



CCAPRINT

A Newsletter Excerpt for Model 204 Users

September 2007

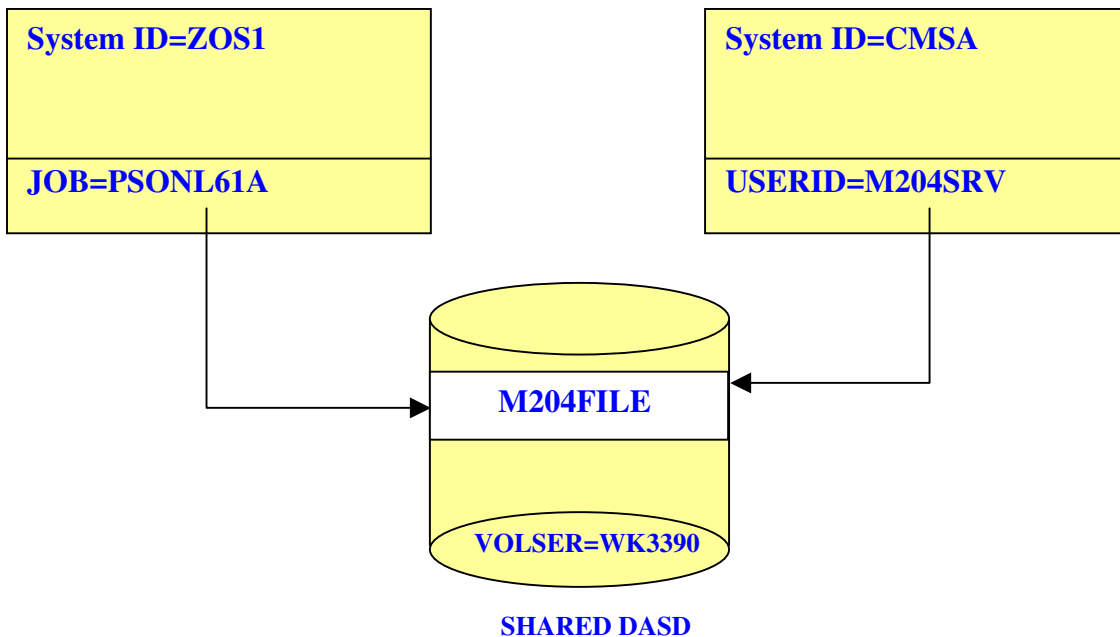
USE OF AND ACCESS TO PRODUCTS AND FEATURES ARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE USER'S SOFTWARE LICENSE. THE PRESENTATION OF MATERIAL HEREIN DOES NOT, IN ANY MANNER, MODIFY SUCH TERMS AND CONDITIONS.

Shared DASD Enqueuing and the ENQCTL Command

By James Damon

Sharing direct access storage devices (DASD) makes datasets accessible among jobs running on physically or logically (LPAR) separate machines or virtual machines (VM). When DASD is shared this way, protecting the data integrity of Model 204 files becomes the responsibility of Model 204. Figure 1 shows what this environment looks like.

Figure 1



Concurrent access by multiple jobs to datasets on shared DASD, when that access is read-only, does not pose data integrity problems. However, when the access is both read and update, you must deal with the serious data integrity issues that arise. Model 204 provides its own data integrity protection in this environment via a facility called Shared DASD Enqueuing.

Implementing Shared DASD Enqueuing

Shared DASD Enqueuing is implemented in the File Parameter List (FPL) of each Model 204 file. This structure is called, not surprisingly, the Shared DASD Enqueue list. For each Model 204 run--BATCH204, ONLINE, IFAM1 or IFAM4--that has a particular file open, there is one entry in the Shared DASD Enqueue list. BATCH2 and IFAM2 jobs do not establish entries; they are established by the Online supporting the BATCH2 or IFAM2 job.

You can display the Shared DASD Enqueuing list with the ENQCTL command. Figure 2 shows the results from an ENQCTL command issued for a file opened under z/OS and z/VM. Two jobs under z/OS and one virtual machine under z/VM have the file open.

ENQCTL Command

Figure 2.

```
ENQCTL DSNLIST
*** M204.0588: ZOS1 SHR PSONL61A ONLIN610 07.264 12:54:34
*** M204.0588: CMSA SHR M204SRV X'F1F3F5F7F8FD4040' 07.264 13:32:07
*** M204.0588: ZOS1 SHR PSBAT61B BATCH204 07.264 13:42:32
```

The details following message M204.0588 are specific for each Online sharing the file. The columns provide the information described in Figure 3.

Figure 3.

```
1. The system id - SYSID
2. Type of file enqueue - SHR, EXCL
3. z/OS, z/VSE: JOBNAME
   z/VM: USERID
4. z/OS, z/VSE: STEPNAME
   z/VM: CPUID
5. Julian date: yy.ddd
6. Time: hh:mm:ss
```

Enqueue Type SHR

If multiple entries are present, each one is of enqueue type SHR. This means that each Model 204 run has opened the file with a read-only password. At this point, any attempt by any Model 204 run to open the file with an update password, will generate the shared DASD enqueue conflict messages shown in Figure 4.

Figure 4.

```
ONLINE
OPEN DSNLIST
*** M204.0347: PASSWORD
UPDATE
*** M204.0582: ACCESS TO FILE DSNLIST WK3390.TEST.DSNLIST.M204 PREVENTED
BY: CMSA SHR M204SRV X'F1FEF5F7F8FD4040'07.264 16:57:27

BATCH204
*** M204.0583: WAITING FOR EXCLUSIVE ACCESS TO FILE DSNLIST
WK3390.TEST.DSNLIST.M204
```

This is one form of data integrity protection. When multiple Model 204 runs on different systems open a Model 204 file, the opens must each be read-only. No updating can take place in this instance, since data integrity cannot be guaranteed.

Enqueue Type EXCL

If a file has been opened with an update password by a user in a multi-user Online, the ENQCTL command will show the entrie in Figure 5.

Figure 5.

```
ENQCTL DSNLIST
*** M204.0588: ZOS1 EXCL PSONL61A ONLINE610
```

This file is now enqueued exclusively by the job PSONL61A and cannot be opened for read or update by any other Model 204 run. It may, of course, be opened for read or update by other users in this Online, since data integrity is protected through the local record and resource locking tables. But since those tables are known only to this Online, they can provide data integrity protection only for files in this Online.

An attempt from another Model 204 run, on any system, to open this file for read or update results in one of two different shared DASD enqueuing conflict messages. If the other Model 204 run is BATCH204, the batch job will wait for access and the messages shown in Figure 6 are displayed.

Figure 6

```
OPEN DSNLIST
READPW
M204.0581: WAITING FOR SHARE ACCESS TO FILE DSNLIST
WK3390.TEST.DSNLIST.M204

or

OPEN DSNLIST
UPDATEPW
M204.0583: WAITING FOR EXCLUSIVE ACCESS TO FILE DSNLIST
WK3390.TESET.DSNLIST.M204
```

The BATCH204 job will then sleep for about five minutes and attempt to open the file again.

If the other Model 204 run is an Online, the open attempt fails immediately with the message shown in Figure 7.

Figure 7

```
OPEN DSNLIST
*** M204.0584: FILE IS IN USE: DSNLIST WK3390.TEST.DSNLIST.M204
*** 4 M204.0630: FILE OPEN COMMAND REJECTED
```

Removing Shared DASD Enqueue List Entries with ENQCTL

If a job is cancelled, ends abnormally, or there is an operating system failure, the Shared DASD Enqueue list entries established by that job are not removed. That may leave the file in a state in which it cannot be opened by Model 204 runs on other systems. When that happens, the ENQCTL command can be used to remove obsolete entries. Figure 8 shows an obsolete entry in the Shared DASD Enqueue list for file DSNLIST.

Figure 8

```
ENQCTL DSNLIST
*** M204.0588: ZOS2 SHR PSBAT61A BATCH204          07.262 13:32:07
*** M204.0588: ZOS1 SHR PSBAT61A ONLIN610          07.264 12:54:34
*** M204.0588: ZOS1 SHR PSBAT61B BATCH204          07.264 13:42:32
```

We know that the job on SYSID=ZOS2 was actually cancelled two days ago and that the entry is obsolete. The following ENQCTL command can be used to remove the obsolete entry:

```
ENQCTL DSNLIST ZOS2 PSBAT61A
```

In many cases, Model 204 can detect obsolete entries and remove them automatically. However, the ENQCTL command is available when automatic removal does not or cannot occur. Nevertheless, it must not be used casually. Removing an entry, if it is not truly obsolete, can expose a file to serious data integrity problems. Be very cautious using the ENQCTL command to remove an entry. Make sure that the entry is indeed, truly obsolete.

In Summary

If users at your site are unable to open files, and they are receiving messages M204.0581, 0582, 0583 or 0584, then the ENQCTL command may be the solution.

*© 2007 Computer Corporation of America
500 Old Connecticut Path, Framingham, MA 01701*