内核简介

MSDN文档：https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/_kernel/

运行模式

在x86下，一般有三种运行模式：

1. 实模式
2. 保护模式
    - 多任务
    - 内存管理：任务内存、虚拟内存
    - 硬件保护
3. 虚拟8086模式
    - 兼容16位程序

权限

权限一般有4层：

- Ring0、Ring1、Ring2为内核态，可操作硬件
- Ring3为用户态，普通应用程序

驱动程序

让其成为操作系统的一个模块，由操作系统来加载：

1. 硬件驱动
2. 内核驱动

双机调试环境配置

参考：https://bianchengnan.gitee.io/articles/vmware-virtualkd-windbg-win10-kernel-debug-setup-step-by-step/

编写第一个驱动程序

入口函数：`DriverEntry`，包含头文件`Ntddk.h`

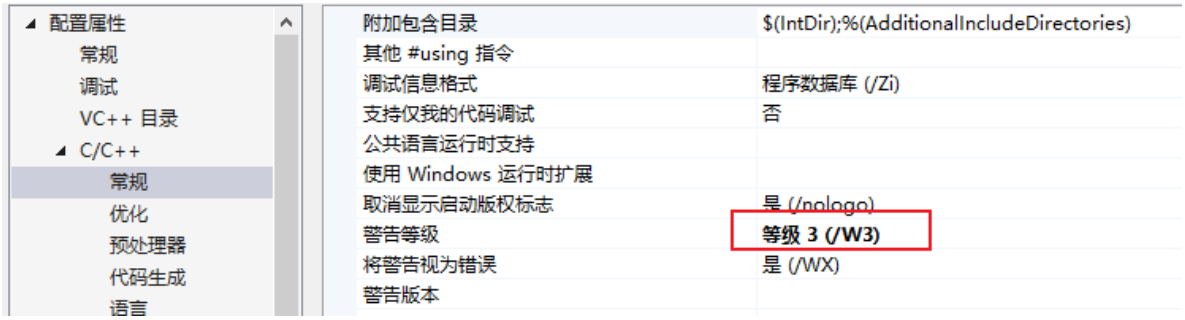
卸载函数：`DriverUnload`

```
#include <Ntddk.h>
```

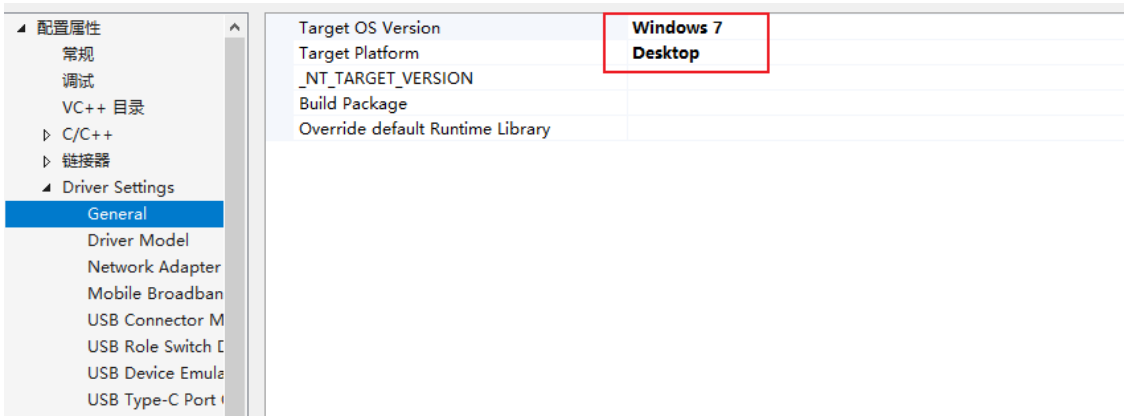
```
// 卸载驱动
DRIVER_UNLOAD DriverUnload;
void DriverUnload(struct _DRIVER_OBJECT* DriverObject)
{
    DbgPrint("Hello Kernel! - UnInstall");
}


DRIVER_INITIALIZE DriverEntry;  // 声明入口函数

// 入口函数
_Use_decl_annotations_
NTSTATUS
DriverEntry(struct _DRIVER_OBJECT* DriverObject, PUNICODE_STRING  RegistryPath)
{
    DbgPrint("Hello Kernel! - Install");

    // 注册卸载函数
    DriverObject->DriverUnload = DriverUnload;

    return STATUS_SUCCESS;  // 按约定，成功返回STATUS_SUCCESS
}
```

vs中项目需要设置的地方：

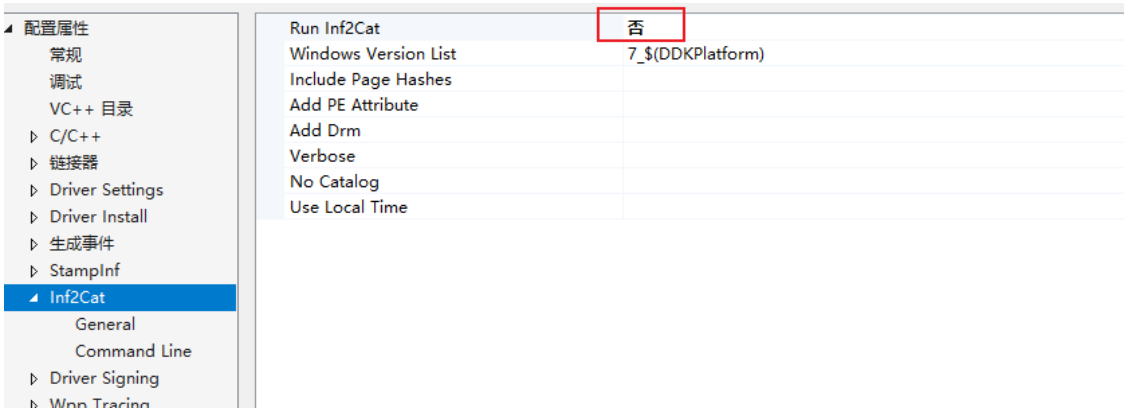
1. 修改警告等级为3



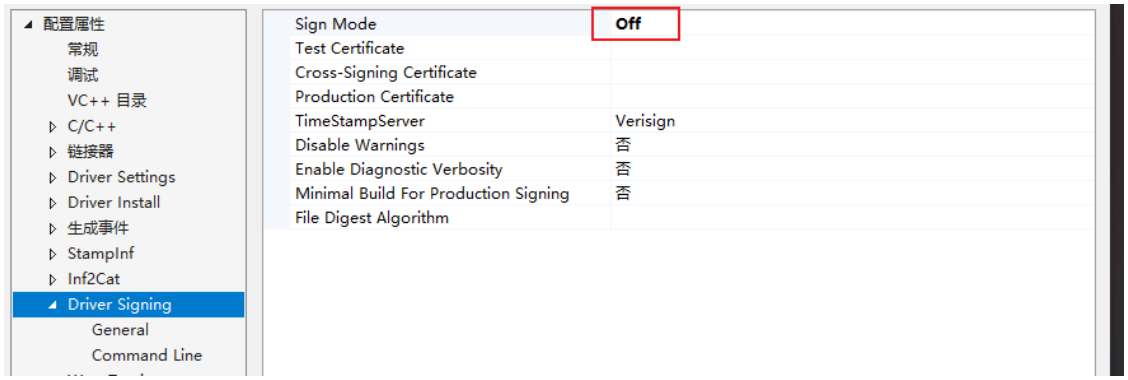
2. 修改平台



3. 不执行Inf2Cat


配置属性
常规
调试
VC++ 目录
C/C++
链接器
Driver Settings
Driver Install
生成事件
StampInf
Inf2Cat
General
Command Line
Driver Signing
Run Inf2Cat
否
Windows Version List
7_$(DDKPlatform)
Include Page Hashes
Add PE Attribute
Add Drm
Verbose
No Catalog
Use Local Time

4. 关闭驱动签名


配置属性
常规
调试
VC++ 目录
C/C++
链接器
Driver Settings
Driver Install
生成事件
StampInf
Inf2Cat
Driver Signing
General
Command Line
Sign Mode
Off
Test Certificate
Cross-Signing Certificate
Production Certificate
TimeStampServer
Verisign
Disable Warnings
否
Enable Diagnostic Verbosity
否
Minimal Build For Production Signing
否
File Digest Algorithm