Registry & Dump Configuration

Registry & Dump Configuration

- Root trees of Registry
- Editing the registry
- Configure DUMP in registry
  - System mode dump
    - regular dump
    - Dedicated Dump
    - NotMyFault
  - Manually force dump
    - keyboard CrashOnCtrlScroll
    - NMI non-maskable interrupt
    - Virtual machines
  - User mode dump
    - Windows Error Reporting WER
    - use Procmon to collect dump

Root trees of Registry

HKEY_CURRENT_CONFIG

> shortcut to ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current***
>
> information about hardware profile.

HKEY_CURRENT_USER

> shortcut to ***HKEY_USERS<active_username>***

HKEY_USERS

> Stores user profiles on the computer.

HKEY_CLASSES_ROOT

> shortcut to ***HKEY_LOCAL_MACHINE\SOFTWARE\Classes***
>
> configurations for filename extensions and COM objects.

HKEY_LOCAL_MACHINE

> contains hives that do system wide configuration.
>
> HARDWARE
>
> Descriptions of Hardwares and device-to-driver mappings.
>
> SAM
>
> local account, group information, and domain account, groups on server runs as domain controllers.
>
> SECURITY
>
> stores system-wide security policies and user rights.
>
> SOFTWARE

> system wide configurations which are not boot related as well as third-party applications configuration.
>
> SYTEM
>
> system boot related configurations, such as device drivers and services to run.

Editing the registry

1. regedit.exe GUI
2. reg.exe CLI

Configure DUMP in registry

System mode dump

regular dump

under key ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl***

add

CrashDumpEnabled	REG_DWORD	2
DumpFile	REG_EXPAND_SZ	c:\MEMORY.DMP

Values for ***CrashDumpEnabled***

- 0 disabled
- 1 complete dump
- 2 kernel dump
- 3 small dump (64KB)
- 7 automatic dump

under key ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management***

add

PagingFiles	REG_EXPAND_SZ	c:\pagefile.sys 8500 8500

first 8500 is initial size, second 8500 is max size. in regular dump, size of pagefile.sys should be RAM+257MB if you want generate complete dump.

kernel dump is roughly RAM * 1/3 + 257MB

Dedicated Dump

dump without pagefile

under ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl***

add

DedicatedDumpFile	REG_SZ	c:\dedicatedfumpfile.sys
DumpFileSize	REG_DWORD	80960
IgnorePageFileSize	REG_DWORD	1
AlwaysKeepMemoryDump	REG_WORD	1

NotMyFault

you can use NMF to test if your DUMP configuration works or not

Manually force dump

keyboard CrashOnCtrlScroll

under ***HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\i8042prt\Parameters***

or ***HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kbdhid\Parameters***

add

CrashOnCtrlScroll	REG_DWORD	1

to trigger, press right ***Ctrl*** and twice ***Scroll***

NMI non-maskable interrupt

under ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl***

add

NMICrashDump	REG_DWORD	1

To trigger, use NMI Switch, or from Hyper-V Host, use PowerShell

```
debug-vm "name_of_guest_machine" -InjectNonMaskableInterrupt -Force
```

to force dump on Hyper-V Guest

Virtual machines

you may use state files, snapshots, checkpoints to create dump for virtual machines

User mode dump

you can simply use task manager, resource manager to generate dump, analyze wait chain

Windows Error Reporting WER

under ***HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\LocalDumps***

add

DumpFolder	REG_EXPAND_SZ	C:\WER
DumpCount	REG_DWORD	10
DumpType	REG_DWORD	2

DumpCount : Maximum how many files to store at once

DumpType : 0 custom; 1 mini; 2 full

use Procmon to collect dump

1. download procdump.zip and extract
2. create a directory to store dumps in C drive such as C:\dumps
3. open elevated cmd prompt, cd to directory where procdump is extracted
4. run procdump -ma -i c:\dumps to set procdump as default debugger
5. when applications/svchost.exe crash, dump will be stored in c:\dumps
6. delete values under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug. to reset default debugger