教你利用组来保证Oracle数据库的安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E6_95_99_E4_BD_A0_E5_88_A9_E7_c102_142830.htm 在操作系统下建立用户组是保证数据库安全性的一种有效方法。Oracle程序为了安全性目的一般分为两类：一类所有的用户都可执行，另一类只DBA可执行。在Unix环境下组设置的配置文件是/etc/group,关于这个文件如何配置，请参阅Unix的有关手册。 保证安全性的几种方法： (1) 在安装OracleServer前，创建数据库管理员组(DBA)而且分配root和Oracle软件拥有者的用户ID给这个组。DBA能执行的程序只有710权限。在安装过程中SQL*DBA系统权限命令被自动分配给DBA组。 (2) 允许一部分Unix用户有限制地访问Oracle服务器系统，增加一个由授权用户组的Oracle组，确保给Oracle服务器实用例程Oracle组ID，公用的可执行程序，比如SQL*Plus，SQL*Forms等，应该可被这组执行，然后该这个实用例程的权限为710，它将允许同组的用户执行，而其他用户不能。 (3) 改那些不会影响数据库安全性的程序的权限为711。注：在我们的系统中为了安装和调试的方便，Oracle数据库中 的两个具有DBA权限的用户Sys和System的缺省密码是manager。为了您数据库系统的安全，我们强烈建议您该掉这两个用户的密码，具体操作如下：在SQL*DBA下键入： alter user sys indentified by password. alter user system indentified by password.其中password为您为用户设置的密码。 Oracle服务器实用例程的安全性 以下是保护Oracle服务器不被非法用户使用的几条建议： (1) 确保$ORACLE_HOME/bin目录下的所有程序的拥有权归Oracle

软件拥有者所有；(2) 给所有用户实用便程(sqiplus,sqiforms,exp,imp等)711权限，使服务器上所有的用户都可访问Oracle服务器；(3) 给所有的DBA实用例程(比如SQL*DBA)700权限。Oracle服务器和Unix组当访问本地的服务器时，您可以通过在操作系统下把Oracle服务器的角色映射到Unix的组的方式来使用Unix管理服务器的安全性，这种方法适应于本地访问。 在Unix中指定Oracle服务器角色的格式如下： ora_sid_role[_dla]其中sid是您Oracle数据库的oracle_sid；role 是Oracle服务器中角色的名字；d (可选)表示这个角色是缺省值；a (可选)表示这个角色带有WITH ADMIN选项，您只可以把这个角色授予其他角色，不能是其他用户。 以下是在/etc/group文件中设置的例子：
ora_test_osoper_d:NONE:1:jim,narry,scott
ora_test_osdba_a:NONE:3:pat
ora_test_role1:NONE:4:bob,jane,tom,mary,jim bin:
NONE:5:root,oracle,dba root:NONE:7:root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WITHADMIN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connectinternal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