**[adplus抓取dmp文件，crash和hang两种方式](http://blog.csdn.net/guomin0907/article/details/6667600)**

http://aloneplayer.spaces.live.com/blog/cns!C3CB6D654135F83D!422.entry?wa=wsignin1.0&sa=10734357

Working with Dump File

如果程序员比作侦探,那Dump文件就像是凶案现场的全息照片.  
导致用户的程序崩溃的原因很复杂,可能是用户的配置,可能是和其他软件冲突,开发人员无法重现此类问题,也无法访问用户的机器,更无法attach到崩溃的进程上,此时解决问题的最好方法就是向用户索取问题发生时的dump文件,然后开始调查.

**Creating Dump File**在Vista环境中抓取Dump文件很方便,在task manager(Ctrl-Shift-Esc)中,选中要生成dump文件的进程,点击context menu中的"Creat Dump File"就可以了.

通常,使用WinDBG目录下(C:\Program Files\Debugging Tools for Windows (x86))的adplus.vbs来抓取dump file.   
adplus -hang -p 2960 //当进程2960失去响应时生成dump  
adplus -crash -pn w3wp.exe //在w3wp.exe终止或被回收时生成dump  
adplus -crash -pn w3wp.exe -NoDumpOnFirst //同上,不对 first chance exceptions生成dump

adplus是一个vb script文件,运行CDB(就是命令行下的WinDBG),负责监视系统中将要发生的异常.

**Adplus参数设置**

|  |  |
| --- | --- |
| -huang | 进程运行时,随时可以使用-hang参数得到一个Dump文件, 而不需要考虑线程是否真的处于死锁中,用于诊断高内存使用率, 高CPU使用率。 在hang模式下，dump file是以非侵入方式被抓取的, 并没有中断线程, 因此不需要跟启动进程有相同的身份,在客户端调试服务器时,hang模式抓取dump file很有用。 |
| -crash | 在进程异常终止时抓取dump file. 进程异常终止有3种情况: 1.unhandled的exception 2.asp.net进程由于iis reset或recycle而终止. 3.出现heap毁坏,栈溢出,内存不足等错误,进程必须退出 |
| -pn | 指定要分析的进程名。使用多个“-pn process name”开关来指定多个进程。 |
| -o | dump file的存储路径,缺省为adplus所在路径 |
| -FullOnFirst | create full dumps on first chance exceptions |
| -MiniOnSecond |  |
| -NoDumpOnFirst | 如果exception被try-catch block处理,使用这个参数就不会生成dump file |
| -NoDumpOnSecond |  |
| -quiet | No dialog boxes will be displayed |

**什么是First Chance Exception 和 Second Chance Exception?**  
当程序抛出异常(.net 或 native exception),此时这个exception为1st chance exception,如果这个exception 没有被 try-catch block处理,这个exception就会成为2nd chance exception (unhandled exception) 当前进程随后终止.

**什么是Mini Dump 和Full Dump?**user-mode Mini Dump,保存了进程crash时virtual memory的部分内容.有些SOS的命令在Mini Dump上不能工作.Mini Dump的内容和大小和被dump的程序有关.Mini Dump所包含的信息并不一定比Full Dump少.  
Full User-Mode Dumps包含了进程的整个内存空间,程序的image,handle table等调试信息.

**Adplus的输出**  
adplus.vbs所在的路径下生成一个目录,形如<crash或huang>\_Mode\_\_Date\_07-22-2008\_\_Time\_10-35-1212,目录中包含

* CDBScripts - 包含用来通知windbg/cdb运行什么命令的配置文件的文件夹。
* ADPlus\_report**.txt** - 记录adplus Attach到进程以后的信息
* PID-<进程ID>\_\_<进程名>.EXE\_\_Date\_07-18-2008\_\_Time\_14-55-0505**.log** - adplus的运行时日志，在hang模式下，这个文件里包括堆栈里所有线程、已经加载的模块的信息和等同于执行!runaway命令的输出结果。如果内存转储文件创建失败，可以到这个文件的底部去查找原因。
* PID-<进程ID>\_\_<进程名>.EXE\_\_full\_1c38\_2008-07-18\_14-59-08-005\_1618.dmp - 就是**dump file**
* Process\_List**.txt** - tlist.exe 的输出，显示在生成内存转储文件的时候，系统中有多少进程在同时运行。

如果程序由于unhandled exception而终止,会得到多个dump,比如  
PID-4588\_\_ASPNET\_WP.EXE\_\_1st\_chance\_AccessViolation\_\_mini\_15b8\_2008-07-22\_10-35-28-827\_11ec.dmp  
PID-4588\_\_ASPNET\_WP.EXE\_\_1st\_chance\_Process\_Shut\_Down\_\_full\_15b8\_2008-07-22\_10-35-36-609\_11ec.dmp  
PID-4588\_\_ASPNET\_WP.EXE\_\_2nd\_chance\_NET\_CLR\_\_full\_15b8\_2008-07-22\_10-35-29-420\_11ec.dmp  
PID-4588\_\_ASPNET\_WP.EXE\_\_Date\_07-22-2008\_\_Time\_10-35-1212.log  
Process\_List.txt

这些dump文件表明:  
首先发生了一个非法访问,也许就是一个NullReferenceException,adplus捕获到这个Exception,生成一个mini dump(1st\_chance\_AccessViolation\_\_mini)  
这个Exception没有被处理,就接着产生CLR exception 对应的dump(2nd\_chance\_NET\_CLR\_\_full)  
然后进程终止,产生dump file: 1st\_chance\_Process\_Shut\_Down\_\_full   
真正用来解决问题的是2nd Chance CLR Exception 对应的dump file  
如果只得到一个dump,就可以证明crash不是由于unhandled exception引起的

**Adplus的高级用法**  
可以给adplus指定配置文件,在某个特定的Exception发生时生成dump file,并把dump file存在特定目录下  
adplus -c myconfig.cfg -pn w3wp.exe

|  |
| --- |
| myconfig.cfg |
| < ADPlus> <Settings> <RunMode>**crash**</RunMode> </Settings> <PreCommands> <Cmd> !load clr10\sos</Cmd> </PreCommands> <Exceptions> <Option> **NoDumpOnFirstChance** </Option> <Option> **NoDumpOnSecondChance** </Option> <Config> **<!-- This is for the CLR exception -->** <Code> clr </Code> <Actions1> Log </Actions1> <CustomActions1> !clr10\sos.cce **System.Runtime.InteropServices.COMException** 1; j ($t1 = 1) ".dump /ma /u **c:\dumps\exceptiondump.dmp**;gn" ; "gn" </CustomActions1> <ReturnAction1> GN </ReturnAction1> <Actions2> Void </Actions2> <ReturnAction2> GN </ReturnAction2> </Config> </Exceptions> < /ADPlus> |

**Dump文件的使用技巧**为Dump文件生成Context Menu,可以方便地打开WinDBG,加载Dump文件,并执行一些初始化命令.详情见Tess的blog: Associate windbg with .dmp files

**参考文档**  
How to install Windbg and get your first memory dump

Mini Dump Snapshots and the New SOS

Post-Mortem Debugging Your Application with Minidumps and Visual Studio .NET

SOS: Commands not working on a mini-dump