某局点CAS集群中一台Windows Server 2008虚拟机出现蓝屏重启的经验案例

李树兵 2020-02-28 发表

组网及说明

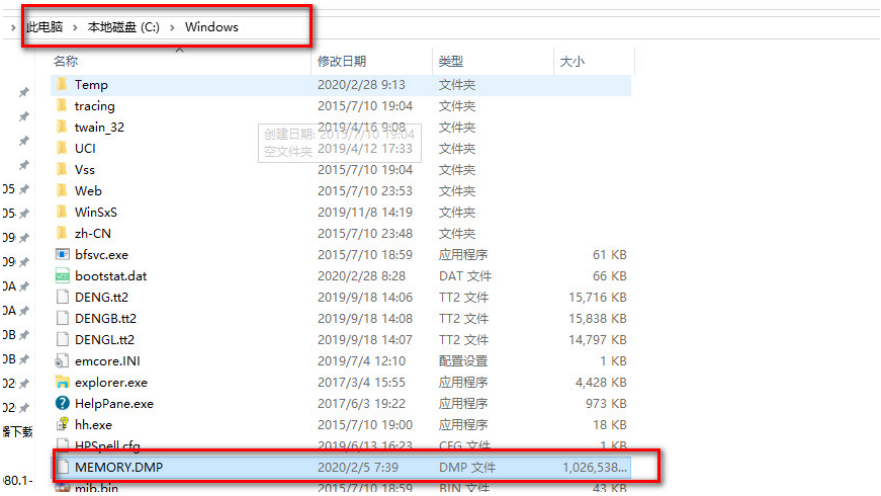
略。

问题描述

某局点一台Windwos Server 2008虚拟机出现蓝屏重启的现象。

过程分析

一般蓝屏重启的原因大多数都是虚拟机系统本身有问题导致，虚拟机出现蓝屏之后会在系统的C盘的Windows目录下生成蓝屏时候内存的dump文件，这个文件是我们分析系统蓝屏的重要文件，一般出现蓝屏都需要收集此文件进行分析定位。



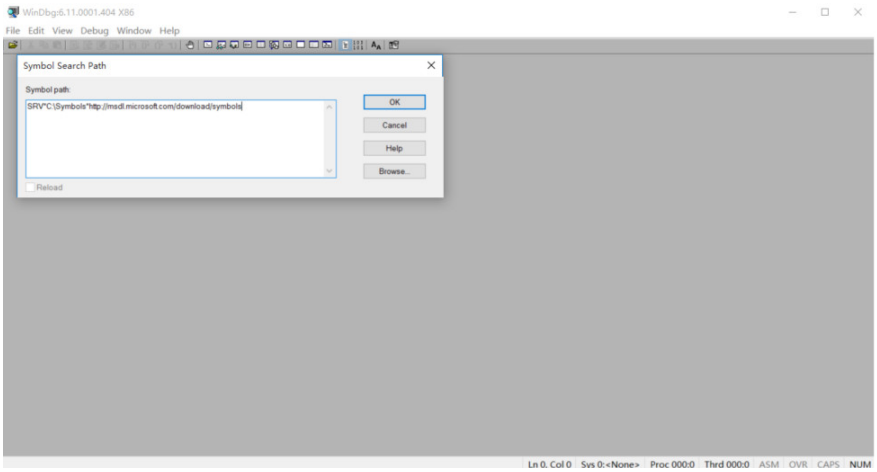
获取到此文件之后，需要使用Debugging Tools for Windows （windebug）软件来分析这个DMP文件。windebug是微软发布的一款相当优秀的源码级(source-level)调试工具，可以用于Kernel模式调试和用户模式调试，还可以调试Dump文件。

目前软件可以通过共享的百度网盘获取

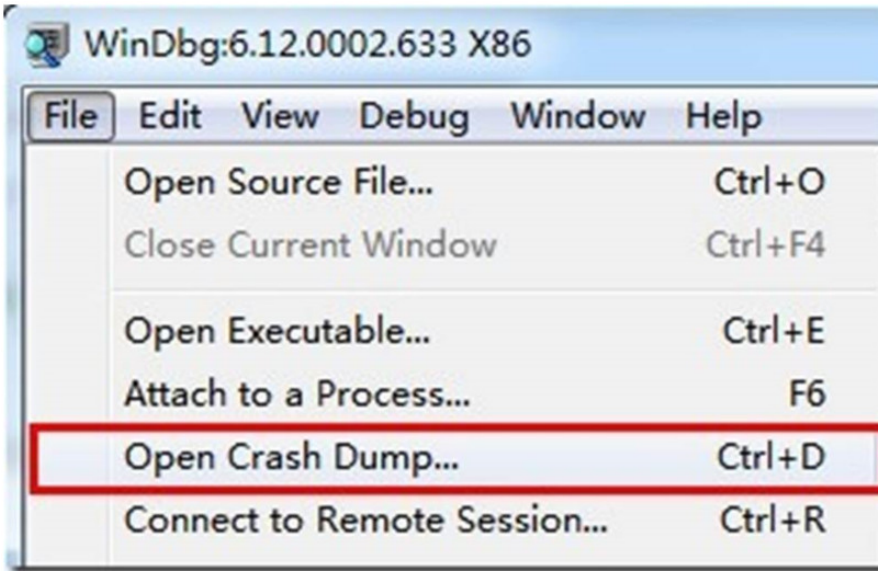
链接：https://pan.baidu.com/s/1D8ExAxUg0Lg2_8c2EDB50Q 提取码：axfl

下载安装完之后需要先配置sysbol符号文件的路径

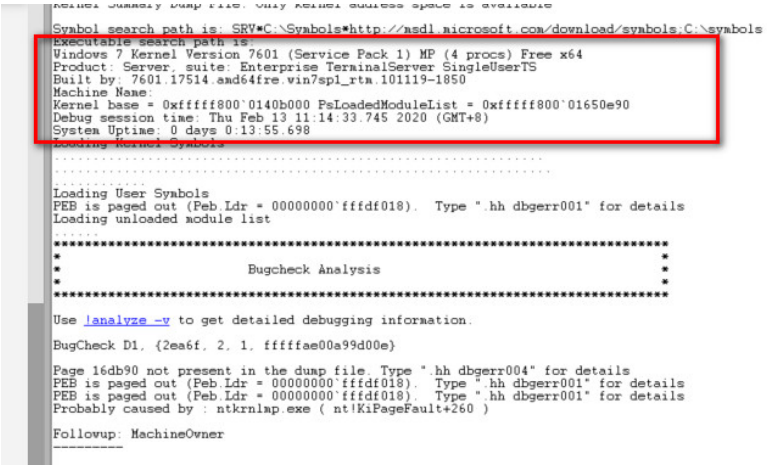
符号表是WinDbg关键的“数据库”，如果没有它，WinDbg基本上就是个废物，无法分析出更多问题原因。所以使用WinDbg设置符号表，是必须要走的一步。 1、运行WinDbg软件，然后按【Ctrl+S】弹出符号表设置窗 2、将符号表地址：SRV*C:\Symbols*http://msdl.microsoft.com/download/symbols粘贴在输入框中，点击确定即可。



然后打开这个DMP文件



打开这个文件可以看到系统信息，以及系统重启的时间和运行的时间等信息



可以点击蓝色的！analyze -v 进行进一步的分析（因为一般DMP文件比较大，所以需要多等待一段时间）

通过日志可以看出里面有个进程Thunder.exe 程序。通过百度或者问题处理经验，这个进程是迅雷下载软件的进程。怀疑是迅雷软件与当前系统不兼容导致出现蓝屏现象。

FAULTING_IP:

+cc1952f0653df38 fffffae0`0a99d00e 4831aef7000000 xor qword ptr [rsi+0F7h],rbp

DEFAULT_BUCKET_ID: VISTA_DRIVER_FAULT

BUGCHECK_STR: 0xD1

PROCESS_NAME: Thunder.exe

TRAP_FRAME: fffff80002817c60 -- (.trap 0xfffff80002817c60)

NOTE: The trap frame does not contain all registers.

解决方法

进一步与用户沟通，确定迅雷软件为最新安装的，安装之后出现蓝屏现象。协调用户将此软件卸载之后未再出现蓝屏现象。

一般出现蓝屏重启的原因有：

1. 系统安装了新的软件与系统不兼容
2. 系统安装了新的硬件以及安装了新的驱动
3. 虚拟机中毒。

对于安装软件导致可以先通过分析dmp文件，确定导致蓝屏的可能进程是什么，从而进一步确定原因。

大多数蓝屏的原因可能是虚拟机系统中毒导致，所以遇到蓝屏的情况，建议先在虚拟机系统里面安装杀毒软件，进行全盘杀毒。