RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 5
Issue 4

October
2011

z/OS UNIX Security Enhancement

Just released APARs OA35973 and OA35974 introduced a new layer of security for z/OS UNIX along with a new resource class - FSACCESS.

The typical UNIX File System is comprised of a set of HFS and zFS datasets that are connected together (i.e., mounted) to form the entire file system. As users navigate within the directory tree, they move transparently between the underlying MVS datasets. Access to directories and files is governed by permission bits, access control lists, and UNIXPRIV authorities.

FSACCESS profiles allow you to control access to the underlying zFS datasets. Profiles match the MVS dataset names of the zFS datasets. Users require either FSACCESS UPDATE permission or System AUDITOR authority to access directories or files in a protected zFS dataset. FSACCESS access is checked before other access authorities, including Superuser.

If no profile protects a zFS dataset, access is allowed. FSACCESS is RACLIST-REQUIRED.

Attend our "RACF - Securing z/OS Unix" class to learn more about protecting z/OS Unix.

Duplicate JOBINIT Records

Multiple SMF Type 30 records are sometimes created for a single job. The RACF SMF Unload Utility IRRADU00 creates a JOBINIT record for each one, making it appear as if the job logged on multiple times. APAR OA37053 provides an ICETOOL job for eliminating the duplicates.

Indicate Permit Level in DATA

Consider using the DATA field of General Resource profiles to document the required permission level(s). For instance, you might add "UPDATE REQUIRED" to the DATA field of profile MVS.CANCEL.** in the OPERCMDS class. This practice can help you administer access without having to consult the manual.

*Is * or ** More Specific?*

For the answer, visit the RACF Center page on our website, find this topic, and click on Answer.

Auditors: Review Tape Dataset Protection Bypass Authority

Configuration options ensure access to tape datasets is protected. (See "*Auditors: Verify Tape Data Protection is Active*" in the July 2009 edition of this newsletter.) Tape management systems, however, generally provide a means of bypassing this protection. This mechanism is triggered when a user codes EXPDT=98000 in a JCL DD statement and is somewhat similar in function to Bypass Label Processing (BLP), which we will discuss in a future newsletter.

Tape management systems allow dataset protection to be bypassed only if the user is permitted access to the resource that governs use of this mechanism. Typically, READ permission is needed to read an existing file and UPDATE is needed to create a new file. The class and resource names differ for each product. Here are the more common ones. ('*volser*' is the volume-serial number of the tape.)

IBM - DFSMS/rmm Removable Media Manager
FACILITY Class (exit EDGUX100)
STGADMIN.EDG.IGNORE.TAPE.*volser*
STGADMIN.EDG.IGNORE.TAPE.RMM.*volser*
STGADMIN.EDG.IGNORE.TAPE.NORMM.*volser*

CA - CA 1 Tape Management
CA@APE Class (parameter FUNC=YES | EXT)
FORRES[.V*volser*.UCB*nnnn*] [with EXT]
FORNORES[.V*volser*.UCB*nnnn*] [with EXT]

BMC - Control-M/Tape
FACILITY Class ($$SECCTT.*qname* defined)
$$CTTBYPASS.*qname*.*volser*

Note that RMM and CA 1 distinguish between in-house tapes [RMM and FORRES] and foreign (external) tapes [NORMM and FORNORES].

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

Password Reset Authority Delegation

In z/OS 1.10, RACF introduced these new FACILITY class resources to enable delegation of USERID resume and password reset authority over designated subsets of users.

IRR.PWRESET.OWNER.*owner*
IRR.PWRESET.TREE.*owning-group*

Access to the first allows password resets for IDs owned by the specified Owner. Access to the second allows resets for IDs owned by the Owning-Group as well as any groups beneath it within its scope of groups. The permission level controls the extent of reset authority:

READ	Reset password and resume
UPDATE	Reset with NOEXPIRED
CONTROL	Reset before MINCHANGE

To exempt certain IDs from resets, the resource IRR.PWRESET.EXCLUDE.*userid* was also introduced. If the user attempting a reset does not have sufficient access permission to this resource, the reset is blocked. (If no EXCLUDE profile exists, the reset succeeds.)

The RACF Security Administrator's Guide suggests that READ access to the EXCLUDE profile is sufficient to allow the reset to succeed. In actuality, a user needs the same level of access to the EXCLUDE profile as is needed to the OWNER or TREE profile in order to perform the reset. For instance, to reset a password with NOEXPIRED, the user needs UPDATE access to the EXCLUDE profile. READ is insufficient.

To prevent a newly defined generic profile from accidentally covering EXCLUDEs (e.g., IRR.**), create profile IRR.PWRESET.EXCLUDE.** and give it UACC of CONTROL. This will allow all resets to succeed unless a more specific EXCLUDE profile is intentionally defined.

CF Rebuild Can Hang Sysplex

When RACF is in data sharing mode, an attempt to rebuild the Coupling Facility (CF) can, under certain conditions, result in a deadlock on RACF enqueues (ENQs). See Hiper APAR OA28906.

RSH News

Were you shocked at the price for remediation services offered by a vendor who gave you a ***"free"*** assessment? Call RSH to get the same level and quality of service for a reasonable fee.

Protecting sensitive data is easy once you know where it is. Finding it is the hard part. **DataSniff** from Xbridge has just the tool you need to locate sensitive data throughout your z/OS system. See the enclosed flyer for more information.

Upcoming ***RSH RACF Training*****:**

- RACF - Audit for Results
  October 25-27, 2011 - Boston, MA
  April 24-26, 2012 - Boston, MA
- RACF - Intro and Basic Administration
  October 11-13, 2011 - Boston, MA
  February 6-10, 2011 - Boston, MA
  May 8-10, 2012 - Boston, MA
- RACF and z/OS Unix
  January 24-26, 2012 - WebEx

See our website for details and registration form.

RSH CONSULTING, INC.
RACF Specialists
www.rshconsulting.com ■ 617-969-9050
29 Caroline Park, Newton, Massachusetts 02468