



## [分享]双机内核调试入门



随风行



1

大侠



2020-8-8 17:28

6843

### 目录

#### 前言

#### 通过管道连接

##### 虚拟机设置

##### 虚拟机系统配置

##### WinDbg Preview 设置

##### 附加成功示意图

##### 异常修复处理

##### 调试器反应慢 卡顿

##### 调试器看不到寄存器、局部变量、Watch

##### 添加一个新的启动加载器

#### 通过工具 VirtualKD-3.0 连接

##### 修改调试器为新版WinDbg Preview

##### WMware15 与 VirtualKD 不兼容 解决方案

#### 设置符号路径

#### 这里插一个调试实用小技巧

#### 参考

1

## 前言

双机调试的配置网上能查到的有很多，但大都大同小异，用早期的版本举例，对新版本的支持有限，缺失异常时的一些处理。

本篇不算原创，是我早先在搭建双机调试环境时，查找相关资料的整理，以及在调试中遇到的部分问题解决的积累。

新版WinDbg Preview是WinDbg的改进版本，具有更多现代视觉效果，更快的窗口，完整的脚本体验，内置支持可扩展的调试器数据模型。同时兼容WinDbg的所有命令，兼容x86与x64系统，更强大的时间旅行调试TTD。

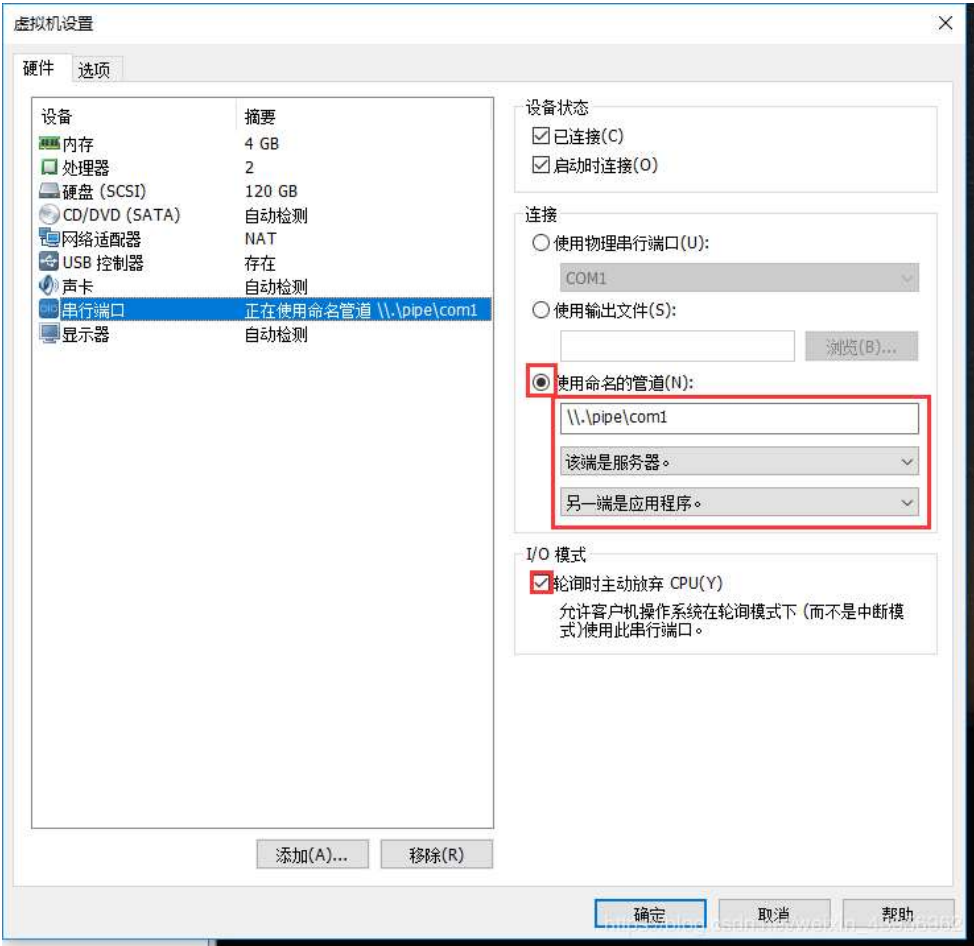
下载：[WinDbg Preview](#)

新版WinDbg Preview配置双机内核调试有两种方法。

## 通过管道连接

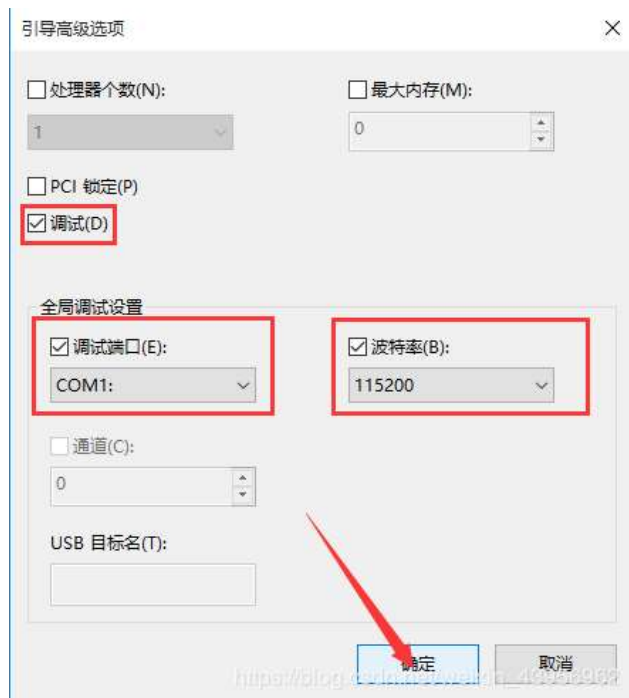
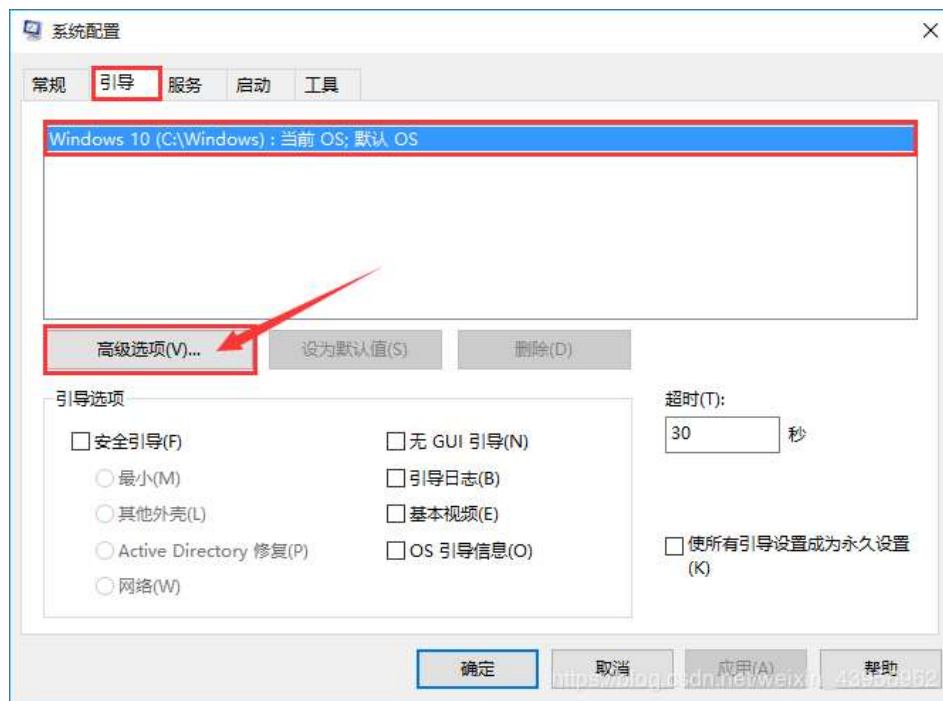
虚拟机设置

删除不必要的设备，添加串行端口。



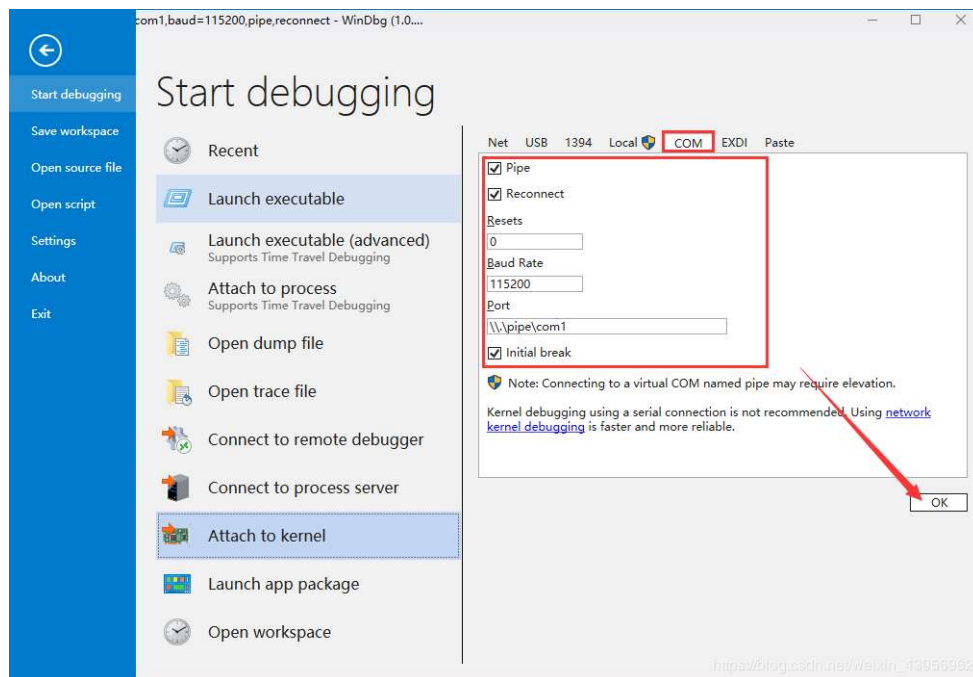
## 虚拟机系统配置

虚拟机中 WIN+R msconfig 打开系统配置

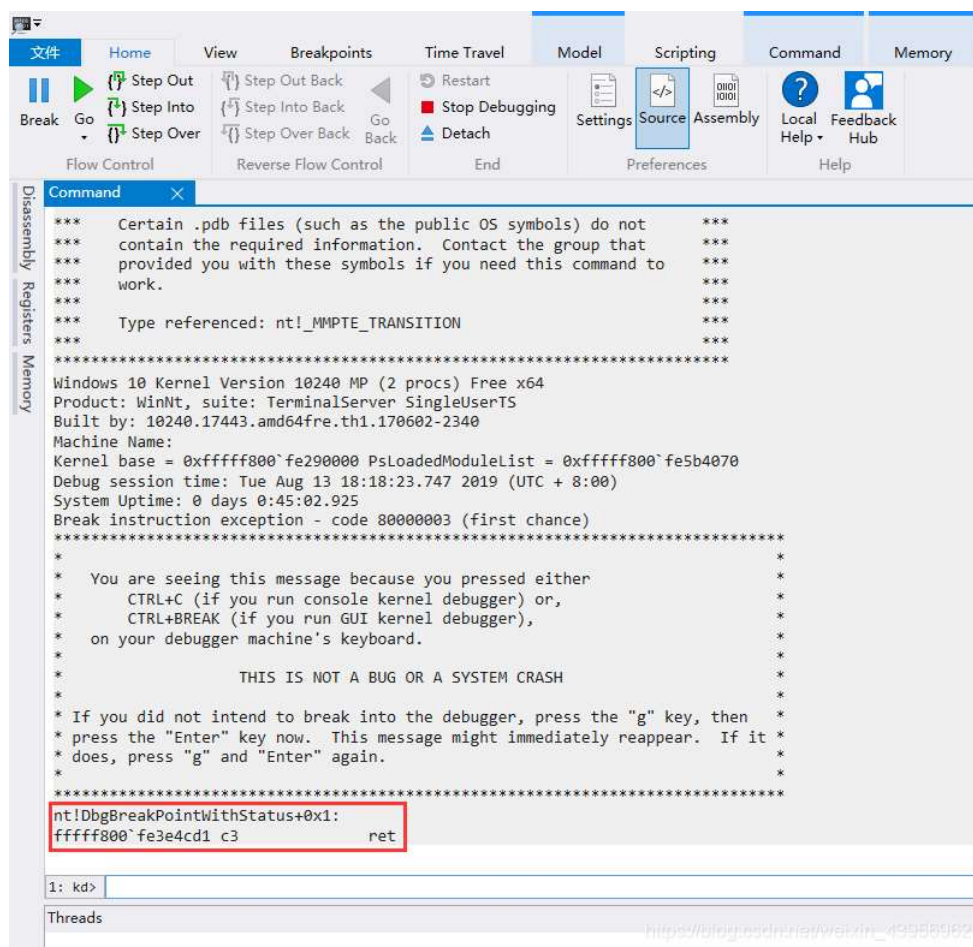


## WinDbg Preview 设置

主机中 打开WinDbg Preview File Attach to kernel



## 附加成功示意图



## 异常修复处理

### 调试器反应慢 卡顿

COM 虚拟串口方式连接，调试器反应极其卡顿，可能由于虚拟机为复制的虚拟机，用iso文件创建新的虚拟机，即可解决该问题

## 调试器看不到寄存器、局部变量、Watch

如果遇到 WinDbg Preview 看不到寄存器、局部变量、Watch 虚拟机中 以管理员权限启动 cmd 添加一个新的启动加载器。

### 添加一个新的启动加载器

输入：

```
1 | bcdedit
```

回车

```
CA 管理员: 命令提示符
Microsoft Windows [版本 10.0.17134.285]
(c) 2018 Microsoft Corporation. 保留所有权利。

C:\Windows\system32>bcdedit

Windows 启动管理器
-----
标识符                {bootmgr}
device                partition=\Device\HarddiskVolume1
path                  \EFI\Microsoft\Boot\bootmgfw.efi
description            Windows Boot Manager
locale                zh-CN
inherit                {globalsettings}
default                {current}
resumeobject           {1c6412d1-...-9d9f-e3e9b726f412}
displayorder           {1c6412d2-...-9d9f-e3e9b726f412}
toolsdisplayorder      {memdiag}
timeout                30

Windows 启动加载器
-----
标识符                {1c6412d2-...-9d9f-e3e9b726f412}
device                partition=C:
path                  \Windows\system32\winload.efi
description            Windows 10
locale                zh-CN
inherit                {bootloadersettings}
recoverysequence       {1c6412d3-...-9d9f-e3e9b726f412}
displaymessageoverride Recovery
recoveryenabled        Yes
isolatedcontext        Yes
allowedinmemorysettings 0x15000075
osdevice               partition=C:
systemroot             \Windows
resumeobject           {1c6412d1-...-9d9f-e3e9b726f412}
nx                     OptIn
bootmenupolicy          Standard

Windows 启动加载器
-----
标识符                {current}
device                partition=C:
path                  \Windows\system32\winload.efi
description            Win10_Dbg
locale                zh-CN
inherit                {bootloadersettings}
recoverysequence       {1c6412d3-...-9d9f-e3e9b726f412}
displaymessageoverride Recovery
recoveryenabled        Yes
isolatedcontext        Yes
allowedinmemorysettings 0x15000075
osdevice               partition=C:
https://blog.csdn.net/weixin_43956962
```

设置端口1 (该处的“1”，对应com接口1)

```
1 | bcdedit /dbgsettings serial baudrate:115200 debugport:1
```

复制开机选项 (这里我命名为: "Win10\_Dbg", 可任意修改)

```
1 | bcdedit /copy {current} /d Win10_Dbg
```

增加开机引导项 (ID填写上一条命令生成的字符串)

```
1 | bcdedit /displayorder {current} {ID}
```

激活debug (ID填写上上一条命令生成的字符串)

重启虚拟机，选择“Win10\_Dbg”为启动项

End

## 通过工具 VirtuakKD-3.0 连接

主机打开vmmon64.exe，设置Windbg路径（先使用旧版Windbg路径）

在Windows10中，WinDbg的目录是固定的，如下所示：

- x86: C:\Program Files (x86)\Windows Kits\10\Debuggers\x86\WinDbg.exe
- x64: C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\WinDbg.exe

虚拟机需禁用驱动程序强制签名 这个网上有很多 就不一一赘述了

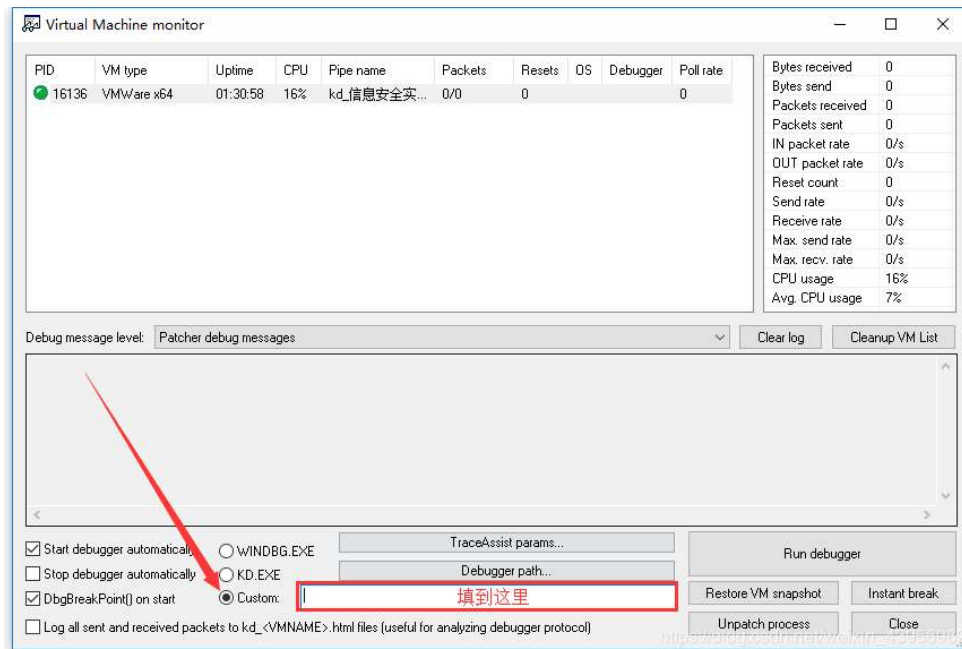
将 target文件夹拷贝到虚拟机 运行vminstall.exe（特别强调：只能装在虚拟机，勿在主机运行）

- 默认设置 无需更改
- 点击 Install
- 重启 选择【调试模式启动】

正常的话，windbg会自动运行

## 修改调试器为新版WinDbg Preview

(DbgX.Shell.exe的路径) /k com:pipe,reset=0,reconnect,port=\\.\pipe\ (此处为虚拟机名)



## WMware15 与 VirtualKD 不兼容 解决方案

Win10 1909 与 旧版本WMware 不兼容

更新WMware到最新15.5.2

但是在新版的WMware上双机内核调试的神器 **VirtuakKD-3.0** 不好使了

这里推荐一个大佬的项目 [VirtualKD-Redux](#)

ZIP压缩包下载链接[VirtualKD-Redux-2020.2](#)

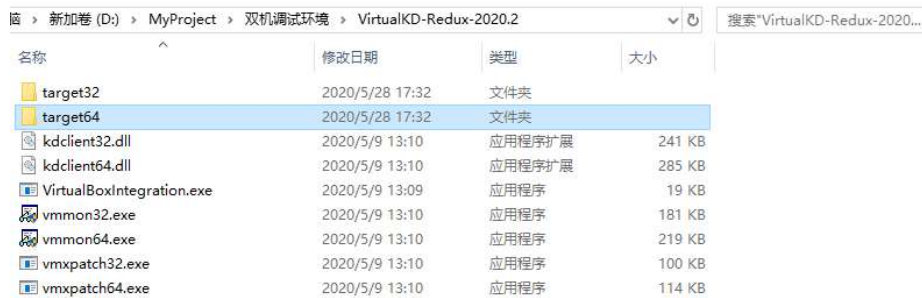
**VirtualKD-Redux** 的用法 与 **VirtuakKD** 一致，而且还支持具有更多现代视觉效果 **WindbgPreview**

安装与使用步骤与**VirtuakKD**一致

这里我简单介绍

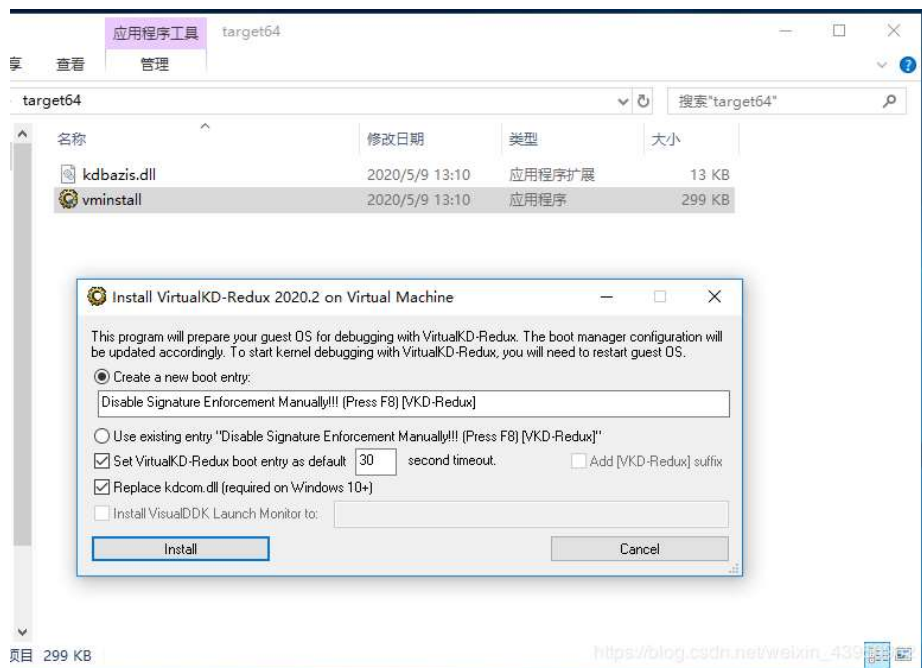


## 1. 拷贝 target 到目标虚拟机 (32位系统拷贝target32, 64位系统拷贝target64)



[https://blog.csdn.net/waixin\\_43956962](https://blog.csdn.net/waixin_43956962)

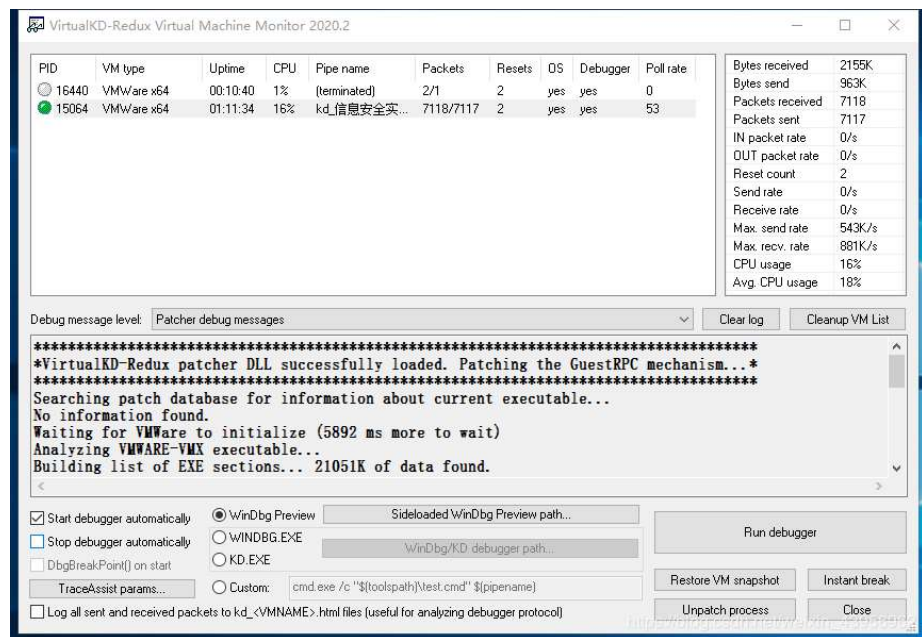
## 2. 虚拟机中执行 target 文件夹中的 vminstall.exe 文件，默认安装即可，最后一步会重启虚拟机



[https://blog.csdn.net/waixin\\_43956962](https://blog.csdn.net/waixin_43956962)

## 3. 根据物理机环境，打开对应版本的 vmmon.exe (32位系统拷贝vmmon32.exe, 64位系统拷贝vmmon64.exe)

## 4. 选取对应的windbg版本， VirtualKD-Redux会替我们自动设置调试器路径，建议 简单检查

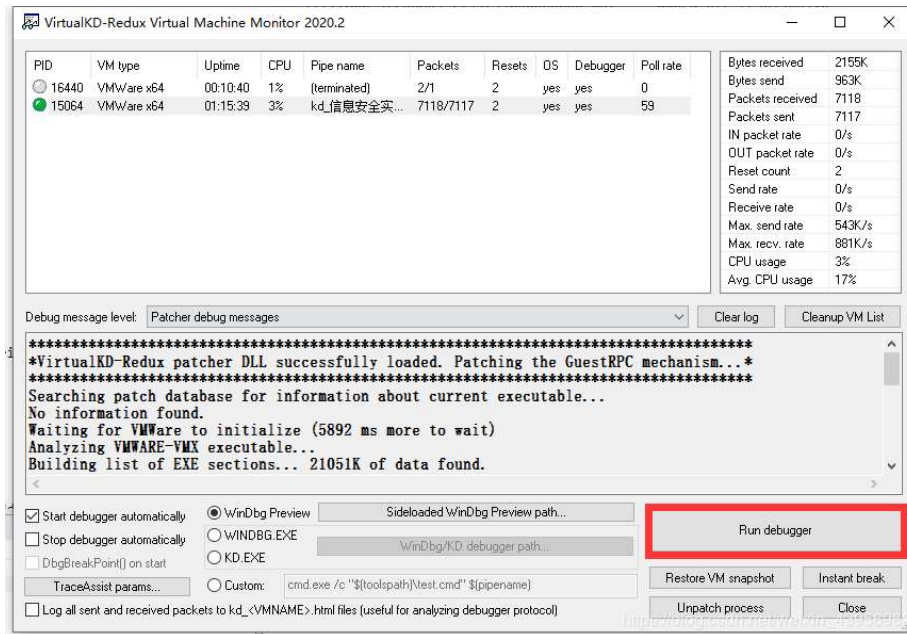


[https://blog.csdn.net/waixin\\_43956962](https://blog.csdn.net/waixin_43956962)

5. 虚拟机在重启中，选择新建的入口，按F8 选择禁用强制签名

Disable Signature Enforcement Manually!!! [Press F8] [VKD-Redux]

6. 虚拟机在重启中VirtualKD会自动拉起我们的调试器，如果没有拉起，可以手动点击 **Run debugger** 打开调试器



## 设置符号路径

```
// 以下命令告诉调试器使用符号服务器从https://msdl.microsoft.com/download/symbols
//的符号存储中获取符号并缓存符号c:\MyServerSymbols。
.symset srv*c:\MyServerSymbols*https://msdl.microsoft.com/download/symbols
```

## 这里插一个调试实用小技巧

双机调试时

普通程序，入口点 main 加 MessageBox(0, 0, 0, 0);

驱动程序，入口点 DriverEntry 加 DbgBreakPoint();

## 参考

- [1]: <https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugging-using-windbg-prev>
- [2]: <https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/symbol-path>
- [3]: <https://blog.51cto.com/14317856/2410156>
- [4]: [https://blog.csdn.net/m0\\_37921080/article/details/82495063](https://blog.csdn.net/m0_37921080/article/details/82495063)
- [5]: <https://www.cnblogs.com/endenvor/p/8926688.html>

[\[2023春季班\]2023. 新的征程，脱壳机更新，iOS/eBPF、赠送云手机套装！一块裸板虚拟化五个容器云手机！3月25日起同时上调价格并赠送新设备！](#)

最后于 2020-8-8 17:29 被随风行编辑，原因：



22



3



收藏 · 22



点赞 · 3



打赏



分享



## 最新回复 (9)



**MsScotch** 2020-8-10 16:50

2楼 0

手把手教学，点赞

极客



**GodSurvive** 2020-8-11 12:06

3楼 0

用vs自带的网络调试不香么，速度还比串口快。😏

极客



**昵称好麻烦** 2020-8-11 17:36

4楼 0

配置windbg preview的时候不用这么麻烦，直接一个bat脚本走起：

```
start "" "C:\Users\[用户名]\AppData\Local\Microsoft\WindowsApps\Microsoft.Windows.Common-UI\WinDbgX.exe" -d -k com:port=\\.\pipe\com_1,baud=115200,pipe -T "Debug Win10X64" -c ".sympath SRV*D:\symbols\symbols10x64*http://msdl.microsoft.com/download/symbols" -c "ed nt!Kd_SXS_Mask 0;ed nt!Kd_FUSION_Mask 0"
```

大侠



**随风行** 2020-8-13 15:28

5楼 0

**GodSurvive** 用vs自带的网络调试不香么，速度还比串口快。[em\_86]

大侠

VS自带的msvsmon双机调试还行，内核调试就不太稳定了😓

可能是我配置的不对，大佬有时间出份教程让我学习一下🙏🏻



**随风行** 2020-8-13 15:39

6楼 0

**昵称好麻烦** 配置windbg preview的时候不用这么麻烦，直接一个bat脚本走起：start "" "C:\Users\[用户名]\AppData\Local\Micros ...

大侠

大佬，请教一下 windbg preview 作为内核调试器时，看不到寄存器、局部变量、Watch，是由于什么问题引起的？🙏🏻



**昵称好麻烦** 2020-8-13 16:36

7楼 0

**随风行** 大佬，请教一下 windbg preview 作为内核调试器时，看不到寄存器、局部变量、Watch，是由于什么问题引起的？[em\_91]

大侠

从Microsoft下载的符号表都是公有符号，不包含局部变量信息，如果是自己写的驱动那就是windbg没有找到符号表；

至于寄存器看不到我也不清楚，试试看".reload"，重新加载一下符号表试试



**随风行** 2020-8-13 16:55

8楼 0

**昵称好麻烦** 从Microsoft下载的符号表都是公有符号，不包含局部变量信息，如果是自己写的驱动那就是windbg没有找到符号表；至于寄存器看不到我也不清楚，试试看".reload"，重新加载一下符号表试试

大侠

嗯，这个我试过，不行的，除了源码、Command、disassembly，其他窗口都是坏的；

现阶段我还是用的windbg，稳定的一批😏

最新回复 (9)



昵称好麻烦 2020-8-13 16:59

9楼 0

大侠

随风行 嗯，这个我试过，不行的，除了源码、Command、disassembly，其他窗口都是坏的；现阶段我还是用的windbg，稳定的一批[em\_78]

额，我一直都用的windbg preview，但我感觉经常坏的是disassembly.....寄存器窗口我一般不用，直接用r指令看寄存器数值



随风行 2020-8-14 09:55

10楼 0

大侠

嗯，我之前也用了一年多windbg preview，重装系统后就怎么都设置不好了😂



游客

[登录](#) | [注册](#) 方可回帖

回帖

表情

[高级回复](#)

返回