRES and BLPNORES control use of BLP with in-house tapes and foreign (external) tapes, respectively.

BMC - Control-M/Tape
FACILITY $$CTTBLP.*qname*.*volser*
Set parameter TBLPCHK to YES to prompt access checking in Basic Definition mode.

Review profiles protecting these resources thoroughly. BLP authority, especially for in-house tapes, should be very strictly controlled.

RSH News

Nearly **80%** of all installations are still relying on **BPX.DEFAULT.USER** to assign UIDs and GIDs. The time to replace it is now. Call us!

Upcoming ***RSH RACF Training*:**

- RACF - Audit for Results
  April 24-26, 2012 - Boston, MA
  October 30-November 1, 2012 - Boston, MA
- RACF - Intro and Basic Administration
  May 8-10, 2012 - Boston, MA
  October 15-19, 2012 - WebEx
- RACF and z/OS Unix
  July 31-August 2, 2012 - WebEx

See our website for details and registration form.

Be sure to attend our ***upcoming presentations*** at Vanguard's 2012 conference and at these RACF User Group meetings:

- RUGONE 5/17 RACF & PCI
  BPX.DEFAULT.USER
- KOIRUG 6/7 CONSOLE & OPERCMDS