网络安全技术基础实验报告

年 月 日

实验名称： 实验4 Windows本地安全策略设置 班级： 软件工程2003

姓名： 徐彬涵 学号： 32001272 同组人：

指导教师评定：

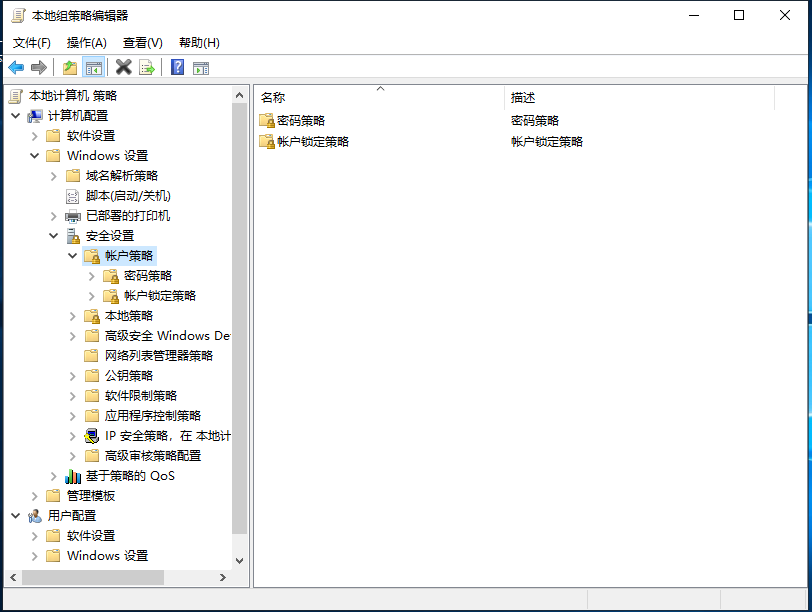
**一、实验目的和要求**

1. 了解操作系统安全的概念。
2. 使用secpol.msc、gpedit.msc、eventvwr.msc、lusrmgr.msc、服务管理等工具实施Windows本地安全策略设置。

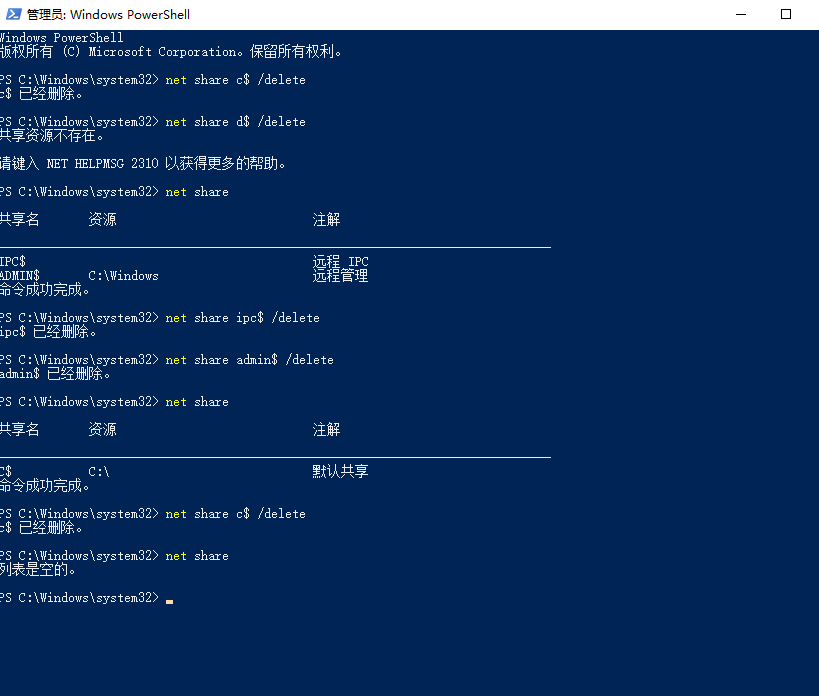
**二、实验内容**

**Windows安全配置**

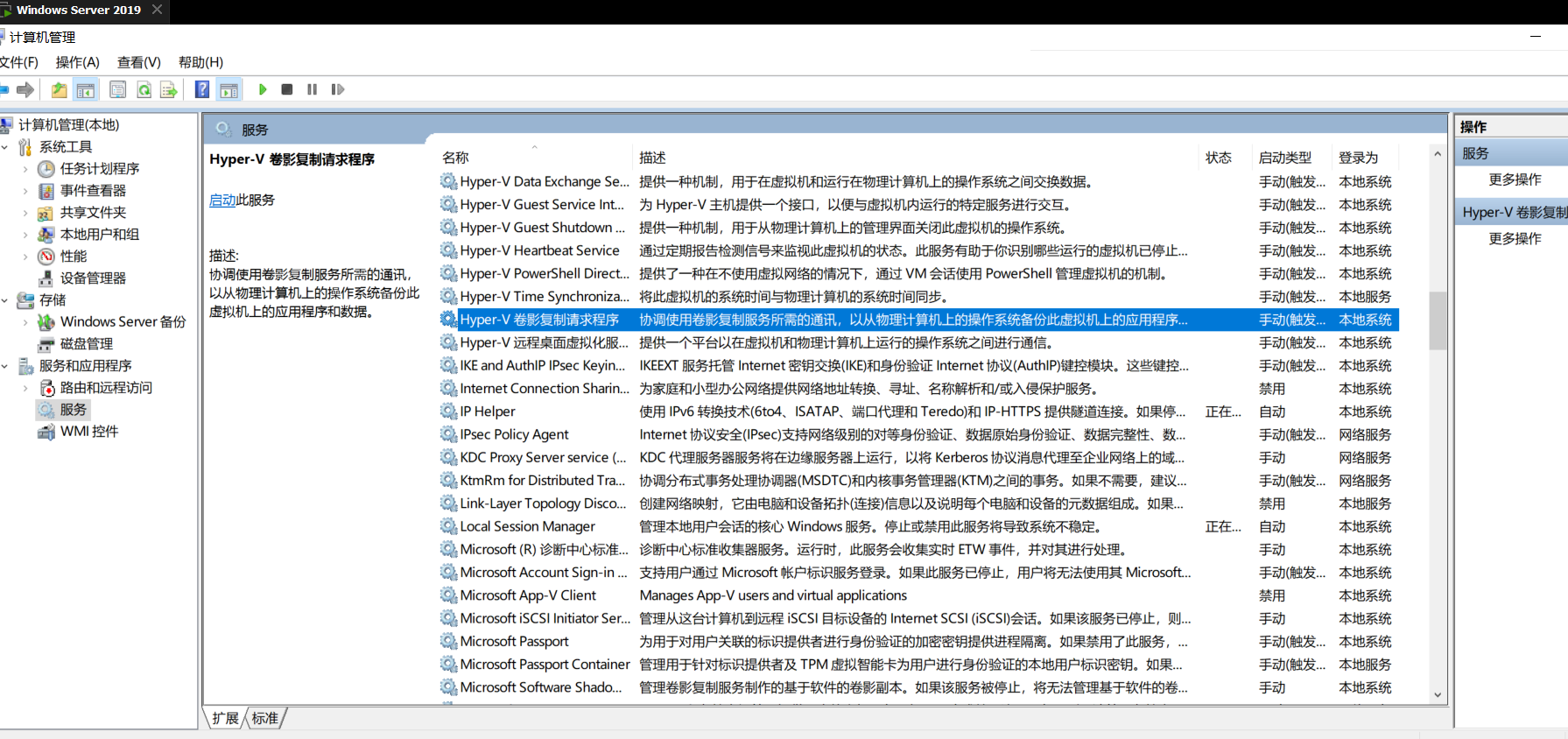
1. 账户管理和安全策略



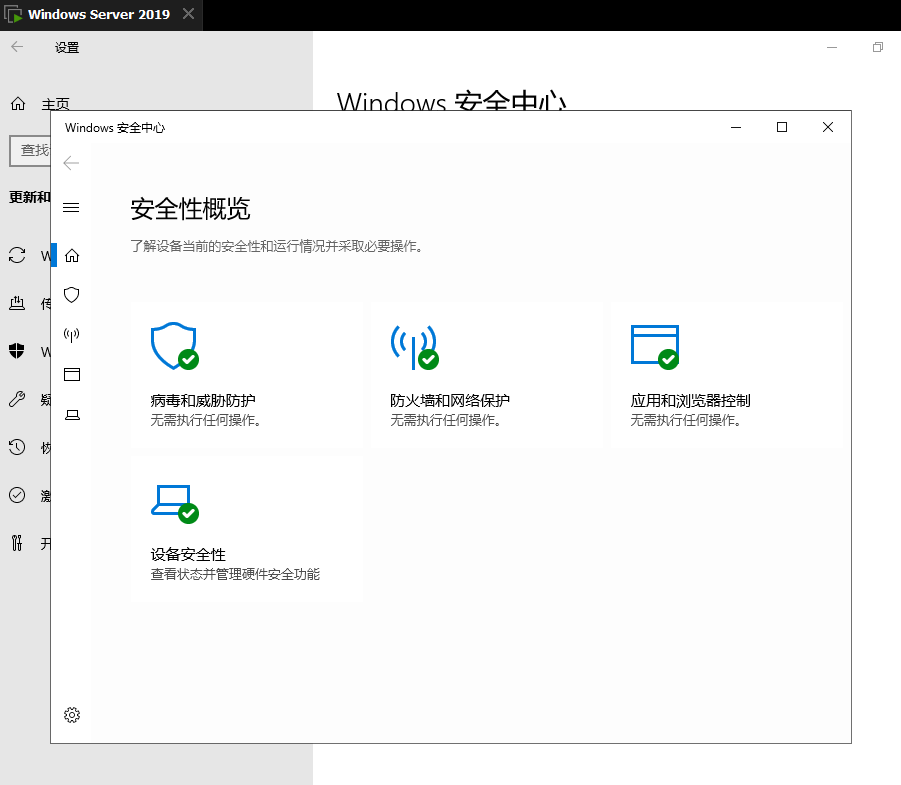
1. 删除所有网络资源共享(管理工具)



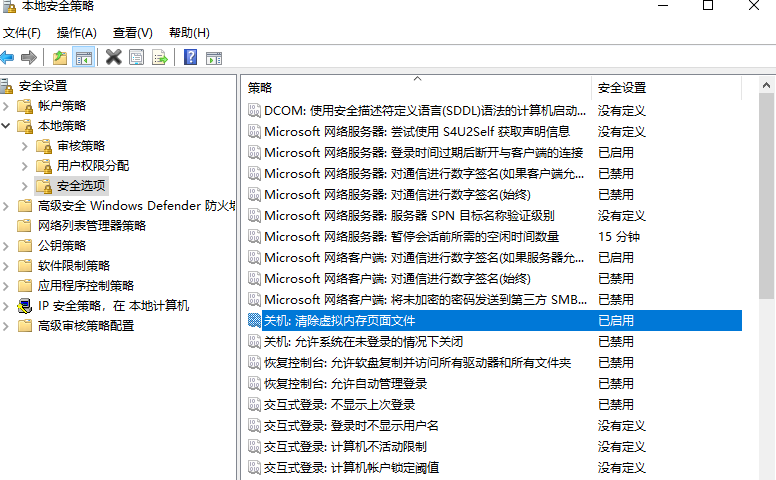
1. 关闭不需要的服务(我的电脑-管理)



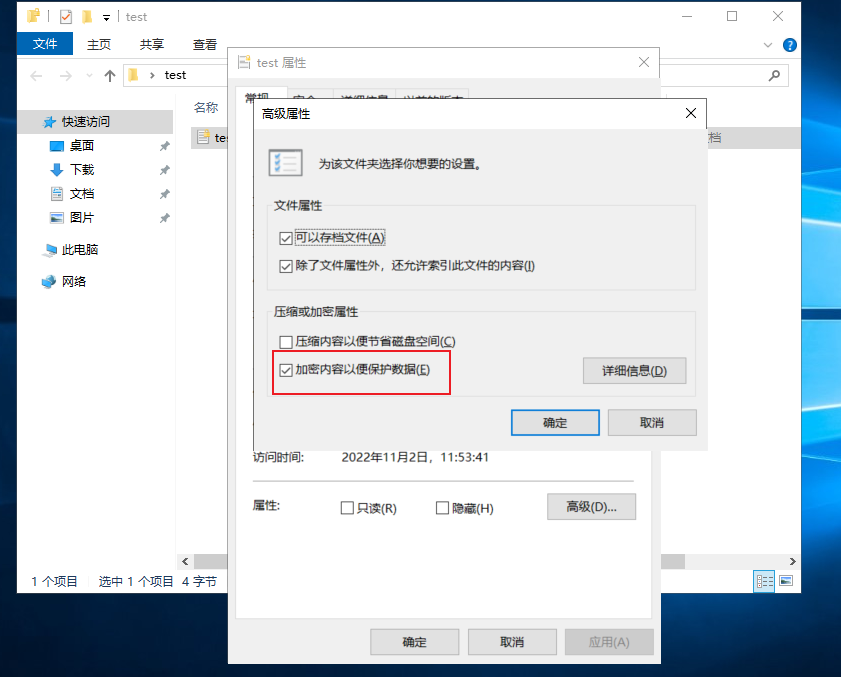
1. 安全管理网络服务

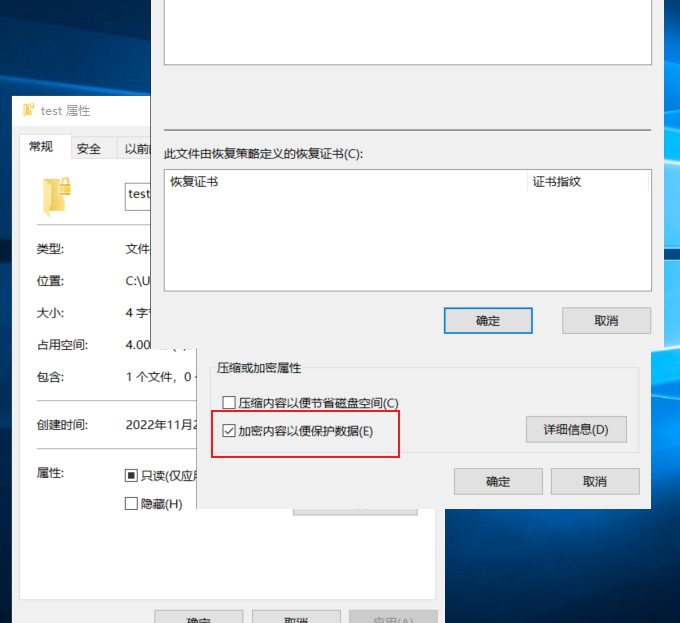


1. 清除页面交换文件

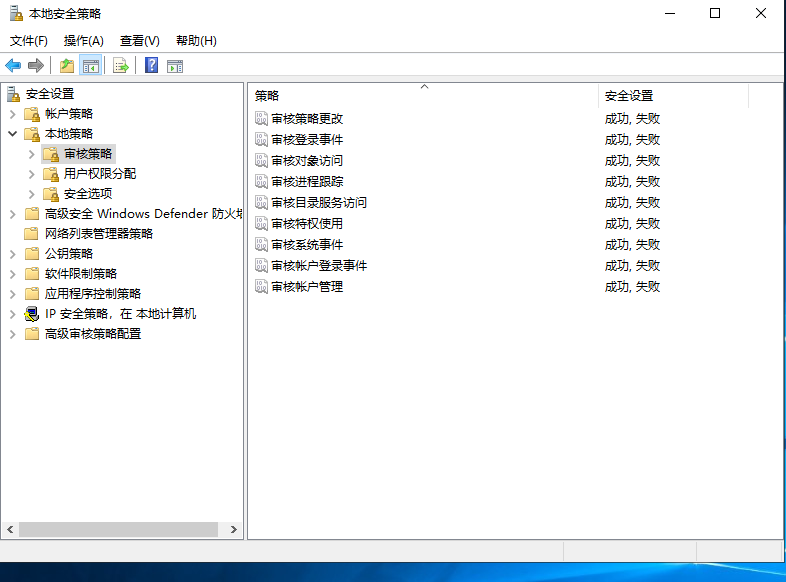


1. 文件和文件夹加密



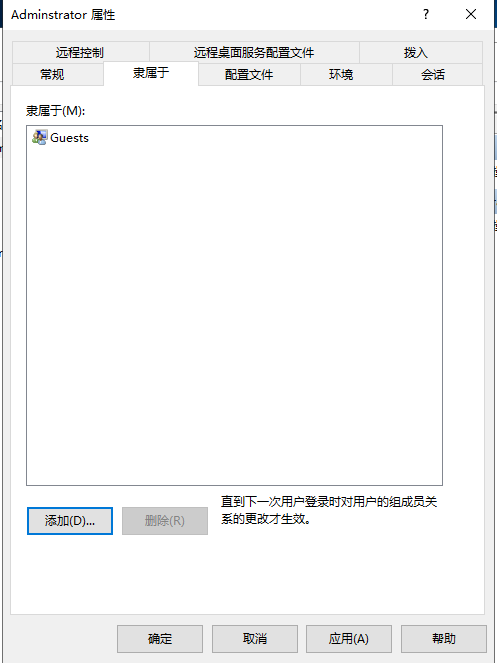


1. 开启系统审计功能。系统权限的设置在本地策略里面-审核策略，将审核策略、审核登录事件、审核对象、审核过程跟踪、审核目录服务访问、审核特权使用、审核系统事件、审核账户登录事件、审核账户管理设置为审计。



1. 创建陷阱账户：首先将系统Administrator账号改名，伪装成普通用户。然后创建一个名为“Administrator”的本地用户，把它的权限设置成最低，什么事也干不了的那种，并加上一个超过10位的超级复杂密码。这样可以让那些 Hacker们忙上一段时间，借此发现它们的入侵企图。测试设置效果



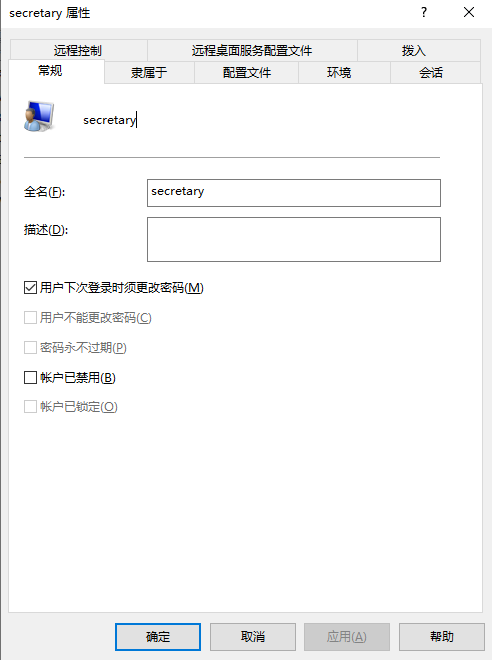


**密码为bex的md5值，前16位小写，后16位大写**

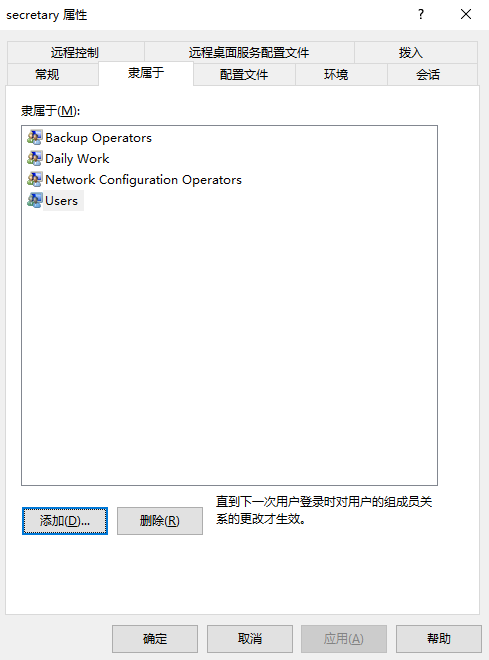
案例：某公司秘书授权可以登录领导的主机，定期为领导备份文件，并执行网络配置方面等有关管理工作，因此，在领导的主机中要新建一个用户组，满足秘书的应用需求。

分析：本地用户管理和组：新建账户“secretary”和用户组“日常工作”，“日常工作”组具有“Network Configuration Operators”的权限，并secretary添加到“日常工作”组中。

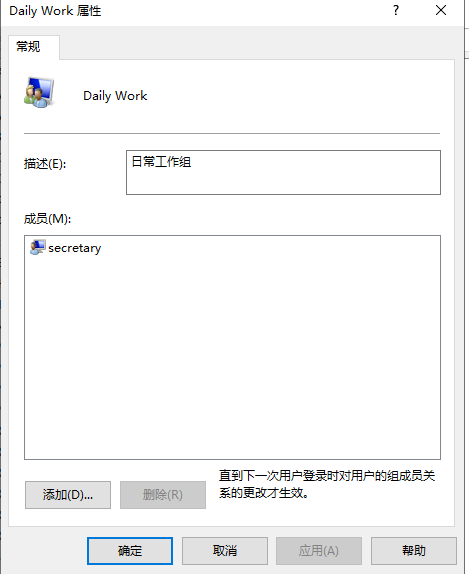
步骤：1）新建账户：“开始”中选择“ Windows管理工具”下的“计算机管理”，弹出窗口，展开“本地用户和组”，右键单击“用户”，新建“secretary”账户，在此窗口中也可以设置密码等属性。



1. 管理账户：右键单击账户，可以设置密码、删除账号或重命名；右键单击账户，选择“属性”，在“隶属于”选项卡中将secretary账户添加到Backup Operations组和Net Configuration Operators组中，即为secretary账户授予Backup Operations组和Net Configuration Operators组的权限。



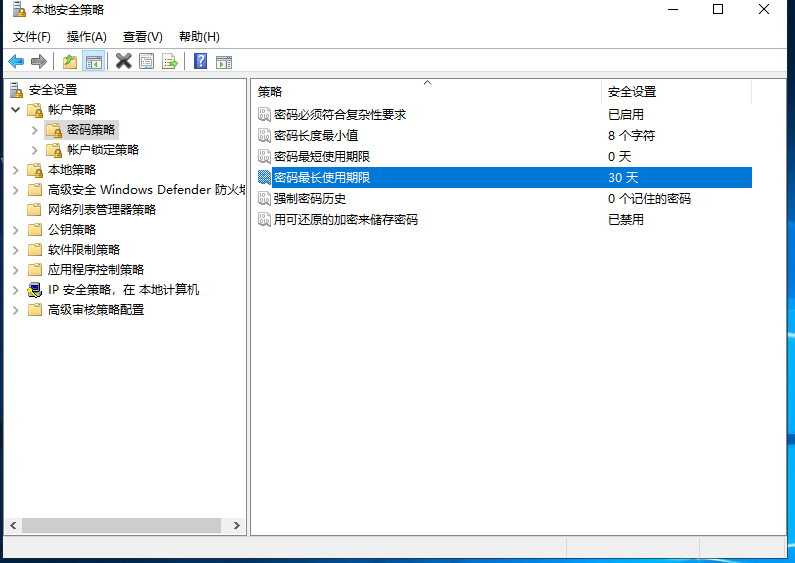
3）新建本地组：右键单击“组”，窗口，填写组名和描述信息，并选择“添加”，将secretary添加到日常工作组中，这样，日常工作组也具有Backup Operations组和Net Configuration Operators组的权限。



案例：公司管理层网络安全策略要求：启用密码复杂性策略，将密码最小长度设置为8个字符，设置密码使用期限为30天，当用户多次输入错误数据超过3次账户将被锁定，锁定时间为5分钟；启用审核登录成功和失败策略，登录失败后，通过事件查看器查看Windows日志；启用审核对象访问策略，用户对文件访问后，通过事件查看器查看Windows日志。

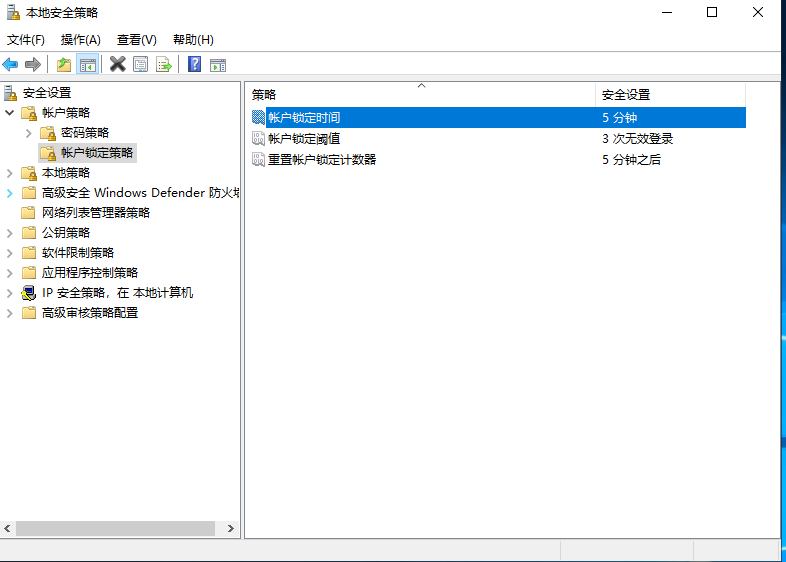
分析：在本地安全策略中分别设置密码策略、账户锁定策略、审核登录时间策略和审核对象访问策略。

步骤：1）密码策略设置：“开始”下的“Windows 管理工具”中“本地安全策略”，选择“账户策略”中的“密码策略”，启动密码复杂性策略；设置“密码长度最小值”为“8”个字符；密码最长使用期限默认为“42”天，设置为“30”天。



2）账户锁定策略设置：“开始”下的“Windows 管理工具”中“本地安全策略”，选择“账户策略”中的“账户锁定策略”，设置账户锁定时间为“5”分钟；账户锁定阈值为“3”次。

注意：初始账户锁定时间和重置账户锁定计数器为“不适用”，需设定账户锁定阈值后才能进行设定。



1. 审核策略设置：“开始”下的“ Windows 管理工具”中“本地安全策略”，选择“本地策略”中的“审核策略”，审核登录事件设置为“失败”；审核对象访问设置为“失败”。

