# 一.账户管理和认证授权

**1.账号**

**1.1 默认账户安全**

禁用“Guest”账户。

禁用或删除其他无用账户（可以先禁用账户3个月，确认没有问题后删除）。

**操作步骤：**

进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：缺省帐户Administrator－>属性Guest帐号->属性

**1.2 按照用户分配帐户**

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

**操作步骤：**

进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：根据系统的要求，设定不同的帐户和帐户组，管理员用户，数据库用户，审计用户，来宾用户。

**1.3 定期检查并删除与无关帐户**

删除或锁定与设备运行、维护等与工作无关的帐户

**操作步骤：**

进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：删除或锁定与设备运行、维护等与工作无关的帐户。

**1.4 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：**进入“控制面板->管理工具->本地安全策略”，打开“本地策略”->“安全选项”->选择“交互式登录:不显示最后的用户名” 设置“已启用”

**配置样例**：



**2.口令**

**2.1 密码复杂度**

密码复杂度要求满足以下策略：

* 最短密码长度 8个字符，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2种：
* 英语大写字母 A, B, C, … Z
* 英语小写字母 a, b, c, … z
* 西方阿拉伯数字 0, 1, 2, … 9
* 非字母数字字符，如标点符号，@, #, $, %, &, \*等

**操作步骤：**

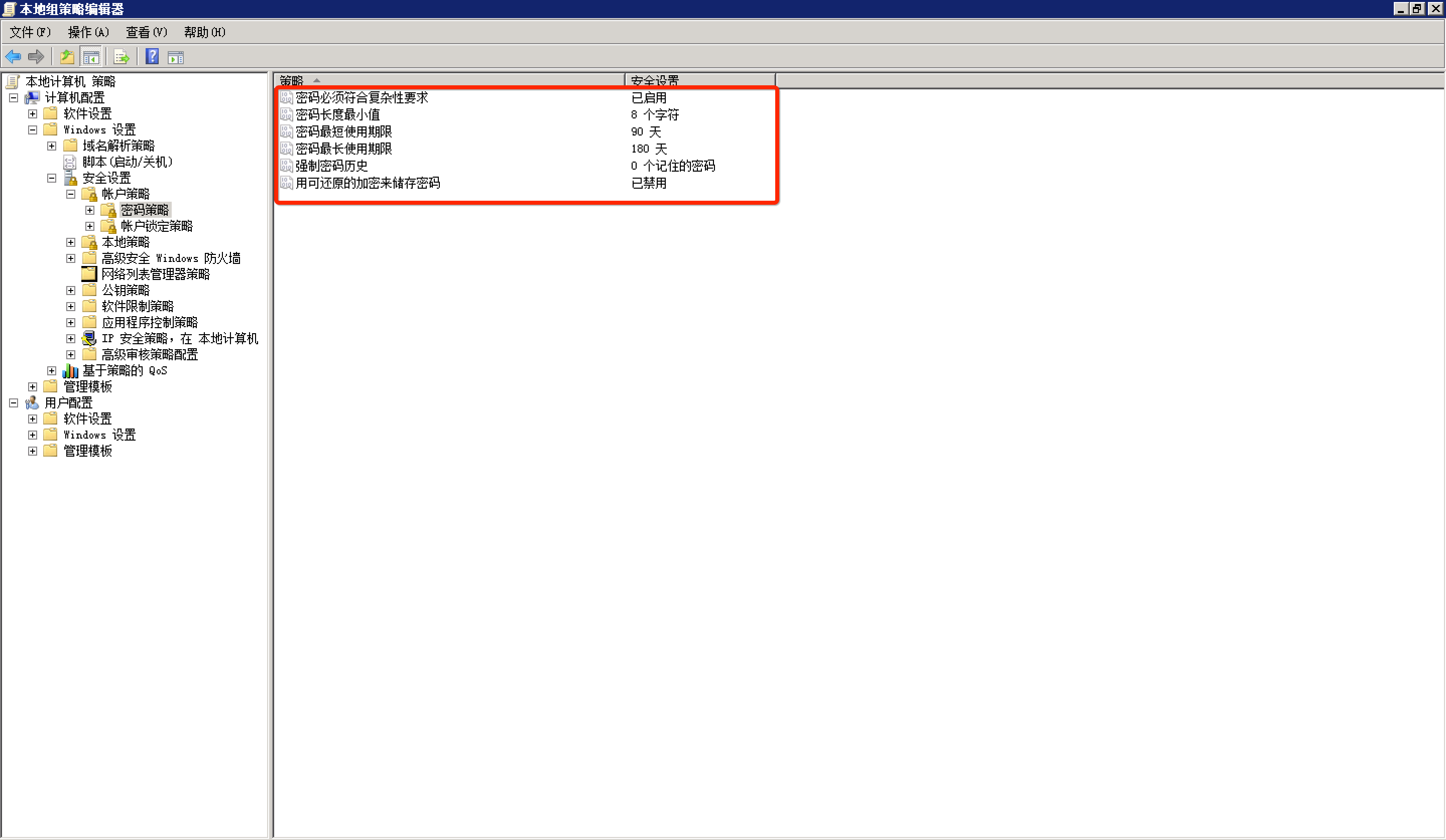
进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：查看是否“密码必须符合复杂性要求”选择“已启动”

**2.2 密码最长留存期**

对于采用静态口令认证技术的设备，帐户口令的生存期不长于90天。

**操作步骤：**进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：配置“密码最长存留期”

**配置样例**：



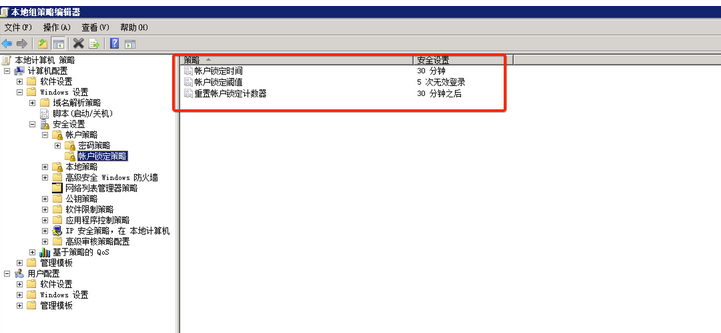
**2.3 帐户锁定策略**

对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过10次，锁定该用户使用的帐户。

**操作步骤：**

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->帐户锁定策略”：配置“帐户锁定阀值”设置。

**配置样例：**



**3.授权**

**3.1远程关机**

在本地安全设置中从远端系统强制关机只指派给Administrators组。

**操作步骤：**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”:配置“从远端系统强制关机”设置

**3.2 本地关机**

在本地安全设置中关闭系统仅指派给Administrators组。

**操作步骤：**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”:授权配置“关闭系统”设置

**3.3 用户权限指派**

在本地安全设置中取得文件或其它对象的所有权仅指派给Administrators

**操作步骤：**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”：“取得文件或其它对象的所有权”设置用户

**3.4 授权帐户登陆**

在本地安全设置中配置指定授权用户允许本地登陆此计算机。

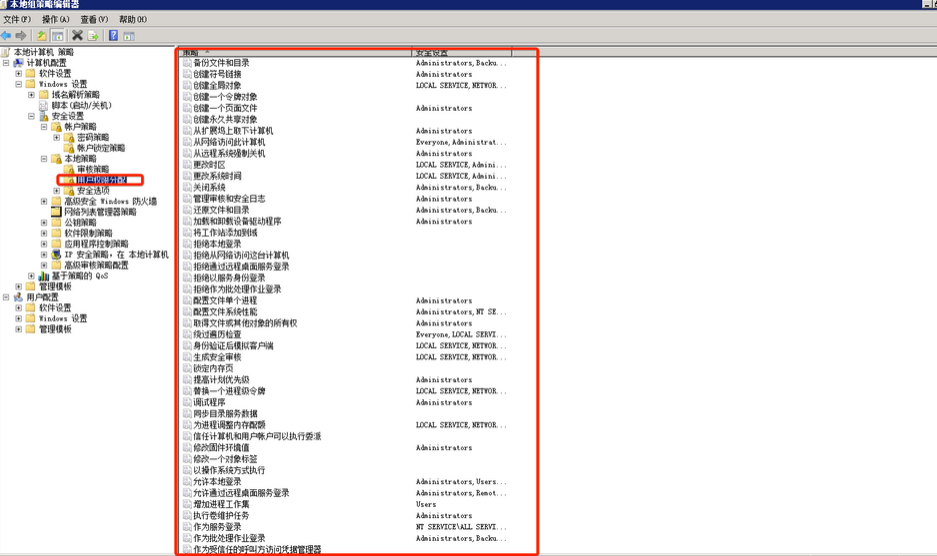
**操作步骤：**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”“从本地登陆此计算机”设置为“指定授权用户”

**3.5 授权帐户从网络访问**

在组策略中只允许授权帐号从网络访问(包括网络共享等，但不包括终端服务)此计算机。

**配置样例：**



**操作步骤**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”“从网络访问此计算机”设置为“指定授权用户”

# 二.日志配置操作

**4.日志配置**

**4.1 审核登录**

设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的帐户，登录是否成功，登录时间，以及远程登录时，用户使用的IP地址。

**操作步骤**

开始->运行-> 执行“ 控制面板->管理工具->本地安全策略->审核策略”审核登录事件。

**4.2 审核策略**

启用组策略中对Windows系统的审核策略更改，成功和失败都要审核

**操作步骤**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中“审核策略更改”设置。

**4.3 审核对象访问**

启用组策略中对Windows系统的审核对象访问，成功和失败都要审核。

**操作步骤**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核对象访问”设置。

**4.4 审核事件目录服务访问**

启用组策略中对Windows系统的审核目录服务访问，失败。

**操作步骤**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核目录服务器访问”设置。

**4.5 审核特权使用**

启用组策略中对Windows系统的审核特权使用，成功和失败都要审核。

**操作步骤**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核特权使用”设置。

**4.6 审核系统事件**

启用组策略中对Windows系统的审核系统事件，成功和失败都要审核。

**操作步骤**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核系统事件”设置。

**4.7 审核帐户管理**

启用组策略中对Windows系统的审核帐户管理，成功和失败都要审核。

**操作步骤**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核帐户管理” 设置。

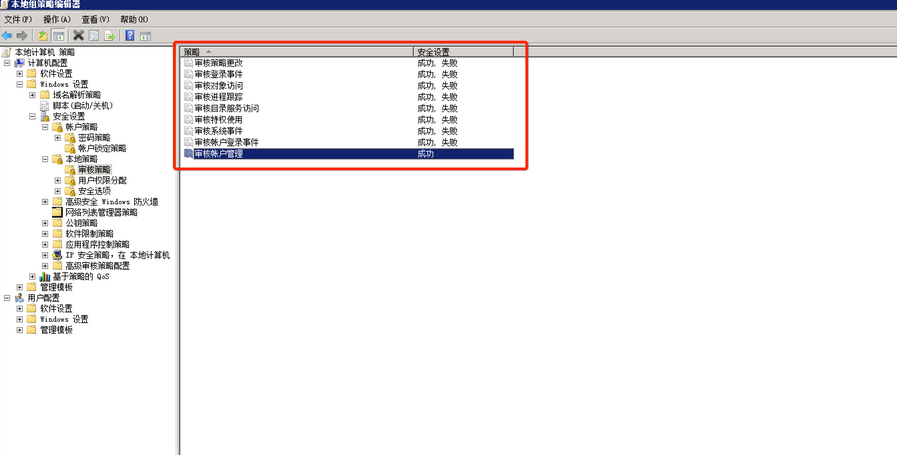
**4.8 审核过程追踪**

启用组策略中对Windows系统的审核过程追踪失败。

**操作步骤**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核过程追踪”设置。

**配置样例：**



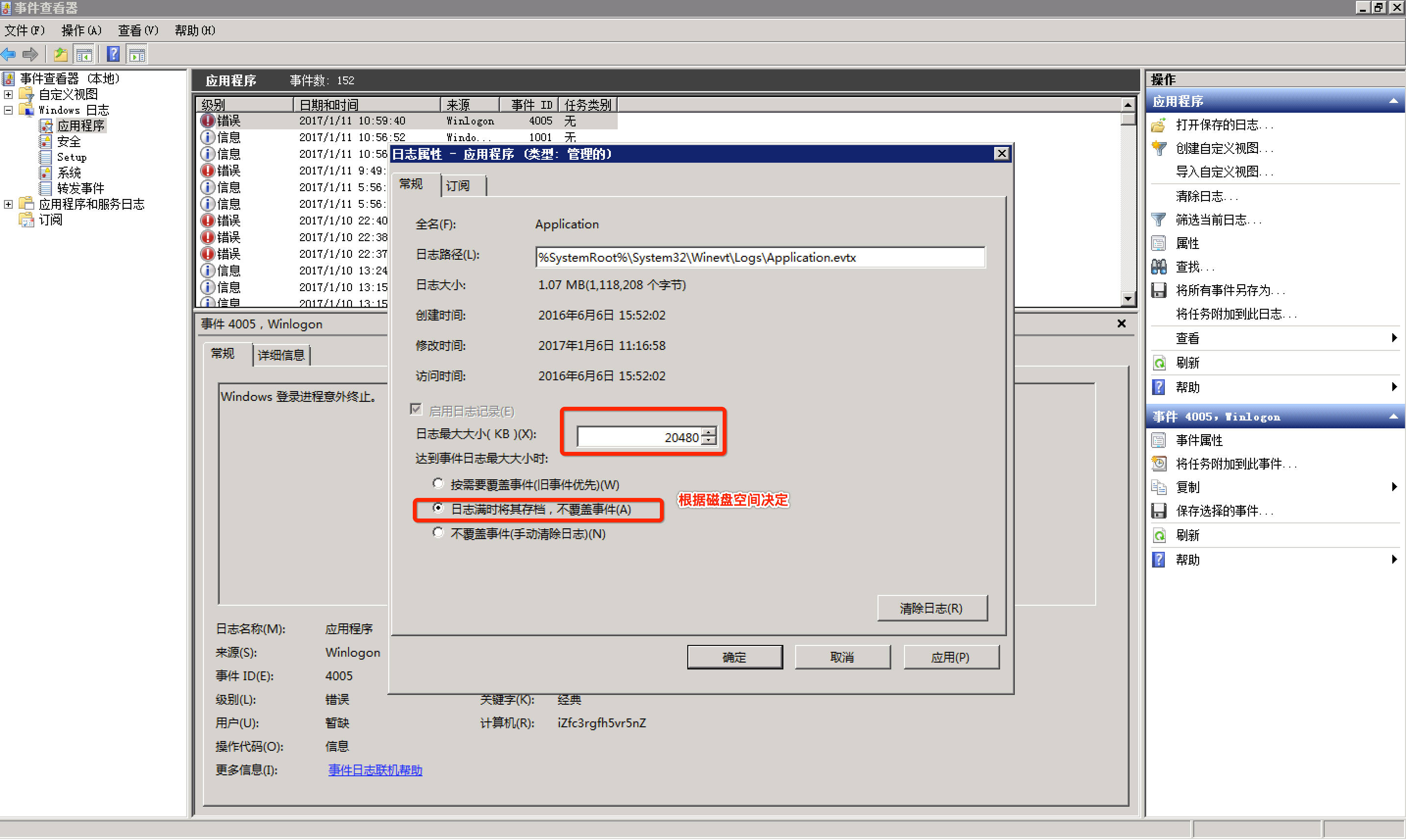
**4.9 日志文件大小**

设置应用日志文件大小至少为8192KB，可以根据磁盘空间配置日志文件大小，尽可能的记录的日志越多越好，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**

进入“控制面板->管理工具->事件查看器”，在“事件查看器（本地）”中：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。

**配置样例：**



# 三.IP协议安全配置

**5.IP协议安全**

**5.1 启用SYN攻击保护**

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连接请求数阀值为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**

在“开始->运行->键入regedit”，推荐值配置：

1. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SynAttackProtect; 推荐值：2。
2. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxPortsExhausted; 推荐值：5。
3. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpen; 推荐值数据：500。
4. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpenRetried。推荐值数据：400。

# 四.文件权限

**6 共享文件夹及访问权限**

**6.1关闭默认共享**

非域环境中，关闭Windows硬盘默认共享，例如C$，D$。

**操作步骤**

进入“开始－>运行－>Regedit”，进入注册表编辑器，推荐值配置：

1. HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer 键，值为 0。

**6.2 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权限共享此文件夹。

**操作步骤**

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”。进入“控制面板->管理工具->计算机管理”，进入“系统工具－>共享文件夹”：查看每个共享文件夹的共享权限。

# 五.服务安全

**7.1禁用TCP/IP上的NetBIOS**

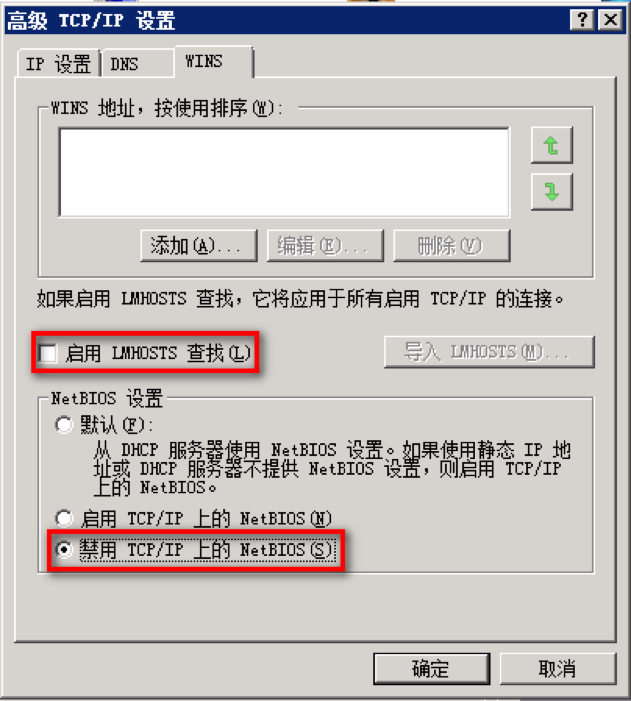
禁用TCP/IP上的NetBIOS协议，可以关闭监听的UDP 137（netbios-ns）、UDP 138（netbios-dgm）以及TCP 139（netbios-ssn）端口。

**操作步骤：**

在系统服务里禁用“TCP/IP NetBIOS Helper”服务。打开网络连接属性“Internet协议版本4（TCP/IPv4）”，点击“高级”，在“WINS”选项卡里，设置如下：

**7.2禁用不必要的服务**

关闭不必要的服务，以下为参考项：



# 六.安全选项

**8.1 启用安全选项**

**操作步骤：**

“本地安全策略”——“安全设置”——“本地策略”——“安全选项”，找到对应的项配置。

**配置样例**：



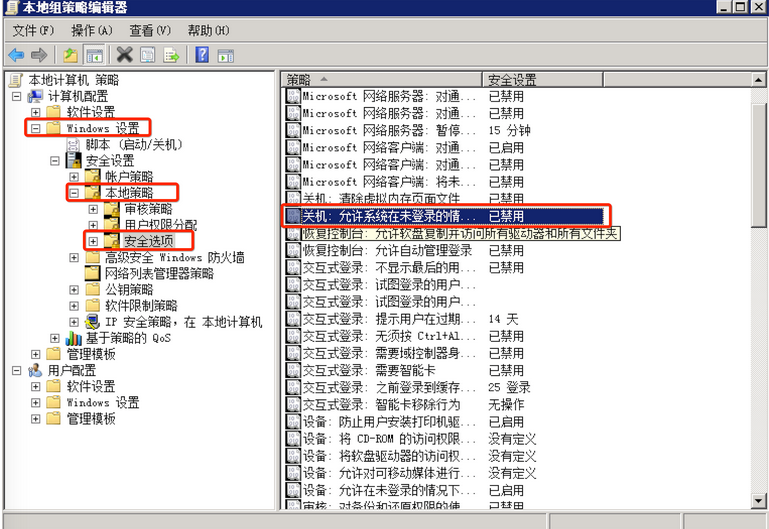
**8.2 禁用未登录前关机**

服务器默认是禁止显示在开机未进入系统前的，如果启用此设置，那么服务器安全性就大大降低，给与远程连接的黑客造成可乘之机，强烈建议禁用未登录前关机功能。

**操作步骤：**

开始—运行—输入gpedit.msc，打开组策略，然后点击 计算机配置—windows设置—本地策略—安全选项——关机: 允许系统在未登录前关机。

**配置样例：**

****

# 七.其他安全配置

**9.1 防病毒管理**

Windows系统需要安装防病毒软件。

**操作步骤：**

安装企业级防病毒软件，并开启病毒库更新及实时防御功能。

**9.2 设置屏幕保护密码和开启时间**

设置带密码的屏幕保护，并将时间设定为5分钟。

**操作步骤：**

启用屏幕保护程序，设置等待时间为“5分钟”，启用“在恢复时使用密码保护”。进入“控制面板－>显示－>屏幕保护程序”：查看是否启用屏幕保护程序，设置等待时间为“5分钟”，启用“在恢复时使用密码保护”。

**9.3 限制远程登陆空闲断开时间**

对于远程登陆的帐号，设置不活动断连时间15分钟。

**操作步骤：**

“Microsoft网络服务器”设置为“在挂起会话之前所需的空闲时间”为15分钟。进入“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：查看是否“Microsoft网络服务器”设置为“在挂起会话之前所需的空闲时间”为15分钟

**9.4 操作系统补丁管理**

安装最新的Hotfix补丁。对服务器系统应先进行兼容性测试。

**操作步骤：**

安装最新的Hotfix补丁。对服务器系统应先进行兼容性测试。

注意：对于生产服务器，建议通知并自动下载更新，但是由管理员选择是否安装更新，而不应自动安装更新，防止自动更新补丁对生产环境产生影响。

**配置样例：**

