RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 3
Issue 3

July
2009

RACLIST REFRESH & STARTED

Changes to profiles in RACLISTed classes do not typically take effect until a REFRESH is performed. However, changes to the STDATA segment of profiles in the STARTED class become effective immediately. The STDATA segment is not cached in memory along with the RACLISTed profile. It is fetched each time the associated Started Task is initiated. Any changes made to the segment will be used the next time the task is started regardless of whether a RACLIST REFRESH is performed.

AUDITOR UNIX APAR

A user with AUDITOR authority is granted Read and Search access permission to all z/OS UNIX directories. In the course of performing extensive work implementing Access Control Lists (ACLs), RSH uncovered a z/OS UNIX software error. The error causes a user with AUDITOR to lose directory access when using the recursive option -R on commands like CHMOD. See APAR OA28648 for details.

RMM Superuser

Granting access permissions to FACILITY class resource STGADMIN.EDG.MASTER may result in unanticipated access authority to Removable Media Manager (RMM) management functions. When you permit CONTROL level access, the user is authorized to perform any RMM function related to the resources listed below without any additional access authorization checking. This check is made first and takes precedence over other access permissions for these resources.

STGADMIN.EDG.ACTIONS.*action*
STGADMIN.EDG.AV.*status*.*volser*
STGADMIN.EDG.CMOVE.*location*.*destination*
STGADMIN.EDG.CRLSE.*action*
STGADMIN.EDG.DV.SCRATCH.*volser*
STGADMIN.EDG.INIT
STGADMIN.EDG.LIST
STGADMIN.EDG.MOVES.*location*.*destination*
STGADMIN.EDG.OWNER.*userid*
STGADMIN.EDG.RELEASE

Furthermore, if a user with less than CONTROL access to STGADMIN.EDG.MASTER attempts to perform a function requiring access to one of the resources above and there is no RACF profile protecting it (i.e., Return Code 4), RMM revisits STGADMIN.EDG.MASTER to decide whether to grant access. If the user’s permission to STGADMIN.EDG.MASTER is at a level sufficient to allow access to the resource had it been protected, RMM will allow the access. Consider the situation where an RMM function would normally require UPDATE authority to STGADMIN.EDG.ACTIONS.RETURN and there is no profile covering this resource. RMM will call RACF to see if the user has UPDATE access to STGADMIN.EDG.MASTER and will allow the action if the user has this permission.

There is an exception to the latter. When a user attempts to use CHANGEVOLUME on a volume the user does not own and the corresponding resource STGADMIN.EDG.OWNER.*userid* is not defined to RACF, access is denied. UPDATE to STGADMIN.EDG.MASTER alone is insufficient to allow the access in this case.

RESTRICTED & UNIX Access

The RESTRICTED attribute prevents a user from gaining access to z/OS resources via permissions in the Global Access Table, a profile's UACC, or a permission to ID(*). However, it does not automatically prevent a user from accessing z/OS UNIX files and directories via the 'Other' permission bits. To extend access restrictions to UNIX resources, define a UNIXPRIV class profile that protects resource RESTRICTED.FILESYS.ACCESS. The mere existence of a covering profile, whether discrete or generic, activates this restriction. We recommend using a discrete profile for clarity. To exempt a particular RESTRICTED user from this control, simply permit the user READ access to this profile.

SEARCH Command Mystery

One SEARCH gave the following results:

ABC.*
ABC.*.**
ABC.**

Another SEARCH gave these results:

ABC.*.**
ABC.*
ABC.**

Why are they different? For the answer, visit the RACF Center page on our website, find this newsletter topic, and click on the link Answer.

Auditors: Verify Tape Data Protection is Active

Datasets on tape are ***not*** protected by default. To enable their protection, options must be activated in either RACF, z/OS, or the tape management software product.

Activating tape protection in RACF is achieved by executing SETROPTS TAPEDSN. Once set, SETROPTS LIST will display the following:

```
TAPE DATA SET PROTECTION IS ACTIVE
```

If TAPEDSN is not active, other options need to be examined to see if they enable protection. If the tape management software is IBM's DFSMSrmm Removal Media Manager, check the following parameters in the z/OS PARMLIB member DEVSUPnn that is currently in effect for the system. Underlined are the defaults; shaded are the recommended settings. TAPEAUTHDSN =YES is equivalent to activating TAPEDSN.

```
TAPEAUTHDSN = YES | NO
TAPEAUTHF1 = YES | NO
TAPEAUTHRC4 = ALLOW | FAIL
TAPEAUTHRC8 = FAIL | WARN
```

If TAPEDSN is not active and the tape management software is CA-1, check the following two CA-1 options. Combined they are the equivalent of TAPEDSN. With CATSEC, either of the shaded choices is acceptable.

```
OCEOV = YES | NO
CATSEC = YES | BYP | NO
```

TSO APPL Class Resource

Beginning with z/OS 1.10, it is possible to restrict TSO logons using APPL class profiles. To activate this control, set PARMLIB member IKJTSOnn parameter VERIFYAPPL to YES (the default is NO). If VTAM generic resources are being used for TSO, define the APPL resource name using the GNAME parameter in PARMLIB member TSOKEYnn. Otherwise, the resource name is TSOssss, where 'ssss' is the SMF system ID from PARMLIB member SMFPRMnn.

RSH News

Do you need to **enhance or reconfigure** RACF but do not have the resources you need to get the job done? **Call RSH.**

Upcoming ***RSH RACF Training***:

- RACF - Intro and Basic Administration
  September 22-24, 2009 - Boston, MA
- RACF - Audit for Results
  November 3-5, 2009 - Boston, MA

See our website for details and registration form.

If you missed our recent RACF User Group and conference presentations, visit our website for copies of the handouts.

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

SECURITY
SUPPORT
SOLUTIONS