Configuring Opportunistic Locking in Windows

This article was previously published under Q296264

Article ID : 296264
Last Review : October 10, 2003
Revision : 1.0

IMPORTANT: This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, click the following article number to view the article in the Microsoft Knowledge Base:

256986 Description of the Microsoft Windows Registry

SUMMARY

By default, opportunistic locking is enabled for server message block (SMB) clients that run one of the Windows operating systems that is listed at the beginning of this article. Opportunistic locking allows clients to lock files and locally cache information without the risk of another user changing the file. This increases performance for many file operations but may decrease performance in other operations because the server that grants the opportunistic lock must manage the breaking of that lock when another user requests access to the file.

MORE INFORMATION

WARNING: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. The location of the client registry entry for opportunistic locking has changed from the earlier location in Microsoft Windows NT. In later versions of Windows, you can disable opportunistic locking by setting the following registry entry to 1:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters

OplocksDisabled REG_DWORD 0 or 1
Default: 0 (not disabled)

NOTE: The OplocksDisabled registry value configures Windows clients to either request or not request opportunistic locks on a remote file.

You can also deny the granting of opportunistic locks by setting the following registry entry to 0:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

EnableOplocks REG_DWORD 0 or 1
Default: 1 (Enabled by Default)

NOTE: The EnableOplocks value configures Windows-based servers (including Workstations sharing files) to allow or deny opportunistic locks on local files.

In addition, you can use the following values to tune opportunistic locking for Windows-based computers that have granted opportunistic locks.

The following value specifies the minimum link throughput that the server allowed before it disables raw and opportunistic locks for this connection:

MinLinkThroughput REG_DWORD 0 to infinite bytes per second
Default: 0

The following value specifies the maximum time that is allowed for a link delay. If delays exceed this number, the server disables raw I/O and opportunistic locking for this connection:

MaxLinkDelay REG_DWORD 0 to 100,000 seconds
Default: 60

The following value specifies the time that the server waits for a client to respond to an oplock break request (smaller values allow detection of crashed clients more quickly, but might potentially cause loss of cached data):

OplockBreakWait REG_DWORD 10 to 180 seconds

Default: 35

APPLIES TO

- Microsoft Windows Server 2003, Standard Edition
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, Datacenter Edition
- Microsoft Windows Server 2003, Web Edition
- Microsoft Windows Server 2003, Datacenter Edition
- Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
- Microsoft Windows XP Professional Edition
- Microsoft Windows XP Tablet PC Edition
- Microsoft Windows XP 64-Bit Edition
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional Edition
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows Small Business Server 2003 Premium Edition
- Microsoft Windows Small Business Server 2003 Standard Edition

Keywords: kbinfo kbfilesystems kbenv KB296264