Remote Microsoft® Windows Server® OS Kernel Debugging Using Dell Windows Debugger Utility (DWDU)

Dell | Product Group

Niranjan Vedavyas March 2, 2010



THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2010 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the *DELL* logo, and the *DELL* badge, are trademarks of Dell Inc. *Microsoft, Windows*, and *Windows Server* are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Table of Contents

Executive Summary	2
Introduction	3
Overview	3
Server Configuration	3
Client Configuration	6
Conclusion	9

Executive Summary

Dell recently launched a new tool, Dell Windows® Debugger Utility (DWDU), to perform server Windows kernel debugging using an Out Of Band (OOB) interface. The tool is designed so that the Dell Remote Access Controller / integrated Dell Remote Access Controller (DRAC/iDRAC) firmware is untouched, and only the host requires new software.

Introduction

This White Paper provides information on using Dell Windows Debugger Utility (DWDU) the way to remotely debug the Windows kernel in case of operating system issues. Currently, the kernel can be debugged using tools such as Windows Debugger(WinDbg) or Kernel Debugger(KD) that are running on a client machine that is connected to the server using a serial interface; the debugging tool must be available on the machine connected to the server. This paper details how to debug a Windows Server OS on a Dell server over the network utilizing DWDU along with the Microsoft tools (WinDbg and KD).

Overview

Dell DRAC products have a Serial over LAN (SOL) feature that redirects serial data over the network. It is mainly used to perform serial console redirection of the server over the network to remote systems. This traffic can be captured using tools like <code>lpmitcol</code> and by enabling the SOL channel to DRAC. The same channel can also be used to redirect the debug data over the network. Once this data reaches the client, it can be serialized and provided to the Microsoft tools; these tools use this connection as a serial connection even though the data is coming over the network.

DWDU has the following features:

- 1. Remote debugging of the Windows Server kernel
- 2. Remotely monitor the Windows boot process
- 3. Real-time Windows Driver debugging

Server Configuration

1. BIOS Setup

The BIOS should be configured so that only the Windows Debug data is redirected over the SOL connection. The BIOS settings are shown in Figure 1 below.

🖉 root::PowerEdge 1950		
Dell Inc. (www.dell. BIOS Version 99.4.2	com) - PowerEdge 1950 [TEST-Aug29IPMIBoot]	
Service Tag: JGZRV1S	Asset Tag:	
System Time Sy Serial Communication On we Me External Serial Connector COM1 CP Failsafe Baud Rate 11520 Remote Terminal Type UT100 SA Redirection After Boot Enab Boot Sequence USB Flash Drive Emulation Type Boot Sequence Retry Integrated Devices PCI IRQ Assignment Serial Communication		
Up,Down Arrow to select SPACE,+,-	to change ESC to exit F1=H	elp

Figure 1: BIOS Settings

2. Enable Windows Server in Debug mode

Configuring Win2K3 Servers

To enable the debug mode, open the Boot.ini file on the target computer and add any of the following options to configure the environment:

- /debug turns on the kernel debugger.
- /debugport specifies the serial port to be used by the kernel debugger; use COM2 for DRAC5/iDRAC tower and rack systems and COM1 for iDRAC modular systems (10G and 11G).
- /crashdebug sends debug information only when a fatal system error (FSE) occurs.
- /baudrate sets the kernel debugger baud rate; set the baud rate to 115200.

Example of a boot.ini file:

```
[boot loader]
```

timeout=5

default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

[operating systems]

```
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Debug (com2)"
/fastdetect
```

/debug /debugport=com2 /baudrate=115200

Configuring Post Win2K3 Servers Consider the following when setting up the OS:

- Enable Windows OS for debug
 - o Bcdedit /debug ON
- For DRAC5, iDRAC6 rack and tower servers:
 - o Set the debug settings to point to COM2

Bcdedit /dbgsettings serial baudrate:115200 debugport:2

- For 10th generation and newer Dell blade servers:
 - o Set the debug settings to point to COM1

Bcdedit /dbgsettings serial baudrate: 115200 debugport: 1

- 3. DRAC/iDRAC Configuration
 - Enable IPMI Over LAN with following settings as shown in Figure 2 below

🏉 Dell Remote Access Cont	roller 5 - Windows Internet Explorer provided by De	ell I/T
🔄 🕞 👻 🙋 https://10.94.3	20.113/cgi-bin/webcgi/main	🔽 😵 Certificate Error 🤄 🗙 Google 🖉 🗸
Elle Edit View Favorites]	Tools Help	
Google	🗸 🔧 Search 🔹 🧒 ד 🚽 🐼 Sl	ihare + 🧕 + 🔲 Sidewiki + 🏠 Bookmarks + 🥙 Check + 👪 Translate + 🎦 AutoFill + 🌽
😪 Convert 🔹 🛃 Select		
S I •	🔍 🍷 Web Search 🔶 🖂 👻 Mail 🔹 🐼 I	My Yahoo! 🔹 🔀 Answers 🔹 🔰 Anti Spy* 🚱 Bookmarks* 😑 Messenger* 😭 Movies 🔹 🔞 Sports 🔹 🕥 News 🔹 🚿 Mobile 🔹 💦
🚖 🏟 🌈 Dell Remote Access	Controller 5	A v R - A v Page v (A Tools v *
Dell Remote Access Contro	oller 5	Support Help About Log Out
		PowerEdge 1950
DØLL		root, Admin
	DRAC Update Properties Configuration Logs	Session Management Diagnostics
- System	Network Users Active Directory SSL Seria	al Senal Over LAN Services Smart Card
Remote Access	Static Gateway	10.94.20.1
Batteries	Static Subnet Mask	255.255.254.0
Intrusion	Use DHCP to obtain DNS server addresses	
Hardware Performance	Static Preferred DNS Server	0.0.0
Power Monitoring	Static Alternate DNS Server	0.0.0.0
Power Supplies	Register DRAC on DNS	
Voltages	DNS DRAC Name	rac-JGZRV1S
, i i i i i i i i i i i i i i i i i i i	Use DHCP for DNS Domain Name	
	DNS Domain Name	
	Auto Negotiation	⊙ On O Off
	Network Speed	C 100 Mb (6 10 Mb
	Duplex Mode	
	[Back to Top]	
	IPMI LAN Settings	
	Enable IPMI Over LAN	
	Channel Privilege Level Limit	Administrator
	Encryption Key	000000000000000000000000000000000000000
	Enable VLAN ID	
	VLAN ID	1
	Priority	0
	(Deals to Tax)	
	[Back to lop]	
		Apply Changes
		~
Done		Stocal intranet 🔍 100% 👻

Figure 2: IPMI over LAN settings

• Enable Serial Over LAN with following settings as shown in Figure 3 below

🏉 Dell Remote Access Contr	roller 5 - Windows Internet Explorer pr	rovided by Dell I/T	_ 0 🔀
🕞 🕞 👻 🛃 https://10.94.2	20.113/cgi-bin/webcgi/main	💌 😵 Certificate Error 🛛 🐓 🗙	Google 🔎 🔻
Eile Edit View Favorites I	[ools Help		
Google	🗙 🔧 Search 🔹 🖓 🗸	📲 🕈 🙋 Share 🔻 🧕 🖲 🔍 Sidewiki 🔹 🏠 Bookmarks 🔹 🍄 Check 🍷 🚂 Translate 💌 📔 AutoFill 🐑 🌽	🔦 🔹 🔘 Sign In 🔹
Convert - Select	A Web Cased		- Carlos - Marchille - San
	v web search o Pi v @	Mail * Wy my Yahoo! * W Answers * W And Spy* Weboxmans* messenger* W movies * Sports	
Dell Remote Access	Controller 5		
Den Remote Access Contro			PowerEdge 1950
DØLL	DRAC Undate Properties Configura	ation Long Session Management Diagnostics	root, Admin
	Network Users Active Directory	SSL Serial Serial Over LAN Services Smart Card	
Remote Access			~
Batteries	Sorial Over LAN Configur	ration	
Intrusion	Senar Over LAN Conligui	Print	Refresh Advanced Settings
Hardware Performance			
Power Supplies	Use this page to configure serial (over LAN settings.	
Voltages	Attribute	Value	
	Enable Serial Over LAN		
	Baud Rate Channel Privilege Level Limit	115.2 kbps V	
	Channel I Hvilege Level Linne		
		Apply Changes	
Done			V Local intranet

Figure 3: Serial over LAN settings

Client Configuration

- 1. Debugging tools there are two Kernel debugging tools available from Microsoft WinDbg and KD
 - WinDbg is a multi-purpose debugger for Microsoft Windows that is distributed on the Web by Microsoft.
 - o KD is the command line debugging tool

These tools are prerequisite for remote debugging and can be downloaded from: <u>http://www.microsoft.com/whdc/devtools/debugging/default.mspx</u>

2. NULL Modem Emulator - the NULL modem emulator (com0com) is an open source kernelmode virtual serial port driver for Windows. You can create an unlimited number of virtual COM port pairs using this tool and use any pair to connect one COM port based application to another. This tool must be installed on the client system, and configured with a COM port pairs for Dwindbg (CNCA1 and COM8). Figure 4 below provides the needed setup information.





For more information, go to the following Website: http://sourceforge.net/projects/com0com/

3. Dwindbg tool - download Dwindbg.msi from https://support.dell.com, and install it on the client machine. Once it is installed, the Windows Debugger Utility icon is on the desktop. Click the icon to display the following screen, as is shown in Figure 5.

(
Dell Windows Debugger	Utility 🛛 🔶 🔀	
DRAC Name or IP Address:		
User Name:		
osci indino.		
Password:		
Debugger Type:	💿 WinDbg	
	🔘 KD	
Debugger Path:		
C:\Program Files\Debugging	g Tools for Windows (x86)\	
	Browse	
Debugger Command Line Options:		
St	art	

Figure 5: Dell Windows Debugger Utility

Enter all of the required parameters - DRAC Name or IP address, User Name, Password, and Debugger Type and press Start. The selected Microsoft debugger will be launched and the environment is ready for debugging. Figure 6 shows the launch screen for WinDbg, and Figure 7 shows the launch screen for KD.



🧶 Kernel 'com:pipe,port=CNCA1,reconnect,baud=115200' - WinDbg:6.11.0001.404 X86	_ 🗆 🗙
Eile Edit Yiew Debug Window Help	
Command	2 🛛
Microsoft (R) Windows Debugger Version 6.11.0001.404 X86 Copyright (c) Microsoft Corporation. All rights reserved.	
<pre>Opened \\CNCA1 Waiting to reconnect Connected to Windows Server 2003 3790 x86 compatible target at (Fri Feb 19 15:45:55.064 2010 (GMT+5)), p Kernel Debugger connection established. Symbol search path is: SRV*c:\local cache*http://msdl.microsoft.com/download/symbols Executable search path is: Windows Server 2003 Kernel Version 3790 (Service Pack 2) MP (2 procs) Free x86 compatible Product: Server, suite: TerminalServer SingleUserTS Built by: 3790.srv03_sp2_rtm.070216-1710 Machine Name: Kernel base = 0x80800000 PsLoadedModuleList = 0x808a6ea8 Debug session time: Thu Feb 18 21:18:43.359 2010 (GMT+6) System Uptime: 0 days 3:41:37.062 Opened log file 'Test' Fri Feb 19 15:46:01.112 2010 (GMT+5): Single step exception - code 80000004 (first chance) First chance exceptions are reported before any exception handling. This exception may be expected and handled. f7609ca4 e81d040000 call f760a0c6</pre>)tr64 FAISE
0: kd>	
Ln 0, Col 0 Sys 0:KdSrv:S Proc 000:0 Thrd 000:0 ASM 0	OVR CAPS NUM

```
Figure 7: Launch Screen for KD
```

🔤 C:\Program Files\Debugging Tools for Windows (x86)\kd.exe	- 🗆 י	ĸ
Microsoft (R) Windows Debugger Version 6.11.0001.404 X86 Copyright (c) Microsoft Corporation. All rights reserved.		
Opened \\.\CNCA1 Waiting to reconnect Connected to Windows Server 2003 3790 x86 compatible target at (Fri Feb 19 :18.752 2010 (GMT+5>), ptr64 FALSE Kernel Debugger connection established. Symbol search path is: *** Invalid *** *********************************	15:5-	
* Symbol loading may be unreliable without a symbol search path. * Use .symfix to have the debugger choose a symbol path. * After setting your symbol path, use .reload to refresh symbol locations. ************************************	* * *	
Executable search path is: ************************************		
* using the _NT_SYMBOL_PATH environment variable. * * using the -y <symbol_path> argument when starting the debugger. * * using .sympath and .sympath+ * **********************************</symbol_path>		
*** ERROR: Symbol file could not be found. Defaulted to export symbols for pamp.exe - Windows Server 2003 Kernel Version 3790 (Service Pack 2) MP (2 procs) Free ompatible	ntk x86	
Product: Server, suite: TerminalServer SingleUserTS Built by: 3790.srv03_sp2_rtm.070216-1710 Machine Name: Kernel base = 0x80800000_PsLoadedModuleList = 0x808a6ea8		
Debug session time: Thu Feb 18 21:18:43.359 2010 (GMT+6) System Uptime: 0 days 3:41:37.062 Single step exception - code 80000004 (first chance) First chance exceptions are reported before any exception handling. This exception may be expected and handled. f7609ca4 e81d040000 call f760a0c6		
	•	-

Conclusion

Dell Windows Debugger Utility (DWDU) is a tool that can be used to perform remote Windows debugging in an environment where servers are maintained in a secured lab, and physical access to the servers is difficult. This tool provides a mechanism to remotely connect to the server through the server's DRAC infrastructure, and then can be used to capture debug traces and perform remote debugging activities.