数据安全传输基础设施平台部署手册

# 1安全传输平台简介

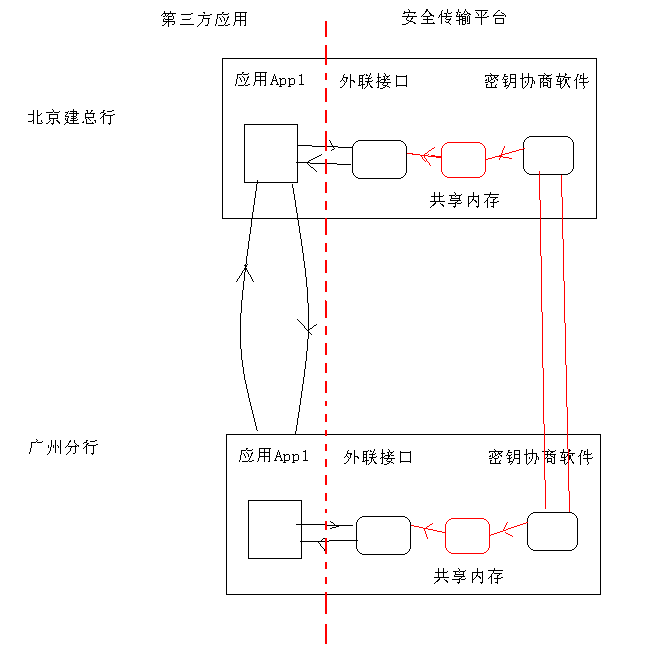
数据安全传输基础设施平台（简称，数据传输平台）是一款基础设施类项目，为集团、企业信息系统的提供统一、标准的信息安全服务；解决企业和企业之间，点与点之间传输安全、消息安全、身份鉴别和认证；能解决新增云服务结点间安全数据传输；也能解决了传统的安全产品部署分散、效率低下、系统脆弱等关键问题。是信息系统“逻辑大集中”、“业务大集中”下的数据安全传输解决方案。

简言之：为第三方信息系统提供加密算法和密钥；保证信息系统点与点之间安全通信。

复杂的说：解决安全密钥分发、高并发的密码运算设备群的调用，统一的加解密接口。管理接入的网点。

# 2安全传输平台方案

## 2.1方案部署原理



以两个网点的应用为例说明部署：

1）在北京建总行网点和N个广州分行网点之间的应用程序，通讯之前进行数据加解密。北京建总行管理N个网点的应用。

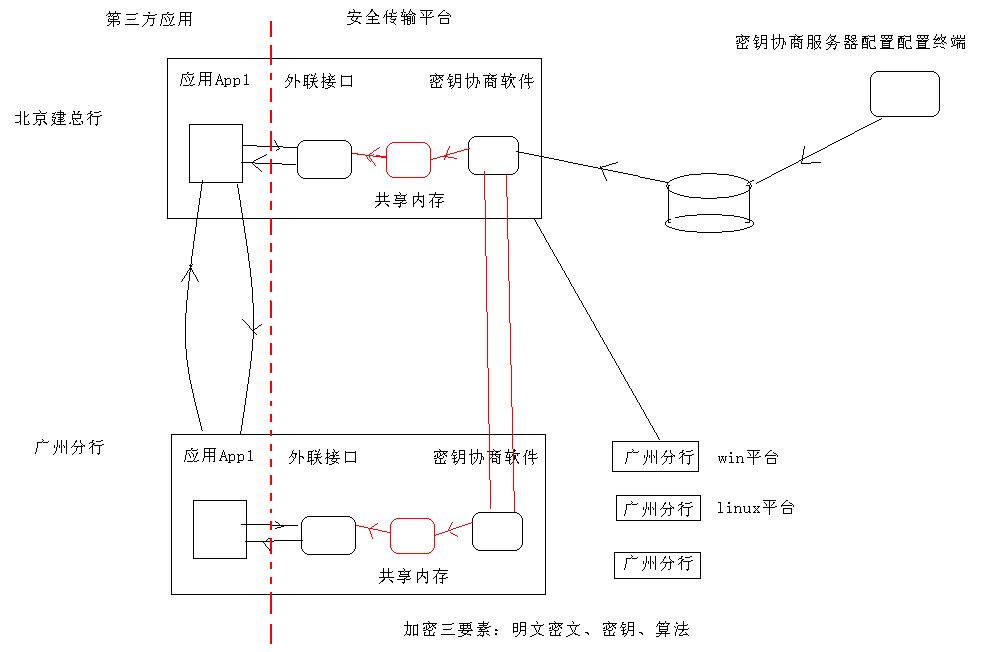
2）北京建总行网点的硬件服务器上，部署外联接口（AppInterface）和密钥协商服务（SecMngKeyServer）程序。

3）广州分行网点的硬件服务器上，部署外联接口（AppInterface）和密钥协商软件客户端（SecMngKeyClinet）程序。

4）密钥协商软件客户端软件可是Win平台、linux平台程序；异构通讯。

5）网点应用通过外联接口（AppInterface）进行加解密。

## 2.2方案介绍



1. 第三方应用app，通过外联接口加密、解密数据。
2. 外联接口通过共享内存查找网点密钥。
3. 密钥协商服务器和密钥协商客户端协商密钥，写共享内存。密钥协商客户端可以是linux平台应用程序、也可以是win平台应用程序。
4. 密钥协商服务器配置终端（SecMngAdmin）管理接入的网点应用，完成网点生命周期管理；密钥协商服务器配置终端（SecMngAdmin）可以进行历史密钥管理、审计管理等等。

## 2.3方案流程



1. 安装数据库，部署安全传输平台sql脚本方案
2. 密钥协商服务器器配置终端SecMngServerAdmin，添加网点信息，配置后台服务器启动参数
3. 启动密钥协商服务器（SecMngServer）后台服务程序
4. 启动密钥协商客户端程序（SecMngClinet），发起协商密钥
5. 第三方信息系统，通过外联接口（AppInterface），加解密

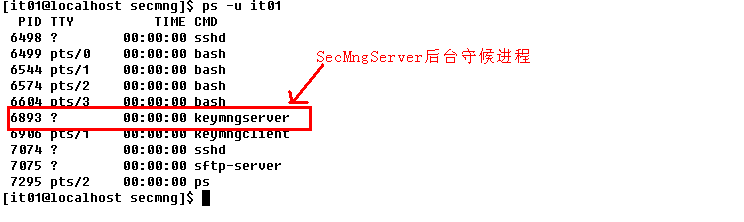
## 2.4方案子系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 编号 | 子系统 | 软件平台 | 主要技术点 | 备注 |
| 01 | 统一数据库访问组件libicdbapi | Linux | 1封装proc访问oracle数据库  2基于数据库连接池  3linux下线程互斥和同步 | 接口的封装和设计 |
| 02 | 统一通讯SocketApi组件 | Linux、Win | 1封装Linux和Win下基本SocketApi  2基于socket 连接池  3 win下和linux下的线程互斥和同步  4 win下和linux下异构通讯 | 接口的封装和设计 |
| 03 | 统一报文编解码组件  Libmessagereal | Linux、win | 1接口的封装和设计  2 win和linux源码的移植  3win和linux平台下动态库的设计与实现 xml json html DER | 接口的封装和设计 |
| 04 | 统一共享内存读写组件 | Linux、win | 1接口的封装和设计  2 win和linux进程间通信机制IPC（共享内存、消息队列） | 接口的封装和设计 |
| 05 | 密钥协商服务程序SecMngServer | Linux | 1 linux服务器框架编写  2各种动态库的集成  3 linux业务流的编写和调试 | Linux服务程序系统开发 |
| 06 | 密钥协商客户端程序SecMngClient | Linux、win | 1 linux客户端编写  2 Win客户端编写  3各种动态库的集成  4 linux和win业务流的编写和调试 | Linux信息系统开发  Win信息系统开发 |
| 07 | 密钥协商服务配置管理终端SecMngServerAdmin | Win | 1MFC框架、视图切分和切换  2各种win动态库的集成  3 win和linux的对接和调试  4win下odbc驱动连接数据库 | Win信息系统开发 |
| 08 | 外联接口AppInterface | Linux、win | 1接口的封装和设计 | 接口设计与实现 |
| 09 | 对称密钥加解密接口 | Linux、win | 1安全基础知识 | 使用第三方接口 |
| 10 | 安全传输平台数据库脚本 | Oracle | 1sql脚本  2oracle数据库的安装、启动、关闭基本管理  3安全传输平台sql脚本的实施 | 信息系统数据库解决方案 |

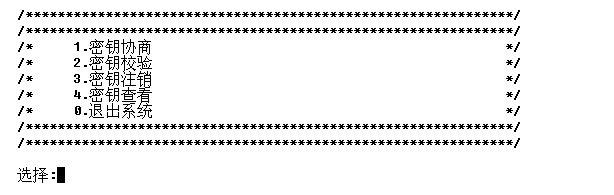
## 2.5方案子系统演示

### 2.5.1 linux平台SecMngServer和SecMngClient

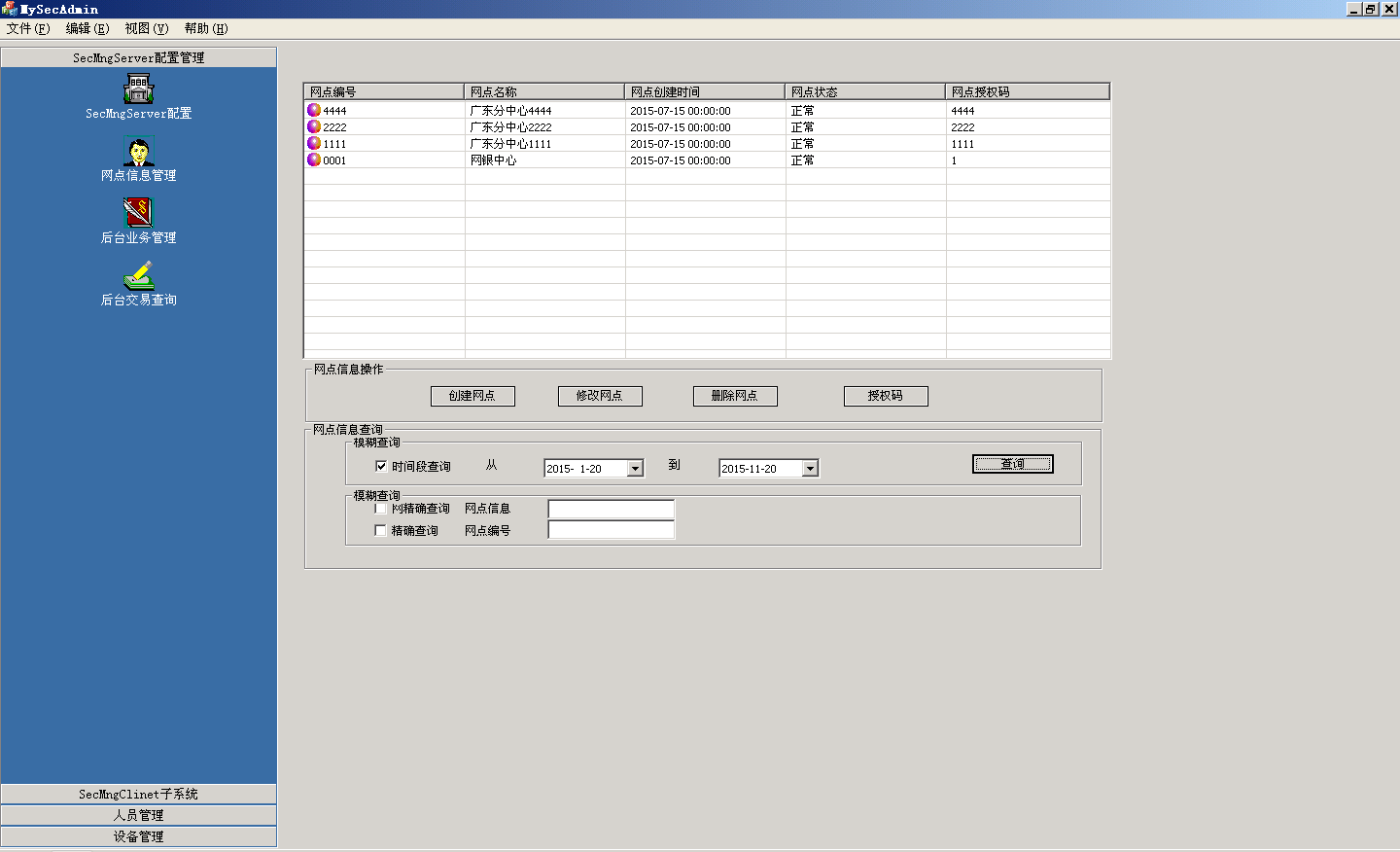
**SecMngServer**



**SecMngClient**



### 2.5.3Win平台SecMngServerAdmin



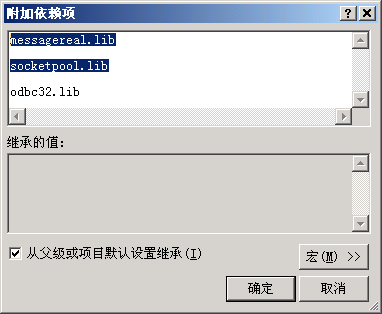
### 2.5.3Win平台SecMngClinet



### 2.5.4 linux基础组件



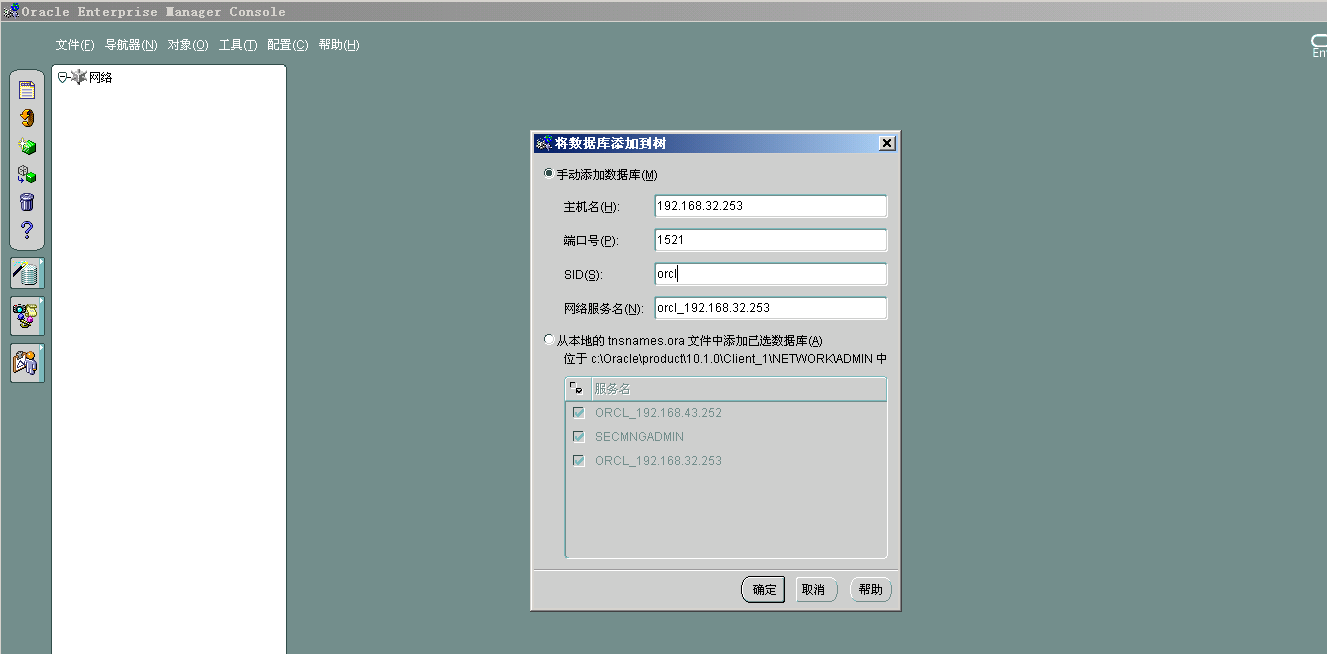
### 2.5.4Win基础组件



# 3安全传输平台部署流程

## 3.1部署安全传输平台的数据库解决方案

1）在win环境下，使用oracle客户端的oracle Enterprise Manger Consol工具，连接linux系统下的oracle数据库



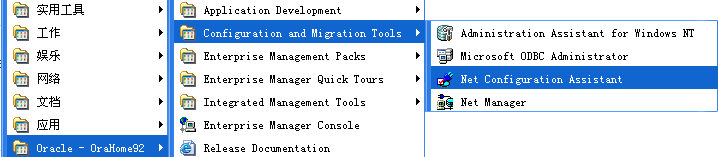
## 3.2部署SecMngServerAdmin管理控制终端

### 3.2.1 ODBC数据库配置

#### 3.2.1.1 终端网络服务名配置

管理终端使用ODBC机制，连接oracle数据库，在连接系统数据库前需要先配置ORACLE网络服务名。

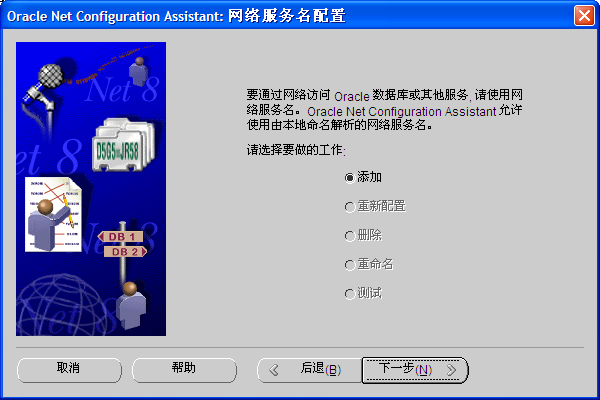
1. 运行“Net Configuration Assistant”



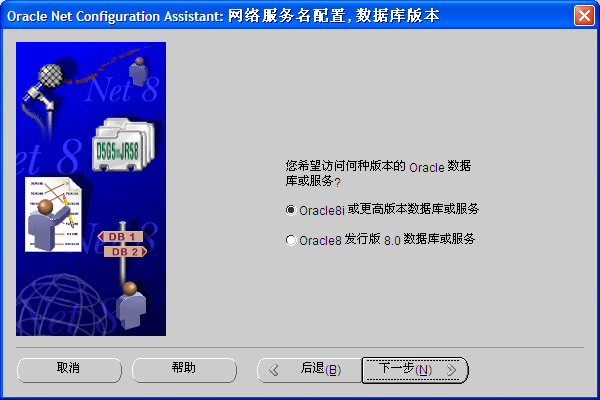
1. 选择“本地网络服务名配置”



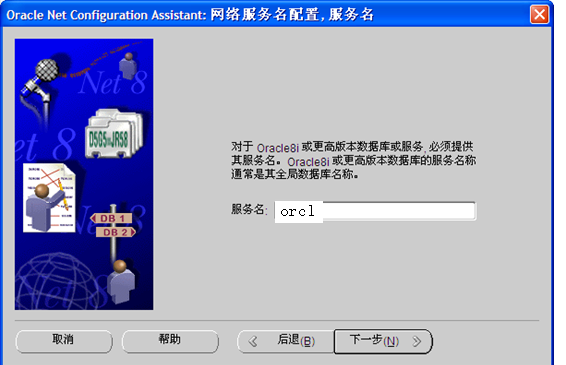
1. 选择“添加”



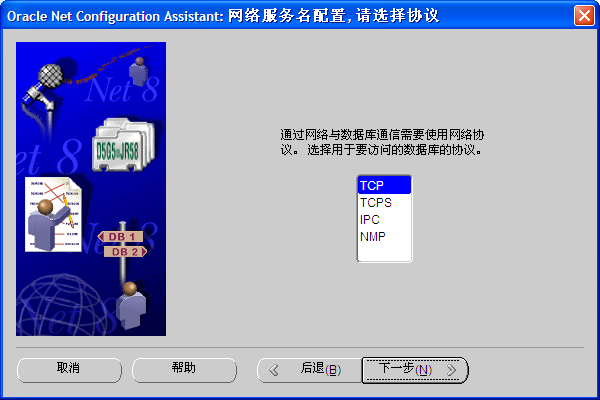
1. 选择“Oracle8i或更高版本数据库或服务”



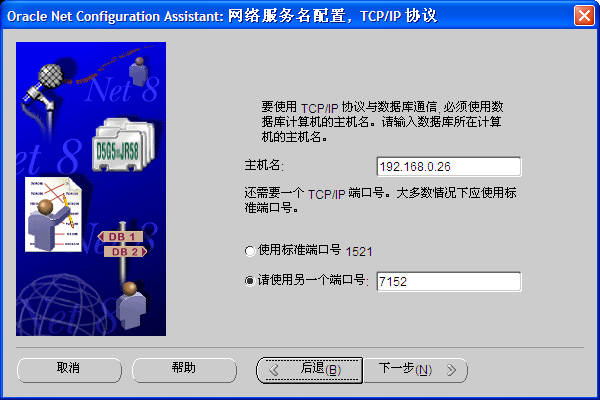
1. 输入服务名（与数据库服务器端一致）



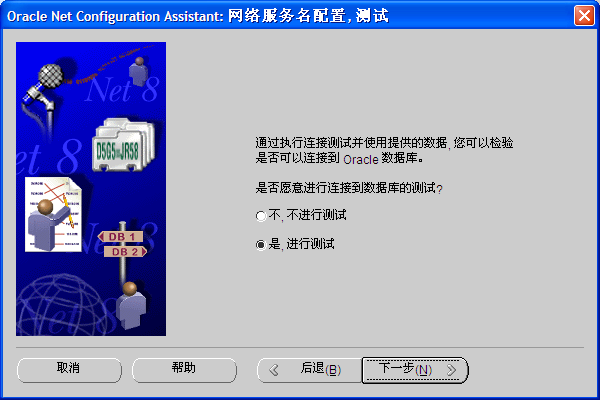
1. 选择“TCP”协议



1. 输入数据库服务器IP地址和端口



1. 测试数据库连接



1. 输出测试结果，完成配置。



#### 3.2.1.2系统终端的的ODBC环境配置

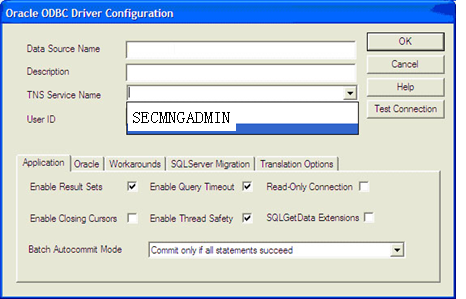
1. 选择“控制面板”->“管理工具”->“数据源(ODBC)”，选择系统DSN选项卡。



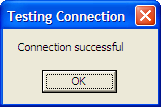
1. 选择“Oracle in OraHome90”，点击“完成”



1. 输入数据源名称（用户自定义），选择服务名，填写数据库用户名



1. 选择“Test Connection”进行数据库连接测试

### 3.2.2使用SecMngServerAdmin管理终端

### 3.2.3部署SecMngServer

创建用户user01

上传tar包

配置用户环境变量

测试数据库环境

注意：本应用程序，serverid 0001 clientid1111 默认

启动服务器

关闭服务器

查看系统共享内存

### 3.2.4部署SecMngClient

#### 3.2.4.1部署win下SecMngClient

保证win主机和linux服务器网络通常

#### 3.2.4.2部署linux下SecMngClient

保证win主机和linux服务器网络通常

### 3.2.5部署外联接口

创建用户user02

上传tar包

配置用户环境变量

测试数据库环境

注意：本应用程序，serverid 0001 clientid1111 默认

测试外联接口

查看系统共享内存

## 4安全传输平台项目的外延

根据项目和行业技能结合程度，可把项目分成如下几个等级：

1）基础设置类（为其他信息系统提供支撑类项目）

2）行业应用模型类（电信、石化、石油、政府类项目）

3）现在新的发展趋势类（大数据项目、分布式等）

安全传输平台的可塑性：

各行各业的学员都能把业务模型和安全传输平台相结合；因本项目是一个基础设施平台项目，可以和行业应用自由自合。

比如：

1）数据传输平台与烟草行业结合：烟草行业总部和分部安全数据传输平台

2）数据传输平台与石油石化行业结合：中石油财务大集中数据保证系统、中石化逻辑大集中数据安全系统

3）数据传输平台与教育部行业资源整合：中国教育部数据安全保证系统

4）数据传输平台与中国建设银行、中国人民银行业务模型做整合：银行类安全架构

5）对于基础差的学员，可以把配置管理终端换成各行各业的信息系统

6）对于没有工作经验，经历少的学员，可以把通用组件，做成一个工作经历

7）对于有工作经验的学员，可以把自己的从业经历，分解成各种linux服务器、MFC、QT客户端信息系统。

因为**安全传输平台**，囊括了基础组件技术、C/S客户端信息系统、C/S服务器端信息系统、行业应用。

# 5附录

## 5.1oracle数据库使用常见问题

1 oracle虚拟机需要固定IP,才能被外面的客户端连接上来

Root登陆linux机器

系统/首选项/网络连接

重启系统

2oracle用户启动oracle服务器

3 在linux环境中，用sqlplus工具访问oracle服务

在oracle用户下，用sqlplus访问oracle服务

必须用scott/aa @orcl这种形成访问成功，则后台服务器程序才能访问成功

在非oracle用户下(比如在test03)，用sqlplus访问oracle服务

必须用scott/aa@orcl这种形成访问成功，则后台服务器程序才能访问成功

chmod 777 /home/oracle\_11/app -R (root用户)

同时配置.bash\_profile

4 在win环境中，用sqlplus工具访问linux环境下的oracle服务

1 Ping 192.168.43.252

2 telnet 192.168.43.252 1521 防火墙没有把端口给封住

//防火墙 linux服务器 1521 端口 放开



3 两个配置文件

tnsnames.ora

listener.ora

5 oracle所在主机的ip被别人占用了,操作者不知道

## 5.2 oracle的12154错误排查

sqlplus scott/aa@orcl

1 test03用其他用户不能访问oracle问题排查

SQL\*Plus: Release 11.2.0.1.0 Production on Mon Jul 6 06:48:12 2015

Copyright (c) 1982, 2009, Oracle. All rights reserved.

ERROR:

ORA-12154: TNS:could not resolve the connect identifier specified

ORA-12154 11.2.0.1.0 ORA-12154

2 解决方法

[oracle@localhost admin]$ pwd

/home/oracle\_11/app/oracle/product/11.2.0/db\_1/network/admin

[oracle@localhost admin]$ ls

看看

listener.ora ===》服务器侦听服务配置

shrept.lst

tnsnames.ora ====》客户端连接服务器配置文件 wbm01客户使用这个文件连接服务

samples

sqlnet.ora

要保证wbm01用户能访问这个目录：ADR\_BASE = /home/oracle\_11/app

3 解决步骤

root用

chomd 775 /home/oracle\_11/app

====>

[wbm01@localhost app]$ cd /home/oracle\_11/app

[wbm01@localhost app]$ pwd

/home/oracle\_11/app

[wbm01@localhost app]$ ls

admin cfgtoollogs checkpoints diag flash\_recovery\_area oracle oradata oradiag\_oracle

[wbm01@localhost app]$ cd admin/

-bash: cd: admin/: 权限不够

[wbm01@localhost app]$

Linux服务器的配置 listener.ora

|  |
| --- |
| LISTENER =  (DESCRIPTION\_LIST =  (DESCRIPTION =  (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))  (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))  )  )  SID\_LIST\_LISTENER =  (SID\_LIST =  (SID\_DESC =  (GLOBAL\_DBNAME = orcl)  (ORACLE\_HOME = /home/oracle\_11/app/oracle/product/11.2.0/db\_1)  (SID\_NAME = orcl)  )  )  ADR\_BASE\_LISTENER = /home/oracle\_11/app |

Win机器的tnsnames.ora

|  |
| --- |
| # tnsnames.ora Network Configuration File: c:\Oracle\product\10.1.0\Client\_1\NETWORK\ADMIN\tnsnames.ora  # Generated by Oracle configuration tools.  ORCL\_192.168.32.253 =  (DESCRIPTION =  (ADDRESS\_LIST =  (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.32.253)(PORT = 1521))  )  (CONNECT\_DATA =  (SID = orcl)  (SERVER = DEDICATED)  )  )  SECMNGADEMIN =  (DESCRIPTION =  (ADDRESS\_LIST =  (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.32.253)(PORT = 1521))  )  (CONNECT\_DATA =  (SERVICE\_NAME = orcl)  )  ) |