基础架构室【2018】第XXX号

**Oracle数据库配置基线规范**

**科技信息部**

**2018年9月**

**版本控制信息**

|  |  |  |
| --- | --- | --- |
| 文件状态：  [√ ] 草稿  [ ] 正式发布  [ ] 正在修改 | 当前版本： | V1.0 |
| 编写部门： | 科技信息部 |
| 作 者： | 于洋、封夏 |
| 完成日期： |  |
| 审 核： | 司徒浩、叶明 |
| 审核日期： |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 版本 | 修订说明 | 修订人 |
| 2017.07.01 | V1.0 | 根据生产环境建库规范和上线检查创建规范 | 于洋 |
| 2017.08.21 | V1.2 | 按照科技部制度规范模板修改 | 于洋 |
| 2018.09.08 | V1.3 | 补充新核心相关的规范，统一格式。 | 于洋 |

目 录

[1 引言 5](#_Toc524299375)

[1.1 目标 5](#_Toc524299376)

[1.2 适用范围 5](#_Toc524299377)

[1.3 术语定义 5](#_Toc524299378)

[2 登录与访问 6](#_Toc524299379)

[2.1 网络访问控制 6](#_Toc524299380)

[2.2 登录账号 6](#_Toc524299381)

[2.3 登录认证 7](#_Toc524299382)

[2.4 权限控制 7](#_Toc524299383)

[3 参数配置 8](#_Toc524299384)

[3.1 初始化参数 8](#_Toc524299385)

[3.2 用户PROFILE 8](#_Toc524299386)

[3.3 初始化参数 9](#_Toc524299387)

[3.4 优化参数 10](#_Toc524299388)

[4 备份与高可用 10](#_Toc524299389)

[4.1 备份配置 10](#_Toc524299390)

[4.2 高可用配置 11](#_Toc524299391)

[5 其他配置 12](#_Toc524299392)

[5.1 版本选择 12](#_Toc524299393)

[5.2 监听配置 12](#_Toc524299394)

[5.3 监控配置 12](#_Toc524299395)

[6 附录一：重要信息系统清单 13](#_Toc524299396)

[7 附录二：Oracle数据库监控指标 14](#_Toc524299397)

# 引言

## 目标

为加强我行信息系统的配置基线管理，提高我行信息系统安全运营水平，保证信息系统稳定运行，特制定本规范。本基线旨在对我行信息系统中的Oracle数据库安全加固和配置进行规范。

本基线规范是Oracle数据库配置和安全相关的配置规范，对于操作系统涉及的操作系统、中间件和虚拟化的基线规范，由对应的操作系统、中间件、数据库和虚拟化基线规范说明。

本基线规范是本行技术规范要求的一部分，可用于新系统上线前的基线检查，同时为数据库管理员的上线前安全检查提供参考标准。

## 适用范围

本基线规范适用于成都农商银行生产信息系统使用的Oracle11g、12C版本，不适用于监管类系统要求的特定版本或其他非Oracle类数据库。

## 术语定义

应用用户：即数据库应用账号，指数据库提供给应用程序连接数据库的账号。

内控管理平台：我行登录生产环境主机、存储、网络和数据库各类设备的统一登录入口。

数据库审计系统：我行用于对业务交易中的SQL语句进行统一审计的安全审计系统。

# 登录控制

## 网络访问控制

**基线说明：**应用用户访问数据库，必须通过防火墙的访问控制，防火墙对访问数据库监听的端口的访问接入进行控制。

**适用范围：**已有、新建的生产系统

**基线规范：**

1. 禁止使用数据库默认监听端口：1521，修改为非默认端口：1688，对应用连接提供数据库访问。
2. 应用服务器连接数据库服务器时，必要的网段需要NAT地址转换和防火墙的访问控制。只允许规定的应用服务器IP地址连接数据库服务器1688端口。
3. 对于跨数据心的应用系统，访问数据库时应通过DNS域名解析。

## 登录账号

**基线说明：**对数据库默认账号进行锁定。数据库只开通特定的数据库用户登录。

**适用范围：**新建的生产信息系统

**基线规范：**

1. 应用程序连接数据库所使用的应用用户；
2. sys、system数据库超级用户，用于执行数据库维护操作；
3. itmuser用户，用于Tivoli监控数据库的专用账号；
4. tm用户，用于执行数据安全脱敏操作的专用账号；
5. dbquery或dbsnmp查询权限用户，用于日常巡检、配置检查等。

## 登录认证

**基线说明：**数据库管理用户可以依赖其宿主操作系统提供的身份认证机制完成对数据库用户的认证。

**适用范围：**已有、新建的生产系统

## 权限控制

**基线说明：**数据库中的用户权限，采用最小授权方式。

**适用范围：**新建的生产信息系统

**基线规范：**

1. 禁止将任何对象权限、系统权限，人为授权给PUBLIC角色。（注：在产品安装过程中，默认授权给public的权限不在该范围）；
2. 应用用户、小权用户禁止拥有dba、exp\_full\_database、imp\_full\_database角色权限等高级系统权限；
3. 应用用户分配规定配额的表空间使用权限，必须通过quota命令逐一对某个表空间进行配额授权。

命令：alter user <APP\_USER> quota unlimited on <TBS\_APP>;

# 参数配置

## 初始化参数

**基线说明：**数据库的初始化参数应参考本项进行设置。

**适用范围：**新建的生产信息系统

**基线规范：**

1. 新建业务系统的数据库字符集为：AL32UTF8/ZHS16GBK。在软件产品支持的前提下，推荐使用AL32UTF8。
2. 内控管理平台进行人工操作行为审计，数据库审计系统进行交易级SQL语句的集中审计，初始化配置中应关闭各个数据库默认开启的审计功能。
   1. audit\_trail = NONE，默认配置为不审计。
   2. audit\_trail = DB，对特别重要的业务系统数据库可设置为DB级。

## 用户PROFILE

**基线说明：**oracle账户的默认用户属性无法达到生产要求，必须修改默认profile的设置。

**适用范围：**新建的生产信息系统

**基线规范：**

1. FAILED\_LOGIN\_ATTEMPTS = unlimited，对重要的业务系统数据库可设为：失败登录次数不超过20次。
2. PASSWORD\_LIFE\_TIME = UNLIMITED，密码过期时间为永不过期。

命令：alter profile default limit PASSWORD\_LIFE\_TIME unlimited;

1. PASSWORD\_VERIFY\_FUNCTION = NULL，默认为不设PROFILE检查函数，对数据库账号密码有复杂度要求的系统可设置为：VERIFY\_FUNCTION\_11G。
2. PASSWORD\_REUSE\_TIME = 3，不允许使用3次以内修改过的数据库密码。

## 初始化参数

**基线说明：**对数据库的初始化参数配置规范

**适用范围：**新建的生产信息系统

**基线规范：**

1. processes=500，数据库最大进程数不低于500个。
2. open\_cursor=300，单个会话允许打开的游标数不低于300个。
3. control\_file\_record\_keep\_time=30，控制文件记录保留周期至少为30天。
4. enable\_ddl\_logging = TRUE，将DDL语句记录到告警日志中。
5. remote\_login\_passwordfile = none，对未启用Oracle Active Dataguard的生产库，建议禁用sysdba使用密码文件登录数据库。
6. ENABLE\_DDL\_LOGGING = true，将数据库中所有执行的DDL语句记录在告警日志中。

## 优化参数

**基线说明：**与性能相关的初始化参数文件的配置规范

**适用范围：**新建的生产信息系统

**基线规范：**

1. sga\_target不低于4GB，不高于OS内存的70%。
2. memory\_target = 0，不开启全内存自动管理（AMM）功能。
3. parallel\_force\_local = TRUE，不开启跨RAC计算节点的并行执行功能。
4. \_optimizer\_mjc\_enabled = FALSE，根据实际需要，可关闭merge join的连接方式以优化执行计划。
5. \_undo\_autotune = FALSE，关闭undo空间自动调整的功能。
6. \_use\_adaptive\_log\_file\_sync = FALSE，根据实际需要，可关闭新特性将polling方式还原成post/wait方式写redo日志。
7. 根据实际批量业务的需要，修改默认的统计信息收集时间窗口，默认启动时间为：22:00~次日2:00。

命令：EXECUTE DBMS\_SCHEDULER.SET\_ATTRIBUTE()

# 备份与高可用

## 备份配置

**基线说明：**对Oracle数据库备份的配置规范要求

**适用范围：**已有、新建的生产信息系统

**基线规范：**

1. 生产系统数据库应开启归档模式。

命令：alter database archivelog;。

1. 生产系统数据库必须通过备份平台统一调度RMAN，对Oracle数据库进行集中备份。特殊系统将根据服务目录，对部分数据刻带出库。

## 高可用配置

**基线说明：**应用连接数据库，应使用Weblogic连接池技术提供的多连接池、使用多地址的JDBC连接串配置。如果使用OCI连接应关注客户端TNS配置的高可用。

**适用范围：**已有、新建的生产信息系统

**基线规范：**

1. JDBC连接串配置如下：

jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS\_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<db1-vip>)(PORT=1688))(ADDRESS=(PROTOCOL=TCP)(HOST=<db2-vip>)(PORT=1688)))(CONNECT\_DATA=(SERVICE\_NAME=<service\_name>)))

1. 对使用Oracle client的连接，在TNS配置中配置基于客户端的TAF特性，或基于数据库服务端TAF特性对会话连接提供高可用保护。对交易类应用FAILOVER\_MODE类型选用TYPE=session类型，数据抽取加载（ETL）类应用选用TYPE=select类型。在tnsnames.ora文件中的CONNECT\_DATA中添加如下配置：

<TNS\_STRING> =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST =<db1-vip>)(PORT = 1688))

(ADDRESS = (PROTOCOL = TCP)(HOST =<db2-vip>)(PORT = 1688))

(CONNECT\_DATA =

(SERVER = DEDICATED)

(SERVICE\_NAME = <service\_name>)

(FAILOVER\_MODE =

(TYPE = [select|session])

(METHOD = basic)

)

)

)

命令：srvctl add service -d <db\_unique\_name> -s <service\_name> -r <preferred\_list> -P BASIC -e SELECT

# 其他配置

## 版本选择

**基线说明：**使用主流的Oracle数据库版本，在新建系统时数据库管理员应选用经过验证的Oracle次新版本PSU补丁，定期对已超过原厂维护期的老旧版本数据库进行升级。

**适用范围：**新建的生产信息系统

## 监听配置

**基线说明：**为方便对监听程序（listener）的监控，不设置监听密码。

**适用范围：**已有、新建的生产信息系统

## 监控配置

**基线说明：**部署Tivoli ux或lz监控代理对数据库服务器进行监控。部署Tivoli rz监控代理对数据库进行监控，使用itmuser用户连接数据库采集监控信息。

**适用范围：**已有、新建的生产信息系统

本基线中未尽事宜，参照科技信息部基础架构室其它相关规范执行。

# 附录一：Oracle数据库监控指标



# 附录二：重要信息系统

|  |  |  |
| --- | --- | --- |
| 序号 | 信息系统 | 信息系统描述 |
| 1 | 人民币综合业务系统 | 提供存贷款、中间业务、内部账务等核心类交易等，以及为其他业务类系统提供核心交易支撑。 |
| 2 | 直销银行 | 处理直销银行业务。 |
| 3 | 金融服务平台 | 渠道类业务中转平台。 |
| 4 | 网上银行系统 | 个人和企业网上客户交易明细查询、活期转定期、转账、代缴、代发工资理财购买、基金购买、贷款查询等。 |
| 5 | 银联前置系统（借记卡） | 处理借记卡、银联相关交易 |
| 6 | 移动银行系统 | 处理移动银行业务。 |
| 7 | 统一支付系统 | 分为大额支付系统和小额支付系统。 |
| 8 | 电话银行系统 | Callcenter 95392 |