学习目标

1. 复习Linux系统编程相关知识点
    - 进程间通信
    - 多线程
    - 套接字通信
    - 数据库
    - Qt
    - shell脚本
    - ...
2. 锻炼快读阅读代码的能力
3. 锻炼对封装好的API的快速上手能力
4. 项目解耦合的解决思路
    a. 高内聚，低耦合
5. 锻炼处理问题的逻辑思维能力
    - 重点:熟悉业务流程

1. 项目简介

1. 项目名称:
    - 数据安全传输基础设施平台
        - 名字不能用
2. 项目适用场景
    - 网点相关
        - 数据传输,消息加密
        - 有级联关系
            - 1:N
                - 树
            - N:N
                - 图
        - 身份鉴别
    - 秘钥相关
        - 秘钥更换(手动,自动)
        - 秘钥异常处理
        - 秘钥分发,校验等
    - 易用性
        - 耦合度低
        - 使用成本低
        - 部署简单
3. 项目要求:
    - 数据安全传输基础设施平台项目.doc
        - 参看第二章
4. 开发流程
    - 第三章
5. 需求分析
    - 学完项目之后总结,用自己的话进行描述
    - 用户需求 ----> 给出可行性方案
        - 功能模块划分
        - 功能模块的对接
        - 业务流程的串联
        - 设计的核心理念
            - 第三方应用改动最小
            - 部署机动灵活
            - 满足社会的各种需求
6. 总体设计特点:
    - 规范化:严格遵循各种相关规范设计。

- 独立性:系统各子系统间互相独立，在保持系统间接口的前提下，各系统间的升级互不干扰。
- 最小耦合性:各子系统进行严格功能分解，每个子系统负责单纯的功能，互不干扰。
- 开放性：系统遵循开放的业界标准。
- 兼容性：兼容各种硬件平台、软件平台、密码设备。
- 灵活性：充分考虑未来业务、技术上的需求，在业务和技术变化时，可平滑升级。

7. 安全相关的知识
   - 对称加密
   - 非对称加密

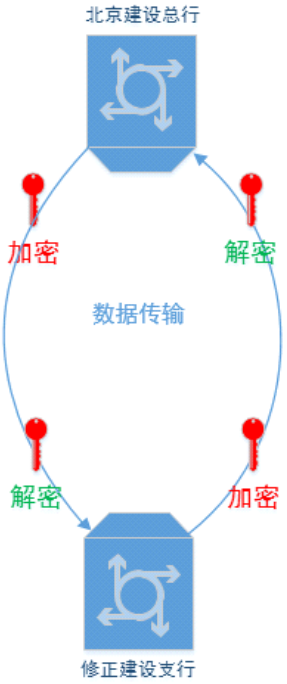
2. 数据的加密和解密

1. 加密三要素

- 明文/密文
- 算法
  - 不需要我们写
  - 直接用现成的
- 秘钥
  - 程序猿生成
    - 就是一个字符串，越长安全
  - 原始数据：520
    - 加密：110(秘钥)
      - 520+110 = 630(密文)
    - 拿到原始数据：算法+秘钥(630-110=520(明文))

2. 常用加密方式

- 对称加密
  - 特点：
    - 加解密使用的是同一个秘钥
    - 加密速度快，效率高(相对，非对称)
    - 适合加密大文件/大数据
    - 加密强度不高(相对于非对称加密)



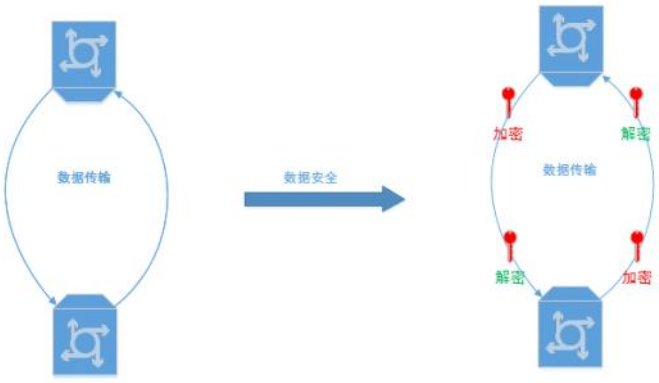
    - 秘钥分发困难
- 非对称加密
  - 特点:
    - 加解密使用的是不同的秘钥
      - 公钥
        - 可以向外公开的
      - 私钥
        - 不能公开
        - 数据属于谁，数据对谁更重要，谁就那私钥
      - 加解密方式:
        - 如果使用公钥加密，私钥解密
        - 如果是私钥加密，公钥解密
    - 加密速度慢，效率低
    - 适合加密小文件/数据
    - 加密强度高
    - 秘钥分发容易
  - 场景分析:
    - 信息加密
      - A写数据,发送给B，信息只允许B读
        - A发送数据：公钥
        - B接收读数据：私钥
    - 登录认证
      - 客户端要登录,连接服务器，向服务器请求个人数据
        - 客户端：私钥
        - 服务器：公钥

- 数字签名(表明信息没有受到伪造，确实是信息拥有者发出来的，附在信息原文的后面)
  - 签名的人：私钥
  - 读信息的人：公钥
- 网银EKY(U盾)
  - 个人：私钥
  - 银行：公钥

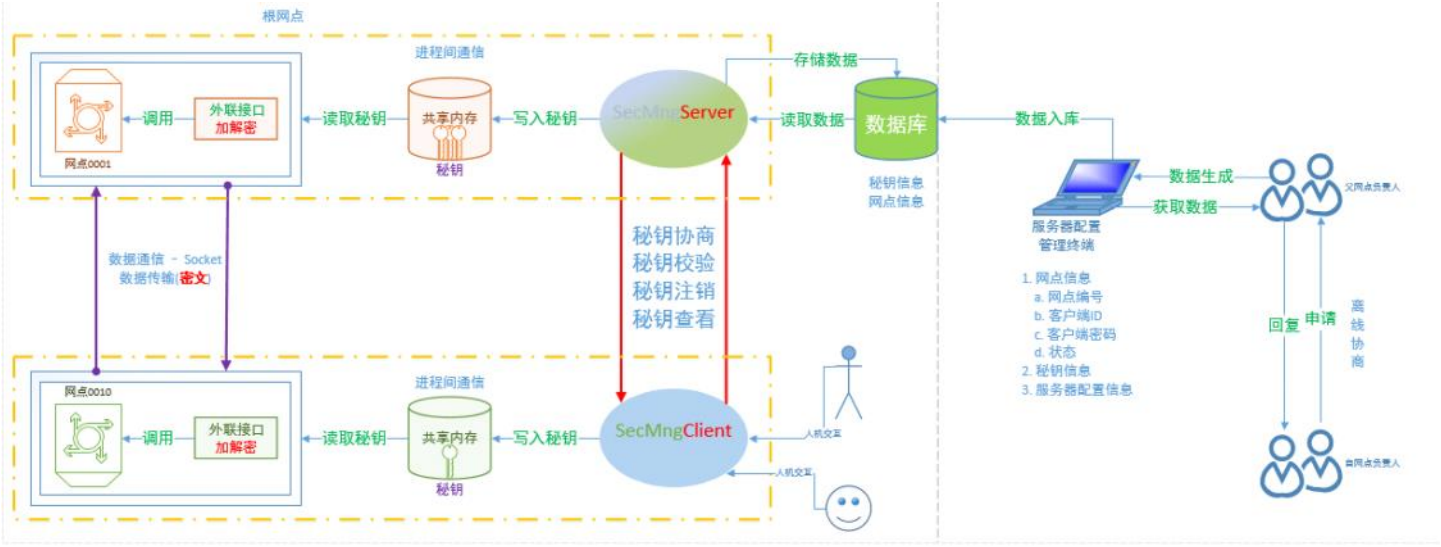
3. 知识点拓展 -- 常用的加密算法：
   - 对称加密：
     - DES/3DES
     - TDEA
     - Blowfish
     - RC2/RC4/RC5
     - IDEA
     - SKIPJACK
     - AES
   - 非对称加密：
     - RSA(数字签名和密钥交换)
     - ECC（椭圆曲线加密算法）
     - Diffie-Hellman(DH,密钥交换)
     - El Gamal(数字签名)
     - DSA（数字签名）
   - Hash 算法：
     - MD2/MD4/MD5
     - HAVAL
     - SHA-1/SHA3/SHA256/SHA512
     - RipeMD
     - WHIRLPOOL
     - HMAC

3. 项目架构图

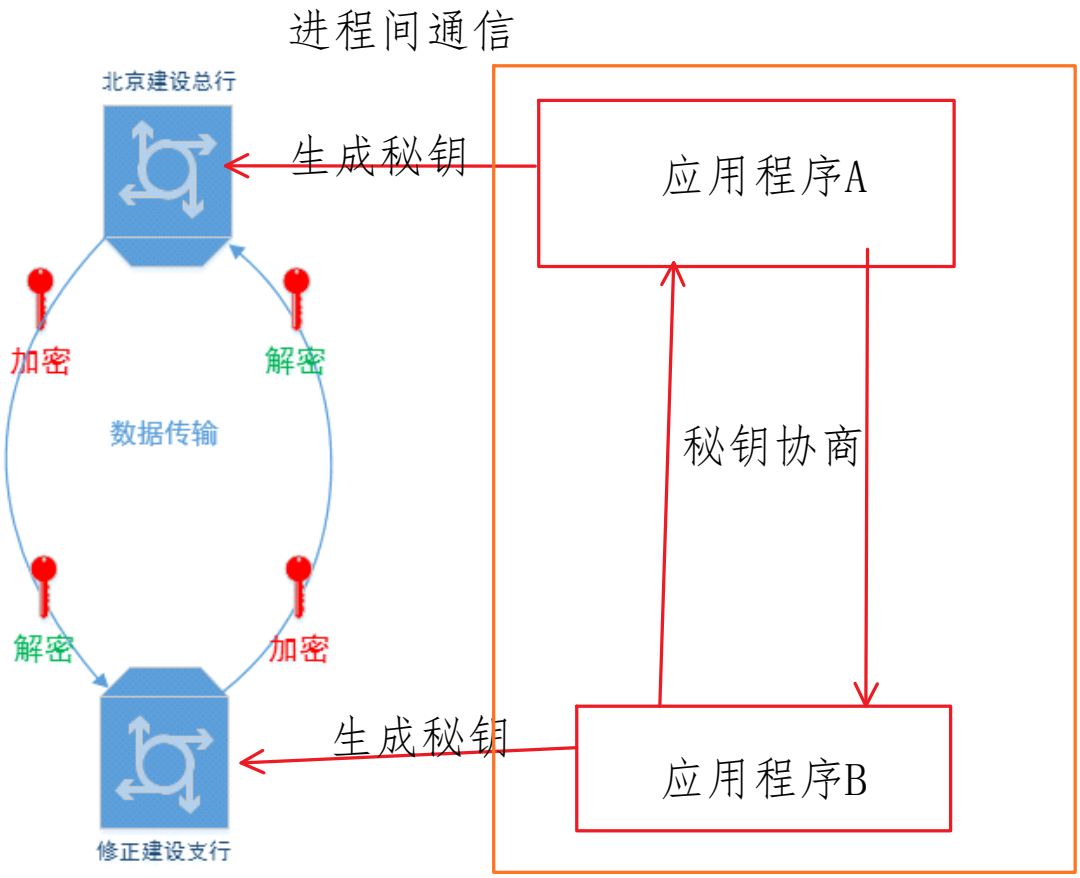
1. 两个系统进行网络通信



单服务器/客户端(1:1)关系图详解



--- 秘钥协商



前提：采用对称加密方式加密

1. 建设总行和修正分行各自使用同样的算法生成秘钥
    - 可行
    - 程序冗余
    - 维护困难
2. 通信的时候是否可以携带秘钥?
    - 不行，秘钥信息容易被拦截
3. 解决方案
    - A端生成一个随机数abc
    - B端生成一个随机数123
    - AB互相把数据发送给对方
        - A：abc123
        - B：abc123
    - AB两端将最终合成的数据当做秘钥
    - A -> 数据给到总行
    - B -> 数据给到支行
4. 思考:

- 将秘钥协商的模块做到银行系统中好不好?

4. 项目整体的模块划分

项目主要四个组成部分:

1. 基础组件模块
    - 报文编解码组件
        - 并不是用于加密的
        - 实现数据的跨平台传输
    - 通信组件
        - socket
    - 共享内存
        - shm
        - 进程间通信
    - 数据库访问组件
        - api接口
2. 秘钥协商服务器 & 客户端
    - 服务器
    - 客户端

3. 图形界面 - Qt
    - 服务器配置管理终端
    - 秘钥协商客户端
        - 文字版(Linux版移植)
4. 加解密接口的封装 & 杂项

5. 连接oracle前的准备工作

1. 用户名和密码

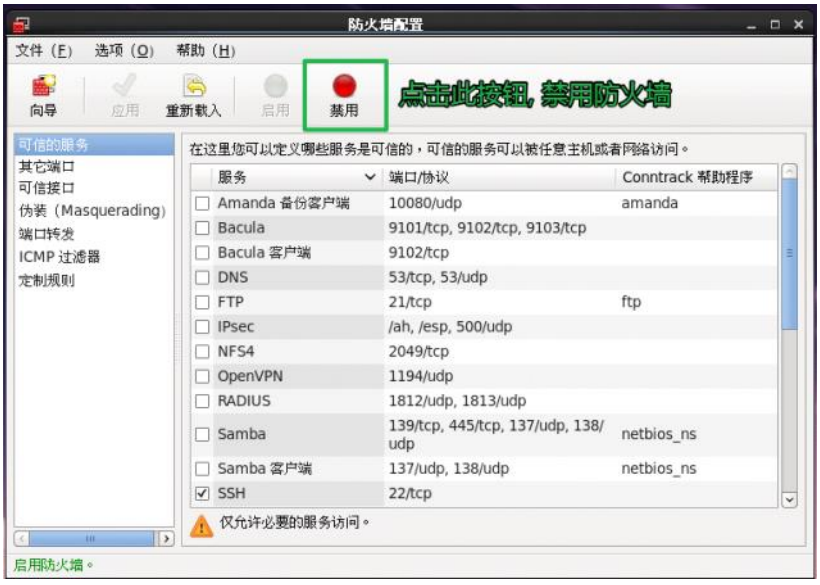
用户名	密码
root	123456
oracle	oracle

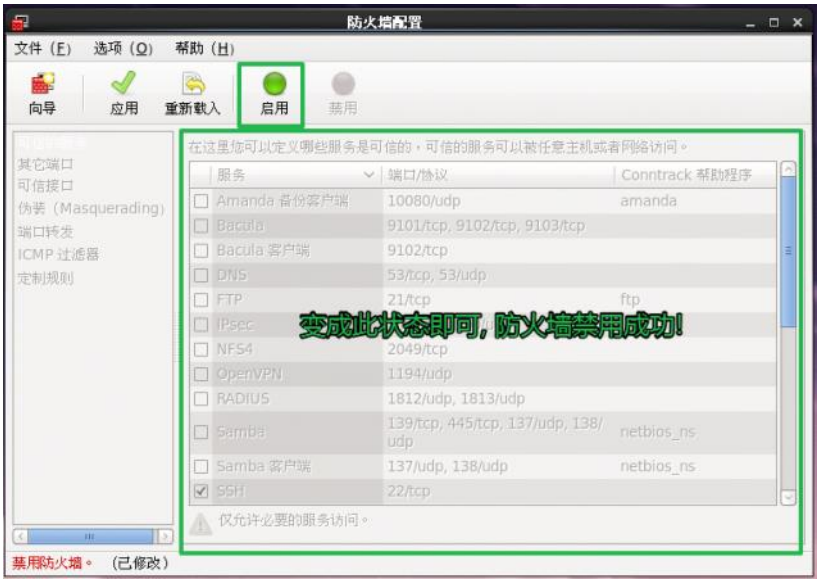
   - 创建新用户
     - useradd newUser;
   - 设置/修改密码
     - passwd newUser;
2. 必要的操作 - 关闭防火墙
   - 第一种方式:
     - 切换到root用户: su - root
       - - 的作用
         - 用户切换的时候系统使用的环境变量跟随用户改变
     - 执行命令:
       - service iptables stop
         - 临时生效, 系统重启需要再次设置

```
[root@localhost ~]# service iptables stop
iptables：清除防火墙规则：                                [确定]
iptables：将链设置为政策 ACCEPT：nat mangle filter        [确定]
iptables：正在卸载模块：                                  [确定]
[root@localhost ~]#
```

   - 第二种方式:
     - 使用root用户登录

abc
su root





- 注意事项:
  - oracle数据库配置好之后,不要关闭虚拟机. 虚拟机关闭后oracle数据库会关闭, 启动时需要再次设置.

6. 连接Oracle数据库

1. 启动Oracle数据库
   - 必须切换成Oracle用户
     - su - oracle
   - 借助sqlplus工具连接Oracle数据库
     - sqlplus /nolog
   - 使用管理员身份借助sqlplus连接oracle数据库
     - connect /as sysdba
       - 提示: Connected to an idle instance.
   - 启动Oracle数据库
     - startup;

```
SQL> startup;
ORACLE instance started.

Total System Global Area  780824576 bytes
Fixed Size                  2217424 bytes
Variable Size             524290608 bytes
Database Buffers          251658240 bytes
Redo Buffers                2658304 bytes
Database mounted.
Database opened.
```

   - 测试-执行一个sql语句
     - select * from scott.emp;
2. 关闭Oracle数据库
   - 关闭
     - shutdown immediate
   - 退出sqlplus连接的Oracle登录
     - quit
3. 启动TNS监听服务(必须)
   - 启动服务
     - lsnrctl start

```
[oracle@localhost ~]$ lsnrctl start

LSNRCTL for Linux: Version 11.2.0.1.0 - Production on 08-OCT-2017 02:58:52

Copyright (c) 1991, 2009, Oracle.  All rights reserved.

Starting /home/oracle_11/app/oracle/product/11.2.0/db_1/bin/tnslsnr: please wait...

TNSLSNR for Linux: Version 11.2.0.1.0 - Production
System parameter file is /home/oracle_11/app/oracle/product/11.2.0/db_1/network/admin/listener.ora
Log messages written to /home/oracle_11/app/diag/tnslsnr/localhost/listener/alert/log.xml
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=localhost)(PORT=1521)))

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 11.2.0.1.0 - Production
Start Date                08-OCT-2017 02:58:54
Uptime                    0 days 0 hr. 0 min. 0 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File   /home/oracle_11/app/oracle/product/11.2.0/db_1/network/admin/listener.ora
Listener Log File         /home/oracle_11/app/diag/tnslsnr/localhost/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=localhost)(PORT=1521)))
The listener supports no services
The command completed successfully
```

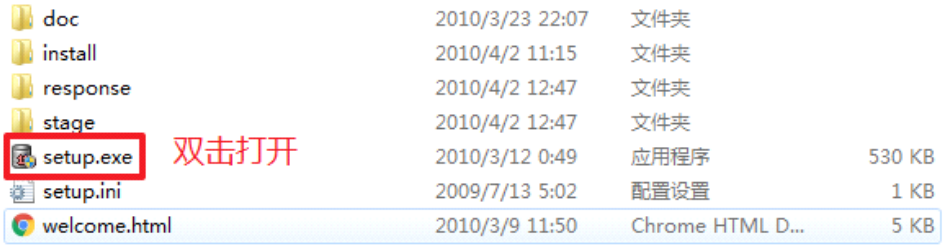
- TNS服务器如果启动失败，解决方案：
  - su - root 切换成root用户，执行 hostname oracle。
  - exit root用户，回到oracle下，重新执行 lsnrctl start命令启动

- 停止服务
  - lsnrctl stop

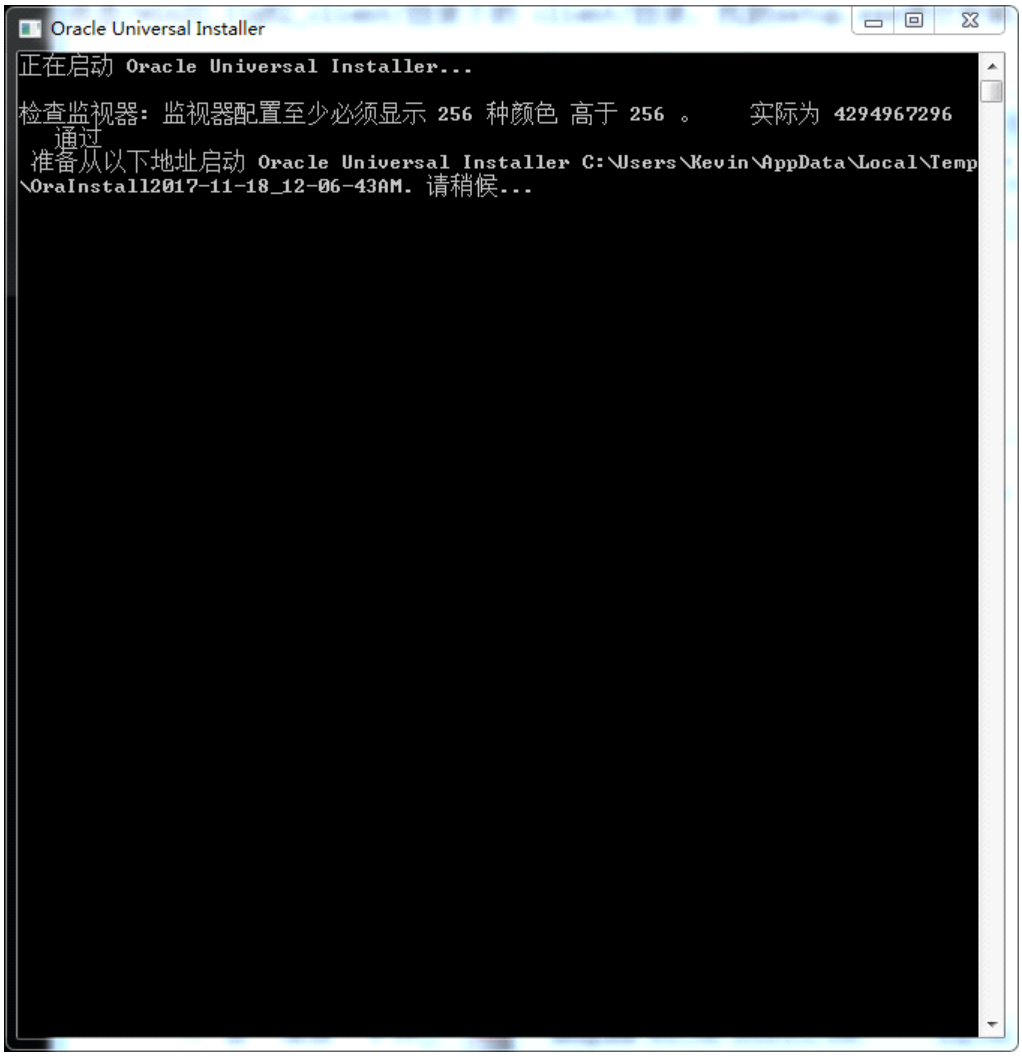
```
[oracle@localhost ~]$ lsnrctl stop

LSNRCTL for Linux: Version 11.2.0.1.0 - Production on 08-OCT-2017 03:00:42

Copyright (c) 1991, 2009, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC1521)))
The command completed successfully
```

7.win32_11gR2_client 安装

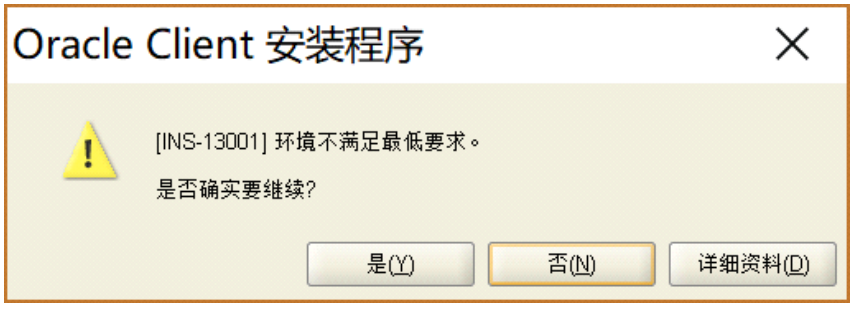
1. 运行setup.exe



2. 弹出黑窗口,等待

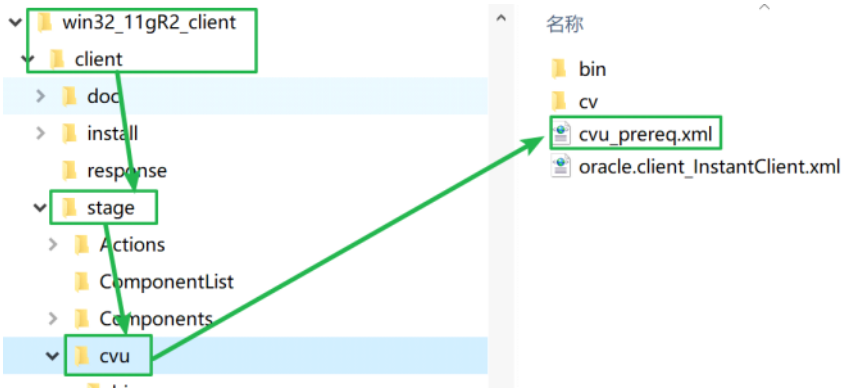


3. win10系统会弹出此对话框



4. 打开你的解压后的database文件夹，找到stage，然后cvu,找到

cvu_prereq.xml文件，用记事本打开，增添一下内容

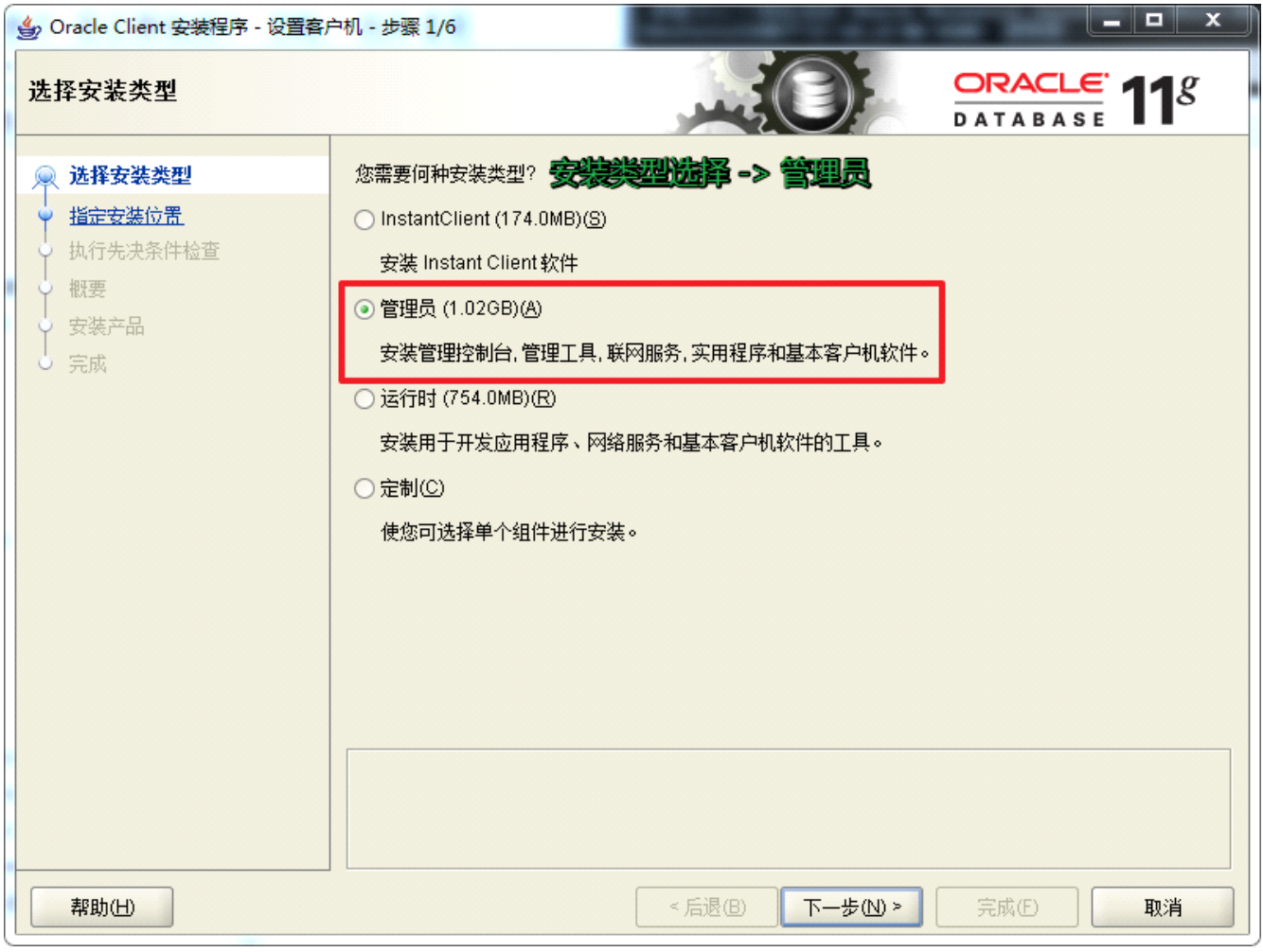



```
<OPERATING_SYSTEM RELEASE="6.2">
            <VERSION VALUE="3"/>
            <ARCHITECTURE VALUE="32-bit"/>
            <NAME VALUE="Windows 10"/>
            <ENV_VAR_LIST>
                <ENV_VAR NAME="PATH" MAX_LENGTH="1023" />
            </ENV_VAR_LIST>
</OPERATING_SYSTEM>
```

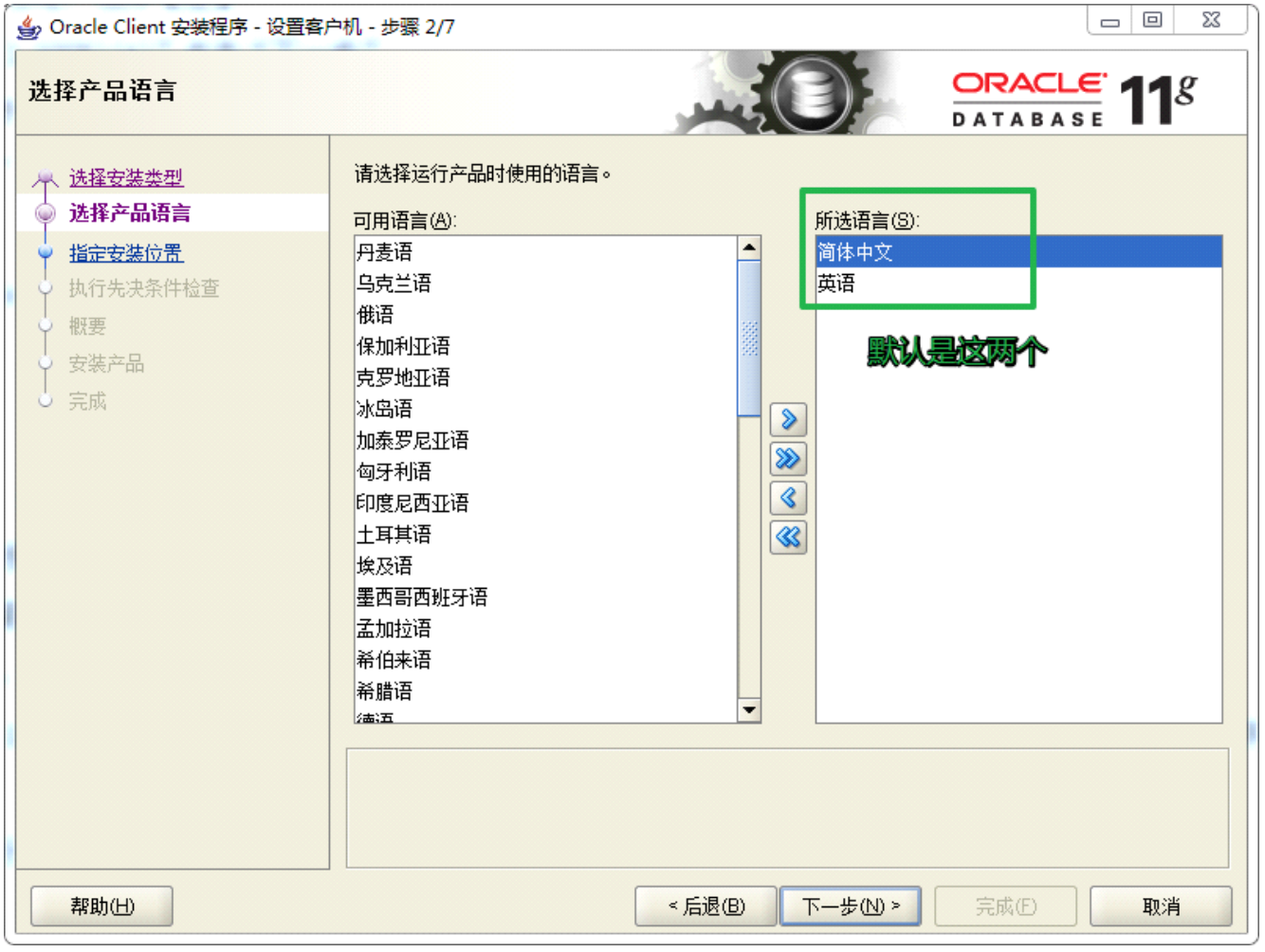
注：以上内容是在CERTIFIED_SYSTEMS标签中添加

```
<CERTIFIED_SYSTEMS>
        <OPERATING_SYSTEM RELEASE="5.0">
        </OPERATING_SYSTEM>
        <OPERATING_SYSTEM RELEASE="5.1">
        </OPERATING_SYSTEM>
        <OPERATING_SYSTEM RELEASE="5.2">
        </OPERATING_SYSTEM>
        <OPERATING_SYSTEM RELEASE="6.0">
        </OPERATING_SYSTEM>
        <OPERATING_SYSTEM RELEASE="6.0">
        </OPERATING_SYSTEM>
    <OPERATING_SYSTEM RELEASE="6.1">
        </OPERATING_SYSTEM>
    <OPERATING_SYSTEM RELEASE="6.2">
          <VERSION VALUE="3"/>  64位安装包，修改为64-bit
          <ARCHITECTURE VALUE="32-bit"/>
          <NAME VALUE="Windows 10"/>
          <ENV_VAR_LIST>
              <ENV_VAR NAME="PATH" MAX_LENGTH="1023" />
          </ENV_VAR_LIST>
    </OPERATING_SYSTEM>
</CERTIFIED_SYSTEMS>
```

5. 选择安装类型:管理员

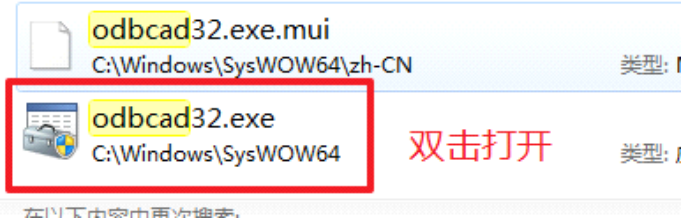

Oracle Client 安装程序 - 设置客户机 - 步骤 1/6
选择安装类型
ORACLE 11g DATABASE
选择安装类型
指定安装位置
执行先决条件检查
概要
安装产品
完成
您需要何种安装类型? 安装类型选择 -> 管理员
InstantClient (174.0MB)(S)
安装 Instant Client 软件
管理员 (1.02GB)(A)
安装管理控制台, 管理工具, 联网服务, 实用程序和基本客户机软件。
运行时 (754.0MB)(R)
安装用于开发应用程序、网络服务和基本客户机软件的工具。
定制(C)
使您可选择单个组件进行安装。
帮助(H)
< 后退(B)
下一步(N) >
完成(F)
取消

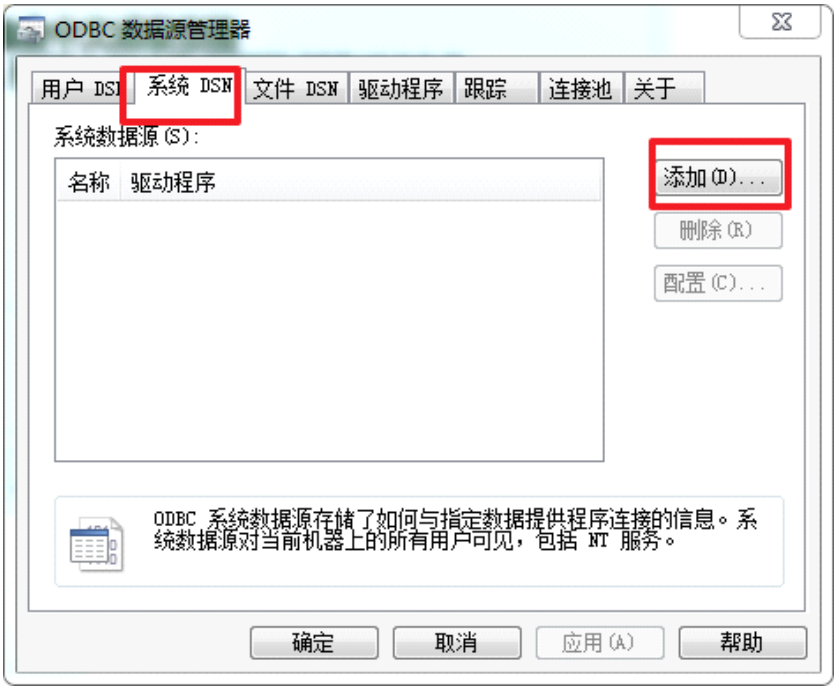
6. 选择语言

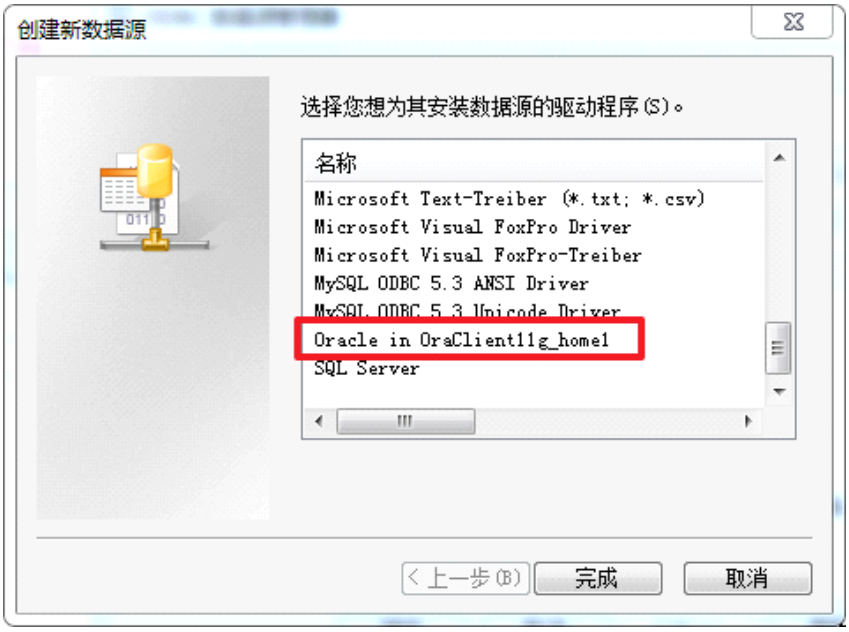

Oracle Client 安装程序 - 设置客户机 - 步骤 2/7
选择产品语言
ORACLE 11g DATABASE
选择安装类型
选择产品语言
指定安装位置
执行先决条件检查
概要
安装产品
完成
请选择运行产品时使用的语言。
可用语言(A):
丹麦语
乌克兰语
俄语
保加利亚语
克罗地亚语
冰岛语
加泰罗尼亚语
匈牙利语
印度尼西亚语
土耳其语
埃及语
墨西哥西班牙语
孟加拉语
希伯来语
希腊语
所选语言(S):
简体中文
英语
默认是这两个
帮助(H)
< 后退(B)
下一步(N) >
完成(F)
取消

7. 指定安装目录


Oracle Client 安装程序 - 设置客户机 - 步骤 3/7
指定安装位置
ORACLE DATABASE 11g
选择安装类型
选择产品语言
指定安装位置
执行先决条件检查
概要
安装产品
完成
指定用于放置所有 Oracle 软件以及与配置相关的文件的 Oracle 基目录路径。此位置是 Oracle 基目录。
Oracle 基目录(O): C:\Oracle
浏览(R)...
指定用于存储 Oracle 软件文件的位置。此位置是 Oracle 主目录。
软件位置(S): C:\Oracle\product\11.2.0\client_1
浏览(W)...
1. 安装目录中不能包含中文或者空格
2. 必须安装到 C 盘, 否则会影响数据源的创建(ODBC)
帮助(H)
< 后退(B)
下一步(N) >
完成(F)
取消

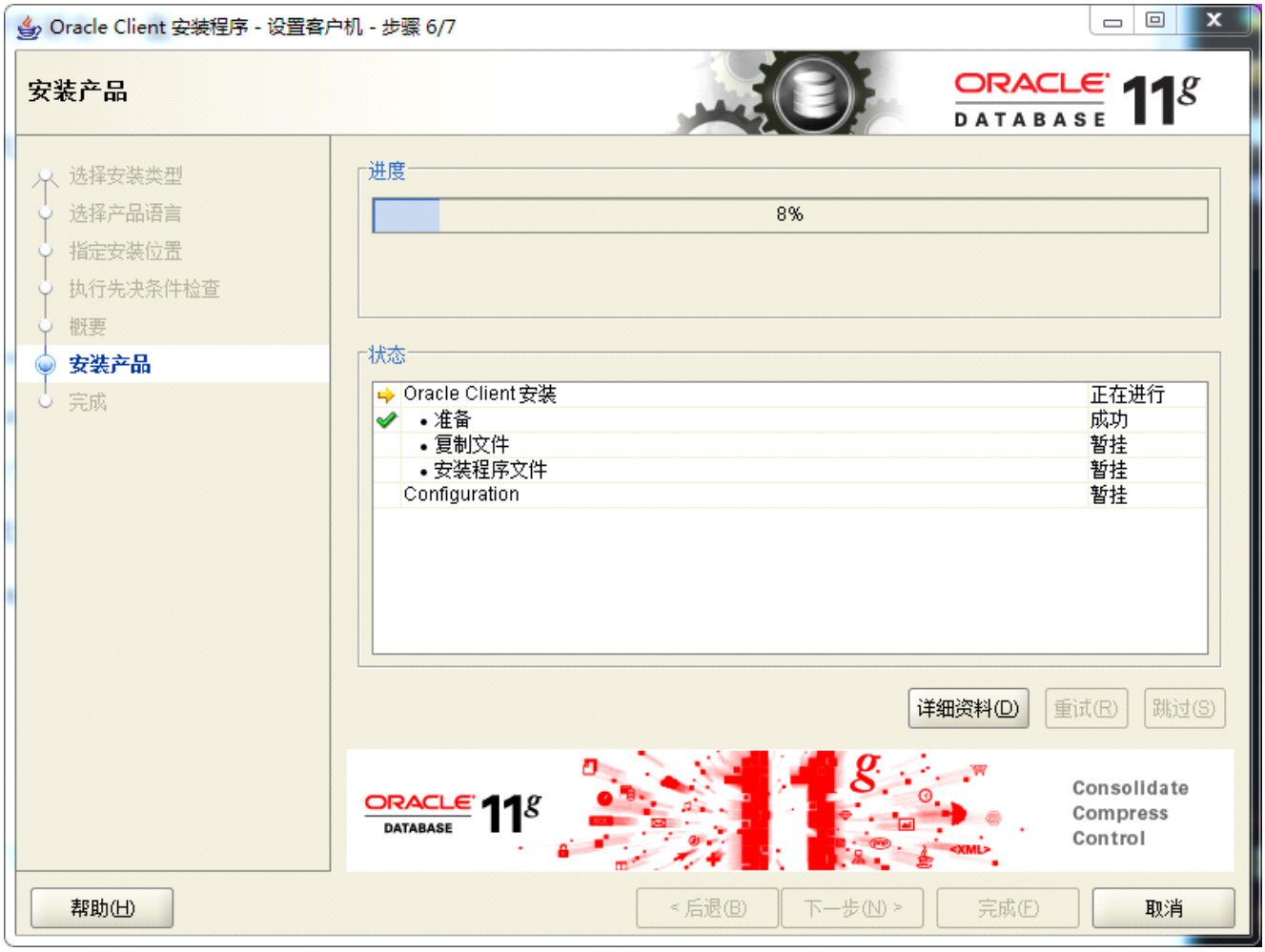
- 
odbcad32.exe.mui
C:\Windows\SysWOW64\zh-CN
odbcad32.exe
C:\Windows\SysWOW64
双击打开

- 
ODBC 数据源管理器
用户 DSN
系统 DSN
文件 DSN
驱动程序
跟踪
连接池
关于
系统数据源(S):
名称
驱动程序
添加(D)...
删除(R)
配置(C)...
ODBC 系统数据源存储了如何与指定数据提供程序连接的信息。系统数据源对当前机器上的所有用户可见，包括 NT 服务。
确定
取消
应用(A)
帮助

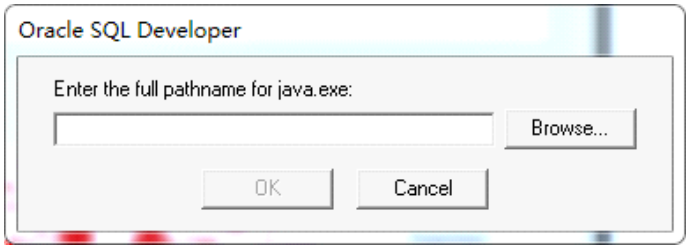
- 
创建新数据源
选择您想为其安装数据源的驱动程序(S)。
名称
Microsoft Text-Treiber (*.txt; *.csv)
Microsoft Visual FoxPro Driver
Microsoft Visual FoxPro-Treiber
MySQL ODBC 5.3 ANSI Driver
MySQL ODBC 5.3 Unicode Driver
Oracle in OraClient11g_home1
SQL Server
< 上一步(B)
完成
取消

8. 检测安装环境

9. 安装客户端
   - 安装期间弹出 “.NET Framework ”相关提示，跳过即可。

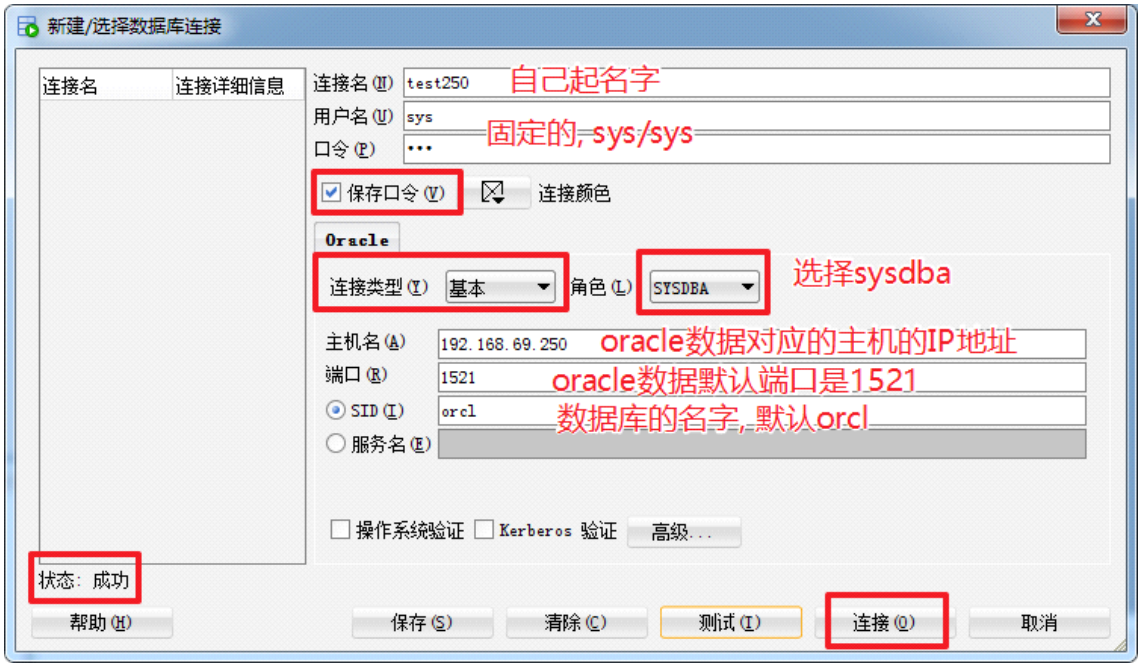


10. 安装完成之后,打开SQL Developer

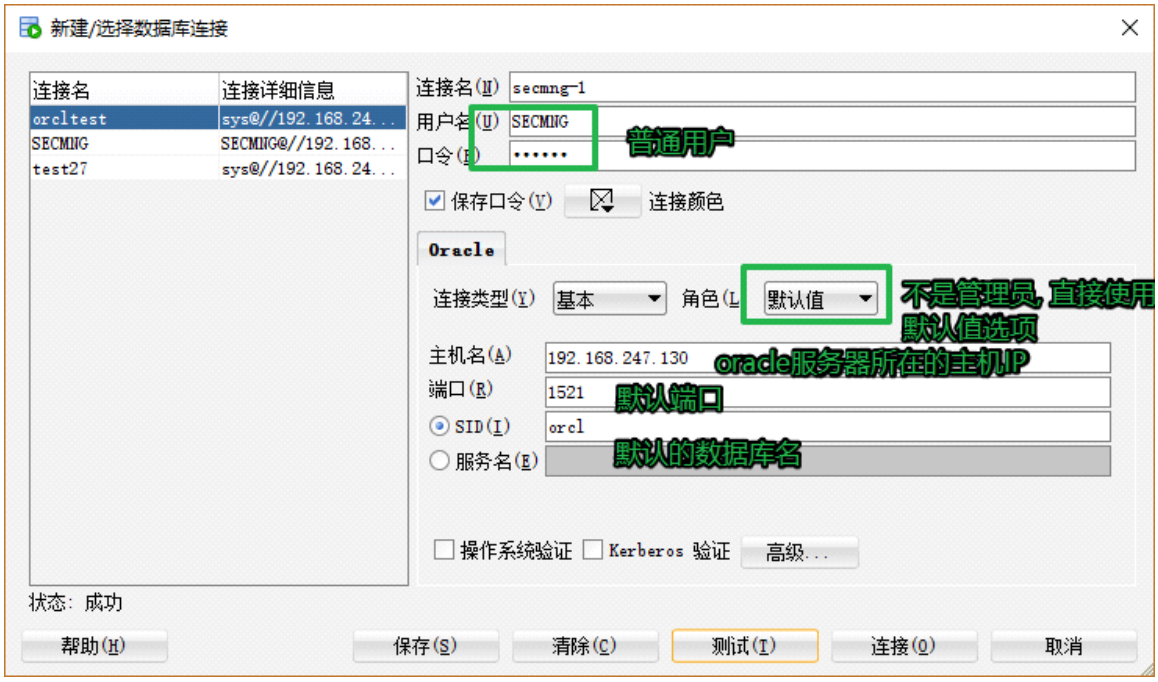


设置数据库连接:

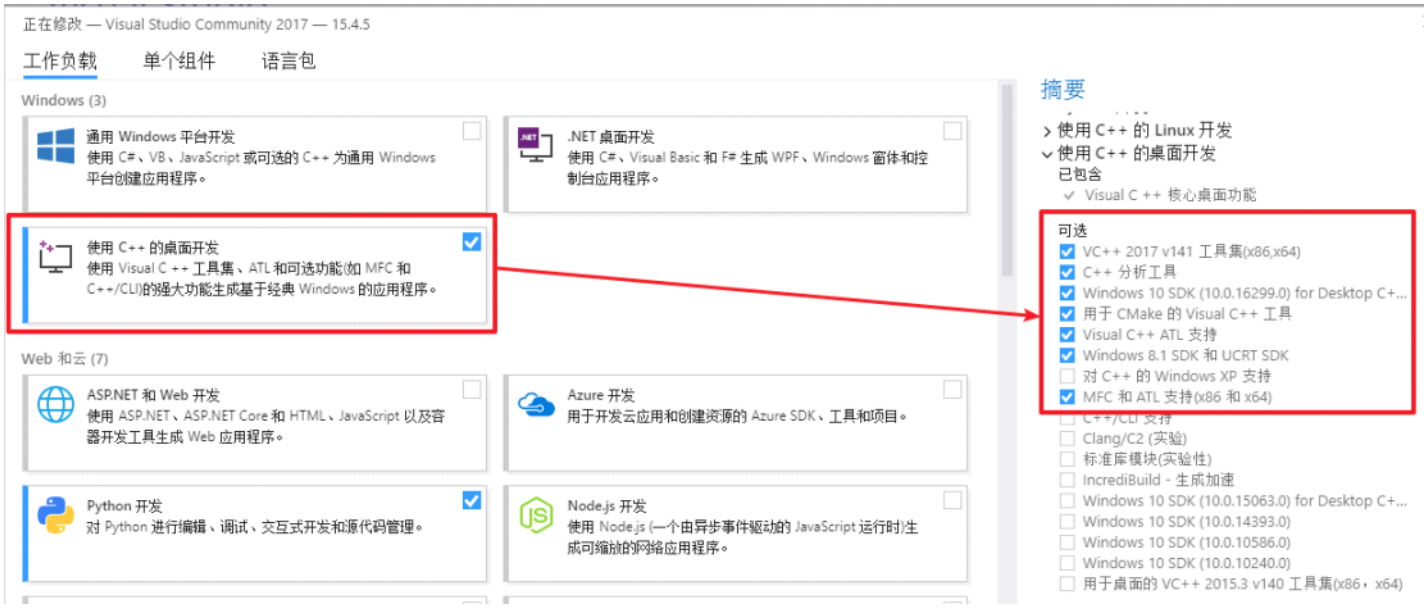
- 使用管理员身份连接oracle数据库

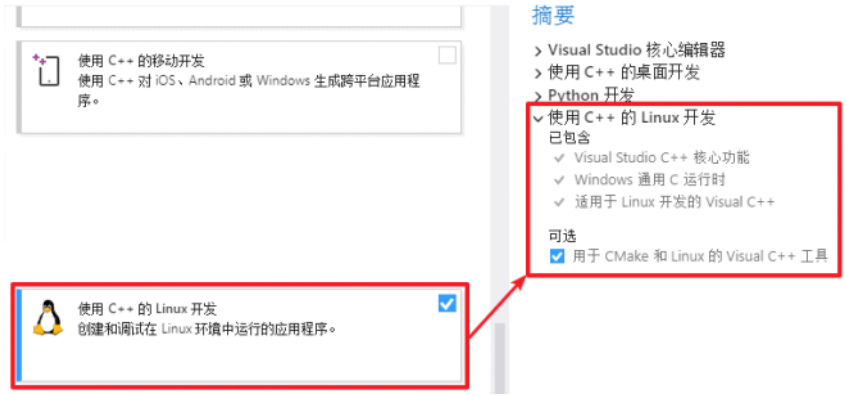

新建/选择数据库连接
连接名
连接详细信息
连接名(N) test250
自己起名字
用户名(U) sys
固定的,sys/sys
口令(P)
保存口令(V)
连接颜色
Oracle
连接类型(Y) 基本
角色(L) SYSDBA
选择sysdba
主机名(A) 192.168.69.250
oracle数据对应的主机的IP地址
端口(R) 1521
oracle数据默认端口是1521
SID(I) orcl
数据库的名字,默认orcl
服务名(E)
操作系统验证
Kerberos 验证
高级...
状态: 成功
帮助(H)
保存(S)
清除(C)
测试(T)
连接(O)
取消

- 如果是普通用户登录

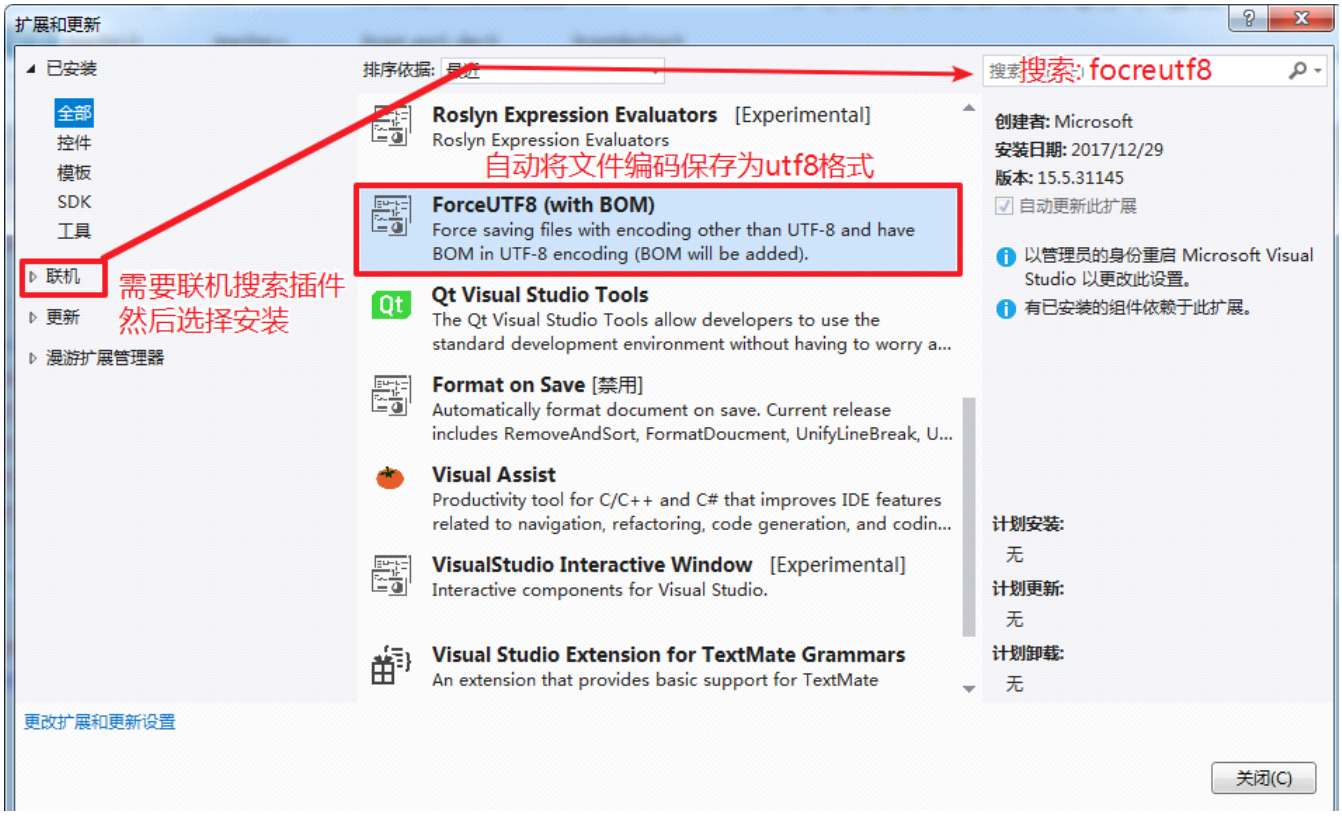

新建/选择数据库连接
连接名
连接详细信息
orcltest
sys@//192.168.24...
SECMNG
SECMNG@//192.168...
test27
sys@//192.168.24...
连接名(N) secmng-1
用户名(U) SECMNG
普通用户
口令(P)
保存口令(V)
连接颜色
Oracle
连接类型(Y) 基本
角色(L) 默认值
不是管理员,直接使用
默认值选项
主机名(A) 192.168.247.130
oracle服务器所在的主机IP
端口(R) 1521
默认端口
SID(I) orcl
服务名(E)
默认的数据库名
操作系统验证
Kerberos 验证
高级...
状态: 成功
帮助(H)
保存(S)
清除(C)
测试(T)
连接(O)
取消

VS2017 安装



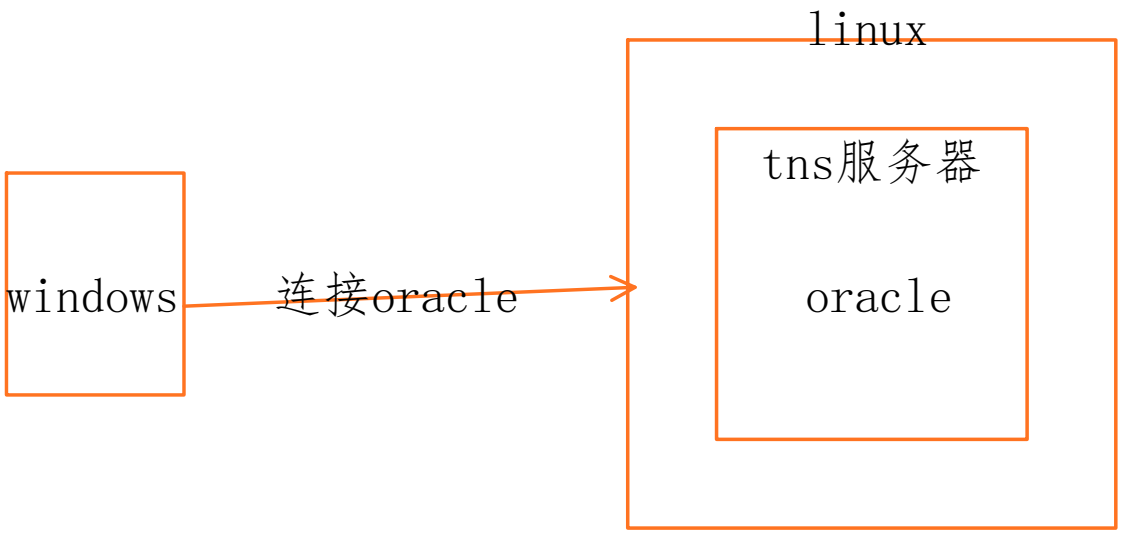


菜单栏: 工具 -> 扩展更新



tns服务器

2018年3月2日 15:23



必须开启linux上的tns服务器，才能在外边访问oracle数据库

- 开启的命令：
  - lsnrctl start
  - 命令执行失败：
    - 切换到root用户：su - root
    - 执行一个命令：hostname oracle
    - 退出root用户：exit
    - 再次执行lsnrctl start

启动oracle数据库

- sqlplus /nolog
- conn /as sysdba
- startup

- sqlplus
- sys/sys as sysdba

创建用户

2018年3月2日　　16:23

1. 命令:
    - useradd 新用户名
        - 新用户名不能有大写字母
        - useradd test
        - 修改test用户的密码
            - passwd test

if(a>0)
if [ ]
.命令 == source