第15章 用户、角色与权限控制

- 在数据库中，数据库的一个重要特性就是安全性。安全性是指保护数据库，以防止不合法的使用所造成的数据泄露、修改和删除。只有使用了合法的用户登录之后，才可以对数据库进行各种操作。这就要求数据库对用户的权限进行控制。本章主要讲解用户及用户的创建、权限及权限的分配、角色及角色的使用。

15.1 用户

- Oracle用户是指可以访问数据库对象的账号，它由管理员管理。每个连接到数据库的用户必须是系统的合法用户。Oracle用户分为两类：系统用户即具有系统管理权限的用户；普通用户。Oracle数据库在创建时，会提供若干默认用户（如系统用户system）；系统用户可以在登录数据库后创建其他用户。本节主要讲述Oracle用户的概况，以及讲解如何创建普通用户。

15.1.1 查看Oracle用户信息

- Oracle数据库有自带的用户，通过视图dba_users可以查询用户的详细信息。我们搜寻视图内容来查看Oracle中的用户概况。

15.1.2 创建新的用户

- Oracle用户是用连接数据库和访问数据库对象的。在开发过程中，除了系统用户外，我们希望单独创建新的用户来管理项目。当利用system用户登录Oracle数据库后，就可以创建用户了。创建新用户的语法如下所示：
- create user 用户名 identified by 密码 default tablespace 名称空间
- 其中，create user命令用户创建新的用户，并指定用户名；identified by选项是必需的，用于指定新用户的密码；default tablespace用于指定新建用户的默认表空间，新用户登录之后，所有操作均默认在该名称空间进行。
- 数据库创建伊始，可以利用系统用户登录，并创建普通用户。

15.1.3 使用模式

- 模式（Schema）是数据库对象的集合。模式是用来创建管理对象的。Schema里面包含了各种对象如表、索引、视图、存储过程等。一个用户一般对应一个Schema，该用户的Schema名等于用户名，并作为该用户缺省Schema。我们可以通过视图dba_objects来查看一个对象的拥有者。

15.1.4 系统用户system与sys

- 在Oracle数据库数据库中，初始状态下，存在的系统默认用户包括sys和system。用户sys是最高权限者，拥有数据字典，可以启动、修改、关闭数据库。system用户是默认的系统管理员，可以创建、删除用户，但不能启动和关闭用户，权限仅次于sys用户。
- 我们在15.1.1节中提到，一个用户的状态有可能是EXPIRED & LOCKED，即被锁定的。

15.2 管理权限

- 如果用户要访问数据库，那么需要为该用户分配对应的权限。为了保证数据库的安全性，就要控制好用户的权限。Oracle数据库中的权限包括系统权限和对象权限。

15.2.1 管理系统权限

- Oracle数据库中，对数据库系统级的操作都可以成称为系统权限。这些权限不指向具体对象，而是针对某种操作而言。例如，创建表的权限，当表未创建时，自然无从谈针对特定表的权限。
- 1、获得系统权限信息
- 视图dba_sys_privs描述了各种系统权限及权限分配情况。我们可以通过指定用户名来查看该用户所具有的系统权限。

15.2.1 管理系统权限

- 2、分配系统权限
- 【示例15-1】对于一个新建用户，是不具有任何权限的。以新用户test2012为例，在视图dba_sys_privs中搜寻其权限信息。
- （1）利用用户test2012登录数据库，Oracle将抛出错误。
- （2）为用户分配权限应该使用命令grant，其语法形式如下所示。
- grant privilege to grantee
- 其中grant用于分配权限；privilege为权限名称；to grantee用于指定权限分配的对象——一般为用户或者角色。在这里，我们暂时讨论用户。将create session的权限分配给用户test2012。

15.2.1 管理系统权限

- （3）用户test2012一旦具有了create session权限，将可以成功登录数据库。
- （4）虽然已经成功登录数据库，但是用户test2012几乎不能做任何事情。
- （5）我们必须为该用户分配创建表的权限。
- （6）利用用户test2012，再次尝试创建表student2012。此时，用户test2012将可成功创建新表。
- （9）而利用system用户可以查看用户test2012此时的系统权限信息。

15.2.1 管理系统权限

- 3、admin option选项
- 对于系统权限，在分配时还可以指定admin option选项。admin option表示当前被授权的用户还可以给其他用户进行系统权限的授予。如对于用户test2012，其create session和create table的权限是由system用户分配。在分配时，并未指定admin option选项。所以，用户test2012是无法将自身的create session和create table权限传播给其他用户的。
- 【示例15-2】新建用户test_user，并利用已有用户test2012为其分配权限。

15.2.1 管理系统权限

- 4、收回用户的系统权限
- 权限不仅可以授予，也允许收回，为一个用户赋予过多的权限是不安全的。根据实际业务需求，可以对其进行权限收回。权限收回时，可以利用revoke命令。其语法形式如下所示。
- revoke privilege from grantee
- revoke命令用户收回权限；privilege为权限名称；from grantee指定从哪个用户或角色收回权限。
- 【示例15-3】可以利用revoke命令收回用户test2012的权限。