按照用户类型分配账号

名称	账号分配检查，避免共享账号与无用账号存在
实施目的	根据系统的要求，设定不同的账户和账户组，管理员用户，数据库用户，审计用户，来宾用户等，防止出现用户越权使用的可能
安全加固方案	**参考配置操作** 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”。 结合要求和实际业务情况判断符合要求，根据系统的要求，设定不同的账户和账户组，管理员用户，数据库用户，审计用户，来宾用户。 如存在与设备运行、维护等与工作无关的账号，可进行删除或锁定。
基线符合性判定依据	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”：查看账户和账户组，管理员用户，数据库用户，审计用户，来宾用户等。根据系统的要求和实际业务情况判断是否符合要求。

重命名Administrator，禁用GUEST

名称	重命名Administrator，禁用GUEST
实施目的	对于管理员帐号，要求更改缺省帐户名称；禁用guest（来宾）帐号。提高系统安全性。
安全加固方案	**参考配置操作** 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”。 Administrator－>重命名 Guest帐号->属性－> 勾选账户已禁用
基线符合性判定依据	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”： 查看管理员账号Administrator名称是否修改，Guest账号是否禁用。。

配置密码策略

名称	配置密码策略
实施目的	设置密码策略，减少密码安全风险；防止系统弱口令的存在，减少安全隐患。对于采用静态口令认证技术的设备，口令长度至少6位，且密码规则至少应采用字母（大小写穿插）加数字加标点符号（包括通配符）的方式。
安全加固方案	**参考配置操作：** 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”。“密码必须符合复杂性要求”选择“已启动”设置如下策略 策略 | 默认设置 | 推荐值 强制执行密码历史记录 | 记住 1 个密码 | 记住 5 个密码 密码最长期限 | 42 天 | 90 天 密码最短期限 | 0 天 | 2 天 最短密码长度 | 0 个字符 | 8 个字符 密码必须符合复杂性要求 | 禁用 | 启用 为域中所有用户使用可还原的加密来储存密码 | 禁用 | 禁用
基线符合性判定依据	“密码必须符合复杂性要求”选择“已启动” “强制密码历史”大于等于5 “密码最长使用期限”小于等于90 “密码最短使用期限”等于2 “密码长度最小值”大于等于8 “用可还原的加密来储存密码”选择“已禁用” 如上配置即合规，否则不合规

配置账户锁定策略

名称	配置账户锁定策略
实施目的	设置有效的账户锁定策略有助于防止攻击者猜出系统账户的密码。
安全加固方案	**参考配置操作** 进入“控制面板->管理工具->本地安全策略”，在“帐户策略->账户锁定策略”。 设置如下策略： 策略 | 默认设置 | 推荐最低设置 账户锁定时间 | 未定义 | 30 分钟 账户锁定阈值 | 0 | 6 次无效登录 复位账户锁定计数器 | 未定义 | 30 分钟
基线符合性判定依据	进入“控制面板->管理工具->本地安全策略”，在“帐户策略->账户锁定策略”： 查看安全策略是否设置为已启动和按要求配置。

授权管理：

远端系统强制关机权限设置

名称	远端系统强制关机设置
实施目的	防止远程用户非法关机，在本地安全设置中从远端系统强制关机只指派给Administrators组
安全加固方案	**参考配置操作** 进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权限分配”，将“从远程系统强制关机”策略设置为只有“Administrators”组
基线符合性判定依据	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”: 查看“从远端系统强制关机”是否设置为“只指派给Administrators组”。

关闭系统权限设置

名称	关闭系统权限设置
实施目的	防止管理员以外的用户在本地非法关机，在本地安全设置中关闭系统仅指派给Administrators组
安全加固方案	**参考配置操作** 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”。 “关闭系统”设置为“只指派给Administrators组”。
基线符合性判定依据	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”: 查看“关闭系统”是否设置为“只指派给Administrators组”。

从网络访问此计算机权限设置

名称	从网络访问此计算机设置
实施目的	防止网络用户非法访问主机
安全加固方案	**参考配置操作** 进入“控制面板==>管理工具==>本地安全策略==>本地策略==>用户权限分配==>从网络访问此计算机”查看列表，将”Users”和”Everyone”组和其他无用组删除
基线符合性判定依据	进入“控制面板==>管理工具==>本地安全策略==>本地策略==>用户权限分配==>从网络访问此计算机”查看列表，不包括”Users”和”Everyone”组和其他无用组为符合要求

日志加固：

系统日志完备性检查

名称	系统日志完备性检查，检查是否启用系统多项审核策略
实施目的	配置完整的审核策略
安全加固方案	**参考配置操作** 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”，将下列每一项都勾选”成功”和”失败”项 审核策略更改 审核登录事件 审核对象访问 审核进程跟踪 审核目录服务访问 审核特权使用 审核系统事件 审核账户管理
基线符合性判定依据	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”，检查是否将安全加固方案每一项都勾选”成功”和”失败”项

日志大小设置检查

名称	日志大小设置检查
实施目的	优化系统日志记录，防止日志溢出
安全加固方案	**参考配置操作** 进入”控制面板==>管理工具==>服务器管理”，在”诊断==>事件查看器==>windows日志”中，将应用程序、安全、Setup、系统 四项的属性设置为日志最大大小不小于100MB，达到日志最大大小时按需要覆盖事件
基线符合性判定依据	进入”管理工具==》服务器管理”，在”诊断==》事件查看器==》windows日志”中，查看 应用程序、安全、Setup、系统 四项的属性页，日志最大大小大于等于100MB，达到日志最大大小时为按需要覆盖事件及合规，否则不合规

远程登录超时配置检查

名称	远程登录超时配置检查
实施目的	防止管理员远程登录后忘记锁定机器导致被非法利用
安全加固方案	**参考配置操作** 进入"管理工具->本地安全策略->本地策略->安全选项->Microsoft网络服务器- 暂停会话前所需的空闲时间量"将时间设置为15分钟或更小
基线符合性判定依据	进入"管理工具->本地安全策略->本地策略->安全选项->Microsoft网络服务器- 暂停会话前所需的空闲时间量"小于等于十五分钟即合规，否则不合规

检查默认共享是否关闭

名称	检查默认共享是否关闭
实施目的	防止攻击者利用系统默认共享如：C$、D$等，非法对系统的硬盘进行访问，以及通过IPC$方式暴力破解帐户和密码
安全加固方案	**参考配置操作** 在桌面新建一个文本文件并编辑该文件，写入内容 net share 查询到的共享名如(ipc$) /delete 将该文件后缀修改为 .bat 后添加到启动项即可
基线符合性判定依据	打开cmd输入命令net share 查看是否有默认共享，有则不符合要求

检查是否设置屏幕密码保护

名称	检查是否设置屏幕密码保护
实施目的	防止管理员忘记锁定机器被非法攻击
安全加固方案	**参考配置操作** 进入"控制面板==>显示==>更改屏幕保护程序"，启用屏幕保护程序，设置等待时间为"5分钟"，启用"在恢复时显示登录屏幕"。
基线符合性判定依据	进入"控制面板==>显示==>更改屏幕保护程序"，屏幕保护程序启用，等待时间为"5分钟"，启用"在恢复时显示登录屏幕"即合规，否则不合规

检查自动播放功能是否关闭

名称	检查自动播放功能是否关闭
实施目的	关闭Windows自动播放，防止从移动设备感染病毒
安全加固方案	**参考配置操作** 点击“开始==>运行==>输入gpedit.msc，打开组策略编辑器，在本地计算机策略==>计算机配置==>管理模板==>windows组件==>自动播放策略==>关闭自动播放，勾选已启用，并在对话框中选择所有驱动器，确定即可
基线符合性判定依据	点击“开始==>运行==>输入gpedit.msc，打开组策略编辑器，在本地计算机策略==>计算机配置==>管理模板==>windows组件==>自动播放策略==>关闭自动播放，勾选已启用，并在对话框中选择所有驱动器即合规，否则不合规

检查防火墙是否启用

名称	检查防火墙是否启用
实施目的	过滤不必要的端口，提高系统安全性
安全加固方案	**参考配置操作** 点击“控制面板==>windows防火墙==>打开或关闭windows防火墙“，将家庭或工作（专用）网络位置设置与公用网络设置都勾选为启用windows防火墙，然后在“控制面板==>windows防火墙==>高级设置“根据业务需要来设置出入站规则
基线符合性判定依据	点击“控制面板==>windows防火墙==>打开或关闭windows防火墙“，将家庭或工作（专用）网络位置设置与公用网络设置都勾选为启用windows防火墙即合规，否则不合规