Oracle 与 SQL Server 基于角色访问控制对比分析

郑丽娟[1],李仲秋[2],任永昌[2]
(1. 渤海大学 大学计算机教研部,辽宁 锦州 121013;
2. 渤海大学 信息科学与技术学院,辽宁 锦州 121013)

摘 要:数据库的安全性极为重要,访问控制技术是保证数据库安全行之有效的方法之一,数据库访问控制安全管理的重要机制就是角色与权限分配。首先,通过 RBAC 通用模型和控制过程形式化表示方法,研究基于角色的访问控制方法;然后,分别研究 Oracle 基于角色访问控制和 SQL Server 基于角色访问控制;最后,对 Oracle 与 SQL Server 基于角色访问控制进行对比分析。结果表明,Oracle 的角色与授权复杂,SQL Server 相对简单;如果对数据库的安全性要求较高,建议选择 Oracle;如果 DBA 的技术水平一般,建议选择 SQL Server。

关键词:数据库系统;Oracle;SQL Server;角色;权限;访问控制;数据库安全
中图分类号:TP311 **文献标识码**:A **文章编号**:1673-629X(2013)05-0104-04
doi:10.3969/j.issn.1673-629X.2013.05.027

Role-based Access Control Comparative Analysis on Oracle and SQL Server

ZHENG Li-juan[1], LI Zhong-qiu[2], REN Yong-chang[2]
(1. Teaching and Research Institute of College Computer, Bohai University, Jinzhou 121013, China;
2. College of Information Science and Technology, Bohai University, Jinzhou 121013, China)

Abstract: The security of the database is extremely important, and access control technology is one of the effective methods to ensure database security, the main mechanism of the database access control on security management is allocation of roles and permissions. First, it studies the role-based access control method through the RBAC model and control process representation method, and then, respectively research role-based access control on Oracle and SQL Server. Finally, it should make comparative analysis about these two aspects. The results show that role and authorization of Oracle is more complex than that of SQL Server. When the requirements of database security are high, it is recommended that Oracle should be chosen, otherwise, choose SQL Server.

Key words: database system; Oracle; SQL Server; role; privilege; access control; database security

0 引 言

数据库是当今信息社会中数据存储和处理的核心,其安全性对于整个信息安全极为重要。数据库安全是指为数据库系统建立和采取的技术与管理方面的安全保护,用以保护数据库系统软件和数据不因偶然或恶意的原因而遭到破坏、更改和泄露[1]。保证数据库安全的方法之一就是访问控制技术。访问控制策略一般有三种[2]:

一是自主访问控制(DAC, Discretionary Access Control),这是一种比较宽松的访问控制,用户可以根据自己的意愿决定是否将自己客体的访问权或部分访问权授予其他主体;

二是强制访问控制(MAC, Mandatory Access Control),将系统中的信息分密级和类进行管理,是对所有主体及其所控制的客体(进程、文件、段、设备)实施强制访问控制;

三是基于角色的访问控制(RBAC, Role-Based Access Control),运用权限和角色之间的关联关系[3],简化授权管理,降低授权管理的复杂性,提高授权的灵活性,是目前应用最广泛,也是最成熟的方法。

Oracle 和 SQL Server 是当前应用最为广泛的两个数据库系统。通过基于角色访问控制对比分析,在进一步认识这两个数据库系统基于角色访问控制的基础上,找出各自的优缺点和适用范围,为数据库管理员进行数据库系统安全管理提供帮助,为公司或企事业单位选择数据库系统提供指导。

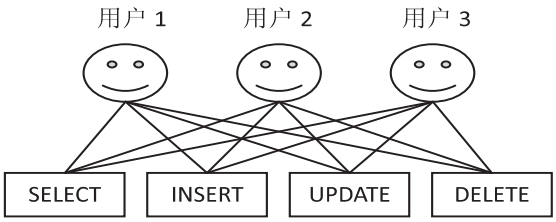
收稿日期:2012-08-11;**修回日期**:2012-11-16
基金项目:国家自然科学基金资助项目(70871067);辽宁省博士基金(20091034)
作者简介:郑丽娟(1966-),女,副教授,从事软件项目管理、计算机应用研究。

1　基于角色的访问控制方法

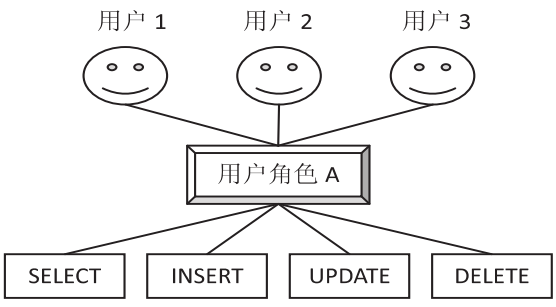
基于角色的访问控制(RBAC,Role-Based Access Control)及相关术语最早出现在 1992 年 Ferraiolo 和 Kuhn 发表的文章中,提出了运用角色对数据库访问进行控制的思想,从此基于角色的访问控制方法在数据库中得到了广泛的应用。

1.1　角色的作用

角色、用户、权限之间存在着错综复杂的关系。用户和权限之间是多对多的关系,即:一个用户具有多种权限,一种权限可以被多个用户所拥有;用户和角色之间是一对多的关系,即:一个用户属于一种角色,一种角色可以被多个用户所拥有;角色和权限之间是多对多的关系,即:一种角色具有多种权限,一种权限可以被多个角色所拥有。如此错综复杂的关系,如果不通过角色辅助权限管理,那么用户权限管理将是非常复杂的工作。对于一个拥有多种权限大量用户的数据库系统来说,角色架起了用户和权限之间的桥梁,通过角色管理用户和权限,简化了权限管理的复杂性,提高了权限分配的效率。假定用户 1、用户 2、用户 3 对表操作具有 SELECT、INSERT、UPDATE、DELETE 4 种权限,如果采用直接授权操作,需要进行 12 次授权,如图 1(a)所示;如果通过使用角色授权,先将 4 种权限授予角色,然后将角色再分别授予用户,需要进行 7 次制授权,如图 1(b)所示[4]。当用户很多且数据库对象及相应的操作很多时,使用角色能显著地简化权限管理。



(a) 直接授权



(b) 通过角色授权

图 1　RBAC 通用模型

1.2　RBAC 通用模型

在访问控制中,主体是访问操作的主动发起者,是系统中信息流的启动者,可以使信息流在实体之间流动;客体是指信息的载体或从其他主体或客体接收信息的实体,在权限管理中客体通常是指数据库对象,即表、视图、连接、过程、记录、字段等。RBAC 通用模型包含五个基本要素:用户集(users)、角色集(roles)、操作集(operators)、对象集(objects)、会话集(sessions),其中操作集和对象集组成授权集(perms)。用户集是主体;对象集是客体;操作集是定义在对象上的多个操作的集合,包括对数据的操作以及对数据库对象的操作等;角色集根据应用的场合不同,可以是一组用户的集合,也可以是一组权限的集合;会话集,是系统登录或通信进程与系统之间的会话。RBAC 通用模型如图 2 所示[5,6],可以形式化描述为五元组 URAOR{用户集 Users,角色集 Roles,访问集 Access,操作集 Operators,资源对象集 Resources}[7]。

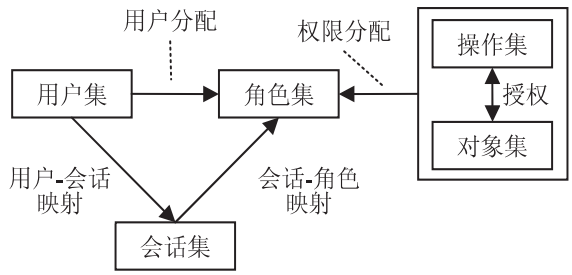


图 2　RBAC 通用模型

1.3　控制过程形式化表示

RBAC 通用模型的要素之间通过一些操作关联起来。形式化表示如下[1]:

(1)用户分配(UA):UA⊆USERS×ROLES。UA 是多对多的关系,记录管理员为用户所分配的角色。如果给用户 user1 分配角色 role1,则 UA = UA ∪ (user1, role1)。

(2)权限分配(PA):PA⊆PERMISSIONS×ROLES。PA 是多对多的关系,记录管理员为角色所分配的权限。如果把权限 permissions1 分配角色 role1,则 PA = PA ∪ (permission1, role1)。

(3)用户登录:user_sessions⊆USERS×SESSIONS。用户登录系统后,系统为用户开启一个会话。user_sessions 是一对多的关系,因为在某些系统中一个用户可以同时登录多次,那么一个用户就同时拥有多个会话。

(4)激活与去活角色:session_roles⊆SESSIONS×ROLES。用户属于角色,会话与角色之间具有对应关系,通过会话可以激活角色,用户就拥有了被激活角色的权限;去活角色是激活角色的反向操作,当用户不需要被激活角色的权限时,通过会话终止已经被激活的角色。

2　Oracle 基于角色访问控制

Oracle 有两种类型的权限,分别是系统权限和对

象权限[8]。可以将权限直接授予用户,也可以先将权限授予角色,再将角色授予用户。

2.1 系统权限

系统权限是指允许用户在数据库的任何模式上执行特定操作所需要的权限。这些操作包括建立、修改和删除数据库对象,数据库对象包括表、视图、回退段、过程、函数、包等。系统权限没有指定任何对象,但在数据库一级上被授予。有些系统权限的功能很强大,只应该授予给可信任的用户。

Oracle 提供了 100 多种系统权限,可以划分为如下三类[9]:

(1)允许在系统范围内操作的权限,如 CREATE SESSION、CREATE TABLESPACE 等;

(2)允许用户在自己的模式内管理对象的权限,如 CREATE TABLE、CREATE VIEW 等;

(3)允许在任何模式内管理对象的权限,如 CREATE ANY TABLE 等。

2.2 对象权限

对象权限是指对一个特定对象进行操作所需要的权限。一个对象的拥有者拥有对对象的所有权限。对象拥有者可以将对象上的权限授予数据库的其他用户,也可以授权给别的用户。对每一类对象可以授予的对象权限可分为 8 类,如表 1 所示[4]。

表 1 Oracle 对象权限

No	Object Privilege	Table	View	Function	Sequence
1	ALTER	◆			◆
2	DELETE	◆	◆		
3	EXECUTE			◆	
4	INDEX	◆			
5	INSERT	◆	◆		
6	REFERENCES	◆			
7	SELECT	◆	◆		◆
8	UPDATE	◆	◆		

2.3 角色分类

在 Oracle 中,通过使用角色,显著地降低权限授予次数,可以进行动态管理,还可以在应用程序中选择要使用的权限。角色包括预定义角色和自定义角色两类。

自定义角色是指建立了数据库之后所建立的角色。建立角色使用 CREATE ROLE 命令,该命令通常由 DBA 执行。如果以其他用户身份建立角色,要求必须具有 CREATE ROLE 系统权限。建立角色时,可以指定角色的验证方式:不验证、数据库验证、OS 验证等。

预定义角色是指 Oracle 所提供的角色,是在建立数据库、安装数据字典视图和 PL/SQL 包时建立的,并且每种角色都用于执行一些特定的管理任务。预定义角色大体可分为四类,如表 2 所示。

表 2 Oracle 预定义角色分类

角色类别	描述
CONNECT	可以登录 Oracle,不可以创建实体,不可以创建数据库结构。当建立了用户后,多数情况下先给用户授予 CONNECT 和 RECOURCE 权限
RECOURCE	具有一般应用开发人员所需要的大多数权限。例如建立存储过程、触发器等
DBA	拥有全部特权,是系统最高权限,只有 DBA 才可以创建数据库结构。具有 WITH ADMIN OPTION 选项。默认的 DBA 用户为 SYS 和 SYSTEM
OTHER	不属于上述三类的角色。如执行数据库的导入和导出、查询数据字典视图、建立恢复目录等

3 SQL Server 基于角色访问控制

在 SQL Server 中,角色用来集中管理数据库或服务器的权限。DBA 将操作数据库的权限赋予角色,再将角色赋予用户,从而使用户拥有相应的权限。SQL Server 中有三种角色,固定服务器角色、固定数据库角色和用户自定义的数据库角色[10]。

3.1 固定服务器角色

一台计算机可以承担多个 SQL Server 服务器的管理任务。固定服务器角色是对服务器级用户即登录账号而言的。是指在登录时授予该登录账号对当前服务器范围内的权限。这类角色可以在服务器上进行相应的管理操作,完全独立于某个具体数据库。

固定服务器角色的信息存储在 master 数据库的 sysxlogins 系统表中,如表 3 所示。固定服务器角色不能被删除、修改和增加;固定服务器角色的任何成员都可以将其他的登录账号增加到该服务器角色中[11]。

表 3 SQL Server 固定服务器角色

No	角色	描述
1	sysadmin	能够执行 SQL Server 上的任何操作
2	serveradmin	对数据库服务器进行配置
3	setupadmin	添加或删除用户 ID
4	securityadmin	访问和安全操作(添加登录、读取错误日志、运行系统过程)
5	processadmin	管理进程(中止正在运行的查询、添加其他登录、取消用户进程)
6	dbcreator	对数据库进行操作(包括建立、修改、删除等操作)
7	diskadmin	对磁盘文件(数据文件、日志文件)进行管理
8	bulkadmin	通过 SQL 语句将本地或远程的数据文件批量导入到数据库中

3.2 固定数据库角色

在一个服务器上可以创建多个数据库,数据库角色对应于单个数据库。固定数据库角色是指 SQL Server 为每个数据库提供的固定角色,信息存储在 sysuers 系统表中,如表 4 所示。可以使用企业管理器查看固定数据库角色,还可以将某些数据库用户添加到固定数据库角色中,使数据库用户成为该角色的成员。也可以将固定数据库角色的成员删除。

表 4　SQL Server 固定数据库角色

No	角色	描述
1	Public	维护所有默认权限
2	db_owner	执行所有数据库角色活动
3	db_accessadmin	权限维护(增加用户、组和角色)
4	db_addadmin	增加、修改或删除数据库对象
5	db_securityadmin	执行语句和对象权限管理
6	db_backupoperator	备份和恢复数据库
7	db_datareader	检索任意表中的数据
8	db_datawriter	增加、修改和删除表中的数据
9	db_denydatareader	不能检索任意一个表中数据
10	db_denydatawriter	不能修改任意一个表中的数据

3.3　用户自定义角色

在许多情况下,固定数据库角色不能满足要求,就需要新角色来完成,而新角色需要系统管理员自己定义,称为用户自定义角色。包括标准角色和应用程序角色两种。

标准角色用于正常的用户管理,可以包括成员。先将用户根据不同权限划分为不同的组,通过对组授权来实现管理的安全性[12]。

应用程序角色是一种特殊角色,通过特定的应用程序存取数据,也可以限定用户对语句或对象的许可。应用程序角色需要指定口令,是一种安全机制。一旦用户使用应用程序角色,就不能使用数据库中的其他角色。

标准角色是通过把用户加入到不同的角色当中而使用户具有相应的语句许可或对象许可,而应用程序角色是首先将权限赋予应用程序,然后将逻辑加入到某一特定的应用程序中,从而通过激活应用程序角色而实现对应用程序存取数据的可控性。只有应用程序角色被激活,角色才是有效的,用户便可以且只可以执行应用程序角色相应的权限。

4　对比分析

通过以上对“Oracle 基于角色访问控制”和“SQL Server 基于角色访问控制”的研究,对数据库系统 Oracle 与 SQL Server 基于角色访问控制对比分析如下:

(1)SQL Server 具有固定服务器角色,可以通过这些固定服务器角色直接为用户制授权,简化了授权操作的复杂性。

(2)在 SQL Server 中,数据库对象的创建者具有对该对象的全部操作权限,而不需要任何额外的授权工作就能实现对该对象的完全控制。而非数据库所有者只能通过授权过程才能完成对数据库对象的特定操作。

(3)Oracle 的权限按其应用范围可分为系统级权限和对象级权限。系统级权限是对整体数据库的各种操作以及对某类群体对象的使用权,通常由 DBA 负责授权;对象级权限是对数据库单一对象的使用权,通常由该对象的拥有者负责授权。

(4)在 Oracle 中,进行授权工作可以使用操作系统命令或图形用户界面工具将角色分配给数据库中的用户。但由于 Oracle 的图形用户界面工具大多是第三方产品,在功能及版本等方面受到限制,大多数 DBA 都使用操作系统命令。在 SQL Server 中,图形用户界面工具是由数据库系统开发商提供的,功能强大且容易使用,所以 SQL Server 中进行授权工作通常使用图形用户界面工具。

(5)Oracle 建立角色时可以指定验证方式。如果是公用角色或用户默认角色,可以采用不验证方式。当建立角色时,如果不指定任何验证方式,表示该角色使用不验证方式。数据库验证方式是指使用数据库来检查角色、口令的方式。当采用这种方式时,角色名及口令存放在数据库,当激活角色时,必须提供口令。对于用户所需要的私有角色来说,在建立角色时应该为其提供口令。

(6)SQL Server 提供了应用程序角色。应用程序角色是一个数据库主体,它使应用程序能够用其自身的、类似用户的特权来运行。使用应用程序角色,可以只允许通过特定应用程序连接的用户访问特定数据。与数据库角色不同的是,应用程序角色在默认情况下不包含任何成员,而且是非活动的。应用程序角色是数据库级别的主体。

(7)Oracle 的授权粒度较少,没有通常的图形用户界面工具,相对于 SQL Server 繁琐,但安全性级别较高。SQL Server 的授权粒度较大,数据库开发商提供了统一的图形用户界面工具,授权简单容易。如果对数据库的安全性要求较高,建议选择 Oracle;如果 DBA 的技术水平一般,建议选择 SQL Server。

5　结束语

数据库的安全性是数据库管理的重要工作之一。数据库安全管理的重要机制就是角色与权限分配[13]。权限分配是制约用户权力的机制,也是维护数据库安全的重要手段。RBAC 降低了安全管理成本和管理复杂性,解决了传统访问控制和自主访问控制管理的难题。通过将一定的系统权限或者对象权限授予一定的角色,然后将角色分配给不同的用户或者用户组,简化了数据库的权限管理,提高了权限管理的效能。角色和权限在数据库系统里对数据库安全起到关键作用,同时也是保障数据库系统安全的非常强大的一种机

(下转第 112 页)

5 结束语

文中介绍了分布式数据库系统中数据复制方法的分类,针对目前的同步复制策略的响应时间过长,系统通信消耗大的缺点,基于组通信中的原子广播机制,提出了一种基于组通信的数据库复制协议,在保证组成员节点副本一致性的同时,减小了系统通信消耗,并在模拟测试中得到了很好的验证。下一步将进一步完善分布式数据库系统中事务并发执行的冲突解决机制,以期达到更好的数据库复制效果。

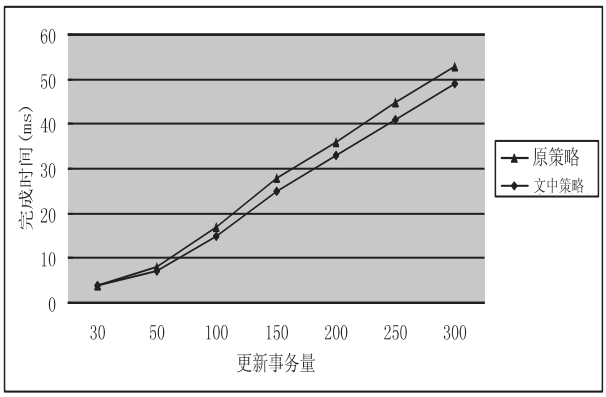


图 4 系统完成事务所需时间

参考文献:

[1] 肖迎元. 分布式实时数据库技术[M]. 北京:科学出版社,2009.

[2] Gray J, Helland P, O'Neil P, et al. The Dangers of Replication and a Solution[C]//Proceedings of SIGMOD 96. [s. l.]:[s. n.],1996:173-182.

[3] 姚 路,杨海涛,王正华,等. 基于 SyncML 协议的数据同步能力适应处理[J]. 计算机工程,2009,35(5):68-72.

[4] 刘 腾. MySQL 复制技术的研究与改进[D]. 杭州:浙江大学,2011.

[5] 王 珏,李立新,张绍月,等. 基于快照隔离的分布式数据库同步协议研究与实现[J]. 计算机应用研究,2012,29(8):3012-3017.

[6] Kemme B, Jiménez-Peris R, Patiño-Martínez M. Database Replication[M]. [s. l.]:Morgan and Claypool,2010.

[7] Amir Y, Tutu C. From total order to database replication[C]//Proceedings of International Conference on Distributed Computing Systems (ICDCS). [s. l.]:[s. n.],2002:494-503.

[8] 舒 后,段成华. 高效同步复制模型的研究[J]. 计算机工程与应用,2003,39(8):194-197.

[9] Júnior A T C. Practical Database Replication[D]. Minho: Minho University,2010.

[10] Kemme B, Pedone F, Alonso G, et al. Using optimistic atomic broadcast in transaction processing systems[J]. IEEE Trans on Knowledge Data Engineering,2003,15(4):1018-1032.

[11] Kemme B, Alonso G. Database replication: a tale of research across communities[J]. Proc of VLDB,2010,3(1-2):5-12.

[12] Amir Y, Nita-Rotaru C, Stan-Ton J, et al. Secure spread: an integrated architecture for secure group communication[J]. IEEE Trans on Dependable and Secure Computing,2005,2(3):248-261.

(上接第 107 页)

制。RBAC 是一种广泛使用的访问控制模型,但在有些环境中很难应用[14]。目前基于模糊的 RBAC 受到关注,通过模糊关系,使授权的相关信息是模糊的,扩大了适用环境,是未来的发展方向。

参考文献:

[1] 张 敏,徐 震,冯登国. 数据库安全[M]. 北京:科学出版社,2005.

[2] 陈红梅,葛德江. SQL Server 中基于角色的访问控制应用[J]. 电脑知识与技术,2008,3(25):1375-1377.

[3] 王晓超,赵卫东,左青香. 基于元数据和角色控制的用户权限管理[J]. 计算机技术与发展,2012,22(3):233-236.

[4] 王海亮,林立新,焦大光,等. Oracle10g 快速入门[M]. 北京:中国水利水电出版社,2007.

[5] 李 岚. 基于角色的数据库安全访问控制的应用[J]. 通信技术,2008,41(10):70-72.

[6] Kim S, Kim Dae-Kyoo, Kim S. A feature-based approach for modeling role-based access control systems[J]. Journal of Systems and Software,2011,84(12):2035-2052.

[7] Richard D, Edward J, Timothy R. Adding Attributes to Role-based Access Control[J]. IEEE Computer,2010,43(6):79-81.

[8] ScienceDirect. Practical Oracle Security[EB/OL]. 2012-07-11. http://www.sciencedirect.com/science/.

[9] 冯凤娟. Oracle 数据库体系结构和管理[M]. 北京:清华大学出版社,2003.

[10] Dewson R. SQL Server2005 基础教程[M]. 北京:人民邮电出版社,2006.

[11] England K, Powell G. Microsoft SQL Server 2005 Performance Optimization and Tuning Handbook[M]. [s. l.]: Digital Press,2007.

[12] 源码天空. SQL 用户自定义角色的创建[EB/OL]. 2012-07-11. http://www.codesky.net/article/201010/144597.html.

[13] 田学志,邵保华. 浅析 Oracle 中的角色与权限[J]. 黑龙江生态工程职业学院学报,2008,21(4):74-75.

[14] Martínez-García C, Navarro-Arribas G, Borrell J. Fuzzy Role-based Access Control[J]. Information Processing Letters,2011,111(10):483-487.

Oracle与SQL Server基于角色访问控制对比分析

作者： 郑丽娟， 李仲秋， 任永昌
作者单位： 郑丽娟(渤海大学 大学计算机教研部,辽宁 锦州121013)， 李仲秋,任永昌(渤海大学 信息科学与技术学院,辽宁 锦州121013)

刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2013(5)