|  |
| --- |
| **老男孩信息系统安全配置基线**  **Oracle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](#_Toc408327539)  [1.1适用范围 4](#_Toc408327540)  [1.2规范依据 4](#_Toc408327541)  [1.3实施策略 4](#_Toc408327542)  [二. 安全配置基线标准 5](#_Toc408327543)  [2.1身份鉴别 5](#_Toc408327544)  [2.1.1删除不必要账户 5](#_Toc408327545)  [2.1.2设置并保证密码复杂度 6](#_Toc408327546)  [2.1.3禁用共享账户 7](#_Toc408327547)  [2.1.4更改默认账户密码 8](#_Toc408327548)  [2.1.5设置认证失败策略 8](#_Toc408327549)  [2.1.6配置重复口令使用次数 9](#_Toc408327550)  [2.1.7设置账户口令的生存期 10](#_Toc408327551)  [2.1.8配置密码变更宽限期 10](#_Toc408327552)  [2.2访问控制 11](#_Toc408327553)  [2.2.1设置监听器启停密码 11](#_Toc408327554)  [2.2.2权限分离 11](#_Toc408327555)  [2.2.3限制账户权限 12](#_Toc408327556)  [2.2.4限制TNS登录IP 14](#_Toc408327557)  [2.2.5限制DBA账户远程登录 15](#_Toc408327558)  [2.2.6配置数据字典访问权限 16](#_Toc408327559)  [2.3安全审计 17](#_Toc408327560)  [2.3.1配置数据库审计 17](#_Toc408327561)  [2.4资源控制 18](#_Toc408327562)  [2.4.1设置连接超时锁定策略 18](#_Toc408327563)  [2.5其它安全项 19](#_Toc408327564)  [2.5.1配置安装最小化 19](#_Toc408327565)  [2.5.2设置通讯传输加密 19](#_Toc408327566)  [2.5.3更新数据库补丁 20](#_Toc408327567)  [三. 评审与修订 20](#_Toc408327568) |

1. 概述
   1. 适用范围

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

* 1. 规范依据

根据老男孩目前Oracle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）
  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 | 删除不必要帐号 | 必须实施 |
| 2 | 身份鉴别 | 设置并保证密码复杂度 | 必须实施 |
| 3 | 身份鉴别 | 禁用共享账号 | 必须实施 |
| 4 | 身份鉴别 | 更改默认帐号密码 | 必须实施 |
| 5 | 身份鉴别 | 设置认证失败策略 | 必须实施 |
| 6 | 身份鉴别 | 配置重复口令使用次数 | 建议实施 |
| 7 | 身份鉴别 | 设置帐号口令的生存期 | 建议实施 |
| 8 | 身份鉴别 | 配置密码变更宽限期 | 建议实施 |
| 9 | 访问控制 | 设置监听器启停密码 | 必须实施 |
| 10 | 访问控制 | 权限分离 | 必须实施 |
| 11 | 访问控制 | 限制账户权限 | 必须实施 |
| 12 | 访问控制 | 限制TNS登录IP | 建议实施 |
| 13 | 访问控制 | 限制DBA账户远程登录 | 建议实施 |
| 14 | 访问控制 | 配置数据字典访问权限 | 建议实施 |
| 15 | 安全审计 | 配置数据库审计 | 按需实施 |
| 16 | 资源控制 | 设置连接超时锁定策略 | 必须实施 |
| 17 | 其它安全项 | 配置安装最小化 | 建议实施 |
| 18 | 其它安全项 | 设置通讯传输加密 | 按需实施 |
| 19 | 其它安全项 | 更新数据库补丁 | 按需实施 |

1. 安全配置基线标准
   1. 身份鉴别
      1. 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-Oracle-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** | 首先锁定不需要的用户  在经过一段时间后，确认该用户对业务确无影响的情况下，可以删除。   1. **参考配置操作**   sqlplus "/ as sysdba"  alter user username account lock;锁定用户  首先锁定不需要的用户，在经过一段时间后，确认该用户对业务确无影响的情况下，可以删除。  如果锁定某用户后对业务造成影响，使用以下命令进行账户解锁：  SQL> alter user username account unlock;   1. **补充操作说明**   Oracle默认开启sys,system,dbsnmp,sysman,mgmt\_view账户，若不需要上述账户，可由数据库管理员禁用。 |
| **检查方法** | 结合要求和实际业务情况判断符合要求，删除或锁定与设备运行、维护等与工作无关的账户。  以下操作需sys权限账户登录  使用sqlplus "/ as sysdba"  SQL> select username,account\_status from dba\_users;命令查看是否存在多余未锁定账户 |
| **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。 |

* + 1. 设置并保证密码复杂度

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置并保证密码复杂度（必须实施） |
| **安全基线编号** | 数据库-Oracle-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。 |
| **配置方法** | 1. 以Oracle用户登录到系统中。  2. 以sqlplus‘/as sysdba’登录到sqlplus环境中。  3、执行select limit from dba\_profiles where  resource\_name='PASSWORD\_VERIFY\_FUNCTION' and profile in (select profile from dba\_users where account\_status='OPEN'  为用户建profile，调整PASSWORD\_VERIFY\_FUNCTION，指定密码复杂度 |
| **检查方法** | 参考配置方法 |
| **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** |  |

* + 1. 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-Oracle-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** | 以下操作需sys权限账户登录   1. **参考配置操作**   新建不同用户参考操作：  sqlplus "/ as sysdba"  create user abc1 identified by password1;  create user abc2 identified by password2;  建立role，并给role授权，把role赋给不同的用户。   1. **补充操作说明**   *abc1*和*abc2*是两个不同的账户名称，可根据不同用户，取不同的名称； |
| **检查方法** | 以下操作需sys权限账户登录  sqlplus "/ as sysdba"  SQL>select username from dba\_users where account\_status='OPEN';输出当前数据库所有用户，根据实际情况删除共享账户。 |
| **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** |  |

* + 1. 更改默认账户密码

|  |  |
| --- | --- |
| **安全基线项目名称** | 更改默认账户密码（必须实施） |
| **安全基线编号** | 数据库-Oracle-4 |
| **安全基线项说明** | 更改数据库默认账户的密码。 |
| **配置方法** | 在以SYSDBA身份登陆时可以修改其他用户的密码，比如：  SQL> alter user user01 identified by user10; //这个是把USER01用户密码修改为USER10  使用上述命令修改下面的Oracle数据库默认账户密码：  system/system、system/manager 、sys/sys、sys/cHAnge\_on\_install、scott/scott、scott/tiger、dbsnmp/dbsnmp、rman/rman、xdb/xdb |
| **检查方法** | 1. 以Oracle用户登录到系统中。  2. 以system/system、system/manager 、sys/sys、sys/cHAnge\_on\_install、scott/scott、scott/tiger、dbsnmp/dbsnmp、rman/rman、xdb/xdb登录sqlplus环境。若登录成功说明使用默认密码需修改。 |
| **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** |  |

* + 1. 设置认证失败策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置认证失败策略（必须实施） |
| **安全基线编号** | 数据库-Oracle-5 |
| **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，锁定该用户使用的账户。 |
| **配置方法** | 1. 以Oracle用户登录到系统中。  2. 以sqlplus‘/as sysdba’登录到sqlplus环境中。  3. 执行select resource\_name, limit from dba\_profiles, dba\_users where dba\_profiles.profile = dba\_users.profile and dba\_users.account\_status='OPEN' and resource\_name='FAILED\_LOGIN\_ATTEMPTS';  需要查询结果中FAILED\_LOGIN\_ATTEMPTS参数值等于10  若不为10则执行没下面的语句进行配置：  ALTER PROFILE DEFAULT LIMIT FAILED\_LOGIN\_ATTEMPTS 10; |
| **检查方法** | 参考配置方法中的第3项给出的查询语句，在返回的查询结果中：  FAILED\_LOGIN\_ATTEMPTS等于10（或根据实际情况定义的其它值）则满足要求。 |
| **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 |

* + 1. 配置重复口令使用次数

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置重复口令使用次数（建议实施） |
| **安全基线编号** | 数据库-Oracle-6 |
| **安全基线项说明** | 对于采用静态口令认证技术的数据库，应配置数据库，使用户不能重复使用最近5次（含5次）内已使用的口令。 |
| **配置方法** | 1. 以Oracle用户登录到系统中。  2. 以sqlplus‘/as sysdba’登录到sqlplus环境中。  3. 执行select resource\_name, limit from dba\_profiles, dba\_users where dba\_profiles.profile = dba\_users  .profile and dba\_users.account\_status='OPEN' and resource\_name='PASSWORD\_REUSE\_MAX';  PASSWORD\_REUSE\_MAX的值应大于等于5。  若不满足则执行下面的语句进行配置：   alter profile profile1 limit  password\_reuse\_max 5; |
| **检查方法** | 参考配置方法中第3项给出的查询语句，查询结果中PASSWORD\_REUSE\_MAX大于等于5。 |
| **依据** | 6.2.1.4 应用安全：身份鉴别（S3）：h) 修改密码时，不允许新设定的密码与旧密码相同。 |
| **备注** |  |

* + 1. 设置账户口令的生存期

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置账户口令的生存期（建议实施） |
| **安全基线编号** | 数据库-Oracle-7 |
| **安全基线项说明** | 对于采用静态口令认证技术的数据库，账户口令的生存期（使用时间）不长于90天。 |
| **配置方法** | 1. 以Oracle用户登录到系统中。  2. 以sqlplus‘/as sysdba’登录到sqlplus环境中。  3、执行select limit from dba\_profiles where  resource\_name='PASSWORD\_LIFE\_TIME' and profile in (select profile from dba\_users where account\_status='OPEN'  PASSWORD\_LIFE\_TIME的值应小于等于90。  若不满足则执行下面的语句进行配置：  ALTER PROFILE DEFAULT LIMIT PASSWORD\_LIFE\_TIME 90; |
| **检查方法** | 参考配置方法中第3项给出的查询语句，查询结果中PASSWORD\_LIFE\_TIME小于等于90才满足要求。 |
| **依据** |  |
| **备注** | **数据库口令有效期更改可能给运维工作增加一定负担。** |

* + 1. 配置密码变更宽限期

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置密码变更宽限期（建议实施） |
| **安全基线编号** | 数据库-Oracle-8 |
| **安全基线项说明** | 配置账户密码更改所宽限的时间（单位：天）。 |
| **配置方法** | 1. 以Oracle用户登录到系统中。  2. 以sqlplus‘/as sysdba’登录到sqlplus环境中。  3. 执行select resource\_name, limit from dba\_profiles, dba\_users where dba\_profiles.profile = dba\_users  .profile and dba\_users.account\_status='OPEN' and resource\_name='PASSWORD\_GRACE\_TIME'  设置PASSWORD\_GRACE\_TIME小于等于7。  若不满足则执行下面的语句配置：  ALTER PROFILE DEFAULT LIMITPASSWORD\_GRACE\_TIME 7; |
| **检查方法** | 参考配置方法中第3项给出的查询语句，查询结果中PASSWORD\_GRACE\_TIME小于等于7。 |
| **依据** |  |
| **备注** | 密码过期后7天内不修改密码，密码将失效 |

* 1. 访问控制
     1. 设置监听器启停密码

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置监听器启停密码（必须实施） |
| **安全基线编号** | 数据库-Oracle-9 |
| **安全基线项说明** | 为数据库监听器（LISTENER）的关闭和启动设置密码。 |
| **配置方法** | 检查$ORACLE\_HOME/network/admin/listener.ora文件中是否设置参数PASSWORDS\_LISTENER。 |
| **检查方法** | 要求正确设置参数PASSWORDS\_LISTENER；  使用lsnrctl start或lsnrctl stop命令起停listener需要密码。 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问； |
| **备注** |  |

* + 1. 权限分离

|  |  |
| --- | --- |
| **安全基线项目名称** | 权限分离（必须实施） |
| **安全基线编号** | 数据库-Oracle-10 |
| **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** | 以下操作需sys权限账户登录  sqlplus "/ as sysdba"  （1）禁止Oracle 远程操作系统认证：  SQL> alter system set remote\_os\_authent=false scope=spfile;  关闭，重新启动数据库  SQL>shutdown  SQL>startup  （2）修改sqlnet.ora，修改为  SQLNET.AUTHENTICATION\_SERVICES=(NONE)，  用户以后连接数据库需要输入用户名和密码。 |
| **检查方法** | 以下操作需sys权限账户登录  （1）检查Oracle 远程操作系统认证：  以Oracle用户身份执行如下命令：  SQL>show parameter remote\_os\_authent;  （2）检查Oracle本地操作系统认证：  打开%ORACLE\_HOME%\network\admin\sqlnet.ora，检查是否有以下行SQLNET.AUTHENTICATION\_SERVICES= (NTS) |
| **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** |  |

* + 1. 限制账户权限

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制账户权限（必须实施） |
| **安全基线编号** | 数据库-Oracle-11 |
| **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。  （1）检查各用户权限是否能满足业务需要且没有除业务需要以外的任何权限；  （2）仅保留必要的包的PUBLIC角色执行权限；  （3）通过设置下面初始化参数来限制只有SYSDBA权限的用户才能访问数据字典：  O7\_DICTIONARY\_ACCESSIBILITY = FALSE |
| **配置方法** | 以下操作需sys权限账户登录   1. 去除不必要的权限，例如： 2. sqlplus "/ as sysdba"   revoke dba from user1;   1. 撤消不必要的包的PUBLIC执行权限： 2. sqlplus "/ as sysdba"   SQL>revoke execute on<包名称> from public;   1. 启用数据字典保护： 2. sqlplus "/ as sysdba"   SQL> alter system set O7\_dictionary\_accessibility=false scope=spfile;  关闭，重新启动数据库  SQL>shutdown  SQL>startup  若业务需要其他账户使用该权限，应做特别说明并存档备查。 |
| **检查方法** | 以下操作需sys权限账户登录  sqlplus "/ as sysdba"  （1）查看系统权限：  SQL> select \* from dba\_sys\_privs;  例如：  SQL> select \* from dba\_sys\_privs where grantee='scott';  查看对象权限：  SQL> select \* from dba\_tab\_privs;  例如，查看scott用户下employees表的权限  SQL> select grantee,privilege,grantor,grantable  from dba\_tab\_privs where  owner='scott' and table\_name='employees';  （2）检查包的PUBLIC执行权限：  SQL> select table\_name from dba\_tab\_privs where grantee='PUBLIC' and privilege='EXECUTE' and table\_name in ('UTL\_FILE', 'UTL\_TCP', 'UTL\_HTTP', 'UTL\_SMTP', 'DBMS\_LOB', 'DBMS\_SYS\_SQL', 'DBMS\_JOB','DBMS\_SCHEDULER');  （3）数据字典保护  SQL> show parameter O7\_dictionary\_accessibility; |
| **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** |  |

* + 1. 限制TNS登录IP

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制TNS登录IP（建议实施） |
| **安全基线编号** | 数据库-Oracle-12 |
| **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** | 1.参考配置操作  只需在服务器上的文件$ORACLE\_HOME/network/admin/sqlnet.ora中设  置以下行：  tcp.validnode\_checking = yes  tcp.invited\_nodes = (ip1,ip2…)  2、补充操作说明  如果网络层已经做过访问控制，该项为可选项，否则为必选项  可信内网地址指：专用维护终端、访问数据库应用服务器、堡垒机，  其他地址段禁止。 |
| **检查方法** | 1、判定条件  在非信任的客户端以数据库账户登录被提示拒绝。  2、检测操作  检查$ORACLE\_HOME/network/admin/sqlnet.ora文件中是否设置参数  tcp.validnode\_checking和tcp.invited\_nodes。 |
| **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。 |

* + 1. 限制DBA账户远程登录

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制DBA账户远程登录（建议实施） |
| **安全基线编号** | 数据库-Oracle-13 |
| **安全基线项说明** | 限制具备数据库超级管理员（SYSDBA）权限的用户远程登录。 |
| **配置方法** | 1. 以Oracle用户登录到系统中。  2. 以sqlplus‘/as sysdba’登录到sqlplus环境中。  3. 使用show parameter命令来检查参数REMOTE\_LOGIN\_PASSWORDFILE设置。  Show parameter REMOTE\_LOGIN\_PASSWORDFILE  4. 检查在$ORACLE\_HOME/network/admin/sqlnet.ora文件中参数SQLNET.AUTHENTICATION\_SERVICES设置。 |
| **检查方法** | 1. 参数REMOTE\_LOGIN\_PASSWORDFILE设置为NONE; （限制远程登录） 2. sqlnet.ora文件中参数SQLNET.AUTHENTICATION\_SERVICES设置成NONE;（限制本地账户权限登录） 3. 加固操作可参考如下命令：   sqlplus "/ as sysdba"  SQL> alter system set remote\_login\_passwordfile=none scope=spfile;  关闭，重新启动数据库  SQL>shutdown  SQL>startup |
| **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。例外况：  若存在rman备份，有从远程发起的备份，比如：connect sys/@crmdb11 as sysdba需重点确认是否有影响。需要数据库管理员确认。请谨慎操作。 |

* + 1. 配置数据字典访问权限

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置数据字典访问权限（建议实施） |
| **安全基线编号** | 数据库-Oracle-14 |
| **安全基线项说明** | 启用数据字典保护，只有SYSDBA权限用户才能访问数据字典基础表。 |
| **配置方法** | 1. 以Oracle用户登录到系统中。  2. 以sqlplus‘/as sysdba’登录到sqlplus环境中。  3. 使用show parameter命令来检查参数O7\_DICTIONARY\_ACCESSIBILITY  需要将参数O7\_DICTIONARY\_ACCESSIBILITY是否设置为FALSE |
| **检查方法** | 参数O7\_DICTIONARY\_ACCESSIBILITY是否设置为FALSE |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问； |
| **备注** |  |

* 1. 安全审计
     1. 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-Oracle-15 |
| **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账户、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：账户创建、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。记录需要包含用户账户，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. 以Oracle用户登录到系统中。  2. 以sqlplus‘/as sysdba’登录到sqlplus环境中。  3. 使用show parameter命令来检查参数audit\_trail是否设置。  4.检查dba\_audit\_trail视图中或$ORACLE\_BASE/admin/adump目录下是否有数据。 |
| **检查方法** | 参数audit\_trail不能设置为NONE。  需设置具体的审计内容。  可以设置数据库参数audit\_sys\_operations=true来审计所有SYS用户的操作。 |
| **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** | 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。通过外围审计实现.数据库开启该项参数后，**对数据库性能影响较大**。  在以往的基线推广中，因数据库审计基线对业务系统影响较大，很难落地实施。 |

* 1. 资源控制
     1. 设置连接超时锁定策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置连接超时锁定策略（必须实施） |
| **安全基线编号** | 数据库-Oracle-16 |
| **安全基线项说明** | 在某些应用环境下可设置数据库连接超时，比如数据库超过10分钟的空闲远程连接将自动断开。  自动断开超过10分钟的空闲远程连接，以防止在长时间远程连接过程中被其他人窃听到敏感信息的泄露。同时方式远程人员在离开时并未锁屏或则有效保护，他人借助此时时间空闲进行违规操作带来不必要的安全风险。 |
| **配置方法** | 1、参考配置操作  在sqlnet.ora中找到“SQLNET.EXPIRE\_TIME”项，设置该项参数为10。  示例如下：  SQLNET.EXPIRE\_TIME=10 |
| **检查方法** | 1. 10分钟以上的无任何操作的空闲数据库连接被自动断开； 2. 检查$ORACLE\_HOME/network/admin/sqlnet.ora文件中是否设置参数SQLNET.EXPIRE\_TIME。 |
| **依据** | 6.2.1.4 应用安全：资源控制（A3）：a) 对于有会话或短连接的应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话； |
| **备注** | **如应用需求有长连接形式存在，该项有一定风险。** |

* 1. 其它安全项
     1. 配置安装最小化

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置安装最小化（建议实施） |
| **安全基线编号** | 数据库-Oracle-17 |
| **安全基线项说明** | 只安装业务需要的选件.。需要业务相关人员、数据库管理员共同确认Oracle需要安装的选件，不需要的选件不进行安装。 |
| **配置方法** | 此检查项以问询方式进行。  可以用[Oracle](http://www.2cto.com/database/Oracle/) Universal Installer卸载Oracle组件。 |
| **检查方法** | 此检查项以问询方式进行，根据当前业务状况进行检查。 |
| **依据** |  |
| **备注** | 该项无具体的检查、安全配置方法。实际情况请以具体需求为准。 |

* + 1. 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-Oracle-18 |
| **安全基线项说明** | 使用Oracle提供的高级安全选件来加密客户端与数据库之间或中间件与数据库之间的网络传输数据。 |
| **配置方法** | 检查$ORACLE\_HOME/network/admin/sqlnet.ora文件中是否设置sqlnet.encryption参数 |
| **检查方法** | 要求正确设置参数sqlnet.encryption；  通过网络层捕获的数据库传输包为加密包。 |
| **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。 |

* + 1. 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-Oracle-19 |
| **安全基线项说明** | 输出数据库版本和补丁信息。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** | 使用sys权限账户登录数据库，执行命令  SQL> select \* from v$version;查看输出的版本，根据当前版本决定是否安装补丁。 |
| **检查方法** | 参考安全配置方法，执行SQL> select \* from v$version;，输出当前版本，与oracle官方网站上比对是否有重要补丁未安装。 |
| **依据** |  |
| **备注** | 补丁版本更新历史（仅供参考，请以官方网站通告为准）  Oracle9i Database Release 1: 9.0.1.0–9.0.1.5 (patchset as of December 2003)  Oracle9i Database Release 2: 9.2.0.1–9.2.0.8 (patchset as of April 2007)  Oracle Database 10g Release 1: 10.1.0.2–10.1.0.5 (patchset as of February 2006)  Oracle Database 10g Release 2: 10.2.0.1–10.2.0.5 (patchset as of April 2010)  Oracle Database 11g Release 1: 11.1.0.6–11.1.0.7 (patchset as of September 2008)  Oracle Database 11g Release 2: 11.2.0.1–11.2.0.3 (patchset as of September 2011) |

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。