# Oracle安全配置规范

# 概述

## 适用范围

本规范适用数广侧内网服务器上部署Oracle数据库的安全配置，旨在减少业务安全漏洞、因配置不当造成的安全问题，保障业务安全。

# Oracle安全配置要求

本规范所指的设备为ORACLE数据库。本规范提出的安全配置要求，在未特别说明的情况下，均适用于ORACLE数据库。

本规范从ORACLE数据库的认证授权功能、安全日志功能，和其他自身安全配置功能提出安全要求。

## 帐号

ORACLE应提供帐号管理及认证授权功能，并应满足以下各项要求。

### 按用户分配帐号

|  |  |
| --- | --- |
| **要求内容** | 应按照用户分配帐号，避免不同用户间共享帐号。 |
| **操作指南** | 1. **参考配置操作**   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**   1、*abc1*和*abc2*是两个不同的帐号名称，可根据不同用户，取不同的名称； |
| **检测方法** | 1. **判定条件**   不同名称的用户可以连接数据库   1. **检测操作**   connect abc1/password1连接数据库成功  **5、补充说明** |

### 删除或锁定无关帐号

|  |  |
| --- | --- |
| **要求内容** | 应删除或锁定与数据库运行、维护等工作无关的帐号。 |
| **操作指南** | 1. **参考配置操作**   alter user username lock;  drop user username cascade;   1. **补充操作说明** |
| **检测方法** | 1. **判定条件**   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  **4、检测操作**  **5、补充说明** |

### 限制SYSDBA用户的远程登录

|  |  |
| --- | --- |
| **要求内容** | 限制具备数据库超级管理员（SYSDBA）权限的用户远程登录。 |
| **操作指南** | **1、参考配置操作**  1. 在spfile中设置REMOTE\_LOGIN\_PASSWORDFILE=NONE来禁止SYSDBA用户从远程登陆。  2. 在sqlnet.ora中设置SQLNET.AUTHENTICATION\_SERVICES=NONE来禁用 SYSDBA 角色的自动登录。  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  1. 不能通过Sql\*Net远程以SYSDBA用户连接到数据库。  2. 在数据库主机上以sqlplus ‘/as sysdba’连接到数据库需要输入口令。  **4、检测操作**  1. 以Oracle用户登陆到系统中。  2. 以sqlplus ‘/as sysdba’登陆到sqlplus环境中。  3. 使用show parameter命令来检查参数REMOTE\_LOGIN\_PASSWORDFILE是否设置为NONE。  Show parameter REMOTE\_LOGIN\_PASSWORDFILE  4. 检查在$ORACLE\_HOME/network/admin/sqlnet.ora文件中参数SQLNET.AUTHENTICATION\_SERVICES是否被设置成NONE。  **5、补充说明** |

### 用户权限最小化

|  |  |
| --- | --- |
| **要求内容** | 在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。 |
| **操作指南** | 1. **参考配置操作**   grant　权限　to username;  revoke 权限　from username;   1. **补充操作说明**   用第一条命令给用户赋相应的最小权限  用第二条命令收回用户多余的权限 |
| **检测方法** | 1. **判定条件**   业务测试正常   1. **检测操作**   业务测试正常  **5、补充说明** |

### 使用ROLE管理对象的权限

|  |  |
| --- | --- |
| **要求内容** | 使用数据库角色（ROLE）来管理对象的权限。 |
| **操作指南** | **1、参考配置操作**  1. 使用Create Role命令创建角色。  2. 使用用Grant命令将相应的系统、对象或Role的权限赋予应用用户。  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  对应用用户不要赋予DBA Role或不必要的权限。  **4、检测操作**  1. 以DBA用户登陆到sqlplus中。  2. 通过查询dba\_role\_privs、dba\_sys\_privs和dba\_tab\_privs等视图来检查是否使用ROLE来管理对象权限。  **5、补充说明** |

### 控制用户属性

|  |  |
| --- | --- |
| **要求内容** | 对用户的属性进行控制，包括密码策略、资源限制等。 |
| **操作指南** | **1、参考配置操作**  可通过下面类似命令来创建profile，并把它赋予一个用户  CREATE PROFILE app\_user2 LIMIT  FAILED\_LOGIN\_ATTEMPTS 6  PASSWORD\_LIFE\_TIME 60  PASSWORD\_REUSE\_TIME 60  PASSWORD\_REUSE\_MAX 5  PASSWORD\_VERIFY\_FUNCTION verify\_function  PASSWORD\_LOCK\_TIME 1/24  PASSWORD\_GRACE\_TIME 90;  ALTER USER jd PROFILE app\_user2;  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  1. 可通过设置profile来限制数据库帐户口令的复杂程度，口令生存周期和帐户的锁定方式等。  2. 可通过设置profile来限制数据库帐户的CPU资源占用。  **4、检测操作**  1. 以DBA用户登陆到sqlplus中。  2. 查询视图dba\_profiles和dba\_usres来检查profile是否创建。  **5、补充说明** |

### 启用数据库字典保护

|  |  |
| --- | --- |
| **要求内容** | 启用数据字典保护，只有SYSDBA用户才能访问数据字典基础表。 |
| **操作指南** | **1、参考配置操作**  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  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  以普通dba用户登陆到数据库，不能查看X$开头的表，比如：  select \* from sys. x$ksppi;  **4、检测操作**  1. 以Oracle用户登陆到系统中。  2. 以sqlplus ‘/as sysdba’登陆到sqlplus环境中。  3. 使用show parameter命令来检查参数O7\_DICTIONARY\_ACCESSIBILITY是否设置为FALSE。  Show parameter O7\_DICTIONARY\_ACCESSIBILITY  **5、补充说明** |

## 口令

### 静态口令认证的密码复杂度控制

|  |  |
| --- | --- |
| **要求内容** | 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4类中至少2类。 |
| **操作指南** | 1. **参考配置操作**   为用户建profile，调整PASSWORD\_VERIFY\_FUNCTION，指定密码复杂度   1. **补充操作说明** |
| **检测方法** | 1. **判定条件**   修改密码为不符合要求的密码，将失败   1. **检测操作**   alter user abcd1 identified by abcd1;将失败  **5、补充说明** |

### 静态口令认证的密码生命周期

|  |  |
| --- | --- |
| **要求内容** | 对于采用静态口令认证技术的数据库，帐户口令的有效期小于90天。 |
| **操作指南** | 1. **参考配置操作**   为用户建相关profile，指定PASSWORD\_GRACE\_TIME为90天   1. **补充操作说明**   在90天内，需要修改密码 |
| **检测方法** | 1. **判定条件**   到期不修改密码，密码将会失效。连接数据库将不会成功   1. **检测操作**   connect username/password报错  **5、补充说明** |

### 静态口令认证的密码重复使用限制

|  |  |
| --- | --- |
| **要求内容** | 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。 |
| **操作指南** | 1. **参考配置操作**   为用户建profile,指定PASSWORD\_REUSE\_MAX为５   1. **补充操作说明**   当前使用的密码，必需在密码修改５次后才能再次被使用 |
| **检测方法** | 1. **判定条件**   重用修改５次内的密码，将不能成功   1. **检测操作**   alter user username identified by password1;如果password1在５次修改密码内被使用，该操作将不能成功  **5、补充说明** |

### 静态口令认证的连续登录失败的帐号锁定策略

|  |  |
| --- | --- |
| **要求内容** | 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达到10次（不含10次），锁定该用户使用的帐号。 |
| **操作指南** | 1. **参考配置操作**   为用户建profile，指定FAILED\_LOGIN\_ATTEMPTS为６   1. **补充操作说明**   如果连续10次连接该用户不成功，用户将被锁定 |
| **检测方法** | 1. **判定条件**   连续10次用错误的密码连接用户，第11次输入错误时用户将被锁定   1. **检测操作**   connect username/password，连续11次失败，用户被锁定  **5、补充说明** |

### 更改数据库默认帐号的密码

|  |  |
| --- | --- |
| **要求内容** | 更改数据库默认帐号的密码。 |
| **操作指南** | **1、参考配置操作**  1. 可通过下面命令来更改默认用户的密码：  ALTER USER XXX IDENTIFIED BY XXX;  2. 下面是默认用户列表：  ANONYMOUS  CTXSYS  DBSNMP  DIP  DMSYS  EXFSYS  HR  LBACSYS  MDDATA  MDSYS  MGMT\_VIEW  ODM  ODM\_MTR  OE  OLAPSYS  ORDPLUGINS  ORDSYS  OUTLN  PM  QS  QS\_ADM  QS\_CB  QS\_CBADM  QS\_CS  QS\_ES  QS\_OS  QS\_WS  RMAN  SCOTT  SH  SI\_INFORMTN\_SCHEMA  SYS  SYSMAN  SYSTEM  TSMSYS  WK\_TEST  WKPROXY  WKSYS  WMSYS  XDB  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  不能以用户名作为密码或使用默认密码的帐户登陆到数据库。  **4、检测操作**  1. 以DBA用户登陆到sqlplus中。  2. 检查数据库默认帐户是否使用了用户名作为密码或默认密码。  **5、补充说明** |

### 操作系统级的帐户安全策略

|  |  |
| --- | --- |
| **要求内容** | Oracle软件帐户的访问控制可遵循操作系统帐户的安全策略，比如不要共享帐户、强制定期修改密码、密码需要有一定的复杂度等。 |
| **操作指南** | **1、参考配置操作**  使用操作系统一级的帐户安全管理来保护Oracle软件帐户。  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  每3个月自动提示更改密码，过期后不能登陆。  **4、检测操作**  每3个月强制修改Oracle软件帐户密码，并且密码需要满足一定的复杂程度，符合操作系统的密码要求。  **5、补充说明** |

## 日志

### 登录日志功能

|  |  |
| --- | --- |
| **要求内容** | 数据库应配置日志功能，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。 |
| **操作指南** | 1. **参考配置操作**   创建ORACLE登录触发器，记录相关信息，但对IP地址的记录会有困难 |
| **检测方法** | 1. **判定条件**   登录测试，检查相关信息是否被记录  **3、检测操作**   1. **补充说明**   触发器与AUDIT会有相应资源开消，请检查系统资源是否充足。特别是RAC环境，资源消耗较大。 |

### DDL日志

|  |  |
| --- | --- |
| **要求内容** | 数据库应配置日志功能，记录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。 |
| **操作指南** | 1. **参考配置操作**   创建ORACLE DDL触发器，记录相关信息，但对IP地址的记录会有困难  **2、补充操作说明** |
| **检测方法** | 1. **判定条件**   做相关操作，检查是否记录成功  **4、检测操作**   1. **补充说明**   触发器与AUDIT会有相应资源开消，请检查系统资源是否充足。特别是RAC环境，资源消耗较大。 |

### 数据库审记

|  |  |
| --- | --- |
| **要求内容** | 根据业务要求制定数据库审计策略。 |
| **操作指南** | **1、参考配置操作**  1. 通过设置参数audit\_trail = db或os来打开数据库审计。  2. 然后可使用Audit命令对相应的对象进行审计设置。  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  对审计的对象进行一次数据库操作，检查操作是否被记录。  **4、检测操作**  1. 检查初始化参数audit\_trail是否设置。  2. 检查dba\_audit\_trail视图中或$ORACLE\_BASE/admin/adump目录下是否有数据。   1. **补充说明**   AUDIT会有相应资源开消，请检查系统资源是否充足。特别是RAC环境，资源消耗较大。 |

## 其他

### VPD与OLS

|  |  |
| --- | --- |
| **要求内容** | 使用Oracle提供的虚拟私有数据库（VPD）和标签安全（OLS）来保护不同用户之间的数据交叉访问。 |
| **操作指南** | **1、参考配置操作**  1. 在表上构建 VPD可以使用Oracle所提供的 PL/SQL 包 DBMS\_RLS 控制整个 VPD 基础架构，具体设置方法较复杂，建议参考Oracle文档进行配置。  2. Oracle标签安全(OLS)是在相关表上通过添加一个标签列来实现复杂的数据安全控制，具体细节请参考Oracle文档。  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  通过视图来检查是否在数据库对象上设置了VPD和OLS。  **4、检测操作**  查询视图v$vpd\_policy 和dba\_policies。  **5、补充说明** |

### Data Vault

|  |  |
| --- | --- |
| **要求内容** | 使用Oracle提供的Data Vault选件来限制有DBA权限的用户访问敏感数据。 |
| **操作指南** | **1、参考配置操作**  Oracle Data Vault是作为数据库安全解决方案的一个单独选件，主要功能是将数据库管理帐户的权限和应用数据访问的权限分开， Data Vault可限制有DBA权限的用户访问敏感数据。设置比较复杂，具体细节请参考Oracle文档。  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  以DBA用户登陆，不能查询其它用户下面的数据。  **4、检测操作**  1. 在视图dba\_users中查询是否存在dvsys用户。  2. 在视图dba\_objects中检查是否存在dbms\_macadm对象。  **5、补充说明** |

### Listener设定密码保护

|  |  |
| --- | --- |
| **要求内容** | 为数据库监听器（LISTENER）的关闭和启动设置密码。 |
| **操作指南** | **1、参考配置操作**  通过下面命令设置密码：  $ lsnrctl  LSNRCTL> change\_password  Old password: <OldPassword> Not displayed  New password: <NewPassword> Not displayed  Reenter new password: <NewPassword> Not displayed  Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=prolin1)(PORT=1521)(IP=FIRST)))  Password changed for LISTENER  The command completed successfully  LSNRCTL> save\_config  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  使用lsnrctl start或lsnrctl stop命令起停listener需要密码  **4、检测操作**  检查$ORACLE\_HOME/network/admin/listener.ora文件中是否设置参数PASSWORDS\_LISTENER。  **5、补充说明** |

### 设定信任IP集

|  |  |
| --- | --- |
| **要求内容** | 设置只有信任的IP地址才能通过监听器访问数据库。 |
| **操作指南** | **1、参考配置操作**  只需在服务器上的文件$ORACLE\_HOME/network/admin/sqlnet.ora中设置以下行：  tcp.validnode\_checking = yes  tcp.invited\_nodes = (ip1,ip2…)  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  在非信任的客户端以数据库帐户登陆被提示拒绝。  **4、检测操作**  检查$ORACLE\_HOME/network/admin/sqlnet.ora文件中是否设置参数tcp.validnode\_checking和tcp.invited\_nodes。  **5、补充说明** |

### 加密网络传输

|  |  |
| --- | --- |
| **要求内容** | 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。 |
| **操作指南** | **1、参考配置操作**  1. 在Oracle Net Manager中选择“Oracle Advanced Security”。  2. 然后选择Encryption。  3. 选择Client或Server选项。  4. 选择加密类型。  5. 输入加密种子（可选）。  6. 选择加密算法（可选）。  7. 保存网络配置，sqlnet.ora被更新。  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  通过网络层捕获的数据库传输包为加密包。  **4、检测操作**  检查$ORACLE\_HOME/network/admin/sqlnet.ora文件中是否设置sqlnet.encryption等参数。  **5、补充说明** |

### 断开超时的空闲远程连接

|  |  |
| --- | --- |
| **要求内容** | 根据业务需要设置数据库连接超时限制，如空闲连接超过30分钟时间自动断开。 |
| **操作指南** | **1、参考配置操作**  在sqlnet.ora中设置下面参数：  SQLNET.EXPIRE\_TIME=30  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  30分钟以上的无任何操作的空闲数据库连接被自动断开  **4、检测操作**  检查$ORACLE\_HOME/network/admin/sqlnet.ora文件中是否设置参数SQLNET.EXPIRE\_TIME。  **5、补充说明** |

### 限制DBA组中的操作系统用户数量

|  |  |
| --- | --- |
| **要求内容** | 限制在DBA组中的操作系统用户数量，通常DBA组中只有Oracle安装用户。 |
| **操作指南** | **1、参考配置操作**  通过/etc/passwd文件来检查是否有其它用户在DBA组中。  **2、补充操作说明** |
| **检测方法** | **3、判定条件**  无其它用户属于DBA组。  **4、检测操作**  通过/etc/passwd文件来检查是否有其它用户在DBA组中。  **5、补充说明** |

## 简明checklist

|  |  |  |  |
| --- | --- | --- | --- |
| 分类 | 检查点 | 检查方法 | 检查结果 |
| 帐号 | 不同应用使用不同帐号连接数据库 | N个应用对应N个不同的帐号 |  |
| 删除或锁定无关帐号 | 检查数据库所有帐号是否都需要使用 |  |
| 限制具备数据库超级管理员（SYSDBA）权限的用户远程登录 | Show parameter REMOTE\_LOGIN\_PASSWORDFILE返回结果必须为NONE |  |
| $ORACLE\_HOME/network/admin/sqlnet.ora文件中参数SQLNET.AUTHENTICATION\_SERVICES配置为NONE |  |
| 用户权限最小化 | 检查每个帐号是否需要写权限等高级权限，检查每个帐号读权限范围是否过宽 |  |
| 使用ROLE管理对象的权限 | 检查是否基于ROLE来分配权限 |  |
| 对用户的属性进行控制，包括密码策略、资源限制等 | 查询视图dba\_profiles和dba\_usres来检查profile是否有相关的密码策略和资源限制配置 |  |
|  | 启用数据库字典保护 | show parameter命令来检查参数O7\_DICTIONARY\_ACCESSIBILITY是否设置为FALSE |  |
| 口令 | 静态口令认证的密码复杂度控制 | 修改任意帐号密码为abcd1，看是否成功。  alter user abcd1 identified by abcd1; |  |
| 静态口令认证的密码生命周期 | 检查用户profile PASSWORD\_GRACE\_TIME是否为90天 |  |
| 静态口令认证的密码重复使用限制 | 检查用户profile PASSWORD\_REUSE\_MAX是否为５ |  |
| 静态口令认证的连续登录失败的帐号锁定策略 | 检查用户profile FAILED\_LOGIN\_ATTEMPTS是否为６ |  |
| 更改数据库默认帐号的密码 | 检查默认帐号是否使用用户密码或默认密码，默认帐号参考前文。 |  |
| 日志 | 登录日志功能 | 登录测试，检查相关信息是否被记录 |  |
| DDL日志 | 修改帐号密码，检查是否记录成功 |  |
| 数据库审记 | 检查初始化参数audit\_trail是否设置 |  |
| 检查dba\_audit\_trail视图中或$ORACLE\_BASE/admin/adump目录下是否有数据。 |  |
| 其他 | VPD与OLS | 通过视图来检查是否在数据库对象上设置了VPD和OLS |  |
| Data Vault | 在视图dba\_users中查询是否存在dvsys用户 |  |
| 在视图dba\_objects中检查是否存在dbms\_macadm对象 |  |
| Listener设定密码保护 | 检查$ORACLE\_HOME/network/admin/listener.ora文件中是否设置参数PASSWORDS\_LISTENER |  |
| 设定信任IP集 | 检查$ORACLE\_HOME/network/admin/sqlnet.ora文件中是否设置参数tcp.validnode\_checking和tcp.invited\_nodes |  |
| 加密网络传输 | 检查$ORACLE\_HOME/network/admin/sqlnet.ora文件中是否设置sqlnet.encryption等参数 |  |
| 断开超时的空闲远程连接 | 检查$ORACLE\_HOME/network/admin/sqlnet.ora文件中是否设置参数SQLNET.EXPIRE\_TIME |  |
| 限制DBA组中的操作系统用户数量 | 通过/etc/passwd文件来检查是否有其它用户在DBA组中 |  |