Andy Hu

佳友终端 | 广州.中国

Windows系统管理的20个技巧

**Effective Windows System Management**

你所不知道的Windows系统管理秘密

简单.高效

目录

[前言 2](#_Toc91499925)

[为什么要做这本电子书？ 2](#_Toc91499926)

[希望达到的目的 2](#_Toc91499927)

[文件操作 3](#_Toc91499928)

[文件备份 3](#_Toc91499929)

[备份的策略 3](#_Toc91499930)

[本地备份工具 4](#_Toc91499931)

[Fast Copy 4](#_Toc91499932)

[Robocopy 5](#_Toc91499933)

[文件搜索工具 6](#_Toc91499934)

[Everythings介绍 6](#_Toc91499935)

[文件字符搜索 8](#_Toc91499936)

[AstroGrep文本搜索 8](#_Toc91499937)

[文件相关的几个命令 8](#_Toc91499938)

[Where命令 8](#_Toc91499939)

[Forfiles 命令 9](#_Toc91499940)

[Curl命令 11](#_Toc91499941)

[Setx 命令 11](#_Toc91499942)

[安全工具 12](#_Toc91499943)

[Sysinternal工具集 12](#_Toc91499944)

[AutoRuns 12](#_Toc91499945)

[Sysmon 12](#_Toc91499946)

[Psping命令 15](#_Toc91499947)

[自动化 15](#_Toc91499948)

[机器人 16](#_Toc91499949)

[脚本语言 16](#_Toc91499950)

[BAT 16](#_Toc91499951)

[VBS 16](#_Toc91499952)

[PowerShell 16](#_Toc91499953)

[开发工具 18](#_Toc91499954)

[Windows WSL介绍 18](#_Toc91499955)

[Visual Studio Code 18](#_Toc91499956)

[Ubuntu for Windows 介绍 18](#_Toc91499957)

[集成环境，WSL + Ubuntu + code 18](#_Toc91499958)

[Zeal API文档管理工具 18](#_Toc91499959)

[知识库管理 19](#_Toc91499960)

[OneNote 19](#_Toc91499961)

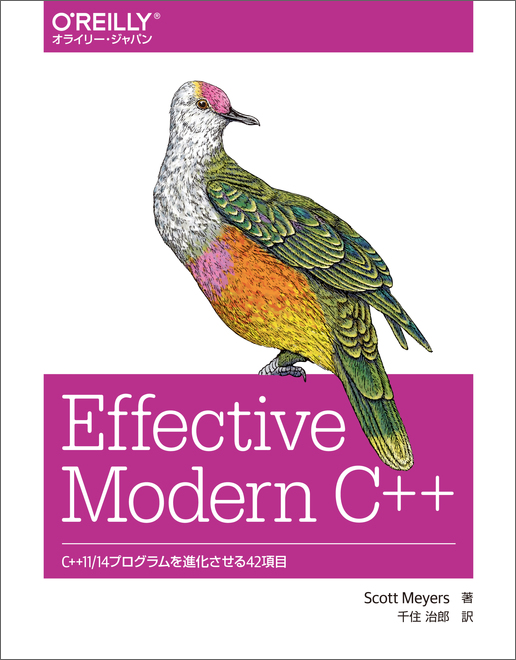
[Microsoft To-do 19](#_Toc91499962)

# 前言

## 为什么要做这本电子书？

说起Windows的管理，可能每个人的第一印象就是大家都懂，但是是否高效就是另外一个问题了。和Linux比起来，windows多了一个图形界面，图形界面这种点击操作，并不是不好，只是让我们会做很多重复的工作，导致我们的工作都是重复劳动，无法提升效率。而这里，我要给大家介绍的是完全脱离了鼠标。使用命令行的方式来管理，通过命令行管理的好处就是在云环境的情况下，可以更加高效，管理大量的管理大量的Windows系统。在日常中，工作的脚本是可以复用的，可以高效的部署，快速的解决问题。比起人工的重复劳动，工作效率至少要高十倍以上。

这边书的名称来源：



## 希望达到的目的

能提高日常工作效率，更加高效的工作和生活。

# 文件操作

## 文件备份

文件=资产

文件=信息安全

电脑总是在你最忙的时候奔溃！

世界上不存在永远不会坏的部件。

### 备份的策略

#### 大文件与小文件

大文件没有策略，随便copy / paste

成千上万的小文件备份比较麻烦，主要表现为：

1. copy时间长;
2. 失败，需要重试;
3. 需要人盯着看，浪费时间；

#### 备份介质(SSD ,机械盘,网络)

机械盘：冷数据，适合用于归档，价钱便宜,容量大。

SSD：适合高速写入，拼速度的场景，即插即用，立即插拔。

百度云盘：（照片）

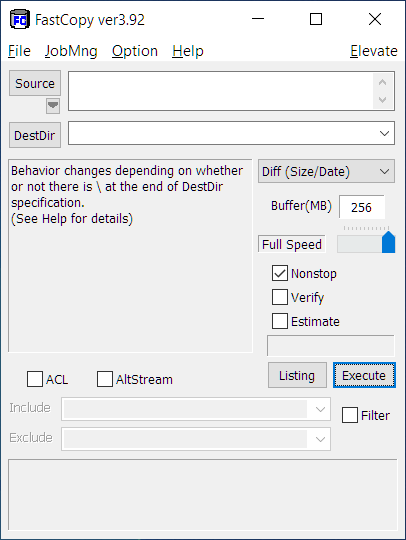
阿里云简单对象存储OSS（分发、共享）

三星移动硬盘SSD T5 500GB（最快的方式）

Apple 产品 ： iCloud 500 GB （家庭共享）

### 本地备份工具

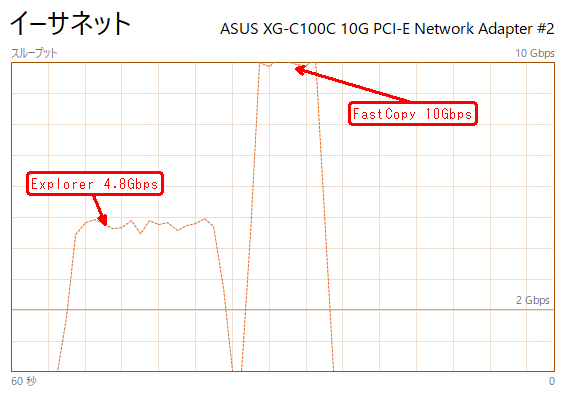
### Fast Copy



<https://fastcopy.jp/img/fastcopy_vs_explorer3.png>

性能：

Fast copy和windows资源管理器性能对比：



### Robocopy

特色：

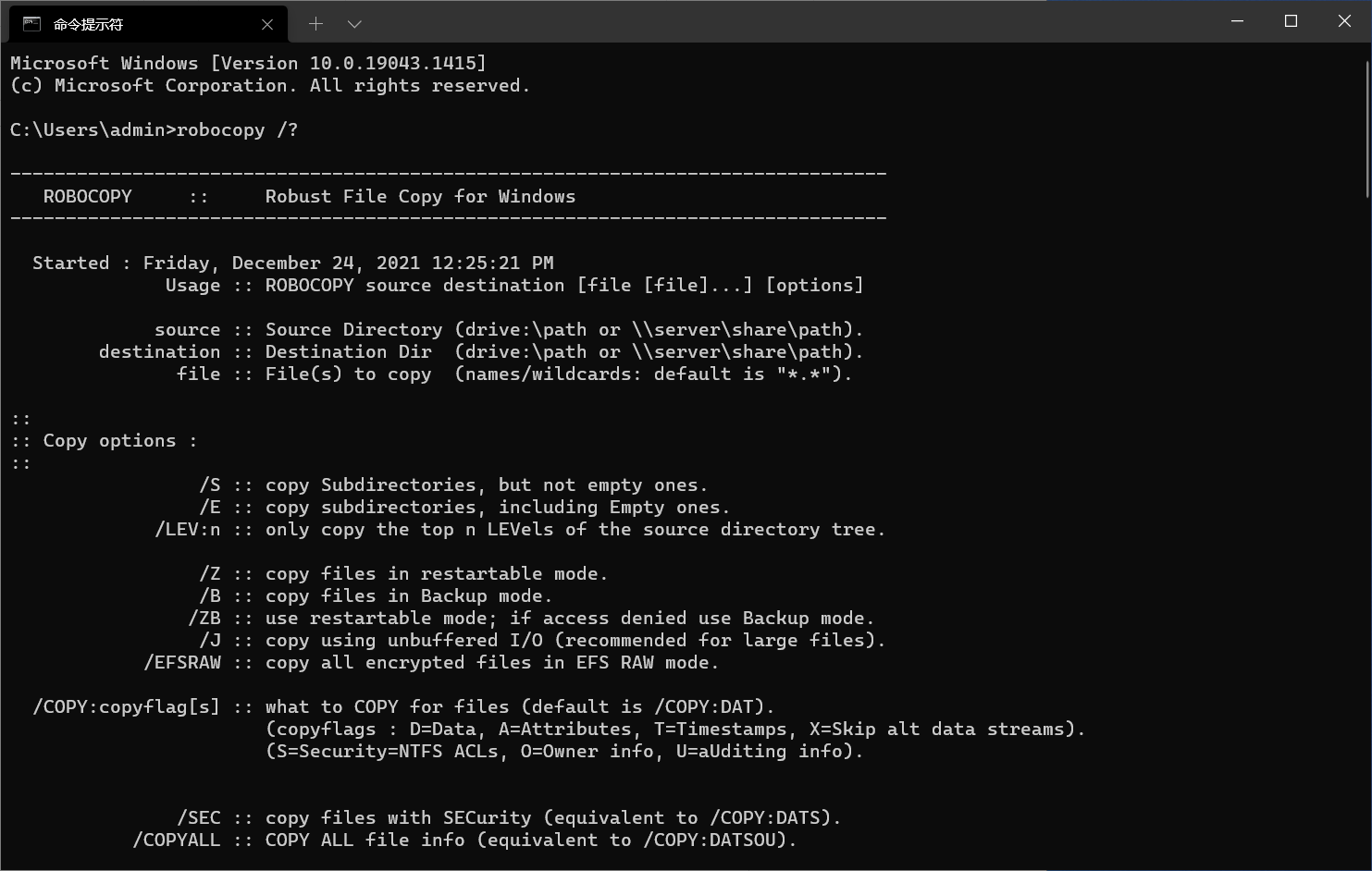
全名：(Robust File Copy for Windows)

Windows系统自带

命令行工具，功能强大

不需要记住所有的，常用的就两个 /S /E 就可以了，/XF 是排除文件，/XD是排除目录

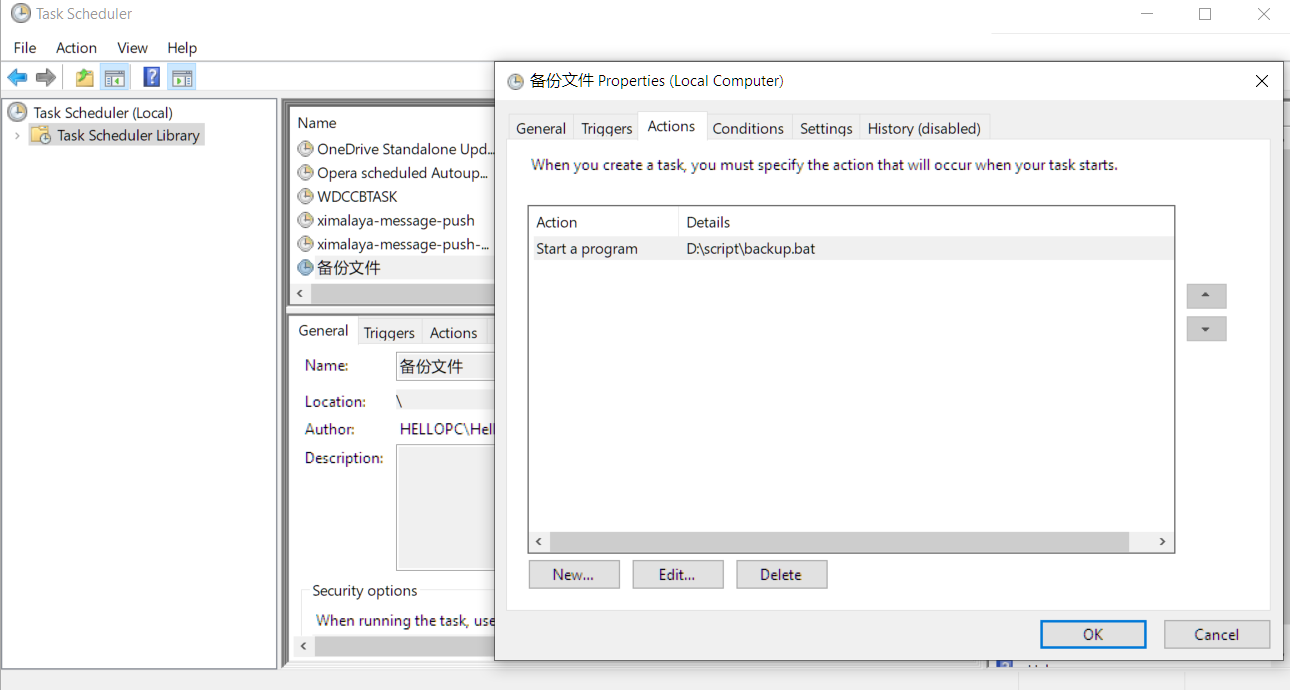
更复杂的需要自己查询 robocopy /? 查询；



可以和计划任务配合的很好

比如定时的备份文件。

robocopy d:\doc \\192.168.1.0\share /MIR



## 文件搜索工具

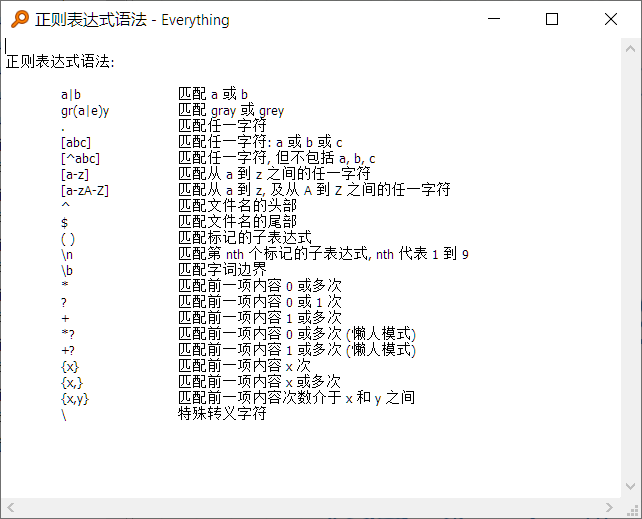
### Everythings介绍

*"Everything" 是什么？*

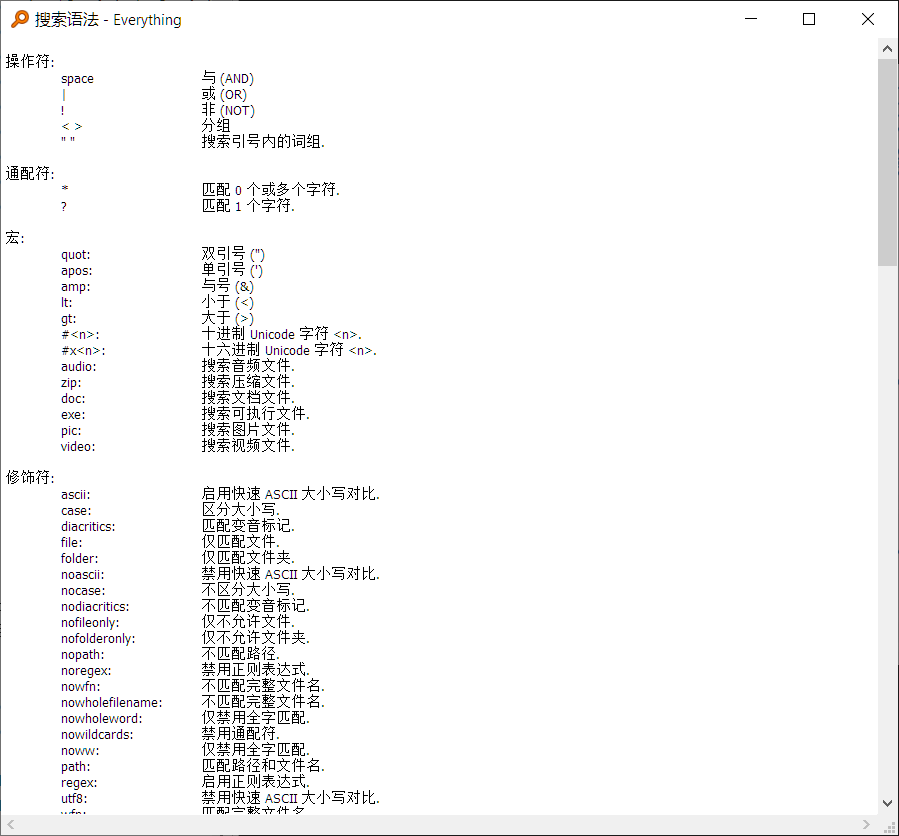
*"Everything" 是 Windows 上一款搜索引擎，它能够基于文件名快速定文件和文件夹位置。*

*不像 Windows 内置搜索，"Everything" 默认显示电脑上每个文件和文件夹 (就如其名 "Everything")。*

正则表达式



搜索语法：

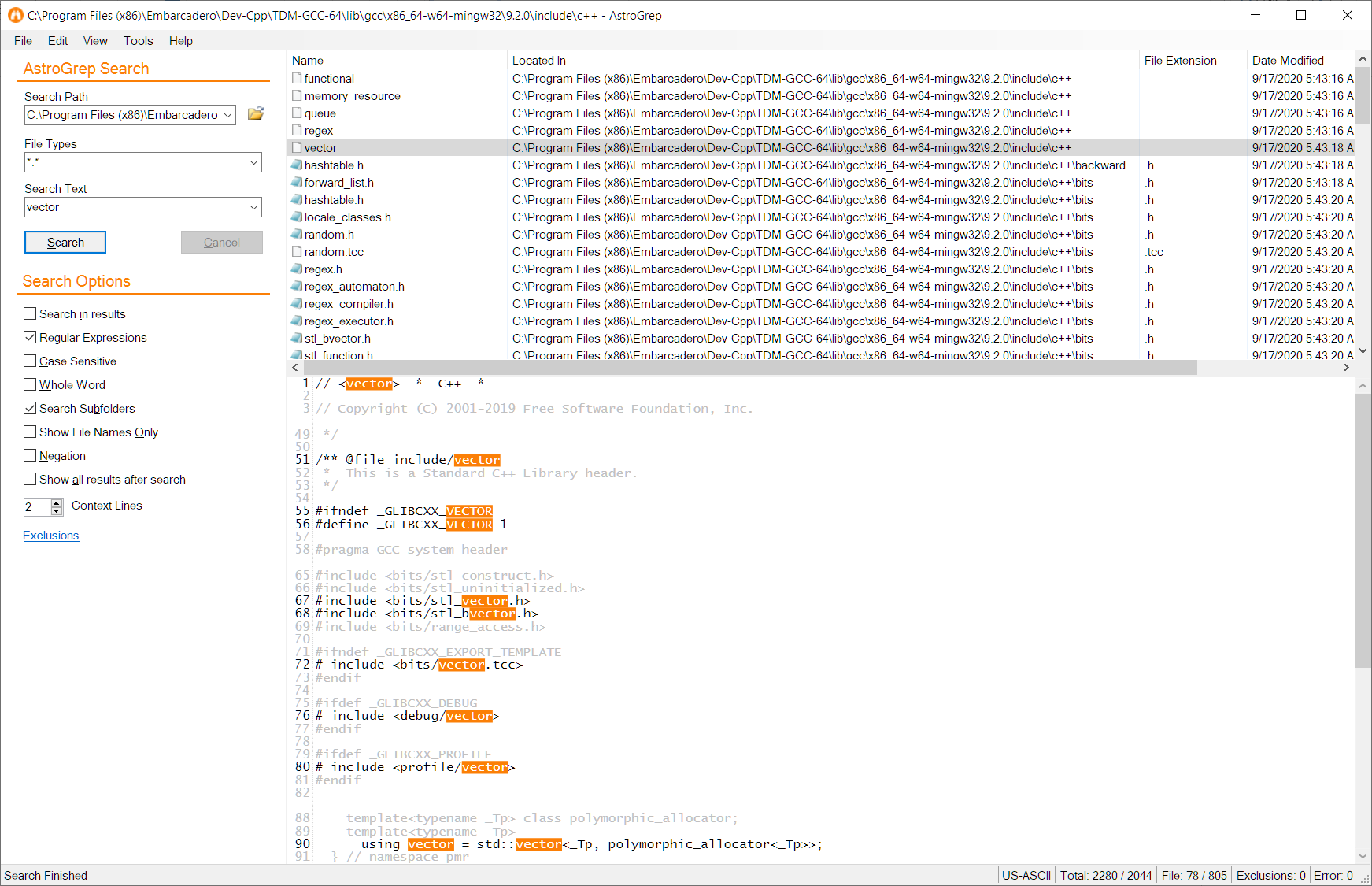


## 文件字符搜索

### AstroGrep文本搜索

代码搜索，相当于Linux下面的命令行工具，Grep

比如搜索某一个函数或者类：



## 文件相关的几个命令

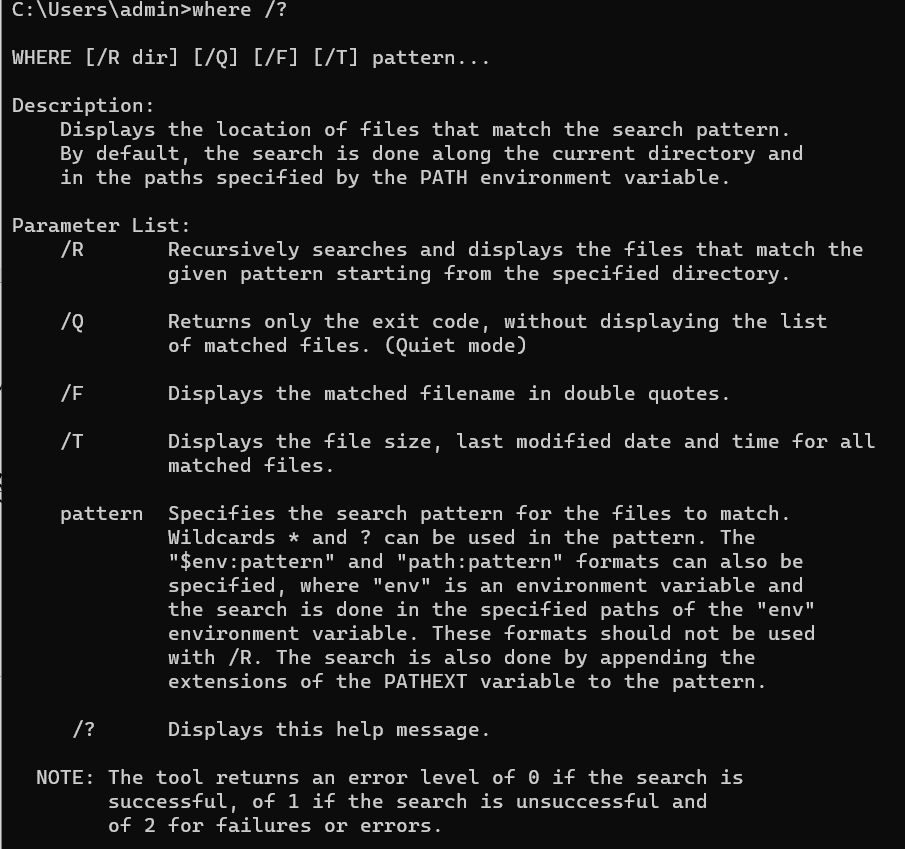
### Where命令

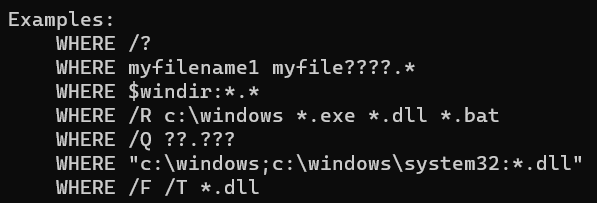
**Description:**

Displays the location of files that match the search pattern.

By default, the search is done along the current directory and

in the paths specified by the PATH environment variable.



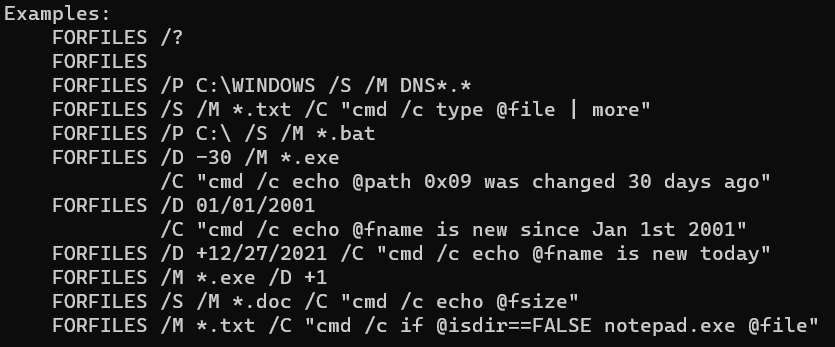


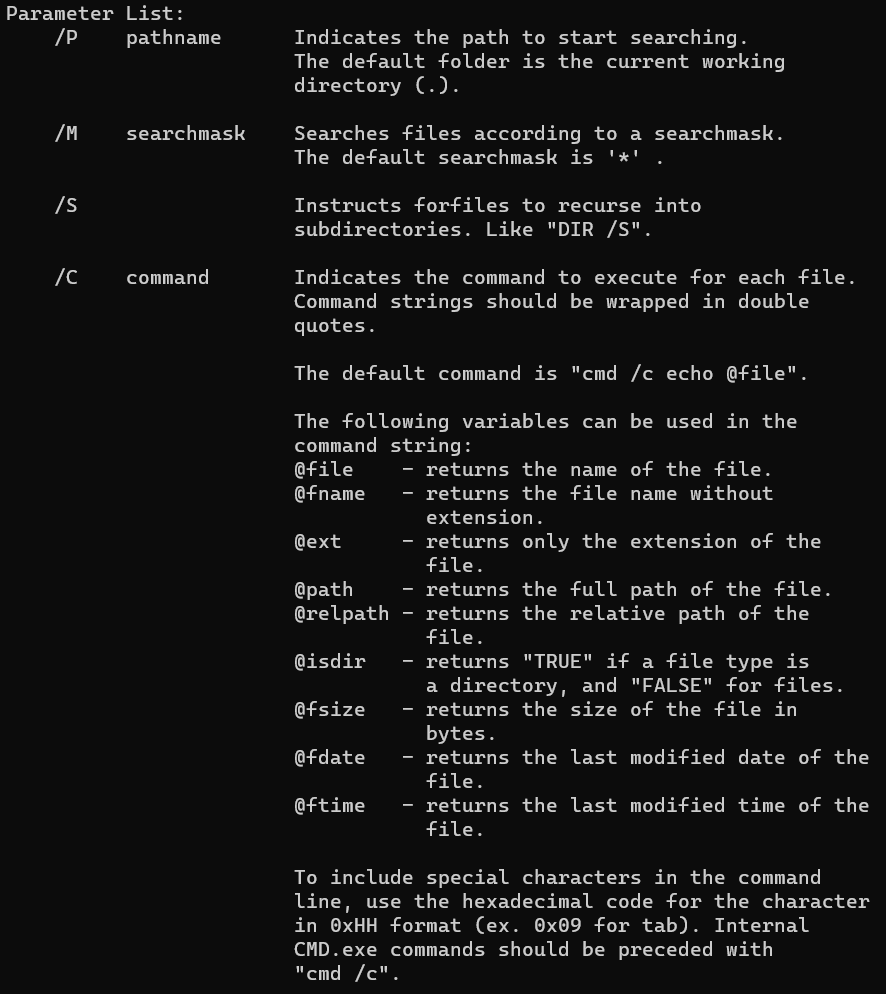
### Forfiles 命令

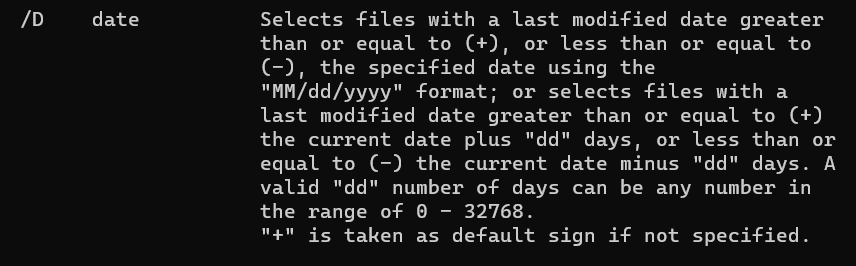
**Description:**

Selects a file (or set of files) and executes a

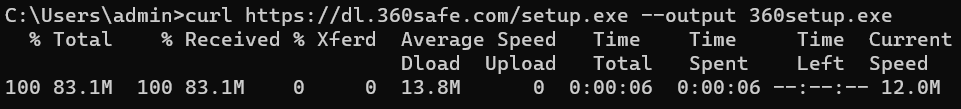
command on that file. This is helpful for batch jobs.







### Curl命令



最简单的用法是用来下载文件

Windows 1803后才加入.

### Setx 命令

NOTE: 1) SETX writes variables to the master environment in the registry.

2) On a local system, variables created or modified by this tool

will be available in future command windows but not in the

current CMD.exe command window.

Set命令的问题是下次启动后,设置的变量就消失了.

Setx 可以将环境变量写入注册表;

# 安全工具

## Sysinternal工具集

## AutoRuns

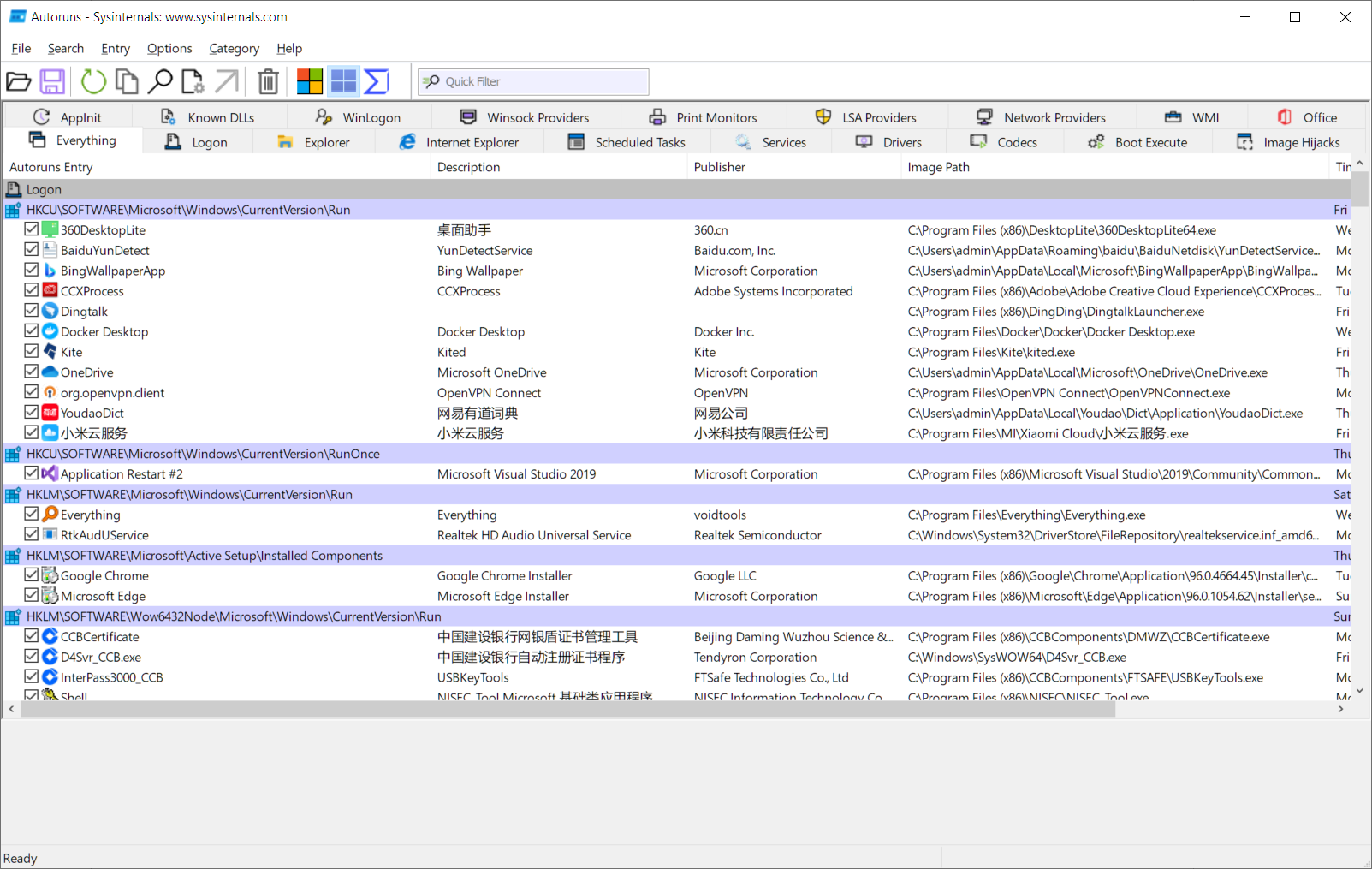
作用：

1 快速获取系统中所有的启动选项，有GUI版本和console版；

2 可以导出到csv文件；

3 结合阿里云日志服务，可以将终端的日志上传到云服务器，来进行存储、分析、和集中展示；

截图：



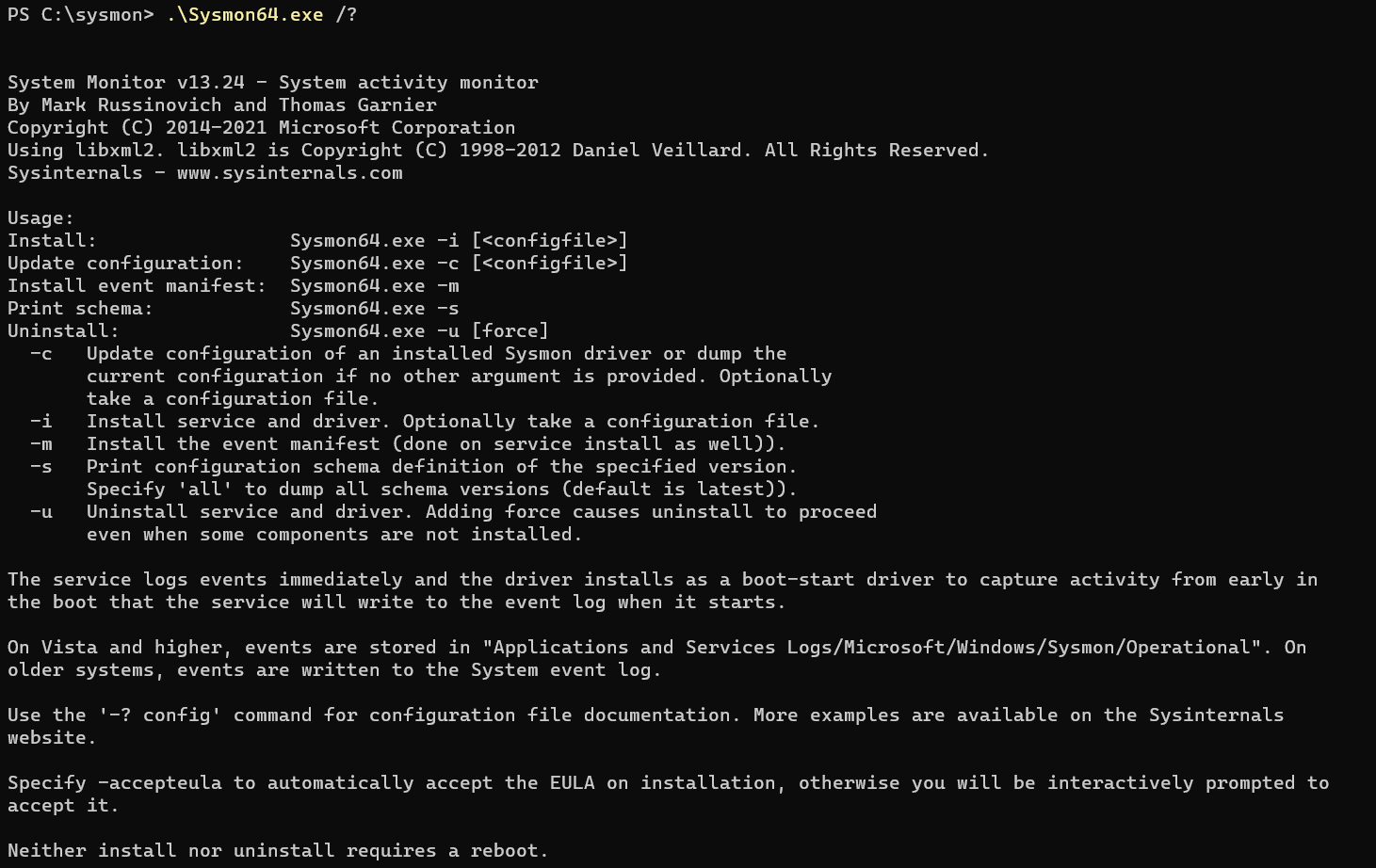
## Sysmon

作用：

System Monitor (Sysmon)是一个Windows系统服务和设备驱动程序，一旦安装在系统上，它将在系统重启期间驻留，以监视系统活动并将其记录到Windows事件日志中。

可以看作一个日志收集器或者一个SIEM平台的前端收集器；

截图：



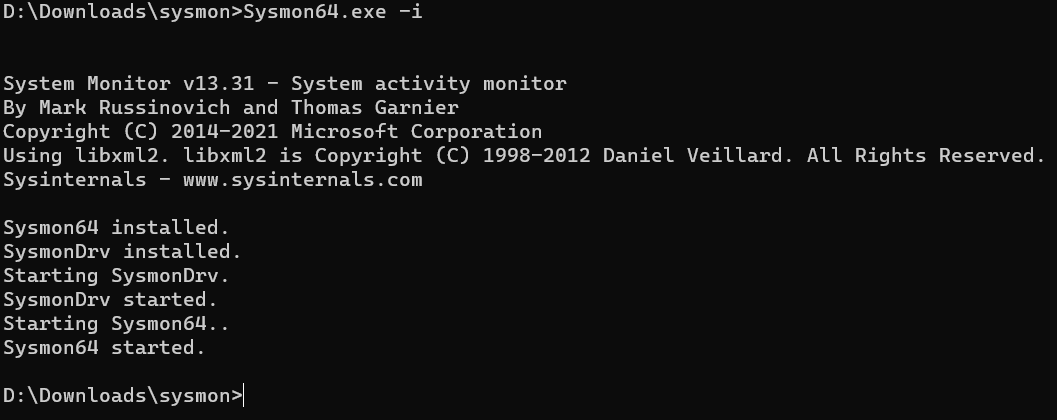
Note: 安装和部署都非常简单，但偶尔会导致系统蓝屏。

可以配合阿里云日志服务系统，使用windows Agent将Sysmon采集到的日志，发送到云服务器集中存储，分析和展示，构建成一个简单的SIEM平台，对小微企业来说，完全够用。

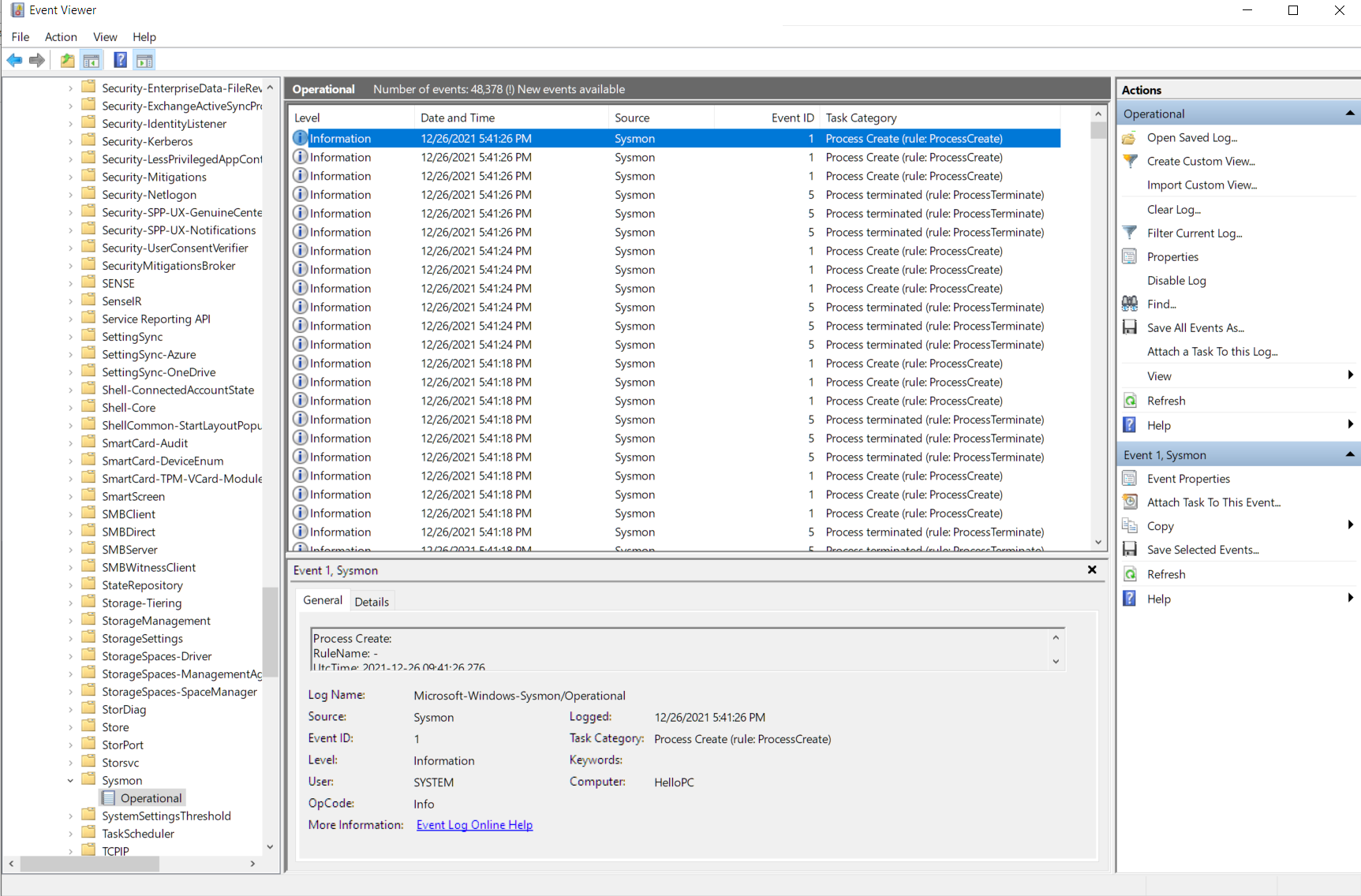
安装需要管理员权限：



安装过程：

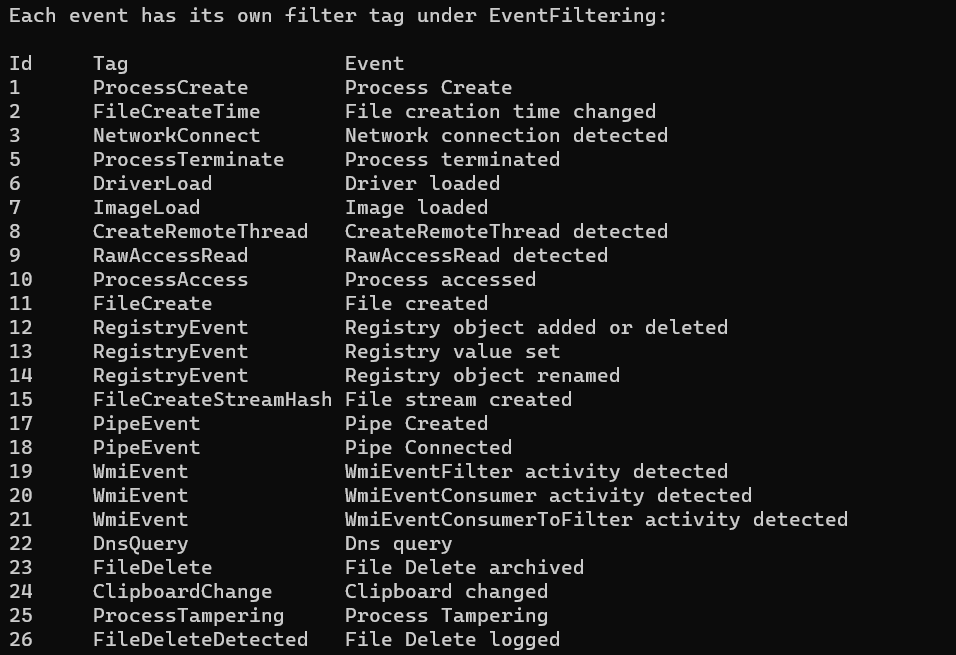


查看生成的日志：



Sysmon的配置文件，可以 通过命令：sysmon -? config查看帮助信息，或者上github上搜索，上面于大量的案例。

支持的日志类别：



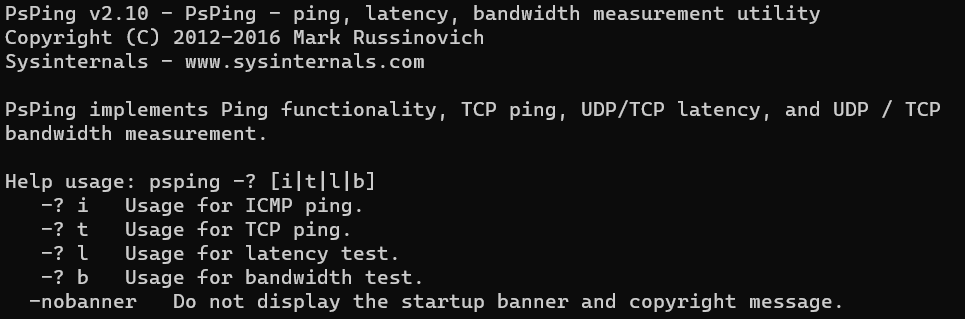
配置文件:



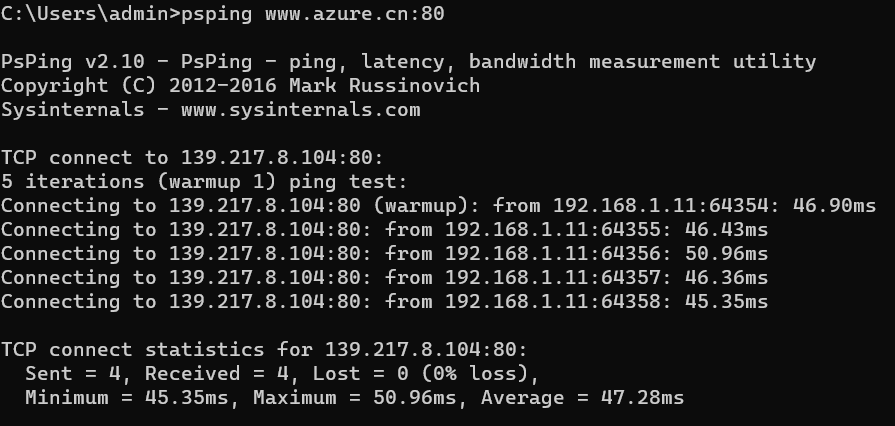
## Psping命令

作用:

使用TCP协议来测试目标地址的端口是否开放.



例如:



# 自动化

## 机器人

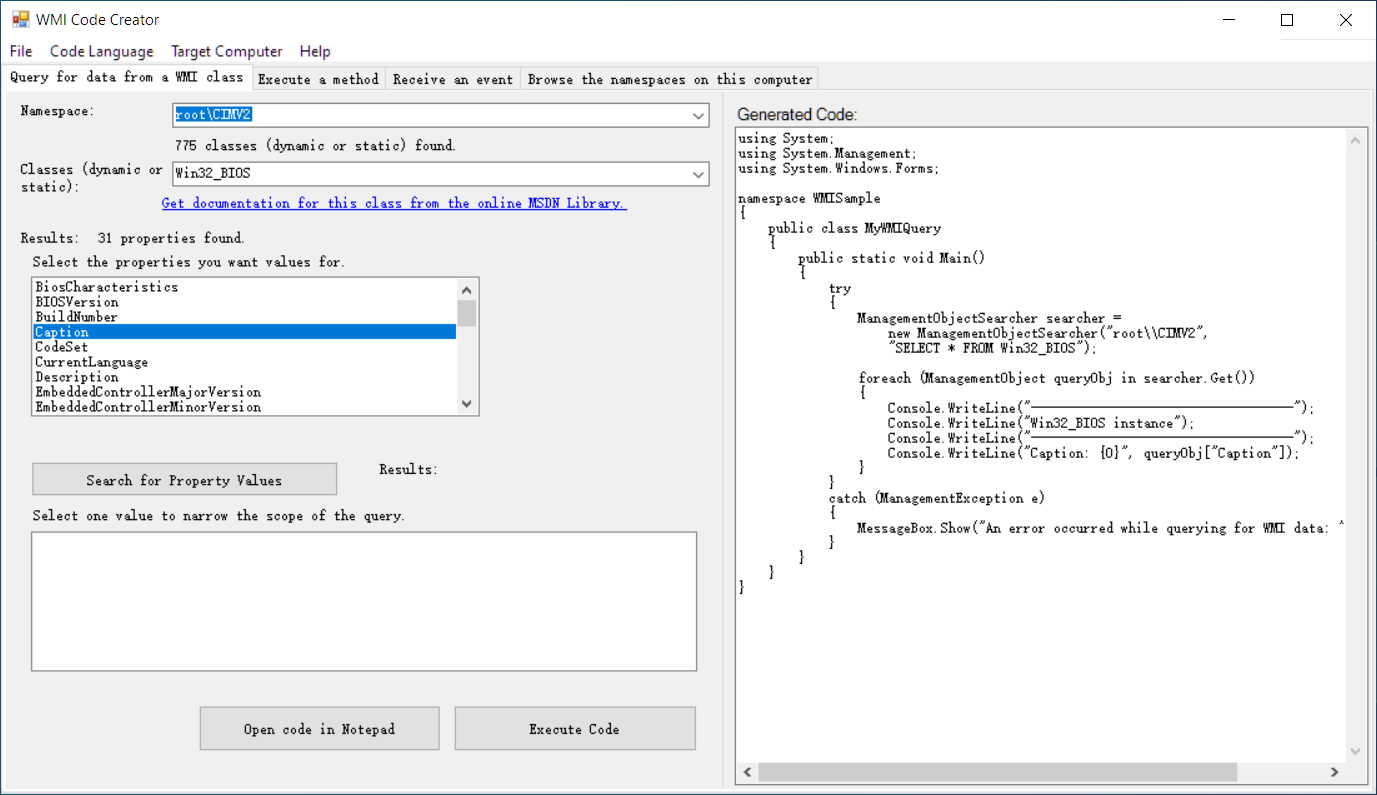
## 脚本语言

### BAT

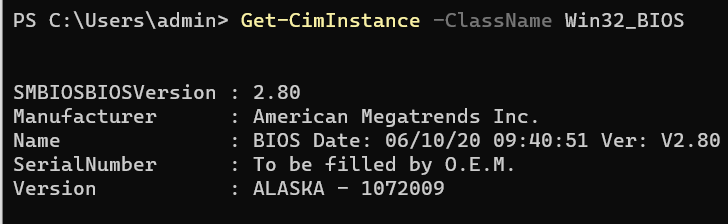
### VBS

有用的工具：

1. WMI namespace 下拉式选取；
2. 对应namespace 下二级Class选取；
3. 对应二级class属性的选取；
4. 一键生成代码，比如vbs, c# 或者VB



### PowerShell



通过PWSH的Get-CimInstance -ClassName 按TAB,也可以补齐默认namespace 下面的class.

# 开发工具

## Windows WSL介绍



## Visual Studio Code

## Ubuntu for Windows 介绍

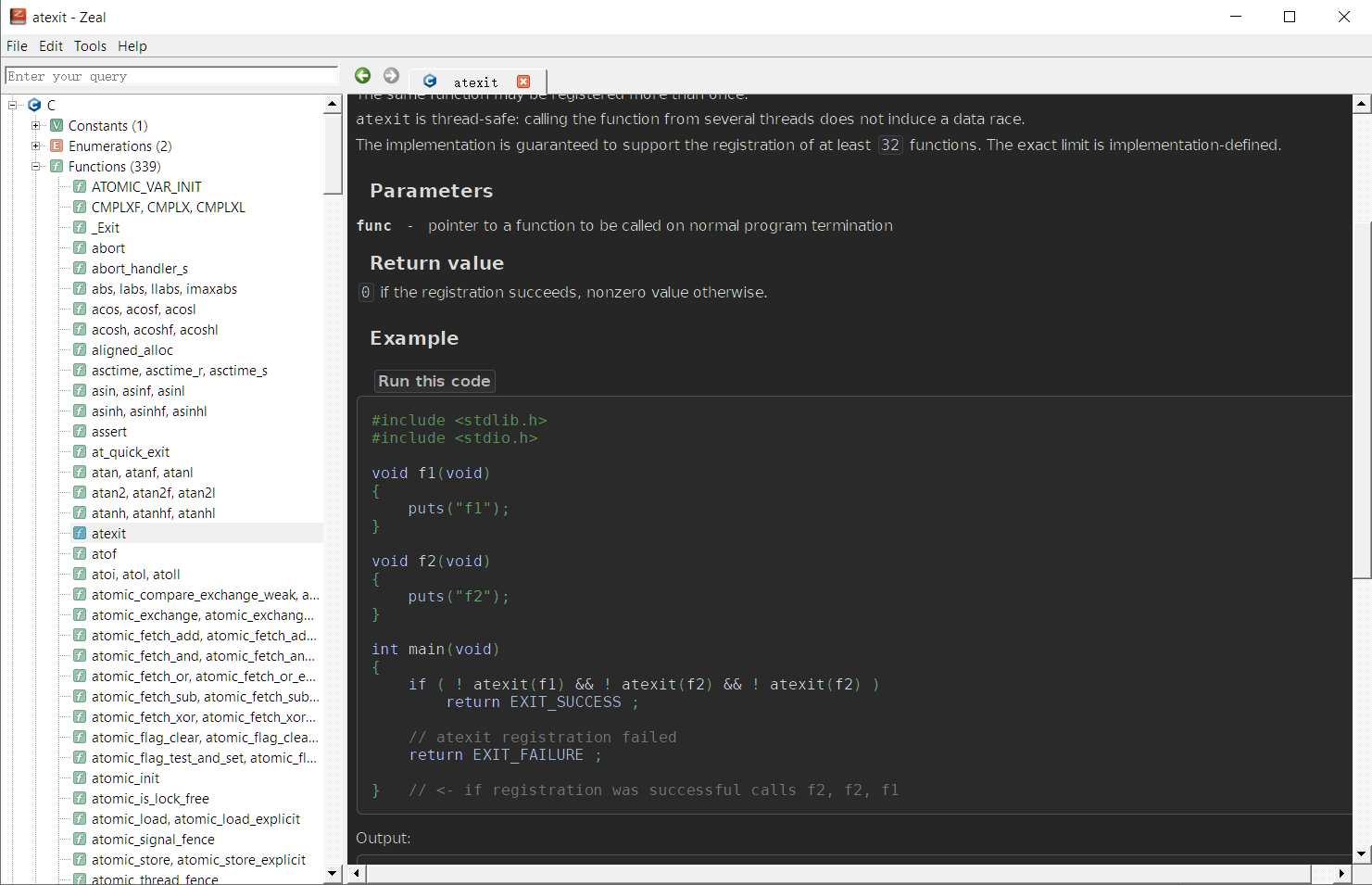
## 集成环境，WSL + Ubuntu + code

## Zeal API文档管理工具

介绍：

Zeal is an offline documentation browser for software developers.

截图：



离线的API文档参考工具，我主要是用来管理C、C++ 、Rust

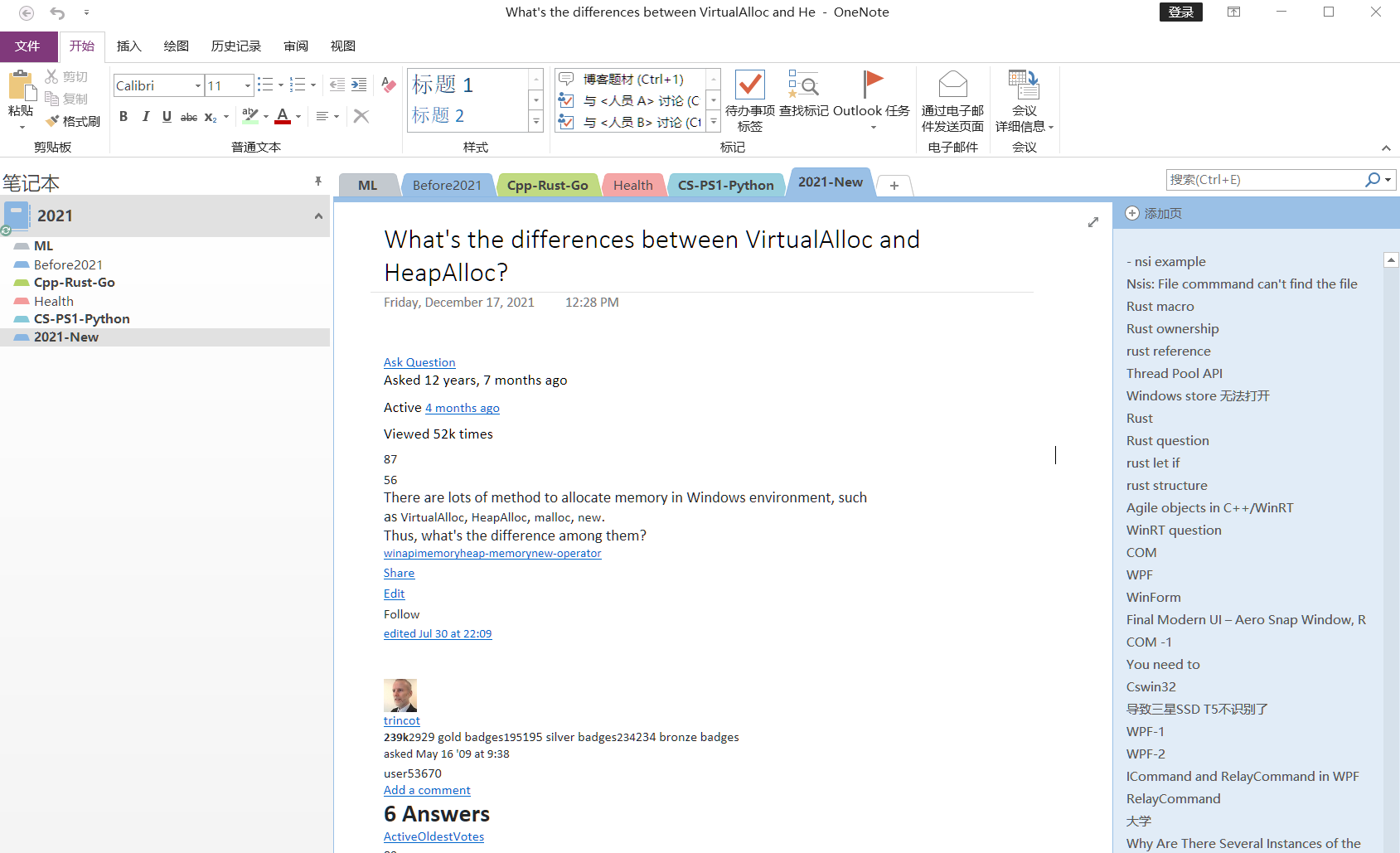
能管理的API文档比较多，不建议拿来管理JAVA的API，JAVA的API太庞大了，经常会把工具搞闪退掉。



# 知识库管理

## OneNote

我们在工作中会遇到一些问题。在我们修复问题的过程中，怎么会查找一些资料？那么怎样快速的去找到一些我们想要的资料呢？当然是通过搜索引擎。虽然收入引擎，我们可以在海量的数据中快速的找到我们想要的数据。同理，KIE，Knowlege is everything, 我们的知识需要存储和整理，以及快速查询。那么使用one note这个工具。能够帮我们快速的管理我们的知识。当我们面对同样的问题时，我们可以迅速的找到解决方案。这样就快速的提高了我们的效率。通过日积月累的积累，我们的知识库会越来越大，解决问题的能力也会越来越高。这样，我们的价值就会越来越高。其他的类似one note的知识管理软件还有很多。大家也不一定要使用one note。只是one note和微软的office软件集成度比较高。虽然手机和iPad也同样可以管理。所以这是一个大家值得尝试的技巧。



## Microsoft To-do