### Windows系统操作手册

**前言：**

1.蓝色字体表示命令行命令，正式执行时不要复制前面的>号，>号只是cmd提示

2.绿色字体表示注释，有时注释太多就不用绿色表示了

3.注意：本文档的所有操作请先在测环境进行实践，请不要直接在真实的服务器中操作！

**版权声明**：

本文档以开源的形式发布，所有条款如下：

1. 无担保：作者不保证文档内容的准确无误，亦不承担由于使用此文档所导致的任何后果

2. 自由使用：任何人可以出于任何目的而自由地 阅读/链接/打印/转载/引用/再创作 此文档，无需任何附加条件

若您 阅读/链接/打印/转载/引用/再创作 本文档，则说明接受以上2个条款。

作者：李茂福

更新日期：2023-08-25

**★windows系统版本**

> ver #查看系统版本

Microsoft Windows [版本 10.0.17763.557]

> dism /online /get-currentedition #查看系统版本

映像版本: 10.0.17763.557

当前版本 : Professional

> wmic os get caption #查看系统版本

Microsoft Windows 10 专业版

**win10版本及os代码**

|  |  |  |  |
| --- | --- | --- | --- |
| version | os build （NT 10.0） | version | os build （NT 10.0） |
| 1507（RTM） | 10.0.10240.xxx | 1809 | 17763 |
| 1511 | 10586 | 1903 | 18362 |
| 1607 | 14393 | 1909 | 18363 |
| 1703 | 15063 | 2004 | 19041 |
| 1709 | 16299 | 20H2 | 19042 |
| 1803 | 17763 |  |  |

**win NT对应系统版本**

|  |  |  |  |
| --- | --- | --- | --- |
| NT版本 | 操作系统 | 时间 |  |
| NT 5.0 | windows 2000 | 2000/2/17 |  |
| NT 5.1 | win XP | 2001/10/15 |  |
| NT 5.2 | win XP 64bit  winSer 2003/2003 R2 | 2003/3  2003/4 |  |
| NT 6.0 | Vista  win Ser 2008 | 2007/1/30  2008/8/27 | 6.0.6002... (sp2) |
| NT 6.1 | win 7  win Ser 2008 R2 | 2009/10/22  2009/10/22 | 6.1.7600...  6.1.7601... (sp1) |
| NT 6.2 | win 8  win Ser 2012 | 2012/10/26  2012/9/4 | 6.2.9200.16384 |
| NT 6.3 | win 8.1  win Ser 2012 R2 | 2013/10/18  2013/10/18 | 6.3.9600...  6.3.9600... |

**★微软生命周期策略**

https://support.microsoft.com/zh-cn/lifecycle/search

https://learn.microsoft.com/en-us/lifecycle/products/

|  |  |  |  |
| --- | --- | --- | --- |
| 系统版本 | 开始时间 | Mainstream End | Extend End Date |
| win 7 | Oct 22, 2009 | Jan 13, 2015 | Jan 14, 2020 |
| win 8 | Oct 30, 2012 |  | Jan 12, 2016 |
| win8.1 | Nov 13, 2013 | Jan 9, 2018 | Jan 10, 2023 |
| winSer 2012 R2 | Nov 25, 2013 | Oct 9, 2018 | Oct 10, 2023 |
| winSer 2016 | Oct 15, 2016 | Jan 11, 2022 | Jan 12, 2027 |
| winSer 2019 | Nov 13, 2018 | Jan 9, 2024 | Jan 9, 2029 |
| Windows 10 Home and Pro | Jul 29, 2015 | Retirement Date : | Oct 14, 2025 |

**★windows故障排查（官网）**

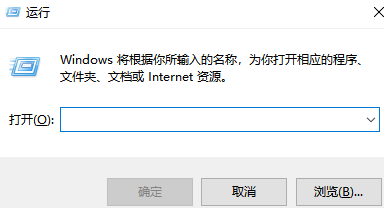
https://learn.microsoft.com/zh-cn/troubleshoot/windows/

https://learn.microsoft.com/zh-cn/troubleshoot/windows-client/welcome-windows-client

https://learn.microsoft.com/zh-cn/troubleshoot/windows-server/welcome-windows-server

**★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 |
| lsdiag.msc | 远程桌面授权诊断器 | |  |
| LicMgr.exe | 远程桌面授权管理器，看lic数量/类型 | |  |
| slmgr.vbs -xpr | -dli -dlv | 查看系统激活信息 |  |
| oobe/msoobe /a | 查看win XP激活信息 | |  |

**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 |  |  |

**锁屏：win+L**

写.bat命令内容如下：

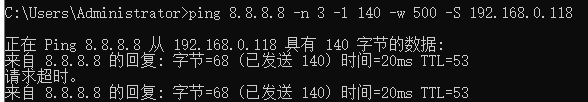
rundll32.exe user32.dll LockWorkStation

**★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

# ping -6 表示使用ipv6



②Tracert

> tracert -d -h 跃点数 -w 超时 目标IP #超时单位毫秒

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 /registerdns #向dns服务器注册本地ip

>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

④nslookup

>nslookup xxx.com #获取域名的IP地址

>nslookup -querytype=查询类型 xxx.com #获取域名的指定记录值，查询类型：txt,ms,a,aaaa

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-p 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

**注册表网卡配置**

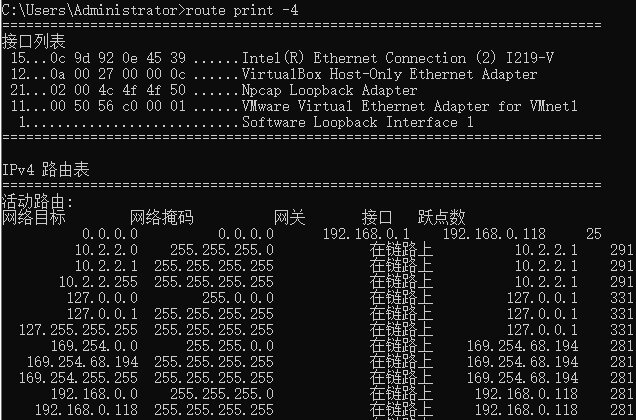
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parametes\Interfaces\Adapters

可根据ip信息去判断对应的哪个网卡

**★路由操作**

以管理员身份运行cmd

>route print [-4] #查看路由表



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

#metric指定优先级为230，if指定出口为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**

> control →程序→启用或关闭windows功能→添加“简单网络管理协议”

> appwiz.cpl →打开或关闭windows功能→添加“简单网络管理协议”

> services.msc →找SNMP service服务，双击→“安全”选项卡→添加社区名称xxxx

→接受来自下列主机的SNMP数据包下面添加IP（管理站的IP）

**win10和win2019的1809及以上版本要使用PowerShell安装：**

PS> Get-WindowsCapability -Online -Name "SNMP\*"

PS> Add-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"

> services.msc 找到 SNMP服务，双击进入，点击“安全”选项卡：

添加社区名称（团体字）

接受来自下列主机的SNMP数据包

**★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.>> C:\Windows\System32\drivers\etc\hosts #先追加一空行

> 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3389**

> 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

**★mstsc删除ip记录**

> regedit

HKEY\_CURRENT\_USER\Software\Microsoft\Terminal Server Client\Default

右边删除不需要记录的ip

**★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（如C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

> regedit

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

**★diskpart磁盘分区操作**

在windows安装界面，按下Shift + F10 进入cmd

> diskpart

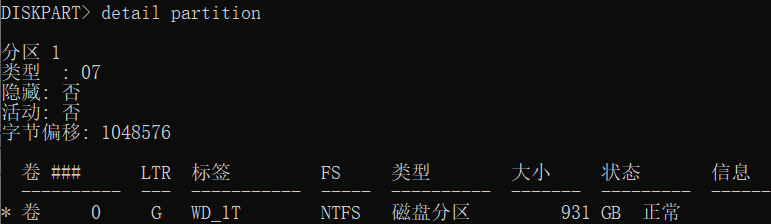
> list disk

> select disk 0

> list partition

> select partition 1

> detail partition



> set id=07 override #设置分区类型，07为NTFS

> list disk

> select disk 1

> clean

> convert mbr #转为mbr分区，convert gpt 为GPT分区类型

**★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 #个人

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup #全局

其他的启动项可能写入注册表了，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字符串，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

Win+R打开运行框：

> slui # slui 3 打开激活向导，输入密钥

> slui 4 #电话激活

**★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]

"Manufacturer"="Lenovv"

"Model"="Z390-Cof"

"SupportPhone"="400-890-1234"

"SupportHours"="周一至周五 9:00~18:00"

"SupportURL"="https://xxxxxx.cn"

"Logo"="C:\logoxxx.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，以管理员身份运行Uninstall.cmd

**★关闭MSE（microsoft security essentials）**

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 #（这行与上面为同一行）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 #-t指定时间，单位秒，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{fe08xxxxxxxxx}

>bcdedit /set {fe08xxxxxxxx} hypervisorlaunchtype Off #设置bcd菜单项

>bcdedit /delete {fe08xxxxxx} #删除

>bcdedit /enum #查看

可用BootICE工具

**★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及win10系统自带.net4.x 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自带.net3.5 不自带.net4.x**

可以用安装包安装： mu\_.net\_fx\_4.6.1\_for\_win7\_7277558.exe

要求先关闭安全软件

.Net安装包下载地址： https://dotnet.microsoft.com/en-us/download/dotnet

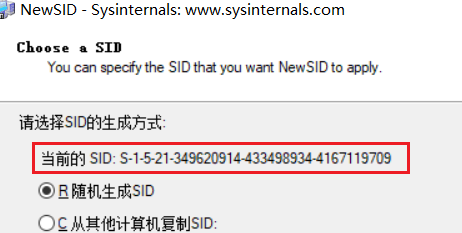
**★Ghost系统修改SID（用户sid）**

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）



C:\Users\cof> whoami /logonid #查看logon id

S-1-5-5-0-562111

C:\Users\cof> whoami /user #查看到计算机的sid加上-用户的sid（3位或4位），加域后看到的为 域sid，而非本地计算机的sid

用户名 SID

========== ============================================

cof-pc\cof S-1-5-21-349620914-433498934-4167119709-1001

**★用户配置文件夹C:\Users\%username%**

> regedit

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\

在下面找相应用户的sid，改配置目录

**★查看登录的用户**

>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

> net user #查看系统的所有用户

> logoff <id> #踢出某个用户

**★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

windows客户端修改uid：

> regedit

HKEY\_LOCAL\_MACHINE\Software\microsoft\ClientForNFS\CurrentVersion\Default

增加： DWORD AnonymousUid 值为自定义

DWORD AnonymousGid 值为自定义

\*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

**★关闭LLMNR服务5355端口**

LLMNR本地链路多播名称解析服务，5355

> gpedit.msc →计算机→策略→管理模板→网络→DNS客户端→关闭多播名称解析：启用

无组策略的：

> regedit

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient

右创建 DWORD类型，名为 EnableMulticast 值为0

**★dism映像操作**

> dism /Get-WimInfo /WimFile:D:\path\to\install.wim #查看镜像里的各个版本信息

> dism /Mount-Image /ImageFile:D:\path\to\install.wim /index:4 /MountDir:E:\temp\mount #将索引4的映像装载至E:\temp\mount路径下

> dism /Image:E:\temp\mount /Add-Driver /Driver:C:\drivers\mydriver.inf #将指定的驱动添加至映像中

> dism /Image:E:\temp\mount /Add-Driver /Driver:C:\drivers /Recurse #装载指定文件夹下的所有驱动

#如果需要加载未签名的驱动程序，则需添加 /ForceUnsigned参数

> dism /image:E:\temp\mount /get-drivers #查看加载的所有第三方驱动列表

> dism /Image:C:\test\install.wim /Remove-Driver /Driver:OEM1.inf /Driver:OEM2.inf #从映像中删除指定的驱动

> dism /image:E:\temp\mount /add-package /packagepath:"WinPE-HTA.cab" #将指定的cab添加到映像中

> dism /Unmount-Image /MountDir:E:\temp\mount /Commit #保存更改并卸载映像

当卸载失败或者挂载时命令窗口关闭导致挂载目录中有残留文件和目录时，可以使用以下命令清除状态。否则可能影响下一次挂载：

> dism /cleanup-mountpoints

> dism /online /get-drivers #在系统下获取安装的第三方驱动信息

> dism /Cleanup-wim #删除与已损坏的已安装WIM映像关联的资源

**★文件目录操作（命令行）**

> dir #列出当前目录下所有文件

> type file.txt #查看文本文件内容

> copy src dest #复制文件

> copy C:\xxx.file D:\ #复制到D盘根目录下

> del xxx.file #删除文件

> more file.txt #查看前几行

> move src dest #移动文件

> mkdir dirxx #创建目录

> rd /s/q dirxx #删除目录

**★windows复制文件保留原属性**

以管理员身份运行：

> Robocopy D:\src\ E:\dst\ /DCOPY:T /COPYALL /E /R:0

/DCOPY:T #保留文件原始时间戳

/COPYALL #复制所有属性，等效于 /COPY:DATSOU

/COPY: D 数据

/COPY: A 属性

/COPY: T 时间戳

/COPY: S NTFS ACL安全组

/COPY: O 所有者信息

/COPY: U 审核信息

/E #递归方式，包含空目录

/R:0 #不重试锁定的文件，因为默认重试100万次

**★SC服务管理（Service Control）**

> sc query 服务名称 #查询服务状态

> sc stop 服务名称 #停止服务

> sc start 服务名称 #启动服务

> sc continue 服务名称 #恢复暂停状态的服务

> sc delete 服务名称 #删除服务

> sc config 服务名称 start=auto #设置服务启动类型，自动

start=demand #手动

start=disabled #禁用

创建服务：

> sc create 服务名称 binpath="C:\path\to\xxx.exe -p 参数" type=share `

start=auto displayname="xxxx" [depend=RpcSs/EventSystem/Tcpip]

# type=share/own/kernel

> net start 服务名称 #

> sc description 服务名称 "注释，描述" #

**#建议使用nssm工具**

nssm（Non-Sucking Service Manager）可把.exe程序做成windows系统服务

下载地址： https://nssm.cc/download

在nssm.exe所处目录打开shell,cmd，以管理员身份运行

> nssm.exe install 服务名 #打开GUI，进行服务配置

> nssm.exe edit 服务名 #编辑

# 先停止服务，再删除服务

> nssm.exe stop 服务名

> nssm.exe remove 服务名

**★进程查看**

> netstat -ano | findstr 80

> tasklist | findstr nginx #查看进程

> taskkill /im 程序名称 -f #结束进程

> taskkill -pid 进程id -f #结束进程

**★设置系统http\_proxy变量**

PS> [Environment]::SetEnvironmentVariable("HTTP\_PROXY","http://user:passwd@ip:port/",[EnvironmentVariableTarget]::Machine)

取消（设置为空即可）

PS> [Environment]::SetEnvironmentVariable("HTTP\_PROXY",$null,[EnvironmentVariableTarget]::Machine)

**★开机后用户自动登录进入桌面**

①未加域的

> netplwiz →选中目标用户，取消勾选：

要使用本计算机，用户必须输入用户名和密码

点击应用，输入密码，确定

②加域的

> regedit

HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

右边找 AutoAdminLogon (RegSZ) 值为1(自动登录)，0为手动登录

DefaultDomainName (RegSZ) cof.com （也可用COF wins名称）

DefaultUserName (RegSZ) coflee

DefaultPassword (RegSZ) passxxx

重启系统即可

**★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

**★win10去除无法连接到网络黄色感叹号**

> regedit

HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Network Connections

右边创建 DWORD 名为 NC\_DoNotShowLocalOnlyIcon 值为 1

**★关闭IE的自动检测源和网页快讯更新**

> inetcpl.cpl

打开Internet选项→内容（下面的“源和网页快讯”）→设置→取消勾选“自动检查源和网页快讯的更新”

在taskschd.msc里有 User\_Feed\_Synchronization 任务，就是“自动检查源..更新”创建的，

触发 system32\msfeedssync.exe sync

**★mstsc证书更换**

非加域版：

1.申请ssl证书，用 .pfx格式

2.导入证书，本地计算机

3.win+R，输入 mmc 打开管理控制台→文件→添加/删除管理单元

右侧选中“证书”→添加，用“计算机帐户”→本地计算机，完成

4.点“证书”→个人→右击“所有任务”→导入.pfx→根证书类型→自动选择证书存储

5.在已导入的证书上右击→所有任务→管理私钥→安全，添加NETWORK\_SERVICE用户的读权限

6. > regedit

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

右侧创建 Reg\_binary类型，名为 SSLCertificateSHA1Hash 值为目标证书的指纹

右侧SelfSignedCertificate为默认的证书指纹，自签名的，在certmgr.msc里没有

**★文件校验工具certutil**

> certutil -hashfile D:\文件 MD5 # SHA1,SHA256

**★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。

**★win system进程占用了443端口**

可能由RRAC Routing and Remote Access服务占用的

**★虚拟机关闭网卡TaskOffLoad**

> regedit

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

右创建 DWOR 名为 DisableTaskOffload 值为1

**★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行从左到右第5个01改为00

**5.推迟检查更新时间设置为100年**

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\UX\Settings

右侧新建类型为 reg\_dword 名为 FlightSettingsMaxPauseDays 值为十进制 36500

**★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

**★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

**★关闭“文件资源管理器”搜索记录**

> gpedit.msc

用户配置→管理模板→Windows组件→文件资源管理器 右边的：

在文件资源管理器搜索框中关闭最近搜索条目的显示 已启用

**★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 （dns cache服务）是否开启，建议不要关闭

**★修改NTP服务器地址**

> regedit

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

找NtpServer项，值为ntp服务器域名/ip加0x1（默认为time.windows.com,0x9）

如： cn.pool.ntp.org,0x1 hk.pool.ntp.org,0x1

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient

找SpecialPoolInterval项，值为poll间隔时间，秒

找Enabled项，值1表示启用ntp客户端

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer

找Enabled项，值1表示启用ntp服务端，自己做ntp服务器

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

找AnnounceFlags项，表示层级stratum

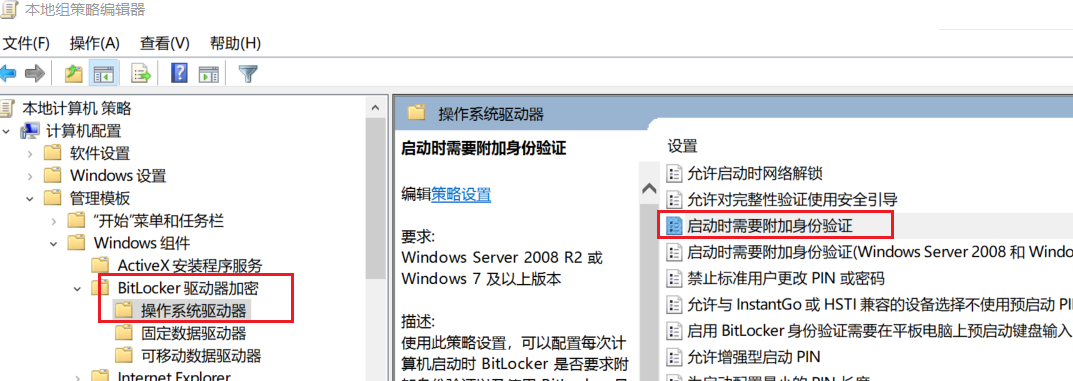
找UpdateInterval项，改为5

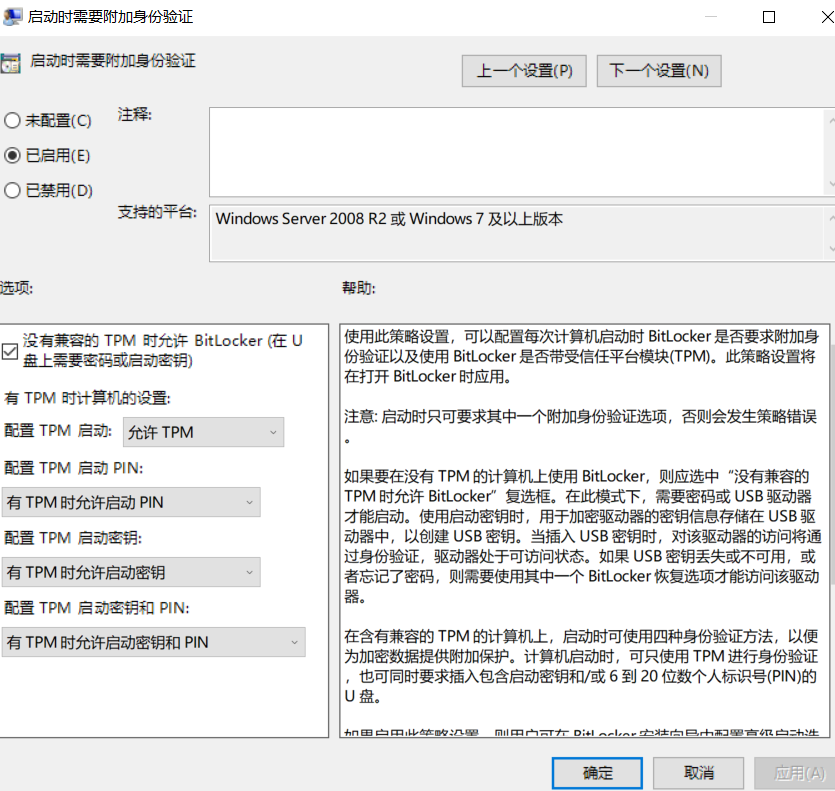
**★开启BitLocker**

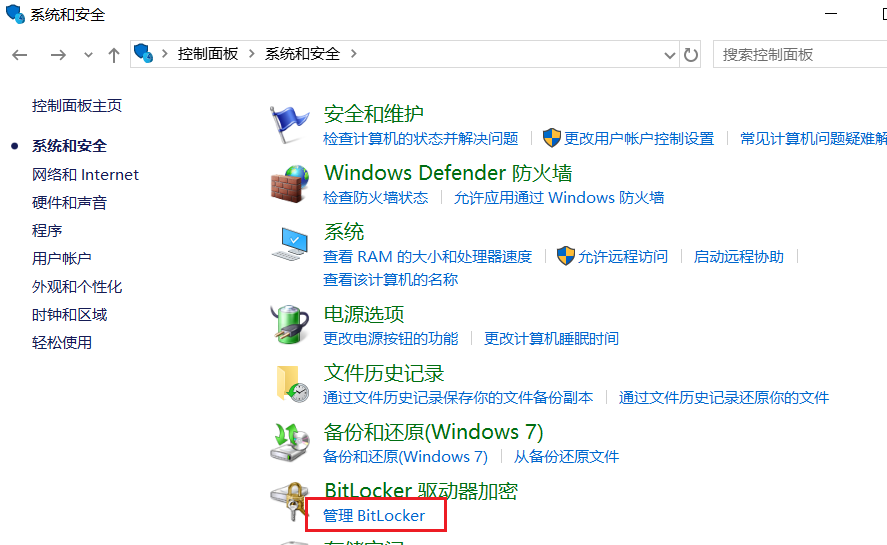
> gpedit.msc

计算机配置→管理模板→Windows组件→BitLocker驱动器加密

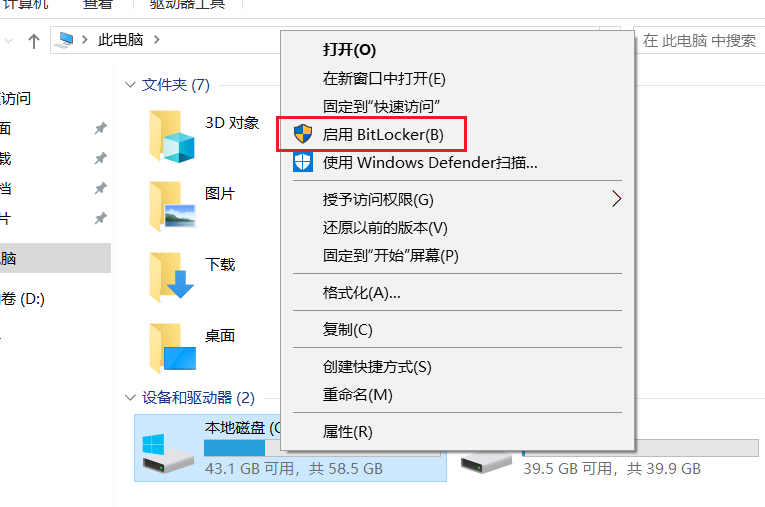
右侧：启动时需要附加身份验证





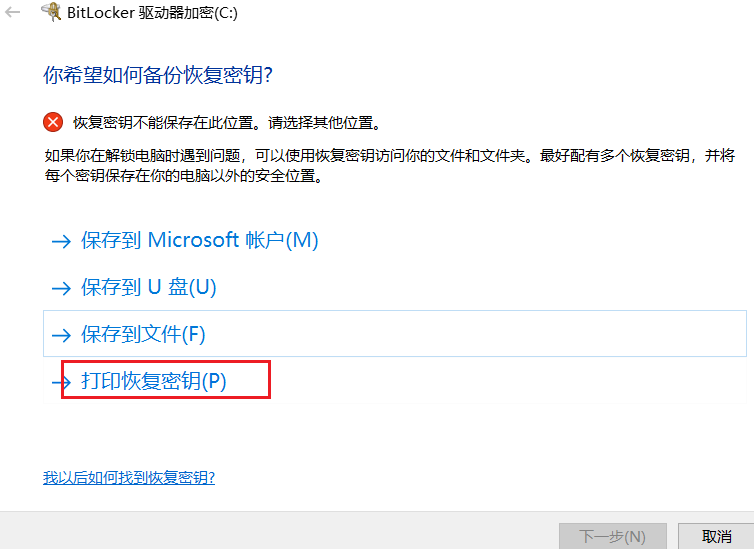


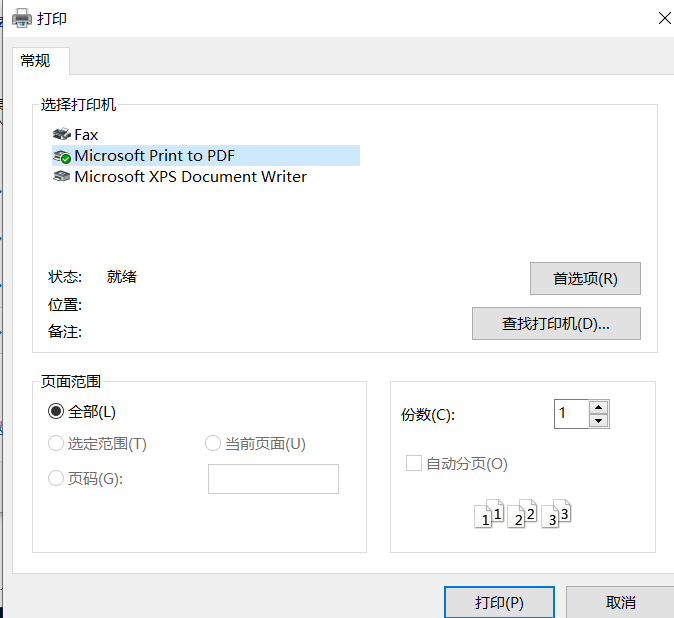


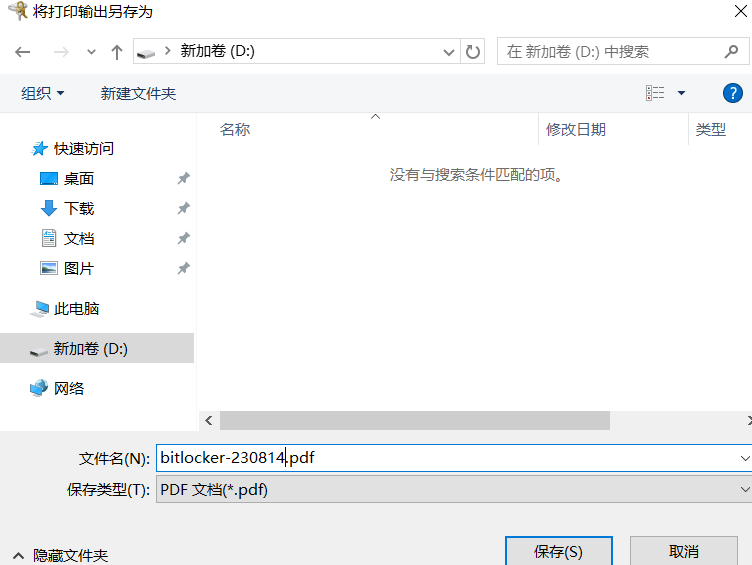






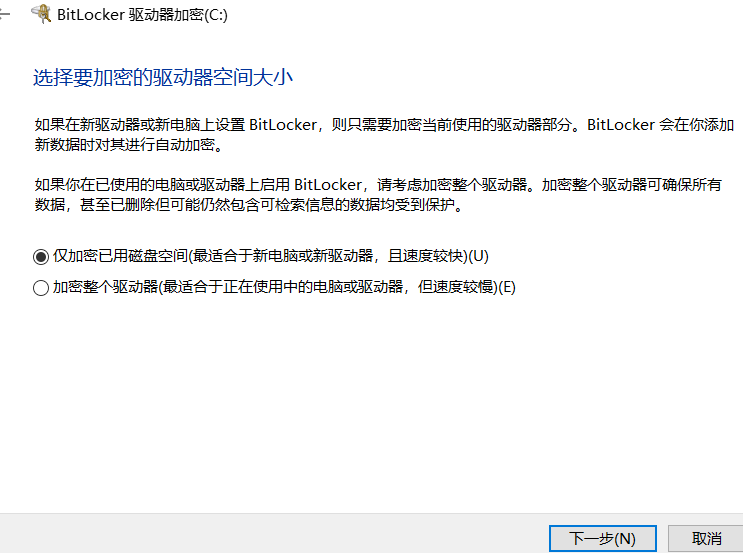


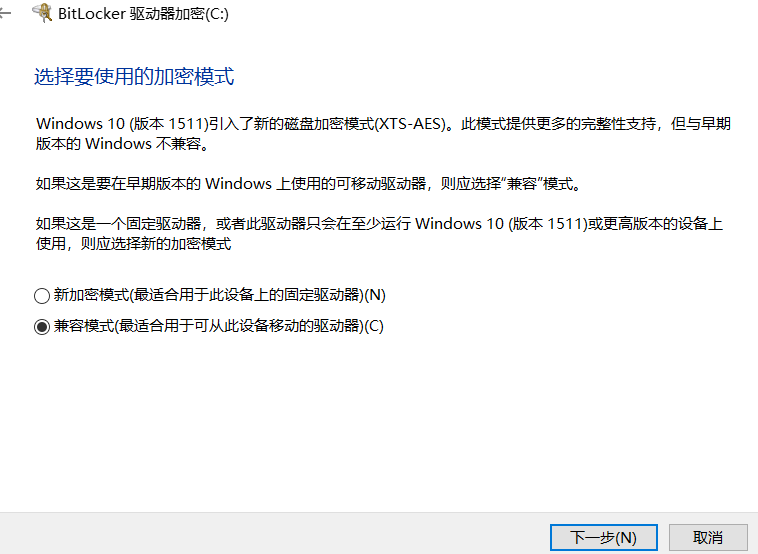


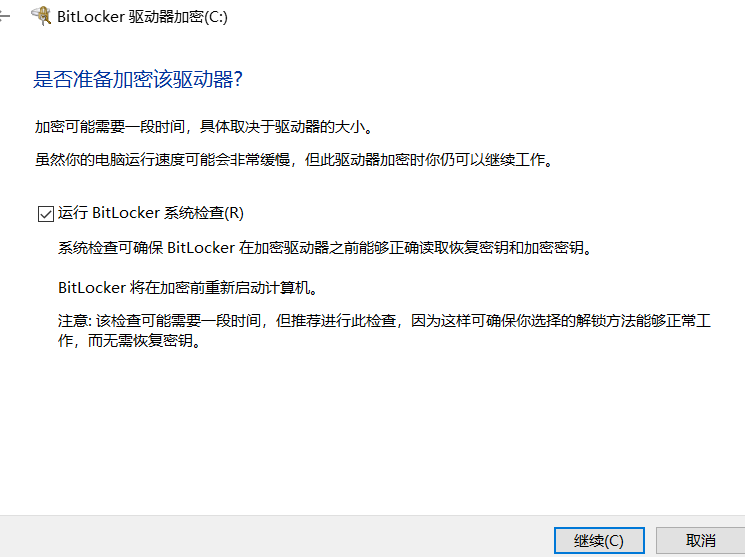


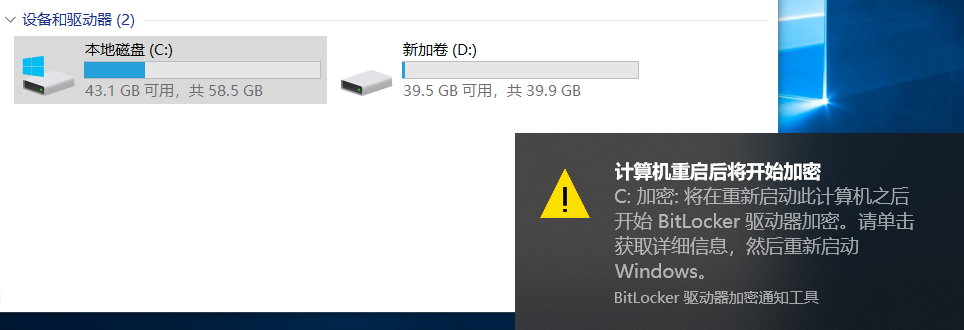
保存后，就可进行下一步操作

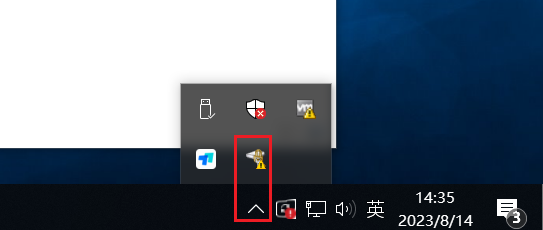


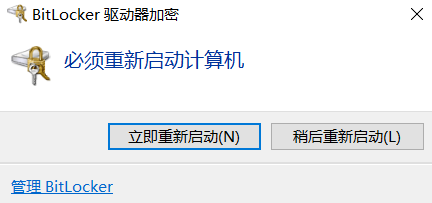






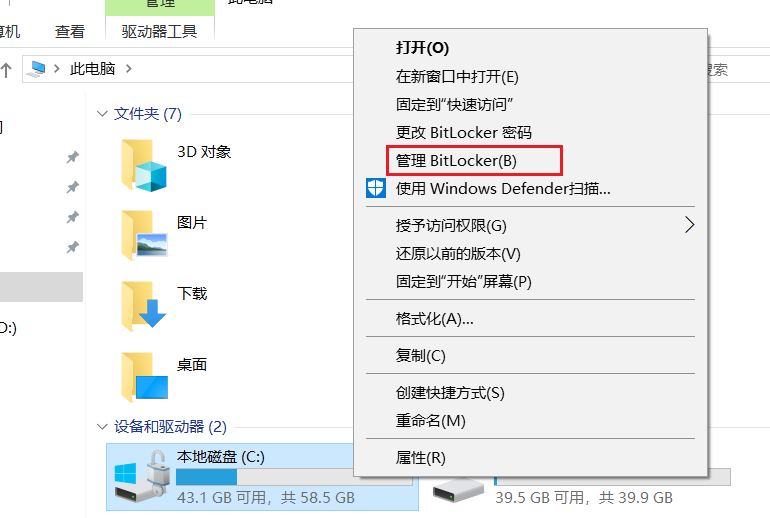








取消bitLocker



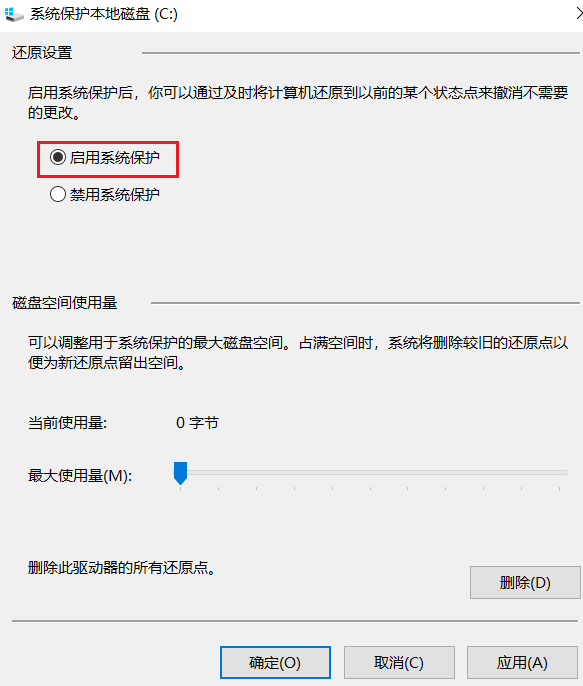


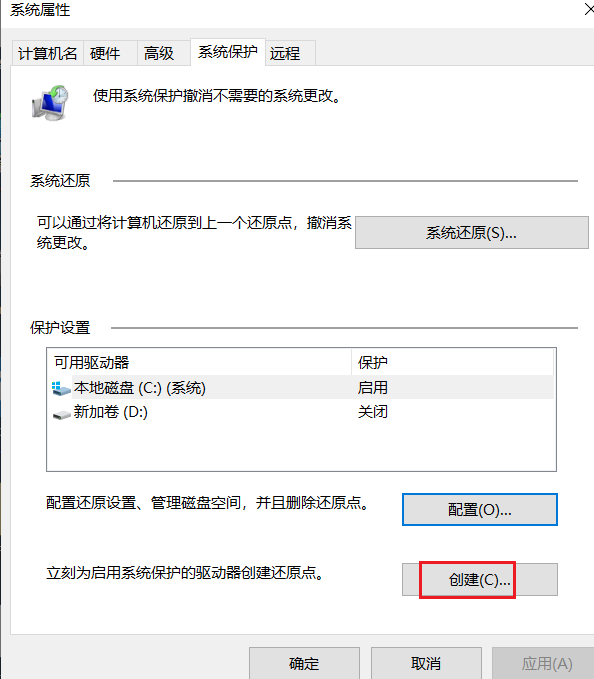
**★创建系统还原点**

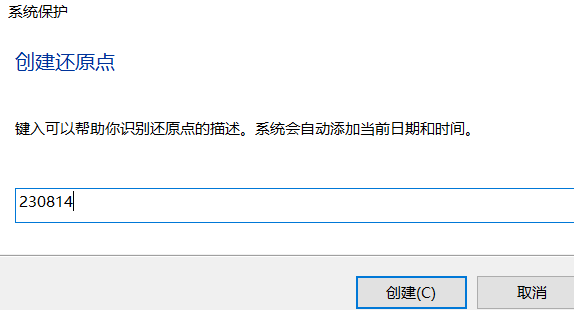
> control system

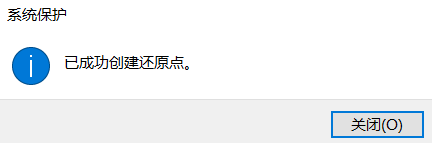










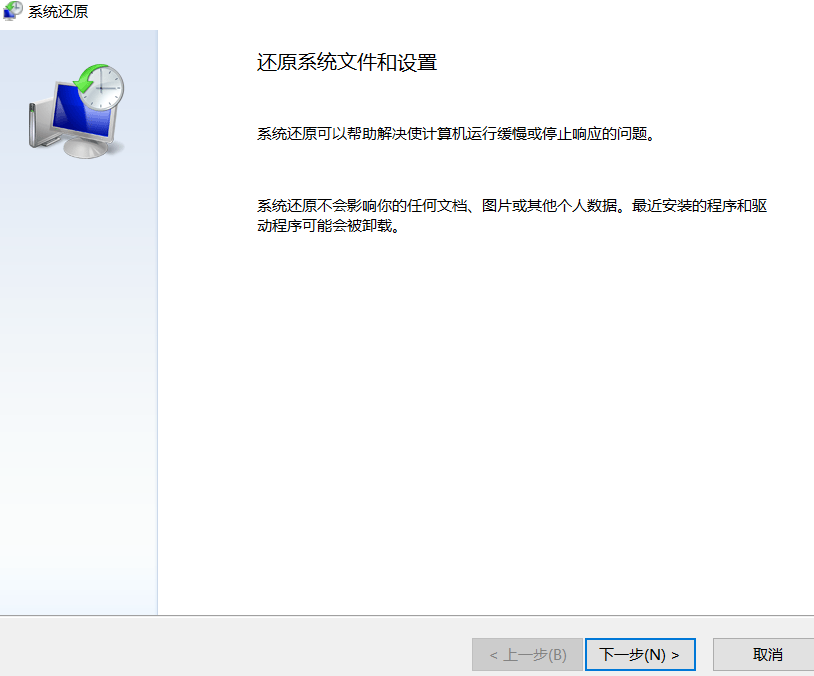


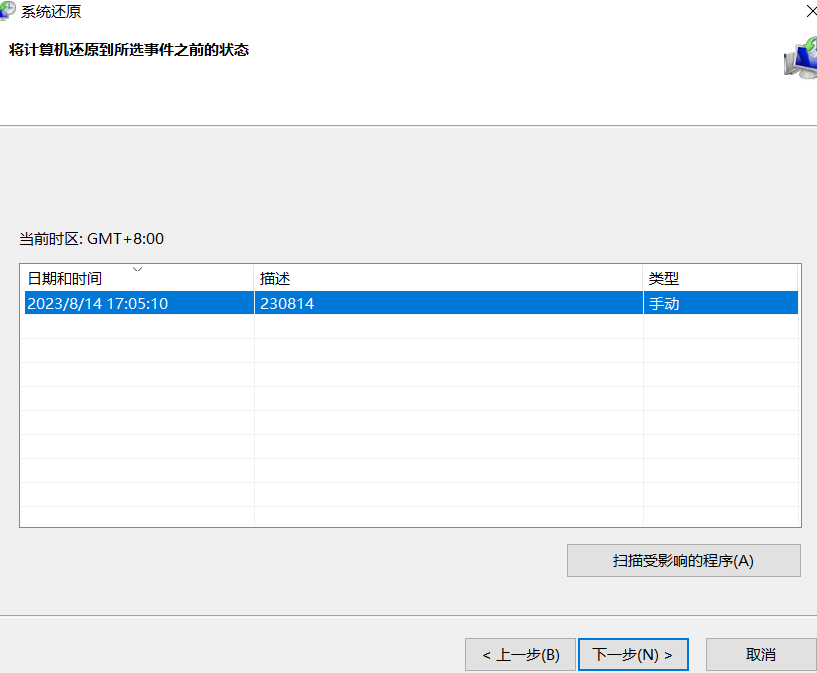
恢复到某个还原点：

> control

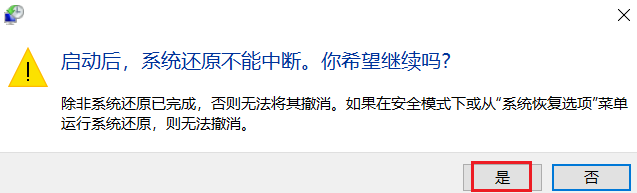










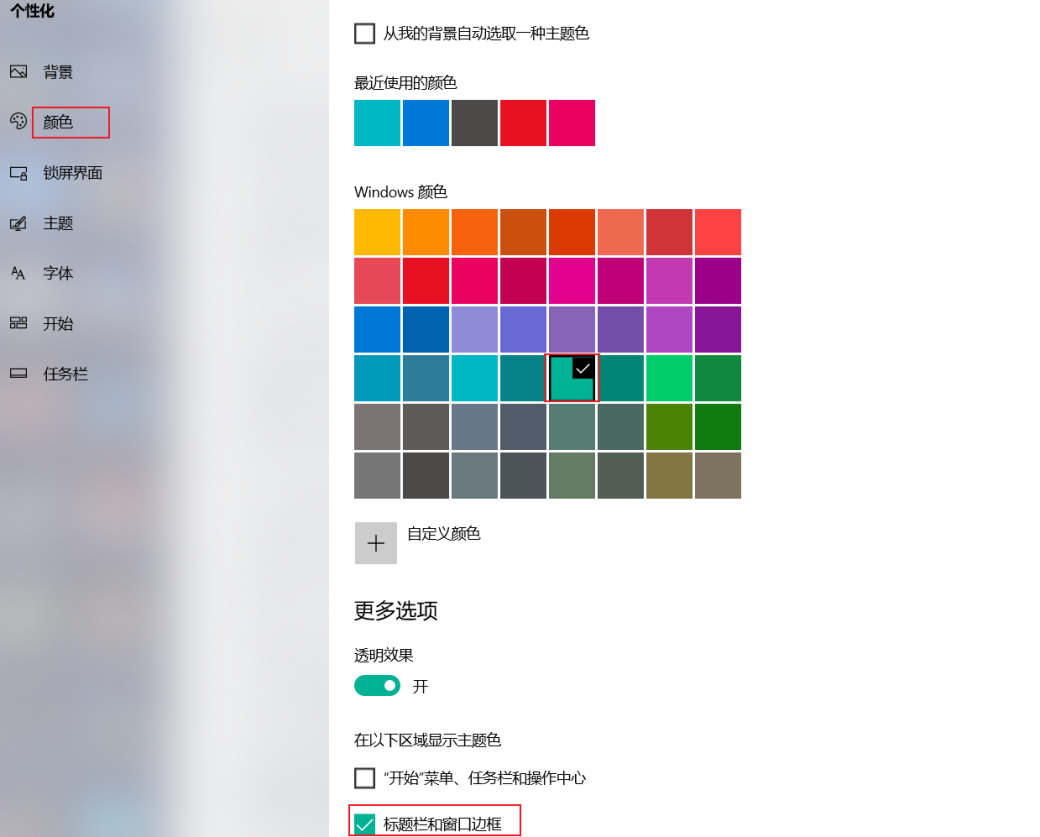


**★个性化标题栏颜色**

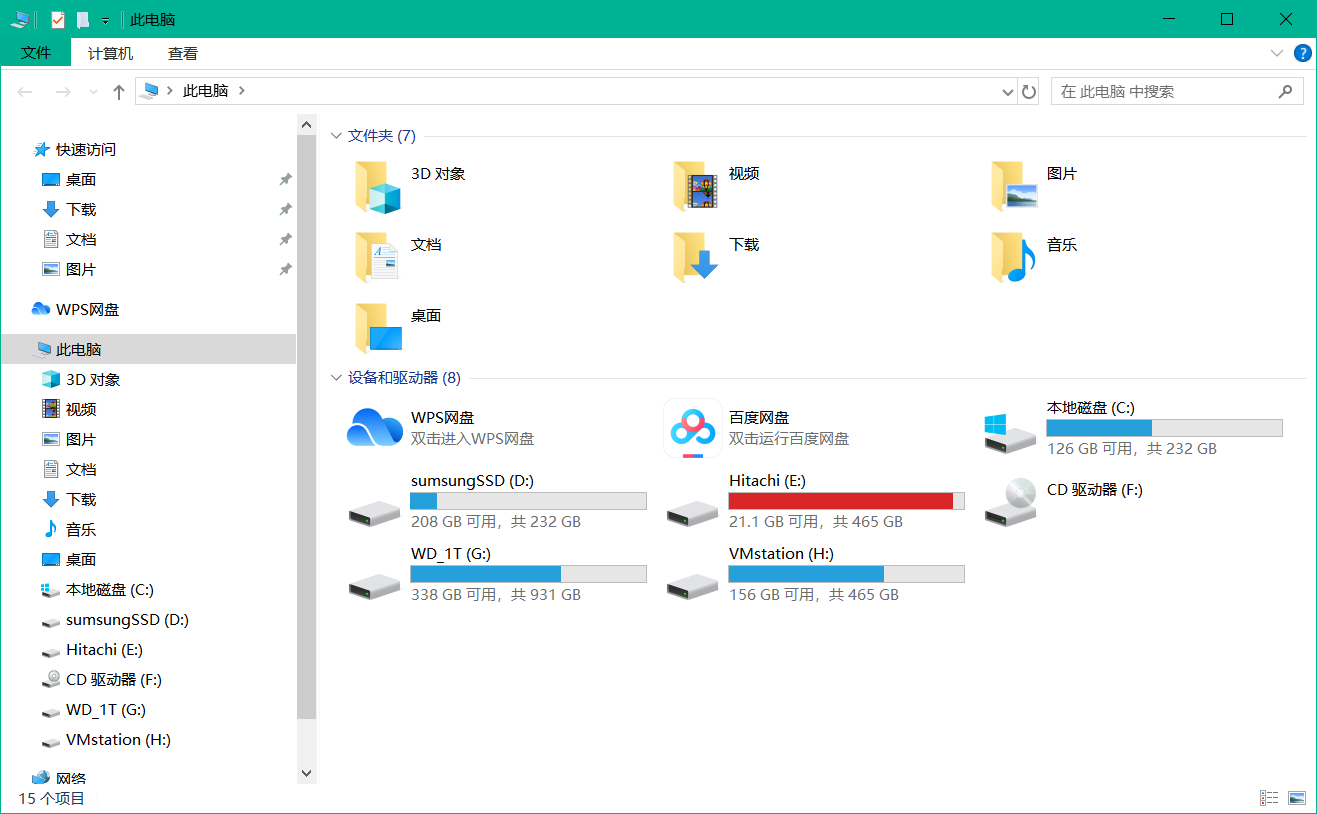
windows 10默认标题栏颜色为白色，不易区分当前窗口是哪个窗口

桌面右击→修改化→颜色

选取一种颜色，勾选“标题栏和窗口边框”

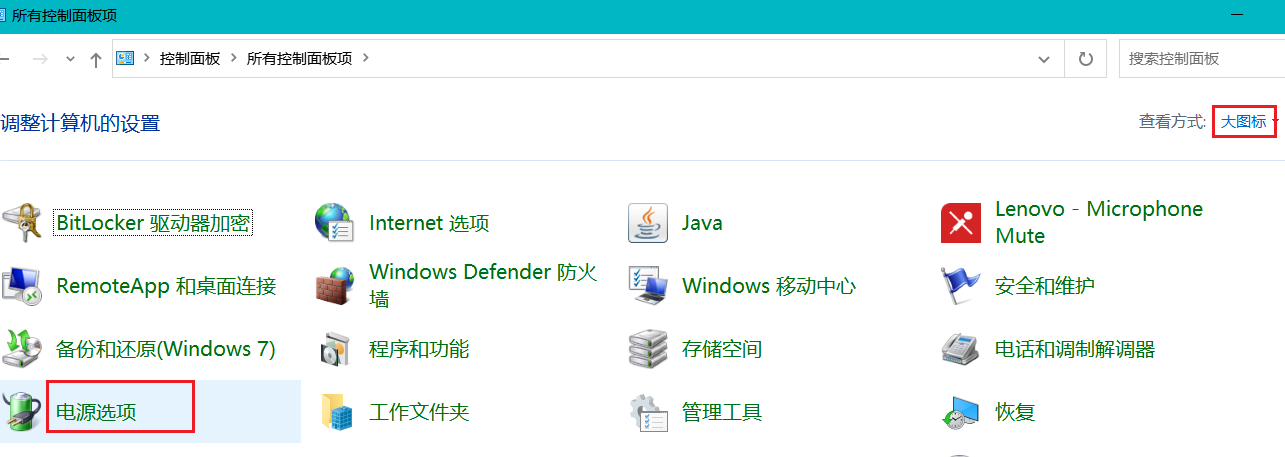


效果如下：



**★关闭快速启动**

> control →控制面板→所有控制面板项→电源选项→选择电源按钮的功能





点击“更改当前不可用的设置”





最后保存修改

**★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

**★windows激活方式**

> slmgr.vbs -dlv



激活方式：

|  |  |
| --- | --- |
| 产品密钥激活 | 联网时，直接输入安装光盘包装盒上的密钥或者从windows商城购买的密钥，MSDN订阅送的密钥即可 |
| OEM激活 | 电脑主板里BIOS里含有特定品牌的字符串SLIC  操作系统里含有对应品牌的OEM证书文件  安装序列号为对应品牌的OEM Key  电脑开机时，只需要以上三者吻合就给予系统激活，不同联网 |
| KMS激活 | 主要用于企业计算机的批量激活方式，VOL密钥，设置一个kms激活服务器，客户端电脑安装密钥，指定kms服务器即可，  特点：每180天得再激活一次 |
| 电话激活 | SLUI 4，提供9组ID给电话机器人客服，获取8组确认ID即可激活 |
| 数字证书激活 | 联网自动激活，在云端微软的服务器上记录主板信息，就算重装系统，不用密钥也能联网自动激活（要求版本对应得上） |
| 模拟OEM激活 | 伪造出OEM激活需要的几样文件，激活工具有：  CHEW-WGA Windows 7 Loader OEM7f7 |
| 伪kms激活 | 伪造kms激活服务器，模拟发送激活信息，激活工具有：  kmspico kms10 HEU kms |
| 去除windows激活技术 | 使用Remove WAT工具，对激活时钟文件实施暴力，使30天激活倒计时彻底停摆（系统不可更新）删除系统的WAT服务 |

激活渠道：

|  |  |
| --- | --- |
| Retail Channel | 零售 |
| Volume\_MAK Channel | 批量授权，用MAK密钥激活 |
| Volume\_KMSClient Channel | 批量授权，用KMS密钥激活 |
| OEM\_COA\_NSLP Channel | OEM非锁定预装 |
| OEM\_DM | 数字证书 |

MOLP微软开放式许可：

|  |  |
| --- | --- |
| VOL MAK | Multiple Activation Key 多次重复激活 |
| VOL GVLK | Generic Volume License Key 用于kms客户端的通用密钥 |
| VOL CSVLK | Custom Service License Key 用于密钥管理服务主机的授权密钥 |
| OEM SLP | System Locked Pre-installation 微软颁发给大的OEM厂商使用的离线激活密钥，需要通过bios的slic字段的验证 |
| OEM NONSLP | Non SLP 微软颁发给小OEM厂商的与零售版类似，需在线激活 |
| OEM COA | Certificate Of Authentication 是OEM电脑随机附带光盘的密钥，与零售版一样，在线激活 |
| OEM DM | 数字权利证书激活，OEM厂商的 |

SLIC（Software Licensing Internal Code）软件许可内部码

**★windows密码重置方法**

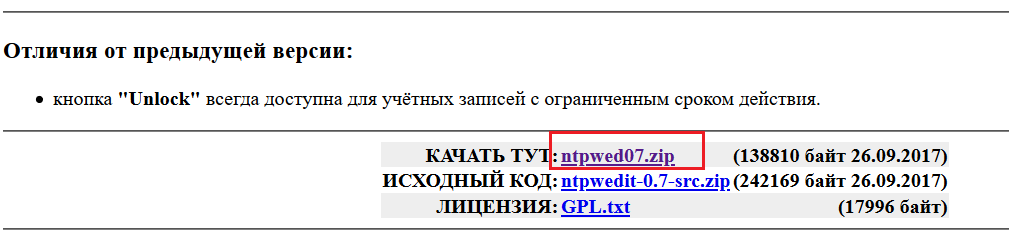
windows操作系统保存用户账号密码的文件为 C:\Windows\System32\config\SAM

重置密码或者清空密码时，就是直接操作这个文件，但当此文件在系统正常使用时是无权限修改的，一般是将要重置密码的服务器关机，然后插入PE系统的启动盘，从PE系统启动，到PE系统里使用相应的软件去修改原系统盘上的 \Windows\System32\config\SAM文件。有时由于特殊情况（比如此服务器为云上的虚拟机，无法挂载pe光盘）无法从pe系统启动，只能将虚拟机的磁盘取消挂载，再挂载到其他能登录的服务器上

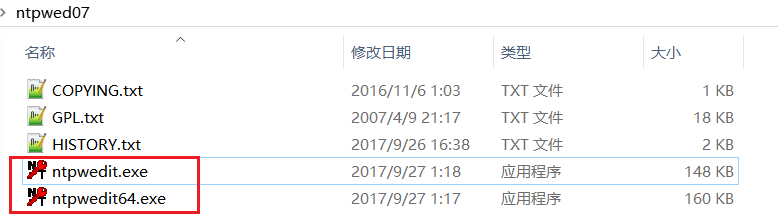
**★windows下重置**

无论是win PE系统还是正式的windows系统，可以使用的重置密码软件有ntpwedit

官网： http://cdslow.org.ru/ntpwedit/



点击**[ntpwed07.zip](http://cdslow.org.ru/files/ntpwedit/ntpwed07.zip)**进行下载，解压后里面有32位及64位的程序，可直接双击运行



也可放到PE系统里运行

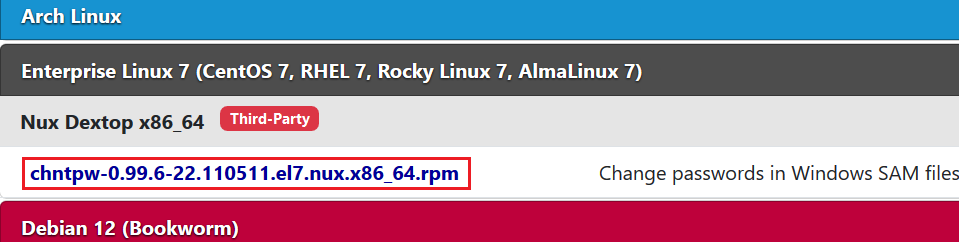
①PE里可直接使用ntpwedit编辑原系统盘的\Windows\System32\config\SAM文件重置密码

②windows系统里，得把原系统盘拔下，插入其他电脑（windows）去重置，其他电脑运行ntpwedit软件，找到\Windows\System32\config\SAM文件去重置，此时这个原系统盘的盘符不再是C盘，得留意，选择相应的盘符

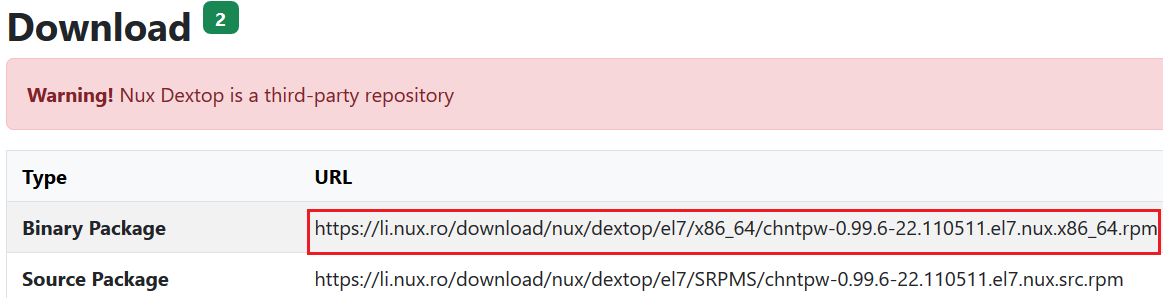
**★linux下重置**

linux下也有相应的工具软件可重置windows操作系统的密码：chntpw

官网： https://pkgs.org/download/chntpw



选择目标linux发行版本的软件包



选择下载二进制文件，复制url下载

https://li.nux.ro/download/nux/dextop/el7/x86\_64/chntpw-0.99.6-22.110511.el7.nux.x86\_64.rpm

下载后，传到centos7服务器里，直接安装即可

# yum install chntpw-0.99.6-22.110511.el7.nux.x86\_64.rpm

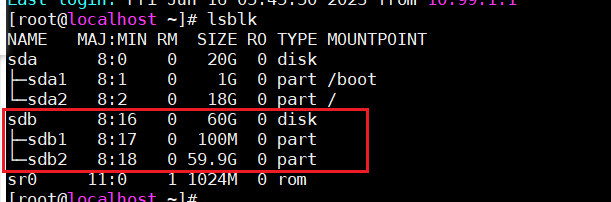
linux上挂载windows系统盘时需要用到ntfs文件系统驱动，安装方法如下：

# yum install epel-release #安装epel的yum源

# yum install ntfs-3g 或者 yum install ntfsprogs

然后，把原系统盘拔下，插入其他电脑（centos7）去重置，其他电脑将原系统盘挂载到某目录下（如/mnt）再运行chntpw程序

# lsblk #查看分区情况，一般带有若干个小分区的100M,300M这些，这个磁盘就是windows系统盘



# mount -t ntfs-3g /dev/sdb2 /mnt #挂载NTFS分区（一般为较大的那个分区，不是100M，也不是300M这些小分区）

# ls -l /mnt #查看里面是否有windows系统盘相关的目录，有即可开始操作

#先备份SAM密码文件

# cp /mnt/Windows/System32/config/SAM /mnt/Windows/System32/config/SAM.bak

# chntpw -u Administrator /mnt/Windows/System32/config/SAM #编辑SAM文件

Failed login count: 0, while max tries is: 0 #这个Failed不是报错，只是SAM文件里的相关信息

Total login count: 4 #此SAM文件里一共有4个账号

- - - - User Edit Menu:

1 - Clear (blank) user password

2 - Edit (set new) user password (careful with this on XP or Vista)

3 - Promote user (make user an administrator)

(4 - Unlock and enable user account) [seems unlocked already]

q - Quit editing user, back to user select

Select: [q] > 1 #选择1，清空密码

Password cleared!

Hives that have changed:

# Name

0 </mnt/Windows/System32/config/SAM>

Write hive files? (y/n) [n] : y #输入y，保存更改

0 </mnt/Windows/System32/config/SAM> - OK

**如果要重置为新的密码，则：**

- - - - User Edit Menu:

1 - Clear (blank) user password

2 - Edit (set new) user password (careful with this on XP or Vista)

3 - Promote user (make user an administrator)

(4 - Unlock and enable user account) [seems unlocked already]

q - Quit editing user, back to user select

Select: [q] > 2 #选择2，设置新密码

New Password: newpasswdxx #输入新密码，屏幕上是显示的

Password changed!

Hives that have changed:

# Name

0 <SAM.bak>

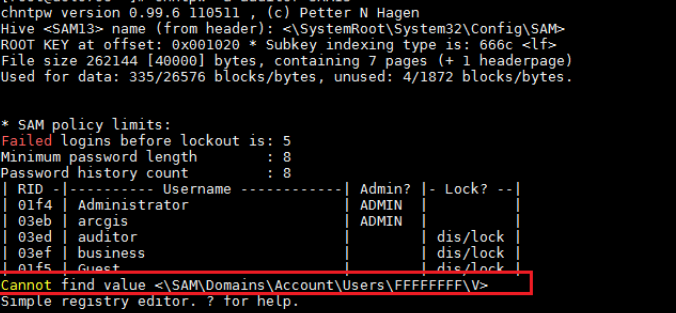
Write hive files? (y/n) [n] : y #输入y，保存更改

0 <SAM.bak> - OK

#然后，取消挂载，将原系统盘插回原服务器，再开机即可无需密码进入系统

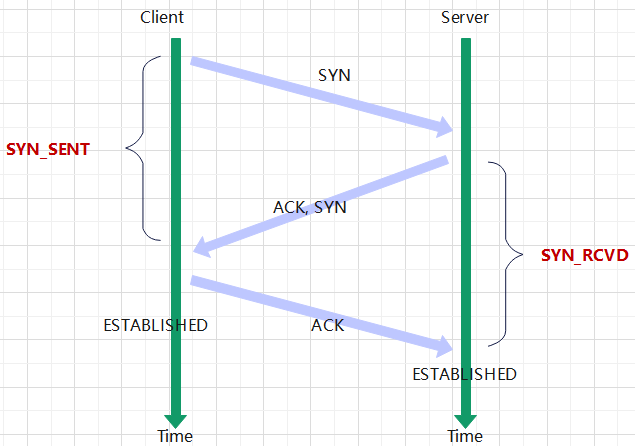
# umount /mnt #取消挂载

★有时linux下无法重置SAM文件密码，可以将SAM文件复制到windows上使用ntpwedit64.exe工具去重置密码



**★TCP连接超时问题**

**①TCP建立连接（三次握手）**

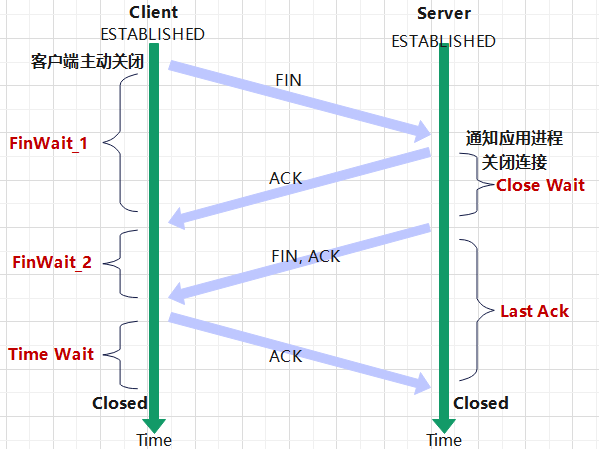


**仅2个超时：**

SYN\_SENT（TCPinitialRTT）等对方回ACK, SYN

SYN\_RCVD 等发起方回复最后一个ACK

**②TCP双向关闭（四次挥手）**



**5个超时：**

|  |  |
| --- | --- |
| FinWait\_1 | （KeepAliveInterval）windows默认1秒；linux开始1秒，重试依次翻倍 |
| CloseWait | （KeepAliveTime）windows及linux默认2小时 |
| FinWait\_2 | （TCPFinWait2Delay）windows默认240秒， |
| LastAck | （KeepAliveInterval）同FinWait\_1 |
| TimeWait | （默认2倍MSL时间）**MSL时间**（Maximum Segment Lifetime），报文最大生存时间，根据操作系统而异：windows 120秒，Linux 60秒，Unix 30秒 |

Windows系统 TCP超时

|  |  |
| --- | --- |
| KeepAliveInterval  （Finwait\_1, LastAck） | HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters  缺省1000毫秒 |
| KeepAliveTime  （CloseWait） | HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters  缺省7200 000毫秒，2小时（建议设置300000五分钟） |
| TCPFinWait2Delay  （FinWait\_2） | HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters  缺省240秒（可设置范围30~300） |
| TcpTimedWaitDelay  （TimeWait） | HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters  缺省240秒（可设置范围30~300） |
| TcpMaxConnectRetries | 建议3次 |
| TcpMaxDataRetransmissions  TcpMaxDataRetries | 建议3次 |
| TCPInitialRTT | SYN连接超时，默认3秒 |

**★Putty会话保存**

putty保存的会话位于注册表里

> regedit

HKEY\_CURRENT\_USER\Software\Simon Tatham\Putty\Sessions