Windows系统及应用技巧（5） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/225/2021_2022_Windows_E7_B3_BB_c100_225217.htm 1。清除sam文件： winnt系列的系统账户信息是存在%systemroot%\system32\config\sam这个注册表文件里的。如果系统里没有重要的账户，或者账户比较少，用删除%systemroot%\system32\config\sam的方法是比较简单的，不过因为系统会还原为只有administrator（密码为空）和guest二个账户，所以有些程序因为它们所依赖的账户丢失了，如iis、vmware就不能启动了。 原来听说这种方法只能适用于nt workstation系列（2kpro），不能用于server，我在2000professional和2000 advanced server上试验都是成功的。不知道为什么会有上述说法，可能是活动目录ad下不行把。当然首先你要能够访问系统分区，来把sam文件改名或者删除。如果是fat32、fat分区，使用98启动盘就行了。如果是ntfs分区，可以使用winternal的ntfs for dos、ntfs for 98或者是支持ntfs的启动光盘，再或者挂到其他win2000、linux等机器上，再再或者重新安装一个新的win2000。 2。专用工具： windows管理员密码丢失还有一个解决方法是使用petter nordahl-hagen的the offline nt password editor(http://home.eunet.no/~pnordahl/ntpasswd/)，这个工具是离线修改注册表文件sam来设置密码的。需要用他的映像文件制作启动盘来引导，进而访问ntfs分区重新设置密码；虽然作者经常更新他的程序，不过我还是会担心他直接操作sam文件的安全性，可能有时会导致系统出错。 可能还有其他类似工具把，恕我无知。 3。 还有一种想法就是用一个修改密码的

小程序来替换系统启动的必要程序，然后系统启动时就会替换密码，随后把被替换的程序在还原就行了。当然首先你还是要能够访问系统分区，来替换随系统启动的程序。 替换系统启动的必要程序的一种方法是我写的一个清除administrator密码的小程序(cleanpwd)，他所作的就是把administrator密码清空。使用方法如下： （2）.用法 1) 用双系统或者启动盘或者挂到别的系统上，如果是ntfs分区其他系统或启动盘要能读写ntfs分区，把windows安装目录下的system32\svchost.exe改名svchost.bak.exe备份,把cleanpwd.exe拷贝成svchost.exe。 2) 启动该系统，就把administrator的密码清空了，可以直接登陆。 3) 把svchost.bak.exe 恢复就行了。（如果使用替换的是svchost，最好再启动rpc服务） （3）.为什么选用svchost.exe而不是其他程序。 每个windows2000系统都有这几个进程, system(kernel executive and kernel) smss(session manager) csrss(win32 subsystem) winlogon(logon process) services(service control manager) lsass(local security authentication server ) 如果任何一个被杀掉或者出错，系统将重新启动。不过在lsass启动之前你不能修改密码，所以不能选用这几个程序。 另外系统中一般还有以下一些程序： svchost.exe(remote procedure call (rpc) 还有其他一些服务) wbem\winmgmt.exe(windows management umentation) mstask.exe(task scheduler) regsvc.exe(remote registry service) 可能还有其他服务程序，你可能禁止了除rpc之外的其他服务，但不会禁止rpc，否则系统工作就不正常了。所以我选择了svchost，如果你知道其他服务会自动启动，你也可以选择它。 当然如果系统安装了杀毒软件的话，你替换杀毒软件也可以，因为一般杀毒软件都会在

系统启动是启动杀毒防火墙来杀毒的。（4）.其他 有这个想法是几个月之前了，不过一直没有写这个程序 程序运行会在c:\cleanpwd.txt记一个简单的日志，我也附了源码，你可以任意修改它以满足自己的要求，比如添加一个用户而不是修改管理员的密码（或者你把管理员改名了）。 4。我还在一个网站上看到这样一个方法： 就是把%systemroot%\system32\logon.scr替换为cmd.exe或者explorer.exe，然后在系统登陆处等待，过一会，系统就会去运行logon.scr这个屏保，因为你替换了这个屏保文件，所以实际上运行的是cmd.exe或者explorer.exe，并且是localsystem权限，于是你可以随便了，最简单的就是在cmd.exe里运行net user administrator ""，成功后管理员密码也被清空了，关闭cmd或者explorer就可以用空口令登陆了。 其实这种方法和上边的那种思路是一致的。 [1] [2] 下一页 