**新建项目**

**计算机学院（软件学院）实验报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **学生姓名** | 徐可可 | **学号** | 171530425 | **实验成绩** |  |
| **专业** | 软件工程 | **班级** | 软工四班 | **实验日期** | 19年11月12日 |
| **课程名称** | 数据库原理 | | | **任课教师** | 马丽 |
| **实验名称** | 数据库安全性 | | | **实验序号** | 4 |
| **实验地点** | S411 | **实验台号** | 25 | **指导教师** | 马丽 |
| 1. **实验目的及要求**   1. 熟练使用DBMS提供的功能组件来实现为数据库中添加用户和角色，以及对用户和角色进行权限管理。  2. 掌握不同的登录帐户及数据库用户对数据库对象的访问权限。 | | | | | |
| **二、实验内容（或实验原理、实验拓扑）**  1. 登录管理。  2. 角色管理。  3. 权限管理。 | | | | | |
| **三、实验设备与环境**  1. 阿里云服务器：Intel(R) Xeon(R) Platinum 8269CY CPU @ 2. 50GHz、2G内存、40G高效云盘、Windows Server 2019 数据中心版、Microsoft SQL Server 2008 R2  2. 本地高配笔记本：Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz  、16G内存、48TB分布式硬盘、Windows 10 1909政府版、SQL Server Management Studio 18.4 | | | | | |
| **四、实验设计方案（包括实验步骤、设计思想、算法描述或开发流程等）** 第一阶段  1. 启动DBMS服务器，视情况决定是否附加实验用数据库。 2. 登录管理 (1) 新建登录名。 (2) 查看登录属性。 (3) 删除登录名。 (4) 开启sa账号。 3. 用户管理 (1) 新建数据库用户 (2) 查看数据库用户属性 (3) 删除数据库用户 4. 角色管理 (1) 服务器角色 设置服务器角色 查看登录的所属服务器角色 (2) 数据库角色 ①固定数据库角色 查看固定数据库角色db\_datawriter的属性，并将数据库用户u2添加到该角色中。 ②用户定义数据库角色 创建用户定义数据库角色db\_user 5. 权限管理 (1) 使用SSMS管理权限 ①管理SC表的权限。 属性-权限-添加-搜索-选择指定的用户或角色-设置权限 (2) 使用T-SQL管理权限 ①查看数据库用户属性 ②删除数据库用户 授予用户U1对“学生-课程库” 中S表的查询和删除操作  第二阶段  1. 以Windows身份验证(管理员)登录，分别创建eshop和school数据库，其中eshop数据库中有三张表(members,products,orders)，school数据库有三张表(Student,Course,SC)，创建上述两个数据库及相应表的SQL语句，见共享文件的eshop.txt和school.txt。 2. 创建U1~U7共7个登录用户。 思考：以U1用户登录，观察该用户能访问哪些数据库，是否可以访问上述创建的eshop和school数据库？ 3. 若想用U1登录用户，访问school数据库该如何处理？ 4. 把查询Student表的权限授给用户U1,然后以U1身份登录数据库，并验证U1是否可以查询Student表，能否修改、删除表中的数据? 授权、查询、修改、删除的SQL语句如何写？ 5. 把对Student表和Course表的全部操作权限授予用户U2和U3,然后以U2身份登录数据库，并验证U2是否具有相应的权限； 授权、查询、修改、删除的SQL语句如何写？ 6. 把对表SC的查询权限授予所有用户； SQL语句如何写？ 7. 把查询Student表和修改学生学号的权限授给用户U4, 然后以U4身份登录数据库，并验证U4是否具有相应的权限； SQL语句如何写？ 8. 把对表SC的INSERT权限授予U5用户，并允许将此权限再授予用户U6； SQL语句如何写？ 9. 回收用户U4修改学生姓名的权限； SQL语句如何写？ 10. 收回所有用户对表SC的查询权限； SQL语句如何写？ 11. 使用SQL语句创建角色ROLE1； 12. 为角色授权，使得角色ROLE1拥有对Student表的SELECT、UPDATE、INSERT权限； SQL语句如何写？ 13. 将用户U1,U3和U7添加到角色ROLE1中； SQL语句如何写？ 14. 对角色ROLE1的权限进行修改，增加对Student表的DELETE权限，并回收对Student表的INSERT权限； SQL语句如何写？ 15. 删除角色ROLE1； SQL语句如何写？  第三阶段  1. 创建登录名并配置角色及用户 （1）使用sa登录SQLServer2008； （2）创建数据库sa\_test，其中创建数据表dbo.saTable； （3）创建登录名L1，具有dbcreator权限，影射用户名U1，映射数据库sa\_test，数据库角色为public； （4）创建登录名L2，具有dbcreator权限，影射用户名U2，映射数据库sa\_test，数据库角色为public。 2. 使用新登录名登录服务器并验证权限 （1）使用L1登录SQLServer2008，验证是否可以浏览表dbo.saTable； （2）创建数据库L1\_test，用户名默认为dbo，模式默认为dbo； （3）在L1\_test中创建数据表dbo.L1Table； （4）使用L2登录SQLServer2008，验证是否可以浏览表dbo.saTable； （5）创建数据库L2\_test，用户名默认为dbo，模式默认为dbo； （6）在L2\_test中创建数据表dbo.L2Table。 3. sa用户对新建用户授权 （1）使用sa登录SQLServer2008； （2）授权U1在dbo.saTable上的select权限； （3）授权U2在dbo.saTable上的insert权限。 4. 新建用户之间授权 （1）使用L1登录SQLServer2008，验证是否可以浏览表dbo.saTable中的数据，是否可以插入数据； （2）授权U2在dbo.L1Table上的select权限和insert权限； （3）授权U2在L1\_test中创建表的权限； 5. 验证用户权限并对指定属性授权 （1）使用L2登录SQLServer2008，验证是否可以浏览表dbo.saTable中的数据，是否可以插入数据； （2）验证是否可以浏览表dbo.L1Table中数据，是否可以插入数据； （3）授权U1在dbo.L2Table上的select权限和修改指定列的权限。 6. 收回权限并验证 （1）使用L1登录SQLServer2008，验证是否可以浏览dbo.L2Table中数据，是否可以修改指定的列； （2）收回U2在dbo.L1Table上的insert权限； 7. 创建角色并授权 （1）使用L1登录SQLServer2008，在L1\_test中创建数据表dbo.L1Table2； （2）创建数据库角色R1； （3）将在dbo.L1Table表上的查询和插入权限授予角色R1，将dbo.L1Table2表上的查询权限和修改指定列权限授予角色R1； （4）将用户添加到角色R1中； （5）使用L2登录SQLServer2008，验证对L1\_test中数据表的操作权限。 8. 收回角色的权限 （1）使用L1登录SQLServer2008，收回角色R1在dbo.L1Table表上的插入权限； （2）使用L2登录SQLServer2008，验证对L1\_test中数据表的操作权限。 | | | | | |

|  |
| --- |
| **五、实验结果（包括设计效果、测试数据、运行结果等）**   1. 创建登录名并配置角色及用户 （1）使用sa登录SQLServer2008； 在这里插入图片描述 （2）创建数据库sa\_test，其中创建数据表dbo.saTable； 在这里插入图片描述 （3）创建登录名L1，具有dbcreator权限，影射用户名U1，映射数据库sa\_test，数据库角色为public； 在这里插入图片描述 在这里插入图片描述 （4）创建登录名L2，具有dbcreator权限，影射用户名U2，映射数据库sa\_test，数据库角色为public。 在这里插入图片描述 在这里插入图片描述 2. 使用新登录名登录服务器并验证权限 （1）使用L1登录SQLServer2008，验证是否可以浏览表dbo.saTable； 答：不能 （2）创建数据库L1\_test，用户名默认为dbo，模式默认为dbo； 在这里插入图片描述 （3）在L1\_test中创建数据表dbo.L1Table； 在这里插入图片描述 （4）使用L2登录SQLServer2008，验证是否可以浏览表dbo.saTable； 答：不能 （5）创建数据库L2\_test，用户名默认为dbo，模式默认为dbo； 在这里插入图片描述 （6）在L2\_test中创建数据表dbo.L2Table。 在这里插入图片描述 3. sa用户对新建用户授权 （1）使用sa登录SQLServer2008； 在这里插入图片描述 （2）授权U1在dbo.saTable上的select权限； 在这里插入图片描述 （3）授权U2在dbo.saTable上的insert权限。 在这里插入图片描述 4. 新建用户之间授权 （1）使用L1登录SQLServer2008，验证是否可以浏览表dbo.saTable中的数据，是否可以插入数据； 可以浏览，不可以插入数据 （2）授权U2在dbo.L1Table上的select权限和insert权限； 在这里插入图片描述 （3）授权U2在L1\_test中创建表的权限； 在这里插入图片描述 5. 验证用户权限并对指定属性授权 （1）使用L2登录SQLServer2008，验证是否可以浏览表dbo.saTable中的数据，是否可以插入数据； 不可以浏览，可以插入 （2）验证是否可以浏览表dbo.L1Table中数据，是否可以插入数据； 均可以 （3）授权U1在dbo.L2Table上的select权限和修改指定列的权限。 在这里插入图片描述 6. 收回权限并验证 （1）使用L1登录SQLServer2008，验证是否可以浏览dbo.L2Table中数据，是否可以修改指定的列； 均可以 （2）收回U2在dbo.L1Table上的insert权限； 在这里插入图片描述 7. 创建角色并授权 （1）使用L1登录SQLServer2008，在L1\_test中创建数据表dbo.L1Table2； 在这里插入图片描述 （2）创建数据库角色R1； 在这里插入图片描述 （3）将在dbo.L1Table表上的查询和插入权限授予角色R1，将dbo.L1Table2表上的查询权限和修改指定列权限授予角色R1； 在这里插入图片描述 （4）将用户添加到角色R1中； 在这里插入图片描述 （5）使用L2登录SQLServer2008，验证对L1\_test中数据表的操作权限。 L2拥有R1的全部权限 8. 收回角色的权限 （1）使用L1登录SQLServer2008，收回角色R1在dbo.L1Table表上的插入权限； 在这里插入图片描述 （2）使用L2登录SQLServer2008，验证对L1\_test中数据表的操作权限。 无法插入数据到dbo.L1Table表。 |
| **六、实验小结（包括收获、心得体会、注意事项、存在问题及解决办法、建议等）**  数据库安全包含两层含义：第一层是指系统运行安全，系统运行安全通常受到的威胁如下，一些网络不法分子通过网络，局域网等途径通过入侵电脑使系统无法正常启动，或超负荷让机子运行大量算法，并关闭cpu风扇，使cpu过热烧坏等破坏性活动； 第二层是指系统信息安全，系统安全通常受到的威胁如下，黑客对数据库入侵，并盗取想要的资料。数据库系统的安全特性主要是针对数据而言的，包括数据独立性、数据安全性、数据完整性、并发控制、故障恢复等几个方面。 数据库安全的防护技术有：数据库加密（核心数据存储加密）、数据库防火墙（防漏洞、防攻击）、数据脱敏（敏感数据匿名化）等。 |

|  |
| --- |
| **七、附录（包括作品、流程图、源程序及命令清单等）**  在多数应用中根本用不到多少系统的存储过程，而SQL Server的这么多系统存储过程只是用来适应广大用户需求的，所以可以删除不必要的存储过程，因为有些系统的存储过程能很容易地被人利用起来提升权限或进行破坏。如果我们不需要扩展存储过程Xp\_cmdshell则可以把它去掉。 使用以下SQL语句：  use master  sp\_dropextendedproc 'Xp\_cmdshell'  Xp\_cmdshell是进入操作系统的最佳捷径，是数据库留给操作系统的一个大后门。如果我们需要这个存储过程，可以用下面这个语句恢复过来。  sp\_addextendedproc 'xp\_cmdshell', 'xpSQL70.dll'  如果我们不需要，则可以丢弃OLE自动存储过程（会造成管理器中的某些特征不能使用）。 丢弃过程如下：  Sp\_OACreate Sp\_OADestroy Sp\_OAGetErrorInfo Sp\_OAGetProperty  Sp\_OAMethod Sp\_OASetProperty Sp\_OAStop  去掉不需要的注册表访问的存储过程，注册表存储过程甚至能够读出操作系统管理员的密码来，命令如下：  Xp\_regaddmultistring Xp\_regdeletekey Xp\_regdeletevalue  Xp\_regenumvalues Xp\_regread Xp\_regremovemultistring  Xp\_regwrite  还有一些其他的扩展存储过程，也最好检查检查。在处理存储过程的时候，请确认一下，避免造成对数据库或应用程序的伤害。 |