

	信息安全规划与实施项目 安全配置基线	
--	-----------------------	--

目录

1 概述	1
1.1 适用范围	1
1.2 术语和定义	1
1.3 符号和缩略语	1
2 WINDOWS 设备安全配置要求	1
2.1 账号管理、认证授权	2
2.1.1 账号	2
2.1.2 口令	3
2.1.3 授权	6
2.2 日志配置操作	9
2.3 设备其他配置操作	15
2.3.1 屏幕保护	15
2.3.2 共享文件夹及访问权限	16
2.3.3 防病毒管理	18

	信息安全规划与实施项目 安全配置基线	
--	-----------------------	--

1 概述

1.1 适用范围

本规范所指的设备为 Windows 系统设备。本规范明确了运行 Windows 操作系统的设备在安全配置方面的基本要求。在未特别说明的情况下，均适用于共享中心在用服务器的 Windows 操作系统，包括 Windows 2012、Windows2016、的 Sever 版本。

基线配置项中的“可选”项，可以根据具体系统和应用环境，选择是否遵守。

1.2 术语和定义

1.3 符号和缩略语

缩写	英文描述	中文描述

2 WINDOWS 设备安全配置要求

本规范从 Windows 系统设备的认证授权功能、安全日志功能以及 IP 网络安全功能，和其他自身安全配置功能四个方面提出安全要求。

	信息安全规划与实施项目 安全配置基线	
--	-----------------------	--

2.1 账号管理、认证授权

认证功能用于确认登录系统的用户真实身份。认证功能的具体实现方式包括静态口令、动态口令、指纹等生物鉴别技术等。授权功能赋予系统账号的操作权限，并限制用户进行超越其账号权限的操作。

2.1.1 账号

编号：安全要求-设备-WINDOWS-配置-1

要求内容	按照用户分配账号。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。
操作指南	1、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”： 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。
检测方法	1、判定条件 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。 2、检测操作 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”： 查看根据系统的要求，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。

编号：安全要求-设备-WINDOWS-配置-2

要求内容	锁定与设备运行、维护等与工作无关的账号。
------	----------------------

信息安全规划与实施项目		
安全配置基线		

操作指南	<p>1、参考配置操作</p> <p>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”：</p> <p>锁定与设备运行、维护等与工作无关的账号。</p>
检测方法	<p>1、判定条件</p> <p>结合要求和实际业务情况判断符合要求，锁定与设备运行、维护等与工作无关的账号。</p> <p>2、检测操作</p> <p>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”：</p> <p>查看是否锁定与设备运行、维护等与工作无关的账号。</p>

编号：安全要求-设备-WINDOWS-配置-3

要求内容	禁用 guest（来宾）帐号。
操作指南	<p>1、参考配置操作</p> <p>Guest 帐号->属性-> 已停用</p>
检测方法	<p>1、判定条件</p> <p>缺省账户 Administrator 名称已更改。</p> <p>Guest 帐号已停用。</p> <p>2、检测操作</p> <p>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”：</p> <p>缺省帐户->属性-> 更改名称</p> <p>Guest 帐号->属性-> 已停用</p>

2.1.2 口令

编号：安全要求-设备-WINDOWS-配置-4

信息安全规划与实施项目		
安全配置基线		

要求内容	<p>最短密码长度 12 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：</p> <ul style="list-style-type: none"> ● 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 <p>非字母数字字符，如标点符号，@, #, \$, %, &, *等</p>
操作指南	<p>1、参考配置操作</p> <p>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”：</p> <p>“密码必须符合复杂性要求”选择“已启动”</p>
检测方法	<p>1、判定条件</p> <p>“密码必须符合复杂性要求”选择“已启动”</p> <p>2、检测操作</p> <p>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”：</p> <p>查看是否“密码必须符合复杂性要求”选择“已启动”</p>

编号：安全要求-设备-WINDOWS-配置-5

要求内容	对于采用静态口令认证技术的设备，账户口令的生存期不长于 90 天。应用系统用户可暂不配置。
操作指南	<p>1、参考配置操作</p> <p>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”：</p> <p>“密码最长存留期”设置为“90 天”</p>
检测方法	<p>1、判定条件</p> <p>“密码最长存留期”设置为“90 天”</p> <p>2、检测操作</p> <p>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”：</p>

信息安全规划与实施项目		
安全配置基线		

	<p>码策略”：</p> <p>查看是否“密码最长存留期”设置为“90 天”</p>
--	--

编号：安全要求-设备-WINDOWS-配置-6

要求内容	对于采用静态口令认证技术的设备，应配置设备，使用户不能重复使用最近 3 次（含 3 次）内已使用的口令。
操作指南	<p>1、参考配置操作</p> <p>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”：</p> <p>“强制密码历史”设置为“记住 3 个密码”</p>
检测方法	<p>1、符合性判定依据</p> <p>“强制密码历史”设置为“记住 5 个密码”</p> <p>2、参考检测方法</p> <p>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”：</p> <p>查看是否“强制密码历史”设置为“记住 5 个密码”</p>

编号：安全要求-设备-WINDOWS-配置-7

要求内容	对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号。
操作指南	<p>1、参考配置操作</p> <p>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”：</p> <p>“账户锁定阈值”设置为 6 次</p> <p>设置解锁阈值：30 分钟</p>
检测方法	<p>1、符合性判定依据</p> <p>“账户锁定阈值”设置为小于或等于 6 次</p> <p>2、参考检测方法</p>

信息安全规划与实施项目		
安全配置基线		

	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”：
	查看是否“账户锁定阈值”设置为小于等于 6 次
	3、补充说明 设置不当可能导致账号大面积锁定，在域环境中应小心设置，Administrator 账号本身不会被锁定。

2.1.3 授权

编号：安全要求-设备-WINDOWS-配置-8

要求内容	在本地安全设置中从远端系统强制关机只指派给 Administrators 组。
操作指南	1、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”： “从远端系统强制关机”设置为“只指派给 Administrators 组”
检测方法	1、判定条件 “从远端系统强制关机”设置为“只指派给 Administrators 组” 2、检测操作 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”： 查看是否“从远端系统强制关机”设置为“只指派给 Administrators 组”

编号：安全要求-设备-WINDOWS-配置-9

要求内容	在本地安全设置中关闭系统仅指派给 Administrators 组。
操作指南	1、参考配置操作

信息安全规划与实施项目		
安全配置基线		

	<p>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”：</p> <p>“关闭系统”设置为“只指派给 Administrators 组”</p>
检测方法	<p>1、判定条件</p> <p>“关闭系统”设置为“只指派给 Administrators 组”</p> <p>2、检测操作</p> <p>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”：</p> <p>查看“关闭系统”设置为“只指派给 Administrators 组”</p>

编号：安全要求-设备-WINDOWS-配置-10

要求内容	<p>在本地安全设置中取得文件或其它对象的所有权只指派给 Administrators 组。防止非 Administrators 组的用户获得过高权限。</p>
操作指南	<p>1、参考配置操作</p> <p>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”：</p> <p>“取得文件或其它对象的所有权”设置为“只指派给 Administrators 组”</p>
检测方法	<p>1、判定条件</p> <p>“取得文件或其它对象的所有权”设置为“只指派给 Administrators 组”</p> <p>2、检测操作</p> <p>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”：</p> <p>查看是否“取得文件或其它对象的所有权”设置为“只指派给 Administrators 组”</p>

编号：安全要求-设备-WINDOWS-配置-11

要求内容	在本地安全设置中配置指定授权用户允许本地登陆此计算机。
操作指南	1、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” “允许本地登录”设置为允许本地登录的用户或组。
检测方法	1、判定条件 “从本地登陆此计算机”设置为“指定授权用户” 2、检测操作 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” 查看是否“允许本地登录”设置为允许本地登录的用户或组。

编号：安全要求-设备-WINDOWS-配置-12

要求内容	在组策略中只允许授权帐号从网络访问(包括网络共享等，但不包括终端服务)此计算机。
操作指南	1、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” “从网络访问此计算机”设置为允许网络访问此计算机的用户或组。
检测方法	1、判定条件 “从网络访问此计算机”设置为允许网络访问此计算机的用户或组。 2、检测操作 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” 查看是否“从网络访问此计算机”设置为允许网络访问此计算机的

	信息安全规划与实施项目 安全配置基线	
--	-----------------------	--

	用户或组。
--	-------

编号：安全要求-设备-WINDOWS-配置-13

要求内容	禁止用户开机自动登陆
操作指南	<p>1、参考配置操作</p> <p>在“开始->运行->键入 regedit”</p> <p>修订注册表项： HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\AutoAdminLogon (REG_DWORD)，值为 0</p>
检测方法	<p>1、符合性判定依据</p> <p>HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\AutoAdminLogon (REG_DWORD)设置为 0</p> <p>2、参考检测方法</p> <p>见前面描述</p>

2.2 日志配置操作

编号：安全要求-设备-WINDOWS-配置-14

要求内容	设备应配置日志功能，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。
操作指南	<p>1、参考配置操作</p> <p>开始->运行-> 执行 “ 控制面板->管理工具->本地安全策略->审核策略”</p> <p>审核登录事件，双击，设置为成功和失败都审核。</p>
检测方法	<p>1、判定条件</p> <p>审核登录事件，设置为成功和失败都审核。</p>

信息安全规划与实施项目		
安全配置基线		

	<p>2、检测操作</p> <p>开始->运行-> 执行 “ 控制面板->管理工具->本地安全策略->审核策略”</p> <p>审核登录事件，双击，查看是否设置为成功和失败都审核。</p>
--	--

编号：安全要求-设备-WINDOWS-配置-15

要求内容	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。
操作指南	<p>1、参考配置操作</p> <p>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</p> <p>“审核策略更改”设置为“成功”和“失败”都要审核</p>
检测方法	<p>1、判定条件</p> <p>“审核策略更改”设置为“成功”和“失败”都要审核</p> <p>2、检测操作</p> <p>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</p> <p>查看是否“审核策略更改”设置为“成功”和“失败”都要审核</p>

编号：安全要求-设备-WINDOWS-配置-16

要求内容	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。
操作指南	<p>1、参考配置操作</p> <p>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：</p> <p>“审核对象访问”设置为“成功”和“失败”都要审核</p>

信息安全规划与实施项目		
安全配置基线		

检测方法	<p>1、判定条件</p> <p>“审核对象访问”设置为“成功”和“失败”都要审核</p> <p>2、检测操作</p> <p>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：</p> <p>查看是否“审核对象访问”设置为“成功”和“失败”都要审核</p>
------	--

编号：安全要求-设备-WINDOWS-配置-17

要求内容	启用组策略中对 Windows 系统的审核目录服务访问，失败。
操作指南	<p>1、参考配置操作</p> <p>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：</p> <p>“审核目录服务访问”设置为“成功”和“失败”都要审核</p>
检测方法	<p>1、判定条件</p> <p>“审核目录服务访问”设置为“成功”和“失败”都要审核</p> <p>2、检测操作</p> <p>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：</p> <p>查看是否“审核目录服务访问”设置为“成功”和“失败”都要审核</p>

编号：安全要求-设备-WINDOWS-配置-18

要求内容	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。
操作指南	<p>1、参考配置操作</p> <p>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：</p> <p>“审核特权使用”设置为“成功”和“失败”都要审核</p>

信息安全规划与实施项目		
安全配置基线		

检测方法	<p>1、判定条件</p> <p>“审核特权使用”设置为“成功”和“失败”都要审核</p> <p>2、检测操作</p> <p>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：</p> <p>查看是否“审核特权使用”设置为“成功”和“失败”都要审核</p>
------	--

编号：安全要求-设备-WINDOWS-配置-19

要求内容	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。
操作指南	<p>1、参考配置操作</p> <p>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：</p> <p>“审核系统事件”设置为“成功”和“失败”都要审核</p>
检测方法	<p>1、判定条件</p> <p>“审核系统事件”设置为“成功”和“失败”都要审核</p> <p>2、检测操作</p> <p>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：</p> <p>查看是否“审核系统事件”设置为“成功”和“失败”都要审核</p>

编号：安全要求-设备-WINDOWS-配置-20

要求内容	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。
操作指南	<p>1、参考配置操作</p> <p>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：</p> <p>“审核账户管理”设置为“成功”和“失败”都要审核</p>

信息安全规划与实施项目		
安全配置基线		

检测方法	<p>1、判定条件</p> <p>“审核账户管理”设置为“成功”和“失败”都要审核</p> <p>2、检测操作</p> <p>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：</p> <p>查看是否“审核账户管理”设置为“成功”和“失败”都要审核</p>
------	--

编号：安全要求-设备-WINDOWS-配置-21

要求内容	启用组策略中对 Windows 系统的审核过程/进程跟踪。
操作指南	<p>1、参考配置操作</p> <p>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：</p> <p>“审核过程跟踪或审核进程跟踪”设置为“失败”需要审核</p>
检测方法	<p>1、判定条件</p> <p>“审核过程跟踪或审核进程跟踪”设置为“失败”需要审核</p> <p>2、检测操作</p> <p>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：</p> <p>查看是否“审核过程跟踪或审核进程跟踪”设置为“失败”需要审核</p>

编号：安全要求-设备-WINDOWS-配置-22

要求内容	设置应用日志文件最大大小 20480KB, 设置当达到最大的日志大小时，按需要覆盖事件。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->事件查看器”，在“事件查看器（本地）”中：</p> <p>“应用程序”属性中的日志最大大小“20480KB”，设置当达到日</p>

信息安全规划与实施项目		
安全配置基线		

	志最大大小时，“按需要改写事件”
检测方法	<p>1、判定条件</p> <p>“应用程序”属性中的日志最大大小“20480KB”，设置当达到日志最大大小时，“按需要覆盖事件”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->事件查看器”，在“事件查看器（本地）”中：</p> <p>查看是否“应用程序”属性中的日志最大大小“20480KB”，设置当达到日志最大大小时，“按需要覆盖事件”</p>

编号：安全要求-设备-WINDOWS-配置-23

要求内容	设置系统日志文件大小至少为 20480KB，设置当达到最大的日志大小时，按需要覆盖事件。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->事件查看器”，在“事件查看器（本地）”中：</p> <p>“系统日志”属性中的日志最大大小“20480KB”，设置当达到日志最大大小时，“按需要覆盖事件”</p>
检测方法	<p>1、判定条件</p> <p>“系统日志”属性中的日志最大大小“20480KB”，设置当达到日志最大大小时，“按需要覆盖事件”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->事件查看器”，在“事件查看器（本地）”中：</p> <p>查看是否“系统日志”属性中的日志最大大小“20480KB”，设置当达到日志最大大小时，“按需要覆盖事件”</p>

编号：安全要求-设备-WINDOWS-配置-24

信息安全规划与实施项目		
安全配置基线		

要求内容	设置安全日志文件大小至少为 20480KB, 设置当达到最大的日志大小时, 按需要覆盖事件。建议将系统日志推送至日志服务器
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->事件查看器”, 在“事件查看器(本地)”中:</p> <p>“安全日志”属性中的日志最大大小“20480KB”, 设置当达到日志最大大小时, “按需要覆盖事件”</p>
检测方法	<p>1、判定条件</p> <p>“安全日志”属性中的日志最大大小“20480KB”, 设置当达到日志最大大小时, “按需要覆盖事件”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->事件查看器”, 在“事件查看器(本地)”中:</p> <p>查看是否“安全日志”属性中的日志最大大小“20480KB”, 设置当达到日志最大大小时, “按需要覆盖事件”</p>

2.3 设备其他配置操作

2.3.1 屏幕保护

编号: 安全要求-设备-WINDOWS-配置-25

要求内容	接通电源情况下, 5 分钟关闭屏幕。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->显示->个性化->电源和睡眠->设置屏幕 5 分组后关闭”:</p>

信息安全规划与实施项目		
安全配置基线		

检测方法	1、检测操作 进入“控制面板—>显示—>个性化-->电源和睡眠”； 查看是否启用屏幕保护程序，设置等待时间为“5 分钟”
------	---

编号：安全要求-设备-WINDOWS-配置-26

要求内容	对于远程登陆的帐号，设置不活动断连时间 15 分钟。
操作指南	1、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->安全选项”： “Microsoft 网络服务器”设置为“在挂起会话之前所需的空闲时间或暂停会话前所需的空闲时间数量”为 15 分钟
检测方法	1、判定条件 “Microsoft 网络服务器”设置为“在挂起会话之前所需的空闲时间或暂停会话前所需的空闲时间数量”为 15 分钟。 2、检测操作 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”： 查看是否“Microsoft 网络服务器”设置为“在挂起会话之前所需的空闲时间或暂停会话前所需的空闲时间数量”为 15 分钟

2.3.2 共享文件夹及访问权限

编号：安全要求-设备-WINDOWS-配置-27

要求内容	非域环境中，关闭 Windows 硬盘默认共享，例如 C\$，D\$。
操作指南	1、参考配置操作 进入“开始—>运行—>Regedit”，进入注册表编辑器， 更改注册表键值：在 HKLM\System\CurrentControlSet\

信息安全规划与实施项目		
安全配置基线		

	Services\LanmanServer\Parameters\下，增加 REG_DWORD 类型的 AutoShareServer 键，值为 0。
检测方法	<p>1、判定条件</p> <p>HKLM\System\CurrentControlSet\</p> <p>Services\LanmanServer\Parameters\ 增加了 REG_DWORD 类型的 AutoShareServer 键，值为 0。</p> <p>2、检测操作</p> <p>进入“开始—>运行—>Regedit”，进入注册表编辑器，更改注册表键值：在 HKLM\System\CurrentControlSet\</p> <p>Services\LanmanServer\Parameters\下，增加 REG_DWORD 类型的 AutoShareServer 键，值为 0。</p>

编号：安全要求-设备-WINDOWS-配置-28

要求内容	查看每个共享文件夹的共享权限，只允许授权的账户拥有权限共享此文件夹。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->计算机管理”，进入“系统工具—>共享文件夹”：</p> <p>查看每个共享文件夹的共享权限，只将权限授权于指定账户。</p>
检测方法	<p>1、判定条件</p> <p>查看每个共享文件夹的共享权限仅限于业务需要，不设置成为“everyone”。</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->计算机管理”，进入“系统工具—>共享文件夹”：</p> <p>查看每个共享文件夹的共享权限。</p>

2.3.3 防病毒管理

编号：安全要求-设备-WINDOWS-配置-29

要求内容	安装防病毒软件，并及时更新。
操作指南	1、参考配置操作 安装防病毒软件，并及时更新。
检测方法	1、判定条件 已安装防病毒软件，病毒码更新时间不早于 1 个月，各系统病毒码升级时间要求参见各系统相关规定。 2、检测操作 控制面板->添加或删除程序，是否安装有防病毒软件。打开防病毒软件控制面板，查看病毒码更新日期。

编号：安全要求-设备-WINDOWS-配置-30

要求内容	关闭 Windows 自动播放功能
操作指南	1、参考配置操作 控制面板-自动播放-取消勾选“为所有媒体和设备使用自动播放”
检测方法	1、判定条件 所有驱动器均“关闭自动播放” 2、检测操作 “关闭自动播放”配置已启用，启用范围：所有驱动器。

编号：安全要求-设备-WINDOWS-配置-31

要求内容	如需启用 SNMP 服务，则修改默认的 SNMP Community String 设置。
操作指南	1、参考配置操作 打开“控制面板”，打开“管理工具”中的“服务”，找到“SNMP Service”，单击右键打开“属性”面板中的“安全”选项卡，在这个配置界面中，可以修改 community

信息安全规划与实施项目		
安全配置基线		

	strings，也就是微软所说的“团体名称”。
检测方法	<p>1、符合性判定依据</p> <p>community strings 已改，不是默认的“public”</p> <p>2、参考检测方法</p> <p>打开“控制面板”，打开“管理工具”中的“服务”，找到“SNMP Service”，单击右键打开“属性”面板中的“安全”选项卡，在这个配置界面中，查看 community strings，也就是微软所说的“团体名称”</p>

编号：安全要求-设备-WINDOWS-配置-32

要求内容	优先建议关闭 windows RDP 服务，接入 ME 平台，接入 ME 平台步骤见相应操作手册
操作指南	>wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 0
检测方法	<p>1、检测操作</p> <p>>netstat -an find "3389"</p>

编号：安全要求-设备-WINDOWS-配置-33

要求内容	禁用匿名访问命名管道和共享
操作指南	<p>1、参考配置操作</p> <p>“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可匿名访问的共享设置为全部删除</p> <p>“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可匿名访问的命名管道 设置为全部删除</p>
检测方法	<p>1、符合性判定依据</p> <p>全部删除匿名访问命名管道和共享</p> <p>2、参考检测方法</p> <p>查看“控制面板->管理工具->本地安全策略”，在“本地策略->安</p>

信息安全规划与实施项目		
安全配置基线		

	全选项”：网络访问：可匿名访问的共享、可匿名访问的命名管道 是否设置为全部删除
--	--

编号：安全要求-设备-WINDOWS-配置-34

要求内容	禁用可远程访问的注册表路径和子路径
操作指南	<p>1、参考配置操作</p> <p>“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可远程访问的注册表路径 设置为全部删除</p> <p>“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可远程访问的注册表路径和子路径 设置为全部删除</p>
检测方法	<p>1、符合性判定依据</p> <p>全部删除可远程访问的注册表路径和子路径</p> <p>3、参考检测方法</p> <p>查看“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问中，查看，可远程访问的注册表路径、可远程访问的注册表路径和子路径是否设置为全部删除</p>

编号：安全要求-设备-WINDOWS-配置-35

要求内容	禁止匿名用户空链接
操作指南	<p>1、参考配置操作</p> <p>修改注册表项：</p> <p>HKEY_LOCAL_MACHINE SYSTEM\Current\Control\Set\Control\Lsa\ restrictanonymous(REG_DWORD) ， 值为 1</p>
检测方法	<p>1、符合性判定依据</p> <p>注册表项： HKEY_LOCAL_MACHINE SYSTEM\Current\Control\Set\Control\Lsa\ restrictanonymous(REG_DWORD)=1</p> <p>2、参考检测操作</p>

	信息安全规划与实施项目 安全配置基线	
--	-----------------------	--

	见前面描述
--	-------