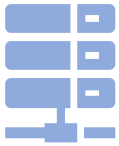
北京航空航天大學
BEIHANG UNIVERSITY

数据管理技术

北京航空航天大学

周号益

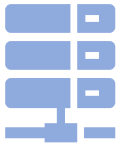
2024年



第七章 数据库安全

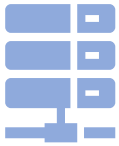
数据库安全

- 问题的提出
  - 数据库的一大特点是数据可以共享
  - 数据库系统中的数据共享不能是无条件的共享
    - ✓ 数据库中数据的共享是在DBMS统一的严格的控制之下的共享，即只允许有合法使用权限的用户访问允许他存取的数据
  - 数据共享必然带来数据库的安全问题
    - ✓ 数据库的安全是指保护数据库，防止因用户非法使用数据库造成数据泄露、更改或破坏等恶意人为破坏问题。



数据库安全

- 安全认证
- 访问控制
- 数据保护
- 数据审计



数据库安全认证

- 安全认证
  - 确认试图登录数据库的用户是否被授权访问数据库的过程
- 认证方式
  - 数据库认证
  - 外部认证：
    - 由操作系统或网络服务执行身份验证
    - 通过中间层服务器来验证用户的身份
    - 其它认证方式...

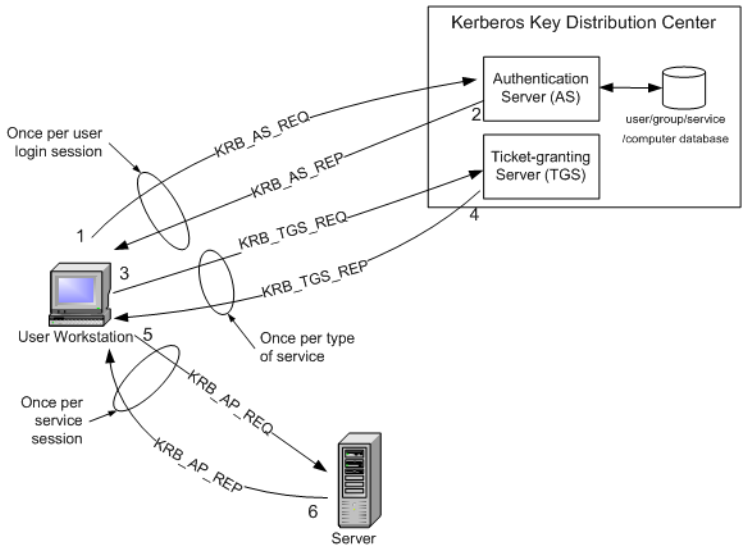
数据库认证

- 数据库认证
  - 使用存储在数据库中的信息对连接到数据库的用户进行验证
  - 最常用的方法：密码认证
- 缺点：
  - 密码容易被盗、伪造和滥用
  - 难以应对复杂的网络攻击
  - 频繁的认证操作影响数据库性能
- 加强密码认证的安全措施
  - 建立密码复杂性标准
  - 密码不包含敏感词，如用户名等
  - 设定密码时效性，定期修改密码

数据库外部认证

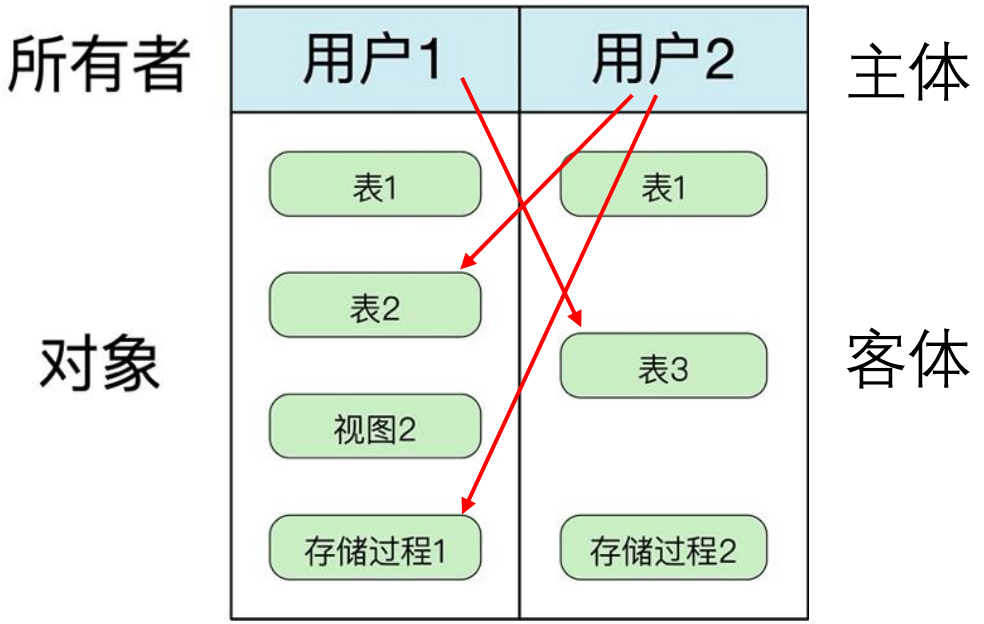
- 外部认证
  - 强身份认证：进行双因素(如密码+短信)或多因素身份验证
  - 代理认证：让中央设施对网络的所有成员进行身份验证
- 强身份认证优点
  - 可根据需要选择不同的身份验证机制
    - 操作系统认证
  - 减少数据库管理开销，提高数据库性能
- 代理认证优点
  - 有效解决网络上节点伪造身份
  - 减少每个数据库认证开销

Kerberos协议：网络身份验证协议



访问控制

- 访问控制
  - 按照用户的身份和权限，控制用户对数据库中数据访问
- 权限
  - 允许或拒绝数据库用户提出的数据访问请求
- 访问控制关注的问题
  - 阻止访问：无权限时，主体不能访问客体
  - 确定访问权限：确定主体是否有权对客体进行访问
  - 授予访问权限：授予主体访问客体的权限
  - 撤销访问权限：删除主体对客体的访问权限

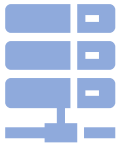


访问控制

- 定义存取权限
  - 在数据库系统中，为了保证用户只能访问他有权存取的数据，必须预先对每个用户定义存取权限。
- 检查存取权限
  - 对于通过鉴定获得上机权的用户（即合法用户），系统根据他的存取权限定义对他的各种操作请求进行控制，确保他只执行合法操作。
- 存取权限由两个要素组成
  - 数据对象
  - 操作类型

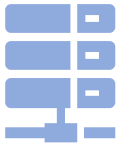
访问控制

- 权限分类
  - 系统权限
    - ✓ 启动、关闭数据库
    - ✓ 转储、恢复数据库
    - ✓ 创建、删除数据库等等
  - 数据对象权限
    - ✓ 对基本表， 视图， 存储过程，函数等数据库对象的操作权限
      - ✓ 增加、删除、修改等
  - 列级权限：包括列的添加、修改、删除等
  - 行级权限：包括行的插入、修改、删除等
  - 连接级权限：包括连接控制等



访问控制

- SQL DCL（Data Control Language)中的权限控制语句
  - 权限授予： Grant
  - 权限收回：Revoke
- 例:
  - 对指定用户授予、收回表级查询权限
    - ✓ Grant select on TableA on UserA
    - ✓ Revoke select on TableA from UserA
  - 限定列级权限
    - ✓ Grant select (a, b) on TableA on UserA

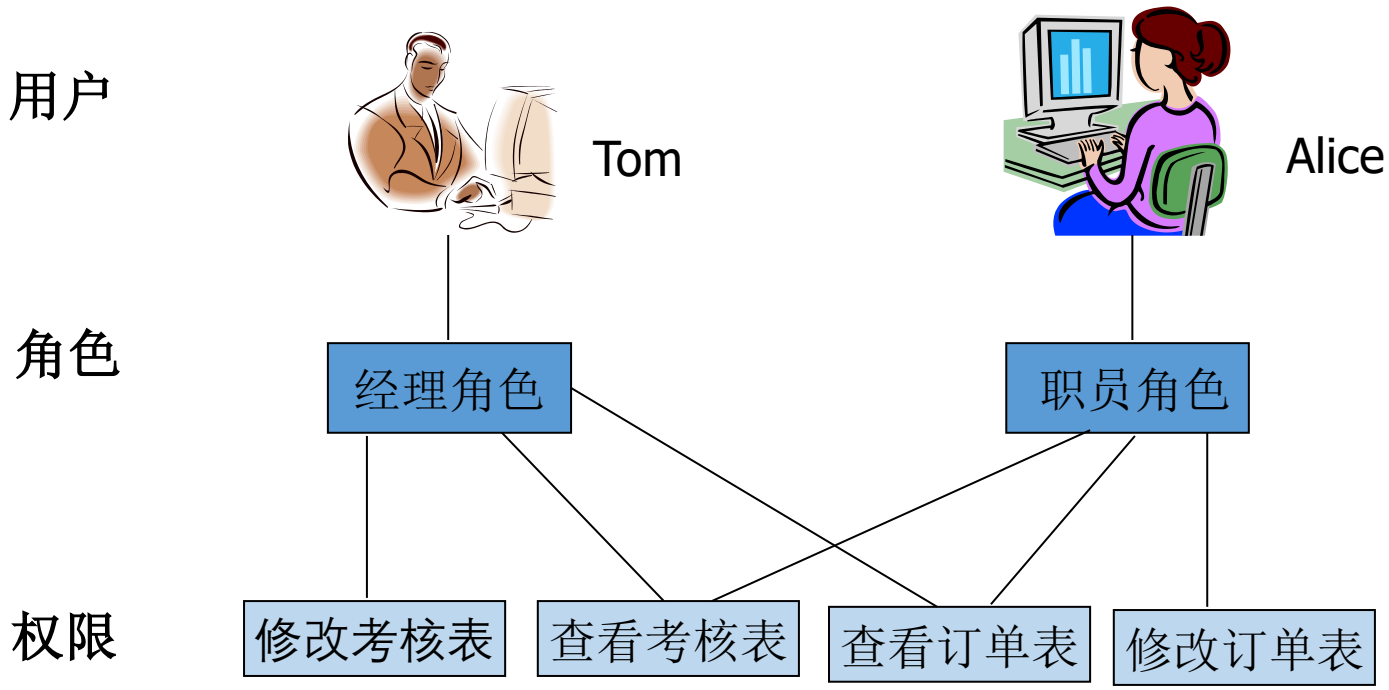


访问控制

- 如何创建新用户?
  - Create user username IDENTIFIED BY ‘password’
  - Grant Usage on dbname.* to username@ ‘%’
    - 授予基本的登录数据库和查看数据的权利
- 谁才能授予、收回权限?
  - 数据对象的创建者
  - DBA
  - 拥有传播权限的用户
    - With Grant Option
    - Grant select on TableA on UserA with grant option
    - 此时UserA可以向其他用户授予TableA的Select权限

访问控制

- 角色
  - 角色是命名的权限集合，使用角色可以方便的进行授权管理



基于角色的访问控制（Role Based Access Control，RBAC）

访问控制

- 角色分类
  - 服务器角色
    - ✓ 系统内建，不可自建
  - 数据库角色
    - ✓ 可自建
  - Public角色
    - ✓ 代表所有用户都具有的权限集合
- 角色可以从属于别的角色，获得别的角色定义的权限（即角色可以继承）

访问控制

- 创建角色
  - Create Role roleA;
    - ✓ 当前用户需具备创建角色的权限
- 向角色逐个授予权限
  - Grant insert, delete on tableA to roleA; Grant execute on procedureA to roleA…
- 将角色赋予指定用户
  - Grant roleA to UserA
  - 此时UserA就继承了roleA的权限
  - 也可以对用户UserA赋予roleA之外的权限

作业

- 课本第154页第1， 6题
- 提交时间：下次上课之前