عنوان مقاله: راهنمای پیکربندی Authentication و Authorization در SQL Server به بهترین روش نویسنده مقاله: تیم فنی نیکآموز تاریخ انتشار: ۱۹ فروردین ۱۴۰۳ منبع: https://nikamooz.com/configuration-of-authentication-and-authorization/

پیکربندی Authentication و Authorization دو رکن اساسی برای تأمین امنیت در SQL Server هستند. این دو مکانیزم در کنارهم، به مدیریت دسترسیها و حفاظت از دادهها کمک میکنند. در این مقاله، به توضیح این دو مفهوم و چگونگی بهبود امنیت دیتابیس با استفاده از آنها میپردازیم. علاوهبراین، میتوانید به آموزش رمزگذاری اطلاعات در SQL Server رجوع کنید تا با مطالعه آن، درک عمیقتری از اهمیت محافظت از دادهها بهدست آورید.

#### Authentication چیست؟

احراز هویت (Authentication) فرآیندی است که به منظور بررسی هویت کاربر یا موجودیتی که قصد دسترسی به SQL Server دارد، به کار میبریم. این فرآیند مشابه این است که از کاربر پرسیده شود «شما چه کسی هستید؟» و در پاسخ، لازم است کاربر اطلاعات شخصی، یعنی نام کاربری و رمز عبور را ارائه دهد.

# انواع روش های احراز هویت در SQL Server

Authentication در SQL Server به روشهای زیر قابل انجام است:

- احراز هویت ویندوز (Windows Authentication): این روش، از حسابهای کاربری و گروههای موجود در ویندوز استفاده میکند. بهدلیل سهولت استفاده و امنیت بالا، احراز هویت ویندوز، بهعنوان روش توصیهشده شناخته میشود؛ زیرا در آن از پروتکل امنیتی Kerberos استفاده شده و نیازی به مدیریت جداگانه نامهای کاربری و رمزهای عبور SQL Server وجود ندارد.
- احراز هویت Mixed: احراز هویت ترکیبی در SQL Server ، نوعی پیکربندی است که بهطور همزمان، امکان استفاده از احراز هویت ویندوز و احراز هویت SQL Server را فراهم میکند. در SQL Server این حالت با نام SQL Server and Windows Authentication



**نکته:** برای تنظیم نوع Authentication میتوانید این کار را به دو صورت انجام دهید:

۱. تنظیم نوع Authentication هنگام نصب SQL Server

🐮 SQL Server 2022 Setup		- 0	×
Database Engine Confi Specify Database Engine auther parallelism, Memory limits, and	guration ntication security mode, administrators, data directories, TempDB, Max degree of Filestream settings.		
Global Rules	Server Configuration Data Directories TempDB MaxDOP Memory FILESTREAM		
Microsoft Update Product Updates	Specify the authentication mode and administrators for the Database Engine.		
Install Setup Files Install Rules	Authentication Mode		_
Installation Type Edition	<u>W</u> indows authentication mode <u>M</u> ixed Mode (SQL Server authentication and Windows authentication)		
License Terms Azure Extension for SQL Server	Specify the password for the SQL Server system administrator (sa) account.		_
Feature Selection	Enter password:		
Feature Rules	Confirm password:		
Instance Configuration Server Configuration	Specify SQL Server administrators		
Database Engine Configuration	MASOUDTAHERNMasoudTaheri (MasoudTaheri). SQL Server administrators have u access to the Database Engine.	inrestricted	

# ۲. تنظیم نوع Authentication پس از نصب SQL Server

Server Properties - MASOUDTAHERI\SQLSERVER2016			$\times$
Select a page	Script 👻 🎼 Help		
Processors Security Connections Database Settings Advanced Permissions	Server authentication <u>W</u> indows Authentication mode <u>SQL</u> Server and Windows Authentication mode		 



### Authorization چیست؟

پس از احراز هویت کاربر در SQL Server ، اعطای مجوز (Authorization) تعیین میکند که کاربر در داخل SQL Server مجاز به انجام چه کارهایی است. این بخش به سؤال «چه اجازهای برای انجام چه کاری دارید؟» پاسخ میدهد. این مجوزدهی ازطریق مجوزها (Permissions) و نقشها (Roles) مدیریت میشود و محدوده دسترسی و اقداماتی را تعریف میکند که یک کاربر میتواند انجام دهد. بهعنوان مثال، امکان خواندن، نوشتن یا تغییر داده، از مواردی هستند که از این طریق انجام میشوند.

### شباهت Authentication و Authorization

مهمترین نقاط شباهت Authentication و Authorization در SQL Server از منظرهای مختلف، به شرح زیر است:

- نقشهای امنیتی: احراز هویت و اعطای مجوز ، هردو برای ایمنسازی سیستمها و منابع، حیاتی محسوب میشوند. این دو مکانیزم اطمینان میدهند که تنها کاربران یا سرویسهای تأییدشده و مجاز میتوانند به اطلاعات یا بخشهای حساس سیستم دسترسی پیدا کنند.
- وابستگی متقابل: احراز هویت و اعطای مجوز اغلب بهعنوان بخشی از یک سیستم کنترل دسترسی با یکدیگر
   کار میکنند. به طور معمول، فرآیندهای اعطای مجوز برای تعیین محدوده دسترسی یک کاربر یا سرویس، به
   احراز هویت موفق وابسته است.
- قابلیت پیکربندی: هردوی این موارد را میتوان براساس الزامات امنیتی خاص یک سیستم، سفارشیسازی و پیکربندی کرد. برای مثال، میتوان سیستمی را راهاندازی کرد که برای امنیت بیشتر به احراز هویت چند عاملی (MFA) نیاز داشته باشد یا سطوح مختلف دسترسی را براساس نقشهای کاربر اعطا کند.
- کاربرد در سیستمهای متنوع: مفاهیم Authentication و Authorization در انواع مختلف سیستمها، ازجمله وباپلیکیشنها، انواع پایگاه های داده و سیستمهای شبکه، قابل اجرا هستند. در عمل، پیکربندی Authorization و مهای دارد، اساسی و مهم Authentication و میآید.

در حالی که احراز هویت و اعطای مجوز در SQL Server از نظر هدف استفاده، فرآیند و نوع اطلاعاتی که استفاده میکنند، متمایز هستند، اما شباهتهای فوق را نیز در نقشهایشان دارند. بنابراین، درک هردو مفهوم بهمنظور طراحی، پیادهسازی و مدیریت سیستمهای امن، ضروری است.

#### تفاوت Authentication و Authorization

در ادامه، به بررسی تفاوت Authentication و Authorization از نقطه نظرهای گوناگون میپردازیم.

### تفاوت Authentication و Authorization: هدف

بهواسطه احراز هویت در SQL Server ، هویت کاربر یا موجودیتی تعیین میشود که قصد دسترسی به سیستم را دارد. این عمل مانند بررسی کارت شناسایی شخص در ورودی یک مکان است؛ در صورتی که اعطای مجوز، تعیین میکند کاربر احراز هویتشده چه اقداماتی را میتواند در داخل سیستم انجام دهد.



### تفاوت Authentication و Authorization: فرآیند

با پیکربندی احراز هویت ، Credential ها، یعنی نام کاربری و رمز عبور، برای تأیید هویت بررسی میشوند. ازسوی دیگر، با استفاده از فرآیند اعطای مجوز ، Permission های مرتبط با کاربر احراز هویتشده، با قوانین سیستم مقایسه میشوند تا دسترسی به سیستم، اعطا یا محدود شود.

### تفاوت Authentication و Authorization: اطلاعات مورد استفاده

در احراز هویت از Credential ها و احتمالاً فاکتورهای دیگری مانند رمزهای عبور یکبار مصرف یا سؤالات امنیتی استفاده میشود. ازسوی دیگر، در Authorization ، پیکربندیها، نقشها و سیاستهایی استفاده میشوند که اقدامات مجاز برای کاربران یا نقشهای مختلف در داخل سیستم را تعریف میکنند.

#### روش های پیکربندی Authentication در SQL Server

همانطور که پیشتر به آن اشاره شد، SQL Server از دو حالت اصلی احراز هویت بههمراه یک گزینه ترکیبی که از مزایای هردو رویکرد بهره میبرد، پشتیبانی میکند. درک و انتخاب روش مناسب احراز هویت ، اولین گام در ایمن سازی محیط SQL Server شما است.

# مراحل پیکربندی احراز هویت : روش Windows Authentication

پیکربندی احراز هویت در روش Windows Authentication ، شامل مجموعهای از مراحل است که اطمینان میدهد اینستنسِ SQL Server از حسابهای کاربری و گروههای ویندوز بهمنظور احراز هویت استفاده میکند. این حالت، بهدلیل مزایای امنیتی خاصی مانند یکپارچهسازی با مکانیزمهای امنیتی ویندوز، ترجیح داده میشود.

در ادامه، مراحل کلیدی برای پیکربندی حالت احراز هویت ویندوز بررسی میشوند:



Instance یا همان نمونه SQL Server زرمافزار SSMS را باز کنید و به Instance یا همان نمونه SQL Server خود Connect شوید. اگر هنوز آن را روی سیستم خود Instal نکردهاید، میتوانید از <u>آموزش نصب گام به گام SSMS</u> بهعنوان راهنما استفاده کنید.

🧏 Microsoft SQL Server Management Studio Quick Launch (Ctrl+Q) 🔎 🗕	<b>—</b> ×
	- A
File Edit View Tools Window Help	
※ 〒 写	
Object Explorer 👻 🦞 🗙	
Connect- 🕴 🎁 🔲 🝸 🖒 🚸	
E CESKTOP-A2URC70\MYSQLSERVER2022	
🗄 💼 Databases 🛛 🖓 Connect to Server 🛛 🗙	
🗄 💼 Security	
Management	
🗄 💼 Integration Services Catalogs Server type: Database Engine 🗸	
SQL Server Agent XPs disable Server name: DESKTOP-A2URC70VMYSQLSERVER2022	
La Zevent Profiler     Authentication: Windows Authentication	
Liker name: UPENKUP-AZUR-AZUR-AZUR-AZUR-AZUR-AZUR-AZUR-AZUR	
rasswuu.	
Connect Cancel Help Options >>	
C Ready	đ

۲. **دسترسی به تنظیمات سرور:** در بخش Object Explorer، روی نام سرور راست کلیک کرده و گزینه Properties را انتخاب کنید.





۳. **تنظیمات امنیتی:** گزینه Security را کلیک کرده و از بخش Server Authentication، گزینه Windows

Nicrosoft SQL Server Management Studio		Quick La	aunch (Ctrl+Q)	ρ_	×
File Edit View Tools Window Help	-A2URC70\MYSQLSERVER2022 -				
○ - ○         13 - □ - □         24         28 New Q         Select a page           ○ - ○         13 - □         -         10 - □         26 General	🕼 Script 🔻 😮 Help				
Object Explorer       Image: Connect + Image: Conne	Server authentication				
Connection	Enable server proxy account				
Server: DESKTOP-A2URC70\MYSQLSEI Connection:	Proxy account: Password:				
UESKTOP-AZURC/O/LENovo	Enable Common Criteria compliance				
YT view connection properties	Enable C2 audit tracing				
	Cross database ownership chaining				
Progress					
C Ready					
<	ОК	Cancel			
☐ Ready					

 ٤. فخیرهسازی تغییرات: برای نهاییسازی اقدامات، روی دکمه OK کلیک کنید. اگر مجبور به تغییر حالت احراز هویت شدهاید، برای اعمالشدن تغییرات، نیاز به راهاندازی مجدد سرویس SQL Server دارید.





#### مراحل پیکربندی احراز هویت : روش Mixed Authentication

برای پیکربندی احراز هویت در SQL Server ، ازطریق روش مبتنیبر SQL Server Authentication ، باید حالت ترکیبی (Mixed Mode) را فعال کنید. این حالت، به هردو روش احراز هویت ویندوز و احراز هویت SQL Server اجازه ورود میدهد. در ادامه، یک راهنمای گامبهگام برای پیکربندی این روش احراز هویت شرح داده خواهد شد.

۱. ورود به Instance : SQL Server Management Studio : SSMS را اجرا کنید و به Instance خود متصل شوید.

Image: Second SQL Server Management Studio         File       Edit       View       Tools       Window       Help         Image: Second Sec	♀   X 口 凸   ? - マ □   N N 町 二 目 目 日	< 82   < #   3 3 4   45 52   10 ;	•   ត្រ 🖋	Quick Launch (Ctrl+Q)	_ م	×
Botabases      Botabases	G <sup>®</sup> Connect to Server Server type: Server name: Authentication: User name: Password:	SQL Server         Database Engine         BESKTOP-A2URC 70 MYSOLSERVER2022         Windows Authentication         DESKTOP-A2URC 70 \Lenovo         Remember password         Connect       Cancel       Help       Optice	X			

۲. اتصال به سرور: برای برقراری اتصال اولیه به سرور، از مشخصات احراز هویت ویندوز خود استفاده کنید.





۳. **ورود به تنظیمات سرور (Server Properties):** روی نام سرور در پنجره Object Explorer راستکلیک کرده و Properties را از منوی زمینه انتخاب کنید.

Microsoft SQL Se	rver Management Studio	Quick Launch (Ctrl+Q)	ρ_	∎ ×
File Edit View	Tools Window Help			
0-0 13-1	コ - 🄄 🗎 📲 📕 New Query 🗿 🔊 🕼 🏫 🏛 🕼 🕹 🗇 奇 🛛 ಶ - ペ - 🛛 🛛 🕣 🏓	• 🗔 🌶 🖮 🖂 • 🖕		
1 1 N	-   > Execute ■ ✓ the 目   he the 副 副 品   恒 恒 任 平   物 =			
Object Explorer	<del>▼</del> # ×			
Connect 👻 🍟 📕				
E B DESKTOP-A 211	Connect			
Databa	Disconnect			
🛞 🛑 Server (	Register			
🕀 📕 Replica 🕀 📁 Always	New Query			
🗉 💼 Manag	Activity Monitor			
SQL Set	Start			
🕢 🔄 XEvent	Stop			
	Pause			
	Resume			
	Restart			
	Policies			
	Facets			
	Start PowerShell			
	Azure Data Studio 🔸			
	Reports +			
	Refresh			
	Properties			
-				
<	>			
Ready				al

٤. انتخاب گزینه Security: در پنجره تنظیمات سرور، روی تب Security از لیست سمت چپ کلیک کنید.

😣 Microsoft SQL Server Management Studio				Qu	ck Launcł	n (Ctrl+Q	۶ ۶	- 1	×
File Edit View Tools Window Help	Server Properties - DESKTOP	-A2URC70\MYSQLSERVER2022		-		×			
O - O 1 1 - 1 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 3 - 3 - 3	ect a page General	🖵 Script 🔻 😯 Help							
Object Explorer       ▼ ↓ ×         Connect • ↓ ×↓ ■ ↓ ↓       ▲         D ESKTOP-A2URC70\MYSQLSERVER2022         ■ Databases         ■ Security         ■ Security         ■ Security         ■ Security         ■ Security         ■ Security         ■ Always On High Availability         ■ Management         ■ Management         ■ Management         ■ SQL Server Agent (Agent XPs disable         ■ XEvent Profiler	Memory Processors Security Connections Database Settings Advanced Permissions	Server authentication Windows Authentication mode SQL Server and Windows Auth Login auditing None Failed logins only Successful logins only Successful logins only Both failed and successful login Server proxy account	entication mode						
	nnection sere: ESKTOP-A2URC70\MYSQLSEI protection: ESKTOP-A2URC70\Lenovo  Vew connection properties gress Ready	Enable server proxy account Proxy account: Password:      Options     Enable Common Citeria comple     Enable C2 audit tracing     Cross database ownenship chail	ance						
< >>			[	ОК	Can	cel			
☐ Ready									al



۵. تغییر حالت احراز هویت سرور: حال در تب Security، بخشی با عنوان Server authentication را مشاهده خواهید کرد. گزینه SQL Server and Windows Authentication mode را انتخاب کنید. این کار، حالت ترکیبی (Mixed Mode) را برایتان فعال میکند. برای ذخیرهسازی تغییرات، روی دکمه OK کلیک کنید.

🛃 Microsoft SQL Server Management Studio			Quick Lau	nch (Ctrl+C	0 8	° –	□ ×	¢
File Edit View Tools Window Help	Server Properties - DESKTOP	-A2URC70\MYSQLSERVER2022	- 0	×				
○ - ○         ☆ - ☆ - ☆ Ш Ш         ●         New Query         ●           ♀ ♡♀         →         >         Execute         ■	Select a page	🖵 Script 🔻 😯 Help						
Object Explorer     Image: Connect - Image: Conn	Memory     Processors     Security     Connections     Advanced     Permissions	Server authentication 1 Windows Authentication mode 1 SQL Server and Windows Authentication mode 1 Login auditing None Failed logins only Successful logins only Both failed and successful logins Server proxy account						
	Connection Server DESKTOP-A2URC70\MYSQLSEI Connection: DESKTOP-A2URC70\Lenovo Y# <u>Wew connection properties</u> Yew connection properties Ready	Enable server proxy account  Proxy account: Password:  Optiona  Enable Common Citeria compliance Enable C2 audit tracing Cross database ownership chaining						
<			K C	ancel				

۲. راهاندازی مجدد سرویس SQL Server: برای اعمال تغییرات، باید سرویس SQL Server را مجدداً راهاندازی کنید. این کار را میتوانید ازطریق SQL Server Configuration Manager یا با استفاده از SQL services در ویندوز انجام دهید. در SQL Server Configuration Manager ، نمونه SQL Server SQL خود را پیدا کنید، روی آن راستکلیک کرده و Restart را انتخاب کنید. شما میتوانید در Services ویندوز، سرویسی را پیدا کنید که نامی شبیه به نمونه SQL Server مما دارد؛ سپس روی آن راستکلیک کرده و Restart را انتخاب کنید.



Services						_		$\times$
File Action View	Help							
0 🗐 🛐 🔶 🗢	à 🗟   🛛 📷   🕨 🔳 II ID							
🔍 Services (Local)	Services (Local)	-						
	SQL Server (MYSQLSERVER2022)	Name	Description	Status	Startup Type	Log On As		^
	Stop the service Pause the service Restart the service Description: Provides storage, processing and controlled access of data, and rapid transaction processing.	Solver Construction     Solver Construction     Solver (MYSQLSERVER2     Sol	Receives tra Receives tra Enables the This service Verifies pote Provides sto Provides sto Executes jo Executes jo Provides SQ CEIP service Provides SQ CEIP service Discovers n Provides re Launches a Provides en Optimizes t	Running Running Running Running Running Running Running Running	Manual Automatic ( Manual (Trig Automatic ( Automatic ( Manual Disabled Automatic ( Automatic ( Automatic Manual Manual Manual Automatic ( Manual Automatic (	Local Service Network S Local Service Local Syste NT Service NT Service NT Service Local Service NT Service Local Syste Local Syste Local Syste Local Syste Local Syste Local Syste		
		Synaptics FP WBF Policy Ser     Sync Host_2387ac94     SynTPEnh Caller Service     SysMain	Synaptics F This service Maintains a	Running Running Running Running	Automatic Automatic ( Automatic Automatic	Local Syste Local Syste Local Syste Local Syste		
		System Event Notification S	Monitors sy	Running	Automatic	Local Syste		$\sim$
	\Extended \Standard /							

#### مبنای احراز هویت از طریق Windows Authentication

در SQL Server از چندین روش مختلف احراز هویت از طریق Windows Authentication پشتیبانی میشود. این امکان ازطریق استفاده از شناسهها و گروههای مختلف ویندوز فراهم میشود. چهار روش اصلی آن عبارتند از:

- Local Windows Account: حساب کاربری محلی ویندوز برای کاربرانی استفاده میشود که فقط برروی کامپیوتر محلی نیاز به دسترسی دارند. این اکانتها مستقیماً روی سیستم هاست SQL Server ایجاد میشوند و میتوانند برای احراز هویت و دسترسی به SQL Server به کار روند.
- Local Windows Group: گروههای محلی ویندوز برای مدیریت دسترسیهای گروهی کاربران در سطح محلی استفاده میشوند. میتوان یک گروه محلی ایجاد کرد و کاربران مختلفی را به آن اضافه کرد، سپس گروه مذکور، دسترسی به SQL Server اعطا کرد. این امر، مدیریت دسترسیها را آسانتر میکند.
- Domain Account: حسابهای دامنه برای کاربرانی استفاده میشوند که در محیط شبکه Windows Active
   Directory قرار دارند. این حسابها توسط مدیر دامنه ایجاد و مدیریت میشوند و امکان دسترسی به منابع مختلف در سراسر دامنه، ازجمله SQL Server را فراهم میکنند.
- Domain Group: گروههای دامنه در Active Directory ایجاد میشوند و به مدیران این امکان را میدهند تا دسترسیها را برای یک گروه خاصی از کاربران در سراسر دامنه مدیریت کنند. این گروهها میتوانند شامل کاربرانی از سراسر Domain باشند و به آنها دسترسی جمعی به SQL Server داده میشود.



#### پیکربندی Authorization در SQL Server

پیکربندی Authorization در SQL Server برای حفظ امنیت و یکپارچگی پایگاه داده بسیار مهم است. SQL Server بهمنظور کنترل دسترسی، از ترکیبی از مجوزهای سطح سرور و سطح پایگاه داده استفاده میکند.

برای کنترل دقیق دسترسی به منابع در SQL Server ، از سه مفهوم اصلی زیر استفاده میشود:

- ۱. Principal ها: موجودیتهایی هستند که امکان درخواست دسترسی به منابع SQL Server را دارند و میتوانند شامل لاگینهای SQL Server، حسابهای کاربری ویندوز یا گروههای کاربری باشند. بهعبارت دیگر، هرکسی یا چیزی که میخواهد به منابع SQL Server دسترسی داشته باشد، یک Principal درنظر گرفته میشود.
- ۲. منابع قابل دسترسی (Securables): منابعی هستند که موتور SQL Server کنترل دسترسی به آنها را مدیریت میکند. منابع قابل دسترسی میتوانند در سطح سرور (مانند دیتابیسها، لاگینها و Endpoint ها) یا در سطح پایگاه داده (مانند جدول و View و پروسیجر) باشند. به بیان ساده، هر منبعی که در SQL Server وجود دارد و نیاز به کنترل دسترسی دارد، یک «منبع قابل دسترسی» محسوب میشود.
- ۳. مجوزها (Permissions): اقداماتی هستند که Principal ها میتوانند روی منابع قابل دسترسی انجام دهند.
   <u>SELECT</u> مجوزها برای سطوح مختلف دسترسی تعریف میشوند. برای <u>اشیا پایگاه داده</u>، مجوزهایی مانند <u>UPDATE</u> (بهروزرسانی) و DELETE (حذف) وجود دارد. در سطح سرور، مجوزهایی مانند (انتخاب)، <u>INSERT</u> (درج)، <u>UPDATE</u> (بهروزرسانی) و CREATE LOGIN (حذف) وجود دارد. در سطح سرور، مجوزهایی مانند Principal مانند OREATE کردی، مجوزهایی مانند روی منابع قابل دسترسی انجام دهند.

شایان ذکر است که لاگینها، User ها، Role ها و Permission ها، مکانیزمهای Authorization محسوب میشوند.

### استفاده از Login و Data User برای پیاده سازی Authorization

ما در SQL Server با استفاده از Login ها میتوانیم برای ورود به SQL Server استفاده کنیم. هر Login با توجه به دسترسی های ارائهشده میتواند Map شود به تعدادی Data User در بانک های اطلاعاتی مختلف.

توجه داشته باشید که کنترل دسترسی به اشیاء سمت سرور (مانند ایجاد لاگین، ایجاد روالهای Audit و...) با استفاده از Login ها و همچنین کنترل دسترسی به اشیاء سمت بانک اطلاعاتی (مانند دسترسی به یک جدول، دسترسی به ویو و...) با استفاده از Data User انجام میشود.





# مراحل پیادہ سازی Authorization

پیکربندی Authorization در SQL Server ، تنظیم مجوزها و کنترلهای دسترسی را شامل میشود. بدین طریق، اطمینان حاصل میشود که کاربران فقط میتوانند اقداماتی را انجام دهند که برای نقش آنها ضروری است. در ادامه، یک راهنمای گامبهگام برای پیکربندی اعطای مجوز در SQL Server آورده شده است:

- ۲. تعیین حالت احراز هویت: از میان دو روش Windows Authentication Mode و Mixed Mode ، یک حالت احراز هویت را انتخاب کنید. درصورت انتخاب حالت ترکیبی، حتماً یک رمز عبور قوی برای حساب کاربری SA تنظیم کنید.
- ۲. ایجاد Login: مشخص کنید که آیا Login موردنظر، یک حساب کاربری ویندوز است یا یک حساب کاربری SQL Server. برای حسابهای کاربری یا گروههای ویندوز، مطمئن شوید که آنها در Active Directory یا روی دستگاه محلی ایجاد شدهاند.

مشابه زیر، از SQL Server Management Studio یا دستورات T-SQL برای ایجاد Login استفاده کنید:

• برای Login ویندوز:

CREATE LOGIN [DOMAIN\User] FROM WINDOWS GO

• برای لاگین SQL Server:

CREATE LOGIN LoginName WITH PASSWORD = 'strong\_password'
GO

۳. ایجاد کاربران پایگاه داده و نگاشت آنها به Login ها: پایگاه دادهای را که کاربر به آن نیاز دارد، انتخاب یا ایجاد کنید. سپس یک کاربر در پایگاه داده ایجاد کرده و آن را ازطریق دستور زیر، به یک Server لاگین نگاشت کنید.



USE YourDatabase GO CREATE USER UserName FOR LOGIN LoginName GO

٤. تخصیص Role ها و Permission ها: برای اعطای مجوز در سطح گسترده، User ها را به شیوه زیر، به Role های یایگاه داده اضافه کنید.

```
EXEC sp_addrolemember 'db_datareader', 'UserName'
GO
```

برای اعطای مجوزهای خاص و کنترل جزئیتر، میتوان Permission ها را بهطور مستقیم به یک کاربر یا نقش اعطا کرد. این عمل، ازطریق دستور امکانیذیر است:

GRANT SELECT, INSERT ON YourTable TO UserName GO

۵. پیکربندی مجوزهای سطح سرور (اختیاری): برای وظایفی که نیاز به دسترسی سطح سرور دارند، مانند ایجاد پایگاه داده یا مدیریت Login ها، ممکن است لازم باشد نقشها یا مجوزهای سطح سرور را اختصاص دهید. این کار را ازطریق دستور زیر انجام دهید:

ALTER SERVER ROLE sysadmin ADD MEMBER [DOMAIN\User]; GO

#### ۲. آزمایش و اعتبارسنجی مجوزها

با استفاده از SSMS ، sqlcmd یا یک ابزار کلاینت دیگر، بهعنوان کاربر جدید وارد شوید تا پیکربندی Authorization را آزمایش کنید. در این گام میتوانید برای انجام اقدامات مطابق با مجوزهای اعطاشده کارکرد کانفیگ مذکور را تست کنید. مشابه زیر، برای آزمایش مجوزها از داخل SQL Server، از دستور EXECUTE AS استفاده کنید:

```
EXECUTE AS USER = 'UserName';
-- Test permissions here
REVERT;
```

#### جمع بندی: راهنمای پیکربندی Authentication و Authorization

در این مقاله، مراحل مربوط به پیکربندی Authentication و Authorization را بهصورت گامبهگام و با جزئیات شرح دادیم و تفاوت و دلایل اهمیت آنها در SQL Server را بررسی کردیم. برای آشنایی هرچه بیشتر با کوئرینویسی و <u>آموزش T-SQL</u> و مقاله اسکریپت های SQL را نیز مطالعه کنید. اگر هنوز شناخت کافی از SQL Server و محیط آن ندارید، بهتر است به <u>آموزش جامع SQL Server</u> نیز رجوع کنید.