主机安全

一、 身份鉴别（S3）

本项要求包括：

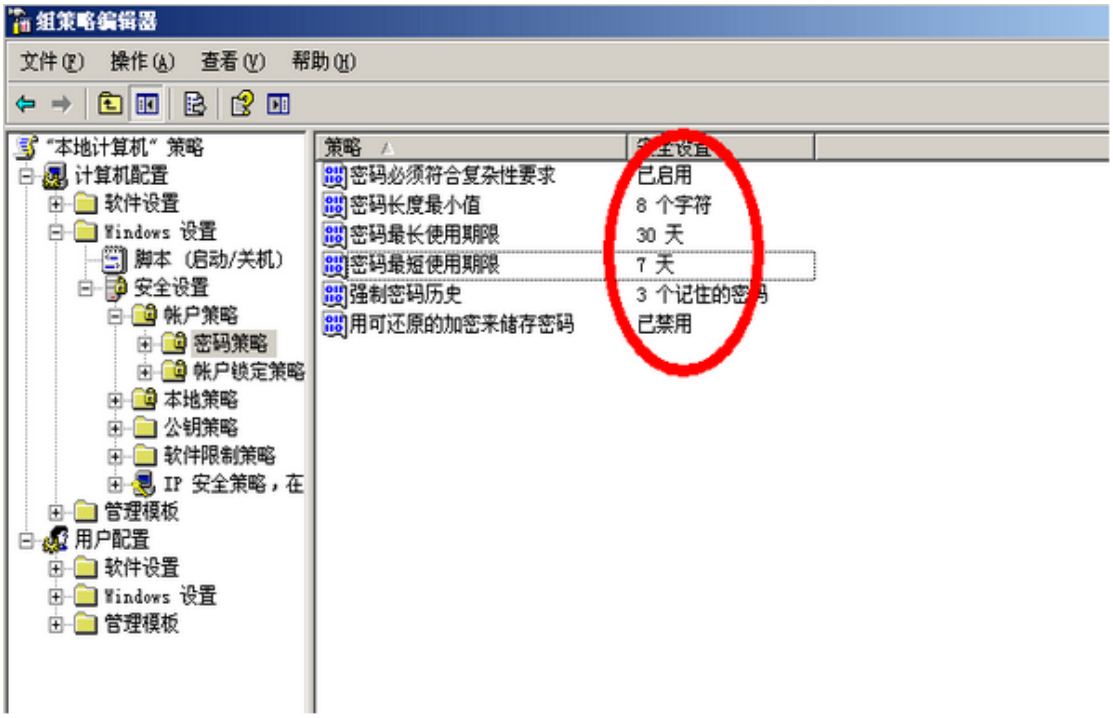
a） 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

设置登陆密码

b） 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度

要求并定期更换；

依次展开[开始]->（[控制面板] ->）[管理工具]->[本地安全策略]->[账户策略]->[密码策略]，查看以下项的情况：1)复杂性要求-启用、2)长度最小值-大于8、3)最长存留期-不为0、4)最短存留期-不为0、5)强制密码历史-大于3。

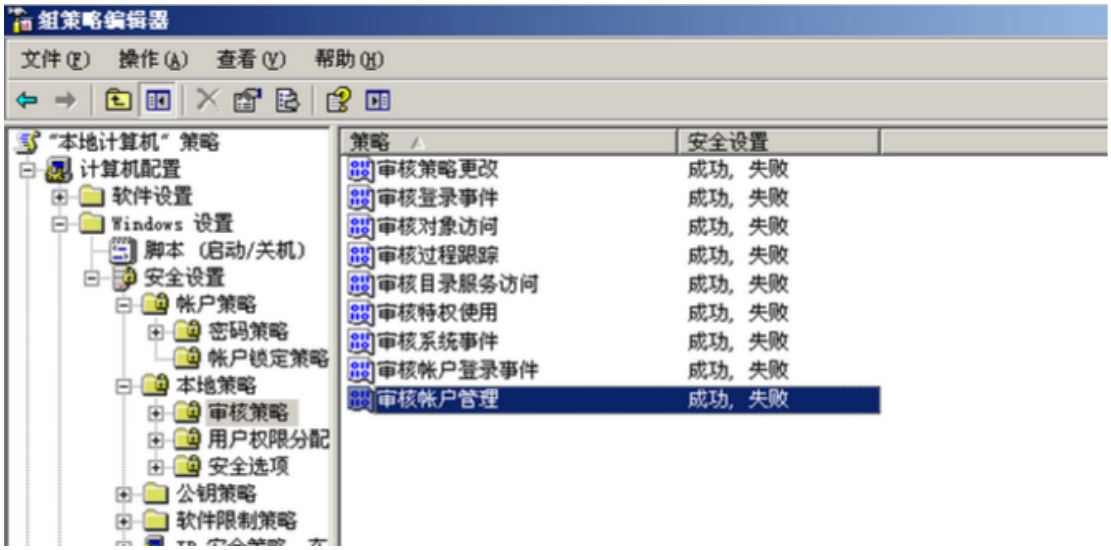


c） 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

依次展开[开始]->（[控制面板] ->）[管理工具]->[本地安全策略]->[账户策略]->[账户锁定策略]；

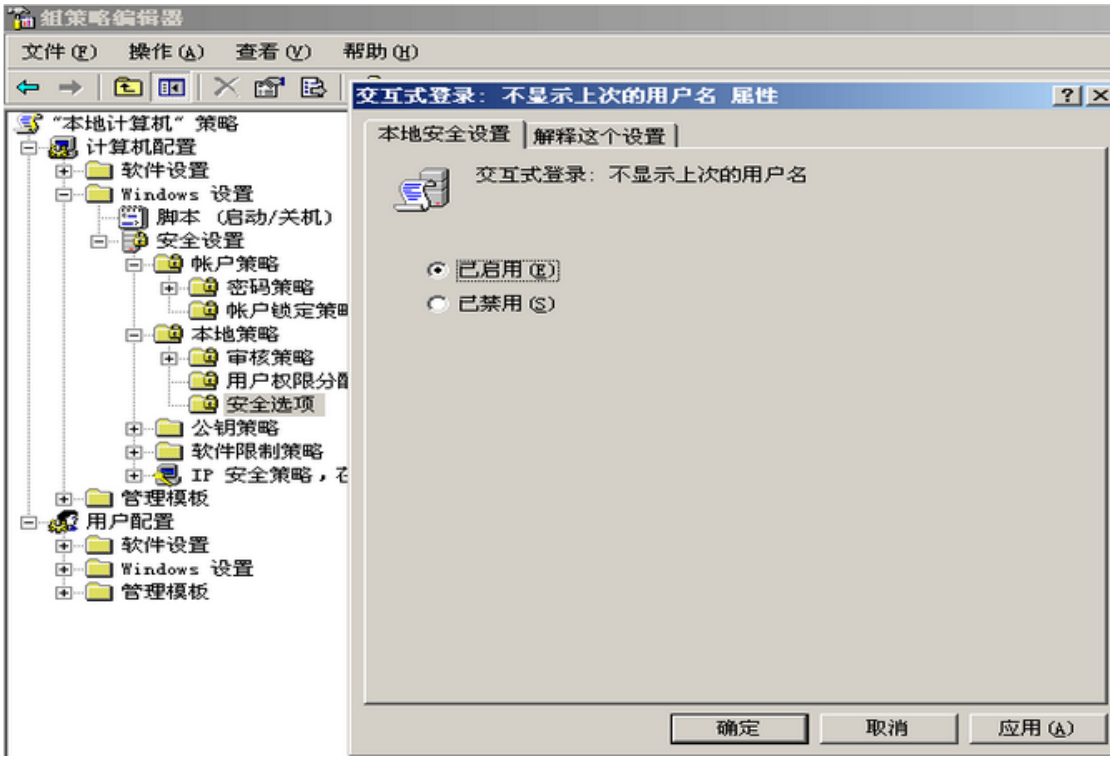
d） 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃
听；
如果是本地管理或KVM等硬件管理方式，此要求默认满足；
如果采用远程管理，则需采用带加密管理的远程管理方式，如启用了加密功能的3389(RDP客户端使用ssl加密)远程管理桌面或修改远程登录端口。

e） 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。
Windows Server 2003默认不存在相同用户名的用户，但应防止多人使用同一个账号。（访谈时无多人共用一个账号）
f） 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。
动态口令、数字证书、生物信息识别等
二、 访问控制（S3）
本项要求包括：
a） 应启用访问控制功能，依据安全策略控制用户对资源的访问；
制定用户权限表，管理员账号仅由系统管理员登陆 删除默认共享 ？
b） 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的
最小权限；
系统管理员、安全管理员、安全审计员由不同的人员和用户担当 c） 应实现操作系统和数据库系统特权用户的权限分离；
应保证操作系统管理员和审计员不为同一个账号，且不为同一个人 访谈时候注意
d） 应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；
重命名系统默认账户，禁用guest、SUPPORT_388945a0这些用户名
e） 应及时删除多余的、过期的帐户，避免共享帐户的存在。
清理已离职员工的账户
确保木有多余账号，确保木有多人共享账号
f） 应对重要信息资源设置敏感标记；
Server2003无法做到
g） 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；
Server2003无法做到
三、 安全审计（G3）
本项要求包括：
a） 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；
b） 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内
重要的安全相关事件；
依次展开[开始]->([控制面板] ->) [管理工具]->[本地安全策略]->[本地策略]->[审核策略]；全部开启

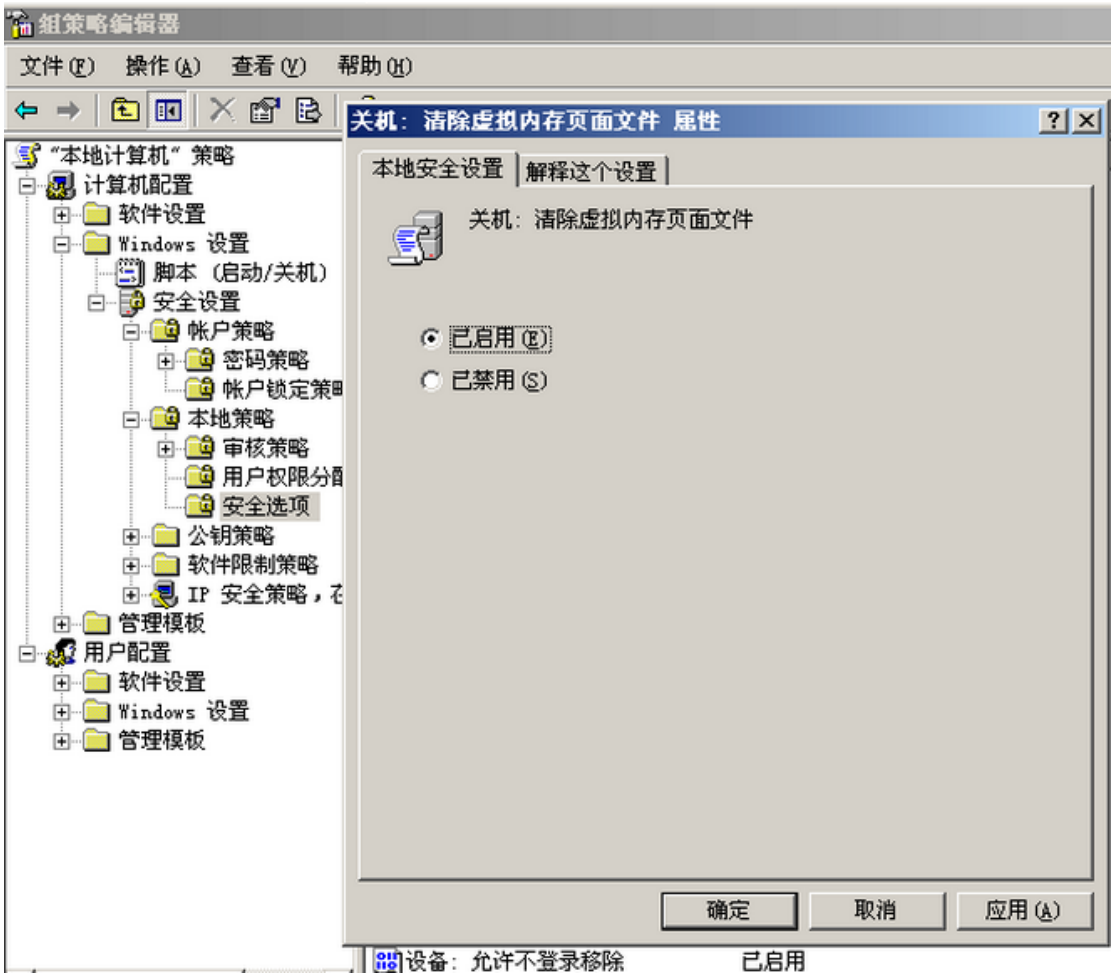


c） 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

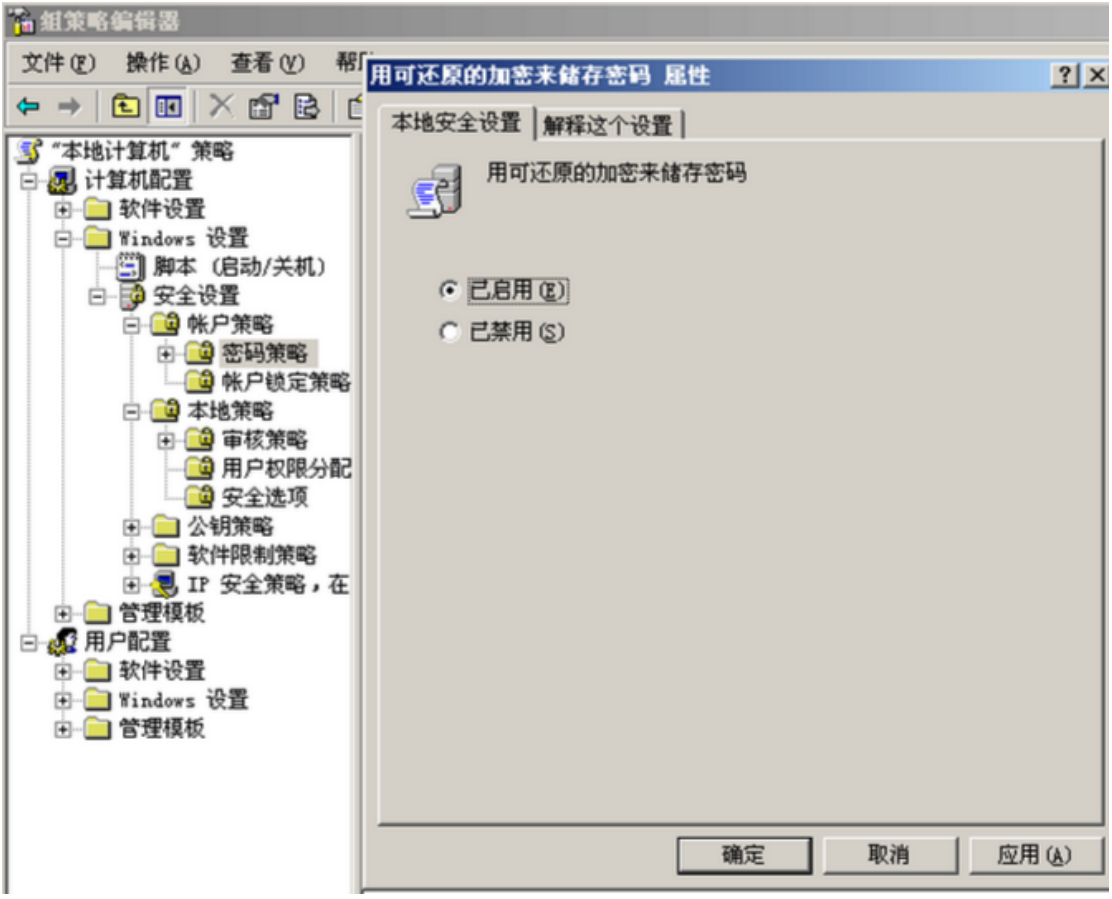
Server2003默认满足
d） 应能够根据记录数据进行分析，并生成审计报表；
第三方工具
e） 应保护审计进程，避免受到未预期的中断；
Server2003默认满足
f） 应保护审计记录，避免受到未预期的删除、修改或覆盖等。 第三方工具
四、 剩余信息保护（S3）
本项要求包括：
a） 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其
他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
依次展开[开始]->([控制面板] ->) [管理工具]->[本地安全策略]->[本地策略]->[安全选项] ->[交互式登陆：不显示上次的登录名] 启用



b）应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配
给其他用户前得到完全清除。
c）依次展开[开始]->([控制面板] ->）[管理工具]->[本地安全策略]->[本地策略]->[安全选项] ->[关机:清理虚拟内存页面文件] 启用



依次展开[开始]->（[控制面板] ->）[管理工具]->[本地安全策略]->[账户策略]->[密码策略] 用可还原的加密来存储密码　　启用



五、 入侵防范（G3）

本项要求包括：

a） 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻

击的目的、攻击的时间，并在发生严重入侵事件时提供报警； 第三方IDS

b） 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；

是否使用一些文件完整性检查工具,对重要文件的完整性进行检查，是否对重要的配置文件进行备份

检查产品的测试报告、用户手册或管理手册，确认其是否具有相关功能；或由第三方工具提供了相应功能。

如果测试报告、用户手册或管理手册中没有相关描述，且没有提供第三方工具增强该功能，则该项要求为不符合。

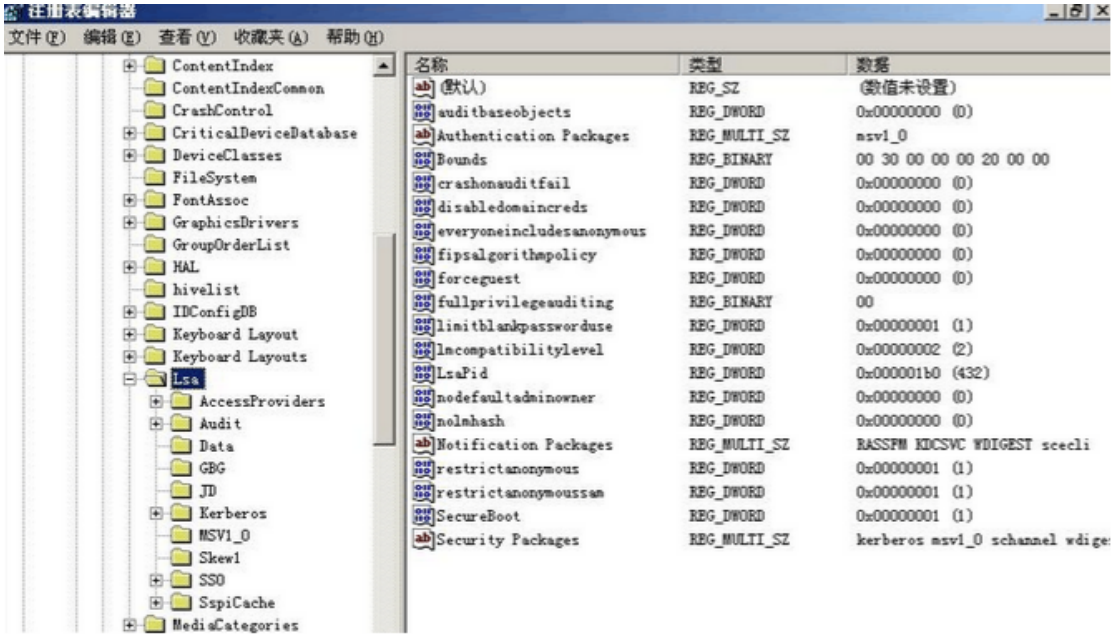
c） 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服

务器等方式保持系统补丁及时得到更新。 系统服务和补丁升级两方面

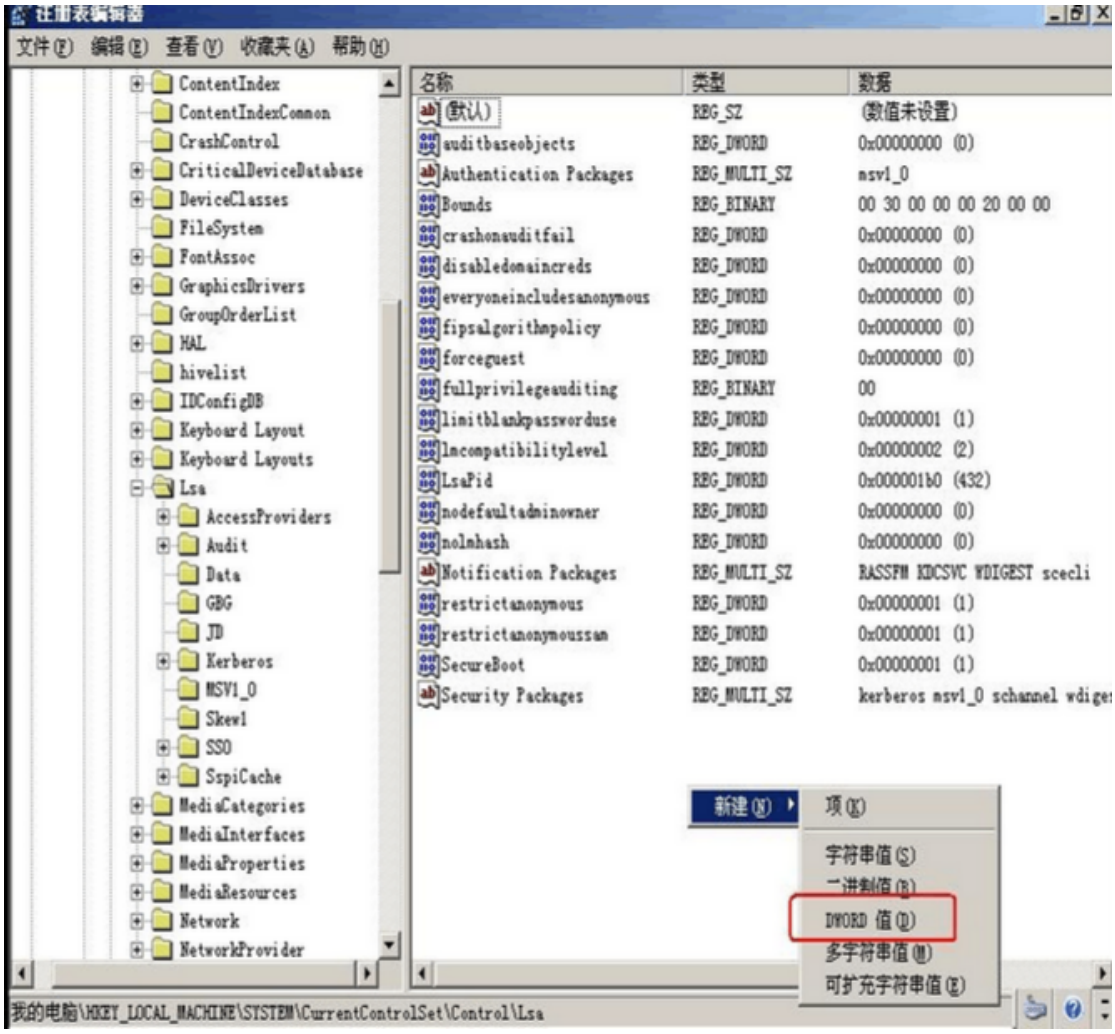
1、不必要的服务关闭，查看已经启动的或者是手动的服务，一些不必要的服务如Alerter、Remote Registry Service、Messenger、Task Scheduler是否已启动； 2、不必要的端口关闭 如145，443()

3、“共享名”列为空，无C$、D$、IPC$等默认共享，HKEY_LOCAL_MACHINE\SYSTEM\currentControlSet\Control\Lsa\restrictanonymous值不为“0”；

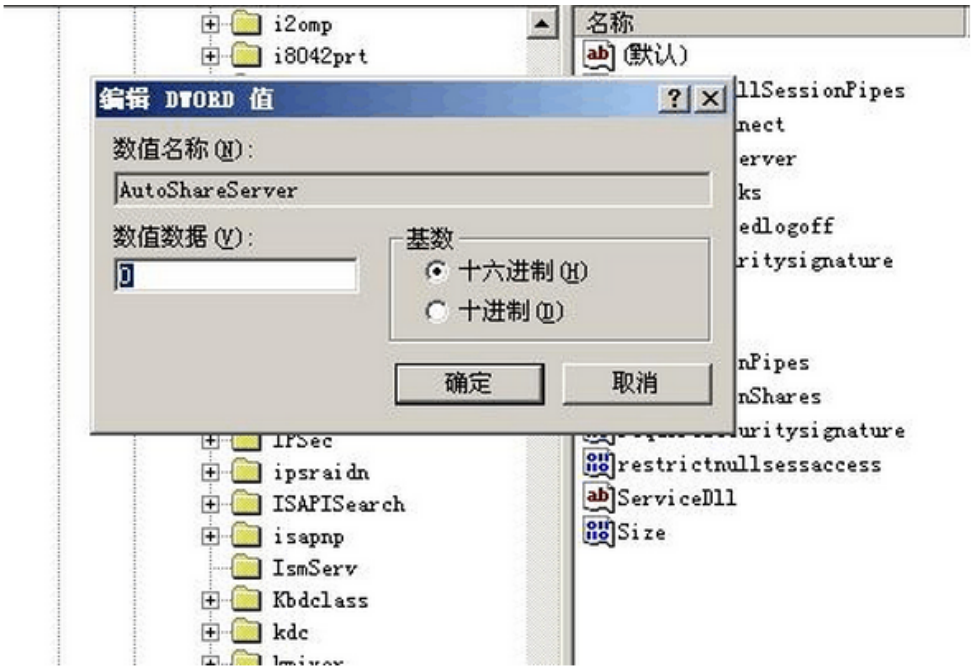
4、系统补丁先测试，再升级；补丁号为较新版本。
“开始”→“运行”输入“regedit”确定后，打开注册表编辑器，找到“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters”项，双击右侧窗口中的“AutoShareServer”项将键值由1改为0，这样就能关闭硬盘各分区的共享。然后还是在这一窗口下再找到“AutoShareWks”项，也把键值由1改为0，关闭admin$共享。如果没有AutoShareServer项和AutoShareWks项，可自己新建"AutoShareServer"=dword:00000000和"AutoShareWks"=dword:00000000。创建键值的方式如下： i.通过regedit进入注册表，选到对应的项



ii.在窗口右侧空白处，右键选新建，选择DWORD值 iii cmd
net share c$ /delete net share D$ /delete



iii.将新建的值命名为AutoShareServer或AutoShareWks，并双击它设置值为0



最后到“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa”项处找到“restrictanonymous”，将键值设为1，关闭IPC$共享。 注意：本法必须重启机器，但一经改动就会永远停止共享。 2）停止服务法: 在“计算机管理”窗口中，单击展开左侧的“服务和应用程序”并选中其中的“服务”，此时右侧就列出了所有服务项目。共享服务对应的名称是“Server”（在进程中的名称为services），找到后双击它，在弹出的“常规”标签中把“启动类型”由原来的“自动”更改为“已禁用”。然后单击下面“服务状态”的“停止”按钮，再确认一下就OK了。

六、 恶意代码防范（G3）
本项要求包括：
a）应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；
安装防病毒软件，且版本最新
b）主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；
访谈系统管理员网络防病毒软件和主机防病毒软件分别采用什么病毒库。 网神和赛门铁克()
c）应支持防恶意代码的统一管理。
防恶意代码统一管理，统一升级 ()
七、 资源控制（A3）
本项要求包括：
a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；
1、 可通过主机防火墙或者TCP/IP筛选功能实现 2、 可通过网络设备和硬件防火墙实现
(0
b）应根据安全策略设置登录终端的操作超时锁定；
设置屏保10分钟以内 ()
c）应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情
况；
第三方工具监控，并设置报警阈值 ()
d）应限制单个用户对系统资源的最大或最小使用限度；
不适用 ()
e）应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。
有第三方主机监控程序，且其提供主动的声、光、电、短信、邮件等形式的一种或多种报警方式。 ()

八、 备份与恢复
双机热备、冷备或集群等方式