بسم الله الرحمن الرحیم

آموزشگاه تحلیل داده

تخصصی ترین مرکز برنامه نویسی و دیتابیس در ایران

نقش های سرویس دهنده و پایگاه داده در SQL Server

مدرس : مهندس افشین رفوآ

دوره آموزش SQL Server Administration

نقش های سرویس دهنده و پایگاه داده در SQL Server

تمامی نسخه های SQL Server از امنیت مبتنی بر نقش بهره می گیرند که امکان تخصیص مجوزهایی را (بجای تنها یک کاربر) به یک نقش یا گروهی از کاربران فراهم می آورد. نقش های ثابت سمت سرور و پایگاه داده، یک مجموعه ای ثابت از مجوزها دارند که به آن ها تخصیص یافته.

نکته ی امنیتی

نقش های ثابت سمت سرور مجموعه مجوزها و اختیاراتی هستند که به کل نمونه ی SQL Server اعمال می شود. این نقش ها قابلیت اصلاح یا حذف شدن را ندارند، با این وجود می توان به آن ها اعضای جدید اضافه کرد.

نقش ثابت سمت سرور sysadmin تمامی نقش های سایر را دربر می گیرد و دارای حوزه ی نامحدود می باشد. توصیه می کنیم تا زمانی که مطمئن نشدید principal ها کاملا قابل اطمینان می باشند، principal به این نقش اضافه نکنید. همان طور که می دانید principal ها موجودیت هایی هستند که می توانند از SQL Server منابع مورد نیاز را درخواست کند. عضوهای نقش sysadmin از اختیارات و مجوزهای مدیریتی غیر قابل فسخ در تمامی منابع و پایگاه های داده ی سرور برخوردار هستند.

در اضافه کردن کاربران جدید به نقش های ثابت سمت سرور (fixed server role)، همیشه بهترین گزینه را انتخاب کنید. به عنوان مثال، نقش bulkadmin به کاربران اجازه می دهد محتویات فایل های محلی را در یک جدول درج کند که این خود باعث به خطر افتادن جامعیت اطلاعات می شود.

نقش های ثابت پایگاه داده (fixed database roles)

نقش های ثابت پایگاه داده مجموعه ای از مجوزها و اختیارات درسطح پایگاه داده هستند.

نقش های ثابت پایگاه داده یک سری مجوز از پیش تعریف شده دارند که امکان مدیریت آسان گروهی از مجوزها را فراهم می سازد. عضوهای نقش db_owner می تواند تمامی عملیات و فعالیت های مربوط به پیکربندی و نگهداشت را بر روی پایگاه داده اجرا کنند.

نقش های کاربری و کاربران پایگاه داده

برای مهیا شدن زمینه کار با اشیا پایگاه داده، لاگین ها بایستی به حساب های کاربری پایگاه داده نگاشت شوند ، پس از آن می توان کاربران پایگاه داده را به نقش های پایگاه داده اضافه کرد. از این طریق کاربران پایگاه داده کلیه ی مجموعه مجوزهای مربوط به آن نقش ها را به ارث می برند و بستر اعطای تمامی مجوزها فراهم می آید.

در این میان باید ، حساب کاربری dbo و همچنین حساب guest را به هنگام طراحی و تعبیه ی امنیت برای برنامه ی کاربردی خود لحاظ کرد.

نقش کاربری public

نقش public در تمامی بانک های اطلاعاتی که شامل یا دربردارنده ی system database هستند، گنجانده شده است، بدین معنا که نمی توان آن را حذف کرده یا کاربرانی را به آن افزوده/اخراج نمود . به این خاطر که کاربران و نقش ها به صورت پیش فرض به نقش public تعلق دارند، مجوزهایی که به نقش کاربری public اعطا می گردد توسط همه ی کاربران و نقش های دیگر نیز به ارث برده می شوند. از این رو توصیه می کنیم تنها مجوزهایی که مایلید تمامی کاربران به ارث ببرند را به نقش public اعطا کنید.

حساب کاربری مالک پایگاه داده (dbo)

Dbo و یا همان مالک پایگاه داده، یک حساب کاربری است که دارای مجوزهای ضمنی برای اجرای تمامی عملیات (فعالیت) لازم در پایگاه داده می باشد. عضوهای نقش ثابت سمت سرور sysadmin به صورت خودکار به dbo نگاشت می شوند.

حساب کاربری dbo به طور مکرر با نقش ثابت پایگاه داده db_owner اشتباه گرفته می شود. حوزه ی (scope) db_owner به یک پایگاه داده محدود می باشد در صورتی که حوزه ی sysadmin تمام سرور را دربر می گیرد. عضویت در نقش db_owner، مجوزها یا اختیارات مالک پایگاه داده را به کاربران اعطا نمی کند.

حساب کاربری guest

هنگامی که کاربری احراز هویت شده و به وی اجازه ی ورود به نمونه ی SQL Server داده می شود، یک حساب کاربری جداگانه باید در هر یک از بانک های اطلاعاتی که کاربر به آن ها دسترسی دارد وجود داشته باشد. درخواست ایجاد یک حساب کاربری درهر یک از پایگاه های داده مانع از این می شود که کاربران به نمونه ی SQL Server متصل شده و در پی آن به تمامی بانک های اطلاعاتی مستقر بر روی یک سرور دسترسی پیدا کند. وجود یک حساب کاربری guest در پایگاه داده با ایجاد امکان ورود (برای دستیابی به پایگاه داده) بدون نیاز به یک حساب کاربری، باعث می شود احتیاج به حضور یک حساب کاربری در هر پایگاه داده کاملا از میان برداشته شود.

حساب کاربری guest یک حساب توکار یا درون ساخته در تمامی نسخه های SQL Server می باشد. در بانک های اطلاعاتی جدید، حساب کاربری نام برده غیرفعال می باشد. چنانچه حساب نام برده از پیش فعال باشد، می توانید آن را با لغو مجوز CONNECT غیر فعال ساخت. برای این منظور بایستی دستور REVOKE CONNECT FROM GUEST را اجرا کنید.

نکته ی امنیتی

از بکار بردن حساب کاربری guest تا حد ممکن پرهیز کنید، زیرا تمامی لاگین های فاقد مجوزهای پایگاه داده ی خود (database permission) مجوزهای دسترسی به پایگاه داده که به این حساب اعطا شده است را کسب می کنند. در صورت لزوم استفاده از حساب کاربری guest، سعی کنید کمترین مجوزها و سطح دسترسی را به آن اعطا کنید.