<<Oracle DBA手记4>>

图书基本信息

书名：<<Oracle DBA手记4>>

13位ISBN编号：9787121172069

10位ISBN编号：7121172062

出版时间：2012-6

出版时间：电子工业出版社

作者：盖国强

页数：371

字数：528000

前言

未雨绸缪，防患未然　　在数据库领域十几年，我发现在国内技术人员往往在充当救火队员的角色，企业也常常认为只有能够力挽狂澜、起死回生的技术人员，才是好的技术人员。
而实际上，能够不犯错误、少犯错误，提前预防、规避灾难的技术人员才是企业技术环境的最有力保障，能够未雨绸缪，防患于未然才是更好的技术实践。
我们每年都帮助很多企业挽救数据、拯救危机。
2011年12月30日和31日，连续的两个整天，从凌晨再到凌晨，连续挽救了几个用户的数据库。
这些灾难发生得那么简单，那么不可思议，在迈入2012这个神秘年份的一刻，深深地触动了我。
我想，如果把这些案例描述出来，就可能让一些用户警醒，避免再陷入这样的困境。
而从别人的挫折中学习，进而在自己的环境中未雨绸缪，防患于未然，是每个数据库管理人员和企业数据环境管理者应该具备的素质。
写作本书还和2011年底众多席卷而来的密码泄露事件有关。
当我注视着最常用的几个密码都在互联网上被公开时，除了手忙脚乱地在各大网站修改密码，剩下的就是深深的遗憾。
几乎所有从事IT行业的人，都深知安全的重要性，可是放在实际执行中，大家又往往习惯性失明，忽视了自己周围本来力所能及之安全，很多专业人士就以这样或者那样的侥幸心理放任了风险的存在，并一步一步走向了安全危机。
对于数据库安全来说，通常缺乏的并非技术手段，更多的是缺乏规范和安全认知，如果用户都能够严格遵循安全守则并应用现有的安全技术手段，数据库的安全性就能够大幅增强，我们的安全事故率也会大大降低。
于是我决定动笔，写下自己多年来所遭遇到的安全案例，以及对于数据安全的思考。
如果本书中的内容能够帮助一些企业规避错误，保全数据，挽救一些技术人员的时间，那么我将感到无比欣喜。
于我们的生命中，最为宝贵的就是时间，寸金难买寸光阴。
信息安全　　在传统的信息安全领域，存在三个基本的安全要素，这三个要素分别是：保密性（Confidentiality）、完整性（Integrity）和可用性（Availability），简写为CIA。
这三个要素的基本定义如下。
保密性：指信息在存储、使用和传输过程中不会泄露给非授权方。
完整性：指信息在存储、使用和传输过程中不被非授权用户篡改、变更，同时防止授权用户对系统及信息进行非授权篡改，保持信息在整个过程中内外的一致性。
可用性：信息系统因其服务使命，必须在用户需要时，可以被正常访问。
授权用户或实体对信息系统的正常使用不应被异常拒绝或中断，应当允许其可靠、及时地访问和获取信息及资源。
高可用系统要求所有时间可用，要确保系统不因电源故障、硬件故障和系统升级等因素影响服务的可用性。
信息安全的三要素是对安全的概括和提炼。
不同机构和组织，因为需求不同，对CIA的侧重也会有所不同。
随着信息安全的发展，CIA经过细化和补充，增加了许多新的内容，包括可追溯性（Accountability）、抗抵赖性（Non-repudiation）、真实性（Authenticity）、可控性（Controllable）等。
与CIA三元组相反的一个概念是DAD三元组，即泄漏（Disclosure）、篡改（Alteration）和破坏（Destruction）。
实际上DAD就是信息安全面临的最普遍的三类风险，是信息安全实践活动最终应该解决的问题。
CIA的核心三要素涉及软件（Software）、硬件（Hardware）和通信（Communications）三个方面，下图清晰地描述了信息安全三要素及相关领域范畴。
信息安全的三要素（引自维基百科）　　从CIA理念出发，通过对信息安全范畴所有相关主题精炼整理得到了一个标准化的知识体系——公共知识体系（Common Body of Knowledge

，CBK）。
CBK包括10个知识范畴（Domain），对安全进行了全面的概括，具有极强的指导意义。
下图对10个领域进行了简单的列举（不同出版物描述略有不同）。
CBK 10 Doamin（参考Handbook of Information Security Management） 以上10个范畴分别为：访问控制，电信、网络和互联网安全，风险管理和商务连续性计划，策略、标准和组织，计算机架构和系统安全，法律、调查和道德，应用程序安全，密码学，计算机操作安全，物理安全。
数据安全 信息安全的核心是数据安全。
在数据安全的范畴内，也包含信息安全的诸多方面。
根据多年的服务经验与思考，我们将安全划分为五大方面，分别是：软件安全、备份安全、访问安全、防护安全和管理安全。
这五大方面是信息安全在数据领域的引申和映射。
在企业数据安全中，这五大方面是相辅相成、互有交叉、共同存在的。
下图是关于安全的一张思维导图，本书案例就涉及了这五大方面。
数据库安全思维导图 在这五大安全方向中，可能出现两种性质的安全问题：第一，由于内部管理不善而导致的数据安全问题；第二，由于外部恶意攻击入侵所带来的安全问题。
通常我们把安全问题狭义化为后者，这实际上是片面的，在数据安全问题上，前者造成的数据损失、数据损毁，其发生率和影响度都远远超过后者。
下面我们对数据安全的五大方面进行简要的分析和探讨。
软件安全是指我们选择的数据库产品、版本是否稳定安全，厂商所能提供的补丁集和Bug修正是否及时，基础硬件与操作系统是否经过认证。
很多用户在部署数据库软件时，仅仅选择了最容易获得的初始发布版本（如Oracle Database 10.2.0.1或者Oracle Database 11.2.0.1等），遗漏了可能已经存在的补丁修正，并且在运行维护中并不能够及时跟踪软件更新，也无法获得Bug信息、补丁修正和安全告警。
这就使得软件本身的很多风险隐患得不到修正。
如果软件安全无法保证，数据库安全的基础也就丧失了。
备份安全是指用户数据能否得到及时有效的备份保全，能否在故障灾难之后获得及时的恢复和挽救。
在数据库运行期，最为重要的就是备份安全，如果没有可靠的备份，将数据集中起来就只能是等待数据灾难，所以我们将备份安全提升到核心地位，备份及随之衍生的容灾安全等，都是企业整体数据架构应该考虑的因素。
很多企业在数据灾难之后因为缺乏有效备份而一蹶不振。
Gartner在2007年的一份调查报告显示，在经历了数据完全丢失而导致系统停运的企业中，有2/5再也没能恢复运营，余下的企业也有1/3在两年内宣告破产。
由此可见，由于备份安全问题导致的企业伤害可能远远大于黑客攻击。
访问安全是指用户数据库的访问来源和访问方式是否安全可控。
通常数据库系统处于IT系统的核心，其安全架构涉及主机、系统、存储、网络等诸多方面。
如果没有明确的访问控制，缺乏足够的访问分析与管理，那么数据库的安全将是混乱和无法控制的。
在应用软件使用和访问数据库时，要正确设置权限，控制可靠的访问来源，保证数据库的访问安全。
唯有保证访问安全才能够确保数据不被越权使用，不被误操作所损害。
通常最基本的访问安全要实现程序控制、网络隔离、来源约束等。
安全防范是指通过主动的安全手段对数据库通信、传输等进行增强、监控、防护、屏蔽或阻断，诸如数据加密、审计、数据防火墙等技术都属于这一范畴。
我们必须认识到，在IT技术高度发展的今天，风险是无处不在、层出不穷的，可能我们从未思考过的安全问题每天都在不断涌现，在数据库环境中采取主动式防护，将可以帮助我们监控分析和屏蔽很多未知风险。
目前已经有很多成熟的产品和技术可以用于安全防范。
管理安全是指在企业数据的日常管理维护范畴内，能否充分保证数据安全及服务的高可用连续提

供。
诸如DBA的维护、文件的管理、参数或数据结构的变更等都可能引入数据风险，管理安全要求我们通过规范、制度及技术手段去确保维护管理安全。
另外，基于硬件、电力等基础平台的故障都可能影响数据库服务的高可用性，在管理中要通过监控手段及时预警，通过集群、备库等的切换与服务分担保障服务的连续性。
这就是数据安全的五大方面。
业界安全事故　　在2011年的新闻报道中，我们注意到很多企业遭受了严重的安全事故，影响深远。
以下摘录了几起广为人知的数据安全事故，让我们一起看一看安全问题都出现在了哪里。
1. 陕西移动近1400万条个人信息遭泄露　　根据新闻报道（案件大约发生在2011年3月），犯罪嫌疑人所在的某技术公司承担着陕西某电信企业手机资费计算系统软件平台的开发、运行、维护、咨询、防毒等多项工作，可以获取该电信运营商拥有的手机用户号码、姓名、年龄、性别、身份证号、住址、每月通信费用等资料。
犯罪嫌疑人为了个人利益，窃取用户信息并出售。
“朋友向我要西安、榆林、延安、渭南等六七个地市的移动手机每个月话费消费20元以上的信息，内容包括手机号码、月话费消费情况、办卡区域、机主性别、出生年月等，我同意了。
第二天我在单位将计算机连接到省移动公司数据库中，提取了1000余万条信息，每个地市建立一个文件夹，存储到我的笔记本计算机中……”　　2. 高阳捷迅工程师利用支付宝漏洞盗取11万　　2009年，支付宝公司开通话费支付业务，用户可以通过购买手机充值卡充入支付宝账户后进行网上购物，高阳公司负责这一话费充值系统的运行维护。
即在支付宝与移动、联通、电信之间搭建平台，负责将支付宝用户购买的手机充值卡转变为支付宝账户的存款。
犯罪嫌疑人是负责这一系统维护的工程师，在2010年1月至3月间，他利用了这个系统的漏洞，多次通过互联网进入高阳公司系统数据库，调取用户充值失败而暂存于此的充值卡信息，然后将其转入自己在支付宝设立的48个账户和在快钱设立的31个账户，共计111650元。
3. CSDN 600余万用户密码泄露事件　　2011年12月21日，一组安全事件在国内引发了轰动，黑客在网上公开了CSDN网站用户数据库，包括600余万个明文的注册邮箱账号和密码可能遭集中曝光。
事件发生之后，CSDN相关网页更一度紧急关闭，以升级为由暂时关闭。

<<Oracle DBA手记4>>

内容概要

《Oracle
DBA手记·4：数据安全警示录》以数据安全为主线将众多灾难挽救过程串联在一起，不仅对各个案例的发生过程进行了详细描述，更为读者提供了具体的规避法则。
其间穿插介绍了很多新鲜的技术细节和恢复方法，以及作者对于数据安全的思考。

本书不仅是写给技术人员看的，更是写给企业数据管理者看的，力求帮助企业避免遭遇本书所述种种灾难。
同时，这也是一本相当深入的技术书，包括了一些相当深入的技术探讨，不仅可以帮助读者加深对于Oracle数据库技术的认知，还可以帮你在遇到类似案例时，做出同样的营救工作。

<<Oracle DBA手记4>>

作者简介

盖国强，Oracle ACE总监，恩墨科技创始人，ITPUB论坛超级版主，远程DBA服务的倡导者和实践者，致力于以技术服务客户。
著有《深入解析Oracle》、《循序渐进Oracle》、《深入浅出Oracle》等书；从2010年开始，致力于《Oracle DBA手记》的撰写与编辑工作，并与张乐奕共同创立了ACOUG用户组，在国内推进公益自由的Oracle技术交流活动。

书籍目录

章节摘录

版权页： 插图： 其实这样的泄密，一看就是无意识的。
很多时候，DBA就是要对无意识的事情，保持高度的警惕。
为了这样的事情，影响到自己的职业生涯，是绝对不划算的。
建议DBA在发布任何会有第三方知道的文档之前，先问问自己，这份东西会导致泄密么？
多问自己几次，多确认几次，如果不能确认，那就和你的主管确认吧。
我还记得，以前我们有一条铁的规定，非项目经理及以上级别，不得公开对甲方发布任何技术文档及承诺。
这条规定就很好，可以避免很多不必要的麻烦。
2.忘记你的系统有备份 虽然我曾经反复强调，备份重于一切，但是我不得不承认，有时候，忘记你的系统有备份的确是一个重要的提示。
在本书部分案例中，客户存在备份，但是由于数据量庞大或者空间有限，使用备份进行恢复的成本很高或者不现实，于是客户不得不选择采取一些较为极端的方式来进行异常修复。
而很多DBA之所以犯下错误，也正是因为觉得别人做过备份，已经有了备份。
这些想当然的前提在故障出现之后可能不再成立，而这正是很多经典故障的根源。
所以，我非常欣赏郭岳在书中提出的观点：在有些时候，忘记你的系统有备份。
很多人，看到这个标题，可能觉得十分诧异，作为一个DBA，需要遵守的守则中的第一条，就是要备份。
在eygle的DBA四大守则中的第一条，写的就是备份重于一切，并且很明白地说明，唯一能使DBA半夜惊醒的事情，就是系统没有备份。
首先不得不说明，我完全同意这个观点，但是在维护电信运营商系统的时候，请你一定要忘记你的系统是有备份的。
我提出这个观点，基于以下两个原因。
首先，对于运营商级别的系统，数据量之大，如果没有到达非常让人崩溃的情况（例如，生产系统崩溃，容灾系统无法启动，并且应急系统也无法运行这样极端），是不会去采用恢复数据的方案的，因为数据量太大，恢复的时间太长，而运营商是要求业务能运行为第一要素的。
其次，人都是有依赖性的，当你知道你的系统有备份的时候，你的操作就开始不那么如履薄冰了，就开始毛躁了，因为你的潜意识会认为，反正我的系统有备份，大不了恢复回来。
忘记你的系统有备份吧，忘记它吧。

<<Oracle DBA手记4>>

版权说明