# bcdedit 配置

使用bcdedit，配合 msconfig，在虚拟机里设置双机调试，这个步骤是最稳的，100%成功，不再有玄学。

bcdedit /copy {current} /d debug

bcdedit /displayorder {937f570e-d369-11eb-8c9f-000c291fc9bf} /addlast

bcdedit /dbgsettings SERIAL DEBUGPORT:1 BAUDRATE:115200

bcdedit /bootdebug {937f570e-d369-11eb-8c9f-000c291fc9bf} ON

bcdedit /debug {937f570e-d369-11eb-8c9f-000c291fc9bf} ON

bcdedit /timeout 30

090f876d-0a19-11eb-91ce-f2d2a66b6220

//虚拟机配置

这里是把windbg快捷方式发送到桌面，在路径后面加一堆参数，根据自己的环境填写

"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\windbg.exe" -y SRV\*E:\symbol\*http://msdl.microsoft.com/download/symbols -b -k com:port=//./pipe/com\_1,baud=115200,pipe

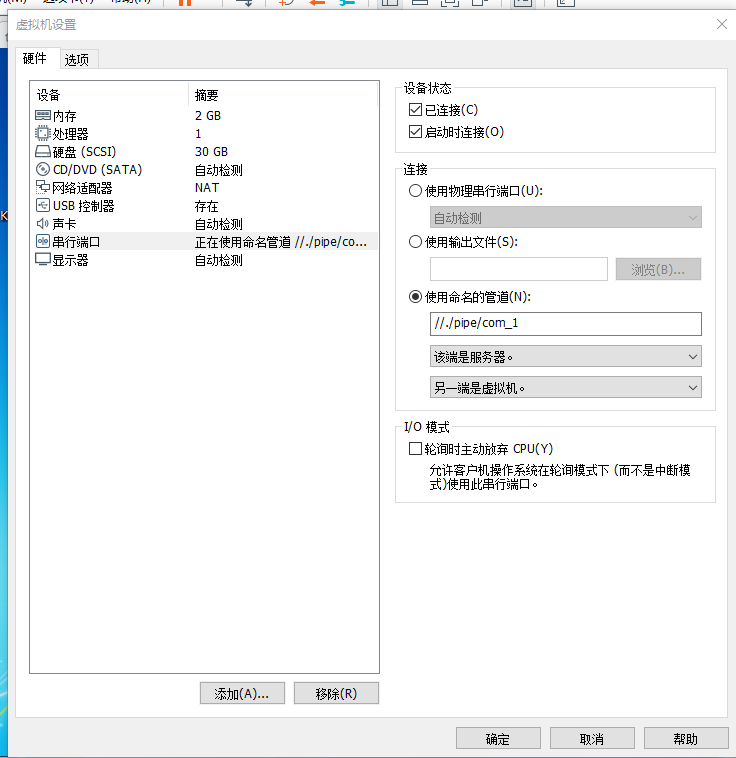
环境变量配置

这个不建议弄，会导致vs调试的时候自动下符号，卡的一笔

\_NT\_SYMBOL\_PATH

SRV\*E:\symbol\* <https://msdl.microsoft.com/download/symbols>

虚拟机设置里面如图所示，主要的注意点就是把打印机删掉



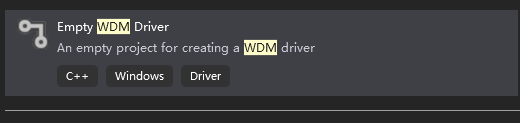
# 虚拟机里需要装一个vs2010

其实版本不重要，就是写R3程序操作段寄存器，做实验用的。

# 驱动开发环境

装VS2019，装WDK，注意WDK版本需和SDK一致。装WDK最后一步要勾选添加到VS插件。

创建驱动项目，



选这个空WDM项目，创建完把inf文件删掉，添加一个c文件

#include <ntifs.h>

VOID DriverUnload(PDRIVER\_OBJECT pDriver)

{

DbgPrintEx(77, 0, "111111111111111111");

}

NTSTATUS DriverEntry(PDRIVER\_OBJECT pDriver, PUNICODE\_STRING pReg)

{

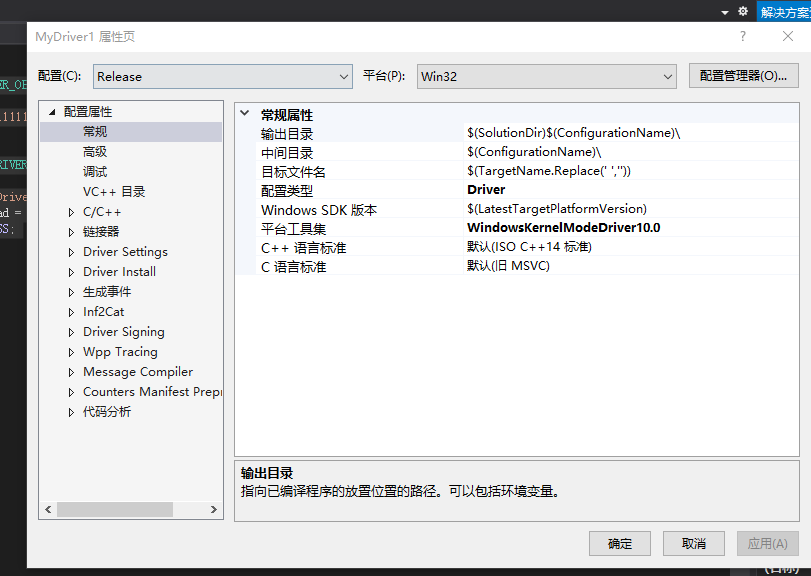
DbgPrintEx(77, 0, "DriverEntry");

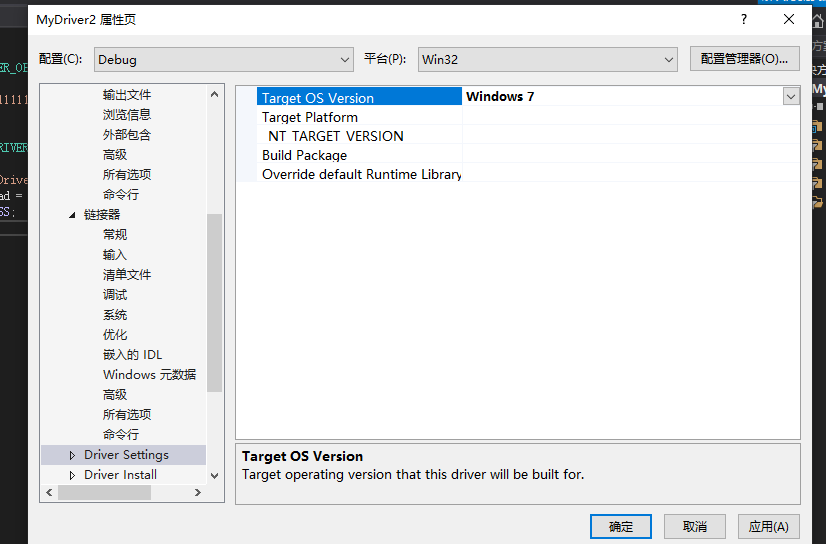
pDriver->DriverUnload = DriverUnload;

return STATUS\_SUCCESS;

}

项目设置如图





没啥特别的，把警告当成错误关掉，目标平台WIN7，就没啥了。

WIN7 32位不需要签名，编译成功的驱动拿到虚拟机，用KMD工具加载一下，DBGVIEW可以看输出，用DBGVIEW之前记得设置双机调试环境，不然看不到输出，

