


服务器安全加固

作者：XX

目录

- 
- 1 Windows系统安全加固
 - 2 Linux系统安全加固
 - 3 应用安全加固
 - 4 代码安全加固

1.1 操作系统安全的概念

- (1) 操作系统本身提供的安全功能和安全服务。目前的操作系统本身往往要提供一定的访问控制、认证与授权等方面的安全服务。
- (2) 针对各种常用的操作系统，进行相关配置，使之能正确对付和防御各种入侵。
- (3) 保证操作系统本身所提供的网络服务能得到安全配置。

1.2 Windows系统安全加固



1 账户、密码安全

2 共享安全

3 注册表安全

4 服务安全

5 策略安全

6 日志安全

7 其他安全（防病毒，补丁）

1.2.1 账户、密码安全

账户安全的第一原则：最小权限原则

最小特权原则是系统安全中最基本的原则之一。所谓最小特权(Least Privilege)，指的是"在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权"。最小特权原则，则是指"应限定网络中每个主体所必须的最小特权，确保可能的事故、错误、网络部件的篡改等原因造成的损失最小"。

账户安全是计算机系统安全的第一关，如果计算机系统账号被盗，那么计算机很危险，轻则入侵者可以任意控制计算机，重则泄露电脑内存储的重要资料，涉密信息以及个人信息等。

1.2.1 账户安全

默认账户安全

禁用Guest账户。

禁用或删除其他无用账户

操作步骤：

打开 控制面板 > 管理工具 > 计算机管理，在 系统工具 > 本地用户和组 > 用户 中，

双击 Guest 帐户，在属性中选中 帐户已禁用。

1.2.1 账户安全

设置用户组

按照用户分配帐户。根据业务要求，设定不同的用户和用户组。例如，管理员用户，数据库用户，审计用户，来宾用户等。

定期账户检查

定期检查并删除与无关帐户

定期删除或锁定与设备运行、维护等工作无关的帐户。

操作步骤

打开 控制面板 > 管理工具 > 计算机管理，在 系统工具 > 本地用户和组 中，删除或锁定与设备运行、维护等工作无关的帐户。

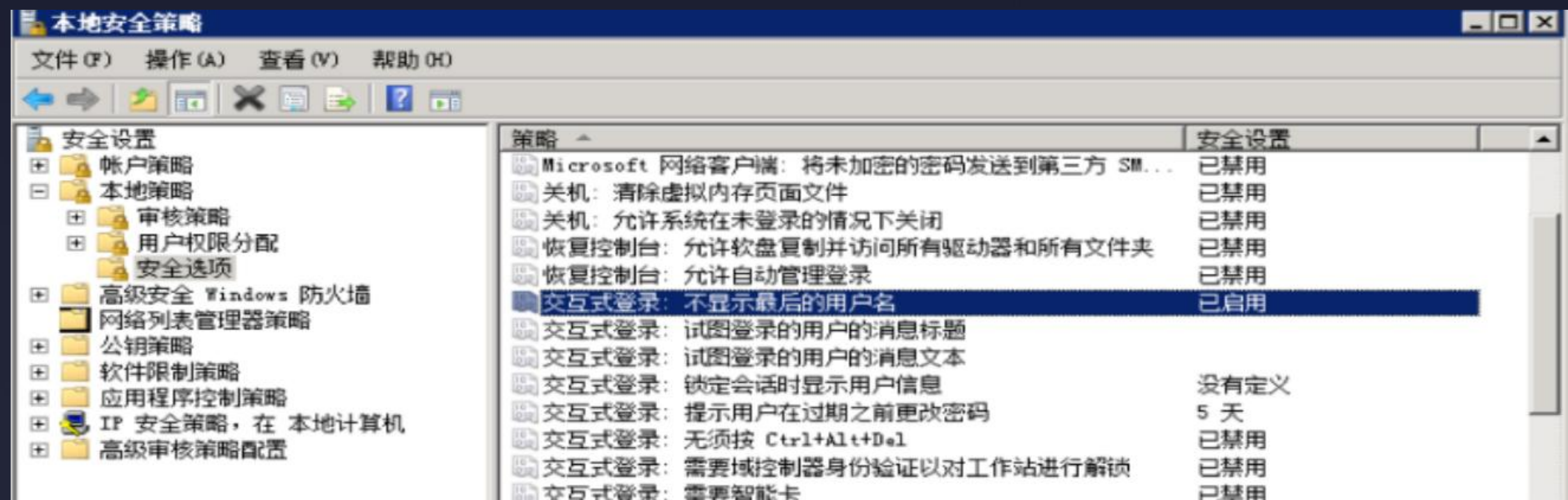
1.2.1 账户安全

不显示最后的用户名

配置登录登出后，不显示用户名称。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 安全选项 中，双击 交互式登录:不显示最后的用户名，选择 已启用并单击 确定。



1.2.1 账户安全

进阶

1. 隐藏账户 (浅隐藏)
2. 克隆账户 (深隐藏)

1.2.1 账户安全

隐藏账户的建立:

```
cmd> net user 用户名$ 密码 /add
cmd> net localgroup administrators 用户名$ /add
```

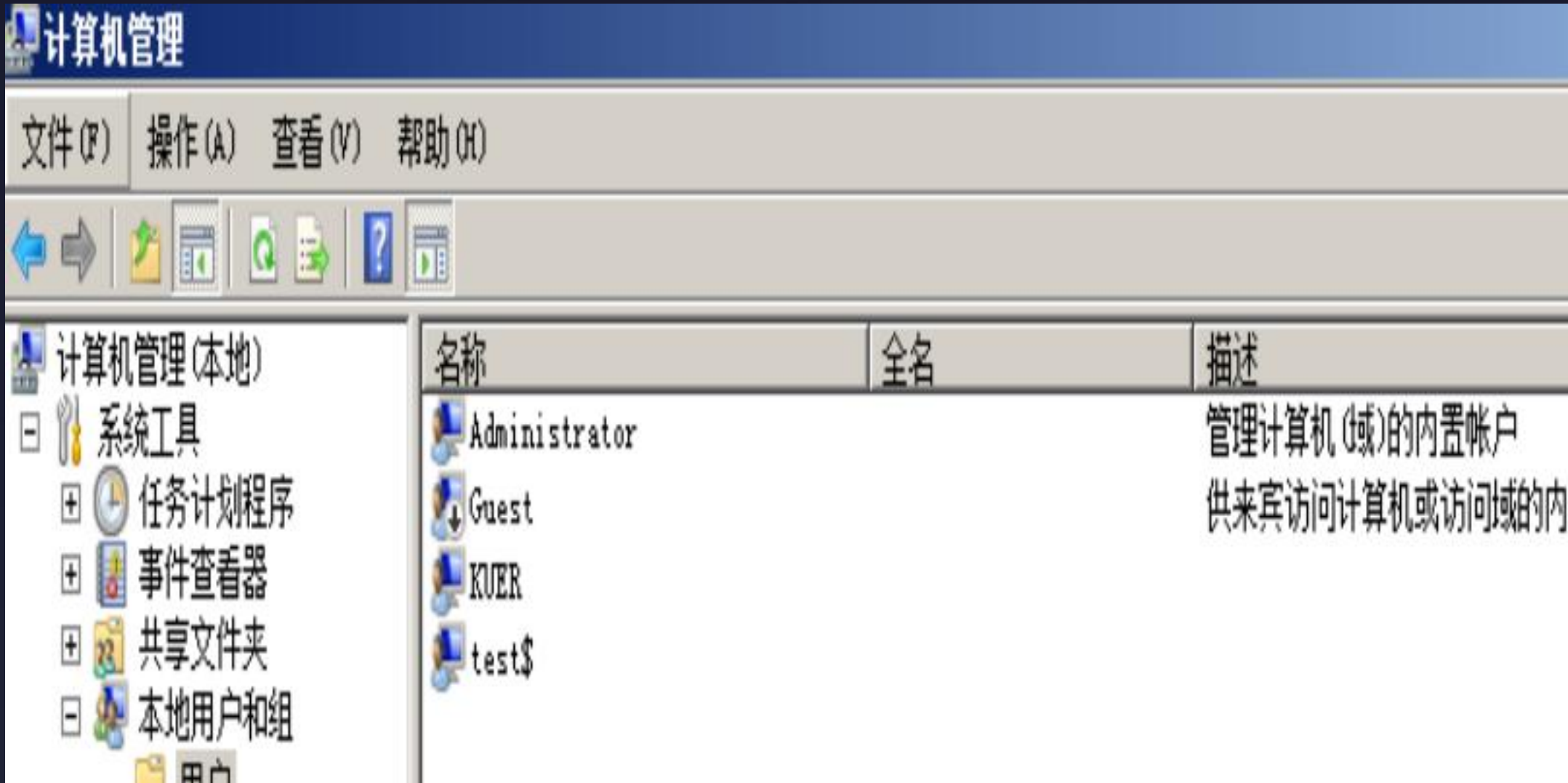
```
C:\Windows\system32>net user test$ /add
命令成功完成。

C:\Windows\system32>net user

\\WIN-5RRPLA984JU 的用户帐户

-----
Administrator          Guest          KUER
命令成功完成。

C:\Windows\system32>
```



1.2.1 账户安全

克隆账户：

参考：<https://3gstudent.github.io/>

- 1. `net user username$ password /add` 添加隐藏账户
- 2. 用注册表导出管理员权限和隐藏账户权限
- 3. 将隐藏账户hex头替换为管理员注册表hex头
- 4. 删掉隐藏账户 `net user username$ /del`
- 5. 导入隐藏账户注册表
- 6. 将注册表SAM权限隐藏（此时cmd 和用户账户看不到隐藏账户）

1.2.1 账户安全

克隆账户的检查:

1. 查看注册表 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\

当然，默认管理员权限无法查看，需要分配权限或是提升至Sytem权限

2. 隐藏帐户的登录记录，可通过查看日志获取

查看账户的登录等信息 net user 用户名

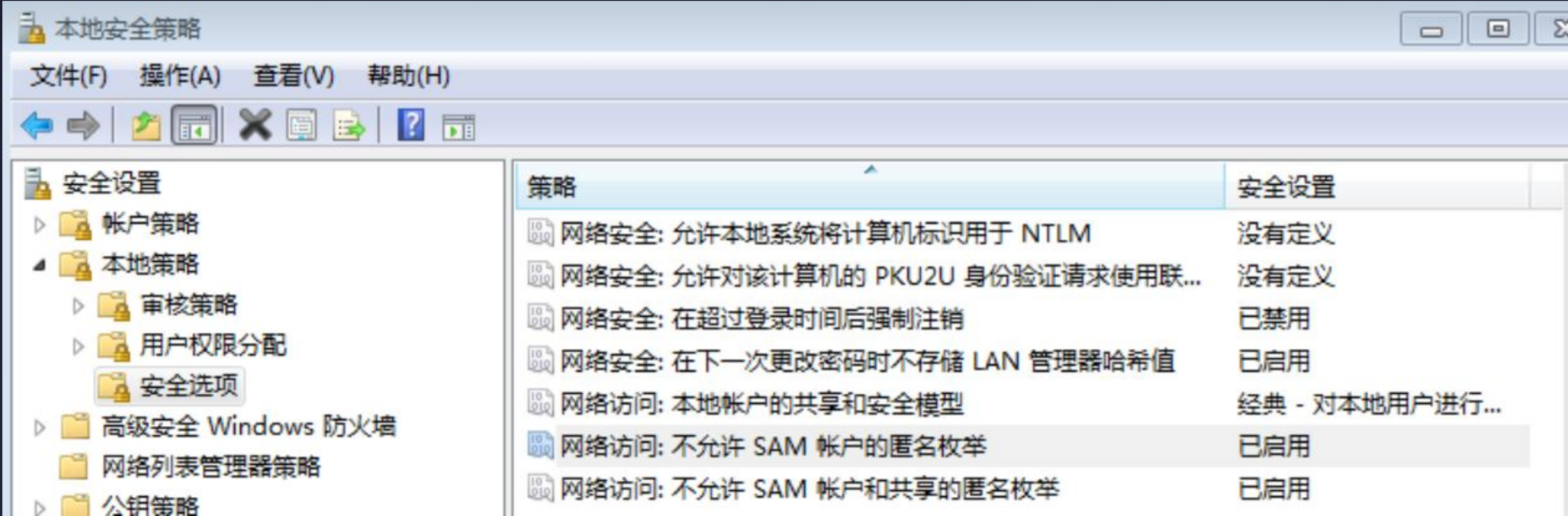
```
上次设置密码      2020/6/1 14:56:51
密码到期          从不
密码可更改        2020/6/1 14:56:51
需要密码          No
用户可以更改密码  Yes

允许的工作站      All
登录脚本
用户配置文件
主目录
上次登录          2020/6/9 13:39:44
```

1.2.1 账户安全

防止 账号克隆 的本地安全设置：

- 1. 控制面板---管理工具---本地安全策略选项
- 2. 将如图中的网络访问: 不允许 SAM 帐户的匿名枚举以及网络访问: 不允许 SAM 帐户和共享的匿名枚举启动



1.2.2 密码安全

1. BIOS密码（物理环境）

2. Windows登录密码

3. 其他应用系统密码

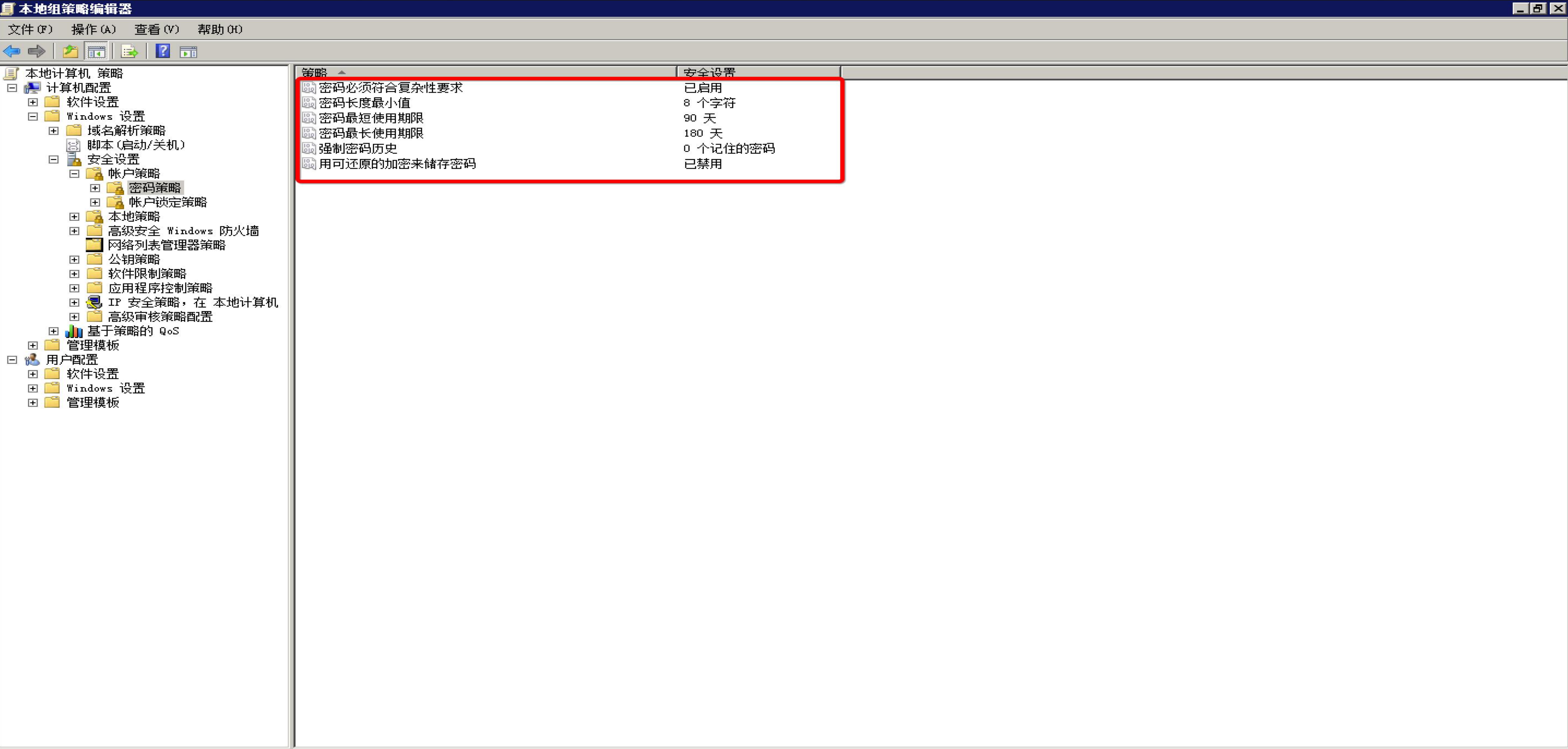
1.2.2 密码安全

密码复杂度必须满足以下策略：

1. 最短密码长度要求八个字符。（建议系统密码14位以上）
2. 启用本机组策略中密码必须符合复杂性要求的策略。即密码至少包含以下四种类别的字符中的两种或三种（三种为佳）：
 - a. 英语大写字母 A, B, C, ... Z
 - b. 英语小写字母 a, b, c, ... z
 - c. 西方阿拉伯数字 0, 1, 2, ... 9
 - d. 非字母数字字符，如标点符号，@, #, \$, %, &, *等
3. 禁止使用常见的弱密码，如Admin@123, Admin#123
4. 禁止使用和自己名称，公司名称，生日等相关作为密码。
5. 多次输入错误应锁定账户

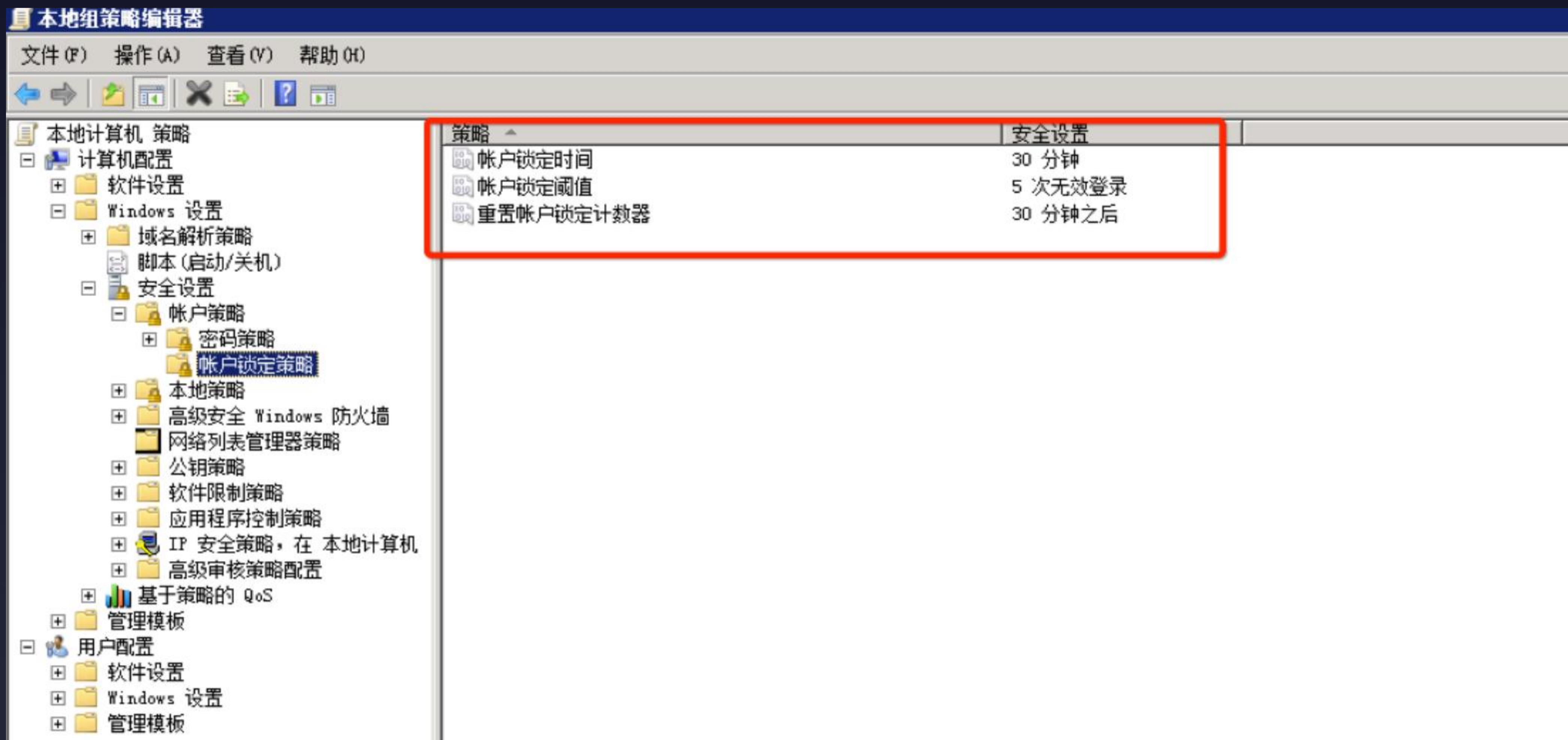
1.2.1 密码安全

控制面板 > 管理工具 > 本地安全策略，在 帐户策略 > 密码策略



1.2.1 密码安全

控制面板 > 管理工具 > 本地安全策略, 在 帐户策略 > 账户锁定策略



1.2.2 共享安全

1. 非域环境中，关闭Windows硬盘默认共享，例如C\$，D\$。

操作步骤

打开 注册表编辑器，根据推荐值修改注册表键值。

注意： Windows Server 2012版本已默认关闭Windows硬盘默认共享，且没有该注册表键值。

HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer

推荐值： 0

1.2.2 共享安全

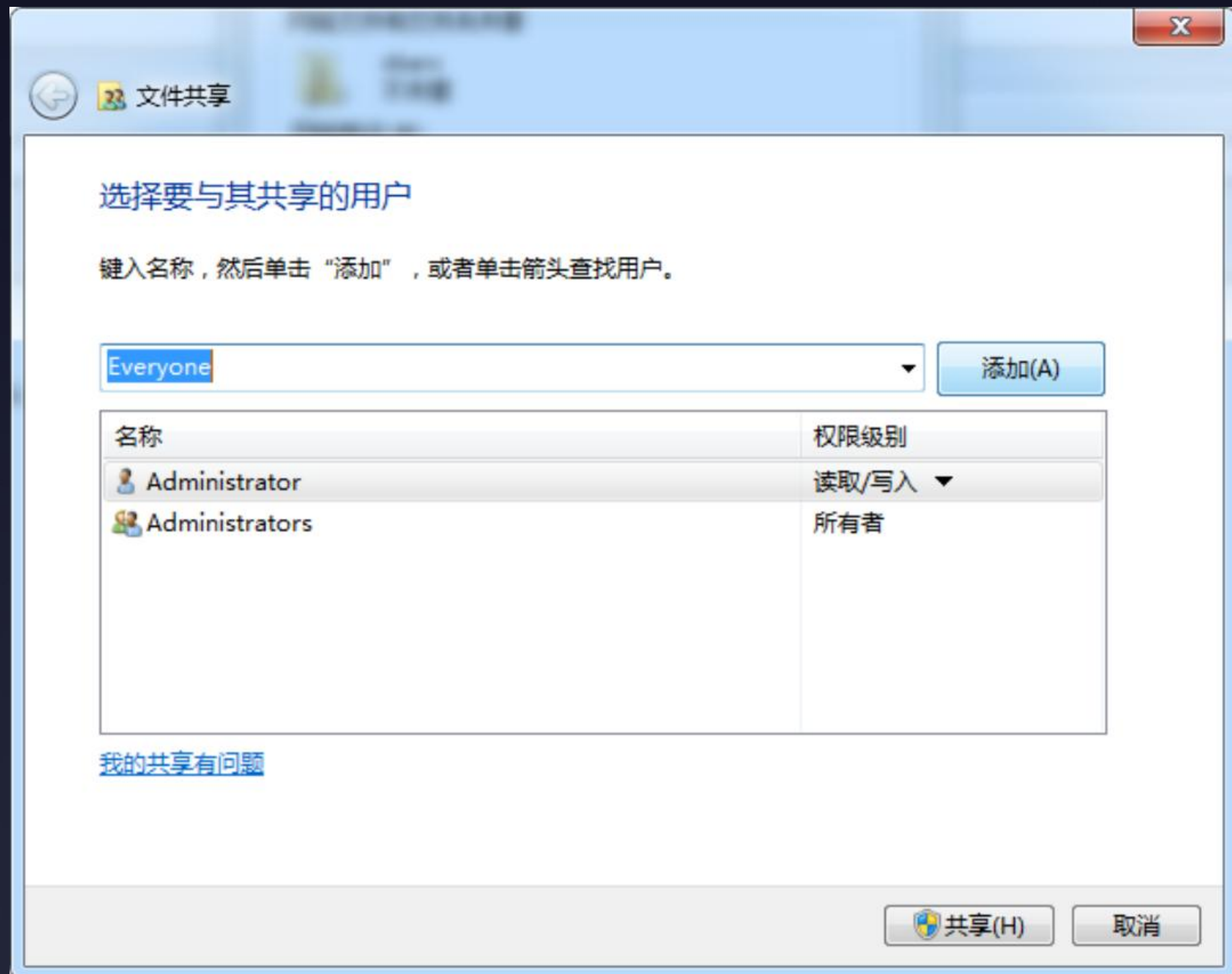
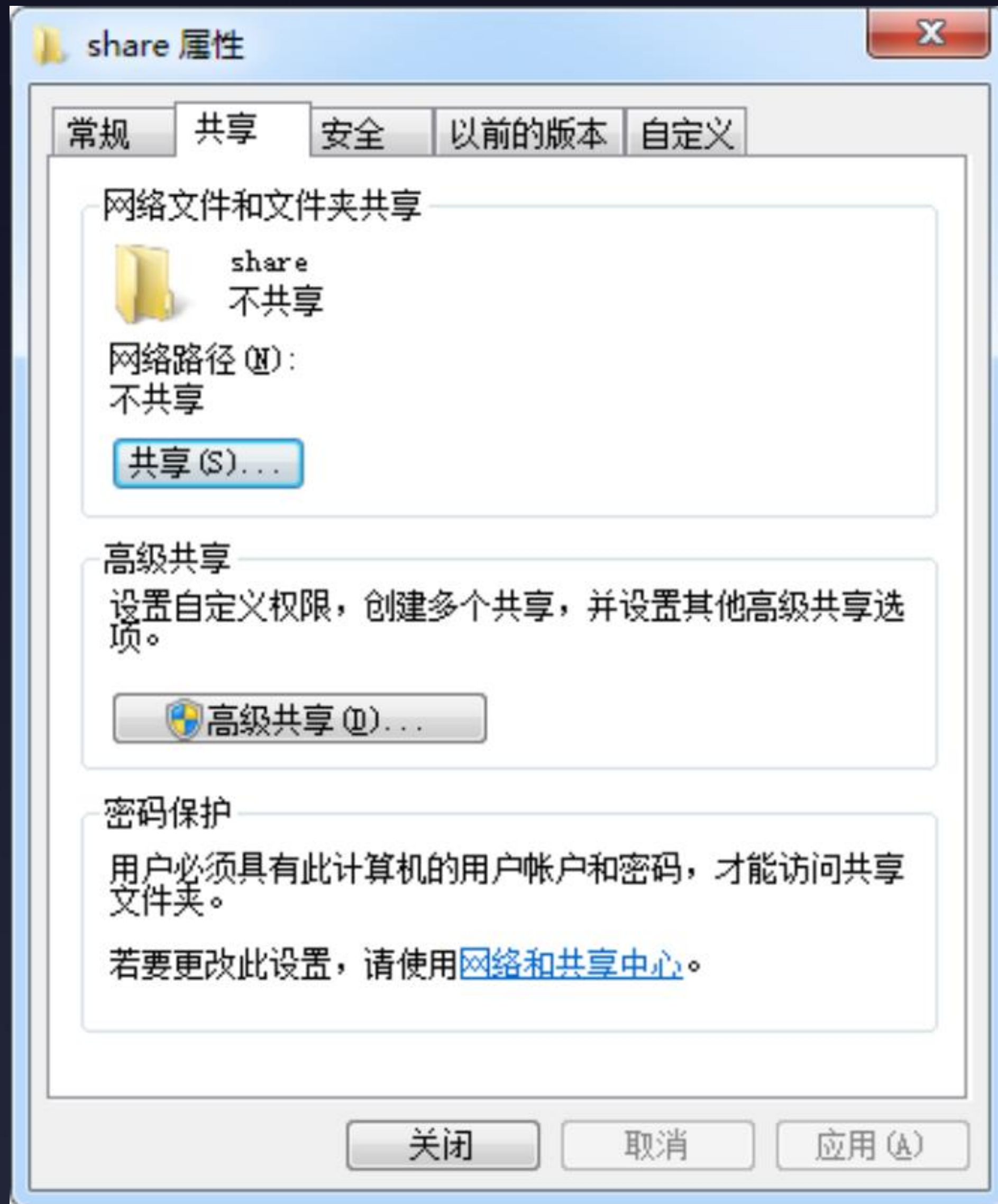
2. 共享文件夹授权访问

每个共享文件夹的共享权限，只允许授权的帐户拥有共享此文件夹的权限。

每个共享文件夹的共享权限仅限于业务需要，不要设置成为 Everyone。将共享文件的权限从“everyon”更改为“授权用户”，“everyone”意味着任何有权进入网络的用户都能够访问这些共享文件。

打开 控制面板 > 管理工具 > 计算机管理，在 共享文件夹 中，查看每个共享文件夹的共享权限。

1.2.2 共享安全



1.2.3 注册表安全

1. 通过注册表，用户可以轻易的添加、删除、修改windows系统内的软件配置信息或硬件驱动程序，这不仅方便了用户对系统软硬件的工作状态进行适时的调整，同时注册表也成为入侵者攻击的目标，通过注册表种植木马，修改软件信息，甚至删除、停用或改变硬件的工作状态。

HKEY_LOCAL_MACHINE包含关于本地计算机系统的信息，包括硬件和操作系统数据。

HKEY_CLASSES_ROOT包含由各种OLE技术使用的信息技术和文件类别关联数据。

HKEY_CURRENT_USER包括环境变量、桌面设置、网络连接、打印机和程序首选项。

HKEY_USERS关于动态加载的用户配置文件和默认的配置文件的的信息。有些信息和HKEY_CURRENT_USER交叉出现。

HKEY_CURRENT_CONFIG包含在启动时由本地计算机系统使用的硬件配置文件的相关信息。

1.2.3 注册表安全

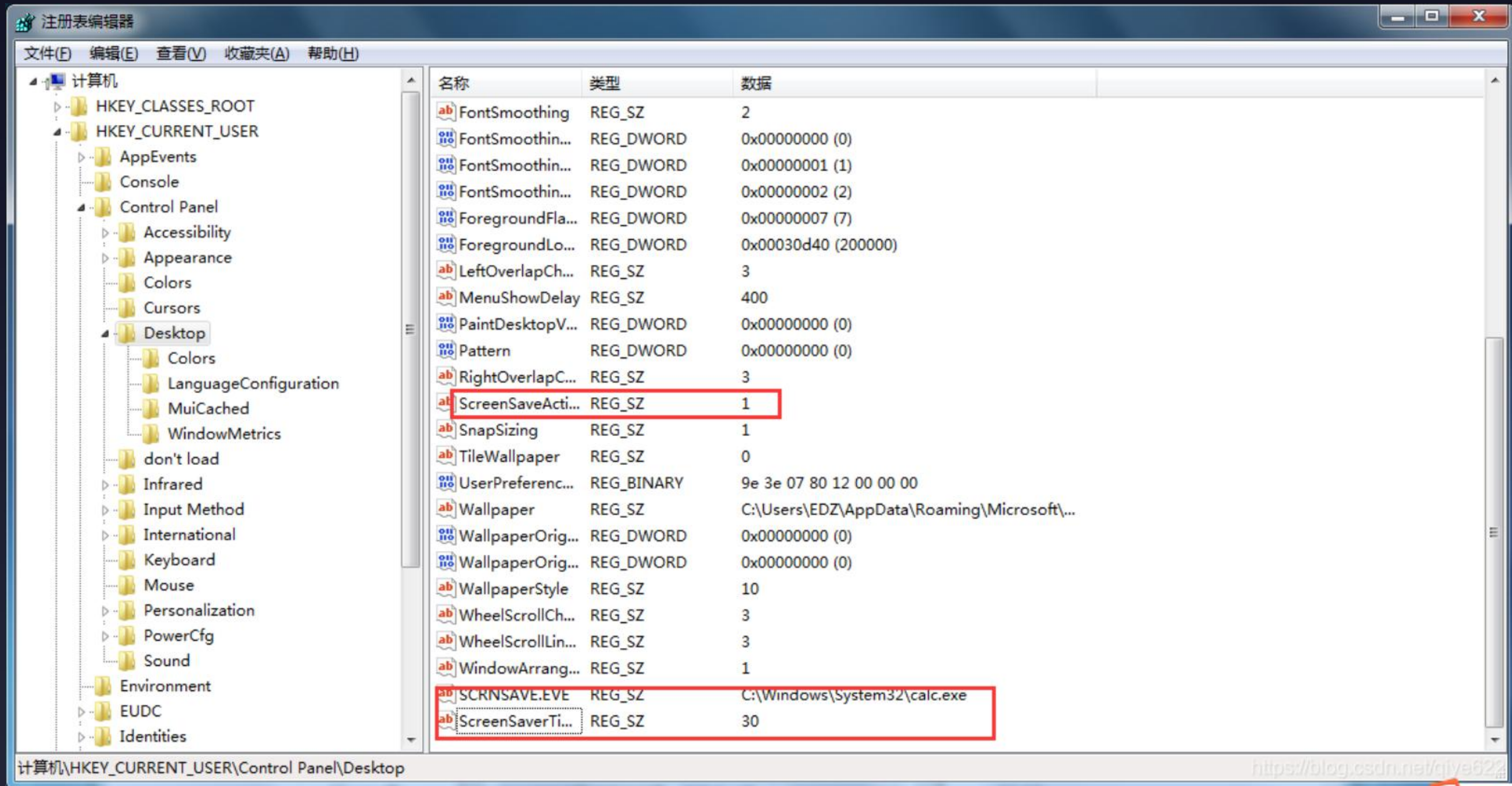
注册表自启动项Run键是病毒最青睐的自启动之所，该键位置是 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] 和 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]，其下的所有程序在每次启动登录时都会按顺序自动执行。还有一个不被注意的Run键，位于注册表 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run] 和 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]，也要仔细查看。B.RunOnce键RunOnce位于 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce] 和 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce] 键，与Run不同的是，RunOnce下的程序仅会被自动执行一次。

1.2.3 注册表安全

屏幕保护程序在对方开启屏幕保护的情况下，我们可以修改品保程序为我们的恶意程序从而达到后门持久化的目的其中屏幕保护的配置存储在注册表中，其位置为：

HKEY_CURRENT_USER\Control Panel\Desktop,关键键值如下;1.SCRNSAVE.EVE; 默认屏幕保护程序，我们可以把这个键值改为我们的恶意程序2.ScreenSaveActive;1表示屏幕保护是启动状态，0表示屏幕保护是关闭状态3.ScreenSaverTimeout; 指定屏幕保护程序启动前系统的空闲事件，单位为秒，默认为900（15分钟）

1.2.3 注册表安全



1.2.3 注册表安全

注册表安全配置

1.隐藏“开始”菜单的部分内容打开注册表，在\HKEY_CURRENT_USER\Software\Micorsoft\Windows\CurrentVersion\Policies\Explorer中新建一个DWORD值“NoSetFolders”，键值为“1”。这样，用户便不能使用“控制面板”并不能使用“设置”中的“打印机”。在该分支下新建一个DWORD值“NoSetTaskbar”，键值为“1”，则“任务栏属性”功能被禁止。在该分支下新建一个DWORD值“NoFind”，键值为“1”，则“查找”功能被禁止。在该分支下新建一个二进制值“NoRun”，键值为“0x00000001”，则“运行”菜单项被关闭。

2.禁用“活动桌面”在关闭了“控制面板”和“打印机”功能后，普通用户可以通过“活动桌面”更改“显示属性，因此要关闭”活动桌面，在“\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policics\System中新建 DIwoRD 值 “NoDispCPL” 键值为 “1”。这样“活动桌面”也被禁用。

3.隐藏桌面上所有图标在、HKEY_CURRENT_UsER\Software\Micorsoft\Windows\CurrentVersion\Policies\Explorer中新建 DOwRD 值 “NoDesktop”，键值为“1”，重新启动计算机后，普通用户桌面上的图标将全部被隐藏。

1.2.3 注册表安全

IP协议安全

启用SYN攻击保护

指定触发SYN洪水攻击保护所必须超过的TCP连接请求数阈值为5。

指定处于 SYN_RCVD 状态的 TCP 连接数的阈值为500。

指定处于至少已发送一次重传的 SYN_RCVD 状态中的 TCP 连接数的阈值为400。

操作步骤

打开 注册表编辑器，根据推荐值修改注册表键值。

Windows Server 2012

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect

推荐值： 2

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen

推荐值： 500

1.2.4 服务安全

Windows服务程序是一个长时间运行的可执行程序，不需要用户的交互，也不需要用户登录。

服务具有两面性，一是合法用户服务，也有可能被入侵者利用。

服务运行方式有两种：

- 1、 独立EXE程序运行。
- 2、 以DLL形式，依附在svchost.exe程序运行。

1.2.4 服务安全

DPCs	n/a	K	K 延迟程序调用
System	4	K	292 K
smss.exe	284	128 K	476 K Windows NT Session Ma... Microsoft Corporation
csrss.exe	332	2,676 K	12,164 K Client Server Runtime... Microsoft Corporation
services.exe	404	3,852 K	4,684 K Services and Controll... Microsoft Corporation
svchost.exe	628	948 K	3,280 K Generic Host Process ... Microsoft Corporation
vmiprvse...	2808	5,596 K	8,612 K WMI Microsoft Corporation
vmiprvse...	3624	1,928 K	5,344 K WMI Microsoft Corporation
svchost.exe	712	1,448 K	4,112 K Generic Host Process ... Microsoft Corporation
svchost.exe	768	3,844 K	4,604 K Generic Host Process ... Microsoft Corporation
svchost.exe	768	3,844 K	4,604 K Generic Host Process ... Microsoft Corporation

1.2.4 服务安全

services.exe4043,852 K4,684 K Services and Controll...Microsoft Corporation

vmacthlp.exe612616 K2,700 K VMware Activation Helper VMware, Inc.

svchost.exe628948 K3,280 K Generic Host Process ...Microsoft Corporation

vmiprvse...28085,636 K8,636 K WMI

vmiprvse...36241,928 K5,344 K WMI

svchost.exe7121,448 K4,112 K Generic Host Process ...Microsoft Corporation

svchost.exe7683,844 K4,604 K Generic Host Process ...Microsoft Corporation

svchost.exe7960,704 K4,072 K Generic Host Process ...Microsoft Corporation

svchost.exe832

wsauctl.exe3952

spoolsv.exe980

msdtc.exe1008

cisvc.exe1164

cidaemon...2776

cidaemon...3376

cidaemon...3488

svchost.exe1188

svchost.exe1324

SafeDogUpd...1368

CloudHelpe...1456

VGAuthServ...2356

vmtoolsd.exe2464

svchost.exe2708

dllhost.exe2856

alg.exe2952

HaoszipSvc.exe3092

d_manage.exe2792

inetinfo.exe3936

svchost.exe328

lsass.exe416

explorer.exe3860

vmtoolsd.exe3960

ctfmon.exe3992

procexp.exe33283.08

onime.exe472

svchost.exe:768 (NetworkService) 属性

线程映像

TOP/IP性能

安全性磁盘和网络

环境性能图表

字符串服务

在这个进程中已注册的服务:

服务	显示名称	路径
Dhcp	DHCP Client	C:\WINDOWS\System32\dhcpcsvc.dll
Dnscache	DNS Client	C:\WINDOWS\System32\dnssrslvr.dll

为此计算机注册并更新 IP 地址。如果此服务停止,计算机将不能接收动态 IP 地址和 DNS 更新。如果此服务被禁用,所有明确依赖它的服务都将不能启动。

权限(P)

停止(S)

暂停(P)

恢复(R)

确定(O)

取消(C)

1.2.4 服务安全

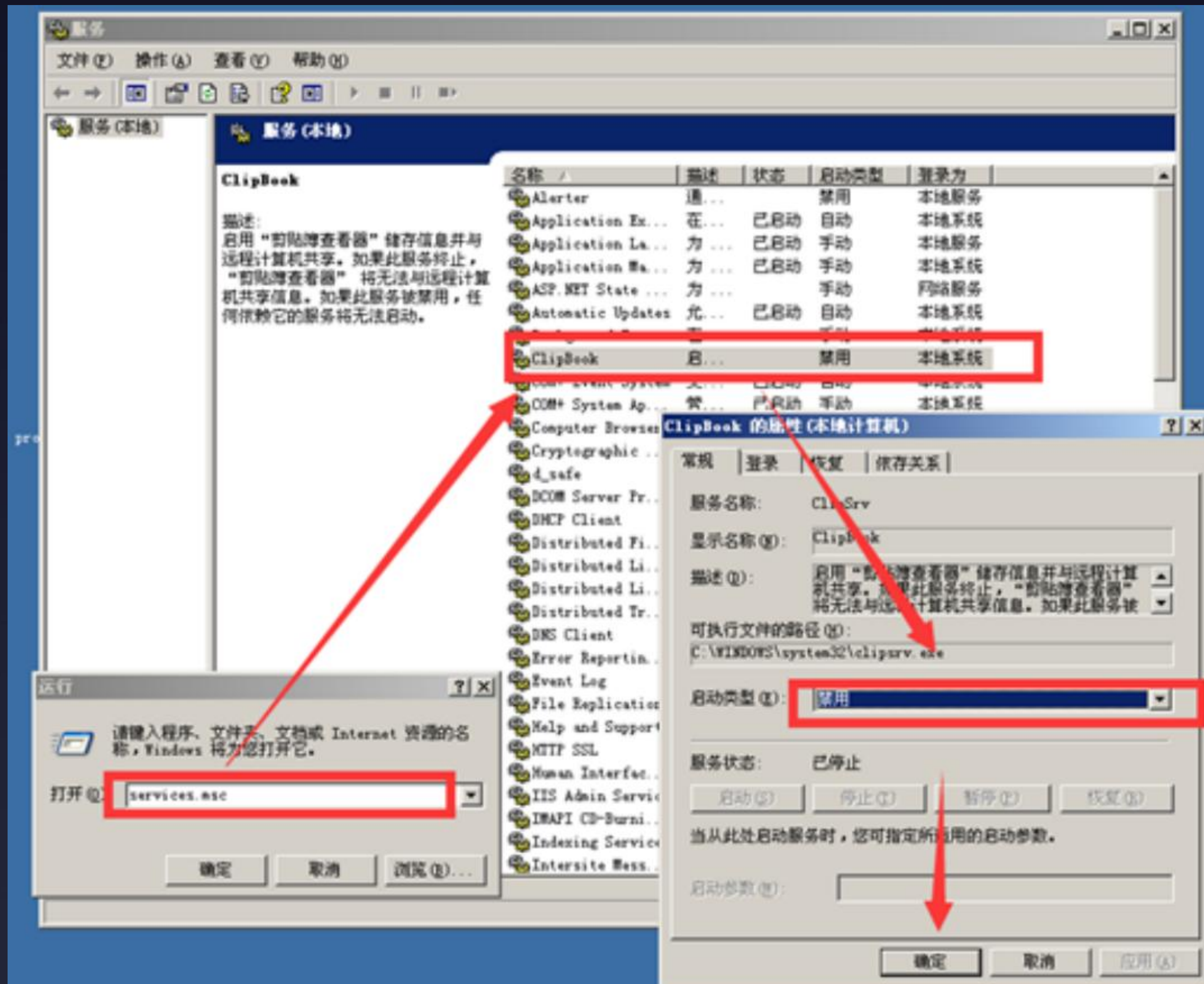
服务包括三种启动类型:自动、手动、禁用。

- 自动--启动时自动加载服务。
- 手动--启动时不自动加载服务，需要的时候手动开启。
- 禁用--启动不加载服务，在需要的时候选择手动或者自动方式开启服务，并重启电脑。

服务启动类型设置：

- 1、 打开"运行"窗口，输入"services.msc"。
- 2、 双击需要配置的服务，出现属性对话框，选择启动方式。

1.2.4 服务安全



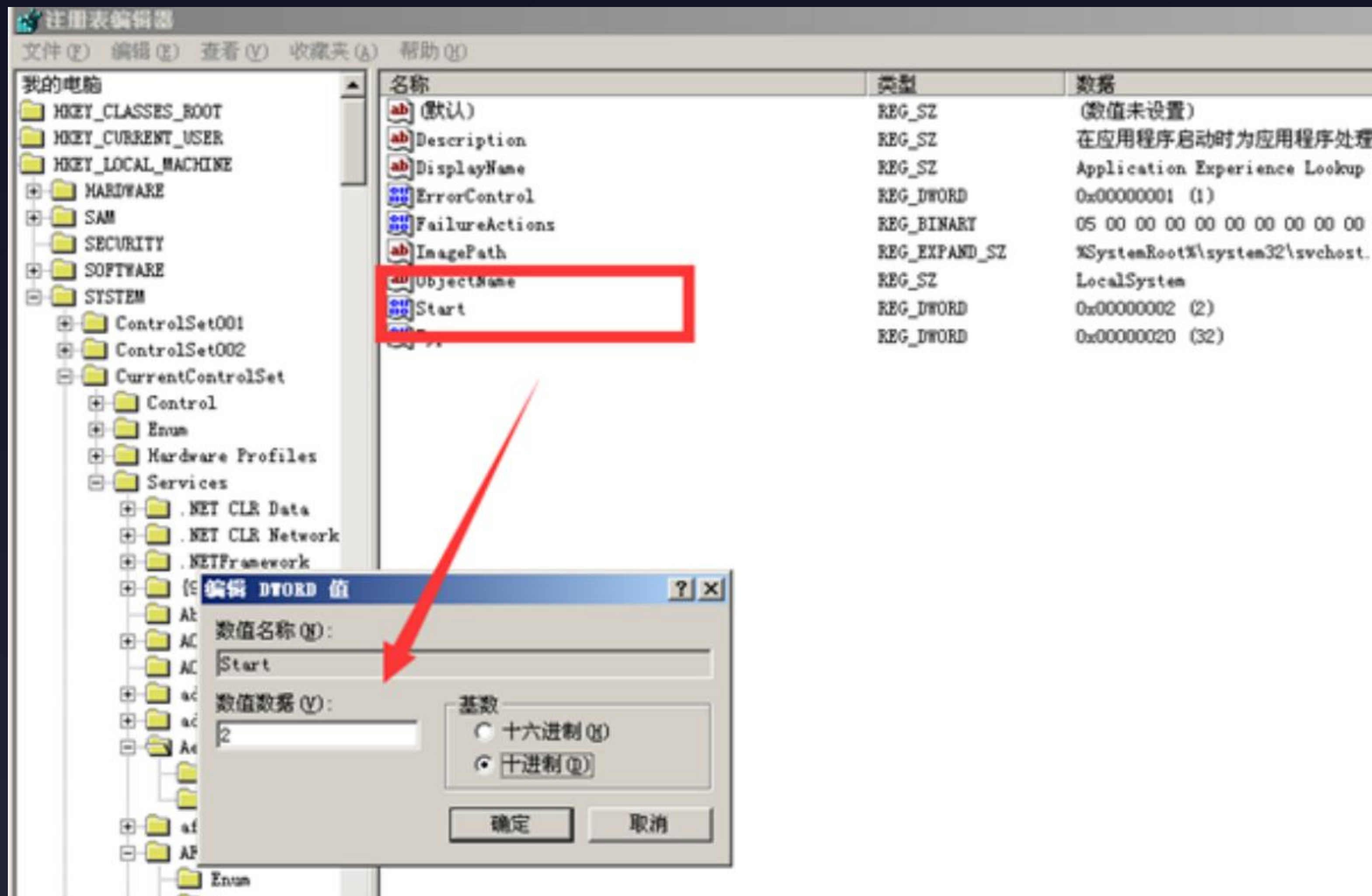
1.2.4 服务安全

注册表下设置的方法：

在HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service底下每一个服务项的子项都有一个Start数值，这个数值的内容依照每一个服务项目的状况而又有不同。Start数值内容所记录的就是服务项目驱动程序该在何时被加载。

Start内容的定义有0、1、2、3、4五种状态，0、1、2分别代表BOOT、System、Auto Load三种意义。而Start数值内容为3的服务项目代表让使用者以手动的方式载入，4则是代表停用的状态，也就是禁用。

1.2.4 服务安全



1.2.4 服务安全

禁用不必要的服务

服务名称	建议
DHCP Client	如果不使用动态IP地址，就禁用该服务
Background Intelligent Transfer Service	如果不启用自动更新，就禁用该服务
Computer Browser	禁用
Diagnostic Policy Service	手动
IP Helper	禁用。该服务用于转换IPv6 to IPv4
Print Spooler	如果不需要打印，就禁用该服务
Remote Registry	禁用。Remote Registry主要用于远程管理注册表
Server	如果不使用文件共享，就禁用该服务。禁用本服务将关闭默认共享，如ipc\$、admin\$和c\$等
TCP/IP NetBIOS Helper	禁用
Windows Remote Management (WS-Management)	禁用
Windows Font Cache Service	禁用
WinHTTP Web Proxy Auto-Discovery Service	禁用

1.2.5 策略安全

1. 账户口令策略
2. 认证策略
3. 限制使用迅雷进行恶意下载
4. 拒绝网络病毒藏于临时文件
5. 禁止来自外网的非法ping攻击
6. 禁止普通用户随意上网访问

1.2.5 策略安全

例如： 拒绝网络病毒藏于临时文件

现在Internet网络上的病毒疯狂肆虐，一些“狡猾”的网络病毒为了躲避杀毒软件的追杀，往往会想方设法地将自己隐藏于系统临时文件夹，那样一来杀毒软件即使找到了网络病毒，也对它无可奈何，因为杀毒软件对系统临时文件夹根本无权“指手划脚”。为了防止网络病毒隐藏在系统临时文件夹中，如在Windows Server 2008系统的软件限制策略：

首先打开Windows Server 2008系统的组策略控制台窗口；

其次在该控制台窗口的左侧位置处，依次选中“计算机配置” / “Windows设置” / “安全设置” / “软件限制策略” / “其他规则” 选项，同时用鼠标右键单击该选项，并执行快捷菜单中的“新建路径规则” 命令；单击其中的“浏览” 按钮，从弹出的文件选择对话框中，选中并导入Windows Server 2008系统的临时文件夹，同时再将“安全级别” 参数设置为“不允许”，最后单击“确定” 按钮保存好上述设置操作，这样一来网络病毒日后就不能躲藏到系统的临时文件夹中了。

1.2.6 日志安全

Windows使用"事件管理器"来管理日志系统，需要用系统管理员身份进入系统进行操作。

Windows的日志文件一般分为三类：

1、系统日志

跟踪各种各样的系统事件，记录由Windows NT的系统组件产生的事件。

如：在启动过程加载驱动程序错误或其他系统组件的失败记录在系统日志中。

2、应用程序日志

记录由应用程序或系统程序产生的事件。

如：应用程序产生的装载dll(动态链接库)失败的信息将出现在日志中。

3、安全日志

记录登陆上网，下网，改变访问权限以及系统启动和关闭等事件以及与创建、打开或删除文件等资源使用相关联的事件。

系统的"事件管理器"可以指定在安全日志中记录需要记录的事件。

启动Windows时，事件日志服务会自动启动，所有用户都可以查看"应用程序日志"，但是只有系统管理员才能访问"安全日志"和"系统日志"。

1.2.6 日志安全



1.2.6 日志安全

登录类型2：交互式登录(Interactive)

指用户在计算机的控制台上进行登录，也就是在本地键盘上进行的登录。(KVM登录属于交互式登录)

登录类型3：网络(Network)

从网络上访问一台计算机时就属于网络登录。如：连接到共享文件夹或者共享打印。

登录类型4：批处理(Batch)

当windows运行一个计划任务时，"计划任务服务"将为这个任务首先创建一个新的登录会话以便他能在此计划任务所配置的用户账号下运行。

登录类型7：解锁(Unlock)

当用户离开计算机，屏保就会启动锁定计算机，需要输入密码才能重新进入。

(失败的类型7登录表明有人输入了错误的密码或者有人在尝试解锁计算机)

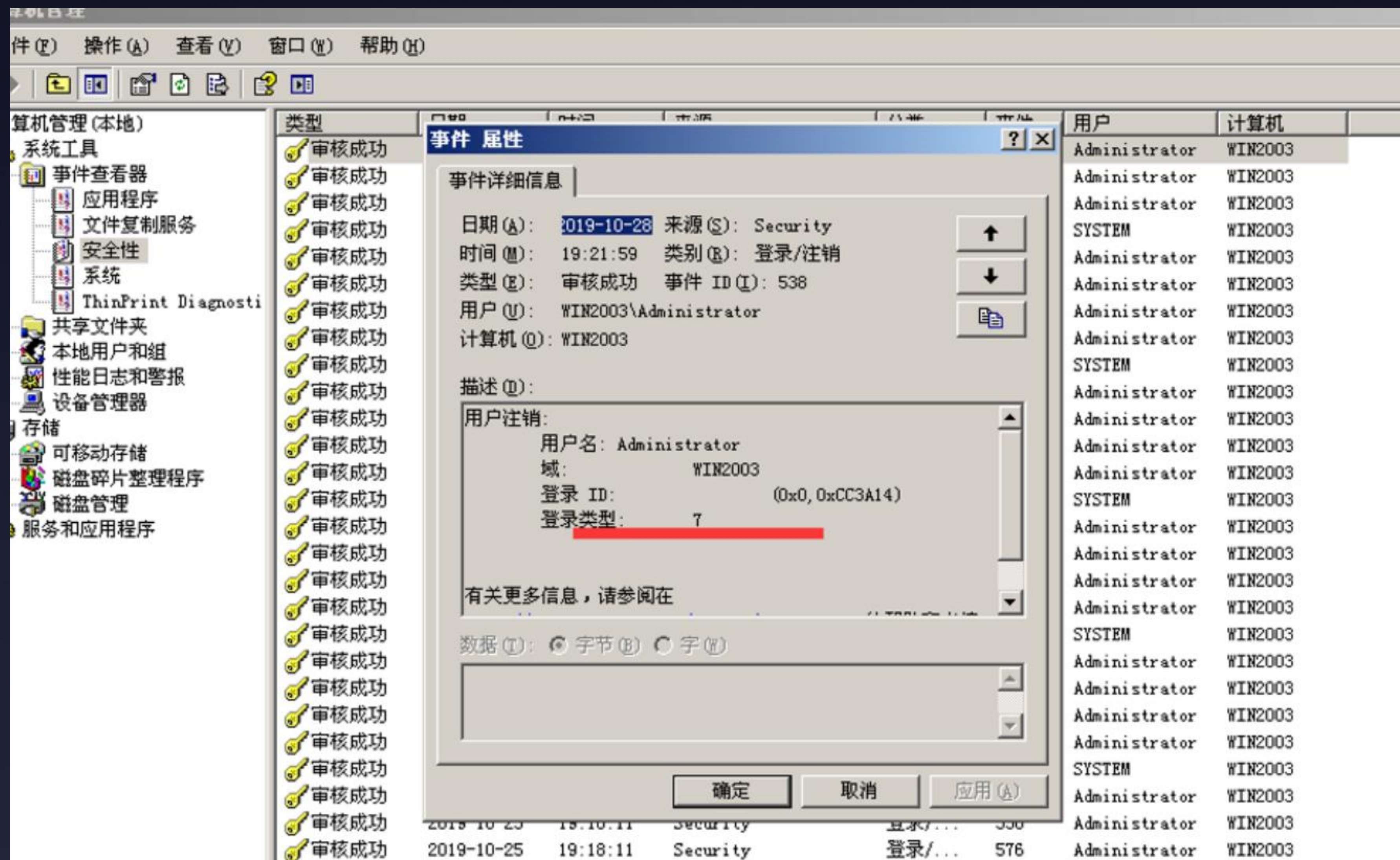
登录类型8：网络明文(NetworkCleartext)

像类型3一样，这种登录的密码在网络上是通过明文传输的。

登录类型10：远程交互(Remote Interactive)

通过终端服务、远程桌面或远程协助访问计算机。

1.2.6 日志安全



1.2.6 日志安全

日志的安全问题

- 1、日志的查看
- 2、日志文件大小设置
- 3、日志文件转移
- 4、日志文件夹的保护设置

日志的转移和防删除

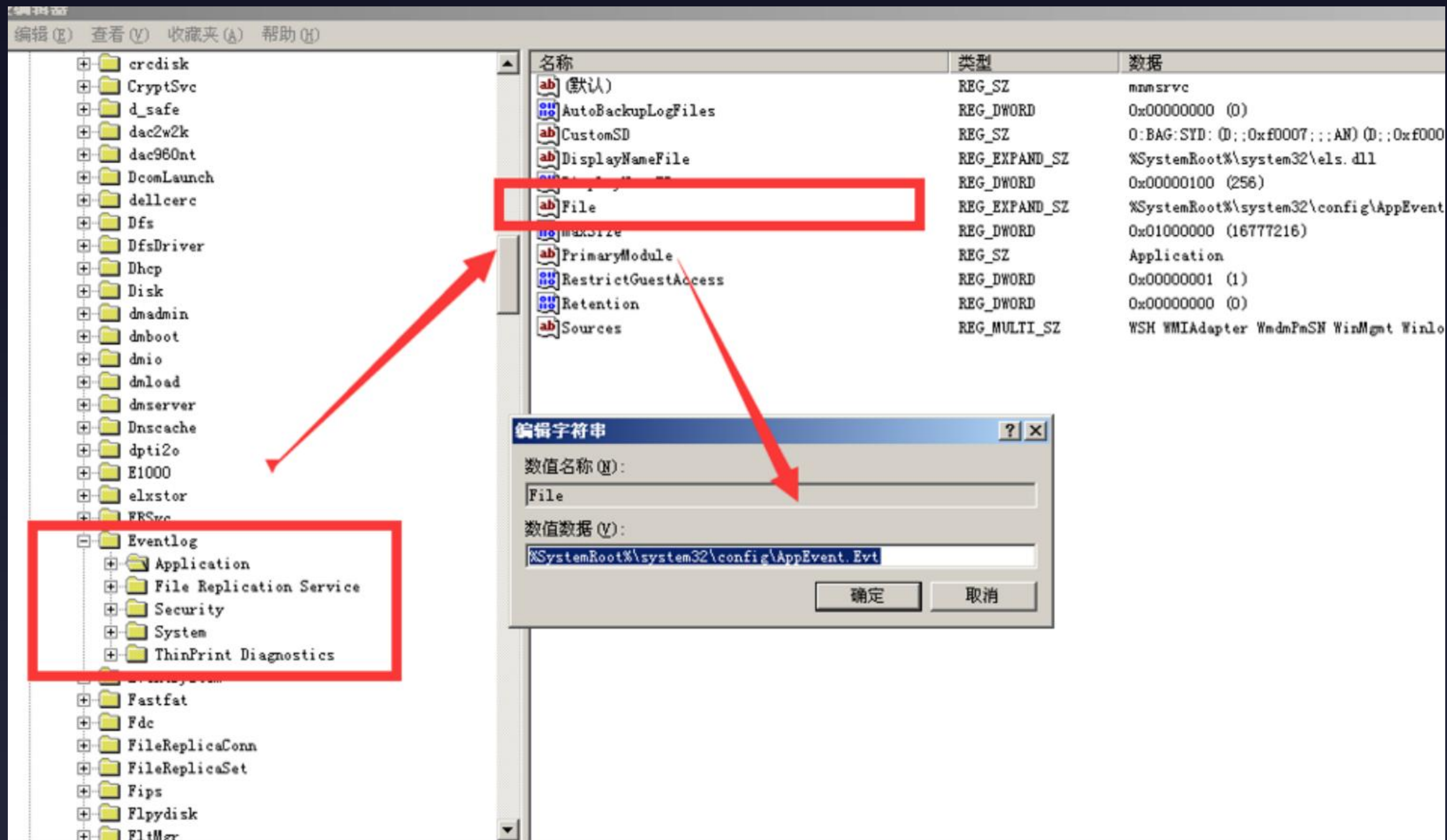
日志文件默认存放在%systemroot\system32\config%，有"应用程序日志"，"安全日志"，"系统日志"，分别对应的文件是：appevent.evt、secevent.evt、sysevent.evt。这些文件不可删除，却可以清空里面的数据。

- 1、修改日志文件的存放位置必须在注册表里修改

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog Application应用程序日志，Security安全日志，System系统日志。file项的值就是"应用程序日志"存放的位置

2. 给予目录除"完全控制"和"修改"之外的所有权限，然后只给"everyone"组只读的权限。

1.2.6 日志安全



1.2.6 日志安全

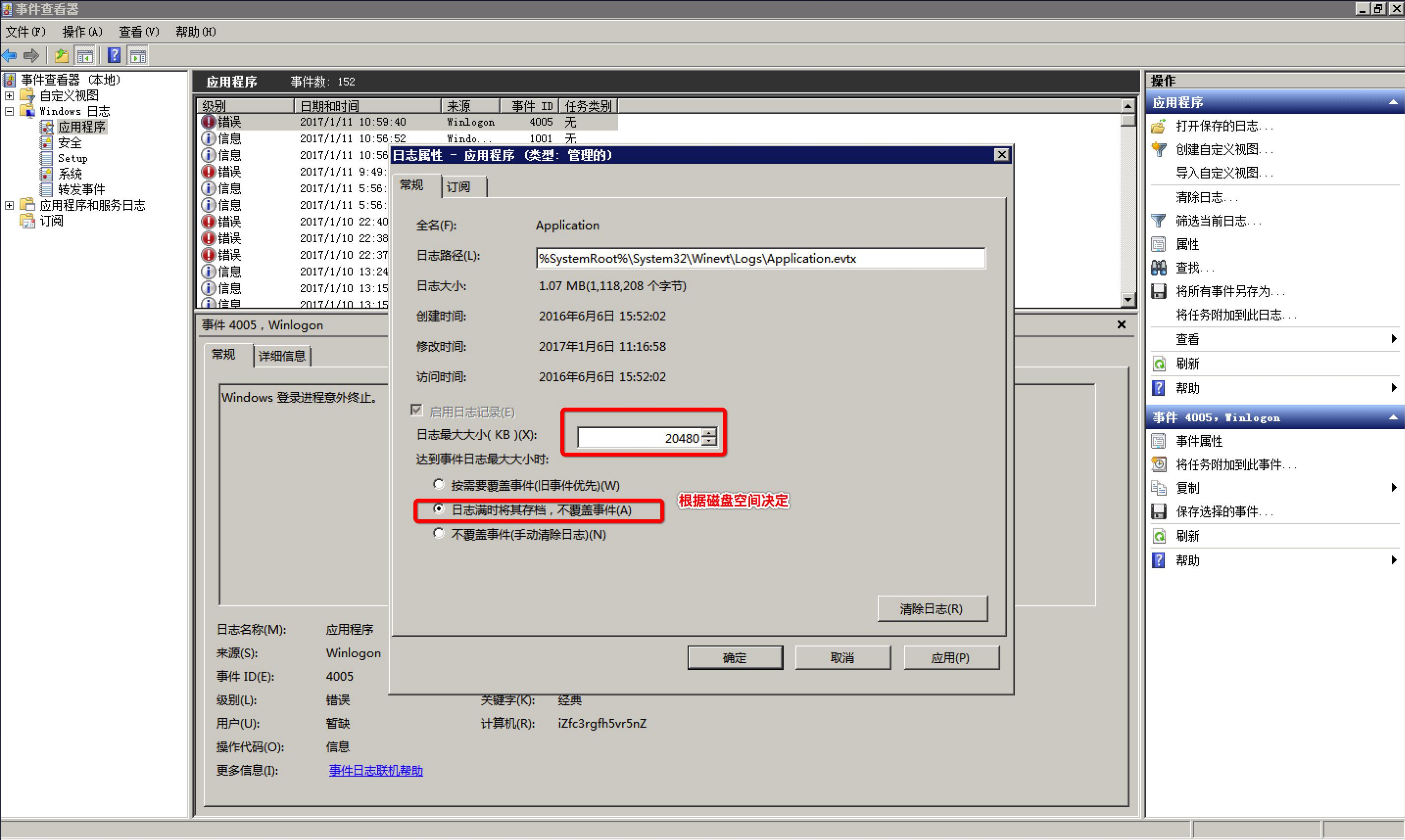
日志文件大小设置

设置应用日志文件大小至少为 8192 KB，可根据磁盘空间配置日志文件大小，记录的日志越多越好。并设置当达到最大的日志尺寸时，按需要轮询记录日志。

操作步骤

打开 控制面板 > 管理工具 > 事件查看器，配置 应用日志、系统日志、安全日志 属性中的日志大小，以及设置当达到最大的日志尺寸时的相应策略。

1.2.6 日志安全



1.2.7 其他安全

1. 防病毒管理

Windows系统需要安装防病毒软件, 并开启病毒库更新及实时防御功能。

2. 设置屏幕保护密码和开启时间

设置从屏幕保护恢复时需要输入密码, 并将屏幕保护自动开启时间设定为五分钟。

3. 限制远程登录空闲断开时间

对于远程登录的帐户, 设置不活动超过时间15分钟自动断开连接。

打开 控制面板 > 管理工具 > 本地安全策略, 在 本地策略 > 安全选项 中, 设置 Microsoft网络服务器: 暂停会话前所需的空闲时间数量 属性为15分钟。

4. 操作系统补丁管理

安装最新的操作系统Hotfix补丁。安装补丁时, 应先对服务器系统进行兼容性测试。

注意: 对于实际业务环境服务器, 建议使用通知并自动下载更新, 但由管理员选择是否安装更新, 而不是使用自动安装更新, 防止自动更新补丁对实际业务环境产生影响。

1.2.7 其他安全

