Windows 系统操作手册 1.2

说明：

1.本文档没有目录，本文档在发布时为 pdf 文档，有章节书签，可以下载到本地来查看，点击书签进入相应的章节。

2.蓝色的字为配置命令，绿色的字为命令的注释，有时命令太密集时，就不用蓝色标出了。

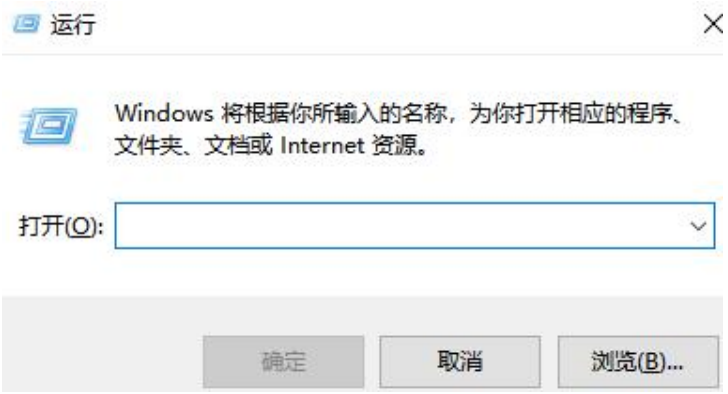
3.注意：本文档的所有操作请先在在虚拟机里进行实践，请不要直接在真实的服务器中操作！

作者：李茂福

日期：2019 年 12 月 27 日

快捷命令及快捷键

快捷命令是在运行栏里输入的命令，按下 Win 键和 R 键打开运行栏



输入命令后，回车即可打开相应的功能界面

命令	打开功能	说明	路径
ncpa.cpl	网络连接	能看见网卡图标	控制面板\网络和 Internet\网络连接
firewall.cpl	防火墙	配置 windows 防火墙	控制面板\系统和安全\Windows Defender 防火墙
sysdm.cpl	系统属性	计算机名，硬件，高级，远程等	控制面板\系统和安全\系统\更改设置
collab.cpl	网络邻居		
telephon.cpl	电话和调制解调器		
inetcpl.cpl	Internet 属性	常规，安全，隐私	
appwiz.cpl	卸载或更改程序	启用或关闭某功能	控制面板\程序\程序和功能
devmgmt.msc	设备管理器		控制面板\系统和安全\系统\设备管理器
gpedit.msc	本地组策略编辑器		
lusrmgr.msc	本地用户和组(本		

	地)		
compmgmt.msc	计算机管理		
taskschd.msc	任务计划程序		
services.msc	服务		
secpol.msc	本地安全策略		
diskmgmt.msc	磁盘管理		
hdwwiz	添加硬件向导		
certmgr.msc	证书管理		
eventvwr.msc	事件查看器		
taskmgr	任务管理器	Ctrl+Alt+Del	
msinfo32	系统信息	硬件资源，组件，软件环境	
msconfig	系统配置	常规，引导，服务，启动	
regedit	注册表编辑器		
mstsc	远程桌面连接		
explorer	资源管理器	Win+E	
osk	屏幕键盘		
magnify	放大镜		
dcomcnfg	组件服务		
calc	计算器		
write	打开“写字板”		
snippingtool	打开“截图”		
SoundRecorder.exe	打开“录音机”		
winver	查看系统版本		
control	控制面板		
control system	系统	查看有关计算机的基本信息	Win+Pause

快捷键

快捷键（组合键）	功能	快捷键（组合键）	功能
Win + D	回到桌面	Win + E	打开资源管理器
Win + R	打开“运行栏”	Win + K	投屏
Win + L	锁定屏幕	Win + P	投屏
Win + Tab	切换窗口	Win + 空格	切换输入法
Alt + F4	关闭当前窗口	F2	重命名
Ctrl + Shift + T	打开上一次关闭的网页	Ctrl + ←→箭头键	向左/右跳过一个单词
Ctrl + Alt +上下左右箭头	切换屏幕显示方向	Ctrl + C	复制
Ctrl + V	粘贴	Ctrl + X	剪切
Ctrl + Z	撤销		

网络诊断工具

①Ping

>ping　目的 IP　-n 次数　-l 大小　-w 超时　-S 源 IP　　//超时为毫秒

```
C:\Users\Administrator>ping 8.8.8.8 -n 3 -l 140 -w 500 -S 192.168.0.118

正在 Ping 8.8.8.8 从 192.168.0.118 具有 140 字节的数据:
来自 8.8.8.8 的回复: 字节=68 (已发送 140) 时间=20ms TTL=53
请求超时。
来自 8.8.8.8 的回复: 字节=68 (已发送 140) 时间=20ms TTL=53
```

②Tracert

>tracert　-d　-h 跃点数　-w 超时　目标 IP

③IPconfig

```
>ipconfig　/all                    //查看所有网卡配置情况
>ipconfig　/displaydns             //查看缓存的 DNS 解析
>ipconfig　/flushdns               //清空 DNS 解析缓存
>ipconfig　/renew　网卡名          //重新获取 dhcp 分配的地址
>ipconfig　/release　网卡名        //释放 dhcp 分配的地址
>ipconfig　/registerdns            //向 dns 服务器注册本地 ip
```

④nslookup

```
>nslookup　xxx.com                          //获取域名的 IP 地址
>nslookup　-qt=查询类型　xxx.com            //获取域名的指定记录值
```

⑤>route　print　-4　　//查看 IPv4 路由信息

⑥>nbtstat　-a　目标 IP　　//查看目标 IP 的 NetBios 信息

⑦

```
>arp　-a                  //查看 arp 表
>arp　-s　10.1.1.1　xx-xx-xx-xx-xx-xx　　//添加静态 arp 项
>arp　-d　10.1.1.1                        //删除静态 arp 项
```

⑧netstat

```
>netstat　-a                //查看所有套接字连接
          -n                //以数字形式显示地址和端口号
          -o                //显示每个连接对应的进程 ID
          -p　tcp 或 udp　　//只查看 tcp 或 udp 的连接
```

网卡操作

①添加虚拟网卡

>hdwwiz 打开“添加硬件向导”→安装我手动从列表选择的硬件→网络适配器

选择网卡类型

VMware 的在“编辑”→虚拟网络编辑器→添加虚拟网卡

②删除网卡

>devmgmt.msc 打开设备管理器→网络适配器→选中目标网卡→右击“卸载”

③CMD 命令行里配置 IP 网关

以管理员身份运行 cmd

>netsh interface ip add address "网卡名" 10.1.1.1 255.255.255.0 10.1.1.254

>netsh interface ip delete address "网卡名" 10.1.1.1 [gateway=10.1.1.254]

删除时若不写上 gateway，则网关（默认路由）仍存在

路由操作

以管理员身份运行 cmd

>route　print　[-4]　　//查看路由表

```
C:\Users\Administrator>route print -4
===========================================================================
接口列表
 15...0c 9d 92 0e 45 39 ......Intel(R) Ethernet Connection (2) I219-V
 12...0a 00 27 00 00 0c ......VirtualBox Host-Only Ethernet Adapter
 21...02 00 4c 4f 4f 50 ......Npcap Loopback Adapter
 11...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0    192.168.0.1    192.168.0.118     25
         10.2.2.0    255.255.255.0         在链路上         10.2.2.1    291
         10.2.2.1  255.255.255.255         在链路上         10.2.2.1    291
       10.2.2.255  255.255.255.255         在链路上         10.2.2.1    291
        127.0.0.0        255.0.0.0         在链路上        127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上        127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上        127.0.0.1    331
      169.254.0.0        255.255.0.0         在链路上    169.254.68.194    281
   169.254.68.194  255.255.255.255         在链路上    169.254.68.194    281
  169.254.255.255  255.255.255.255         在链路上    169.254.68.194    281
      192.168.0.0    255.255.255.0         在链路上     192.168.0.118    281
    192.168.0.118  255.255.255.255         在链路上     192.168.0.118    281
```

接口列表下的数字，如 15,12,21,11,1 是网卡的序号

网卡序号后的 0c 9d 92 0e 45 39 等数字是网卡的 mac 地址

最后一字段是网卡名称

路由器表最后一字段跃点数表示路由优先级，超小越优先

>route　delete　0.0.0.0　0.0.0.0　192.168.0.1　　//删除默认路由

>route　add　10.1.1.0　mask　255.255.255.0　192.168.1.254　　//添加静态路由

>route　add　目的网段　mask　子网掩码　下一跳 IP　metric　230　if　15

//指定优先级为 230，出口为 15 号网卡

>route　-p　add/delete ….　　// -p 表示永久生效，写入注册表中的

Wmic 查看计算机信息

```
>wmic   bios   get   Manufacturer,Name              //查看 Bios 版本型号
>wmic   bios   get   SerialNumber                  //查看 bios 序列号
>wmic   bios   get   ReleaseDate                   //查看 bios 出厂日期
>wmic   bios   get   version                       //查看 bios 版本，品牌
>wmic   bios   get   biosversion                   //查看 bios 版本，品牌

>wmic   computersystem   get   domain,name        //查看域，计算机名

>wmic   cpu   get   caption                        //查看 cpu 信息
>wmic   cpu   get   name                         //查看名称 Inter Core TM i5.8400 xxx@2.8Ghz
>wmic   cpu   get   numberofcores                  //查看 cpu 核心数
>wmic   cpu   get   datawidth                      //位宽

>wmic   desktopmonitor   get   screenwidth,screenheight      //查看屏幕分辨率

>wmic   diskdrive   get   caption,InterfaceType,Size        //硬盘型号，接口类型，容量（字节

>wmic   memphysical   get   maxcapacity            //查看支持的最大内存（字节）

>wmic   os   get   caption              //查看操作系统版本

>wmic   BaseBoard   get   SerialNumber             //查看主板序列号（和 bios 序列号不同）
>wmic   BaseBoard   get   manufacturer             //查看主板厂商，品牌
>wmic   BaseBoard   get   product                  //型号，平台
```

开启 snmp 管理

>appwiz.cpl→打开或关闭 windows 功能→添加“简单网络管理协议”
>services.msc→找到 SNMP service 服务，双击→“安全”选项卡→添加社区名称为 publicxx →接受来自下列主机的 SNMP 数据包下面添加 IP（管理站的 IP）

查看连接过的 wifi 密码

>netsh wlan show profile name="wifi-ssid" key=clear
在“安全设置”的关键内容下面

添加静态 dns 解析

C:\Windows\System32\drivers\etc\hosts 文件为本地域名解析文件
以管理员身份运行 cmd，用命令追加一条 dns 解析条目：
>echo 10.1.1.1 xxx.com >> C:\Windows\System32\drivers\etc\hosts
//dns 解析条目前后不能有引号"" 一条一行
之所以用命令添加，是因为有时候无法直接编辑该 hosts 文件，用管理员身份运行也无法编辑。

修改 TTL 值

>regedit //在注册表里修改
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
右边新建 DWORD32bit 类型，名为 DefaultTTL 值为自己设置的 ttl，十进制 1~255
重启生效

更改远程桌面端口号

>regedit
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal\Server\WinStation\RDP-Tcp
右边找 PortNumber 值改为自定义的 23389
重启远程桌面服务（Remote Desktop Services）
客户端远程时填写 x.x.x.x:23389

关闭磁盘开机自检

重启/开机时磁盘自检是因为 磁盘有坏道，暂时的解决方法：

1.开机时屏蔽检测该磁盘，以管理员身份进入 cmd
>chkdsk /x C
2.取消所有的磁盘开机自检，以管理员身份进入 cmd
>chkntfs /t:0
3.修改注册表
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
右边找 BootExecute 将其值清空
重启电脑生效
4.修复坏道

Windows 开机启动项位置

这个所谓的开机启动项，并不是随开机启动的，而是只有用户登录时（开启一个 console 连接会话时）才会启动目标程序
C:\Users\用户名\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
其他的启动项可以写入注册表了，需要用 Autoruns 工具查看

去除桌面图标的左下角的小箭头

桌面上的程序图标 其实只是该程序的一个快捷方式（链接），链接文件的图标是带有一个小箭头的，要想去掉该箭头，可以修改注册表
>regedit
HKEY_CLASSES_ROOT\lnkfile
右边选中 IsShortCut 删除该项即可（该项数据类型为 REG_SZ，默认值为空）
重启系统生效

slmgr 命令

Software License Manager
>slmgr /ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX //安装密钥
>slmgr skms kms.03k.org //设置 kms 服务器
>slmgr /ato //尝试在线激活，Attempt Online
>slmgr.vbs -xpr //查看当前许可证的截止日期，是否为永久激活
>slmgr.vbs -ilc /xxx.lic //导入 OEM 证书
>slmgr.vbs -cpky //从注册表中清除产品密钥信息
>slmgr.vbs -upk //卸载当前产品密钥，重启后显示未激活状态

修改 OEM 信息

新建文本文件，后缀为.reg（即注册表文件），内容如下

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation]          //这是一行
"Manufacturer"="Lenove"
"Model"="Y460n-IFI"
"SupportPhone"="400-810-9111"
"SupportHours"="周一至周五 9:00~18:00"
"SupportURL"="https://xxxxxx.cn"
"Logo"="C:\xxxx.bmp"                    //只支持.bmp 文件作为图标
```

保存，双击运行该文件，以管理员身份运行，即可注册

关闭 Windows Defender

>gpedit.msc　　//打开“本地组策略编辑器”

计算机配置→管理模板→Windows 组件→Windows Defender

右边“关闭 Windows Defender”→右击编辑“已启用”

卸载：可使用 WindowsDefenderRemoveScript 工具

关闭 MSE

Microsoft Security Essentials

1.开机不自启

>msconfig →启动→启动项里打开 Microsoft Security Essentials，取消勾选

2.程序里设置不启用保护

双击运行 C:\Program Files\Microsoft SecurityClient\msseces.exe

设置→实时保护：关

3.或者直接 appwiz.cpl 里卸载该软件

IE 提示有风险不能下载

>inetcpl.cpl→高级→找到安全下面的“启用 Smartscreen 筛选器”，取消勾选

OutLook 邮箱客户端

*使用 IMAP 时
邮件默认存放地址 C:\Users\用户名\AppData\Local\Microsoft\Outlook\邮箱地址.ost
关闭 outlook 后，可用 Advanced Exchange Recovery 工具转为.pst 数据文件
前提是邮箱服务器可用，
最好是用 outlook 导出为.pst 文件
*使用 POP3 时
邮件默认存放地址 C:\Users\用户名\Documents\Outlook 文件\邮箱地址.pst
.pst 文件可直接导入/打开（用 outlook）

SysWoW64

wow64（Windows On Windwos 64）是 windows 系统的子系统，使得 32 位的程序可以在 64 位的系统中正常运行，32 位程序在访问 64 位系统里的 system32 文件夹时被重定向到 syswow64 文件夹里。
64 位系统里的:
system32 文件夹里的 dll 为 64 位的
syswow64 文件夹里的 dll 为 32 位的

端口转发（仅 tcp）

```
>netsh interface portproxy show v4tov4                    //查看端口转发
>netsh interface portproxy add v4tov4 listenport=12001 listenaddress=0.0.0.0
        connectport=3389 connectaddress=10.1.1.4          //创建端口转发
>netsh interface portproxy delete v4tov4 listenport=12001 listenaddress=0.0.0.0
                                                          //删除一条端口转发
```

网卡 MTU

```
>netsh interface ipv4 show subinterfaces                  //查看 mtu 及流量
>netsh interface ipv4 set subinterface "网卡名" mtu=1500 store=persistent
                                                  //该 mtu 含 ip 头部
```

注册表上改：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\
在 Interfaces 下有多个子项，分别点击查看 ipaddress
找到目标 IP 的那个子项，右边新建 DWORD 型数据，名为 MTU，值为 1500 自定义的

shutdown 定时关机

```
>shutdown   -s              //关闭计算机
>shutdown   -r              //重启
>shutdown   -t   10         //10 秒，定时，可配合 -s ，-r
>shutdown   -f              //强制
>shutdwon   -a              //取消定时关机/重启
```

例：

```
>shutdwon   -s   -t   1                 //1 秒后强制关机
```

创建 bcd 启动菜单

创建一个不运行 Hyper-V 的启动菜单项

```
>bcdedit   /copy   {current}   /d   "Windows 10 no Hyper-V"          //以现有的为基础
  //提示已将该项成功复制到{fe08xxxxxxxx}
>bcdedit   /set   {fe08xxxxxxxx}   hypervisorlaunchtype   Off        //设置 bcd 菜单项

>bcdedit   /delete   {fe08xxxxxx}                    //删除
>bcdedit   /enum                                  //查看
```

修改 ARP 老化时间

```
>regedit
```

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
右边新建名为 ArpCacheLife 类型为 DWORD，值为 120 秒自定义的
右边新建名为 ArpCacheMinReferencedLife 类型为 DWORD，值为 600 秒自定义
如果一个 arp 缓存在 120 秒内被用到，则其期限再延长 120 秒，直到最大生命 600 秒。
不管在 600 秒最大生命内是否被访问到，到了 600 秒时间都会删除该缓存，再重新获取

Windows 允许多用户同时远程登录

WindowsXP 和 Vista 和 Windows 7 这几个可以使用 Universal Termsrv.dll Patch 通用补丁，
以管理员身份运行 UniversalTermsrvPath-x64.exe，点击破解，重启系统即可
更高版本的 windows 可以用 RDPwrap 工具

安装.Net

Windows 8.1 系统不自带.net3.5 的文件，要从安装光盘镜像文件里提取 sources\sxs 文件夹下的所有文件到本地的某个目录下，如 G:\sources\sxs
以管理员身份运行 cmd:
>dism /online /enable-feature /featurename:NetFX3 /Source:G:\sources\sxs

Windows 7 不自带.net4.x
可以用安装包安装： mu_.net_fx_4.6.1_for_win7_7277558.exe

Ghost 系统修改 SID

C:\Windows\system32\sysprep> sysprep.exe /generalize /oobe //运行
或双击该目录下的 sysprep.exe →“进入系统全新体验 oobe”，勾选“通用”
重启后要求重新输入密钥，重创建用户及密码

可用 NewSID 工具查看计算机的 SID（仅查看，不要用该工具修改）
>whoami /user //查看到计算机的 sid 加上-用户的 sid（3 位或 4 位）

查看用户

```
>whoami                          //查看当前用户名
>whoami  /user                   //查看用户名及 uid（sid+xxx）
>query  user                     //查看当前登录到系统的所有用户
>qwinsta  /server:10.1.1.1       //查看目标主机上的登录会话
>rwinsta  /server:10.1.1.1  3            //强制结束目标会话，3 为会话 ID
```

连接 NFS、SMB 共享

*连接 NFS
要安装客户端，>appwiz.cpl→启用或关闭 windows 功能→NFS 服务
cmd> mount \\10.1.1.1\nfsShare x: //挂载远程的 nfs 共享文件夹到本地的 x:
然后用资源管理器查看 X：盘里的文件
cmd> umount x: //取消挂载

*连接 SMB（cifs）
Win+R 输入 \\10.1.1.2\shareName //输入用户名和密码后，和 FTP 差不多，也可挂载到某个盘符上详见下面的 IPC$

IPC$

>net share //查看共享的文件夹或资源，$表示隐藏的共享
没开启 windows 自带的防火墙时，无需密码也能连接这些共享
IPC$ 使用 139，445 端口，应当关闭
关闭 139 端口：选中网卡→属性→TCP/IPv4 协议→高级→WINS→NetBIOS 设置→禁用
>net share C$ /del //删除共享，临时的，重启系统后又有了
>net share D$ /del

>net use \\IP 地址\共享名 "密码" /user:"用户名"
>net use Z: \\x.x.x.x\C$ //将远程主机的 C 盘共享映射成本机的 Z：盘
>net use \\x.x.x.x\共享名 /del //断开共享的连接

>shutdown -r -m \\x.x.x.x -t 0 //远程关机，前提是先连接 IPC$

注册表是永久关闭某些默认的共享
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
右边创建 AutoShareServer REG_DWORD 0x0 //C$，D$
AutoShareWks REG_DWORD 0x0 //ADMIN$
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
右边改 restrictanonymous REG_DWORD 0x0 为缺省
0x1 为匿名用户无法列举用户列表
0x2 为匿名用户无法连接本机 IPC$共享
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
右边新建 SMBDeviceEnabled REG_DWORD 0

Win 8.1 开机后直接进入桌面

右击桌面下的任务栏→属性→导航→“开始屏幕”→勾选第一项
重启生效

使用 RDCman.exe 远程连接时提示：拒绝请求的会话访问

RDCman 上 右击目标主机→属性→连接设置→取消勾选☐Connect to console
//Properties→Connection settings

安装 Office 时提示：此副本不能在运行终端服务的计算机上使用

原因是　计算机系统开启了"远程桌面会话主机服务"，删除此角色即可。
可以开启远程桌面登录服务，默认是只允许一个用户同时登录，服务器版本为 2 个用户。
可以用 RDPwrap-v1.6.2 工具解除连接限制，以实现远程桌面会话主机服务的目的。
或者是安装批量许可版本。

关闭、禁止 windows 自动更新

1.服务中关闭
>services.msc→找到 Windows Update 服务→常规（禁用），恢复（无操作）
2.任务计划中关闭
>taskschd.msc→任务计划程序库→Microsoft→Windows→Windows Update 禁止所有项
3.组策略
>gpedit.msc→计算机配置→管理模板→Windows 组件→Windows 更新，右边：
　　配置自动更新，已禁用
　　删除使用所有 windows 更新功能的访问权限，已启用
4.注册表
>regedit
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsoSvc
右边找到 Start 改属性十六进制值为 4
　　FailureActions 改第 4 行从右到左第 5 个 01 改为 00

加域时提示找不到网络路径

可能是某些服务未启用，启动以下服务：
computer browser、remote procedure(RPC)、tcp/ip netbios helper、server、
windows management instrumentation、workstation、messenager、alerter

Office 激活查看

>cscript　"C:\Program Files\Microsfot Office\Office15\ospp.vbs"　/dstatus
>slmgr.vbs　-xpr　"SKU ID"　　//输入上面刚刚查看到的 sku id

可以用 Windows Toolkit 工具查看 Productkey 和激活渠道

不在“快速访问”中显示最近使用的文件

Win+E 打开“资源管理器”→点击菜单栏上的 View（查看）→菜单栏最右边出现“选项”
→点击“更改文件夹和搜索选项”→常规下的 隐私下：→取消勾选以下 2 项
☐在快速访问中显示最近使用的文件
☐在快速访问中显示常用文件夹

打开“文件资源管理器”时不打开“快速访问”

Win+E 打开“资源管理器”→点击菜单栏上的 View（查看）→菜单栏最右边出现“选项”
→点击“更改文件夹和搜索选项”→常规下的 第一行：
打开文件资源管理器时打开 此电脑

修改系统的 DNS 缓存时间

Windows 系统的 DNS 缓存时间默认为 86400 秒（24 小时）
>regedit
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
创建 DWORD 的 MaxCacheTtl 值为自定义的时间，秒
创建 DWORD 的 MaxNegativeCacheTtl 值为（dns 缓存的否定回答超时），秒

>services.msc 查看 DNS Client （dnscache 服务）是否开启，建议不要关闭。