eBook Gratuit

APPRENEZ WinDbg

eBook gratuit non affilié créé à partir des **contributeurs de Stack Overflow.**

#windbg

Table des matières

À propos

You can share this PDF with anyone you feel could benefit from it, downloaded the latest version from: windbg

It is an unofficial and free WinDbg ebook created for educational purposes. All the content is extracted from Stack Overflow Documentation, which is written by many hardworking individuals at Stack Overflow. It is neither affiliated with Stack Overflow nor official WinDbg.

Use the content presented in this book at your own risk; it is not guaranteed to be correct nor accurate, please send your feedback and corrections to info@zzzprojects.com

Chapitre 1: Démarrer avec WinDbg

Remarques

Cette section fournit une vue d'ensemble de ce qu'est windbg et pourquoi un développeur peut vouloir l'utiliser.

Il devrait également mentionner tous les grands sujets au sein de windbg, et établir un lien avec les sujets connexes. La documentation de windbg étant nouvelle, vous devrez peut-être créer des versions initiales de ces rubriques connexes.

Versions

Versions importantes de WinDbg, pour les versions prises en charge de WinDbg. Voir aussi une liste détaillée avec des versions historiques en ligne.

Il est important de noter qu'il existe un système de gestion des versions qui est passé de l'ancienne version 6.12 à la nouvelle version 6.1. Les anciennes versions ont des nombres faibles (<100) à la troisième place, tandis que les nouvelles versions ont des nombres élevés (> 6000).

Dans de nombreux cas, les versions WinDbg fournies pour les nouvelles versions de Windows fonctionnent encore sur les anciennes versions de Windows, par exemple la version 10 de WinDbg peut toujours être utilisée sur Windows 7. Cependant, certaines commandes peuvent utiliser des appels API non disponibles. Par conséquent, il est bon d'avoir plusieurs versions de WinDbg disponibles.

Version	La description	Date de sortie
6.12.0002.633	fourni pour Windows 7 et .NET Framework 4	2010-05-21
6.1.7600.16385		2009-07-24
6.2.8400.0	mise à jour pour Windows 8 (?)	2012-06-23
6.2.9200.16384	fourni pour Windows 8 et .NET Framework 4.5	2012-11-15
6.3.9600.16384	fourni pour Windows 8.1	2013-10-17
10.0.10075.9	fourni pour Windows 10	2015-04-29
10.0.10586.567	fourni depuis Windows 10, build 1511	2015-10-30
10.0.14321.1024	fourni depuis Windows 10, build 1607	2016-07-29

Examples

Installation ou configuration

Microsoft décrit 3 façons d'installer WinDbg:

- dans le cadre du WDK (Windows Driver Kit)
- dans le cadre du SDK (Software Development Kit)
- avec l'installateur du SDK et désélectionner tout sauf "Outils de débogage pour Windows"

Pour obtenir le programme d'installation, visitez Télécharger les outils WDK, WinDbg et associés et faites défiler jusqu'à une section intitulée «Obtenir les outils de débogage».

Codemachine est une source bien connue et pratique, mais vous pouvez également télécharger les anciennes versions des outils de débogage directement.

La configuration elle-même est simple. Cliquez sur l'installateur jusqu'à ce qu'il se termine.

Débogueurs

WinDbg est souvent utilisé comme abréviation de "Outils de débogage pour Windows". Il contient différents débogueurs:

Débogueur	La description
WinDbg	le débogueur avec une interface graphique
CDB	**C** onsole **d** e **b** ugger, débogueur en mode utilisateur qui s'exécute dans la console actuellement ouverte
NTSD	**n** ew **t** erminal **s** ymbolic **d** ebugger, le mode d'emploi débogueur qui ouvre un nouveau terminal (console) comme son nom l' indique
KD	**k** Ernel **d** ebugger, qui se déroule dans la console currrently ouverte
NTKD	**n** ew **t** erminal **k** ernel **d** ebugger, ouvre un nouveau terminal

Les commandes sont identiques, sauf qu'il peut y avoir des commandes liées à l'interface graphique qui ne fonctionnent pas dans les versions de la console.

Lire Démarrer avec WinDbg en ligne: https://riptutorial.com/fr/windbg/topic/1833/demarrer-avec-windbg

Chapitre 2: Analyse de crash

Examples

Analyse de crash en mode utilisateur de base

`.exr -1` vous donne des détails sur la dernière exception lancée.

`!analyze -v` fait aussi du bon travail.

Pour .NET, la commande `!pe` de l'extension SOS affiche des détails sur l'exception .NET renvoyée.

Lire Analyse de crash en ligne: https://riptutorial.com/fr/windbg/topic/5389/analyse-de-crash

Chapitre 3: Débogage à distance

Examples

Commandes importantes

- .server - crée un serveur de débogage
- .clients - Répertorie les clients de débogage connectés au serveur
- .endsrv - Termine un serveur de débogage
- .servers - liste les connexions du serveur de débogage
- .remote - lance un serveur remote.exe
- .noshell - Empêche les commandes shell

Lire Débogage à distance en ligne: https://riptutorial.com/fr/windbg/topic/5977/debogage-a-distance

Chapitre 4: Débogage du mode utilisateur / application

Examples

Commandes importantes

Documenter votre travail

Rappelez-vous ce que vous avez fait et conservez les sorties longues qui ne peuvent pas être conservées dans le tampon de WinDbg. Il est toujours bon d'avoir un journal disponible pour reproduire les étapes de débogage, par exemple pour poser des questions sur le débordement de la pile.

Commander	Objectif
`.logopen`	créer un fichier journal
`.logclose`	ferme le fichier journal
`.dump`	enregistrer le fichier de vidage sur incident (instantané de la session de débogage en cours)

Travailler avec des symboles

Sans ou avec des symboles incorrects, vous pouvez recevoir des informations erronées et être induits en erreur. Assurez-vous de bien connaître ces commandes avant de commencer à travailler dans WinDbg. Voir aussi Comment configurer des symboles dans WinDbg .

Commander	Objectif
`.symfix`	définir ou ajouter des symboles au chemin d'accès officiel Microsoft
`.sympath`	définir ou ajouter des symboles propres ou de tiers
`.reload`	recharger les symboles
`.symopt`	définir les options de manipulation des symboles
`!sym`	symbole de chargement
`x`	examiner les symboles
`ln`	liste des symboles les plus proches

Analyse de crash

Découvrez ce qui s'est passé (dans les vidages sur incident) et comment gérer les événements (dans le débogage en direct).

Commander	Objectif
`.exr`	afficher l'enregistrement d'exception
`.lastevent`	afficher le dernier événement
`sx`	définir la gestion des exceptions
`!analyze`	analyser un crash ou se bloquer
`!avrf`	vérificateur d'application

L'environnement

Vérifiez le nom du processus et les informations de version.

Commander	Objectif
| (tuyau)	traitement de l'information
`lm`	liste des modules

Threads, piles d'appels, registres et mémoire

Inspectez les détails.

Commander	Objectif
`~`	liste de fils
`r`	registres
`k`	pile d'appels
`d` *	afficher la mémoire
`e` *	modifier la mémoire
`s`	recherche mémoire
`.formats`	convertir entre les formats de nombres

Commander	Objectif
`?`	évaluer l'expression
`u` *	démonter
`a`	assembler
`!address`	infos mémoire

Contrôler la cible

Dans le débogage en direct, prenez le contrôle de l'exécution.

Commander	Objectif
`g`	aller / continuer
`gu`	monter
`p`	pas à pas
`t`	trace (registres à pas unique et à sortie)
`bp`	définir le point d'arrêt
`bl`	liste des points d'arrêt

Travailler avec des extensions

Les extensions peuvent offrir des avantages et des améliorations significatifs.

Commander	Objectif
`.load`	extension de charge (chemin complet)
`.loadby`	extension de charge relative au module
`.chain`	afficher les extensions chargées
`.unload`	décharger l'extension

Arrêtez le débogage

Commander	Objectif
`q`	quitter et terminer l'application

Commander	Objectif
`qd`	détacher et quitter

Attacher et détacher

Commander	Objectif
`.tlist`	liste des processus
`.attach`	attacher à traiter
`.create`	créer un processus et attacher
`.childdbg`	définir le comportement de débogage du processus enfant
`.detach`	se détacher d'un processus
`.kill`	tuer un processus
`.restart`	redémarrer le processus

Comportement de WinDbg

Commander	Objectif
`.prefer_dml`	définir la gestion du langage de balisage du débogueur
`.effmach`	changer le bitness

Commandes d'utilisabilité

Commander	Objectif
`.cmdtree`	Charge un fichier texte avec des commandes prédéfinies dans une fenêtre séparée

Obtenir des aides

Commander	Objectif
`.hh`	Affiche le manuel d'aide pour les commandes WinDbg

Créer une fenêtre de commande personnalisée dans Windbg

La commande `.cmdtree` permet d'ouvrir un fichier `.txt` avec des commandes prédéfinies que vous pouvez simplement double-cliquer pour exécuter.

Comment créer un fichier de commandes

Créez le fichier en utilisant ce modèle

```
windbg ANSI Command Tree 1.0
title {"Window title"}
body
{"Group Heading"}
 {"Name of command to display"} {"command"}
 {"Name of command to display"} {"command"}
{"Group Heading"}
 {"Name of command to display"} {"command"}
```

Choses à faire

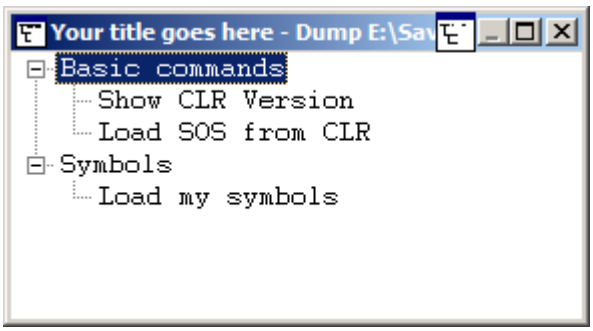
1. Le format du modèle doit être suivi précisément pour ouvrir le fichier dans Windbg.
2. La nouvelle ligne est requise après chaque `{Group Heading}` .
3. Chaque paire `{Name of command to display} {command}` doit se trouver sur une ligne et doit être suivie d'une nouvelle ligne.

Exemple de fichier de commande personnalisé

```
windbg ANSI Command Tree 1.0
title {"Your title goes here"}
body
{"Basic commands"}
 {"Show CLR Version"} {"lmv m clr"}
 {"Load SOS from CLR"} {".loadby sos clr "}
{"Symbols"}
 {"Load my symbols"} {".sympath+ "c:\DebugSymbols" ; .reload"}
```

Comment ouvrir l'interface utilisateur de commande à partir de la fenêtre de commande

Exécutez `.cmdtree <path of your .txt file>` pour ouvrir la fenêtre. Vous verrez une fenêtre comme celle-ci



Double-cliquez sur la commande à exécuter.

Lire Débogage du mode utilisateur / application en ligne:
https://riptutorial.com/fr/windbg/topic/5384/debogage-du-mode-utilisateur---application

Chapitre 5: Débogage du noyau

Examples

Commandes importantes

- ! process - liste les processus en mode utilisateur
- .process - définit le contexte du processus
- ! peb - affiche le bloc d'environnement de processus
- ! teb - affiche le bloc d'environnement de thread
- ! locks - analyse de blocage
- .dump - enregistre un fichier de vidage sur incident sur le disque

Lire Débogage du noyau en ligne: https://riptutorial.com/fr/windbg/topic/6076/debogage-du-noyau

Chapitre 6: DML (langage de marquage du débogueur)

Examples

Allume / éteint

.prefer_dml 1 active la sortie dmlformat

.prefer_dml 0 désactive la sortie dmlformat

Lire DML (langage de marquage du débogueur) en ligne:
https://riptutorial.com/fr/windbg/topic/7987/dml--langage-de-marquage-du-debogueur-

Chapitre 7: Les extensions

Examples

SOS

SOS (son of strike) est l'extension officielle WinDbg de Microsoft pour .NET. Il est installé dans le cadre de .NET et est donc disponible par défaut.

Comme toute extension, il peut être chargé en utilisant `.load x:\full\path\to\sos.dll` , mais il existe des moyens plus simples. Selon la version de .NET, l'extension est située côte à côte avec `mscorwks.dll` (.NET CLR 2), `clr.dll` (.NET CLR 4) ou `coreclr.dll` (applications Silverlight et Universal). Les commandes suivantes devraient fonctionner:

```
.loadby sos clr
.loadby sos coreclr
.loadby sos mscorwks
```

Pour une liste des commandes disponibles, consultez `!help` .

SOSex

SOSex est une extension de SOS, écrite par Steve Johnson , un employé de Microsoft. Il fournit gratuitement SOSex en téléchargement , mais ce n'est pas open source.

En règle générale, l'extension n'est pas disponible côte à côte avec une autre DLL, il est donc généralement chargé avec `.load x:\full\path\to\sosex.dll` .

Outre la simplification du débogage de .NET, la commande `!dlk` peut également être utilisée dans des environnements natifs pour vérifier les blocages des sections critiques.

Pour une liste des commandes disponibles, consultez `!help` de SOSex.

PyKD

PyKD est une extension WinDbg qui vous permet d'écrire des scripts Python. C'est open source.

En général, l'extension n'est pas disponible côte à côte avec une autre DLL, elle est donc généralement chargée avec `.load x:\full\path\to\pykd.pyd` , où PYD est l'extension d'une DLL python, mais que vous pouvez renommer à DLL si vous voulez.

Démarrer avec PyKd

PyKD n'offre pas d' `!help` , alors consultez la documentation de Codeplex. De nombreux développeurs semblent provenir de Russie et la documentation la plus récente et la plus complète est probablement en russe. Google Translater fait un travail décent.

Comme les autres extensions, utilisez le bitness correct de l'extension qui correspond à celui de WinDbg. De plus, Python doit également être installé avec le même bitness.

`!py` exécute un interpréteur REPL et `!py x:\path\to\script.py` exécute un script python. Les scripts doivent utiliser

```
from pykd import *
```

en tant que première ligne pour utiliser les fonctionnalités de PyKD, alors que cette ligne n'est pas nécessaire dans l'interpréteur REPL. L'interpréteur peut être quitté en utilisant `exit()` .

NetExt

NetExt est une extension pour .NET qui fournit

- Requêtes LINQ-like pour les objets sur le tas (`!wselect !wfrom`)
- capacités d'affichage pour des objets spéciaux comme les dictionnaires et les tables de hachage (`!wdict !whash`)
- Commandes associées à ASP.NET / HTTP (`!wcookie !wruntime !whttp`)
- plusieurs autres commandes liées au réseau

En règle générale, l'extension n'est pas disponible côte à côte avec une autre DLL, elle est donc généralement chargée avec .load x: \ full \ path \ to \ netext.dll

Vue d'ensemble des extensions

Une liste incomplète des extensions WinDbg qui ne sont pas installées avec WinDbg lui-même:

Extension	Objectif
SOS	.NET (extension officielle Microsoft)
SOSex	.NET (extension pour SOS)
CoSOS	.NET (extension pour SOS)
NetExt	.NET (en mettant l'accent sur la mise en réseau)
PyKD	Script Python
PDE	Windows native et applications de stockage (exceptions stockées)
PSSCOR	.NET
SDbgExt	.NET
MEX	.NET

CoSOS

COSOS (cousin de SOS) est une extension open source pour WinDbg se concentrant sur la fragmentation de la mémoire .NET (`!gcview`) et les questions de filetage (`!wfo` , `!tn`).

En règle générale, l'extension n'est pas disponible côte à côte avec une autre DLL, elle est donc généralement chargée avec `.load x:\full\path\to\cosos.dll` . Il nécessite que SOS soit chargé et fonctionne actuellement avec des applications 32 bits uniquement.

Lire Les extensions en ligne: https://riptutorial.com/fr/windbg/topic/5391/les-extensions

Crédits

S. No	Chapitres	Contributeurs
1	Démarrer avec WinDbg	Community, Thomas Weller
2	Analyse de crash	Thomas Weller
3	Débogage à distance	Thomas Weller
4	Débogage du mode utilisateur / application	Piyush Parashar, Thomas Weller, X. Liu
5	Débogage du noyau	Thomas Weller
6	DML (langage de marquage du débogueur)	Wang Zhengzhang
7	Les extensions	Jason Evans, Lieven Keersmaekers, Thomas Weller