Oracle9i 数据库的安全管理机制

竹 勇,叶水生
(南昌航空工业学院 计算机系,江西 南昌 330034)

摘 要:数据库安全和数据安全机制是数据库开发设计者必须考虑的重要问题之一。Oracle 数据库管理系统在数据库安全方面为数据库管理员和应用开发者提供了很好的安全机制。文中从不同侧面和角度讨论并分析了 Oracle9i 数据库系统的安全管理机制,为数据库管理员和数据用户如何尽可能地保障自己的信息安全提供借鉴。

关键词:权限;视图;备份;角色;审计
中图分类号:TP309.2 **文献标识码**:A **文章编号**:1673-629X(2006)06-0142-03

Secure Management Mechanism of Oracle9i DBMS

ZHU Yong, YE Shui-sheng
(Department of Computer, Nanchang Institute of Aeronautical Technology, Nanchang 330034, China)

Abstract: Database security and data security mechanism are the preferential consideration of the database developer. Oracle9i DBMS supplies the preferable secure mechanism in the database security for DBA and developer. This paper discusses and analyses the secure management mechanism of Oracle9i DBMS from different facts and fields, offers references for DBA and user to ensure their information security as much as possible.

Key words: privilege; view; backup; role; audit

系统的开放性、网络化给应用系统安全提出了更高的要求,作为信息聚集体的数据库系统处于计算机信息系统的核心地位,其安全性至关重要。Oracle9i 数据库安全管理机制中数据库安全可划分为系统安全和数据安全两类。系统安全包括的安全机制可以在整个系统范围内控制对数据库的访问和使用,如有效的用户名和口令、是否授权于用户连接数据库、用户能执行的系统操作等。数据安全包括的安全机制可以在对象(如表、视图、索引等)这一级上控制对数据库的访问和使用,例如,哪些用户可以访问某特定的对象及对这个对象允许执行的操作(如允许查询、插入、删除操作)等。Oracle9i 数据库管理系统的安全机制可以防止未授权的数据库访问,防止对具体对象的未授权访问、控制磁盘及系统资源(如 CPU 时间)的分配和使用、稽核用户行为等[1]。

1 用户和系统的安全策略

数据库的安全性不仅要防止敏感数据被窥探,而且要防止开发人员或普通用户有意或无意地进行任何干扰数据库的操作。数据库系统包括了一般用户、最终用户、数据库管理员、应用程序开发人员、应用程序管理人员等用户。Oracle9i 数据库系统安全管理的第一步是为每一个用户(包括系统开发人员及应用系统的操作人员)创建相应的数据库账号,任何用户对数据库提出的任何操作都必须强制通过系统的安全设置检查之后方能实施。SYS 账号拥有系统所有的数据字典基表和相关的数据库对象,SYSTEM 账号拥有一些附加的数据字典和视图以及 Oracle9i 应用开发工具所用到的表和视图[2]。在网络上的远端用户注册 Oracle 数据库时,如用不加密方式键入密码,用户的密码很有可能被非法用户截取。为了更好地保护口令的机密性,可以为客户机/服务器和服务器/服务器连接设置参数来强制 Oracle 口令值编码。对客户机,把 SQLNET.ORA 文件中的参数 ORA-ENCRYPT LOGIN 设置为 TRUE;对服务器,把 INIT.ORA 文件中的参数 DBLINK-ENCRYPT LOGIN 设置为 TRUE;这样口令以加密的形式在客户机到服务器和服务器到服务器之间传送。需要强调的是数据库系统管理员对 SYS 和 SYSTEM 两个特殊的账户的保密管理,要经常更改这两个账户的口令,防止被盗用[3]。

为了保护 Oracle 服务器的安全,应保证 $ Oracle-HOME/bin 目录下所有内容的所有权为 Oracle 用户所有。数据库管理员必需有建立和删除文件的操作系统权限,如数据库文件和联机日志文件等。输出文件和其他的备份文件也必须受到保护。一般数据库用户不应该有建立和删除与数据库相关文件的操作系统权限,对数据库中对象

收稿日期:2005-09-26
基金项目:江西省教育厅资助项目(DB200406011);江西省测控中心资助项目(ZX200328002)
作者简介:竹 勇(1981-),男(回族),河南固始人,硕士研究生,研究方向为 Web 数据挖掘、人工智能;叶水生,教授,研究方向为 Web 数据挖掘、人工智能。

的访问是通过权限(privilege)来完成的。通过grant命令就可以针对特定的数据库对象使用特定的数据库命令。例如,如果用户SCOTT拥有一个叫做EMPLOYEE的表并执行命令GRANT SELECT. UPDATE ON EMPLOYEE TO PUBLIC;可以使用角色来管理对用户有效的系统级命令,这些命令包括create table和alter index。对于每种数据库对象的操作都是有各自的权限授权的。也可以创建一些自定义的系统级角色,这些角色只向用户授予他们在数据库中所需的权限而不是过多的特权。

2　基于视图和审计的安全措施

视图主要用于设置数据的记录组权限,允许用户访问表中的某些记录而不是表中所有记录。通过建立视图可以保护表中的敏感数据,如职工表中包括薪水等敏感数据,若在该表上建立一个视图不包括这些列,且只允许用户读取该视图,那么就起到保护敏感数据的作用。表的属主或DBA可以通过创建视图的方法对表的若干行或若干列进行授权,对视图授权的方法与对表的授权相同,但视图授权仅限于SELECT, INSERT, UPDATE和DELETE操作。视图特权可使该视图的行或列享有某些权限,同时那些未包含在视图中的行或列自动地受到保护。

一个带选择条件的视图可以用来维护行级的安全性,那些不满足条件的行自动地得到保护。同时那些未被定义为视图字段的表的其他字段也自动地被保护起来,从而实现数据库列级的安全性。利用视图机制实现属主或网络位置的透明可以很便捷地实现更深层次的数据库的安全保护力度。当授权用户对表进行存取时必须在FROM子句中指明表的属主,在网络环境中还必须指明数据所在的机器位置,通过创建相应视图可以隐含有关信息,即使发生网络结构变化、数据库变化或数据分布变化,也只需修改视图的定义,所有的应用程序不必做任何修改,同时也能有效防止数据的意外丢失或蓄意破坏。

Oracle9i具有审计发生在其内部所有动作的能力,审计记录可以写入SYS. AUDIT或操作系统的审计踪迹。每个连接数据库的试图都可被审计,影响数据库对象如表空间、同义词、回滚段、索引的任何操作也都可被审计。除了系统级的对象操作,对对象的数据交换操作如对表插入、更新等也可以审计。由于数据库审计踪迹表是存在数据库内的,任何写入的审计记录必须得到保护。如果必须在SYS. AUD$上存储信息,就必须先保护该表。Oracle9i提供了两个SQL脚本来管理与审计有关的数据字典视图:CATAUDIT. SQL和CATNOAUD. SQL。数据字典包含与审计有关的两类视图:第一类确定哪些项目被审计;第二类建立在审计表上,表示从各种角度的审计记录。

3　数据库备份与恢复

3.1　数据库备份所使用的结构

Oracle数据库使用几种结构来保护数据:数据库备份文件、日志文件和控制文件。数据库备份文件是对Oracle数据库系统的所有物理文件的操作系统备份。当发生物理介质故障进行数据库恢复时,可利用备份的文件来恢复毁坏的数据文件或控制文件。日志文件记录数据库中对数据所作的全部修改。数据库的日志文件有非归档模式(NOARCHIVELOG MODE)和归档模式(ARCHIVELOG MODE)两种运行方式。在归档模式下当在线日志写满后,系统会自动切换日志组并形成归档日志文件。归档日志文件主要用于对数据库进行数据恢复(结合数据库的备份文件,可进行基于Until time, Until cancel或数据的全部恢复,保证系统提交事物的安全性)。控制文件用于存储数据库的物理结构的状态(包括文件名称、文件的物理位置及系统的同步标识等),在实例恢复和介质恢复期间引导Oracle数据库系统的正确启动[4]。

3.2　数据库的备份

备份主要可分为逻辑备份和物理备份。逻辑备份是利用SQL从数据库中抽取数据并存入二进制文件,这些数据可以重新引入原来的数据库,或者以后引入其他数据库。Oracle提供的Export/Import工具可用于进行数据库的逻辑备份。物理备份是实际物理数据库文件从一处拷贝到另一处的备份。操作系统备份、脱机备份和联机备份都是物理备份的例子。

数据库的逻辑备份包括读一个数据库记录集和将记录集写入一个文件中,这些记录的读出与其物理位置无关。Oracle的Export实用程序用来读取数据库(包括数据字典)和把输出写入到一个叫做导出转储文件(export dump file)的二进制文件中。可以导出整个数据库(FUIL DATABASE)、指定用户(USER)或指定表(TABLE)。在导出期间,可以选择是否导出与表相关的数据字典信息,如权限、索引和与其相关的约束条件。可以对所有表执行全数据库导出(Complete export)或者仅对上次导出后修改过的表执行全数据库导出。一旦数据已经导出就可以通过Import实用程序将其导入。如果导入一个全导出的整个导出转储文件,则所有数据库对象(包括表空间、数据文件和用户)都会在导入时创建。不过,为了在数据库中指定对象的物理分配,通常预先创建表空间和用户。

物理备份是拷贝构成数据库的文件而不管其逻辑内容如何。进行操作系统备份包括关闭数据库并从系统上注销所有用户。当所有访问权都被解除之后,系统关闭并以单用户(维护)方式重启,其控制权在系统控制台提供给管理员。由于备份过程只是从磁盘读取数据,所以在系统关闭进行备份时磁盘上的数据在该时间点是连续的。如果这个备份过程要用于恢复系统,那么系统配置、用户数据、用户文件的所有改动都将丢失。数据库正常关闭时使用脱机备份。当数据库处于"offline"时要备份下列文件:所有数据文件和控制文件、所有联机重做日志init. ora文件(可选择)。当数据库关闭时对所有这些文件进行备份可以提供一个数据库关闭时的完整镜像,以后可以从备份

中获取整个文件集来恢复数据库。可以为正在ARCHIVELOG方式下运行的数据库使用联机备份。在这种方式下,联机重做日志被归档,ARCH(Archiver)后台进程在写入前将每个重做日志文件做一个拷贝。数据库可从一个联机备份中完全恢复,并且可以通过归档的重做日志回滚到任一时刻。联机备份过程提供了完全的时间点恢复,并且允许数据库保持打开状态。因此,即使在数据库不能关闭时也能备份文件系统。

3.3 数据库的恢复

DBA的一个主要任务是保持数据库的及时性,并准备应付可能出现的硬件、软件、网络、进程和系统故障。恢复处理的不同取决于发生的故障类型、受到影响的结构以及所需的恢复类型。常见的错误或故障一般有3种:

(1)实例失败:从实例失败中恢复应自动进行。数据库需要访问位于正确位置的所有控制文件、联机重做日志文件和数据文件。数据库中任何未提交的事务都要回滚。当一个实例失败后数据库启动时,即使数据库未运行在ARCHIVELOG方式中,Oracle也要检查数据文件和联机重做日志文件,并把所有文件同步到同一个时间点上。

(2)介质失败:介质失败常发生于一个磁盘上驻留的当前数据库文件变得无法被数据库读出时。驻留联机重做日志文件的磁盘应总是被镜像(通过使用重做日志组或在操作系统级镜像文件)。如果丢失的是控制文件,应关闭数据库并从保留有控制文件的地方拷贝一份;如果丢失的是数据文件,可用前一次的联机备份进行恢复[5]。

(3)用户失误的拯救:有时用户会犯下一些不能回滚或撤消的错误,这些错误可能由DDL命令或DML命令组成。在这些情况下,用户希望返回到他们要取消的某一数据库事件前的一个时间点,这需要时间点恢复。最简单的时间点恢复是使用最新的导出转储文件。如果返回最近的导出还不够,则用户可能需要一个更新版本的表。若要执行时间点恢复,必须在ARCHIVELOG方式下运行[6]。

4 基于角色的权限管理

对于一个具有诸多表、诸多用户及各种不同职责的应用环境,如果数据库管理员把权限直接授予各个用户,从长远来看很容易出问题。Oracle9i基于角色的权限管理较好地解决了这些问题,只需根据部门和企业的安全政策、操作规则划分出不同的数据库角色,为机构的每个职务定义一个数据库角色,然后根据需要把这些角色授予相应用户,即使某职务的权限发生了改变也只需简单地修改该职务相对应的角色的权限,这样不仅保证了数据库的安全性,还大大降低了权限管理的负担和代价,减少了系统的安全漏洞。

Oracle9i的角色控制具有很强的实时性,授予角色的权限立即被分配给角色的用户使用;从一个角色取消某项权限就会立即阻止与该角色有关联的所有用户使用该权限;角色还可根据需要处于激活或停顿状态,以便控制用户所授予角色的活动。角色本身还可以得到口令保护。基于角色的权限管理极大地加强了系统安全控制的灵活性,进一步增强了系统的安全性能。此外,角色还有以下优点:

(1)角色可以通过操作系统授予,即角色可以使用操作系统命令或实用程序将角色指定给数据库中的用户;

(2)非连带回收,对象权限可以被回收,但是并不能导致连带回收;

(3)改善系统性能,当角色被设置成使不能时,在语句的执行期间只需要很少的权限检查确认,角色的使用减少了保存在系统数据字典中权限的授予个数[7]。

5 数据字典与权限跟踪

Oracle9i数据字典是Oracle9i数据库的重要组成部分,是一组描述数据库结构、数据库用户及其存取权限等数据库信息的系统表或视图,起着系统状态的目录表的作用,真实描述数据库的当前信息。数据字典由系统自动建立和维护,用户不能修改数据字典的任何内容。出于安全原因,系统权限的授权中不包含对数据字典的访问授权。借助Oracle9i的数据字典可以有效跟踪系统的授权状况,了解哪些权限分配给哪些用户或角色;哪些角色当前是激活的或是禁止的等等。对相应的数据字典实行SELECT操作,便可查询了解相关的授权信息。

6 结束语

Oracle安全性包括许多不同方面,需要通盘考虑才能交付业务用户所需的性能和可用性。安全考虑应该切入到Oracle系统的整个端到端的基础结构中,包括用户身份验证、网络和名称解析、数据和字典保护[8],等等。Oracle提供了强制所需的安全程度的大多数特性,但是要应用这些特性还是要DBA付出相当的努力。

参考文献:

[1] Abbey M,Corey M,Abramson I. Oracle9i初学者指南[M]. 王海峰,莫伟锋,等译. 北京:机械工业出版社,2002.

[2] 王新民,王 飞. Oracle9i数据库安全管理机制剖析[J]. 信息技术,2002(12):23-26.

[3] 金定勇. Oracle数据库安全性探讨[J]. 计算机工程,2002,28(6):125-126.

[4] 杨国权,赵建东. ORACLE数据库系统的数据安全策略[J]. 承钢技术,2003(2):5-7.

[5] 张海龙,王德江. Oracle数据库的安全策略[J]. 信息技术,2001(7):18-19.

[6] 李海波. Oracle数据库的安全及备份恢复[J]. 电脑知识与技术:认证考试,2004(4):13-15.

[7] 刘志敏. Oracle数据库应用管理解决方案[M]. 北京:电子工业出版社,2002.

[8] Ingram G. High-performance Oracle[M]. 北京:清华大学出版社,2003.