|  |
| --- |
| **老男孩信息系统安全配置基线**  **MS-SQLServer数据库分册（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 4](#_Toc408341502)  [1.1 适用范围 4](#_Toc408341503)  [1.2 规范依据 4](#_Toc408341504)  [1.3 实施策略 4](#_Toc408341505)  [二. 安全配置基线标准 5](#_Toc408341506)  [2.1 身份鉴别 5](#_Toc408341507)  [2.1.1 删除不必要账户 5](#_Toc408341508)  [2.1.2 设置密码并保证复杂度 6](#_Toc408341509)  [2.1.3 禁用共享账户 7](#_Toc408341510)  [2.1.4 设置认证失败锁定策略 8](#_Toc408341511)  [2.2 访问控制 9](#_Toc408341512)  [2.2.1 配置数据库启动账户安全 9](#_Toc408341513)  [2.2.2 设置用户权限最小化 10](#_Toc408341514)  [2.2.3 限制数据库验证方式 11](#_Toc408341515)  [2.2.4 限制登录IP 12](#_Toc408341516)  [2.3 安全审计 13](#_Toc408341517)  [2.3.1 配置数据库审计 13](#_Toc408341518)  [三. 其它安全项 15](#_Toc408341519)  [3.1.1 配置安装最小化 15](#_Toc408341520)  [3.1.2 设置通讯传输加密 17](#_Toc408341521)  [3.1.3 更新数据库补丁 18](#_Toc408341522)  [四. 评审与修订 19](#_Toc408341523) |

# 概述

## 适用范围

本配置基线适用于老男孩的MS-SQLServer数据库，主要涉及MS-SQLServer数据库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MS-SQLServer数据库。

## 规范依据

根据老男孩目前MS-SQLServer数据库的安全现状，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）

## 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 | 删除不必要账户 | 必须实施 |
| 2 | 身份鉴别 | 设置密码并保证复杂度 | 必须实施 |
| 3 | 身份鉴别 | 禁用共享账户 | 必须实施 |
| 4 | 身份鉴别 | 设置认证失败锁定策略 | 必须实施 |
| 5 | 访问控制 | 配置数据库启动账户安全 | 必须实施 |
| 6 | 访问控制 | 设置用户权限最小化 | 必须实施 |
| 7 | 访问控制 | 限制数据库验证方式 | 必须实施 |
| 8 | 访问控制 | 限制登录IP | 建议实施 |
| 9 | 安全审计 | 配置数据库审计 | 按需实施 |
| 10 | 其它要求项 | 配置安装最小化 | 必须实施 |
| 11 | 其它要求项 | 设置通讯传输加密 | 按需实施 |
| 12 | 其它要求项 | 更新数据库补丁 | 按需实施 |

# 安全配置基线标准

## 身份鉴别

### 删除不必要账户

|  |  |
| --- | --- |
| **安全基线项目名称** | 删除不必要账户（必须实施） |
| **安全基线编号** | 数据库-MS-SQLServer-1 |
| **安全基线项说明** | 应删除或锁定与数据库运行、维护等工作无关的账户。 |
| **配置方法** | SQL SERVER企业管理器-〉安全性-〉登陆中删除无关账户；  SQL SERVER企业管理器-〉数据库-〉对应数据库-〉用户中删除无关账户；      最后和管理员（数据库、应用管理员）沟通确认哪些为无关删号。 |
| **检查方法** | 可参考配置方法中（操作步骤）的截图，和管理员（数据库、应用管理员）沟通确认无关删号是否存在。 |
| **依据** | 6.2.1.4 应用安全：身份鉴别（S3）：c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用； |
| **备注** | 需要手工判断，实际情况应与具体需求为准，谨慎操作。 |

### 设置密码并保证复杂度

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置密码并保证复杂度（必须实施） |
| **安全基线编号** | 数据库-MS-SQLServer-2 |
| **安全基线项说明** | 对于采用静态口令进行认证的数据库，口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类。  且5次以内不得设置相同的口令。密码应至少每90天进行更换。 |
| **配置方法** | （1）强制启用密码策略并强制密码过期：  登录企业管理器  1) 展开“安全性”\“登录名”条目，双击弱密码账户  2) 确保勾选“强制实施密码策略”和“强制密码过期”    （2）修改空口令或弱口令：  登录企业管理器  1) 展开“安全性”\“登录名”条目，双击弱密码账户。  2) 修改账户弱密码为包含英文大小写、数字、特殊字符的复杂密码。 |
| **检查方法** | 1.检查sa是否为空口令或弱口令并实际登录测试。  2.采取问询的方式询问数据库管理员是否配置满足要求的密码（口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类  ）。 |
| **依据** | 6.2.1.4 应用安全：身份鉴别（S3）：g) 对于系统自动分配或者预设的强度较弱的初始密码，系统应强制用户首次登录时修改初始密码； |
| **备注** |  |

### 禁用共享账户

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁用共享账户（必须实施） |
| **安全基线编号** | 数据库-MS-SQLServer-3 |
| **安全基线项说明** | 数据库应按照用户分配账户，避免不同用户间共享账户。  共享账户带来管理和操作记录无法对应到各个用户使用者，以造成审计和记录不便，存在安全风险。 |
| **配置方法** | 1. 参考配置操作   sp\_addlogin 'user\_name\_1','password1'  sp\_addlogin 'user\_name\_2','password2'  或在企业管理器中直接添加远程登陆用户  建立角色，并给角色授权，把角色赋给不同的用户或修改用户属性中的角色和权限。   1. 检测方法：   在查询分析器中用user\_name\_1/password1连接数据库成功。   1. 补充操作说明   user\_name\_1和user\_name\_1是两个不同的帐号名称，可根据不同用户，取不同的名称。 |
| **检查方法** | 在查询分析器中用user\_name\_1/password1连接数据库成功。  此项检查可以采取问询的方式，然后登录到数据库用户界面后进行查证。 |
| **依据** | 6.2.1.4 应用安全：身份鉴别（S3）：c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用； |
| **备注** |  |

### 设置认证失败锁定策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置认证失败锁定策略（必须实施） |
| **安全基线编号** | 数据库-MS-SQLServer-4 |
| **安全基线项说明** | 对于采用静态口令认证技术的数据库，应配置当用户连续认证失败次数超过10次，锁定该用户使用的帐号（锁定时间不低于3分钟）。 |
| **配置方法** | 强制启用密码策略：  登录企业管理器  1) 展开“安全性”\“登录名”条目，双击账户  2) 确保勾选“强制实施密码策略” |
| **检查方法** | 查看账户锁定策略设置是否符合要求。参照配置方法截图检查是否勾选了“强制实施密码策略”选项。 |
| **依据** | 6.2.1.4 应用安全：身份鉴别（S3）：d) 应提供登录失败处理功能，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** | 根据应用场景的不同，如部署场景需开启此功能，则强制要求此项。对核心库、生产用户不能设置此基线。误操作或恶意超过10次，导致用户锁定，有一定风险，可能会导致应用异常。 |

## 访问控制

### 配置数据库启动账户安全

|  |  |
| --- | --- |
| **安全基线项目名称** | 数据库启动账户安全（必须实施） |
| **安全基线编号** | 数据库-MS-SQLServer-5 |
| **安全基线项说明** | 使用普通账户启动SQLServer服务，防范攻击者获取系统账户或管理员权限。 |
| **配置方法** | 新建SQL Server服务账户，建议将其从User组中删除，且不要把该账户提升为Administrators组的成员，以所需最小权限启动 SQL Server服务：  说明: http://img1.51cto.com/attachment/201007/234052473.png  在属性界面中选择新建的普通账户启动服务。 |
| **检查方法** | 以SQL SERVER2005为例，通过“SQL Server configuration manager”查看，如下所示，SQL Server服务的登陆身份为Local System：    检查结果如上图所示则满足该检查项。 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系； |
| **备注** |  |

### 设置用户权限最小化

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置用户权限最小化（必须实施） |
| **安全基线编号** | 数据库-MS-SQLServer-6 |
| **安全基线项说明** | 应根据实际业务需要，配置用户的最小权限。 |
| **配置方法** | 更改数据库属性，取消业务数据库账户不需要的服务器角色；  更改数据库属性，取消业务数据库账户不需要的“数据库访问许可”和“数据库角色中允许”中不需要的角色。 |
| **检查方法** | 查看数据库属性中业务数据库账户是否有不需要的服务器角色。  查看数据库属性中业务数据库账户是否有不需要的“数据库访问许可”和“数据库角色中允许”中不需要的角色。 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系； |
| **备注** |  |

### 限制数据库验证方式

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置数据库验证方式（必须实施） |
| **安全基线编号** | 数据库-MS-SQLServer-7 |
| **安全基线项说明** | 不允许使用操作系统管理员远程或本地登录数据库。 |
| **配置方法** | 打开SQL Server企业管理器，点击数据库属性页面的“安全性”选项卡，如下图所示： |
| **检查方法** | 打开SQL Server企业管理器，点击数据库属性页面的“安全性”选项卡，查看身份验证方式是否为“SQL Server和Windows”，若是则满足此项要求。 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系； |
| **备注** |  |

### 限制登录IP

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制登录IP（建议实施） |
| **安全基线编号** | 数据库-MS-SQLServer-8 |
| **安全基线项说明** | 通过数据库所在操作系统或防火墙限制，只有信任的IP 地址才能通过监听器访问数据库。 |
| **配置方法** | 在防火墙中做限制，只允许与指定的 IP 地址建立1433 的通讯。当然，  从更为安全的角度来考虑，应该把1433 端口改成其他的端口。  1. 在“Windows 防火墙”对话框中，单击“例外”选项卡。  2. 单击“添加端口”。  3. 键入您要允许的端口名称，键入端口号，然后单击“TCP”或“UDP”  以提示这是 TCP 还是 UDP 端口。  4. 单击“更改范围”。  5. 指定要为其阻止此端口的一系列计算机，然后单击“确定”。 |
| **检查方法** | 无关IP不允许连接1433端口。  检查系统防火墙（ACL）配置。 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作； |
| **备注** | 根据应用场景的不同，如部署场景需开启此功能，则强制要求此项。 |

## 安全审计

### 配置数据库审计

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置数据库审计（按需实施） |
| **安全基线编号** | 数据库-MS-SQLServer-9 |
| **安全基线项说明** | 根据业务要求制定数据库审计策略。  对用户登录进行记录，记录内容包括用户登录使用的帐号、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；  用户对数据库的操作，包括但不限于以下内容：帐号创建、删除和权限修改、口令修改、读取和修改数据库配置、读取和修改业务用户的话费数据、身份数据、涉及通信隐私数据。记录需要包含用户帐号，操作时间，操作内容以及操作结果；  记录对与数据库相关的安全事件。 |
| **配置方法** | （1）打开“Microsoft SQL Server Management Studio”；  （2）右键点击服务器，在右键菜单中点击“属性”；  （3）点击选择页下的“安全性”，更改审核设置，将登陆审核设置为“失败和成功的登录”，勾选“启用C2审核跟踪”前的复选框。 |
| **检查方法** | （1）打开“Microsoft SQL Server Management Studio”。  （2）右键点击服务器，在右键菜单中点击“属性”。  （3）点击选择页下的“安全性”，查看审核设置。 |
| **依据** | 6.2.1.4 应用安全：安全审计（G3）：a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计； |
| **备注** | 数据库审计策略开启后，有可能导致磁盘I/O较高，请根据实际要求、性能开启。 |

# 其它安全项

### 配置安装最小化

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置安装最小化（必须实施） |
| **安全基线编号** | 数据库-MS-SQLServer-10 |
| **安全基线项说明** | 停用不必要的存储过程 |
| **配置方法** | 禁用xp\_cmdshell扩展存储过程，使用：  use master  sp\_dropextendedproc 'xp\_cmdshell'  依据以上操作，禁用以下不需要的扩展存储过程：  Sp\_OACreate  Sp\_OADestroy  Sp\_OAGetErrorInfo  Sp\_OAGetProperty  Sp\_OAMethod  Sp\_OASetProperty  Sp\_OAStop  Xp\_regaddmultistring  Xp\_regdeletekey  Xp\_regdeletevalue  Xp\_regenumvalues  Xp\_regremovemultistring  xp\_sdidebug  xp\_availablemedia  xp\_cmdshell  xp\_deletemail  xp\_dirtree  xp\_dropwebtask  xp\_dsninfo  xp\_enumdsn  xp\_enumerrorlogs  xp\_enumgroups  xp\_enumqueuedtasks  xp\_eventlog  xp\_findnextmsg  xp\_fixeddrives  xp\_getfiledetails  xp\_getnetname  xp\_grantlogin  xp\_logevent  xp\_loginconfig  xp\_logininfo  xp\_makewebtask  xp\_msverxp\_perfend  xp\_perfmonitor  xp\_perfsample  xp\_perfstart  xp\_readerrorlog  xp\_readmail  xp\_revokelogin  xp\_runwebtask  xp\_schedulersignal  xp\_sendmail  xp\_servicecontrol  xp\_snmp\_getstate  xp\_snmp\_raisetrap  xp\_sprintf  xp\_sqlinventory  xp\_sqlregister  xp\_sqltrace  xp\_sscanf  xp\_startmail  xp\_stopmail  xp\_subdirs  xp\_unc\_to\_drive  xp\_dirtree |
| **检查方法** | 以sa身份登录查询分析器，执行以下命令：  exec master..xp\_cmdShell 'dir c:\'  输出结果应已禁用xp\_cmdshell，如下所示：    如果未禁用xp\_cmdshell则会返回dir c:\的执行结果。 |
| **依据** |  |
| **备注** | 实际情况请以具体需求为准。 |

### 设置通讯传输加密

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置通讯传输加密（按需实施） |
| **安全基线编号** | 数据库-MS-SQLServer-11 |
| **安全基线项说明** | 使用通讯协议加密。 |
| **配置方法** | 1.参考配置操作  sqlserver 2000：启动服务器网络配置工具，在“常规”中选择“强制协议加密”；    SQLServer 2005：启动SQL Server 2005 Configuration Manager，打开SQL Server 2005网络配置，右键MSSSQLSERVER的协议，查看属性，在标志栏里面将FourceEncryption设置为是；    补充操作说明  更改通讯协议加密后需要重新启动SQL Server数据库。 |
| **检查方法** | 启动服务器网络配置工具，在“常规”中查看是否选择“强制协议加密”。 |
| **依据** | 6.2.1.4 应用安全：通信保密性（S3）：b) 对于通过互联网对外提供服务的系统，在通信过程中的整个报文或会话过程，应通过专用的通信协议或加密的方式保证通信过程的机密性。 |
| **备注** | 根据应用场景的不同，如部署场景需开启此功能，则强制要求此项。 |

### 更新数据库补丁

|  |  |
| --- | --- |
| **安全基线项目名称** | 更新数据库补丁（按需实施） |
| **安全基线编号** | 数据库-MS-SQLServer-12 |
| **安全基线项说明** | 由于不定期厂商会对存在的漏洞发布补丁进行修复，需要及时关注厂商发布漏洞补丁情况来进行修复和升级操作。 |
| **配置方法** | **参考配置操作：**  检查当前所有已安装的数据库产品的版本信息，运行SQL查询分析器，执行：  select @@version  安装补丁详细操作请参照其中的readme文件。 |
| **检查方法** | 根据返回结果判断，是否需要安装补丁。  返回结果说明举例：  2005.90.1399 －——————SQL Server 2005 RTM  2005.90.2047 －——————SQL Server 2005 Service Pack 1  2005.90.3042 －——————SQL Server 2005 Service Pack 2 |
| **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等方式保持系统补丁及时得到更新。 |
| **备注** | 根据实际要求更新。 |

# 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。