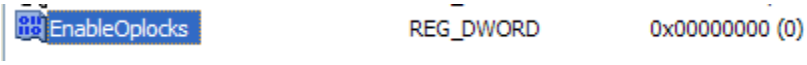
Opportunistic Locking (oplocks) on the Network File Server

Opportunistic Locking is the main reason for corruption and repair problems with Access. It should be DISABLED on any Windows server (even a peer-to-peer server in Windows NT or later) that is host of a shared Access database.

On the server, change the registry to deny the granting of opportunistic locks by adding***** or setting the following registry entry to 0, then reboot:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
EnableOplocks REG_DWORD 0 or 1
Default: 1 (Enabled by Default) should be 0 Disabled
NOTE: The EnableOplocks value configures Windows servers (including workstations sharing files) to allow or deny opportunistic locks on local files.

To add OpLocks to the Registry:

- navigate to the key
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
- in right window, right click
- highlight the New option that appears
- select DWORD Value from the second menu.
- The new value is called **New Word Value #1** – rename it to EnableOplocks



- If the value isn't set to (0) at the end, right click on EnableOplocks and choose Modify–set the value from 1 to 0

The www.microsoft.com knowledgebase articles http://support.microsoft.com/default.aspx?scid=kb;en-us;296264 also talk about turning off opportunistic locking requests on client workstations with the OplocksDisabled (Windows 2000 or later) or UseOpportunisticLocking (Windows NT 4.0) keys. These are not necessary as long as the server where Pearl is stored has EnableOplocks disabled as above.