Windows 操作系统配置安全基线标准与操作指南

目 录

第1章 概述

1.1 安全基线概念

安全基线是指满足最小安全保证的基本要求。

1.2 文档编制目的

本文档针对安装运行微软 Windows 系列操作系统的计算机（包括服务器、工作站、终端PC）主机所应当遵循的通用基本安全设置要求提供了参考建议，部分内容参照了网络信息安全等级保护技术标准的基本要求，供用户在安装使用Windows 系列操作系统过程中进行安全配置合规性自查、检查、加固提供标准依据与操作指导。

1.3 文档适用范围

本文档适用于 Windows 系列操作系统的各类版本，部分操作系统或版本的特定配置与操作见括号内说明。文档使用人员包括系统管理员及终端计算机用户。

1.4 文档修订

第 2 章 账户管理、认证授权

2.1 操作系统账户

2.1.1 管理缺省账户

安全基线名称	操作系统账户管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-02-01-01
安全基线说明	对于管理员帐号，应使用非缺省 Administrator 帐户名称，即重命名管理员帐户；禁用 guest（来宾）帐户。
设置操作步骤	1、开始->运行->输入“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows 设置\安全设置\本地策略\安全选项”，在右边窗格中找到“(帐户:)重命名(系统)管理员帐户”，更改其默认设置“Administrator”； 2、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->用户”：Guest -> 属性，勾选“帐户已禁用”。
基线符合性判定依据	缺省账户 Administrator 已更名、Guest 已停用。
备注	应删除或锁定与系统运行、维护等工作无关的账户。

2.2 口令

2.2.1 密码复杂度

安全基线名称	操作系统帐户密码管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-02-02-01
安全基线说明	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三种： 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
设置操作步骤	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“已启用”。
基线符合性判定依据	查看本地安全策略，“密码必须符合复杂性要求”选择“已启用”。
备注	密码最短长度 8 位依据《南京农业大学计算机信息系统密码安全管理办法》相关规定。

2.2.2 密码历史

安全基线名称	操作系统帐户密码历史安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-02-02-02
安全基线说明	对于采用静态口令认证技术的系统，账户口令的生存期不长于 90 天。
设置操作步骤	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“密码最长存留期”（Windows XP、2000、2003）或“密码最长使用期限”（Windows Vista、7、2008）的值。
基线符合性判定依据	查看本地安全策略，“密码最长存留期”设置不长于 90 天。
备注	0：表示未设置，账号使用期无限长。根据《南京农业大学计算机信息系统密码安全管理办法》规定，密码最长有效期为 30/60/90 天，视不同系统需要而定，最长不超过 90 天。

2.2.3 帐户锁定策略

安全基线名称	操作系统账户锁定策略安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-02-02-03
安全基线说明	对于采用静态口令认证技术的系统，应配置当用户连续认证失

	败次数超过 5 次（不含 5 次）后，锁定该用户使用的账号。
设置操作步骤	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”：查看“账户锁定阀值”设置
基线符合性判定依据	查看本地安全策略,“账户锁定阀值”设置为小于或等于 5 次，“账户锁定时间”设置为 30 分钟
备注	0：表示未设置，可无限尝试口令。

2.3 授权

2.3.1 远程关机授权

安全基线名称	操作系统远程关机策略安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-02-03-01
安全基线说明	在本地安全设置中，从远端系统强制关机只指派给 Administrators 组。
设置操作步骤	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”：进入“从远端系统强制关机”设置，只保留 Administrtors 组。
基线符合性判定依据	查看本地安全策略，“从远端系统强制关机”设置为“只指派给 Administrtors 组”。
备注	Windows7、10 中为“用户权限分配”项。

2.3.2 本地关机授权

安全基线名称	操作系统本地关机策略安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-02-03-02
安全基线说明	在本地安全设置中，关闭系统仅指派给 Administrators 组。

设置操作步骤	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”:进入“关闭系统”设置，只保留 Administrtors 组。
基线符合性判定依据	查看本地安全策略，“关闭系统”设置为“只指派给 Administrators 组”
备注	

2.3.3 文件或其它对象的所有权授权

安全基线名称	操作系统文件或其它对象的所有权管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-02-03-03
安全基线说明	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。
设置操作步骤	进入“控制面板 ->管理工具 ->本地安全策略”，进入“取得文件或其它对象的所有权”设置，只保留 Administrtors 组。
基线符合性判定依据	查看本地安全策略，“取得文件或其它对象的所有权”设置为“只指派给 Administrators 组”
备注	

2.4 身份鉴别

2.4.1 禁止 Windows 自动登录

安全基线名称	操作系统登录认证管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-02-04-01
安全基线说明	操作系统登录应对用户身份进行标识和鉴别。
设置操作步骤	从“开始 ->运行 ->输入： regedit”，查看注册表项:

基线符合性判定依据	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon，将名称为“AutoAdminLogon”的数值修改为 0。
备注	AutoAdminLogon 值 1 为自动登录。

第 3 章 日志配置操作

3.1 日志配置

3.1.1 审核登录

安全基线名称	操作系统审核登录策略安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-03-01-01
安全基线说明	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账号，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。
设置操作步骤	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”中进入“审核登录事件”设置，勾选“成功”和“失败”。
基线符合性判定依据	查看本地安全策略，审核登录事件，设置为成功和失败都审核。
备注	配置日志记录有利于系统故障排查与安全事件取证。

3.1.2 审核策略更改

安全基线名称	操作系统审核策略更改安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-03-01-02
安全基线说明	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。
设置操作步骤	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”中进入“审核策略更改”设置，勾选“成功”和“失败”。
基线符合性判定依据	查看本地安全策略，“审核策略更改”设置为成功和失败都审核。
备注	

3.1.3 审核对象访问

安全基线名称	操作系统审核对象访问安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-03-01-03
安全基线说明	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。
设置操作步骤	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”中进入“审核对象访问”设置，勾选“成功”和“失败”。
基线符合性判定依据	查看本地安全策略，“审核对象访问”设置为成功和失败都审核。
备注	

3.1.4 审核事件目录服务器访问

安全基线名称	操作系统审核事件目录服务器访问策略安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-03-01-04
安全基线说明	启用组策略中对 Windows 系统的审核目录服务访问，成功和失败都要审核。
设置操作步骤	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”中进入“审核目录服务访问”设置，勾选“成

	功”和“失败”。
基线符合性判定依据	查看本地安全策略，“审核目录服务访问”设置为成功和失败都审核。
备注	

3.1.5 审核特权使用

安全基线名称	操作系统审核特权使用策略安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-03-01-05
安全基线说明	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。
设置操作步骤	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”中进入“审核特权使用”设置，勾选“成功”和“失败”。
基线符合性判定依据	查看本地安全策略，“审核特权使用”设置为成功和失败都审核。
备注	

3.1.6 审核系统事件

安全基线名称	操作系统审核系统事件策略安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-03-01-06
安全基线说明	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。
设置操作步骤	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”中进入“审核系统事件”设置，勾选“成功”和“失败”。
基线符合性判定依据	查看本地安全策略，“审核系统事件”设置为成功和失败都审核。

备注	

3.1.7 审核账户管理

安全基线名称	操作系统审核账户管理策略安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-03-01-07
安全基线说明	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。
设置操作步骤	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”中进入“审核账户管理”设置，勾选“成功”和“失败”。
基线符合性判定依据	查看本地安全策略，“审核账户管理”设置为成功和失败都审核。
备注	

3.1.8 审核过程追踪

安全基线名称	操作系统审核过程追踪策略安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-03-01-08
安全基线说明	启用组策略中对 Windows 系统的审核过程追踪失败。
设置操作步骤	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”中进入“审核过程跟踪”设置，勾选“失败”。
基线符合性判定依据	查看本地安全策略，“审核过程跟踪”设置为失败需要审核。
备注	

3.1.9 日志文件大小

安全基线名称	操作系统日志容量安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-03-01-09
安全基线说明	设置应用日志文件大小最大 20480KB(20M,至少为 8192KB 即

	8M），设置当达到最大的日志尺寸时，按需要覆盖事件。
设置操作步骤	进入“控制面板 ->管理工具 -> 事件查看器”，在“事件查看器（本地）”中：查看“应用日志”、“系统日志”、“安全日志”属性中的日志大小,设置至少为 8192KB、当达到最大的日志尺寸时“按需要覆盖事件”。
基线符合性判定依据	“应用日志”、“系统日志”、“安全日志”属性中的日志大小设置最大不超过“20480KB ”,设置当达到最大的日志尺寸时，“按需要覆盖事件”。
备注	

第 4 章 IP 协议安全配置

4.1 入侵防范

4.1.1 启用 SYN 攻击保护

安全基线名称	操作系统 SYN 攻击保护安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-04-01-01
安全基线说明	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。
设置操作步骤	在“开始 ->运行 ->键入 regedit”查看注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ a.启用 SYN 攻击保护：SynAttackProtect 推荐值：2(十六进制)，若该值不存在，可以自己创建，类型为 DWORD; b.指定在触发 SYN flood 保护之前超过的 TCP 连接请求阈

	值：TcpMaxPortsExhausted 推荐值：5(十六进制)，若该值不存在，可以自己创建，类型为 DWORD； c.指定 SYN_RCVD 状态中的 TCP 连接阈值，超过该值则触发 SYN flood 保护：TcpMaxHalfOpen 推荐值：500(十六进制)，若该值不存在，可以自己创建，类型为 DWORD； d.指定至少发送一次重传的 SYN_RCVD 状态中的 TCP 连接阈值，超过该值则触发 SYN flood 保护：TcpMaxHalfOpenRetried 推荐值：400(十六进制)，若该值不存在，可以自己创建，类型为 DWORD。
基线符合性判定依据	查看注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ SynAttackProtect 推荐值：2 TcpMaxPortsExhausted 推荐值：5 TcpMaxHalfOpen 推荐值：500 TcpMaxHalfOpenRetried 推荐值：400
备注	SYN 攻击属于 DOS 攻击的一种，它利用 TCP 协议缺陷，通过发送大量的半连接请求，耗费 CPU 和内存资源。

4.1.2 启用 ICMP 攻击保护

安全基线名称	操作系统 ICMP 攻击保护安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-04-01-02
安全基线说明	在收到 ICMP 重定向数据包时禁止创建高成本的主机路由，防止形成 DDOS 攻击。
设置操作步骤	在“开始 ->运行 ->键入 regedit” 查看注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ EnableICMPRedirect 项，推荐值：0，若该值不存在，可以自己创建，类型为 DWORD。
基线符合性判定依据	查看注册表项，EnableICMPRedirect 值为 0。
备注	有效值：0（禁用），1（启用）。ICMP 协议属于网络层协议，

	主要用于在主机与路由器之间传递控制信息，非常容易被用于攻击网络上的路由器和主机。

4.1.3 启用 SNMP 攻击保护

安全基线名称	操作系统 SNMP 攻击保护安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-04-01-03
安全基线说明	禁止攻击者强制切换到备用网关。
设置操作步骤	在“开始 ->运行 ->键入 regedit” 查看注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ EnableDeadGWDetect 项 推荐值：0，若该值不存在，可以自己创建，类型为 DWORD。
基线符合性判定依据	查看注册表项，EnableDeadGWDetect 值为 0。
备注	有效值：0（禁用），1（启用）。简单网络管理协议(SNMP)用来对通信网络设备进行管理，易被用于形成大流量的 SNMP 攻击。

4.1.4 禁用 IP 源路由

安全基线名称	操作系统禁用 IP 源路由安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-04-01-04
安全基线说明	禁用 IP 源路由，防范数据包欺骗。
设置操作步骤	在“开始 ->运行 ->键入 regedit”，查看注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ DisableIPSourceRouting 项，推荐值：1，若该值不存在，可以自己创建，类型为 DWORD。
基线符合性判定依据	查看注册表项，DisableIPSourceRouting 值为 1。
备注	有效值：0（转发所有数据包），1（不转发源路由数据包），2（丢弃所有传入的源路由数据包）。

4.1.5 启用碎片攻击保护

安全基线名称	操作系统 TCP 碎片攻击保护安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-04-01-05
安全基线说明	设置系统防止遭 TCP 碎片攻击导致崩溃或拒绝服务。
设置操作步骤	“开始->运行”，输入 regedit，运行注册表编辑器，找到注册表项: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters, 新建 DWORD 值，名称为 EnablePMTUDiscovery，值为 0
基线符合性判定依据	查看注册表项，EnablePMTUDiscovery 值为 0
备注	碎片攻击指的是一种计算机程序重组的漏洞,IP 数据包最长只能为 0xFFFF,就是 65535 字节。如果有意发送总长度超过 65535 的 IP 碎片，一些老的系统内核在处理的时候就会出现问题，导致崩溃或者拒绝服务。注册表键值 0 表示不自动探测 MTU 大小，都使用 576 字节的 MTU，1 表示自动探测 MTU 大小，可能会被攻击者强制 MTU 值变得非常小，从而导致堆栈的负荷过大。

第 5 章 设备其他配置操作

5.1 访问控制管理

5.1.1 共享文件夹权限控制

安全基线名称	操作系统共享文件权限控制安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-01-01
安全基线说明	共享分区、文件夹或文件应设置访问权限，用户里不应包含 Everyone(任何人)。
设置操作步骤	计算机管理(本地)— >系统工具— >共享文件夹— >共享，查看每个自定义共享文件夹的共享权限，若其中包含

	“Everyone(任何人)”，则将其删除。
基线符合性判定依据	查看自定义共享文件夹的共享权限，默认共享如果需要，也应设置访问权限。
备注	

5.1.2 网络访问用户授权

安全基线名称	操作系统网络访问用户授权安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-01-02
安全基线说明	授权指定系统用户，防止用户非法从网络访问主机。
设置操作步骤	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”，删除“Guest”用户、“Everyone”组。（Windows xp,Windows 2000） 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”。“从网络访问此计算机”，删除“Guest”用户、“Everyone”组。（Windows Vista、7、2003、2008）
基线符合性判定依据	查看系统本地策略“从网络访问此计算机”的用户是否已删除“Guest”用户、“Everyone”组。
备注	只允许存在 Administrators、Backup Operators、Power Users、users，如存在其他用户请删除。

5.1.3 匿名用户连接权限管理

安全基线名称	操作系统匿名用户连接权限管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-01-03
安全基线说明	限制匿名用户连接权限，防止用户远程枚举本地帐号。
设置操作步骤	进入控制面板->管理工具->本地安全策略->本地策略->安全选项->网络访问:不允许 SAM 帐户和共享的匿名枚举->属性->已启用。（Windows xp,Windows 2000,Windows 2003,Windows Vista,Windows 7,Window 8） 进入控制面板->管理工具->本地安全策略->本地策略->安全选项->对匿名连接的额外限制->属性->不允许枚举 SAM 帐号和共享。（Windows 2008）
基线符合性判定依据	查看系统本地策略是否已限制匿名用户连接权限。

备注	

5.1.4 远程桌面服务端口管理

安全基线名称	操作系统远程桌面服务端口管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-01-04
安全基线说明	修改远程桌面服务默认端口,增强访问安全性。
设置操作步骤	开始->运行->Regedit，查找注册表项: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp 找到“PortNumber”子项，默认值 00000D3D，是 3389 的十六进制表示形式。切换到十进制，修改成除 3389 外的其他任何值，并保存新值，重新启动系统。
基线符合性判定依据	查看注册表“PortNumber”值是否已修改。
备注	需要修改两处注册表项，在 win10 系统中 CurrentControlSet 已经变更为 CurrentControlSet001。

5.1.5 禁止远程访问注册表路径和子路径

安全基线名称	操作系统注册表路径和子路径访问控制安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-01-05
安全基线说明	应禁止远程访问操作系统注册表路径和子路径，防止系统被入侵破坏。
设置操作步骤	开始->运行->输入“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略->计算机配置->Windows 设置->安全设置->本地策略->安全选项”,在右边窗格中找到“网络访问：可远程访问的注册表路径和子路径”，配置为空。
基线符合性判定依据	查看组策略中“网络访问：可远程访问的注册表路径和子路径”，配置应为空。
备注	

5.2 数据防护管理

5.2.1 数据执行保护

安全基线名称	操作系统数据执行保护安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-02-01
安全基线说明	对 Windows 操作系统程序和服务启用系统自带 DEP 功能（数据执行保护），防止在受保护内存位置运行有害代码。
设置操作步骤	进入“控制面板— >系统”，在“高级”选项卡的 “性能”下的“设置”。进入 “数据执行保护”选项卡。查看“仅为基本 Windows 操作系统程序和服务启用 DEP”。
基线符合性判定依据	“数据执行保护”选项卡已设置为“仅为基本 Windows 操作系统程序和服务启用 DEP”。
备注	适用于 Windows XP SP2 及 Windows 2003，可能影响部分程序运行，选用。

5.2.2 恶意代码防范

安全基线名称	操作系统恶意代码防范安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-02-02
安全基线说明	使用正版授权的计算机病毒防护软件，可安全有效地查杀各类计算机病毒，防范恶意代码执行，自动更新病毒特征库。
设置操作步骤	访问校园网 kvirus.njau.edu.cn，按照说明下载安装校园网计算机病毒防护软件。
基线符合性判定依据	查看系统是否安装计算机病毒防护软件
备注	学校统一采购正版授权计算机病毒防护软件，供校园网用户免费使用。

5.3 资源控制管理

5.3.1 终端服务登录管理

安全基线名称	操作系统终端服务登录管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-03-01
安全基线说明	默认情况下，终端服务接入服务器时，登录对话框会显示上次登录的账户名，应设置禁止显示上次登录名。
设置操作步骤	在“系统-运行”中执行命令 regedit 打开注册表，修改下述内容： HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 之下,将 DontDisplayLastUserName 的值设置为 1，若该值不存在，可以自己创建，类型为 DWORD。
基线符合性判定依据	查看 DontDisplayLastUserName 值是否为 1。
备注	适用于服务器

5.3.2 系统登录管理

安全基线名称	操作系统登录管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-03-02
安全基线说明	默认情况下，操作系统登录时，登录对话框会显示上次登录的账户名，应设置禁止显示上次登录名。
设置操作步骤	进入“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项” “交互式登录：不显示最后的用户名”，点击“已启用”
基线符合性判定依据	查看本地安全策略中“交互式登录：不显示最后的用户名”是否启用。
备注	

5.3.3 用户登录超时管理

安全基线名称	操作系统用户登录超时管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-03-03
安全基线说明	应设置用户登录超时自动注销或断开。
设置操作步骤	开始->运行->输入“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略->计算机配置->Windows 设置->安全设置->本地策略->安全选项”,在右边窗格中找到“Microsoft 网络服务器：当登录时间用完时自动注销用户”，或“Microsoft 网络服务器：登录时间过期后断开与客户端的连接”，配置为“已启用”。
基线符合性判定依据	查看本地计算机策略的安全选项是否已启用用户登录超时自动注销或断开。
备注	

5.3.4 虚拟内存管理

安全基线名称	操作系统虚拟内存管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-03-04
安全基线说明	防止非法用户从虚拟内存中获取其他用户的数据。
设置操作步骤	进入“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项” “关机：清除虚拟内存页面文件”，点击“已启用”。
基线符合性判定依据	查看“关机：清除虚拟内存页面文件”是否启用。
备注	确保可能会进入页面文件的进程内存中的敏感信息不会被设法通过直接访问页面文件的未经授权用户使用。

5.4 启动项

5.4.1 关闭 Windows 自动播放功能

安全基线名称	操作系统 Windows 自动播放安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-04-01
安全基线说明	关闭 Windows 自动播放功能。

设置操作步骤	打开“开始 →运行”，在对话框中输入“gpedit.msc 命令，在出现“本地组策略编辑器”窗口中依次选择“计算机配置 →管理模板 →所有设置”，双击“关闭自动播放”，选“启用”。
基线符合性判定依据	在关闭自动播放的“设置”选项卡中“已启用”选项已选定。
备注	可防止计算机病毒和恶意代码自动运行。

5.5 时间校准

5.5.1 配置系统时间同步

安全基线名称	操作系统时间同步安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-05-01
安全基线说明	校准系统时间，自动与时间服务源同步。
设置操作步骤	控制面板→“日期和时间”→ “Internet 时间”→“更改设置”，勾选“与 Internet 时间服务器同步”，服务器框里填：“ntp.njau.edu.cn”，点“立即更新”，直到显示同步成功。
基线符合性判定依据	按上述步骤查看同步结果，同步成功则符合。
备注	校准主机时间，对计划任务准时执行等至关重要。 ntp.njau.edu.cn 是南京农业大学校园网时间同步服务器。

5.6 系统服务管理

5.6.1 系统服务管理

安全基线名称	操作系统服务管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-05-06-01
安全基线说明	关闭不必要的系统服务。

设置操作步骤	进入“控制面板->管理工具->计算机管理”，进入“服务和应用程序”，查看所有服务，建议关闭以下服务： Error Reporting Service、错误报告服务 Computer browser 浏览局域网计算机列表 Print Spooler 打印队列服务（服务器上关闭，个人终端开启） Remote Registry 远程注册表操作 Routing and Remote Access 路由与远程访问 Shell Hardware Detection 为自动播放硬件事件提供通知 Telnet 远程管理 TCP/IP NetBIOS Helper 允许客户端共享文件，打印机和登录到网络
基线符合性判定依据	查看上述服务是否关闭。
备注	关闭不必要的服务，提高系统安全性。

第 6 章 系统更新

6.1 系统更新

6.1.1 操作系统补丁更新

安全基线名称	操作系统补丁安装管理安全基线要求项
安全基线编号	NJAUSBL-Windows-V01-06-01-01
安全基线说明	应安装关键和重要系统补丁，开启系统自动更新功能。
设置操作步骤	控制面板－Windows Update,启用 Windows Update，校园网用户建议安装校内 Windows Update 自动更新脚本，详见 http://winupdate.njau.edu.cn 说明
基线符合性判定依据	查看系统安装的 SP 情况：点击开始－运行，输入命令“winver ”，回车；记录当前的 SP 版本号。查看安装的其他补丁的情况:控制面板－Windows Update－查看更新历史记录。
备注	WSUS（Windows System Update Service）是微软公司提供的系统自动更新补丁服务,南京农业大学校园网已启用本地 WSUS

	服务器，用户只要安装自动更新脚本程序，可定时通过校园网WSUS 服务器自动更新系统补丁。