See in Memory Descriptor List whats on

Posted by Steffen78 - 22 Feb 2010 - 13:29

Hello Girls and Boys,

i have a problem with a w2k3 server ent. sp2. The machine is an x86 32bit system with an MS SQL 2005 installed for enteo. the server part of enteo is ionstalled to. antivirus is mcafee.

Now the problem, the "non paged pool" is running out of free space till the server is crashing. the "biggest" pooltag in poolmon is the "mdl".

Is there a way to analyze with driver is exhausting the mdl. can i analyze this problem with a full memory dump or should i take the driver verifier for this?

thank you very much for your help.

sorry about my english.

==========

Re: See in Memory Descriptor List whats on

Posted by Robert Kuster - 03 Apr 2010 - 15:17

Steffen welcome.

It is easy to find out which driver is leaking or consuming a lot of memory.

Theory
In order to use Pool tags one generally has to enable them with GFlags -> System Registry -> "Enable pool tagging". Luckily on Windows Server 2003 pool tagging is always enabled. From the documentation: "Pool tagging is permanently enabled on Windows Server 2003 and later versions of Windows, including Windows Vista. On these systems, the Enable pool tagging check box on the Global Flags dialog box is dimmed and commands to enable or disable pool tagging fail.". Also alongside your WinDbg installation you should find ..Debugging Tools for Windows (x86)triage pooltag.txt which lists all tags used by kernel mode components and drivers. Here is what it says about the Mdl tag:

- -
Mdl - - Io, Mdls

MDLs are described here: What Is Really in That MDL? Further you should use Driver Verifier to track Pool Usage and configure it as follows:"Create custom settings" -> Next"Selet individual settings from a full list" -> NextSelect "Pool tracking" -> Next"Automatically select all drivers installed on this computer" -> Finish, Restart computer
Start Driver Verifier Manager again an select "Display information about currently verified drivers" -> Next (3x). Now you will see the pool usage of each driver:

http://windbg.info/images/fbfiles/images/pool_usage.PNG

In WinDbg
After enabling driver verifier you can get even more information from WinDbg. Attach WinDbg as a kernel debugger to the target machine and use the following commands:

```
0: kd> !verifier 1

Driver Verification List

Entry     State          NonPagedPool   PagedPool   Module

8a7e6ee8 Loaded          00000000       00000000    kdcom.dll
8a7e6e68 Loaded          00000000       00000000    BOOTVID.dll
8a7e6df0 Loaded          00023708       00003760    ACPI.sys
8a7e6d70 Loaded          00000000       00000000    WMILIB.SYS
8a7e6480 Loaded          00003710       0001b310    pci.sys
....


; to see all individual allocations of each driver
0: kd> !verifier 0x3

Driver Verification List

Entry     State          NonPagedPool   PagedPool   Module

8a7e6df0 Loaded          00023708       00003760    ACPI.sys

Current Pool Allocations  00000059    00000023
Current Pool Bytes        00023708    00003760
Peak Pool Allocations     000000d3    0000002d
Peak Pool Bytes           00024b88    00003be8

PoolAddress  SizeInBytes    Tag      CallersAddress
e10115a8     0x00000080     AcpM      b9fa1c47
8a783148     0x00000018     AcpS      b9f7fabb
8a7bd148     0x00000018     AcpS      b9f7fae7
8a786a10     0x00000030     AcpS      b9f836a6
8a7c0130     0x00000030     AcpR      b9f877c9
....
```

I hope this helps,
Robert

==========