**SQL Server 系统角色**

2011-07-14 10:37:00|  分类： [MSSQL备忘](http://xinluwork.blog.163.com/blog/#m=0&t=1&c=fks_084066086084087068087095082095092085089070085085087070) |  标签： |字号大中小 订阅

为便于管理数据库中的权限，SQL Server 提供了若干“角色”，这些角色是用于分组其他主体的安全主体。它们类似于 Microsoft Windows 操作系统中的组。数据库级角色的权限作用域为数据库范围。

SQL Server 中有两种类型的数据库级角色：数据库中预定义的“固定数据库角色”和您可以创建的“灵活数据库角色”。

固定数据库角色是在数据库级别定义的，并且存在于每个数据库中。db\_owner 和 db\_securityadmin 数据库角色的成员可以管理固定数据库角色成员身份。但是，只有 db\_owner 数据库角色的成员能够向 db\_owner 固定数据库角色中添加成员。msdb 数据库中还有一些特殊用途的固定数据库角色。

您可以向数据库级角色中添加任何数据库帐户和其他 SQL Server 角色。固定数据库角色的每个成员都可向同一个角色添加其他登录名。

重要提示：  
请不要将灵活数据库角色添加为固定角色的成员。这会导致意外的权限升级。

下表显示了固定数据库级角色及其能够执行的操作。所有数据库中都有这些角色。

数据库级别的角色名称  说明   
db\_owner  
 db\_owner 固定数据库角色的成员可以执行数据库的所有配置和维护活动，还可以删除数据库。  
   
db\_securityadmin  
 db\_securityadmin 固定数据库角色的成员可以修改角色成员身份和管理权限。向此角色中添加主体可能会导致意外的权限升级。  
   
db\_accessadmin  
 db\_accessadmin 固定数据库角色的成员可以为 Windows 登录名、Windows 组和 SQL Server 登录名添加或删除数据库访问权限。  
   
db\_backupoperator  
 db\_backupoperator 固定数据库角色的成员可以备份数据库。  
   
db\_ddladmin  
 db\_ddladmin 固定数据库角色的成员可以在数据库中运行任何数据定义语言 (DDL) 命令。  
   
db\_datawriter  
 db\_datawriter 固定数据库角色的成员可以在所有用户表中添加、删除或更改数据。  
   
db\_datareader  
 db\_datareader 固定数据库角色的成员可以从所有用户表中读取所有数据。  
   
db\_denydatawriter  
 db\_denydatawriter 固定数据库角色的成员不能添加、修改或删除数据库内用户表中的任何数据。  
   
db\_denydatareader  
 db\_denydatareader 固定数据库角色的成员不能读取数据库内用户表中的任何数据。

有关数据库级固定角色权限的特定信息，请参阅固定数据库角色的权限（数据库引擎）。

 msdb 角色  
msdb 数据库中包含下表显示的特殊用途的角色。

msdb 角色名称  说明   
db\_ssisadmin

db\_ssisoperator

db\_ssisltduser  
 这些数据库角色的成员可以管理和使用 SSIS。从早期版本升级的 SQL Server 实例可能包含使用 Data Transformation Services (DTS)（而不是 SSIS）命名的旧版本角色。有关详细信息，请参阅 使用 Integration Services 角色。  
   
dc\_admin

dc\_operator

dc\_proxy  
 这些数据库角色的成员可以管理和使用数据收集器。有关详细信息，请参阅数据收集器的安全性。  
   
PolicyAdministratorRole  
 db\_ PolicyAdministratorRole 数据库角色的成员可以对基于策略的管理策略和条件执行所有配置和维护活动。有关详细信息，请参阅使用基于策略的管理来管理服务器。  
   
ServerGroupAdministratorRole

ServerGroupReaderRole  
 这些数据库角色的成员可以管理和使用注册的服务器组。有关详细信息，请参阅创建服务器组。  
   
重要提示：  
db\_ssisadmin 角色和 dc\_admin 角色的成员也许可以将其权限提升到 sysadmin。之所以会发生此权限提升，是因为这些角色可以修改 Integration Services 包，而 SQL Server 可以使用 SQL Server 代理的 sysadmin 安全上下文来执行 Integration Services 包。若要防止在运行维护计划、数据收集组和其他 Integration Services 包时出现此权限提升，请将运行包的 SQL Server 代理作业配置为使用拥有有限权限的代理帐户，或只将 sysadmin 成员添加到 db\_ssisadmin 和 dc\_admin 角色。

 使用服务器级角色  
下表说明了用于服务器级角色的命令、视图和函数。

功能  类型  说明   
sp\_helpdbfixedrole (Transact-SQL)  
 元数据  
 返回固定数据库角色的列表。  
   
sp\_dbfixedrolepermission (Transact-SQL)  
 元数据  
 显示固定数据库角色的权限。  
   
sp\_helprole (Transact-SQL)  
 元数据  
 返回当前数据库中有关角色的信息。  
   
sp\_helprolemember (Transact-SQL)  
 元数据  
 返回有关当前数据库中某个角色的成员的信息。  
   
sys.database\_role\_members (Transact-SQL)  
 元数据  
 为每个数据库角色的每个成员返回一行。  
   
IS\_MEMBER (Transact-SQL)  
 元数据  
 指示当前用户是否为指定 Microsoft Windows 组或 Microsoft SQL Server 数据库角色的成员。  
   
CREATE ROLE (Transact-SQL)  
 命令  
 在当前数据库中创建新的数据库角色。  
   
ALTER ROLE (Transact-SQL)  
 命令  
 更改数据库角色的名称。  
   
DROP ROLE (Transact-SQL)  
 命令  
 从数据库中删除角色。  
   
sp\_addrole (Transact-SQL)  
 命令  
 在当前数据库中创建新的数据库角色。  
   
sp\_droprole (Transact-SQL)  
 命令  
 从当前数据库中删除数据库角色。  
   
sp\_addrolemember (Transact-SQL)  
 命令  
 为当前数据库中的数据库角色添加数据库用户、数据库角色、Windows 登录名或 Windows 组。  
   
sp\_droprolemember (Transact-SQL)  
 命令  
 从当前数据库的 SQL Server 角色中删除安全帐户。

 public 数据库角色  
每个数据库用户都属于 public 数据库角色。如果未向某个用户授予或拒绝对安全对象的特定权限时，该用户将继承授予该对象的 public 角色的权限。