Obtaining a Windows Memory Dump with ProcDump

A White Paper From

GOLDSTAR SOFTWARE
www.GoldstarSoftware.com

For more information, see our web site at
http://www.goldstarsoftware.com

Obtaining a Windows Memory Dump with ProcDump

Last Updated: 01/09/2023

Sometimes, in the course of working a problem with a complex application or service like Actian PSQL/Zen, it becomes imperative to capture the state of the process and send it to the software developer for analysis. This paper describes the process of capturing a memory dump of the database engine with a tool called ProcDump.

Obtain the ProcDump Executable

Download the ProcDump program from Microsoft's web site. At the time of this writing, the current version (v11.0) can be found here:

https://learn.microsoft.com/en-us/sysinternals/downloads/procdump

Install ProcDump

Open the compressed download file and extract the files PROCDUMP.EXE and PROCDUMP64.EXE to a suitable location on your server. If you want it to be always available, consider moving it to your Windows folder, or some other suitable location in the search path. If you have a 64-bit environment, you want to use ProcDump64.

View a List of ProcDump Command Line Options

To see a list of ALL of the ProcDump command line options, start an Administrative Command Prompt and run ProcDump by itself to get a complete list of options and parameters.

```
C:\ProcDump>procdump

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

Monitors a process and writes a dump file when the process exceeds the
specified criteria or has an exception.

Capture Usage:
   procdump.exe [-mm] [-ma] [-mt] [-mp] [-mc <Mask>] [-md <Callback_DLL>] [-mk]
                [-n <Count>]
                [-s <Seconds>]
                [-c|-cl <CPU_Usage> [-u]]
                [-m|-ml <Commit_Usage>]
                [-p|-pl <Counter> <Threshold>]
                [-h]
                [-e [1] [-g] [-b] [-ld] [-ud] [-ct] [-et]]
                [-l]
                [-t]
                [-f  <Include_Filter>, ...]
                [-fx <Exclude_Filter>, ...]
                [-dc <Comment>]
                [-o]
                [-r [1..5] [-a]]
                [-at <Timeout>]
                [-wer]
                [-64]
                {
                 {{[-w] <Process_Name> | <Service_Name> | <PID>} [<Dump_File> | <Dump_Folder>]}
                |
                 {-x <Dump_Folder> <Image_File> [Argument, ...]}
                }
Install Usage:
   procdump.exe -i [Dump_Folder]
                [-mm] [-ma] [-mt] [-mp] [-mc <Mask>] [-md <Callback_DLL>] [-mk]
                [-r]
                [-at <Timeout>]
                [-k]
                [-wer]
Uninstall Usage:
   procdump.exe -u

Dump Types:
   -mm     Write a 'Mini' dump file. (default)
           - Includes directly and indirectly referenced memory (stacks and what they reference).
           - Includes all metadata (Process, Thread, Module, Handle, Address Space, etc.).
   -ma     Write a 'Full' dump file.
           - Includes all memory (Image, Mapped and Private).
           - Includes all metadata (Process, Thread, Module, Handle, Address Space, etc.).
   -mt     Write a 'Triage' dump file.
           - Includes directly referenced memory (stacks).
           - Includes limited metadata (Process, Thread, Module and Handle).
           - Removal of sensitive information is attempted but not guaranteed.
   -mp     Write a 'MiniPlus' dump file.
           - Includes all Private memory and all Read/Write Image or Mapped memory.
           - Includes all metadata (Process, Thread, Module, Handle, Address Space, etc.).
           - To minimize size, the largest Private memory area over 512MB is excluded.
             A memory area is defined as the sum of same-sized memory allocations.
             The dump is as detailed as a Full dump but 10%-75% the size.
           - Note: CLR processes are dumped as Full (-ma) due to debugging limitations.
   -mc     Write a 'Custom' dump file.
           - Includes the memory and metadata defined by the specified MINIDUMP_TYPE mask (Hex).
   -md     Write a 'Callback' dump file.
           - Includes the memory defined by the MiniDumpWriteDump callback routine
             named MiniDumpCallbackRoutine of the specified DLL.
           - Includes all metadata (Process, Thread, Module, Handle, Address Space, etc.).
   -mk     Also write a 'Kernel' dump file.
           - Includes the kernel stacks of the threads in the process.
           - OS doesn't support a kernel dump (-mk) when using a clone (-r).
           - When using multiple dump sizes, a kernel dump is taken for each dump size.

Conditions:
   -a      Avoid outage. Requires -r. If the trigger will cause the target
           to suspend for a prolonged time due to an exceeded concurrent
           dump limit, the trigger will be skipped.
   -at     Avoid outage at Timeout. Cancel the trigger's collection at N seconds.
   -b      Treat debug breakpoints as exceptions (otherwise ignore them).
   -c      CPU threshold above which to create a dump of the process.
   -cl     CPU threshold below which to create a dump of the process.
   -dc     Add the specified string to the generated Dump Comment.
   -e      Write a dump when the process encounters an unhandled exception.
           Include the 1 to create dump on first chance exceptions.
           Add -ld to create a dump when a DLL (module) is loaded (filtering applies).
           Add -ud to create a dump when a DLL (module) is unloaded (filtering applies).
           Add -ct to create a dump when a thread is created.
           Add -et to create a dump when a thread exits.
   -f      Filter (include) on the content of exceptions, debug logging and filename at DLL
load/unload.
           Wildcards (*) are supported.
   -fx     Filter (exclude) on the content of exceptions, debug logging and filename at DLL
load/unload.
           Wildcards (*) are supported.
   -g      Run as a native debugger in a managed process (no interop).
   -h      Write dump if process has a hung window (does not respond to
           window messages for at least 5 seconds).
   -k      Kill the process after cloning (-r), or at end of dump collection.
   -l      Display the debug logging of the process.
   -m      Memory commit threshold in MB at which to create a dump.
   -ml     Trigger when memory commit drops below specified MB value.
   -n      Number of dumps to write before exiting.
   -o      Overwrite an existing dump file.
   -p      Trigger when the Performance Counter is at, or exceeds, the specified Threshold.
           Some Counters and/or Instance Names can be case-sensitive.
   -pl     Trigger when the Performance Counter falls below the specified Threshold.
   -r      Dump using a clone. Concurrent limit is optional (default 1, max 5).
           OS doesn't support a kernel dump (-mk) when using a clone (-r).
           CAUTION: a high concurrency value may impact system performance.
           - Windows 7   : Uses Reflection. OS doesn't support -e.
           - Windows 8.0 : Uses Reflection. OS doesn't support -e.
           - Windows 8.1+: Uses PSS. All trigger types are supported.
   -s      Consecutive seconds before dump is written (default is 10).
   -t      Write a dump when the process terminates.
   -u      Treat CPU usage relative to a single core (used with -c).
   -w      Wait for the specified process to launch if it's not running.
   -wer    Queue the (largest) dump to Windows Error Reporting.
   -x      Launch the specified image with optional arguments.
           If it is a Store Application or Package, ProcDump will start
           on the next activation (only).
   -64     By default ProcDump will capture a 32-bit dump of a 32-bit process
           when running on 64-bit Windows. This option overrides to create a
           64-bit dump. Only use for WOW64 subsystem debugging.

Install/Uninstall:
   -i      Install ProcDump as the AeDebug postmortem debugger.
           Only -mm, -ma, -mt, -mp, -mc, -md and -r are supported as additional options.
           Uninstall (-u only) restores the previous configuration.
   -u      As the only option, Uninstalls ProcDump as the AeDebug postmortem debugger.

License Agreement:
   Use the -accepteula command line option to automatically accept the
   Sysinternals license agreement.

Automated Termination:
   -cancel <Target Process PID>
           Using this option or setting an event with the name "ProcDump-<PID>"
           is the same as typing Ctrl+C to gracefully terminate ProcDump.
           Graceful termination ensures the process is resumed if a capture is active.
           The cancellation applies to ALL ProcDump instances monitoring the process.

Filename:
   Default dump filename: PROCESSNAME_YYMMDD_HHMMSS.dmp
   The following substitutions are supported:
           PROCESSNAME   Process Name
           PID           Process ID
           EXCEPTIONCODE Exception Code
           YYMMDD        Year/Month/Day
           HHMMSS        Hour/Minute/Second

Examples:
   Use -? -e to see example command lines.
```

Capture a ProcDump From Any Failing Process

If the server is running and stable, then it is possible to enable ProcDump to capture data from ANY failing process, which is the easiest option. However, note that this option will capture a dump from ANY failing process, so if there are other processes running on the server that are experiencing issues, then this may capture multiple crash dumps, filling up the disk needlessly.

To enable ProcDump to capture *any* failing process, first create a ProcDump folder on a disk with plenty of free space, then use a command like this from an administrative Command Line:

```
procdump -ma -I c:\ProcDump
```

This installs ProcDump as the crash handler, and when any process crashes on the system, a new file with the naming convention of PROCESSNAME_YYMMDD_HHMMSS.dmp will be written to the indicated folder.

When you are done capturing the crash dumps, be sure to uninstall ProcDump as the crash handler with this command:

```
procdump -u
```

Capture a ProcDump From A Specific Process

If your server has other processes running (and crashing), then you might want to get a bit more specific and only monitor one the database engine for crashes. To do this, you need to know the name of your engine executable file. For Actian PSQL, this will be one of the following:

Engine Type	Executable File
32-bit Server Engine	NTDBSMGR.EXE
64-bit Server Engine	NTDBSMGR64.EXE
Workgroup Engine	W3DBSMGR.EXE

For Actian Zen, this will be one of the following:

Engine Type	Executable File
32-bit Server Engine	ZENENGNSVC32.EXE
64-bit Server Engine	ZENENGNSVC.EXE
Workgroup Engine App	ZENENGNAPP.EXE
Workgroup Engine Service	ZENENGNSVC32.EXE

You should then launch ProcDump with the engine executable name, like this:

```
procdump -e -t -ma ntdbsmgr64.exe c:\ntdbsmgr64.dmp
```

The –e switch is used to create the dump when an unhandled exception is encountered, such as an Access Violation (0xC0000005). The -t switch will cause a dump to occur when the process terminates. The –ma switch dumps all memory, and is usually required to see what is happening inside the engine. (Other switches may be useful for capturing other conditions, such as a high CPU usage event, but this is not covered here.)

When ProcDump launches, it will display a screen like this:

```
R:\>procdump -e -t -ma zenengnsvc.exe C:\zencrashdump.dmp

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

Process:               zenengnsvc.exe (41276)
Process image:         C:\Program Files\Actian\Zen\bin\zenengnsvc.exe
CPU threshold:         n/a
Performance counter:   n/a
Commit threshold:      n/a
Threshold seconds:     n/a
Hung window check:     Disabled
Log debug strings:     Disabled
Exception monitor:     Unhandled
Exception filter:      [Includes]
                       *
                       [Excludes]
Terminate monitor:     Enabled
Cloning type:          Disabled
```

```
Concurrent limit:       n/a
Avoid outage:           n/a
Number of dumps:        1
Dump folder:            C:\
Dump filename/mask:     zencrashdump
Queue to WER:           Disabled
Kill after dump:        Disabled


Press Ctrl-C to end monitoring without terminating the process.
```

Leave this window open in this state until the next crash occurs, and the userdump should be generated in the indicated folder and file name. (If you need to terminate the crash monitoring, simply press Ctrl-C as indicated, and ProcDump will exit.)

Note that the size of the DMP file will depend on how much memory the database engine process is using, so if your L1 cache is set to 8GB, the DMP file will be at least that big. Before starting this process, be sure that you have sufficient disk space on the drive to which the DMP file will be written, or specify an alternate location on the command line.

Run ProcDump to Capture Engine Memory State Immediately

In certain cases, you may not want to capture a dump when a crash occurs, but rather you want to capture a dump immediately. In this case, you won't be using the flags that wait for an exception, but rather switches to capture an immediate dump, like this:

```
procdump -ma ntdbsmgr64.exe c:\ntdbsmgr64.dmp
```

Submit the Dump to Actian Corporation

If you do not have an active incident opened with Actian, then you will need to either open one or contact Goldstar Software's issue clearinghouse (if previously notified) for the next steps. If you **do** have an active incident opened with Actian, then you can submit your dump directly to them. Zip up the file to shrink it first to reduce transfer time. Be sure to name the ZIP file with the incident number, then upload it by going to this location in your browser:

https://communities.actian.com/s/supporting-case-documentation

If you are currently logged into the Actian Web Portal, then you will need to use the Login Button in the upper right corner to log in as a new user:

Login Name: PSQL_Customer@actian.com

Password: PsqlCustomer1

Actian changes their Upload Process from time to time, so be sure to contact them directly to obtain current login information.

If you still can't get it to work, contact Goldstar Software and let us work with you to help!