بسم الله الرحمن الرحیم

آموزشگاه تحلیل داده

تخصصی ترین مرکز برنامه نویسی و دیتابیس در ایران

اعتبارسنجی (authentication) در SQL Server

مدرس : مهندس افشین رفوآ

دوره آموزش SQL Server Administration

اعتبارسنجی (authentication) در SQL Server

SQL Server در کل دو نوع مد اعتبارسنجی ارائه می دهد که عبارتند از: Windows authentication (مد اعتبارسنجی ویندوز) و mixed mode (حالت ترکیبی).

1. مد اعتبارسنجی ویندوز حالت پیش فرض بوده و معمولا از آن با نام امنیت یکپارچه (integrated security) یاد می شود زیرا که این مدل امنیتی SQL Server به گونه ای منسجم با ویندوز پیوند خورده است. کاربرهای ویژه ی ویندوز و حساب های کاربری گروهی قابل اطمینان بوده و موجوز ورود به SQL Server را دارا می باشند. آن دسته از کاربران ویندوزی که از پیش احراز هویت شده اند، ملزوم به ارائه ی مقادیر اعتبارسنجی (credentials) اضافه بر سازمان نیستند.
2. حالت ترکیبی (mixed mode) از هر دو مد اعتبارسنجی ویندوز و SQL Server پشتیبانی می کند. جفت های متشکل از اسم کاربری و گذرواژه درون SQL Server نگهداری می شوند.

نکته ی امنیتی: توصیه می کنیم تا حد امکان از اعتبارسنجی ویندوز بهره بگیرید. این نوع اعتبارسنجی با استفاده از یک سری پیغام های کدگذاری شده کاربران را احراز هویت می کند. اما هنگامی که از SQL Server login به منظور اعتبارسنجی استفاده می شود، گذرواژه ها و اسم های مورد نیاز برای لاگین و ورود به SQL Server از طریق شبکه ارسال می گردد که این امر باعث می شود امنیت آن ها به مراتب کاهش یابد.

در مورد اعتبارسنجی ویندوز، کاربران از پیش وارد به ویندوز شده و دیگر مجبور نیستند مجدد و به صورت جداگانه به SQL Server لاگین کنند. نمونه ی زیر، SqlConnection.ConnectionString، اعتبارسنجی را از طریق windows authentication انجام داده و برای ورود هیچ نیازی به اسم کاربری یا گذرواژه ندارد.

"Server=MSSQL1;Database=AdventureWorks;Integrated Security=true;

نکته: توجه داشته باشید که ثبت ورود یا لاگین کاملا از database user ها مجزا می باشد. بایستی لاگین ها یا گروه های ویندوز (Windows group) را در عملیاتی جداگانه به نقش های کاربری یا کاربران پایگاه داده نگاشت (map) کنید، سپس مجوزهای لازم را به کاربران یا نقش های کاربری، به منظور دسترسی به اشیا پایگاه داد، اعطا کنید.

سناریوهای مختلف احراز هویت

در شرایط ذکر شده در زیر، استفاده از اعتبارسنجی ویندوز بهترین گزینه ی پیشرو می باشد:

1. در صورت وجود یک کنترلگر دامنه (domain controller).
2. در صورتی که برنامه و پایگاه داده هر دو بر روی یک رایانه مستقر (نصب) باشند.
3. در صورتی که نسخه ی مورد استفاده ی شما نمونه ای از SQL Server Express یا LocalDB باشد.

SQL Server login در موارد زیر کاربرد دارد:

1. درصورت کار با یک workgroup (شبکه محلی نظیر به نظیر).
2. در مواردی که کاربران از دامنه های غیر قابل اطمینان مختلفی وصل می شوند.
3. برنامه های تحت وب، همچون ASP.NET.

نکته: با تعریف اعتبارسنجی ویندوز، SQL Server login غیرفعال نمی شود. به منظور غیر فعال کردن لاگین های بسیار ویژه SQL Server بایستی از دستور Transact-SQ " ALTER LOGIN DISABLE " بهره جست.

انواع ثبت ورود (login types)

SQL Server از انواع ثبت ورود متفاوت پشتیبانی می کند:

1. یک حساب کاربری محلی ویندوز (local Windows user account) و یا domain account قابل اطمینان. SQL Server برای اعتبار سنجی و احراز هویت Windows user account به ویندوز تکیه می کند.
2. Windows group. اعطای مجوز به یک windows group مساوی است با اعطای مجوز به تمامی اعضای آن گروه.
3. SQL Server login. SQL Server هم اسم کاربری و هم یک نسخه ی هش شده از گذرواژه را در master database ذخیره می کند. این کار را با استفاده از روش های اعتبار سنجی داخلی برای verify (بازبینی و تایید) کردن تلاش ها برای ثبت ورود انجام می دهد.

نکته: SQL Server لاگین هایی فراهم می نماید که از گواهی نامه ها (certificate) و کلیدهای نامتقارن (asymmetric key) ایجاد شده و تنها برای code signing (به فرایند امضای دیجیتالی فایل های اجرایی و اسکریپت ها به منظور تایید توسعه دهنده ی برنامه گفته می شود که عدم دستکاری شدن کد یا خراب شدن آن از زمان امضای آن با استفاده ازتابع درهم‌ساز رمزنگارانه را تضمین می کند.) مورد استفاده قرار می گیرند.

اعتبار سنجی ترکیبی (mixed mode)

در صورت لزوم استفاده از حالت ترکیبی، ابتدا بایستی لاگین های SQL Server ایجاد کنید. این لاگین ها در SQL Server ذخیره می گردند، سپس باید نام کاربری و گذرواژه ی مورد نیاز SQL Server را در زمان اجرا ارئه نمایید.

نکته ی بسیار مهم امنیتی

SQL Server با یک لاگین به نام sa نصب می شود (سرواژه ی "system administrator یا مدیر سیستم"). لازم است یک گذرواژه ی منحصربفرد به این لاگین تخصیص داده و بعد از آن به هیچ وجه لاگین نام برده را در برنامه ی کاربردی خود استفاده نکنید. این لاگین به نقش ثابت سمت سرور (fixed server role) sysadmin نگاشت می شود. Sa دارای اعتبار نامه و مدارک هویت مدیر (administrative credentials) در کل سرور می باشد که غیر قابل برگشت و قطعی می باشد. چنانچه یک هکر در نقش مدیر به سیستم دسترسی پیدا کند، میزان آسیب هایی که این شخص می تواند وارد کند غیر قابل باور خواهد بود. تمامی اعضای گروه توکار/مدیران

ویندوز، به صورت پیش فرض کاربران عضو نقش sysadmin نیز هستند. اما این امکان وجود دارد که اعضای نام برده را از نقش مورد نظر اخراج کرد.

SQL Server سازکارهایی در خصوص سیاست رمزگذاری و انتخاب گذرواژه برای لاگین های SQL Server، هنگامی که SQL Server بر روی Windows server 2003 و یا نسخه های جدیدتر اجرا می شود ارائه می دهد. سیاست های تعدد گذرواژه ها (Password complexity policies) به منظور جلوگیری یا محافظت در برابر حملات شدید تعبیه شده است. همان طور که از اسم آن پیدا است، این سیاست با افزایش تعداد گذرواژه های ممکن امنیت را بهبود می بخشد. SQL Server قادر است همان سیاست های مربوط به پیچیدگی و انقضا (complexity & expiration) که در Window Server 2003 پیاده سازی می شوند را به گذرواژه های بکار رفته در SQL Server نیز اعمال کند.

نکته ی امنیتی

متصل سازی connection string وارد شده توسط کاربر ممکن است شما را در برابر حمله ی تزریق connection string آسیب پذیر سازد. برای جلوگیری از این رخداد، با استفاده از SqlConnectionStringBuilder، connection string هایی با ساختار نگارشی صحیح، در زمان اجرا ایجاد کنید.