Oracle安全数据系统架构全接触[14] PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/275/2021_2022_Oracle_E5_AE_89_E5_c67_275010.htm 词组“ ora_test_osoper_d ”表示组的名字.词组“ NONE ”表示这个组的密码.数字1表示这个组的ID.接下来的是这个组的成员。前两行是Oracle服务器角色的例子，使用test作为sid，osoper和osdba作为Oracle服务器角色的名字。osoper是分配给用户的缺省角色，osdba带有WITH ADMIN选项。为了使这些数据库角色起作用，您必须shutdown您的数据库系统，设置Oracle数据库参数文件initORACLE_SID.ora中os_roles参数为True，然后重新启动您的数据库。如果您想让这些角色有connect internal权限，运行orapwd为这些角色设置密码。当您尝试connect internal时，您键入的密码表示了角色所对应的权限。 SQL*DBA命令的安全性: 如果您没有SQL*PLUS应用程序，您也可以使用SQL*DBA作SQL查权限相关的命令只能分配给Oracle软件拥有者和DBA组的用户，因为这些命令被授予了特殊的系统权限。 (1) startup (2) shutdown (3) connect internal 数据库文件的安全性: Oracle软件的拥有者应该这些数据库文件($ORACLE_HOME/dbs/*.dbf)设置这些文件的使用权限为0600:文件的拥有者可读可写，同组的和其他组的用户没有写的权限。 Oracle软件的拥有者应该拥有包含数据库文件的目录，为了增加安全性，建议收回同组和其他组用户对这些文件的可读权限。 网络安全性: 当处理网络安全性时，以下是额外要考虑的几个问题。 (1) 在网络上使用密码在网上的远端用户可以通过加密或不加密方式键入密码，当您用不加密

方式键入密码时，您的密码很有可能被非法用户截获，导致破坏了系统的安全性。 (2) 网络上的DBA权限控制您可以通过下列两种方式对网络上的DBA权限进行控制: A 设置成拒绝远程DBA访问. B 通过orapwd给DBA设置特殊的密码。 建立安全性策略: 系统安全性策略 (1)管理数据库用户:数据库用户是访问Oracle数据库信息的途径，因此，应该很好地维护管理数据库用户的安全性。按照数据库系统的大小和管理数据库用户所需的工作量，数据库安全性管理者可能只是拥有create，alter，或0drop数据库用户的一个特殊用户，或者是拥有这些权限的一组用户，应注意的是，只有那些值得信任的个人才应该有管理数据库用户的权限。 (2) 用户身份确认:数据库用户可以通过操作系统，网络服务，或数据库进行身份确认，通过主机操作系统进行用户身份认证的优点有: A 用户能更快，更方便地联入数据库. B 通过操作系统对用户身份确认进行集中控制:如果操作系统与数据库用户信息一致，Oracle无须存储和管理用户名以及密码. C 用户进入数据库和操作系统审计信息一致。 (3) 操作系统安全性 A 数据库管理员必须有create和0delete文件的操作系统权限. B 一般数据库用户不应该有create或0delete与数据库相关文件的操作系统权限. C 如果操作系统能为数据库用户分配角色，那么安全性管理者必须有修改操作系统帐户安全性区域的操作系统权限。