**windows默认共享的打开和关闭**

windows默认共享的打开和关闭

Windows启动时都会默认打开admin$ ipc$ 和每个盘符的共享，对于不必要的默认共享，一般都会把它取消掉，可当又需要打开此默认共享时，又该从哪里设置呢，一般来说有两个地方，MSDOS命令和计算机管理共享文件夹，下面主要从DOS命令来设置，因为比较简单，也可进行批处理。

一、因为Windows是默认打开默认共享的，还是先从删除默认共享开始吧：

首先从[注册表](https://so.csdn.net/so/search?q=%E6%B3%A8%E5%86%8C%E8%A1%A8&spm=1001.2101.3001.7020)里永久禁止打开默认共享：

如果要禁止C$、D$、E$一类的共享，可以单击“开始→运行”命令，在运行窗口键入“Regedit”后回车，打开注册表编辑器。依次展开[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters ]分支，将右侧窗口中的DOWRD值“AutoShareServer”设置为“0”即可。  
如果要禁止ADMIN$共享，可以在同样的分支下，将右侧窗口中的DOWRD值“AutoShareWKs” 设置为“0”即可。  
如果要禁止IPC$共享，可以在注册表编辑器中依次展开[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]分支，将右侧窗口中的DOWRD值“restrictanonymous”设置值为“1”即可。

当不想改动注册表，或只是临时删除这些共享时，可以使用 net share 命令：

输入net share 命令时可以查看当前所有的共享

**net share c$ /del  
net share d$ /del  
net share ipc$ /del  
net share admin$ /del**

想每次开机后自动删除默认共享，只需把上面的命令保存为.bat文件，开机自动运行就可以了

二、打开默认共享：

先在控制面板的“服务”，看SERVER服务是否启动，如果没有启动，则将设置为自动或者手动，然后再选择启动。  
开启系统的默认共享的方法  
1.检查AutoShareServer和AutoShareWks注册表值是否为0。  
2.找到注册表中的HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters。  
3.将下面子项中的AutoShareServer和AutoShareWks DWORD值改为1。  
4.重启。通常Win2003、Win2000\XP会在启动时自动创建。  
5.启动后，可以通过运行CMD命令进入命令行模式，再运行net share，再共享列表中会看到Admin$、C$\IPC$等默认共享。  
  注意：如果按以上方法仍无效。可能是病毒或恶意程序破坏了系统，这时因先杀毒和恢复系统。  
  此外关闭Server服务、在网卡上去掉Microsoft客户端驱以及在网卡上去掉“文件和打印共享”等都会关闭默认共享。此时要将相应项恢复设置。  
  
  
也可以在开始菜单的运行中输入CMD，然后输入以下的命令  
**net share c$=c:  
net share d$=d:  
net share ipc$  
net share admin$**

在计算机管理中的共享文件中也可以对所有的共享目录进行设置，右键“我的电脑”->“管理”->“共享文件”，由于是图形界面比较简单，这里就不在详细说明。

在Windows  2000/XP系统中，隐藏着一种据说是可以“致命”的漏洞，它让很多人一听到就谈“虎”色变。在“我的电脑”上右击“管理”，依次选择“系统工具→共享文件夹→共享”，就会看到右边窗口中的默认共享(见图1)。这些带有美元“$”标记的符号就是Windows系统默认共享，也就是Windows在安装完毕后自动共享的功能，很多人都听说是个漏洞。  
  
IPC$、ADMIN$、C$、D$都是什么?  
  
IPC$(Internet Process Connection)可以被理解为一种“专用管道”，可以在连接双方建立一条安全的通道，实现对远程计算机的访问。Windows NT/2000/XP提供了IPC$功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑共享(C$,D$,E$……)和系统目录(ADMIN$)共享。所有这些共享的目的，都是为了方便管理员的管理，但在有意无意中，导致了系统安全性的隐患。  
  
微软在不经意间造成的隐患，引起了很多关注，关于他们的种种说法也流传于网络间。看看下面几种流行的理论，你是不是也有同样的看法呢?  
  
观点一：默认共享本身就是漏洞，因此要避免安全隐患，必须删除所有的默认共享。  
  
观点二：默认共享就好像普通共享一样，任何人都可以随意使用ADMIN$，C$，D$等共享从你电脑里偷东西。  
  
观点三：IPC$是可以删除的，而且不会再次出现。  
  
观点四：要想删除默认共享，只要在Windows开机脚本中创建一个批处理文件就能实现。  
  
答1:既然默认共享是漏洞，微软干嘛不补上?其实默认共享是一项非常有用的功能，只是我们平时用不到罢了。微软的初衷是便于网管进行远程管理。试想一下。在一个大型网络里。管理员有必要亲自跑到某台机上去看一些东西或是删除一些东西吗?这些管理员坐在主机前通过默认共享可以很轻松地办到。这是微软为了方便管理而提供的功能。不知从什么时候开始，它变成人家口中所说的漏洞了。  
  
答2:如果你开放了所有的默认共享。人家就可以利用默认共享到你电脑里偷东西吗?答案是否定的。除非是你自己想放他进来。默认共享是管理员级别或是有相对应权限的账户的操作。你试试guest级用户能使用默认共享吗?不能!为什么说是你自己想放别人进来呢?你问问自己。你的管理员密码呢?要么直接为空。要么就是些123，1234之类的弱口令。用扫描工具短短时间内就能被猜解的。你已经打开了大门，人家有什么理由不进来呢?  
  
就算是你密码为空或是弱口令，对方也不一定能用默认共享进入你的电脑进行管理员级别的操作。为什么?当共享方式为仅来宾方式时。任何连接的用户权限只能是guest级别的。guest能有多少权限?不信你可以做一次实验。向一台启用了仅来宾且开放默认共享的主机用net use命令进行连接。例如:net use \\ip\IPC$ "password" /user:"administrator"我可以肯定的告诉你：无论你的password填的是什么。都会提醒你"命令成功完成"。你实际上得到了管理员权限吗?答案是否定的。你得到的只是guest权限。很庆幸的是，Windows XP安装后的默认共享方式就是"仅来宾"的方式。  
  
答3:Windows 2000下IPC$共享是可以删除的，然而在XP下就不行了。网上产生这种说法无非是没有亲身体会直接把Windows 2000下的理论搬到了XP吧。让我们看看微软是怎么说的:“服务器服务需要使用默认 IPC$ 系统管理共享。因此，您不可以删除此共享，我们建议您不要删除由 Windows 为根分区和卷创建的(如 C$)和为系统根文件夹创建的 (ADMIN$) 系统管理共享。删除这些文件夹可能会给依赖这些共享的管理员和程序或服务带来问题。” 看到了吧，只要服务器服务"Server"正在运行当中，你就不可能删除IPC$。试图删除只会出现"拒绝访问"的错误提示。当你停止了Server服务后。IPC$会自动消失。  
  
答4:创建脚本的确可以删除默认共享。但网上很多人都会提到通过组策略配置开机脚本。事实上。创建开机脚本并不能删除默认共享。如果不信大家可以去试一试。按网上的说法利用net share命令删除共享创建一个批处理脚本。然后加入到组策略当中“计算机配置→Windows 设置→脚本(启动/关闭)”去，重启后再用net share命令查看一下。你会发现：默认共享并没有被删除!这个脚本没有起作用。  
  
总结:  
  
默认共享并不是个漏洞。造成安全隐患的并不是默认共享本身。而是系统使用者本身。大家在看网上或书上的一些文章的时候。尽量经过自已亲自动手实践才能证明是否正确，有很多东西你传我我传你，传来传去就变了味。  
  
建议:  
  
1.Windows的漏洞是一个接着一个。除了及时的补丁。安装杀毒软件和防火墙外。我们自己能做的就是给自己的管理员账号设置一个强有力的密码!特别要注意的是administrator内置管理员账号。很多人的系统这个账号没有被禁用且密码为空。我们虽然并不必要符合Windows要求的密码复杂性。但最好采用一些人家并不了解而你自己熟悉的数字加字母的密码。  
  
2.利用注册表关闭默认共享的方法:  
  
打开注册表。在HKEY\_LOCAL\_MACHINE \SYSTEM \CurrentControlSet \Services \lanmanserver \parameters下建立一个DWORD值，将AutoShareServer和AutoShareWks数值配置为0即可!  
  
3.杀毒软件和防火墙是必要的。奉劝那些自认为自己高手而拿机器在网上"裸奔"的人。常在河边走，怎能不湿鞋? 不要过分相信自己的能力!