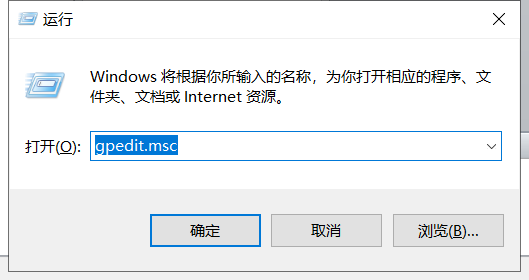
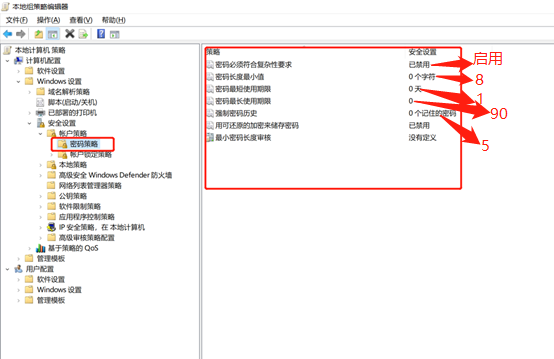
1. 密码策略

密码策略配置如下（运行>gpedit.msc>本地组策略编辑器>计算机配置>Windows设置>安全设置>帐户策略>密码策略）：密码必须符合复杂性要求->已启用、密码长度最小值->8个字符、密码最长使用期限->90天、密码最短使用期限->1天、强制密码历史->5个

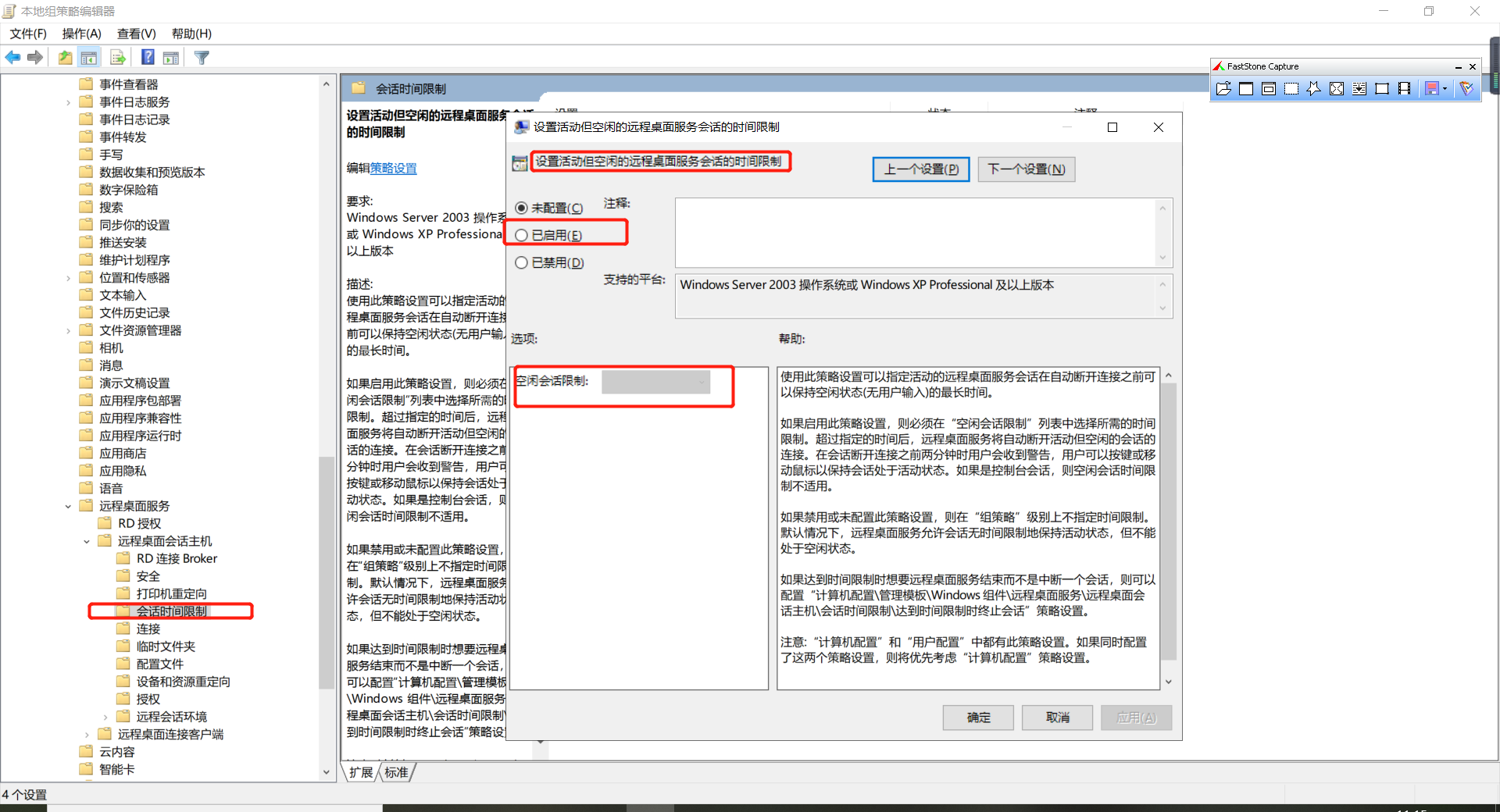


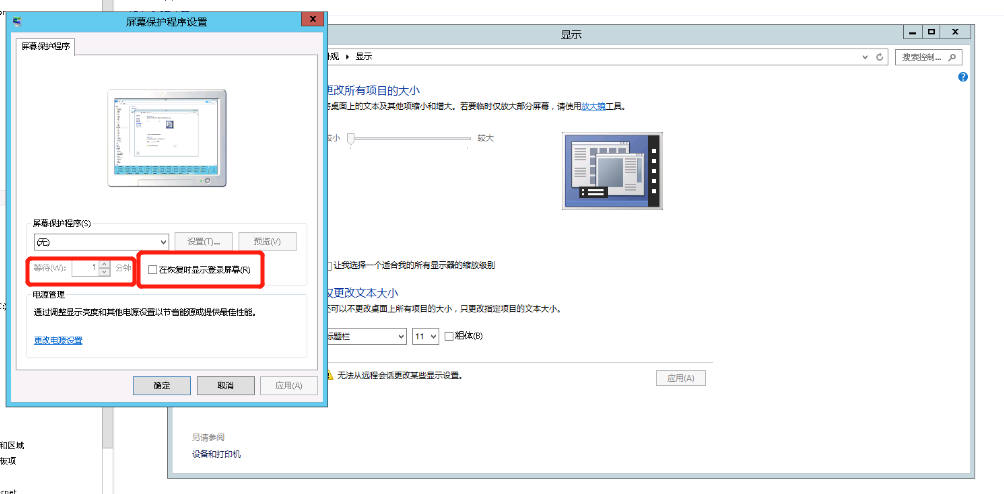


1. 超时自动退出时间

配置终端登录的超时锁定功能（运行>gpedit.msc>本地组策略编辑器>计算机配置>管理模板>Windows组件>远程桌面服务>远程桌面会话主机>安全>会话时间限制>设置活动但空闲的远程桌面服务会话的时间限制>已启用>5分钟）

开启屏幕保护时间（5分钟），并在恢复登录时需要重新鉴定

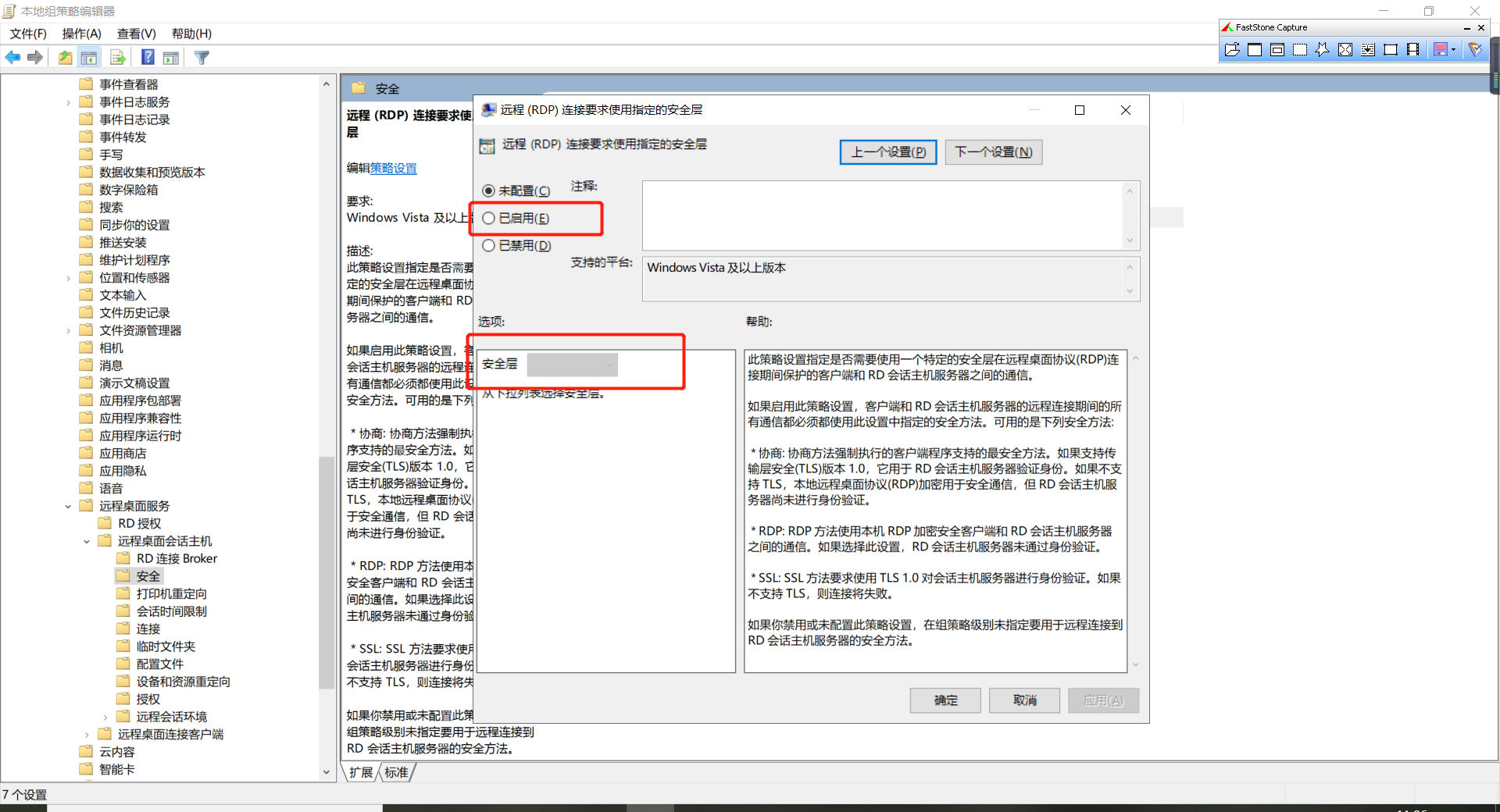


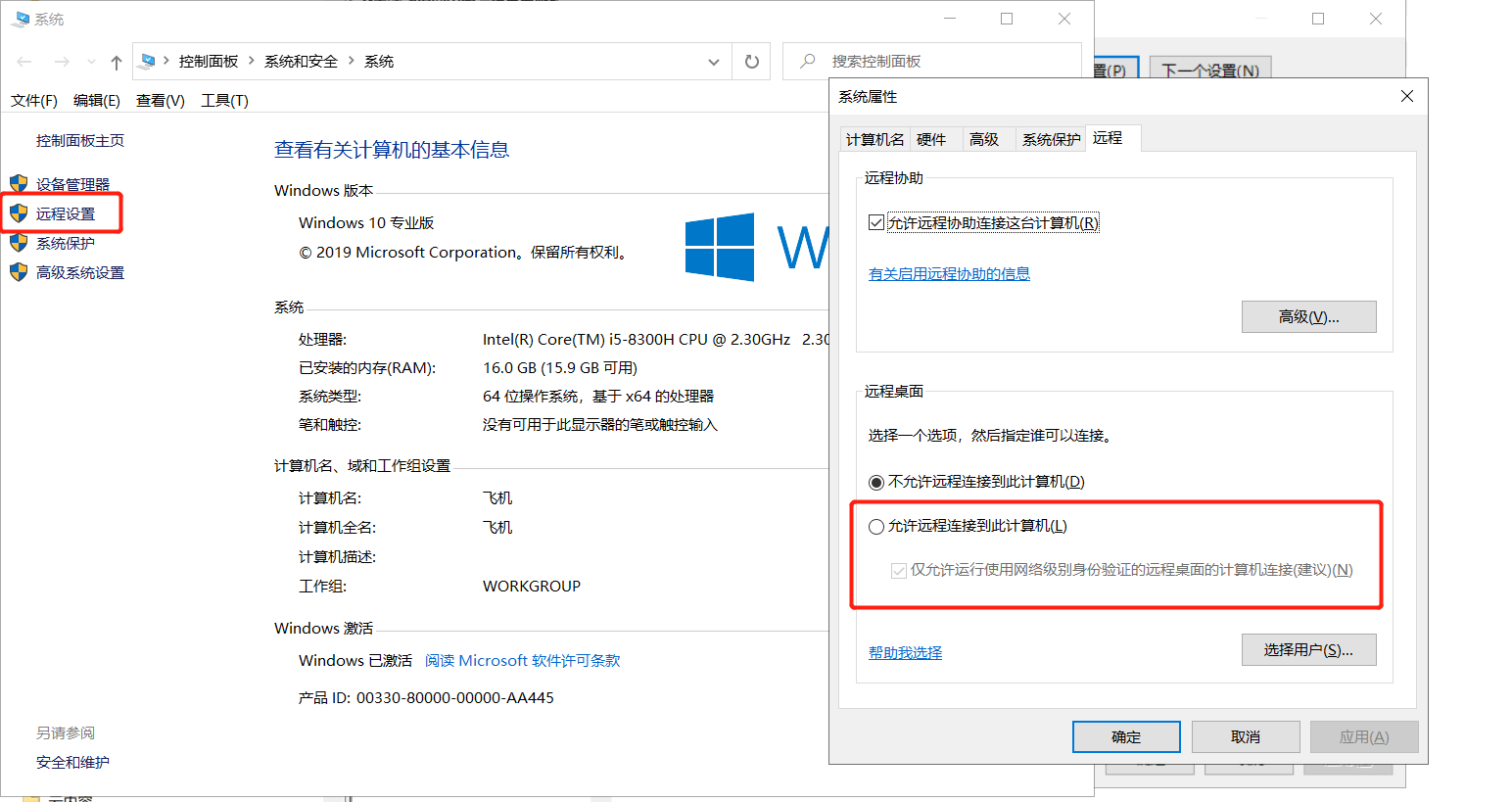


1. 未开启ssl安全层

建议（点击系统属性->远程）启用“仅允许运行使用网络级别身份验证的远程桌面的计算机连接（更安全）”

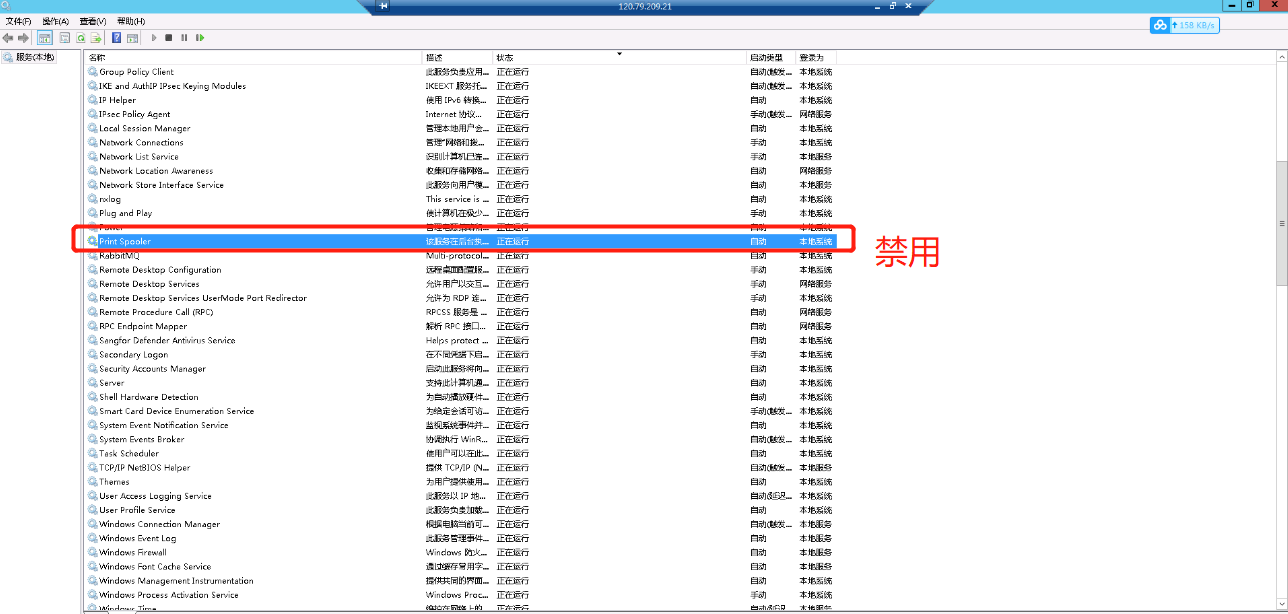
配置“远程（RDP)连接使用SSL安全层”措施（运行>gpedit.msc>本地组策略编辑器>计算机配置>管理模板>Windows组件>远程桌面服务 >远程桌面会话主机>安全>远程（RDP）连接要求使用指定的安全层>已启用> 选择SSL安全层 ），防止鉴别信息在网络传输过程中被窃听

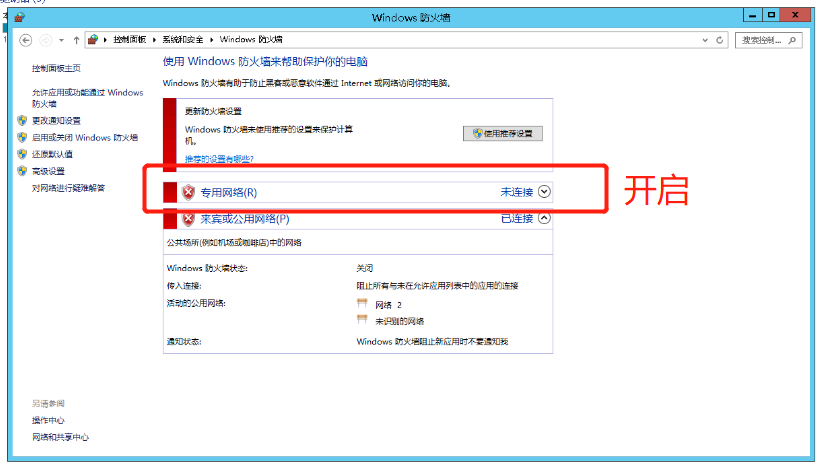




1. 未关闭多余服务、端口和默认共享

建议关闭多余的服务Print Spooler，关闭多余端口21、135、137、139、445、3389等



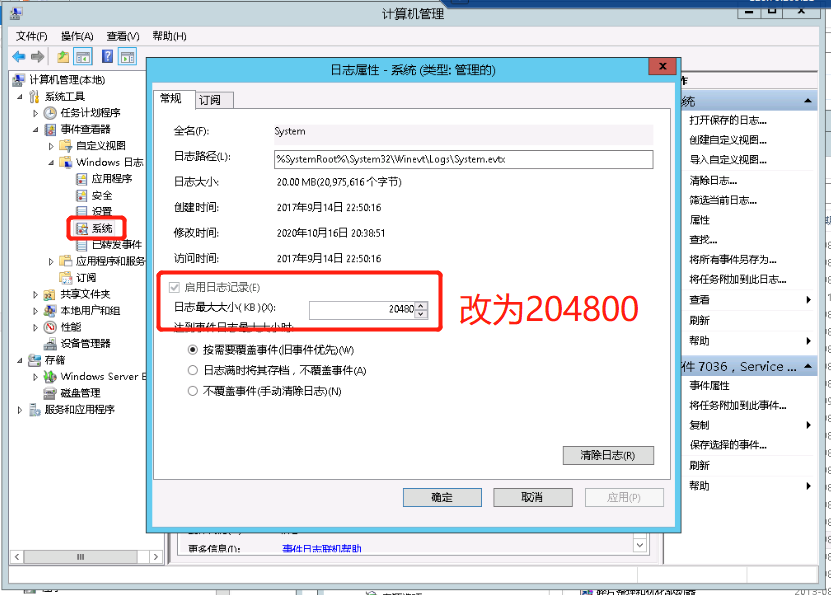
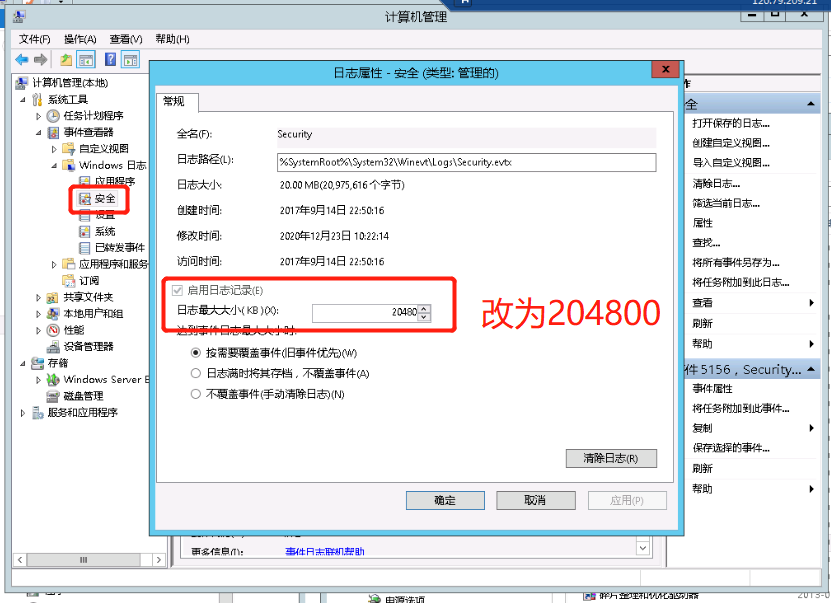
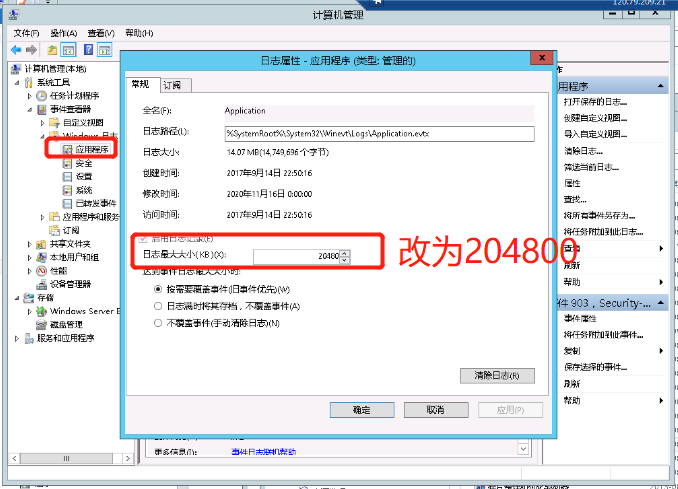




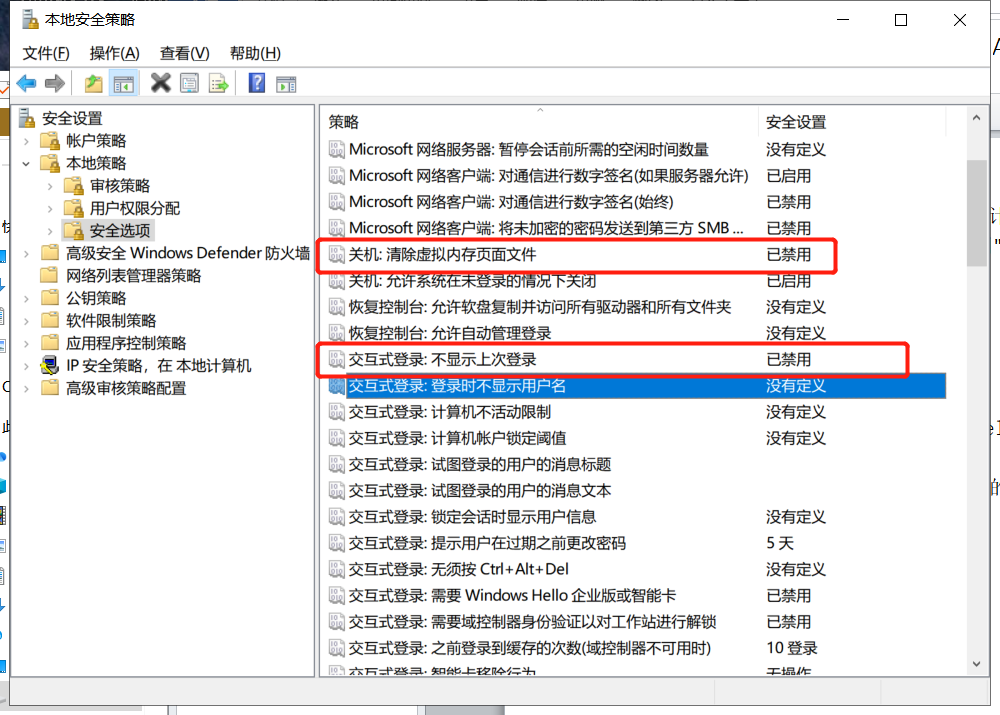
1. 日志容量不够200M

建议系统、安全、应用日志保存容量满足200M-1024M

计算机管理->事件查看器->Windows日志->系统、安全、应用日志->属性->日志最大大小改为204800

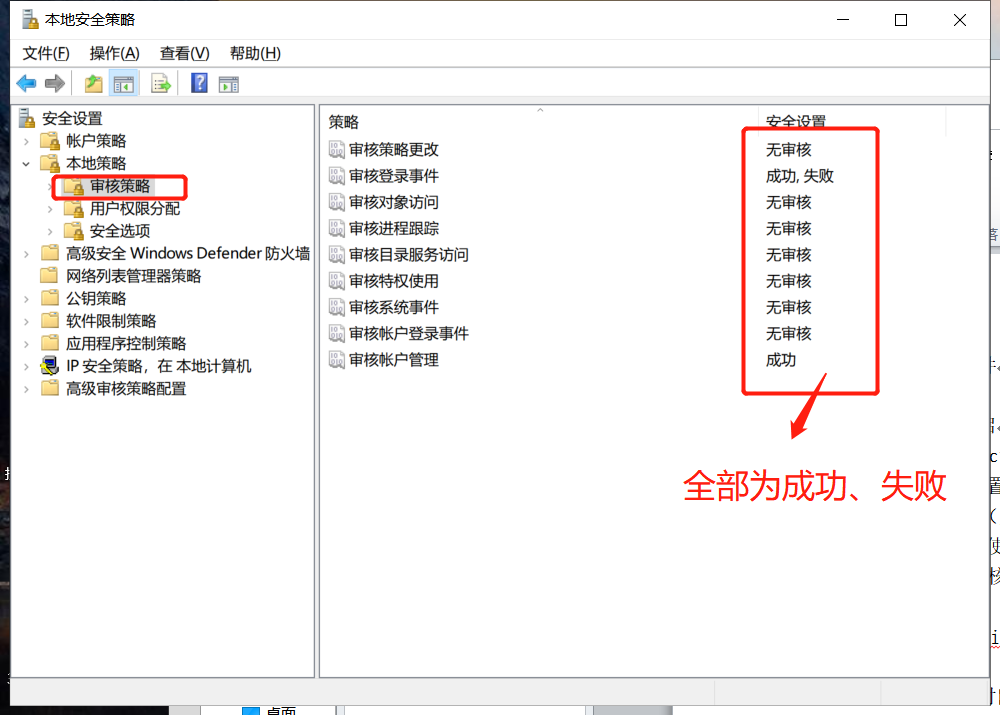


1. 清除用户信息（配置策略为本地计算机策略->计算机配置->Windows设置->安全设置->本地策略->本地策略->安全选项->启用"关机: 清除虚拟内存页面文件"和"交互式登录: 不显示上次登录"）

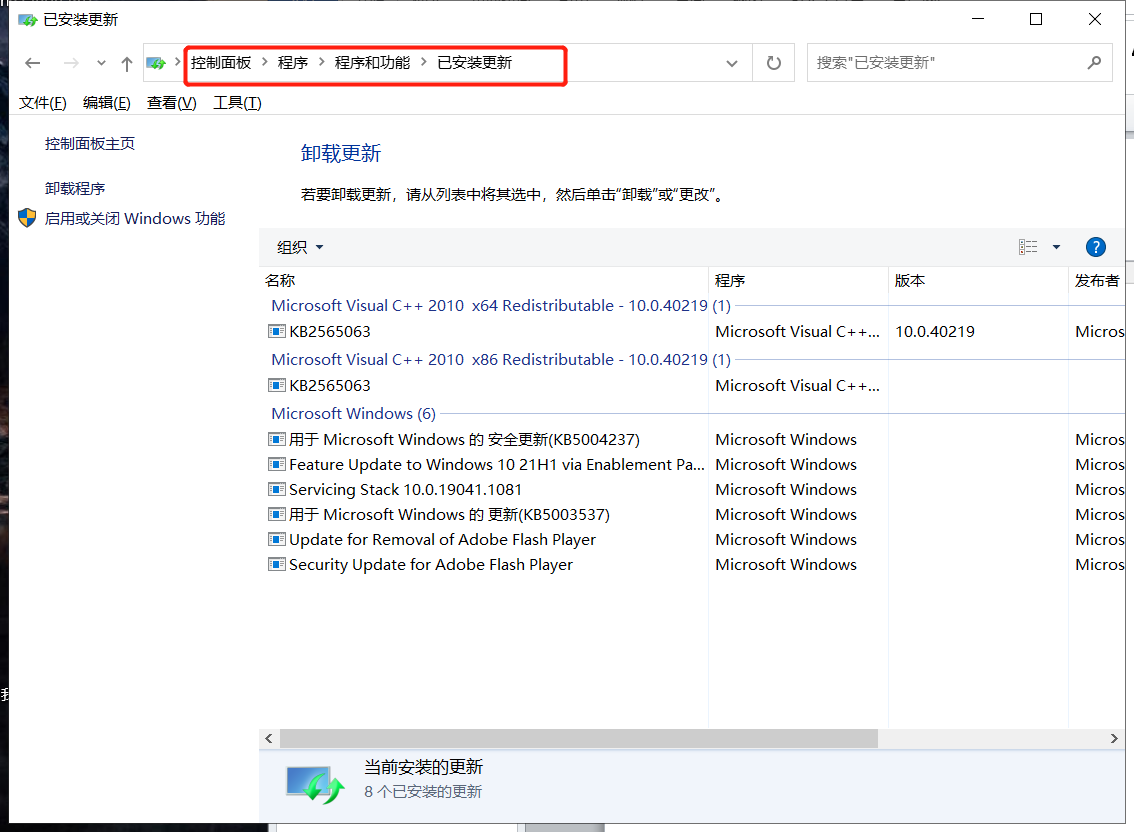


1. **安装杀毒软件（比如最新的360、火绒、安全管家等）**
2. 审计功能开启

运行“gpedit.msc”在计算机配置->Windows设置->安全设置->本地策略->审核策略），策略配置为：策略配置为：审核帐号登录事件 （成功，失败）、审核帐号管理 （成功，失败）、审核登录事件 （成功，失败）、审核对象访问 （成功,失败）、审核策略更改 （成功，失败）、审核特权使用 （成功，失败）、审核过程跟踪 （成功，失败）、审核系统事件 （成功，失败）、审核目录服务访问（成功、失败）

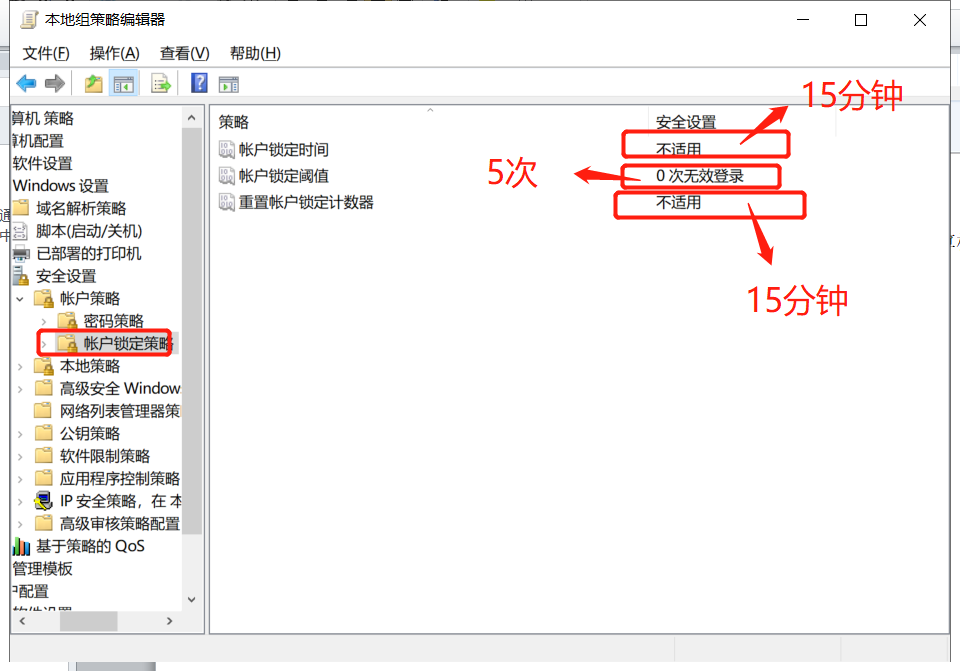


9. 截图系统补丁更新时间



10. 登录失败处理功能

登录失败处理功能配置如下（运行>gpedit.msc>本地组策略编辑器>计算机配置>Windows设置>安全设置>账户锁定策略



11. 定期进行备份

