

بسم الله الرحمن الرحيم

آموزشگاه تحلیل داده

تخصصی ترین مرکز برنامه نویسی و دیتابیس در ایران

جداسازی مالکیت از schema در SQL Server

مدرس : مهندس افشین رفوآ

دوره آموزش SQL Server Administration

جداسازی مالکیت از schema در SQL Server

یکی از مفاهیم پایه ای مبحث امنیت در SQL Server این است که مالک اشیا دارای اختیارات و مجوزهای غیر قابل بازگشت برای مدیریت اشیا ذکر شده می باشد، بدین معنا که امکان سلب این اختیارات از صاحب شی وجود نداشته و همچنین نمی توان کاربرانی که در پایگاه داده صاحب اشیایی هستند را از آن اخراج (حذف) کرد.

جداسازی schema از کاربر (user-schema separation)

جداسازی schema از کاربر این مفهوم را می رساند که شماها دیگر برابر با کاربران پایگاه داده نیستند، بلکه یک فضای نام متمایز محسوب می شوند که کاملاً از کاربری که بانک اطلاعاتی را در ابتدا امر ایجاد کرد مستقل می باشد. به عبارتی دیگر، schema صرفاً یک container است که برای اشیا نقش ظرف (دربردارنده) را ایفا می کند. کلید ی کاربران می توانند مالک schema باشند، همچنین امکان انتقال مالکیت آن به سایر کاربران وجود دارد.

جداسازی schema از کاربر (user-schema separation)، مدیریت مجوزهای اشیا پایگاه داده را به مراتب آسان تر می سازد. همان طور که پیشتر شرح داده شد، schema یک ظرف نام گذاری شده برای اشیا پایگاه داده می باشد که قابلیت گروه بندی اشیا به فضاهای نامی مجزا را به ارمغان می آورد. به عنوان مثال، می توان

پایگاه داده ی نمونه ی **AdventureWorks** را نام برد که دربردارنده ی **schema** هایی ویژه ی **Production** (بخش تولید)، **Sales** (بخش فروش) و **HumanResources** (بخش منابع انسانی) می باشد.

ساختار نگارشی:

Server.Database.DatabaseSchema.DatabaseObject

مالک ها و مجوزهای schema

هر **principal** ای می تواند مالکیت **schema** را بر عهده داشته باشد. همچنین یک **principal** قادر است همزمان مالک چندین **schema** باشد. می توان قوانین امنیتی را به یک **schema** اعمال کنید. این قوانین توسط کلید ی اشیای موجود در **schema** بر ارث برده می شوند. پس از اینکه مجوزهای دسترسی برای یک **schema** راه اندازی شد، مجوزهای مذکور همین که اشیا جدید به **schema** ی مورد نظر افزوده می شوند، به صورت خودکار اعمال می شوند. می توان به کاربران یک **schema** ی پیش فرض تخصیص داد، همچنین چندین کاربر پایگاه داده می توانند به طور همزمان در یک **schema** مشترک باشند.

به صورت پیش فرض، هنگامی که توسعه دهندگان اشایی را در یک **schema** خلق می کنند، این اشیا تحت مالکیت **security principal** (یک موجودیت است که توسط سیستم کامپیوتر یا شبکه احراز هویت می شود) قرار گرفته که خود صاحب **schema** می باشد، به عبارتی دیگر این **security principal** است که صاحب اشیا می باشد و مالکیت اشیا به توسعه دهنده تعلق ندارد. مالکیت اشیا را می توان با بهره گیری از دستور **ALTER AUTHORIZATION** انتقال داد. یک **schema** همچنین می تواند دربردارنده ی اشایی باشد که تحت مالکیت کاربران دیگر قرار داشته و دارای مجوزهایی با سطح **granularity** بالاتر در مقایسه با آن مجوزهایی است که به **schema** تخصیص داده شده است باشد، اگرچه این کار اصلا توصیه نمی شود زیرا که به موجب آن مدیریت مجوزها کمی پیچیده تر می شود (**granularity** در خصوص مجوزها، اعتباردهی و مبحث امنیت دلالت بر سطوح مختلف (متعدد) مجوزها دارد؛ قابلیت محدود سازی اجرای برخی عملیات و در عین حال اعطای مجوز به اجرای برخی دیگر). می توان اشیا را از یک **schema** به **schema** ی دیگر منتقل کرد، به طور مشابه می توان مالکیت **schema** را از یک **principal** به **principal** دیگر انتقال داد. این امکان نیز وجود دارد که کاربران را بدون تحت تاثیر قرار دادن **schema** ها از پایگاه داده حذف کرد.

Schema های توکار و درون ساخته

SQL Server با ده **schema** ی از پیش تعریف شده عرضه می شود که دارای اسم های یکسان با نقش ها و کاربران پایگاه داده توکار می باشد. **Schema** های پیش گفته غالباً به منظور ایجاد قابلیت سازگاری با نسخه های قبلی ارائه می شوند. شما می توانید آن **schema** هایی را که اسم آن ها با اسم نقش های ثابت پایگاه داده (**fixed database roles**) یکسان هست (و در حال حاضر به آن ها نیازی ندارید) را حذف کنید. با این حال اجازه ی حذف **schema** های فهرست شده در زیر به شما داده نمی شود:

dbo

guest

sys

INFORMATION_SCHEMA

اگر شما **schema** های نام برده را از پایگاه داده ی مدل پاک کنید، **schema** های حذف شده دیگر در پایگاه داده های جدید موجود نخواهند بود.

توجه

Schema های **sys** و **INFORMATION_SCHEMA** برای اشیا سیستم رزرو شده اند، از این رو شما نمی توانید در این **schema** ها شی ایجاد کرده و یا شی از آن حذف کنید.

dbo Schema

dbo، **schema** ی پیش فرض یک پایگاه داده ی جدید بوده و تحت مالکیت حساب کاربری **dbo** می باشد. کاربرانی که از طریق اجرای دستور **CREATE USER Transact-SQL** ایجاد می گردند، **dbo** به عنوان **schema** ی پیش فرض، خودکار به آن ها اختصاص می یابد.

کاربرانی که **dbo** به آن ها تخصیص می یابد، مجوزهای حساب کاربری **dbo** را نیز به ارث می برند. دقت داشته باشید که این کاربران نیستند که از **schema** مجوز به ارث می برند بلکه مجوزهای حساب کاربری **dbo** توسط اشیا پایگاه داده ی موجود در **schema** ی مورد نظر به ارث گرفته می شوند.

توجه

زمانی که اشیا مورد نظر توسط اسمی که تنها از یک بخش تشکیل شده مورد اشاره قرار می گیرند (ارجاع داده می شوند)، **SQL Server** ابتدا در **schema** ی پیش فرض کاربر جستجو را انجام می دهد. در صورت یافت نشدن شی مدنظر، **SQL Server** جستجوی خود را در **dbo** ادامه می دهد. حال چنانچه شی مورد نظر در **dbo** نیز نبود، یک پیغام خطا بازگردانده می شود.

Tahildadeh