Reference Stack Traces

Windows Server® 2008 and Windows Vista™

Editor: Dmitry Vostokov

OpenTask

Published by OpenTask, Republic of Ireland

OpenTask books are available through booksellers and distributors worldwide. For further information or comments send requests to press@opentask.com.

Microsoft, MSDN, Visual C++, Visual Studio, Win32, Windows, Windows Server and Windows Vista are registered trademarks of Microsoft Corporation. Other product and company names mentioned in this book may be trademarks of their owners.

A CIP catalogue record for this book is available from the British Library.

ISBN-13: 978-1-906717-23-0 (Paperback)

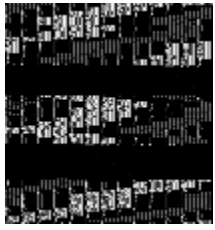
First printing, 2009

SYSTEM

```
PROCESS 82f15d90  SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 00122000  ObjectTable: 86400288  HandleCount: 532.
    Image: System
    VadRoot 84895778 Vads 525 Clone 0 Private 1356. Modified 18570. Locked 64.
    DeviceMap 86408878
    Token                             864038e8
    ElapsedTime                       00:22:45.652
    UserTime                          00:00:00.000
    KernelTime                        00:00:01.466
    QuotaPoolUsage[PagedPool]         0
    QuotaPoolUsage[NonPagedPool]      0
    Working Set Sizes (now,min,max)  (835, 0, 0) (3340KB, 0KB, 0KB)
    PeakWorkingSetSize                4386
    VirtualSize                       8 Mb
    PeakVirtualSize                   18 Mb
    PageFaultCount                    18297
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1365

        THREAD 82f15ae8  Cid 0004.0008  Teb: 00000000 Win32Thread: 00000000 GATEWAIT
        Not impersonating
        DeviceMap                 86408878
        Owning Process            82f15d90       Image:         System
        Wait Start TickCount      87705          Ticks: 682 (0:00:00:10.639)
        Context Switch Count      2943
        UserTime                  00:00:00.000
        KernelTime                00:00:02.074
        Win32 Start Address nt!Phase1Initialization (0x81b60ae4)
        Stack Init 8039a000 Current 80399c90 Base 8039a000 Limit 80397000 Call 0
        Priority 1 BasePriority 0 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        80399ca8 81abf3bf nt!KiSwapContext+0x26
        80399cec 81a4184d nt!KiSwapThread+0x44f
        80399d24 81a708a2 nt!KeWaitForGate+0x21b
        80399d74 81b60af6 nt!MmZeroPageThread+0x129
        80399d7c 81bdda1c nt!Phase1Initialization+0x12
        80399dc0 81a36a3e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f39d78  Cid 0004.0010  Teb: 00000000
        Win32Thread: 00000000 WAIT: (Executive) KernelMode
        Non-Alertable
            81b15a90  SynchronizationEvent
        Not impersonating
        DeviceMap                 86408878
        Owning Process            82f15d90       Image:         System
        Wait Start TickCount      17             Ticks: 88370 (0:00:22:58.580)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!PopIrpWorkerControl (0x81a0a39f)
        Stack Init 803c9000 Current 803c8c98 Base 803c9000 Limit 803c6000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        803c8cb0 81abf3bf nt!KiSwapContext+0x26
        803c8cf4 81a5ccf8 nt!KiSwapThread+0x44f
        803c8d4c 81a0a3c4 nt!KeWaitForSingleObject+0x492
        803c8d7c 81bdda1c nt!PopIrpWorkerControl+0x25
        803c8dc0 81a36a3e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```



SVCHOST.EXE (LOCALSERVICENETWORKRESTRICTED)

```
PROCESS 8563c7b8  SessionId: 0  Cid: 03f4    Peb: 7ffda000  ParentCid: 026c
    DirBase: 3bfec1a0  ObjectTable: a07ece78  HandleCount: 458.
    Image: svchost.exe
    VadRoot 8563e310 Vads 166 Clone 0 Private 1523. Modified 254. Locked 6.
    DeviceMap a07df7e0
    Token                             a07f1498
    ElapsedTime                       00:21:51.972
    UserTime                          00:00:00.686
    KernelTime                        00:00:01.341
    QuotaPoolUsage[PagedPool]         90632
    QuotaPoolUsage[NonPagedPool]      12768
    Working Set Sizes (now,min,max)  (2795, 50, 345) (11180KB, 200KB, 1380KB)
    PeakWorkingSetSize                2811
    VirtualSize                       62 Mb
    PeakVirtualSize                   70 Mb
    PageFaultCount                    5016
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      3893

        THREAD 8563e030  Cid 03f4.03f8  Teb: 7ffdf000 Win32Thread: 00000000 WAIT:
        (Executive) UserMode Non-Alertable
            8563e8ac  NotificationEvent
        IRP List:
            856e18b8[1]: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a07df7e0
        Owning Process            8563c7b8       Image:         svchost.exe
        Wait Start TickCount      85537          Ticks: 2850 (0:00:00:44.460)
        Context Switch Count      65
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00332083)
        Stack Init 87d1c000 Current 87d1bbc8 Base 87d1c000 Limit 87d19000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        87d1bbe0 81abf3bf nt!KiSwapContext+0x26
        87d1bc24 81a5ccf8 nt!KiSwapThread+0x44f
        87d1bc78 81c5458d nt!KeWaitForSingleObject+0x492
        87d1bcac 81c144af nt!IopSynchronousServiceTail+0x251
        87d1bd38 81a5fa7a nt!NtReadFile+0x646
        87d1bd38 77259a94 nt!KiFastCallEntry+0x12a (TrapFrame @ 87d1bd64)
        0025fa9c 77258c74 ntdll!KiFastSystemCallRet
        0025faa0 75fa046b ntdll!ZwReadFile+0xc
        0025fb18 75e9d260 kernel32!ReadFile+0x210
        0025fb44 75e9d306 ADVAPI32!ScGetPipeInput+0x2a
        0025fbb0 75e9d949 ADVAPI32!ScDispatcherLoop+0x65
        0025fe28 00331308 ADVAPI32!StartServiceCtrlDispatcherW+0xce
        0025fe30 003323b9 svchost[2]!SvcHostMain+0x12
        0025fe34 00332147 svchost!wmain+0x5
        0025fe78 75fa4911 svchost!_initterm_e+0x163
        0025fe84 7723e4b6 kernel32!BaseThreadInitThunk+0xe
        0025fec4 7723e489 ntdll!__RtlUserThreadStart+0x23
        0025fedc 00000000 ntdll!_RtlUserThreadStart+0x1b
```

[1] IRP [\FileSystem\Npfs]
[2] svchost.exe - Host Process for Windows Services