|  |
| --- |
| **老男孩信息系统安全配置基线**  **Windows操作系统分册（初稿）** |
| **版本 V1.0** |

**二○一九年一月**

|  |  |  |  |
| --- | --- | --- | --- |
| ■版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 目录 |
| [一. 概述 5](#_Toc408244789)  [1.1适用范围 5](#_Toc408244790)  [1.2规范依据 5](#_Toc408244791)  [1.3实施策略 5](#_Toc408244792)  [二. 安全配置基线标准 7](#_Toc408244793)  [2.1身份鉴别 7](#_Toc408244794)  [2.1.1配置口令复杂度 7](#_Toc408244795)  [2.1.2设置口令认证失败锁定次数 7](#_Toc408244796)  [2.1.3设置重置账户锁定计数器 8](#_Toc408244797)  [2.1.4配置口令生存期 9](#_Toc408244798)  [2.1.5设置口令到期提示 9](#_Toc408244799)  [2.1.6禁用域环境密码修改 10](#_Toc408244800)  [2.1.7配置历史口令使用策略 10](#_Toc408244801)  [2.1.8限制匿名远程连接 11](#_Toc408244802)  [2.1.9配置会话锁定 11](#_Toc408244803)  [2.1.10配置口令最短使用时间 12](#_Toc408244804)  [2.2访问控制 12](#_Toc408244805)  [2.2.1禁止共享账户 12](#_Toc408244806)  [2.2.2禁用来宾账号（Guest） 13](#_Toc408244807)  [2.2.3禁止匿名账户枚举本地信息 14](#_Toc408244808)  [2.2.4配置共享权限 14](#_Toc408244809)  [2.2.5设置指派文件权限 15](#_Toc408244810)  [2.2.6变更默认管理员账号 15](#_Toc408244811)  [2.2.7修改SNMP默认口令 16](#_Toc408244812)  [2.2.8设置磁盘分区为NTFS格式 17](#_Toc408244813)  [2.2.9配置本机防火墙 17](#_Toc408244814)  [2.2.10控制本机端口访问 18](#_Toc408244815)  [2.2.11配置远程关机权限 18](#_Toc408244816)  [2.2.12配置系统关闭授权 19](#_Toc408244817)  [2.2.13关闭自动播放 19](#_Toc408244818)  [2.2.14配置操作系统分区位置及数量 20](#_Toc408244819)  [2.2.15设置授权用户本地登录 20](#_Toc408244820)  [2.2.16禁用Ctrl + Alt + Del 21](#_Toc408244821)  [2.2.17设置域验证解锁 22](#_Toc408244822)  [2.2.18配置指定可以远程访问的用户（组） 22](#_Toc408244823)  [2.3安全审计 23](#_Toc408244824)  [2.3.1配置登录日志审核 23](#_Toc408244825)  [2.3.2设置系统日志完备性性 23](#_Toc408244826)  [2.3.3配置使用NTP 24](#_Toc408244827)  [2.3.4配置日志文件容量 24](#_Toc408244828)  [2.4入侵防范 25](#_Toc408244829)  [2.4.1配置补丁管理 25](#_Toc408244830)  [2.4.2禁用不需要的服务 26](#_Toc408244831)  [2.5恶意代码防范 27](#_Toc408244832)  [2.5.1设置防病毒管理 27](#_Toc408244833)  [2.6资源控制 27](#_Toc408244834)  [2.6.1设置屏保密码保护 27](#_Toc408244835)  [2.6.2设置远程登录超时 28](#_Toc408244836)  [2.6.3设置登录超时 29](#_Toc408244837)  [2.7其它安全项 29](#_Toc408244838)  [2.7.1禁止显示上次的用户名 29](#_Toc408244839)  [2.7.2配置清除虚拟内存页面文件 30](#_Toc408244840)  [2.7.3设置前次登录缓存数量 30](#_Toc408244841)  [三. 评审与修订 31](#_Toc408244842) |

1. 概述
   1. 适用范围

本配置基线适用于老男孩的Microsoft Windows系列操作系统，主要涉及Windows操作系统安全配置方面的基本要求，用于指导安全例行工作、新系统入网安全检查等场合。

在未特别说明的情况下，均适用于所有运行的Windows系列操作系统。

* 1. 规范依据

根据老男孩目前Windows操作系统的安全现状，综合参考各信息系统运维部门的意见，结合金融行业等级保护实施指引，制定适合于老男孩的基线配置规范。

主要参考依据如下：

* JR/T0071-2012《金融行业信息系统信息安全等级保护实施指引》（2012年7月发布）
  1. 实施策略

结合网络和信息系统建设情况，考虑安全配置项影响的范围，结合以往工作经验，提出如下安全项目实施策略：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **配置类别** | **安全基线项目名称** | **实施策略** |
| 1 | 身份鉴别 | 配置口令复杂度 | 必须实施 |
| 2 | 身份鉴别 | 设置口令认证失败锁定次数 | 必须实施 |
| 3 | 身份鉴别 | 设置重置账户锁定计数器 | 必须实施 |
| 4 | 身份鉴别 | 配置口令生存期 | 必须实施 |
| 5 | 身份鉴别 | 设置口令到期提示 | 必须实施 |
| 6 | 身份鉴别 | 禁用域环境密码修改 | 建议实施 |
| 7 | 身份鉴别 | 配置历史口令使用策略 | 建议实施 |
| 8 | 身份鉴别 | 限制匿名远程连接 | 建议实施 |
| 9 | 身份鉴别 | 配置会话锁定 | 按需实施 |
| 10 | 身份鉴别 | 配置口令最短使用时间 | 按需实施 |
| 11 | 访问控制 | 禁止共享账户 | 必须实施 |
| 12 | 访问控制 | 禁用来宾账号（Guest） | 必须实施 |
| 13 | 访问控制 | 禁止匿名账户枚举本地信息 | 必须实施 |
| 14 | 访问控制 | 配置共享权限 | 必须实施 |
| 15 | 访问控制 | 设置指派文件权限 | 必须实施 |
| 16 | 访问控制 | 变更默认管理员账号 | 必须实施 |
| 17 | 访问控制 | 修改SNMP默认口令 | 必须实施 |
| 18 | 访问控制 | 设置磁盘分区为NTFS格式 | 必须实施 |
| 19 | 访问控制 | 配置本机防火墙 | 建议实施 |
| 20 | 访问控制 | 控制本机端口访问 | 建议实施 |
| 21 | 访问控制 | 配置远程关机权限 | 建议实施 |
| 22 | 访问控制 | 配置系统关闭授权 | 建议实施 |
| 23 | 访问控制 | 关闭自动播放 | 建议实施 |
| 24 | 访问控制 | 配置操作系统分区位置及数量 | 建议实施 |
| 25 | 访问控制 | 设置授权用户本地登录 | 建议实施 |
| 26 | 访问控制 | 禁用Ctrl+Alt+Del | 建议实施 |
| 27 | 访问控制 | 设置域验证解锁 | 按需实施 |
| 28 | 访问控制 | 配置指定可以远程访问的用户（组） | 按需实施 |
| 29 | 安全审计 | 配置登录日志审核 | 必须实施 |
| 30 | 安全审计 | 设置系统日志完备性性 | 必须实施 |
| 31 | 安全审计 | 配置使用NTP | 必须实施 |
| 32 | 安全审计 | 配置日志文件容量 | 建议实施 |
| 33 | 入侵防范 | 配置补丁管理 | 必须实施 |
| 34 | 入侵防范 | 禁用不需要的服务 | 必须实施 |
| 35 | 恶意代码防范 | 设置防病毒管理 | 必须实施 |
| 36 | 资源控制 | 设置屏保密码保护 | 必须实施 |
| 37 | 资源控制 | 设置远程登录超时 | 必须实施 |
| 38 | 资源控制 | 设置登录超时 | 必须实施 |
| 39 | 其它安全项 | 禁止显示上次的用户名 | 必须实施 |
| 40 | 其它安全项 | 配置清除虚拟内存页面文件 | 建议实施 |
| 41 | 其它安全项 | 设置前次登录缓存数量 | 建议实施 |

1. 安全配置基线标准
   1. 身份鉴别
      1. 配置口令复杂度

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置口令复杂度（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-1 |
| **安全基线项说明** | 建议最短密码长度为 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，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 |
| **配置方法** | **登录系统，以管理员权限进行如下操作（以下两种方法任选其一）：**  **第一种方法：**进入“开始->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”、“密码长度最小值”设置为“8个字符”。  **第二种方法：**进入“开始”->“运行”输入“gpedit.msc”回车，在打开的“组策略”对话框中选择“windows设置”->“安全设置”->“账户策略”->“密码策略”中“密码必须符合复杂性要求”选择“已启动”、“密码长度最小值”设置为“8个字符”。  \*注意：进行上述配置后，建议重启计算机（生效）。 |
| **检查方法** | 任选一种配置方法中提供的操作步骤进入“密码策略”菜单，检查“密码必须符合复杂性要求”是否已设置为“已启动”、“密码长度最小值”是否已设置为“8个字符”，如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），c）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。 |
| **备注** |  |

* + 1. 设置口令认证失败锁定次数

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置口令认证失败锁定次数（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-2 |
| **安全基线项说明** | 应配置当用户短时间内连续认证失败次数超过10次（不含10次），锁定该用户使用的账号；设置账户锁定时间为3分钟。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000**  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“帐户锁定阀值”设置。  **版本：Windows Server 2003、Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->本地安全策略->帐户策略->帐户锁定策略”：  “账户锁定阀值”设置为 10次无效登录；  “账户锁定时间”设置为3分钟。 |
| **检查方法** | 登录系统进入“开始->管理工具->本地安全策略->帐户策略->帐户锁定策略”检查：  “账户锁定阀值”是否设置为“10次”，如果是则符合，否则不符合；  “账户锁定时间”是否设置为“3分钟”，如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），d）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。 |
| **备注** |  |

* + 1. 设置重置账户锁定计数器

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置重置账户锁定计数器（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-3 |
| **安全基线项说明** | 此安全设置确定在某次登录尝试失败之后将登录尝试失败计数器重置为 0 次错误登录尝试之前需要的时间。可用范围是 1 到 99,999 分钟。  如果定义了帐户锁定阈值，此重置时间必须小于或等于帐户锁定时间。  默认值: 无，因为只有在指定了帐户锁定阈值时，此策略设置才有意义。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入控制面板->管理工具->本地安全策略->帐户策略->账号锁定策略->复位（重置）账号锁定计数器->属性（或在此选项上双击鼠标左键）->设置“复位账号锁定计数器”的值。  该值需根据实际需求配置。  参考值：15~30（分钟之后） |
| **检查方法** | 两种检查方法（任选其一）：  1.依照配置方法中的步骤进入到“复位账号锁定计数器”，检查是否设置值（例如：15~30分钟），如果是则符合，否则不符合。  2.在合适的情况下，连续输错密码后，观察被锁定的时间〉=（大于等于）计数器设置的时间，如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），d）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。 |
| **备注** |  |

* + 1. 配置口令生存期

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置口令生存期（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-4 |
| **安全基线项说明** | 要求操作系统的账户口令的最长生存期不长于90天。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”，强制密码历史策略配置为24个。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->本地安全策略->帐户策略->密码策略”：  “密码最长使用期限”设置为“90天”。 |
| **检查方法** | 登录系统依照配置方法中给出的操作进入到“密码策略”里，检查“密码最长存留期”或“密码最长使用期限”里设置的值是否满足要求（90天），如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），c）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。 |
| **备注** |  |

* + 1. 设置口令到期提示

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 口令到期提示（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-5 |
| **安全基线项说明** | 配置成在密码有效期14天前，通知用户更改密码。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入控制面板->管理工具->本地安全策略->安全选项->密码到期前提示用户更改密码  配置成14天前，通知用户更改密码。 |
| **检查方法** | 依照配置方法进入“安全选项”里，检查“交互式登录: 提示用户在密码过期之前进行更改”是否设置为“15天”，如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，系统的静态口令应在8位以上并由字母、数字、符号等混合组成并每三个月更换口令； |
| **备注** |  |

* + 1. 禁用域环境密码修改

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 禁用域环境密码修改（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-6 |
| **安全基线项说明** | 禁止域环境下，登录用户修改本地计算机密码。  如果是域控制域内的成员，检测是否禁用更改机器账户密码。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  检测是否禁用更改机器账户密码 配置方法：进入“控制面板”->“管理工具”->“本地安全策略”->“安全选项”->“禁用更改机器账户密码”设置为“已禁用”。  **版本：Windows Server 2008、Windows Server 2012**  进入“控制面板->管理工具->本地安全策略->本地策略->安全选项”：  将“域成员: 禁用计算机帐户密码更改”设置为“已禁用”。 |
| **检查方法** | 依照配置方法打开“安全选项”，检查“禁用更改机器账户密码”或“域成员: 禁用计算机帐户密码更改”是否均设置为“已禁用”，如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），b) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别 |
| **备注** | 非域控服务器、非域成员不检查此项。 |

* + 1. 配置历史口令使用策略

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置历史口令使用策略（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-7 |
| **安全基线项说明** | 要求操作系统的账户口令的不能使用最近3次内已使用的口令 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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“是否强制密码历史”设置为大于等于标准值（3）。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->本地安全策略->帐户策略->密码策略”：  “强制密码历史”设置为“3个记住的密码”。 |
| **检查方法** | 依照配置方法打开“密码策略”，查看“强制密码历史”是否设置〉=3的值，如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，系统的静态口令应在8位以上并由字母、数字、符号等混合组成并每三个月更换口令； |
| **备注** |  |

* + 1. 限制匿名远程连接

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 限制匿名远程连接（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-8 |
| **安全基线项说明** | 限制匿名用户连接权限，防止用户远程枚举本地帐号，不允许枚举SAM帐号和共享。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入“开始->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 帐户的匿名枚举”设置为“已启用” |
| **检查方法** | 依照配置方法打开“安全选项”，检查如果是则符合，检查“网络访问：不允许 SAM 帐户的匿名枚举”是否设置为“已启用”，如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），b) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别 |
| **备注** |  |

* + 1. 配置会话锁定

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置会话锁定（按需实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-9 |
| **安全基线项说明** | 如果是域控制域内的成员，检测会话锁定时显示用户信息 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System”，添加名称为“DontDisplayLockedUserId”、类型为DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为1-3，其中1表示显示名称、域名、用户名，2表示仅显示用户名称，3表示不显示用户信息。Windows2000没有此设置，不检查此项。 |
| **检查方法** | 锁定用户后，检查界面上是否显示用户信息，如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），b) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别 |
| **备注** | 不是域控服务器或域成员不检查此项。Windows2000没有此设置，不检查此项。 |

* + 1. 配置口令最短使用时间

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置口令最短使用时间（按需实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS -10 |
| **安全基线项说明** | 密码最短使用期限设置为2天 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入控制面板->管理工具->本地安全策略->帐户策略->密码策略->密码最短存留期 |
| **检查方法** | 依照  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.1 主机：身份鉴别（S3），c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，系统的静态口令应在8位以上并由字母、数字、符号等混合组成并每三个月更换口令； |
| **备注** |  |

* 1. 访问控制
     1. 禁止共享账户

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 禁止共享账户（必须实施） |
| **安全基线**  **编号** | 操作系统--WINDOWS--11 |
| **安全基线项说明** | 系统需按照实际用户分配账号；  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，避免出现共享账号情况。  该项采用问询的方式。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  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。 |
| **检查方法** | 通过问询方式检查是否存在共享使用的账户，若无则满足安全需求；若存在则根据实际需求新建不同类型、权限的账户。 |
| **依据** | 7.1.3.2 主机：访问控制(S3），b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。 |
| **备注** |  |

* + 1. 禁用来宾账号（Guest）

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 禁用来宾账号（guest）（必须实施） |
| **安全基线**  **编号** | 操作系统—WINDOWS—配置-12 |
| **安全基线项说明** | 禁用guest（来宾）帐号。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”：  Guest帐号->属性－>已停用  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->服务器管理->配置>本地用户和组->用户”：  Guest帐号->属性－>已停用 |
| **检查方法** | 依照配置方法进入“本地用户和组”菜单内，检查Guest帐号是否已停用。如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），d) 应禁用或严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； |
| **备注** |  |

* + 1. 禁止匿名账户枚举本地信息

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 禁止匿名账户枚举本地信息（必须实施） |
| **安全基线**  **编号** | 操作系统—WINDOWS -13 |
| **安全基线项说明** | 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。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  打开命令提示符，运行命令“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: 不允许 SAM 帐户的匿名枚举”，配置为“启用”(在Windows2000下，无此设置，不检查此项)。 |
| **检查方法** | 依照配置方法进入“安全选项”菜单内，检查“网络访问: 不允许 SAM 帐户的匿名枚举”一项是否已配置成“启用”，如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），b) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限 |
| **备注** |  |

* + 1. 配置共享权限

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置共享权限（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-14 |
| **安全基线项说明** | 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” |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”：  查看每个共享文件夹的共享权限，只将权限授权于指定帐户，不设置成为“everyone”。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->控制面板->管理工具->共享和存储管理”：  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，不设置成为“everyone”。 |
| **检查方法** | 参考安全配置方法。  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”。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a）应启用访问控制功能，依据安全策略控制用户对资源的访问。  7.1.3.2 主机：访问控制（S3），f）宜对重要信息资源设置敏感标记。  7.1.3.2 主机：访问控制（S3），g）宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** |  |

* + 1. 设置指派文件权限

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置指派文件权限（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-15 |
| **安全基线项说明** | 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。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”：  “取得文件或其它对象的所有权”设置为“只指派给Administrators组”  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->本地安全策略”，在“本地策略->用户权限分配”：  “取得文件或其他对象的所有权”设置为只指派给“Administrators”组。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a）应启用访问控制功能，依据安全策略控制用户对资源的访问。 |
| **备注** |  |

* + 1. 变更默认管理员账号

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 变更默认管理员账号（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-16 |
| **安全基线项说明** | 对于管理员帐号，要求更改缺省帐户名称administrator |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”：  缺省帐户Administrator－>右键－>重命名  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->服务器管理->配置>本地用户和组->用户”：  缺省帐户Administrator－右键－>重命名 |
| **检查方法** | 进入“开始->管理工具->服务器管理->配置>本地用户和组->用户”。  检查是否已经更改缺省账户名称Administrator，如果没有更改则不符合，否则符合。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），d）应禁用或严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令。 |
| **备注** | 修改后会导致使用原管理员账号名启动的服务或应用出现异常，请同步管理员账号。  该配置不能从域控制系统下发，需要在本地去执行。 |

* + 1. 修改SNMP默认口令

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 修改SNMP默认口令（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-17 |
| **安全基线项说明** | 如需启用SNMP服务，则修改默认的SNMP Community String设置。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->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，修改community strings，也就是微软所说的“团体名称”。 |
| **检查方法** | 参考安全配置方法；community strings已改，不是默认的“public”。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），d）应禁用或严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令。 |
| **备注** | 如果服务器没有安装SNMP服务，则不必配置该项。 |

* + 1. 设置磁盘分区为NTFS格式

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置磁盘分区为NTFS格式（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-18 |
| **安全基线项说明** | 检查所有分区格式，最好采用较为安全的NTFS格式划分磁盘。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  检查所有分区格式 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），d) 应禁用或严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； |
| **备注** |  |

* + 1. 配置本机防火墙

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置本地防火墙（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-19 |
| **安全基线项说明** | 启用Windows自带防火墙。根据业务需要限定允许访问网络的应用程序，和允许远程登录该设备的IP地址范围。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入“控制面板－>网络连接－>本地连接”，在高级选项的设置中  启用Windows防火墙。  在“例外”中配置允许业务所需的程序接入网络。  在“例外->编辑->更改范围”编辑允许接入的网络地址范围。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a) 应启用访问控制功能，依据安全策略控制用户对资源的访问 |
| **备注** | 如果服务器前有网络防火墙，则可不必配置该项。 |

* + 1. 控制本机端口访问

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 控制本地端口访问（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-20 |
| **安全基线项说明** | 对没有自带防火墙的Windows系统，启用Windows系统的IP安全机制(IPSec)或网络连接上的TCP/IP筛选，只开放业务所需要的TCP，UDP端口和IP协议。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入“控制面板－>网络连接－>本地连接”，进入“Internet协议（TCP/IP）属性－>高级TCP/IP设置”，在“选项”的属性中启用网络连接上的TCP/IP筛选，只开放业务所需要的TCP，UDP端口和IP协议。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a) 应启用访问控制功能，依据安全策略控制用户对资源的访问 |
| **备注** | 如果服务器前有网络防火墙，则可不必配置该项。本配置项不适用windows2008系统。 |

* + 1. 配置远程关机权限

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置远程关机权限（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-21 |
| **安全基线项说明** | 在本地安全设置中从远端系统强制关闭本地计算机的权限（远程关机权限）只指派给Administrators组。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”设置。  **版本：Windows Server 2008、Windows Server 2012**  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”设置为“只指派给Administrators组”。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a）应启用访问控制功能，依据安全策略控制用户对资源的访问。 |
| **备注** |  |

* + 1. 配置系统关闭授权

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置系统关闭授权（建议实施） |
| **安全基线**  **编号** | 操作系统—WINDOWS -22 |
| **安全基线项说明** | 检测本地安全设置中关闭系统仅指派给Administrators组 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”设置。  **版本：Windows Server 2008、Windows Server 2012**  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”。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a）应启用访问控制功能，依据安全策略控制用户对资源的访问。 |
| **备注** |  |

* + 1. 关闭自动播放

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 关闭自动播放（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-23 |
| **安全基线项说明** | 关闭Windows自动播放功能 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  打开“开始→运行”，在对话框中输入“gpedit.msc”命令，在出现“组策略”窗口中依次选择“在计算机配置→管理模板→系统”，双击“关闭自动播放”查看，对话框中选择所有驱动器，确定即可。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->服务”：禁用Shell Hardware Detection。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a）应启用访问控制功能，依据安全策略控制用户对资源的访问。 |
| **备注** |  |

* + 1. 配置操作系统分区位置及数量

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置操作系统分区位置及数量（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-24 |
| **安全基线项说明** | 检查系统是否安装在磁盘的第一个逻辑分区，至少建立两个或以上磁盘分区，通过分区来保护服务器的业务安全和系统运行稳定。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  检查服务器应磁盘分区数量，检查系统是否安装在磁盘的第一个逻辑分区，直接进入第一个逻辑分区查看系统文件。 |
| **检查方法** | 参考安全配置方法。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a) 应启用访问控制功能，依据安全策略控制用户对资源的访问； |
| **备注** |  |

* + 1. 设置授权用户本地登录

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置授权用户本地登录（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-25 |
| **安全基线项说明** | 本地安全设置中配置：“指定授权用户”允许“本地登录此计算机” |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”“从本地登陆此计算机”设置为“指定授权用户”。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->本地安全策略”，在“本地策略->用户权限分配”：  设置“允许本地登录”的用户或组。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a）应启用访问控制功能，依据安全策略控制用户对资源的访问。 |
| **备注** |  |

* + 1. 禁用Ctrl + Alt + Del

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 禁用Ctrl + Alt + Del（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-26 |
| **安全基线项说明** | 该安全设置确定用户是否需要按 Ctrl+Alt+Del 才能登录。  如果在计算机上启用此策略，则用户无需按 Ctrl+Alt+Del 便可登录。不必按 Ctrl+Alt+Del 会使用户易于受到企图截获用户密码的攻击。用户登录之前需按 Ctrl+Alt+Del 可确保用户输入其密码时通过信任的路径进行通信。  如果禁用此策略，则任何用户登录 Windows 之前都需要按 Ctrl+Alt+Del。  域计算机上的默认设置: 已启用: 至少 Windows 8/已禁用: Windows 7 或早期版本。独立计算机上的默认设置: 已启用。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入控制面板->管理工具->本地安全策略->安全选项->禁用“不需要按 ctrl + alt + del”  或“”计算机配置“windows设置”“安全设置”“本地策略”“安全选项”找到“不需要按Ctrl + Alt + Del”，然后在这个选项上双击鼠标左键弹出对话框，选择“已禁用”，然后点击该对话框下面的“确认”按钮结束配置。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a) 应启用访问控制功能，依据安全策略控制用户对资源的访问 |
| **备注** |  |

* + 1. 设置域验证解锁

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置域验证解锁（按需实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-27 |
| **安全基线项说明** | 在域控制器内，启用要求域控制器身份验证以解锁工作站 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入控制面板->管理工具->本地安全策略->安全选项->启用要求域控制器身份验证以解锁工作站 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a) 应启用访问控制功能，依据安全策略控制用户对资源的访问 |
| **备注** | 不是域控服务器或域成员不检查此项。 |

* + 1. 配置指定可以远程访问的用户（组）

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置指定可以远程访问的用户（组）（按需实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-28 |
| **安全基线项说明** | 组策略只允许授权帐号可以远程访问本地计算机。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  打开命令提示符，运行命令“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\用户权限分配(用户权利指派)”，在右边窗格中找到“从网络访问此计算机”，配置为指定授权用户或组。 |
| **检查方法** | 参考安全配置方法；  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.2 主机：访问控制（S3），a) 应启用访问控制功能，依据安全策略控制用户对资源的访问 |
| **备注** |  |

* 1. 安全审计
     1. 配置登录日志审核

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置登录日志审核（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-29 |
| **安全基线项说明** | 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。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  开始->运行->执行“控制面板->管理工具->本地安全策略->审核策略”  审核登录事件。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->本地安全策略->本地策略🡪审核策略”  审核登录事件，双击，设置为成功和失败都审核。 |
| **检查方法** | 参考安全配置方法, 审核登录事件设置为成功和失败都审核。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.3 主机：安全审计（G3），a）审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。 |
| **备注** |  |

* + 1. 设置系统日志完备性性

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置系统日志完备性（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-30 |
| **安全基线项说明** | 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。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  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”中，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”。需要配置的策略：   * 审核策略更改； * 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； |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.3 主机：安全审计（G3），a）审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。  7.1.3.3 主机：安全审计（G3），b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动等系统内重要的安全相关事件。 |
| **备注** |  |

* + 1. 配置使用NTP

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置使用NTP（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-31 |
| **安全基线项说明** | NTP为网络时间协议，windows可设置并开启windows time服务（设置为自动）来进行操作系统时间同步，便于确定出现问题后的时间。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  配置方法：控制面板->管理工具->服务->开启时间服务 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.3 主机：安全审计（G3），c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等，并定期备份审计记录，涉及敏感数据的记录保存时间不少于半年； |
| **备注** |  |

* + 1. 配置日志文件容量

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置日志文件容量（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-32 |
| **安全基线项说明** | 设置应用日志文件大小至少为16384KB，设置当达到最大的日志尺寸时，按需要改写事件。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 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：  查看“应用日志”“系统日志”“安全日志”属性中的日志大小 ,以及设置当达到最大的日志尺寸时的相应策略。  **版本：Windows Server 2008、Windows Server 2012**  进入“控制面板->管理工具->事件查看器”，在“事件查看器（本地）”中：  各日志属性中的日志大小设置不小于“16384KB” ,设置当达到最大的日志尺寸时，“按需要改写事件”。 |
| **检查方法** | 参考安全配置方法，“应用日志”“系统日志”“安全日志”属性中的日志大小设置不小于“16384KB” ,设置当达到最大的日志尺寸时，“按需要改写事件”。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.3 主机：安全审计（G3），c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。  7.1.3.3 主机：安全审计（G3），d）应能够根据记录数据进行分析，并生成审计报表。  7.1.3.3 主机：安全审计（G3），e）应保护审计进程，避免受到未预期的中断。 |
| **备注** |  |

* 1. 入侵防范
     1. 配置补丁管理

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置补丁管理（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-33 |
| **安全基线项说明** | 应安装最新的Service Pack补丁集和Hotfix补丁。对服务器系统应先进行兼容性测试。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  安装最新的Service Pack补丁集。  Windows Server 2000的Service Pack为SP4  Windows Server2003的Service Pack为SP2  Windows Server2008 R2的Service Pack为SP2  Windows Server2012 R2尚无  控制面板->添加或删除程序->显示更新打钩，查看最近安装的Hotfix补丁是否为微软最新发布。 |
| **检查方法** | 参照漏洞扫描结果，服务器是否存在高危风险漏洞。也可以运行微软自动扫描工具MBSA (支持群组扫描)。 |
| **依据** | 7.1.3.5 主机：入侵防范（G3），c) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器、系统软件预防性维护服务等方式保持系统补丁及时得到更新; |
| **备注** |  |

* + 1. 禁用不需要的服务

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 禁用不需要的服务（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-34 |
| **安全基线项说明** | 列出所需要服务的列表(包括所需的系统服务)，通过与系统管理员确认无异常服务存在。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  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，输出所有服务列表，查看是否有异常服务。  通常可被禁止的服务有：   * Alert * Application Layer Gateway Service * Error Reporting Service * Help and Suppor * NetMeeting Remote Desktop Sharing, * Portable Media Serial Number, * Print Spooler * Remote Desktop Help Session Manager * Server * Shell Hardware Detection * Telnet * WebClient * Wireless Zero Configuration * WMI Performance Adapter   \*上述服务为推荐的服务，请依照自身需求进行选择（禁用）。 |
| **检查方法** | 依照配置方法进入“服务和应用程序”菜单，  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.5 主机：入侵防范（G3），c) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器、系统软件预防性维护服务等方式保持系统补丁及时得到更新; |
| **备注** |  |

* 1. 恶意代码防范
     1. 设置防病毒管理

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置防病毒管理（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-35 |
| **安全基线项说明** | 安装防病毒软件，并及时更新。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  安装防病毒软件，并及时更新。 |
| **检查方法** | 检查是否安装主流杀软，病毒库为最新。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.6 主机：恶意代码防范（G3），a）应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。 |
| **备注** |  |

* 1. 资源控制
     1. 设置屏保密码保护

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置屏保密码保护（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-36 |
| **安全基线项说明** | 设置带密码的屏幕保护，并将时间设定为5分钟。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  进入“控制面板－>显示－>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“在恢复时使用密码保护”。  **版本：Windows Server 2008、Windows Server 2012**  进入“控制面板－>外观🡪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“在恢复时使用密码保护”。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.7 主机：资源控制（G3），b) 应根据安全策略设置登录终端的操作超时锁定。 |
| **备注** |  |

* + 1. 设置远程登录超时

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置远程登录超时（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-37 |
| **安全基线项说明** | 检查设置：对于远程登录的帐号，设置不活动断连时间15分钟 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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](http://www.newasp.cn/)服务器”设置为“在挂起会话之前所需的空闲时间”为15分钟。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->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：暂停会话前所需的空闲时间量”设置为“15分钟”。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.7 主机：资源控制（G3），b) 应根据安全策略设置登录终端的操作超时锁定。 |
| **备注** |  |

* + 1. 设置登录超时

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置登录超时（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-38 |
| **安全基线项说明** | 启用超过登录时间后强制注销 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入控制面板->管理工具->本地安全策略->安全选项->启用超过登录时间后强制注销 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.7 主机：资源控制（G3），b) 应根据安全策略设置登录终端的操作超时锁定。 |
| **备注** |  |

* 1. 其它安全项
     1. 禁止显示上次的用户名

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 禁止显示上次登录的用户名（必须实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-39 |
| **安全基线项说明** | 在服务器启动时，不显示上次登录的用户名，防止信息泄露 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”：启用“不显示上次登录用户名”。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->本地安全设置”，进入“本地策略->安全选项”：  将“交互式登录: 不显示最后的用户名”配置为“已启用”。 |
| **检查方法** | 参考安全配置方法，启用“不显示上次登录用户名”。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.4 主机：剩余信息保护（G3），a）应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他使用人员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。 |
| **备注** |  |

* + 1. 配置清除虚拟内存页面文件

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 配置清除虚拟内存页面文件（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-40 |
| **安全基线项说明** | 关闭服务器前，应清除虚拟内存页面，一保护暂存在在缓存中的数据。 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  **版本：Windows Server 2000、Windows Server 2003**  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”：选中“关机前清除虚拟内存页面”。  **版本：Windows Server 2008、Windows Server 2012**  进入“开始->管理工具->本地安全设置”，进入“本地策略->安全选项”：  将“关机：清除虚拟内存页面文件”配置为“已启用”。 |
| **检查方法** | 参考安全配置方法。  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.4 主机：剩余信息保护（G3），a）应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他使用人员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。 |
| **备注** |  |

* + 1. 设置前次登录缓存数量

|  |  |
| --- | --- |
| **安全基线**  **项目名称** | 设置前次登录缓存数量（建议实施） |
| **安全基线**  **编号** | 操作系统-WINDOWS-41 |
| **安全基线项说明** | 设置可被缓存的前次登录个数为5 |
| **配置方法** | **登录系统，以管理员权限进行如下操作：**  进入控制面板->管理工具->本地安全策略->安全选项->交互式登录：设置可被缓存的前次登录个数为5 |
| **检查方法** | 参考安全配置方法  如果是则符合，否则不符合。 |
| **依据** | 7.1.3.4 主机：剩余信息保护（G3），b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他使用人员前得到完全清除。 |
| **备注** |  |

1. 评审与修订

本标准由老男孩定期进行审查，根据审视结果修订标准，并颁发执行。