数据库的访问控制

本 章 概 要

4.1 访问控制策略概述

4.2 自主访问控制

4.3 强制访问控制

4.4 多级安全访问控制模型

4.5 安全数据视图模型

4.6 贾让第一沙胡模型

4.7 RBAC96模型

4.1 访问控制策略概述

在数据库中，访问控制可以分为两大类：

（1）基于能力的访问控制：以访问主体为判断对象实现访问控制。访问主体能力列表中的一个元素表示为一个二元组（o, a），其中o表示资源客体，a表示一种访问控制方式。

（2）基于访问控制列表的访问控制：以资源客体为判断对象实现访问控制。资源客体访问控制列表中的一个元素表示为一个二元组（s, a），其中s表示访问主体，a表示一种访问控制方式。

4.1 访问控制策略概述

4.1.1 自主访问控制概述

- 自主访问控制是一种最为普遍的访问控制手段，用户可以按自己的意愿对系统的参数做适当修改以决定哪些用户可以访问他们的资源，亦即一个用户可以有选择地与其它用户共享他的资源。用户有自主的决定权。

自主访问控制模型中，用户对信息的控制基于对用户的鉴别和访问规则的确定。它基于对主体及主体所属的主体组的识别，来限制对客体的访问，还要校验主体对客体的访问请求是否符合存取控制规定来决定对客体访问的执行与否。这里所谓的自主访问控制是指主体可以自主地（也可能是单位方式）将访问权，或访问权的某个子集授予其它主体。

4.1.2 强制访问控制概述

- 强制访问控制是指主体与客体都有一个固定的安全属性。系统通过检查主体和客体的安全属性匹配与否来决定一个主体是否可以访问某个客体资源。安全属性是强制性的规定，它是由安全管理员，或者是操作系统根据限定的规则确定的，用户或用户的程序不能加以修改。

如果系统认为具有某一个安全属性的主体不适于访问某个资源，那么任何人（包括资源的拥有者）都无法使该主体具有访问该文件的权力。

强制安全访问控制可以避免和防止大多数数据库有意或无意的侵害，因此在数据库管理系统中有很大的应用价值。