LiveKd v5.63

Article • 03/23/2021 • 4 contributors

Feedback

In this article

By Mark Russinovich and Ken Johnson

Published: April 28, 2020

Download LiveKd (700 KB)

Introduction

LiveKD, a utility I wrote for the CD included with *Inside Windows 2000, 3rd Edition*, is now freely available. *LiveKD* allows you to run the Kd and Windbg Microsoft kernel debuggers, which are part of the Debugging Tools for Windows package, locally on a live system. Execute all the debugger commands that work on crash dump files to look deep inside the system. See the Debugging Tools for Windows documentation and our book for information on how to explore a system with the kernel debuggers.

While the latest versions of Windbg and Kd have a similar capability on Windows Vista and Server 2008, LiveKD enables more functionality, such as viewing thread stacks with the !thread command, than Windbg and Kd's own live kernel debugging facility.

Installation

First download and install the Debugging Tools for Windows package from Microsoft's web site:

https://msdn.microsoft.com/library/windows/hardware/ff551063(v=vs.85).aspx

If you install the tools to their default directory of \Program Files\Microsoft\Debugging Tools for Windows, you can run *LiveKD* from any directory; otherwise you should copy LiveKD to the directory in which the tools are installed.

If you haven't installed symbols for the system on which you run *LiveKD*, *LiveKD* will ask if you want it to automatically configure the system to use Microsoft's symbol server (see the Debugging Tools for Windows documentation for information on symbol files and the Microsoft symbol server).

NOTE: The Microsoft debugger will complain that it can't find symbols for LIVEKDD.SYS. This is expected, since I have not made symbols for LIVEKDD.SYS available, and does not affect the behavior of the debugger.

Download PDF

Using LiveKd

usage:

liveKd [[-w]|[-k <debugger>]|[-o filename]] [-vsym] [-m[flags] [[-mp process]|[pid]]] [debugger options]
liveKd [[-w]|[-k <debugger>]|[-o filename]] -ml [debugger options]
liveKd [[-w]|[-k <debugger>]|[-o filename]] [[-hl]|[-hv <VM name> [[-p]|[-hvd]]]] [debugger options]

Expand table

Parameter	Description
-hv	Specifies the name or GUID of the Hyper-V VM to debug.
-hvd	Includes hypervisor pages (Windows 8.1 and above only).
-hvl	Lists the names and GUIDs of running Hyper-V VMs.
-k	Specifies complete path and filename of debugger image to execute
-m	Creates a mirror dump, which is a consistent view of kernel memory. Only kernel mode memory will be available, and this option may need significant amounts of available physical memory. A flags mask that specifies which regions to include may optionally be provided (drawn from the following table, default 0x18F8): 0001 - process private, 0002 - mapped file, 0004 - shared section, 0008 - page table pages, 0010 - paged pool, 0020 - non-paged pool, 0040 - system PTEs, 0080 - session pages, 0100 - metadata files, 0200 - AWE user pages, 0400 - driver pages, 0800 - kernel stacks, 1000 - WS metadata, 2000 - large pages The default captures most kernel memory contents and is recommended. This option may be used with -o to save faster, consistent dumps. Mirror dumps require Windows Vista or Windows Server 2008 or above. Sysinternals RamMap provides a graphical summary of the distribution of the available memory regions that can be selected for inclusion.
-ml	Generate live dump using native support (Windows 8.1 and above only).
-mp	Specifies a single process whose user mode memory contents should be included in a mirror dump. Only effective with the -m option.
-o	Saves a memory.dmp to disk instead of launching the debugger.
-p	Pauses the target Hyper-V VM while LiveKd is active (recommended for use with -o). Specifies the name or GUID of the Hyper-V VM to debug.
-vsym	Displays verbose debugging information about symbol load operations.
-w	Runs windbg instead of kd

All other options are passed through to the debugger.

Note: Use Ctrl-Break to terminate and restart the debugger if it hangs.

By default LiveKd runs kd.exe.

Download LiveKd **(700 KB)**

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Additional resources

Training

Module

Interactively debug .NET apps with the Visual Studio debugger - Training

Learn how to efficiently debug your .NET app by using Visual Studio to fix your bugs quickly. Use the interactive debugger within Visual Studio to analyze and fix your C# applications.