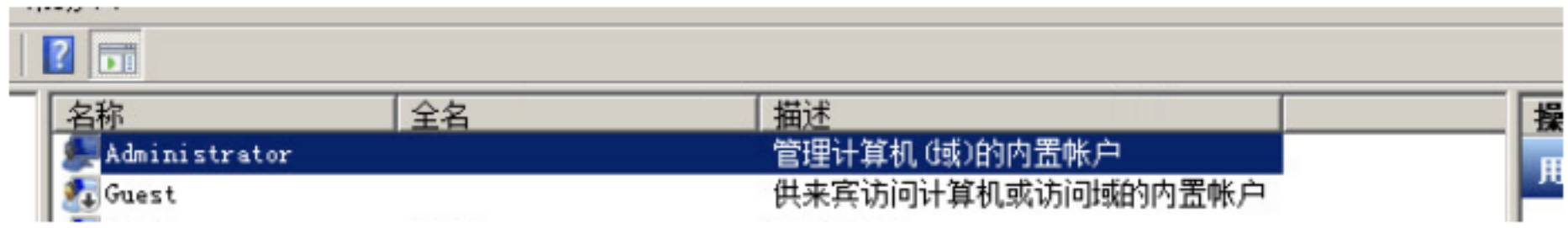
服务器安全加固 (以 Windows Server 2008 为示例， Windows server 2003 和 Windows Server 2012 根据实际需要进行修正)

1、 服务器登录安全加固

1） 为登录用户添加密码，密码长度在 10 位以上，并满足密码包括字母数字和特殊字符组成等复杂度要求。 （请回答）

2） 禁用系统多余帐号，如不需要 Guest 帐号访问服务器，则应禁用。 （请截图）

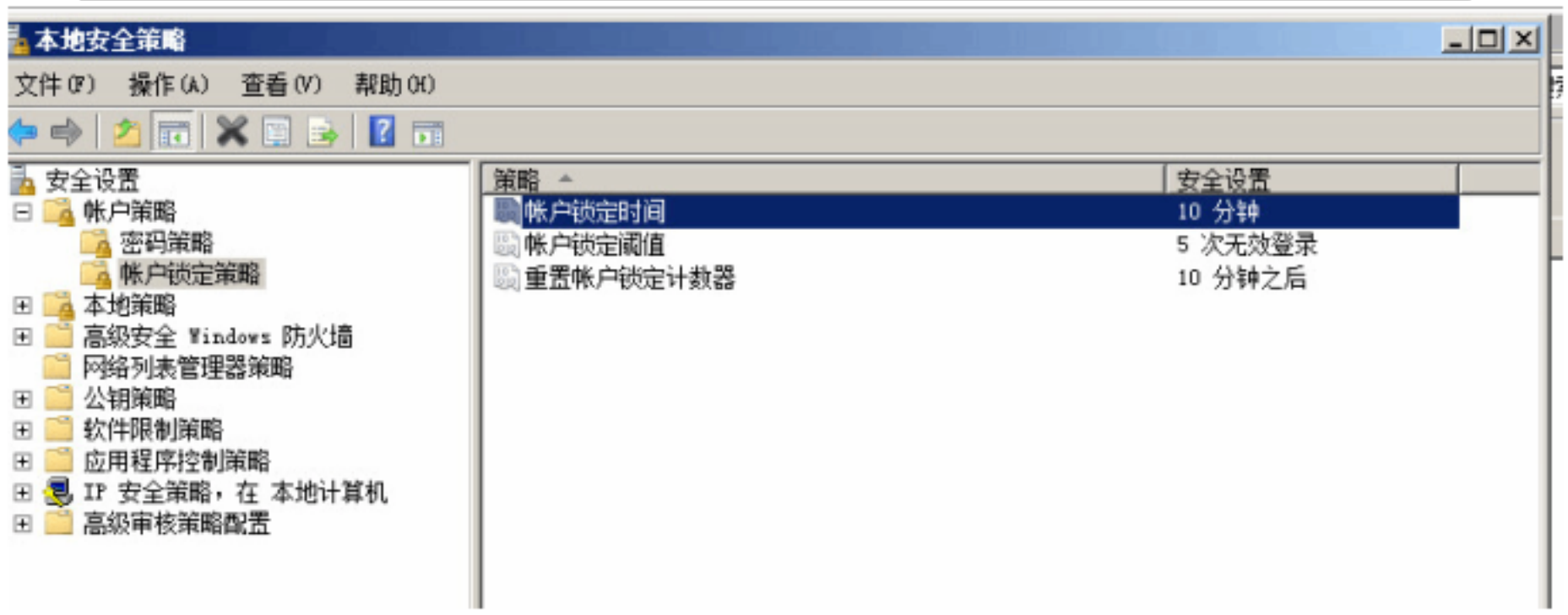


3） 设置 Windows 用户密码策略， 可通过“ 控制面板－管理工具－本地安全策略 ” 中“ 帐户策略 ” 下的“ 帐户策略 ” 进行安全设置如下。 （请截图）

序号	属性	可选择值
1	密码必须符合复杂性要求	已启用
2	密码长度最小值	10 个字符
3	密码最短使用期限	5 天
4	密码最长使用期限	40 天
5	强制密码历史	3 次
6	用可还原的加密来储存密码	已禁用

4） 设置 Windows 系统非法登录锁定次数， 可通过“ 控制面板－管理工具－本地安全策略 ” 中“ 帐户策略 ” 下的“ 帐户锁定策略 ” 进行安全加固，参数设置参考如下； （请截图）

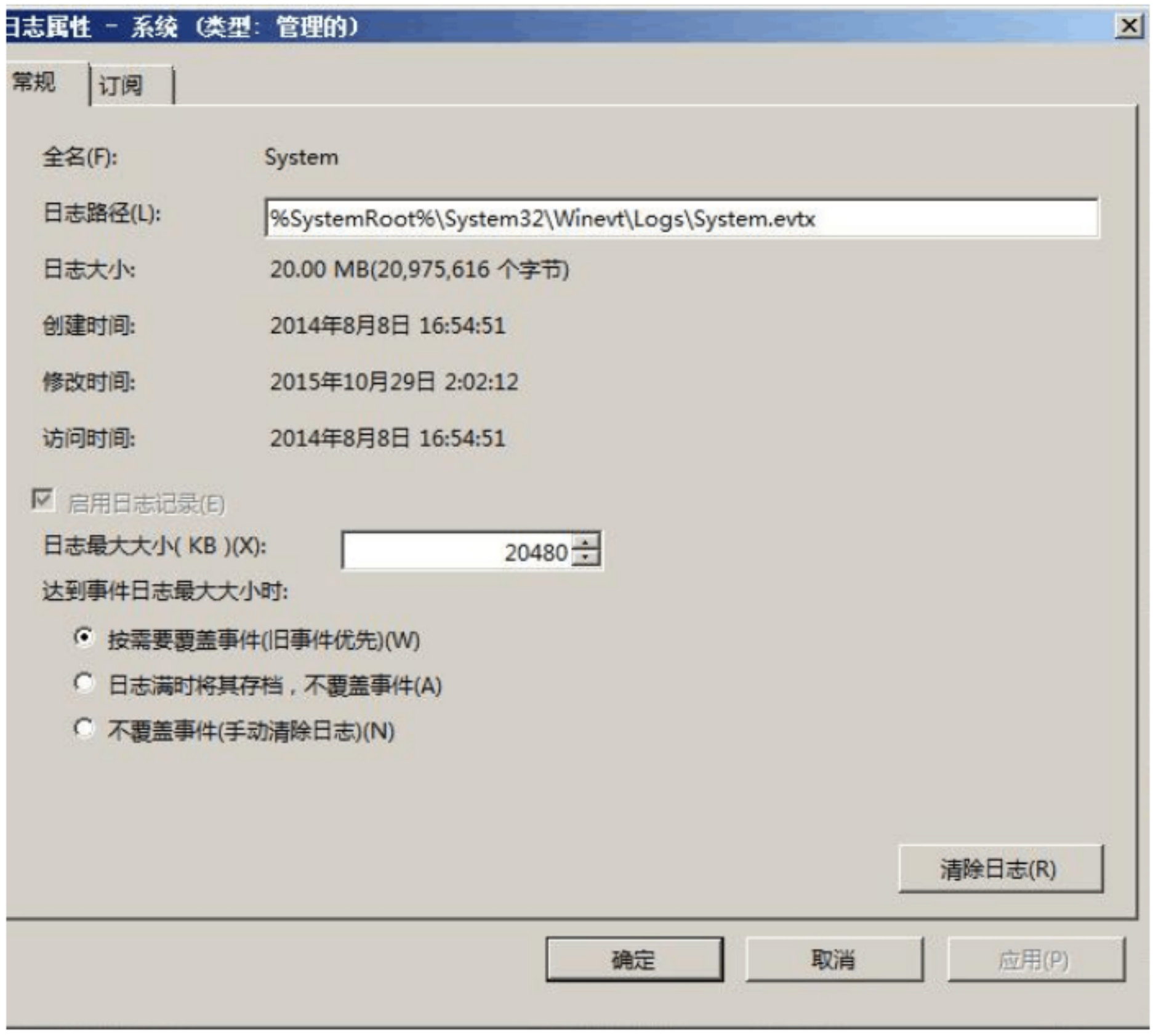
序号	属性	可选择值
1	帐户锁定阈值	5 次
2	帐户锁定时间	10 分钟

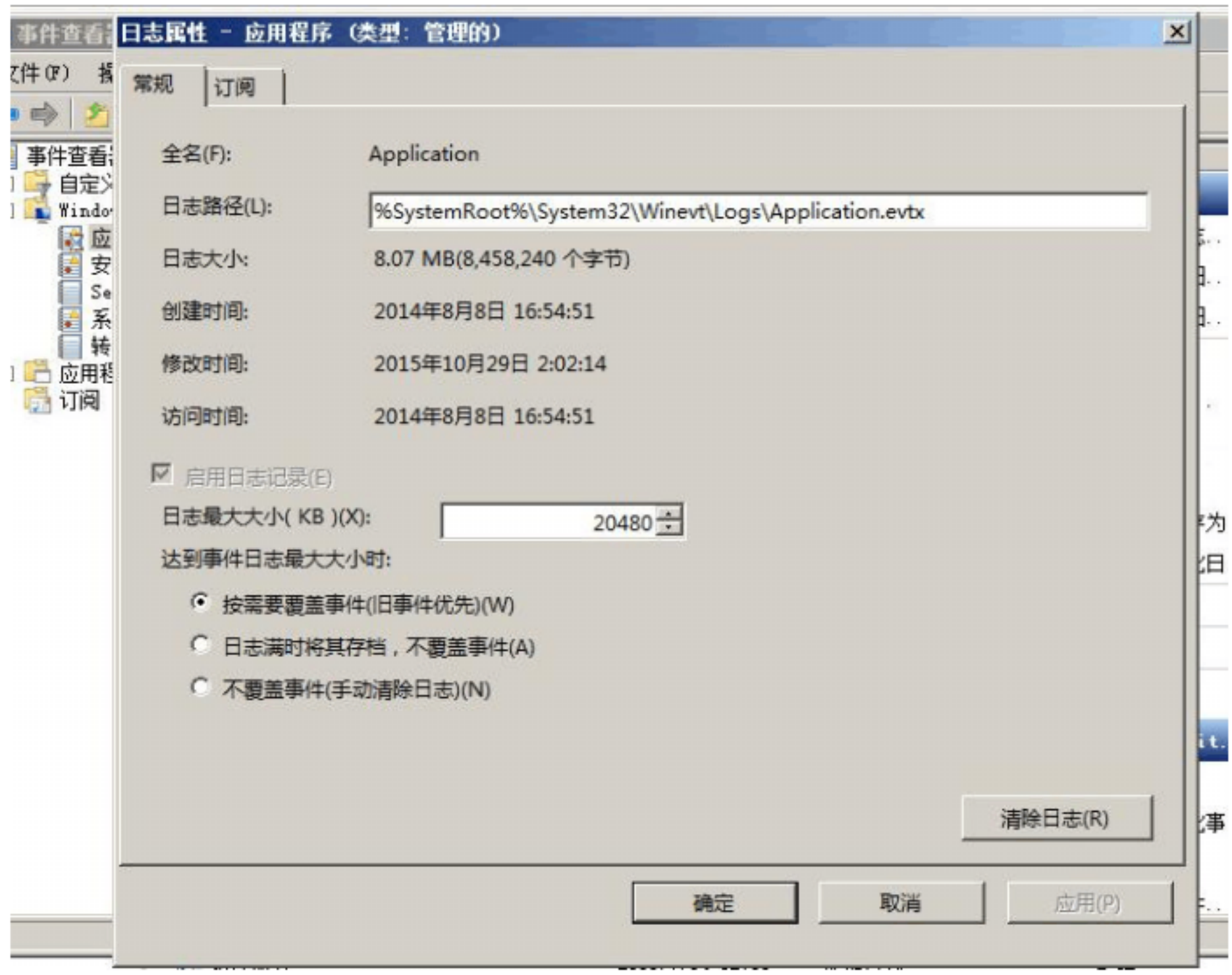


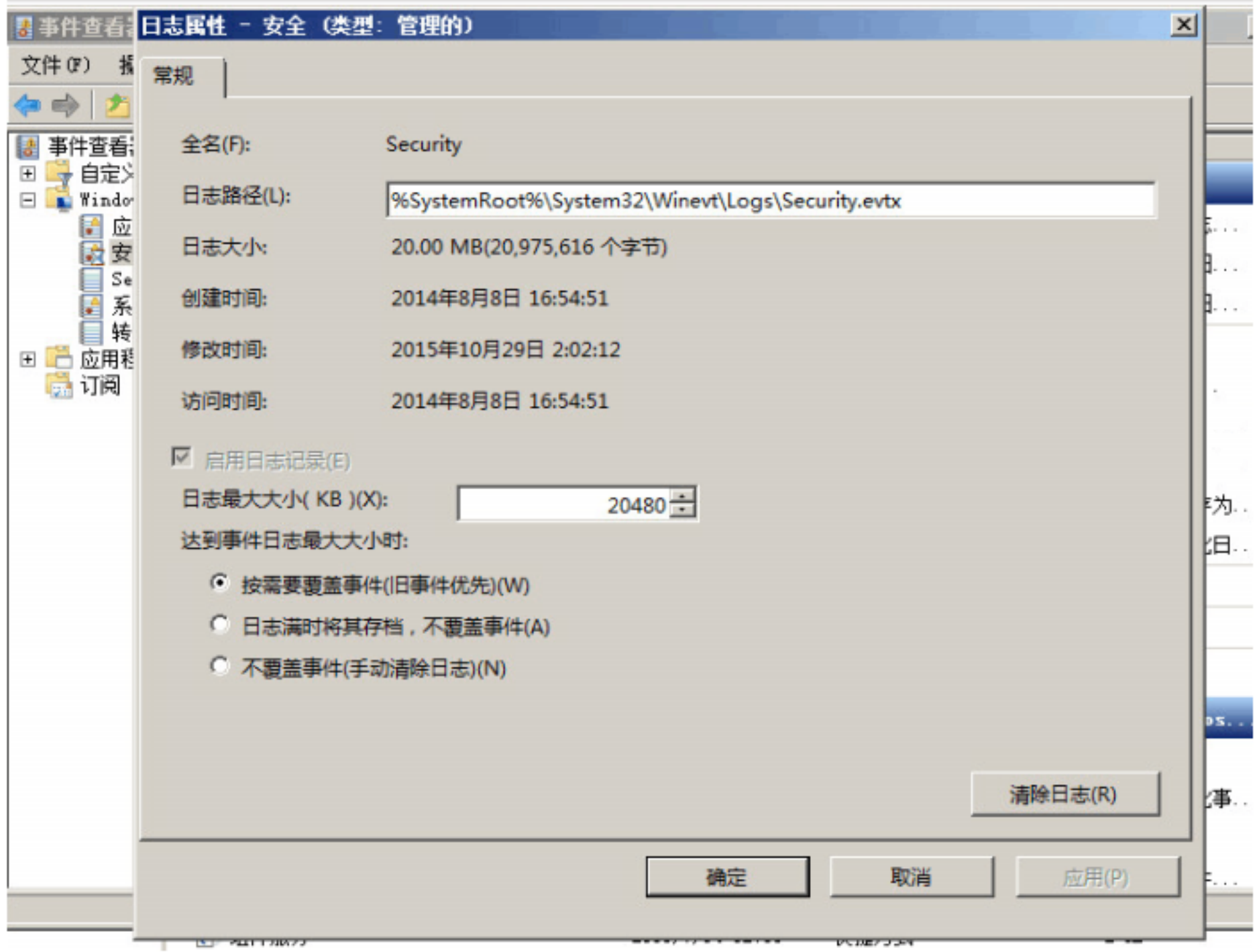
2、 服务器安全事件审核安全加固。 （请截图）

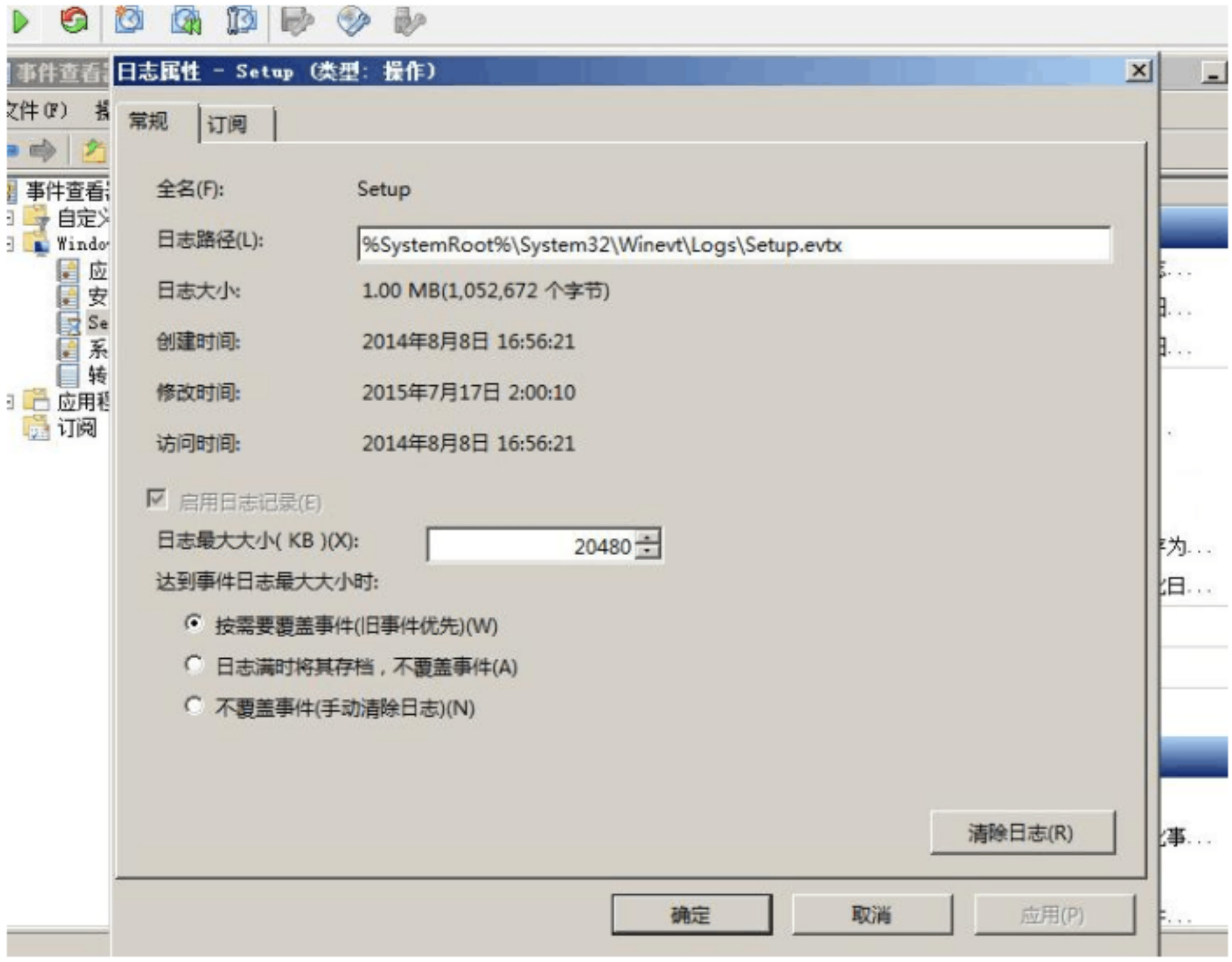
1） 设置 Windows 服务器安全事件审核策略， 可通过“ 控制面板－管理工具－本地安全策略 ”中“ 本地策略 ”下的“ 审核策略 ”进行安全设置，将其下的所有审核都设置成“ 成功 ”、“ 失败 ”（默认为“ 无审核 ” ）。

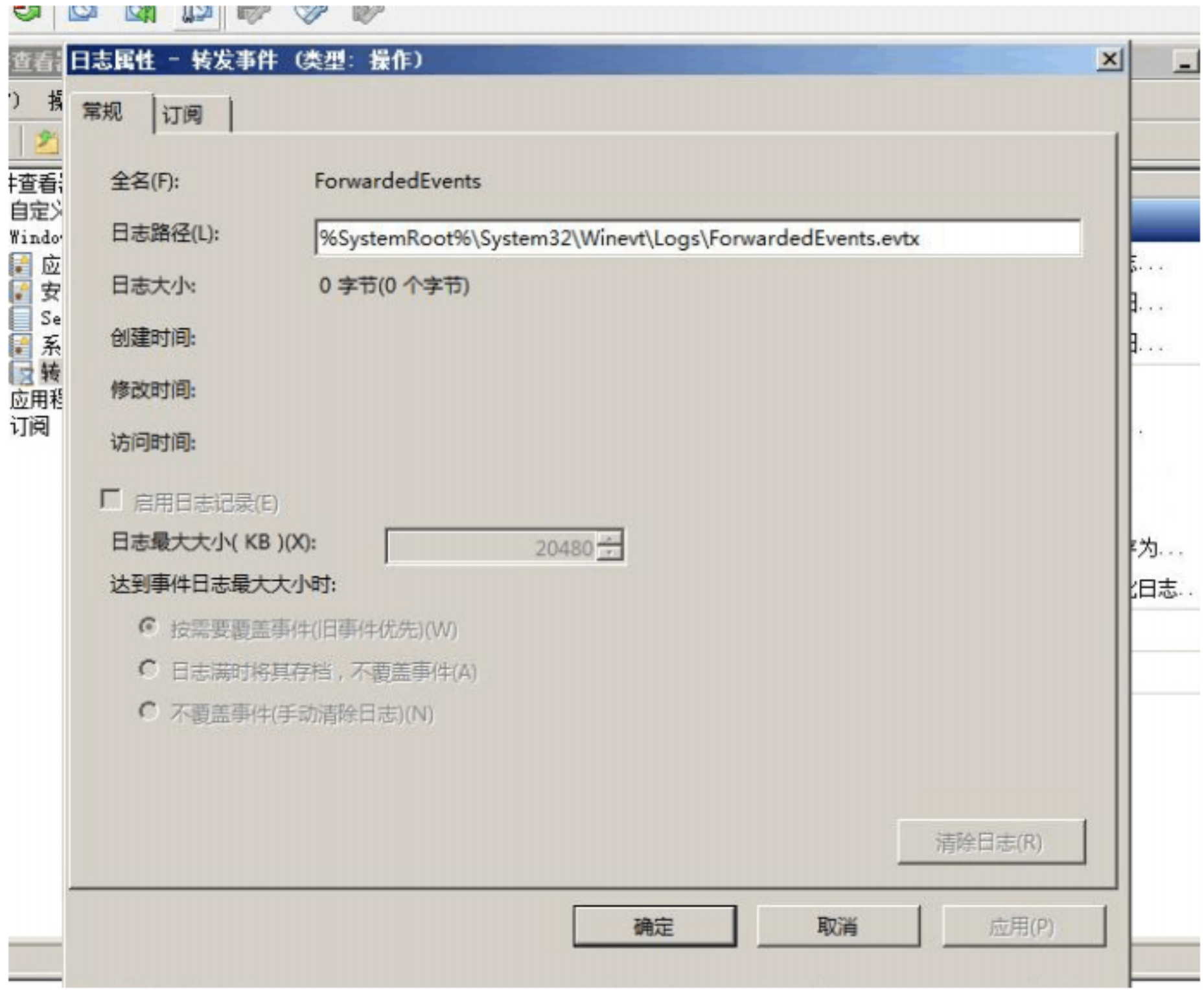
2） 设置日志系统的安全加固，打开“ 控制面板－管理工具－事件查看器 ”中，在“ Windows 日志 ”中选择一个日志类型，右击鼠标，设置“ 属性 ”的存储大小不小于 512KB （4096KB ）；覆盖周期不小于 15 天（ 60 天）。（请截图）



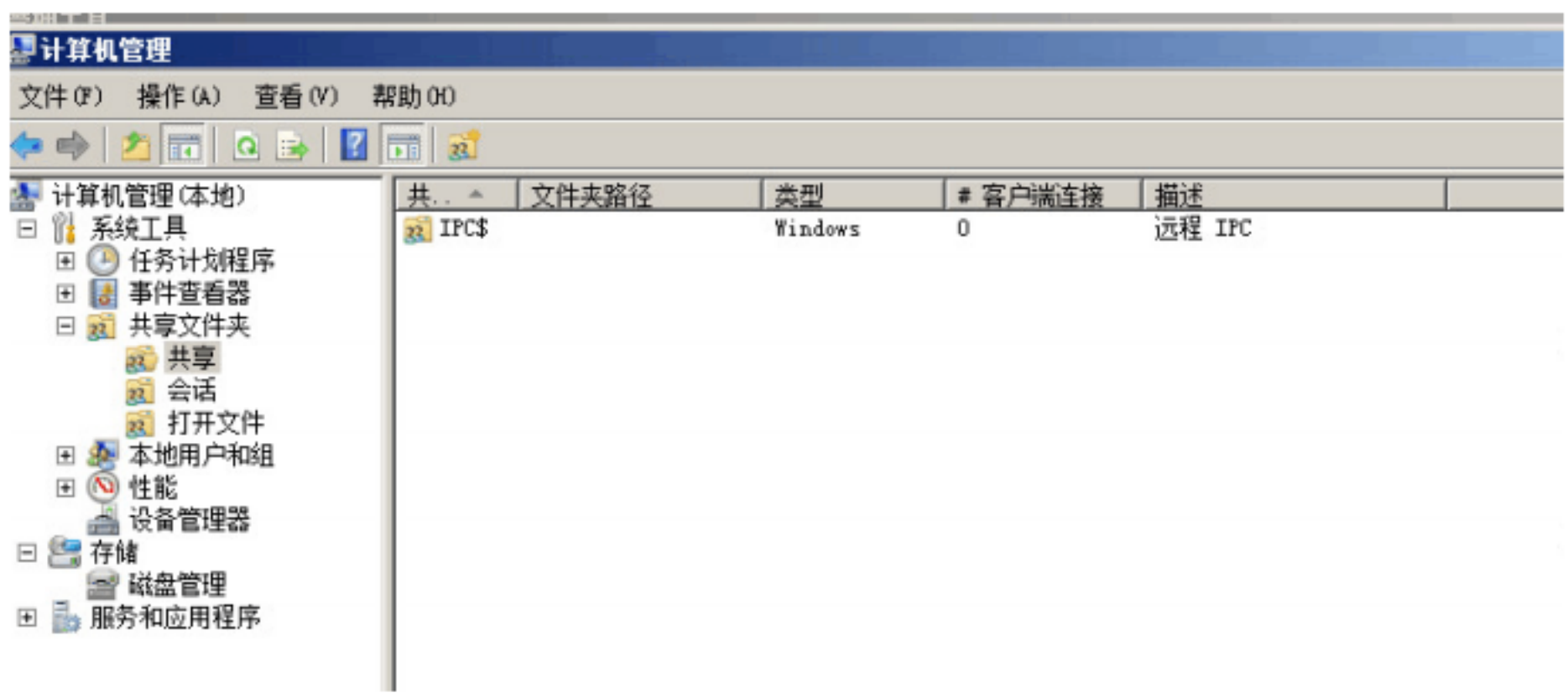

日志属性 - 应用程序 (类型: 管理的)
常规
订阅
全名(F): Application
日志路径(L): %SystemRoot%\System32\Winevt\Logs\Application.evtx
日志大小: 8.07 MB(8,458,240 个字节)
创建时间: 2014年8月8日 16:54:51
修改时间: 2015年10月29日 2:02:14
访问时间: 2014年8月8日 16:54:51
启用日志记录(E)
日志最大大小(KB)(X): 20480
达到事件日志最大大小时:
按需要覆盖事件(旧事件优先)(W)
日志满时将其存档，不覆盖事件(A)
不覆盖事件(手动清除日志)(N)
清除日志(R)
确定
取消
应用(P)


日志属性 - 安全 (类型: 管理的)
常规
全名(F): Security
日志路径(L): %SystemRoot%\System32\Winevt\Logs\Security.evtx
日志大小: 20.00 MB(20,975,616 个字节)
创建时间: 2014年8月8日 16:54:51
修改时间: 2015年10月29日 2:02:12
访问时间: 2014年8月8日 16:54:51
启用日志记录(E)
日志最大大小(KB)(X): 20480
达到事件日志最大大小时:
按需要覆盖事件(旧事件优先)(W)
日志满时将其存档，不覆盖事件(A)
不覆盖事件(手动清除日志)(N)
清除日志(R)
确定
取消
应用(P)


日志属性 - Setup (类型: 操作)
常规
订阅
全名(F):
Setup
日志路径(L):
%SystemRoot%\System32\Winevt\Logs\Setup.evtx
日志大小:
1.00 MB(1,052,672 个字节)
创建时间:
2014年8月8日 16:56:21
修改时间:
2015年7月17日 2:00:10
访问时间:
2014年8月8日 16:56:21
启用日志记录(E)
日志最大大小(KB)(X):
20480
达到事件日志最大大小时:
按需要覆盖事件(旧事件优先)(W)
日志满时将其存档，不覆盖事件(A)
不覆盖事件(手动清除日志)(N)
清除日志(R)
确定
取消
应用(P)



3、 关闭服务器共享资源， 可通过“控制面板－管理工具－计算机管理”中，选择“共享文件夹－共享”查看系统共享资源，删除不必要的多余共享资源。（请截图）



4、 自动锁屏设置

桌面点击右键－属性－屏幕保护程序，设置服务器自动锁屏时间为 3 分钟（参考）。（请截图）

5、 对系统安装的 FTP 中建立的用户进行用户权限管理，根据“最小资源配置原则”，为每个 FPT 用户分配最小访问目录权限，访问目前权限设置，如用户可进行写操作，则对用户可分配的磁盘空间大小进行限制。（是否开启 FTP）

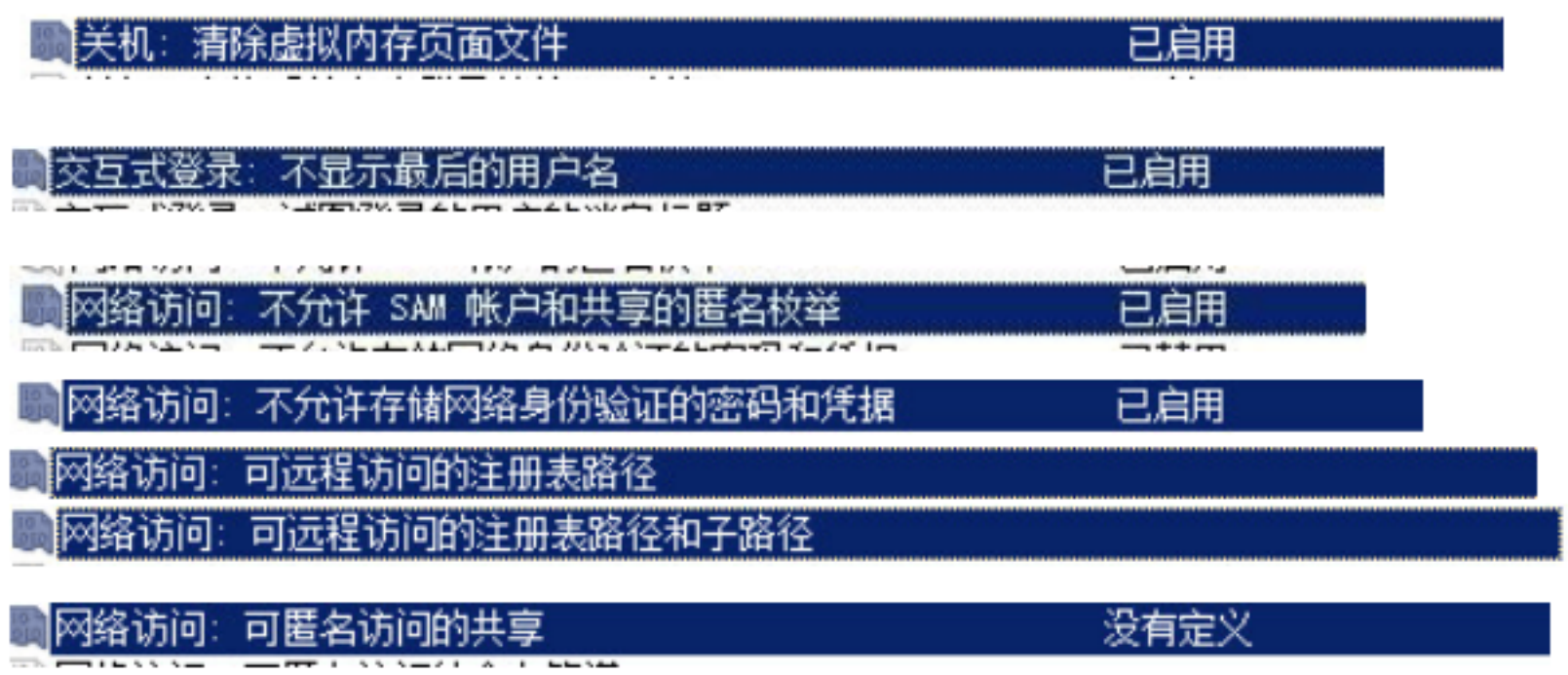
6、 根据工作的需要，为每个访问服务器的工作人员创建访问权限合理的用户，或建立工作人员访问服务器的纸质操作记录。（是否只有一个管理员操作）

7、 设置系统剩余信息保护安全加固

1） 设置 Windows 服务器安全事件审核策略，可通过“控制面板－管理工具－本地安全策略”中“本地策略”下的“安全选项”进行安全设置。

序号	属性	可选择值
1	关机：清除虚拟内存页面文件	已启用
2	交互式登录 ：不显示最后的用户名	已启用
3	网络访问：不允许 SAM 帐户和共享的匿	已启用

	名枚举	
4	网络访问：不允许为网络身份验证储存凭证	已启用
5	网络访问：可远程访问的注册表路径	全部删除
6	网络访问：可远程访问的注册表路径和子路径	全部删除
7	网络访问 :可匿名访问的共享	全部删除 (根据实际共享情况要配置)



8、 请根据实际需要为系统安装病毒查杀软件（ 360、瑞星防毒）、防木马软件（ 360 木马查杀、安全卫士），安全狗服务器版（ safedog）等类似的软件并定期进行病毒库升级，以及定期进行系统安全检测，做好该项工作的纸质记录的存档。 （请回答）
已安装：

9、 在系统服务中关闭不必要的系统服务，如：DHCP、FTP等（请截图）

10、打开“组策略” gpedit.msc 中，在“计算机配置” ->“管理模板” ->“ Windows 组件” ->“远程桌面服务” ->“远程桌面会话时间限制”中，查看在“会话时间限制”中，对空闲的会话（没有客户端活动的会话）继续留在服务器上的最长时间进行配置。 （请截图）

11、能够通过 360 等软件对系统补丁进行自动更新。 （请截图）

服务器安全狗(v4.2增强版)
我的服云
服务器优化
杀毒
网络防火墙
主动防御
定时任务
防护日志
软件管家
云备份
服务器安全狗
服务器体检
系统漏洞修复
系统帐号优化
目录权限优化
数据库优化
系统服务优化
注册表优化
垃圾清理
扫描结束,共有补丁6个,0个高危漏洞需要立即修复!
重新扫描
修复漏洞
忽略选中漏洞
补丁管理
严重程度
补丁描述
发布日期
状态
操作
高危漏洞补丁(0)
可选补丁(6)
KB2836502 不能显示某些 JPEG 图像 详情 2013-06-10 未修复
KB2835174 在Windows Server 2008 R2 SP1 中的产品激活… 详情 2013-05-13 未修复
KB2794119 Windows 更新程序 详情 2013-01-21 未修复
KB2757817 Windows Server 2008 和 Windows Server 2008… 详情 2012-10-08 未修复
KB2548388 解决打开程序的系统菜单时 Microsoft Narrato… 详情 2011-6-13 未修复
KB2529073 某些 USB 驱动程序中的二进制文件没有进行更新 详情 2011-5-9 未修复
组件升级(0)