Oracle数据安全面面观(2) PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/224/2021_2022_Oracle_E6_95_B0_E6_c102_224649.htm (二)来自内部的另外一个隐患--用户管理以及密码问题 在这里，其实作为一个差不多点的数据库管理员都很清楚，Oracle数据库本身就使用了很多种手段来加强数据库的安全性，经常见到的就有密码，角色，权限等等。那么我们就从最简单的DBSNMP说起： Oralce数据库如果采用典型安装后，自动创建了一个叫做DBSNMP的用户，该用户负责运行Oracle系统的智能代理（Intelligent Agent），该用户的缺省密码也是“ DBSNMP ”。如果忘记修改该用户的口令，任何人都可以通过该用户存取数据库系统。现在我们来看一下该用户具有哪些权限和角色，然后来分析一下该用户对数据库系统可能造成的损失。 启动SQL/PLUS程序，使用该用户登录进入： SQL> 0select * from session_privs. CREATE SESSION ALTER SESSION UNLIMITED TABLESPACE CREATE TABLE CREATE CLUSTER CREATE SYNONYM CREATE PUBLIC SYNONYM CREATE VIEW CREATE SEQUENCE CREATE DATABASE LINK CREATE PROCEDURE CREATE TRIGGER ANALYZE ANY CREATE TYPE CREATE OPERATOR CREATE INDEXTYPE 可以看到该用户不是SYS或SYSTEM管理用户，然而，它却具有两个系统级权限：UNLIMITED TABLESPACE和CREATE PUBLIC SYNONYM。 看到这两个权限你应该马上想到，这些都是安全隐患，尤其是UNLIMITED TABLESPACE，它是破坏数据库系统的攻击点之一。如果这时候你还依然认为，即使有人利

用这个没有修改的口令登录进数据库也造成不了什么损失的话，我就不得不提醒你：该用户具有UNLIMITED TABLESPACE的系统权限，它可以写一个小的脚本，然后恶意将系统用垃圾数据填满，这样数据库系统也就无法运行，并将直接导致最终的瘫痪。目前很多数据库系统都要求7X24的工作，如果出现了系统用垃圾数据填满的情况，那么，等数据库系统恢复时，恐怕不可挽回的损失已经造成了。 可是除了DBSNMP还有很多其他的用户，怎么办呢？让我们先看一下目前普遍存在于Oracle数据库中的用户管理问题：（1）权限过大：对ORACLE数据库编程和浏览的一般用户常常具有DBA (数据库管理员权限)，能对数据库系统做任何修改或删除。（2）安全性差：很多ORACLE用户缺省存储位置都在系统表空间，这样不仅影响系统的正常工作，而且不同用户的数据信息互相影响、透明，保密性差。随着数据的不断加入，有可能使整个数据库系统崩溃。（3）密码有规律：在ORACLE调试初期形成的用户名和密码一致的不良习惯保留到现在；系统用户SYS和SYSTEM的密码也众所皆知。 知道了这些普遍的“ 毛病 ”，我们怎么做呢？下面是我的一些建议：（1）ORACLE DBA (数据库管理员)的规范 SUN Solaris操作系统下ORACLE用户密码应严格保密，绝不该把密码设成ORACLE；并指定专门的数据库管理员定期修改。ORACLE初始化建立的SYS和SYSTEM系统管理员用户密码应由原来MANAGER改成别的不易被记忆的字符串。 ORACLE WEB SERVER的管理端口具备DBA浏览数据库的能力，因此其管理者ADMIN的密码也应保密，不该把密码设成MANAGER；并指定专门的数据库管理员定期修改。

ORACLE DBA最好在SUN SPARC服务器控制台上用窗口式界面实现管理。前提是ORACLE用户启动服务器，然后在窗口式命令行下输入SVRMGRM，即启动了ORACLE SERVER MANAGER菜单式管理；用SYSDBA身份登录后，就可做数据库系统维护工作了 （2）SQL*PLUS编程用户的规范 存储结构的规范 考虑到用SQL*PLUS编程可实现各行各业、各公司、各部门多种多样的应用需求，我们的SQL*PLUS编程用户也应该朝这个方向规范：不同种类的应用必须有不同的用户；不同种类的应用必须有不同的存储位置，包括物理文件、缺省表空间、临时表空间的创建和规划：当准备编写某一较大规模(从ORACLE数据量和面向用户量考虑)应用程序时，首先应该创建一个逻辑的存储位置-表空间，同时定义物理文件的存放路径和所占硬盘的大小。 ①、物理文件缺省的存放路径 在/oracle_home/dbs下，在命令行下用UNIX指令df -k 可查看硬盘资源分区的使用情况。如果oracle_home使用率达90‰以上，而且有一个或多个较为空闲的硬盘资源分区可以利用，我们最好把物理文件缺省的存放路径改到较为空闲的硬盘资源分区路径下。在此路径下我们可以这样规划资源物理文件的存储： xxx表空间xxx行业/ xxx公司/ xxx 部门/ xxx 服务.dbf DEMO表空间default_datafile_home1/col /elec/sys4/demo1.dbf default_datafile_home1/col /elec/sys4/demo2.dbf 公司系统四部摹拟演示系统物理文件 HUMAN表空间default_datafile_home1/col/elec/human/human.dbf 公司人事部人事管理系统物理文件 BOOK表空间default_datafile_home1/col/elec/book/book.dbf 公司资料室图书管理系统物理文件 QUESTION表空

间default_datafile_home1/col/elec/client/question.dbf 公司客户服务部问题库系统物理文件 PC表空间default_datafile_home1/col/chaoxun/client/pc.dbf 公司PC机售后服务系统物理文件 ……表空间default_datafile_home2/…… …… 等等 说明：其中default_datafile_home1指oracle_home/dbs；default_datafile_home2指较为空闲的硬盘资源分区路径。 ②、物理文件的大小根据应用系统的数据量、数据对象、程序包的多少来定。一般用于摹拟演示的小系统，表空间初始的物理文件为2M即能满足要求，如果信息量满，还可以增加物理文件，扩充表空间(每次扩充大小也可暂定为2M)；一般实际运行的应用系统可适当增加表空间初始的物理文件大小，但也不要一次分配太大(因为不易回收空间，却易扩充空间)，这也需要根据具体情况具体分析：信息量大、需长时间保存的应用在条件允许情况下，表空间可以大到几百M甚至上G；信息量小、短期经常刷新的应用，表空间可以控制在2M以下。 ③、表空间的名称应该采用同系统应用相似的英文字符或字符缩写，表空间所对应的一个或多个物理文件名也应有相关性。不同用户所处的缺省表空间不同，存储的信息就不能互相访问。这比把所有用户信息都储存在系统表空间，安全性大大提高了。如果用ORACLE WEB SERVER管理端口创建的用户，其缺省和临时表空间一定是系统表空间，DBA切记要改变用户的缺省表空间。临时表空间存放临时数据段，处理一些排序、合并等中间操作，根据实际应用的需求可以把它们放在专门创建的表空间里；如果系统表空间大，也可以把它们放在系统表空间。用户创建的数据索引最好和数据文件分开存放在不同表空间，以减少数据

争用和提高响应速度。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com