GOPAS
IT ŠKOLIACE STREDISKO

Advanced Debugging .NET

ShowIT 2016
& Security Day

Ing. Bc. Robert Haken
MVP Development | MCT
haken@havit.cz | @RobertHaken

Agenda

Windows Debugger + .NET extensions

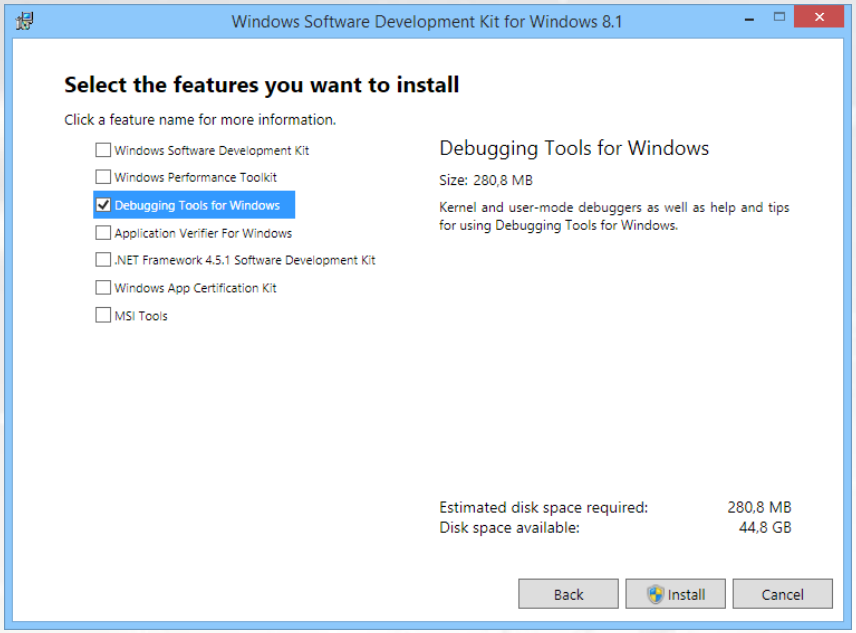
DebugDiag

dema

DEMO

StackOverflowException – DebugDiag, WinDbg

Debugging Tools for Windows



WinDbg – „GUI“

NTSD – new console

CSD – classic console

DebugDiag - samostatné

součást Windows SDK

www.windbg.org

Debugger Extensions pro .NET

```
.load C:\path\to\extension.dll
```

SOS.dll – Son of Strike, součást .NET

```
.loadby sos mscorwks
```
(.NET < 4)

```
.loadby sos clr
```
(.NET >= 4)

PSSCOR2/PSSCOR4 – širší SOS (web)

SOSEX, NetEx – 3rd party

```
!help [<command>]
```

Záludnosti použití Debuggeru

Platform - x86 vs. x64 vs. ...

Symbols

```
.symfix
```
(MSFT Symbols Server)

```
.sympath, .sympath+
.reload
```

.NET Data Access Layer (mscordacwks.dll)

```
.cordll -ve -u -l
```

stejná verze, jako na laděném stroji (dtto SOS)

Režimy práce s Debuggerem

- Open Executable... (g pro Run)
- Attach to a Process...
- Open Crash Dump...
  - Task Manager / Create Dump File (!!32-bit vs. x64 stroj)
  - DebugDiag / ADPLUS
  - Windows Error Reporting
  - WIN32 API (extern v .NET)
  - Windows Crash Dump (native)

DebugDiag

„user“-friendly UI

připravené analýzy

sběr dat/dumpů

pod pokličkou debugger services

voláno např. i z Azure Web Apps KUDU

DEMO

DebugDiag demo report

Stack Examination

```
!ClrStack [-i] [-a] [-l] [-p]
!DumpStack [-EE]
!EEStack [-EE] (all threads)
!DumpStackObjects (typy)
```

DEMO

01-StackHeap, x64

Heap Examination

```
!DumpHeap [-stat] [-type <name>]
          [-mt <MTaddr>] [-live|dead]
!HeapStat [-inclUnrooted]
!GCRoot <ObjAddr>          !GCHandles
!EEHeap –gc
!FinalizationQueue [-allReady]
!FindAppDomain <ObjAddr>
```

Object Inspection

```
!DumpObject <ObjAddr>
!DumpArray <ObjAddr>
!DumpVC <MTaddr> <ObjAddr>
dd <addr>
dq <addr>
!ObjSize <ObjAddr>
```

Error Diagnostics

```
!PrintException [ObjAddr] [-nested]
!DumpAllExceptions (PSSCOR4)
!wdae              (NETEXT)
!wpe               (NETEXT)
!VerifyHeap
!VerifyObj <ObjAddr>
!analyze -v        (native)
```

Threads

```
!Threads
~123s
!ThreadPool
```

```
!ThreadState <state>
```

.NET Internals - AppDomains

System

- zakládá Shared a Application
- loaduje mscorlib.dll (into Shared)
- spravuje AppDomains, spravuje strings
- předvytvoří instance výjimek OoM, SO, ...

Shared

- obsahuje mscorlib.dll + basic types - string, enum, ..

Application (n)

- user code

```
!DumpDomain [<addr>]
```

.NET Internals - Assemblies

Assembly = unit of deployment

- manifest
- jeden nebo několik Modules
- self-describing

```
!DumpAssembly <AssAddr>
!DumpModule [-mt] <ModuleAddr>
!DumpMT <MTaddr>
!IP2MD <IPaddr>      !DumpMD <MDaddr>
```

www.showit.sk

www.gopas.sk