Oracle安全数据系统架构全接触[15] 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_275009.htm 数据的安全性策略: 数据的生考虑应基于数据的重要性。如果数据不是很重要，那么数据的安全性策略可以稍稍放松一些。然而，如果数据很重要，那么应该有一谨慎的安全性策略，用它来维护对数据对象访问的有效控制。 用户安全性策略: (1) 一般用户的安全性: A 密码的安全性:如果用户是通过数据库进行用户身份的确认，那么建议使用密码加密的方式与数据库进行连接。这种方式的设置方法如下: 在客户端的oracle.ini文件中设置ora_encrypt_login数为true. 在服务器端的initORACLE_SID.ora文件中设置dbling_encypt_login参数为true。 B 权限管理:对于那些用户很多，应用程序和数据对象很丰富的数据库，应充分利用“角色”这个机制所带的方便性对权限进行有效管理。对于复杂的系统环境，“角色”能大大地简化权限的理。 (2) 终端用户的安全性: 您必须针对终端用户制定安全性策略。例如，对于一个有很多用户的大规模数据库，安全性管理者可以决定用户组分类为这些用户组创建用户角色，把所需的权限和应用程序角色授予每一个用户角色，以及为用户分配相应的用户角色。当处理特殊的应用要求时，安全性管理者也必须明确地把一些特定的权限要求授予给用户。您可以使用“角色”对终端用户进行权限管理。 数据库管理者安全性策略: (1) 保护作为sys和system用户的连接: 当数据库创建好以后，立即更改有管理权限的sys和system用户的密码，防止非法用户访问数据库。当作为sys和system用户连入数据库后，用户有强

大的权限用各种方式对数据库进行改动。 (2) 保护管理者与数据库的连接: 应该只有数据库管理者能用管理权限连入数据库，当以sysdba或startup，shutdown，和recover或数据库对象(例如create,0drop，和0delete等)进行没有任何限制的操作。 (3) 使用角色对管理者权限进行管理 应用程序开发者的安全性策略: (1) 应用程序开发者和他们的权限数据库应用程序开发者是唯一一类需要特殊权限组完成自己工作的数据库用户。开发者需要诸如create table,create，procedure等系统权限，然而，为了限制开发者对数据库的操作，只应该把一些特定的系统权限授予开发者。 (2) 应用程序开发者的环境: A 程序开发者不应与终端用户竞争数据库资源. B 用程序开发者不能损害数据库其他应用产品。 (3) free和controlled应用程序开发应用程序开发者有一下两种权限: A free development 应用程序开发者允许创建新的模式对象，包括table,index,procedure,package等，它允许应用程序开发者开发独立于其他对象的应用程序。 B controlled development 应用程序开发者不允许创建新的模式对象。所有需要table,indes procedure等都由数据库管理者创建，它保证了数据库管理者能完全控制数据空间的使用以及访问数据库信息的途径。但有时应用程序开发者也需这两种权限的混和。 (4) 应用程序开发者的角色和权限数据库安全性管理者能创建角色来管理典型的应用程序开发者的权限要求。 A create系统权限常常授予给应用程序开发者，以至于他们能创建他的数据对象。 B 数据对象角色几乎不会授予给应用程序开发者使用的角色。 (5) 加强应用程序开发者的空间限制作为数据库安全性管理者，您应该特别地为每个应用程序开发者设置以下的一些限制: A 开发者可以创建table或index的表空间.

B 在每一个表空间中，开发者所拥有的空间份额。应用程序管理者的安全在有许多数据库应用程序的数据库系统中，您可能需要一应用程序管理者，应用程序管理者应负责起以下的任务: a)为每一个应用程序创建角色以及管理每一个应用程序的角色. b)创建和管理数据库应用程序使用的数据对象. c)需要的话，维护和更新应用程序代码和Oracle的存储过程和程序包。 我相信有了以上的这些建议，作为一个Oracle的管理者绝对可以做好他本职的工作了。可是，我们再怎么努力，都始终得面对这样一个现实，那就是Oracle毕竟是其他人开发的，而我们却在使用。所以，Oracle到底有多少漏洞--我想这个不是你和我所能解决的。不过既然作为一篇讨论Oracle数据安全的文章，我认为有必要把漏洞这一块也写进去，毕竟这也是“ 安全 ”必不可少的一部分。呵呵! 所以…… 【Oracle漏洞举例】: Oracle9iAS Web Cache远程拒绝服务攻击漏洞(2002-10-28) Oracle 8.1.6的oidldapd中的漏洞 Oracle 9iAS OracleJSP 泄漏JSP文件信息漏洞 Linux ORACLE 8.1.5漏洞 想必我没有理由再往下举了，因为读者肯定已经从其他有效的途径得到了关于Oracle漏洞的最新情报。我这里就不再赘述了。总而言之一句话--“ Oracle数据安全是一个博大而又精深的话题.如果你没有耐心，就永远不会得到它的精髓之所在。 ”