Windows 系统通用安全配置基线

一：共享账号检查

配置名称：账号分配检查，避免共享账号存在

配置要求：

1、系统需按照实际用户分配账号；

2、根据系统的使用需求，设定不同的账户和账户组，包括管理员用户，数据库用户，审计用户，来宾用户等；

3、避免出现共享账号情况；

操作指南：参考配置操作（适用 2000、2003）

”控制面板->管理工具->计算机管理->系统工具->本地用户和组”。

参考配置操作（适用 2008 x64）

”管理工具->服务器管理->配置->本地用户和组”。

检查方法：查看已创建账户和账户组，与管理员确认有无无用的或共用的账户，如果每一账户都按需创建和划分账户组的则符合要求。

配置方法：根据系统实际使用需求，设定不同的账户和账户组，如：管理员用户，数据库用户，审计用户，来宾用户。

使用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64。

二：来宾账户检查

配置名称：禁用来宾账户

配置要求：禁用 guest（来宾）用户

操作指南：参考配置操作（适用 2000、2003）

”控制面板->管理工具->计算机管理”，在”系统工具->本地用户和组->Guest 账户>属性->“常规”页

参考配置操作（适用 2008 x64）

”管理工具->服务器管理”，在”配置->本地用户和组->Guest 账户->属性-> “常规”页

检查方法：检查复选框”账户已禁用”项状态，勾选为已禁用来宾账号

配置方法：勾选复选框”账户已禁用”项，禁用来宾账号。

适用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64。

三：口令复杂度策略

配置名称：口令复杂度策略

配置要求：

1、最短密码长度 12 个字符；

2、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：

- υ 英语大写字母 A, B, C, … Z
- υ 英语小写字母 a, b, c, … z
- υ 西方阿拉伯数字 0, 1, 2, … 9
- υ 非字母数字字符，如标点符号，@, #, $, %, &, *等

操作指南：参考配置操作（适用 2000、2003）

1、”控制面板->管理工具->本地安全策略->帐户策略->密码策略->密码长度最小值->属性”

2、”控制面板->管理工具->本地安全策略->帐户策略->密码策略->密码必须符合复杂性要求->属性”

参考配置操作（适用 2008 x64）

1、”管理工具->本地安全策略->帐户策略->密码策略->密码长度最小值->属性”

2、”管理工具->本地安全策略->帐户策略->密码策略->密码必须符合复杂性要求->属性”

检查方法：1、检查最小值设置，大于等于 12 为符合要求；

2、检查单选框”已启动”状态，选中”已启动”为符合。

配置方法：1、将密码最小值设置为大于等于 12；

2、将”密码必须符合复杂性要求”项，选中”已启动”。

使用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64

四：口令最长生存期策略

配置名称：口令最长生存期策略

配置要求：要求操作系统的账户口令的最长生存期不长于 90 天。

操作指南：参考配置操作（适用 2000、2003）

”控制面板->管理工具->本地安全策略->帐户策略->密码策略->密码最长存留期->属性”

参考配置操作（适用 2008 x64）

”管理工具->本地安全策略->帐户策略->密码策略->密码最长存留期->属性”

检查方法：检查”密码最长使用期限”小于等于 90 为符合。

配置方法：检查”密码最长使用期限”小于等于 90 为符合。

使用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64

五：远程关机授权

配置名称：本地安全设置中远程关机授权只指派给 Administrators 组

配置要求：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：参考配置操作（适用 2000、2003）

”控制面板->管理工具->本地安全策略->本地策略->用户权利指派->从远端系统强制关机->属性”

参考配置操作（适用 2008 x64）

”管理工具->本地安全策略->本地策略->用户权限分配->从远程系统强制关机->属性”

检查方法：查看”从远端系统强制关机”权限指派情况”，仅指派给 administrators，符合要求。

配置方法：设置为”只指派给 Administrators 组”

使用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64

六：系统关闭授权

配置名称：本地安全设置中关闭系统仅指派给 Administrators 组

配置要求：检测本地安全设置中关闭系统仅指派给 Administrators 组

操作指南：参考配置操作（适用 2003）

”控制面板->管理工具->本地安全策略->本地策略->用户权利指派->关闭系统->属性”

参考配置操作（适用 2008 x64）

”管理工具->本地安全策略->本地策略->用户权限分配->关闭系统->属性”

检查方法：查看”关闭系统”权限指派情况，内容为 administrators，表示符合要求。

配置方法：设置为”只指派给 Administrators 组”

使用版本：Windows Server 2003、Windows Server 2008 X64

七：文件权限指派

配置名称：文件权限指派

配置要求：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。

操作指南：参考配置操作（适用 2003）

”控制面板->管理工具->本地安全策略->本地策略->用户权利指派->取得文件或其它

对象的所有权->属性”

参考配置操作（适用 2008 x64）

”管理工具->本地安全策略->本地策略->用户权限分配->用户权利指派->取得文件或其它对象的所有权->属性”

检查方法 :查看“取得文件或其它对象”的仅限指情况 ,指派给 Administrators”为符合要求。

配置方法：设置为”只指派给 Administrators 组”

使用版本：Windows Server 2003、Windows Server 2008 X64

八：匿名权限限制

配置名称：网络连接中限制匿名用户连接权限

配置要求：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：参考配置操作（适用 2003）

”控制面板->管理工具->本地安全策略->本地策略->用户权利指派->从网络访问此计算机->属性”

参考配置操作（适用 2008 x64）

”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->属性”

检查方法 :检查属性列表 ,不包括”Users”和”Everyone”组和其他无用组为符合要求.

配置方法：根据需求添加访问组。

适用版本：Windows Server 2003、Windows Server 2008 X64

八：登陆日志检查

配置名称：检测是否设置审核账户登录事件

配置要求：系统应启用日志功能，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：参考配置操作（适用 2000、2003）

”控制面板->管理工具->本地安全策略->审核策略->审核登录事件->属性”。

参考配置操作（适用 2008 x64）

”管理工具->本地安全策略->审核策略->审核登录事件->属性”。

检查方法：检查是否同时勾选了”成功”和”失败”，同时勾选为符合要求。

配置方法：设置为成功和失败都审核。

适用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64

九：系统日志完备性检查

配置名称：系统日志完备性检查，检查是否启用系统多项审核策略

配置要求：系统应配置完整的审核策略，启用本地策略中审核策略中如下项。每项都需要设置为”成功”和”失败”都要审核。

参考配置操作（适用 2000、2003）

”控制面板->管理工具->本地安全策略->需要配置的策略：

参考配置操作（适用 2008 x64）

”管理工具->本地安全策略->需要配置的策略：

- 审核策略更改
- 审核对象访问

- υ 审核进程跟踪
- υ 审核目录服务访问
- υ 审核特权使用
- υ 审核系统事件
- υ 审核账户管理

操作指南：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->审核策略”中。进入如下项的”属性页”

- υ λ审核策略更改
- υ λ审核对象访问
- υ λ审核进程跟踪
- υ λ审核目录服务访问
- υ λ审核特权使用
- υ λ审核系统事件
- υ 审核账户管理

检查方法：检查项包括以下 7 子项：

- υ 检测是否启用对 Windows 系统的审核策略更改
- υ 检测是否启用对 Windows 系统的审核对象访问
- υ 检测是否启用 Windows 系统审核目录服务访问
- υ 检测是否启用 Windows 系统审核特权使用
- υ 检测是否启用 Windows 系统审核系统事件
- υ 检测是否启用 Windows 系统的审核账户管理

υ检测是否启用 Windows 系统的审核过程追踪

以上每一项都要勾选”成功”和”失败”项，才符合要求。

配置方法：分别进入以上 7 个子项配置页，勾选”成功”和”失败”复选框。

适用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64

十：日志大小设置

配置名称：检测系统日志、应用日志、安全日志的大小以及扩展设置是否符合规范

配置要求：

1、设置系统日志文件大小至少为 32MB ,设置当达到最大的日志尺寸时，按需要改写事件。

2、设置应用日志文件大小至少为 32M B，设置当达到最大的日志尺寸时，按需要改写事件。

3、设置安全日志文件大小至少为 32M B，设置当达到最大的日志尺寸时，按需要改写事件。

操作指南：参考配置操作（适用 2000、2003）

进入”控制面板->管理工具->事件查看器”,在”事件查看器（本地）”中的：

“系统日志”属性页；

“应用日志”属性页；

“安全日志”属性页。

参考配置操作（适用 2008 x64）

进入”管理工具->服务器管理”， 在”诊断->事件查看器->windows 日志”中的：

“系统日志”属性页；

“应用日志”属性页；

“安全日志”属性页。

检查方法：检查包括以下 6 子项

- υ 应用日志文件大小至少为 32M B
- υ 当达到最大的应用日志尺寸时，按需要改写事件
- υ 系统日志文件大小至少为 32M B
- υ 当达到最大的应用日志尺寸时，按需要改写事件
- υ 安全日志文件大小至少为 32M B
- υ 当达到最大的安全日志尺寸时，按需要改写事件

以上检查内容符合，整体才符合要求。

配置方法：1、设置应用日志文件大小至少为 32M B

设置当达到最大的应用日志尺寸时，按需要改写事件

2、设置系统日志文件大小至少为 32M B

设置当达到最大的应用日志尺寸时，按需要改写事件

3、设置安全日志文件大小至少为 32M B

设置当达到最大的安全日志尺寸时，按需要改写事件

适用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64

十一：远程登录超时配置

配置名称：远程登陆超时配置

配置要求：检查设置：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：参考配置操作（适用 2003）

”控制面板->管理工具->本地安全策略->本地策略->安全选项->Microsoft 网络服务器”

参考配置操作（适用 2008 x64）

”管理工具->本地安全策略->本地策略->安全选项->Microsoft 网络服务器”

检查方法：检查”对于远程登陆的帐号设置”，不活动断连时间 15 分钟或小于 15 分钟为符合要求。

配置方法：设置为”在挂起会话之前所需的空闲时间”为 15 分钟或更小。

适用版本：Windows Server 2003、Windows Server 2008 X64

十二：默认共享检查

配置名称：默认共享检查

配置要求：非域环境中，关闭 Windows 硬盘默认共享，例如 C$，D$。

操作指南：参考配置操作

”开始 - >运行 - >net share”

检查方法：检查有无默认共享，无任何默认共享为符合要求。

配置方法：”开始 - >运行 - >Regedit”，进入注册表编辑器，

定位到

HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\下，

增加 REG_DWORD 类型的 AutoShareServer 键，值为 0。

Windows Server 2008X64 环境配置检查位置：HKEY_LOCAL_MACHINE//SYSTEM//CurrentControlSet//Services//lanmanserver//parameters”

适用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64

十三：共享权限检查

配置名称：共享权限检查

配置要求：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，禁止使用共享权限为”everyone”

操作指南：参考配置操作（适用 2000、2003）

”控制面板->管理工具->计算机管理->系统工具 - >共享文件夹”

参考配置操作（适用 2008 x64）

”管理工具->共享和存储管理”

检查方法：

1、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”

2、输出所有共享文件夹信息和具体权限信息；但权限是否符合需求需要后期处理确认

配置方法：在”共享文件”属性页中，只保留需要的账户。

适用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64

十四：防范病毒管理

配置名称：防病毒管理

配置要求：安装防病毒软件，并及时更新。

操作指南：参考配置操作

定位到杀毒软件版本信息页面。

检查方法：检查防病毒进程运行是否正常及当前病毒库版本是否为最新。

配置方法：安装防病毒软件，并检查是否更新到最新病毒定义。

适用版本：Windows Server 2003 、Windows 2000 Server、Windows Server 2008 X64