Oracle数据安全面面观(1) 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_224652.htm 随着计算机的普及以及网络的发展，数据库已经不再仅仅是那些程序员所专有的话题。而Oracle数据库更是凭借其性能卓越，操作方便灵活的特点，在数据库的市场中已经占据了一席之地。但是同样随着网络技术的不断进步，数据信息的不断增加，数据安全已经不再是以前的“ 老生长谈 ”，也更不是以前书本上那些“ 可望不可及 ”的条条框框。 或许很久以前，大家都觉得Oracle数据库的安全并不存在隐患，因为Oracle公司在去年11月份开始促销其数据库软件时提出的口号是“ 只有Oracle9i能够做到绝对安全 ”。但是不管它这么说是为了促销，还是为了扩大知名度，总之伴去年12 月份，英国的安全专家 David Litchfield 发现的9iAS 中存在的程序错误导致的缓冲溢出漏洞以及后来，PenTest Limited 和 eEye Digital Security 各自提出了一个小的漏洞，所有使用Oracle公司产品的人都不由地紧张了原本松弛的大脑--这个对于用户来说，毕竟关系到了自己的“ 身家性命 ”。 下面笔者将带着大家走进Oracle数据安全的世界。由于笔者水平有限，所以不足之处在所难免，望大家不吝赐教。 （一）Oracle数据库的一些基本常识 这里仅仅是为了以后的安全奠定一些基础，因为我们后面要用到它们。呵呵~！ 1.Oracle所包含的组件 在 Oracle，数据库是指整个 Oracle RDBMS 环境，它包括以下组件： Oracle 数据库进程和缓冲（实例）。 SYSTEM 表空间包含一个集中系统类目，它可以由一个或多个数据文件构成。 其它由数据库管理员 (DBA)（可

选）定义的表空间，每个都由一个或多个数据文件构成。 两个以上的联机恢复日志。 归档恢复日志（可选）。 其它文件（控制文件、Init.ora、Config.ora 等）。 每个 Oracle 数据库都在一个中央系统类目和数据字典上运行，它位于SYSTEM 表空间。 2.关于“ 日志 ”Oracle数据库使用几种结构来保护数据：数据库后备、日志、回滚段和控制文件。下面我们将大体上了解一下作为主要结构之一的“ 日志 ”： 每一个Oracle数据库实例都提供日志，记录数据库中所作的全部修改。每一个运行的Oracle数据库实例相应地有一个在线日志，它与Oracle后台进程LGWR一起工作，立即记录该实例所作的全部修改。归档（离线）日志是可选择的，一个Oracle数据库实例一旦在线日志填满后，可形成在线日志归档文件。归档的在线日志文件被唯一标识并合并成归档日志。 关于在线日志：一个Oracle数据库的每一实例有一个相关联的在线日志。一个在线日志由多个在线日志文件组成。在线日志文件（online redo log file）填入日志项（redo entry），日志项记录的数据用于重构对数据库所作的全部修改。 关于归档日志：Oracle要将填满的在线日志文件组归档时，则要建立归档日志（archived redo log）。其对数据库备份和恢复有下列用处：数据库后备以及在线和归档日志文件，在操作系统和磁盘故障中可保证全部提交的事物可被恢复。 在数据库打开和正常系统使用下，如果归档日志是永久保存，在线后备可以进行和使用。 数据库可运行在两种不同方式下：NOARCHIVELOG方式或ARCHIVELOG 方式。数据库在NOARCHIVELOG方式下使用时，不能进行在线日志的归档。如果数据库在ARCHIVELOG方式下运行，可实施在线日

志的归档。 3.物理和逻辑存储结构 Oracle RDBMS是由表空间组成的，而表空间又是由数据文件组成的。表空间数据文件被格式化为内部的块单位。块的大小，是由DBA在Oracle第一次创建的时候设置的，可以在512到8192个字节的范围内变动。当一个对象在Oracle表空间中创建的时候，用户用叫做长度的单位（初始长度（(initial extent)、下一个长度（next extent）、最小长度（min extents）、以及最大长度（max extents））来标明该对象的空间大小。一个Oracle长度的大小可以变化，但是要包含一个由至少五个连续的块构成的链。（二）Oracle数据安全的维护 记得某位哲学家说过：“ 事物的变化离不开内因和外因。 ”那么对于Oracle数据安全这个话题而言，也势必分为“ 内 ”和“ 外 ”两个部分。那么好，我们就先从“ 内 ”开始说起： 1.从Oracle系统本身说起 我们先抛开令人闻风色变的“ hacker ”和其他一些外部的原因，先想一下我们的数据库。什么硬盘损坏，什么软件受损，什么操作事物……一系列由于我们的“ 疏忽 ”而造成的系统问题就完全可以让我们辛苦建立的数据库中的数据一去不复返。那么，我们就先从自己身上找找原因吧。 【一】解决系统本身问题的方法--数据库的备份及恢复 数据库的备份： 关于Oracle数据库的备份，标准地有三中办法：导出/导入（Export/Import）、冷备份、热备份。导出备份是一种逻辑备份，冷备份和热备份是物理备份。 导出/导入（Export/Import） 利用Export可将数据从数据库中提取出来，利用Import则可将提取出来的数据送回Oracle数据库中去。 a.简单导出数据（Export）和导入数据（Import） Oracle支持三种类型的输出： （1）表方式（T方式），将指定表的数据导出。 （2）用户方式（U方

式），将指定用户的所有对象及数据导出。（3）全库方式（Full方式），将数据库中的所有对象导出。 数据导出（Import）的过程是数据导入（Export）的逆过程，它们的数据流向不同。 b.增量导出/导入 增量导出是一种常用的数据备份方法，它只能对整个数据库来实施，并且必须作为SYSTEM来导出。在进行此种导出时，系统不要求回答任何问题。导出文件名缺省为export.dmp，如果不希望自己的输出文件定名为export.dmp，必须在命令行中指出要用的文件名。 增量导出包括三个类型：（1）“ 完全 ”增量导出（Complete） 即备份整个数据库，比如： $ exp system/manager inctype=complete file=990702.dmp （2）“ 增量型 ”增量导出备份上一次备份后改变的数据。比如： $ exp system/manager inctype=incremental file=990702.dmp （3）“ 累计型 ”增量导出（Cumulative） 累计型导出方式只是导出自上次“ 完全 ”导出之后数据库中变化了的信息。比如： $ exp system/manager inctype=cumulative file=990702.dmp 数据库管理员可以排定一个备份日程表，用数据导出的三个不同方式合理高效地完成。比如数据库的备份任务可作如下安排： 星期一：完全导出（A） 星期二：增量导出（B） 星期三：增量导出（C） 星期四：增量导出（D） 星期五：累计导出（E） 星期六：增量导出（F） 星期日：增量导出（G） 如果在星期日，数据库遭到意外破坏，数据库管理员可按以下步骤来恢复数据库： 第一步：用命令CREATE DATABASE重新生成数据库结构； 第二步：创建一个足够大的附加回段。 第三步：完全增量导入A： $ imp system./manager inctype= RECTORE FULL=Y FILE=A 第四步：累计增量导入E： $ imp system/manager

inctype= RECTORE FULL=Y FILE =E 第五步：最近增量导入F ： $ imp system/manager inctype=RESTORE FULL=Y FILE=F 冷备份 冷备份发生在数据库已经正常关闭的情况下，当正常关闭时会提供给我们一个完整的数据库。冷备份是将关键性文件拷贝到另外位置的一种说法。对于备份Oracle信息而言，冷备份是最快和最安全的方法。冷备份的优点是：是非常快速的备份方法（只需拷贝文件） 容易归档（简单拷贝即可） 容易恢复到某个时间点上（只需将文件再拷贝回去） 能与归档方法相结合，作数据库“ 最新状态 ”的恢复。 低度维护，高度安全。 但冷备份也有如下不足： 单独使用时，只能提供到“ 某一时间点上 ”的恢复。 在实施备份的全过程中，数据库必须要作备份而不能作其它工作。也就是说，在冷备份过程中，数据库必须是关闭状态。 若磁盘空间有限，只能拷贝到磁带等其它外部存储设备上，速度会很慢。 不能按表或按用户恢复。 如果可能的话（主要看效率），应将信息备份到磁盘上，然后启动数据库（使用户可以工作）并将所备份的信息拷贝到磁带上（拷贝的同时，数据库也可以工作）。冷备份中必须拷贝的文件包括：所有数据文件 所有控制文件 所有联机REDO LOG文件 Init.ora文件（可选） 值得注意的是冷备份必须在数据库关闭的情况下进行，当数据库处于打开状态时，执行数据库文件系统备份是无效的 下面是做冷备份的完整例子： （1） 关闭数据库 $ sqldba lmode=y SQLDBA >connect internal. SQLDBA >shutdown normal. （2） 用拷贝命令备份全部的时间文件、重做日志文件、控制文件、初始化参数文件 SQLDBA >! cp （3） 重启Oracle数据库 $ sqldba lmode=y SQLDBA >connect internal. SQLDBA >startup. 热备份

热备份是在数据库运行的情况下，采用archivelog mode方式备份数据的方法。所以，如果你有昨天夜里的一个冷备份而且又有今天的热备份文件，在发生问题时，就可以利用这些资料恢复更多的信息。热备份要求数据库在Archivelog方式下操作，并需要大量的档案空间。一旦数据库运行在archivelog状态下，就可以做备份了。热备份的命令文件由三部分组成：1．数据文件一个表空间一个表空间地备份。（1）设置表空间为备份状态（2）备份表空间的数据文件（3）恢复表空间为正常状态 2．备份归档log文件。（1）临时停止归档进程（2）log下那些在archive redo log目标目录中的文件（3）重新启动archive进程（4）备份归档的redo log 文件 3．用alter database backup controlfile命令来备份拷贝文件 热备份的优点是：可在表空间或数据文件级备份，备份时间短。备份时数据库仍可使用。可达到秒级恢复（恢复到某一时间点上）。可对几乎所有数据库实体作恢复。恢复是快速的，在大多数情况下在数据库仍工作时恢复。热备份的不足是：不能出错，否则后果严重。若热备份不成功，所得结果不可用于时间点的恢复。因难于维护，所以要特别仔细小心，不允许“以失败而告终”。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