# Windows服务器基线检查结果汇总

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题描述** | **影响对象** | **加固建议** |
| 0 | 未禁用或重命名管理员账户Administrator |  | 进入“控制面板->管理工具->计算机管理”，在弹出框中选择“系统工具->本地用户和组->用户”，在右侧查看用户中是否包含 Administrator。  重命名账户：鼠标右键->重命名，键入新的账户名称。 |
| 1 | 未禁用Guest账户 |  | 进入“ 控制面板->管理工具->计算机管理” ，在弹出框中选择“ 系统工具->本地用户和组->用户”，在右侧选择 Guest，双击鼠标左键查看，勾选“账户已禁用”。 |
| 2 | 未删除无关账户 |  | 进入“控制面板->管理工具->计算机管理”，在弹出框中选择“系统工具->本地用户和组->用户”，在右侧查看系统中现有账户。双击鼠标左键查看无关账户，勾选“账户已禁用”。 |
| 3 | 未开启密码必须符合复杂性要求的策略 |  | 进入“ 控制面板->管理工具->本地安全策略”，在“ 账户策略->密码策略->密码必须符合复杂性要求”，鼠标右键->属性->选择“ 已启用“。 |
| 4 | 密码长度最小值不符合 |  | 进入“ 控制面板->管理工具->本地安全策略”，在“ 账户策略->密码策略->密码长度最小值”，鼠标右键->属性-> 8 ->确定。 |
| 5 | 密码最长使用期限不符合 |  | 进入“ 控制面板->管理工具->本地安全策略”，在“ 账户策略->密码策略->密码最长使用期限”，鼠标右键->属性-> 90 ->确定。 |
| 6 | 未强制密码历史 |  | 进入“ 控制面板->管理工具->本地安全策略”，在“ 账户策略->密码策略->强制密码历史”，鼠标右键->属性-> 5 ->确定。 |
| 7 | 账户锁定阈值不符合 |  | 进入“ 控制面板->管理工具->本地安全策略”，在“ 账户策略->账户锁定策略->账户锁定阈值”，鼠标右键->属性-> 6 ->确定。 |
| 8 | 允许非管理员组用户从远程桌面关机 |  | 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->从远程系统强制关机”，鼠标右键->属性->设置为只指派给 Administrators 组。 |
| 9 | 允许非管理员组用户从取得文件其他对象的所有权 |  | 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->取 得 文 件 戒 其 他 对 象 的 所 有 权 ”， 鼠 标 右 键 -> 属 性 -> 设 置 为 只 指 派 给Administrators 组。 |
| 10 | 未审核策略更改 |  | 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->审核策略更改”，鼠标右键->属性->勾选“ 成功” 与“ 失败” 两项。 |
| 11 | 未审核登录事件 |  | 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->审核登录事件”，鼠标右键->属性->勾选“ 成功” 与“ 失败” 两项 |
| 12 | 未审核对象访问 |  | 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->审核对象访问”，鼠标右键->属性->勾选“ 成功” 与“ 失败” 两项 |
| 13 | 未审核进程跟踪 |  | 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->审核进程跟踪”，鼠标右键->属性->勾选”失败”。 |
| 14 | 未审核目录服务访问 |  | 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->审核目录服务访问”，鼠标右键->属性->勾选“ 成功” 与“ 失败” 两项。 |
| 15 | 未审核特权使用 |  | 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->审核特权使用”，鼠标右键->属性->勾选“ 成功” 与“ 失败” 两项 |
| 16 | 未审核系统事件 |  | 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->审核系统事件”，鼠标右键->属性->勾选“ 成功” 与“ 失败” 两项 |
| 17 | 未审核账户管理 |  | 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->审核账户管理”，鼠标右键->属性->勾选“ 成功” 与“ 失败” 两项 |
| 18 | 应用程序日志最大大小不符合 |  | 进入“ 控制面板->管理工具->事件查看器”， 选择“ 事件查看器（本地）->Windows 日志”，  1）在“ 应用程序” 中，鼠标右键单击选择“属性”，将“ 日志最大大小” 设置为“40960KB”，“ 达到事件日志最大大小时“ 选择“ 按需要覆盖事件（旧事件优先）”。  2）在“ 安全” 中，鼠标右键单击选择“属性”，将“ 日志最大大小” 设置为“40960KB，“ 达到事件日志最大大小时“ 选择“ 按需要覆盖事件（旧事件优先）”。  3）在“ 系统” 中，鼠标右键单击选择“属性”，将“ 日志最大大小” 设置为“40960KB”，“ 达到事件日志最大大小时“ 选择“ 按需要覆盖事件（旧事件优先）”。 |
| 19 | 是否开启Windows 防火墙 |  | 进入“ 控制面板->Windows 防火墙->打开戒关闭 Windows 防火墙” ，查看“家庭戒工作（与用）网络位置设置“不”公用网络位置设置“中防火墙的配置情况。 |
| 20 | 未关闭自动播放功能 |  | 开始->运行-> gpedit.msc，打开本地组策略编辑器，在“计算机配置->管理模板->Windows 组件 ->自动播放策略”中，选择“关闭自动播放”，查看其状态。 |
| 21 | 最新补丁安装情况 |  | 更新到最新漏洞补丁。 |
| 22 | 未关闭默认共享 |  | 开始->运行-> regedit.exe，进入注册表编辑器，更改注册表键值：HKEY\_LOCAL\_MACHINE  \SYSTEM\CurrentControlSet\  Services\LanmanSer  ver\Parameters\下，增加 REG\_DWORD 类型的 AutoShareServer 键，值为 0 |
| 23 | 未关闭远程桌面 |  | 鼠标右键点击“ 我的电脑”，选择“ 属性”，选择“ 远程设置”， 在“远程桌面”的下方查看，如果勾选了“ 不允许连接到这台计算机”，表明关闭了远程桌面，符合安全要求 |
| 24 | 未更改默认远程桌面端口 |  | 开始->运行-> regedit.exe，进入注册表编辑器，更改注册表键值：HKEY\_LOCAL\_MACHINE\  SYSTEM\CurrentControlSet\  Control\Terminal Server\WinStations\RDP-Tcp |