Jabber for Windows Crash Dump Analysis mit dem WinDbg-Tool

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Durchführen einer Absturzanalyse für Cisco Jabber für Windows WinDbg-Symbolkonfiguration Absturzanalyse in WinDbg

Einführung

Dieses Dokument beschreibt die Vorgehensweise zum Analysieren der **.dmp-**Datei, die beim Absturz des Cisco Jabber für Windows-Clients erstellt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Cisco Jabber für Windows zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Jabber für Windows Version 9.x und Cisco Unified Personal Communicator (CUPC) Version 8.6.x.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Durchführen einer Absturzanalyse für Cisco Jabber für Windows

Verwenden Sie das WinDbg-Tool, um eine Crash-Dump-Analyse durchzuführen. Laden Sie das Tool von der <u>WinDbg-Website herunter.</u>

WinDbg-Symbolkonfiguration

- 1. Um den Symbolpfad zu ändern, navigieren Sie zu Datei > Symbol File Path > Symbol Path.
- 2.
- 3. Fügen Sie den Text in das Fenster ein:

SRV*c:\websymbols*http://msdl.microsoft.com/download/symbols

- 4.
- 5. Klicken Sie auf OK.

Absturzanalyse in WinDbg

1. Starten Sie WinDbg.



2. 3 Klicken Sie im M

3. Klicken Sie im Menü Datei auf Crash Dump öffnen.

WinDbg:6.2.9200.16384 X86		
ile Edit View Debug Window	Help	
Open Source File Close Current Window	Ctrl+O Ctrl+F4	
Open Executable Attach to a Process	Ctrl+E F6	
Open Crash Dump	Ctrl+D	
Connect to Remote Session Connect to Remote Stub	Ctrl+R	
Kernel Debug	Ctrl+K	
Symbol File Path Source File Path Image File Path	Ctrl+S Ctrl+P Ctrl+I	
Open Workspace Save Workspace Save Workspace As Clear Workspace Delete Workspaces Open Workspace in File Save Workspace to File	Ctrl+W	
Map Network Drive Disconnect Network Drive		
Recent Files		
Exit	Alt+F4	Sys 0: <none> Proc 000:0 Thrd 000:0 ASM OVR CAPS NU</none>

4. Wählen Sie die Datei **.dmp** (memory.dmp, user.dmp usw.) aus, und klicken Sie auf **Öffnen** oder ziehen Sie die Datei **.dmp** in WinDbg. In diesem Beispiel wird die **Volldump-**Datei verwendet.



5.

6. Geben Sie im Befehlsfenster unten **!analyze - v ein**, und drücken Sie die Eingabetaste.



7.

8. Sie sehen den Fortschritt der Analyse unten links im Bildschirm. In diesem Bild lautet der Status "BUSY".

- 0 23 Dump C:\Users\asishtla\Desktop\chris jones\fulldump.dmp - WinDbg:6:2.9200.16384 X86 Edit View Debug Window Help File Cô. Command - Dump C:\Users\asishtla\Desktop\chris jones\fulldump.dmp - WinDbg:6.2.9200.1638... Loading unloaded module list ٠ eax=03c64370 ebx=00000001 ecx=00000002 edx=00000000 esi=0013fdb0 edi=0013fd94 eip=776f7094 esp=0013fc94 ebp=0013fcb0 iopl=0 cs=001b ss=0023 ds=0023 es=0023 fs=003b e nv up ei pl zr na pe nc es=0023 fs=003b gs=0000 ef1=00000246 ntdll!KiFastSystemCallRet: 776f7094 c3 ret 0:000> !analyze -v Exception Analysis WARNING: Unable to verify timestamp for CiscoJabber.exe Module load completed but symbols could not be loaded for CiscoJabb *** ERROR: *** WARNING: Unable to verify timestamp for JabberUtils.dll Module load completed but symbols could not be loaded for JabberUti *** ERROR: *** WARNING: Unable to verify timestamp for msvcr90.dll *** WARNING: Unable to verify timestamp for VoicemailService.dll *** ERROR: Module load completed but symbols could not be loaded for Voicemail *** WARNING: Unable to verify timestamp for servicesframework.dll *** ERROR: Module load completed but symbols could not be loaded for servicesf: *BUSY* Ln 0, Col 0 Sys 0:C:\User Proc 000:11b4 Thrd 000:197c ASM OVR CAPS NUM

Dieser Befehl führt eine Analyse mit einer ausführlichen Anzeige von Daten durch und ist hilfreich, um weitere Informationen abzurufen.

9.

10. Geben Sie zum Beenden **q** im Befehlsfenster ein, und drücken Sie die **Eingabetaste**. Hier ein Beispiel für die Ausgabe eines Dump-Analyzers:

```
> !analyze -v
<snip>
STACK_TEXT:
WARNING: Frame IP not in any known module. Following frames may be wrong.
02f4e80c 01457967 7ffdac00 00000104 02f4e86c 0x0
02f4e848 0145637d 0000001 02f4e86c 02f4ed58 wxvault+0x7967
02f4ea88 7c8138b7 7ffdac00 0000000 02f4eac8 wxvault+0x637d
02f4ed1c 009a436f 00b413b4 02f4ed58 0000000
kernel32!FindFirstFileA+0x3a
02f4edb8 00000000 00000000 00000000 CUPCK9+0x5a436f
STACK_COMMAND: ~8s; .ecxr ; kb
SYMBOL_STACK_INDEX: 1
SYMBOL_NAME: wxvault+7967
```

FOLLOWUP_NAME: MachineOwner

MODULE_NAME: wxvault

IMAGE_NAME: wxvault.dll

DEBUG_FLR_IMAGE_TIMESTAMP: 450162c1

FAILURE_BUCKET_ID: NULL_INSTRUCTION_PTR_c0000005_wxvault.dll!Unknown

BUCKET_ID: APPLICATION_FAULT_NULL_INSTRUCTION_PTR_NULL_POINTER_READ_DETOURED_NULL_IP_ wxvault+7967

Überprüfen Sie **MODULE_NAME** und **IMAGE_NAME**. Diese Informationen wie **wxvault.dll** oder **CiscoJabber.exe** geben an, welche Anwendung den Absturz verursacht hat. In diesem Fall ist der Absturz aufgrund von Problemen mit der Anwendung Cisco Jabber.exe und nicht mit dem Computer des Benutzers aufgetreten. Eine Google-Suche zeigt, dass **wxvault.dll** mit der DELL Embassy Trust Suite in Zusammenhang steht.

Senden Sie den Cisco Jabber-Problembericht an das Cisco Technical Assistance Center, um festzustellen, ob das Absturzsignal mit einem bekannten Fehler zusammenhängt, der möglicherweise behoben werden kann.