链滴

SQL Server 相关权限

作者：Giles

原文链接：https://ld246.com/article/1626247660281

来源网站：链滴

<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/bing/20200619.jpg?imageView2/1/w/960/h/540/interlace/1/q/100">
数据库角色的成员可以分为如下几类：
1、Windows 用户组或用户账户
2、SQL Server 登录
3、其他角色
SQL Server 的安全体系结构中包括了几个含有特定隐含权限的角色。除了数据库拥有者创建的
色之外，还有两类预定义的角色。这些可以创建的角色可以分为如下几类：
1、固定服务器
2、固定数据库
3、用户自定义
4、固定服务器
由于固定服务器是在服务器层次上定义的，因此它们位于从属于数据库服务器的数据库外面。下
列出了所有现有的固定服务器角色。
<h2 id="固定服务器角色">固定服务器角色</h2>
说　明
<table>
<thead>
<tr>
<th>sysadmin</th>
<th>执行 SQL Server 中的任何动作</th>
</tr>
</thead>
<tbody>
<tr>
<td>serveradmin</td>
<td>配置服务器设置</td>
</tr>
<tr>
<td>setupadmin</td>
<td>安装复制和管理扩展过程</td>
</tr>
<tr>
<td>securityadmin</td>
<td>管理登录和 CREATE DATABASE 的权限以及阅读审计</td>
</tr>
<tr>
<td>processadmin</td>
<td>管理 SQL Server 进程</td>
</tr>
<tr>
<td>dbcreator</td>
<td>创建和修改数据库</td>
</tr>
<tr>
<td>diskadmin</td>
<td>管理磁盘文件</td>
</tr>
</tbody>
</table>
下面两个系统过程用来添加或删除固定服务器角色成员：
sp_addsrvrolemember
sp_dropsrvrolemember
注意：您不能添加、修改或删除固定服务器角色。另外，只有固定服务器角色的成员

能执行上述两个系统过程来从角色中添加或删除登录账户。
sa 登录
sa 登录是系统管理员的登录。在以前的 SQL Server 版本中不存在角色，sa 登录具有所有可能关于系统管理工作的权限。在 SQL Server 2005 中，sa 登录保持了向后兼容性。sa 登录永远是固定务器角色 syadmin 中的成员，并且不能从该角色中删除。
注意：只有当没有其他方法登录到 SQL Server 系统中时，再使用 sa 登录。
<h2 id="固定服务器角色及其权限">固定服务器角色及其权限</h2>
在某个 SQL Server 系统中，每个固定服务器角色都有其隐含的权限。使用系统过程 sp_srvrolepermission 可以浏览每个固定服务器角色的权限。该系统过程的语法形式为：
sp_srvrolepermission[[@srvrolename =] 'role']
如果没有指定 role 的值，那么所有的固定服务器角色的权限都将显示出来。下面的部分将讨论个固定服务器角色的权限。
1. sysadmin
固定服务器角色 sysadmin 的成员被赋予了 SQL Server 系统中所有可能的权限。例如，只有这角色中的成员(或一个被这个角色中的成员赋予了 CREATE DATABASE 权限的用户)才能够创建数据。
固定服务器角色和 sa 登录之间有着特殊的关系。sa 登录一直都是固定服务器角色中的成员，并不能从该角色中删除。
2. serveradmin
固定服务器角色 serveradmin 的成员可以执行如下的动作：
向该服务器角色中添加其他登录
运行 dbcc pintable 命令(从而使表常驻于主内存中)
运行系统过程 sp_configure(以显示或更改系统选项)
运行 reconfigure 选项(以更新系统过程 sp_configure 所做的所有改动)
使用 shutdown 命令关掉数据库服务器
运行系统过程 sp_tableoption 为用户自定义表设置选项的值
3. setupadmin
固定服务器角色 setupadmin 中的成员可以执行如下的动作：
向该服务器角色中添加其他登录
添加、删除或配置链接的服务器
执行一些系统过程，如 sp_serveroption
4. securityadmin
固定服务器角色 securitypadmin 中的成员可以执行关于服务器访问和安全的所有动作。这些成可以进行如下的系统动作：
向该服务器角色中添加其他登录
读取 SQL Server 的错误日志
运 行如下的系统过程：如 sp_addlinkedsrvlogin、sp_addlogin、sp_defaultdb、 sp_defaultlnguage、sp_denylogin、sp_droplinkedsrvlogin、sp_droplogin、 sp_grantlogin、sp_helplogin、sp_remoteoption 和 sp_revokelogin(所有这些系统过程都与系统安 全相关。)
5. processadmin
固定服务器角色 processadmin 中的成员用来管理 SQL Server 进程，如中止用户正在运行的查。这些成员可以进行如下的动作：
向该服务器角色中添加其他登录
执行 KILL 命令(以取消用户进程)
6. dbcreator
固定服务器角色 dbcreator 中的成员用来管理与数据库创建和修改有关的所有动作。这些成员以进行如下的动作：
向该服务器角色中添加其他登录
运行 CREATE DATABASE 和 ALTER DATABASE 语句
使用系统过程 sp_renamedb 来修改数据库的名称
7. diskadmin
固定服务器角色 diskadmin 的成员可以进行如下与用来存储数据库对象的文件和文件组有关的

作：
向该服务器角色中添加其他登录
运行如下系统过程：sp_ddumpdevice 和 sp_dropdevice。
运行 DISK INIT 语句
<h2 id="固定数据库角色">固定数据库角色</h2>
固定数据库角色在数据库层上进行定义，因此它们存在于属于数据库服务器的每个数库中。下表列出了所有的固定数据库角色。
固定数据库角色
说　明

db_owner　　可以执行数据库中技术所有动作的用户
db_accessadmin　　可以添加、删除用户的用户
db_datareader　　可以查看所有数据库中用户表内数据的用户
db_datawriter　　可以添加、修改或删除所有数据库中用户表内数据的用户</stron>
db_ddladmin　　可以在数据库中执行所有 DDL 操作的用户
db_securityadmin　　可以管理数据库中与安全权限有关所有动作的用户</l>
db_backoperator　　可以备份数据库的用户(并可以发布 DBCC 和 CHECKPOINT 语，这两个语句一般在备份前都会被执行)
db_denydatareader　不能看到数据库中任何数据的用户
db_denydatawriter　不能改变数据库中任何数据的用户

除了上表中列出的固定数据库角色之外，还有一种特殊的固定数据库角色，名为 public，这里将先介绍这一角色。
<h2 id="public角色">public 角色</h2>
public 角色是一种特殊的固定数据库角色，数据库的每个合法用户都属于该角色。它为数据库中用户提供了所有默认权限。这样就提供了一种机制，即给予那些没有适当权限的所有用户以一定的(通是有限的)权限。public 角色为数据库中的所有用户都保留了默认的权限，因此是不能被删除的。

一般情况下，public 角色允许用户进行如下的操作：
使用某些系统过程查看并显示 master 数据库中的信息
执行一些不需要一些权限的语句(例如 PRINT)
<h2 id="固定数据库角色及其权限">固定数据库角色及其权限</h2>
在数据库中，每个固定数据库角色都有其特定的权限。这就意味着对于某个数据库来说，固定数库角色的成员的权限是有限的。使用系统过程 sp_dbfixedrolepermission 就可以查看每个固定数据角色的权限。该系统过程的语法为：
sp_db.xedrolepermission [[@rolename =] 'role']
如果没有指定 role 的值，那么所有固定数据库角色的权限都可以显示出来。下面的几节将讨论个固定数据库角色的权限。

db_owner

固定数据库角色 db_owner 的成员可以在特定的数据库中进行如下的动作：
向其他固定数据库角色中添加成员，或从其中删除成员
运行所有的 DDL 语句
运行 BACKUP DATABASE 和 BACKUP LOG 语句
使用 CHECKPOINT 语句显式地启动检查点进程
运行下列 dbcc 命令：dbcc checkalloc、dbcc checkcatalog、dbcc checkdb、dbcc updateuage
授予、取消或剥夺每一个数据库对象上的下列权限：SELECT、INSERT、UPDATE、DELETE 和 RFERENCES
使 用下列系统过程向数据库中添加用户或角色：sp_addapprole、sp_addrole、sp_addrolem

mber、 sp_approlepassword、sp_changeobjectowner、sp_dropapprole、sp_droprole、 sp_drprolemember、sp_dropuser、sp_grantdbaccess
使用系统过程 sp_rename 为任何数据库对象重新命名
2. db_accessadmin
固定数据库角色 db_accessadmin 的成员可以执行与数据库访问有关的所有动作。这些角色可在具体的数据库中执行下列操作：
运行下列系统过程：sp_addalias、sp_dropalias、sp_dropuser、sp_grantdbacess、sp_revokdbaccess
为 Windows 用户账户、Windows 组和 SQL Server 登录添加或删除访问
3. dbdatareader
固定数据库角色 dbdatareader 的成员对数据库中的数据库对象(表或视图)具有 SELECT 权限。而，这些成员不能把这个权限授予其他任何用户或角色。(这个限制对 REVOKE 语句来说同样成立。)
4. dbdatawriter
固定数据库角色 dbdatawriter 的成员对数据库中的数据库对象(表或视图)具有 INSERT、UPDAT 和 DELETE 权限。然而，这些成员不能把这个权限授予其他任何用户或角色。(这个限制对 REVOKE 句来说也同样成立。)
5. db_ddladmin
固定数据库角色 db_ddladmin 的成员可以进行如下的动作：
运行所有 DDL 语句
对任何表上授予 REFERENCESE 权限
使用系统过程 sp_procoption 和 sp_recompile 来修改任何存储过程的结构
使用系统过程 sp_rename 为任何数据库对象重命名
使用系统过程 sp_tableoption 和 sp_changeobjectowner 分别修改表的选项和任何数据库对的拥有者
6. db_securityadmin
固定数据库角色 db_securityadmin 的成员可以管理数据库中的安全。这些成员可以进行如下的作：
运行与安全有关的所有 Transact-SQL 语句(GRANT、DENY 和 REVOKE)
运 行以下系统过程：sp_addapprole、sp_addrole、sp_addrolemember、sp_approlepasswod、 sp_changeobjectowner、sp_dropapprole、sp_droprole、sp_droprolemember
7. db_backupoperator
固定数据库角色 db_backupoperator 的成员可以管理数据库备份的过程。这些成员可以进行如动作：
运行 BACKUP DATABASE 和 BACKUP LOG 语句
用 CHECKPOINT 语句显式地启动检查点进程
运行如下 dbcc 命令：dbcc checkalloc、dbcc checkcatalog、dbcc checkdb、dbcc updateusage
8. db_denydatareader 和 db_denydatawriter
顾名思义，固定数据库角色 db_denydatareader 的成员对数据库中的数据库对象(表或视图)没有 SELECT 权限。如果数据库中含有敏感数据并且其他用户不能读取这些数据，那么就可以使用这个角。
固定数据库角色 db_denydatawriter 的成员对数据库中的任何数据库对象(表或视图)没有 INSER、UPDATE 和 DELETE 权限。