MSSQL Authentication Modes

MSSQL Authentication Modes

- Protecting data starts with the ability to authenticate users and authorize their access to specific data.
- To this end, SQL Server includes an authentication mechanism for verifying the identities of users trying to connect to a SQL Server instance.
- as well as an authorization mechanism that determines which data resources that authorized users can access and what actions they can take.
- Authentication and authorization are achieved in SQL Server through a combination of security principals, securable, and permissions.
- SQL Server supports two authentication modes:
- *Windows Authentication.*
- *SQL Server and Windows Authentication.*

Windows Authentication

- Sometimes referred to as *integrated security.*
- Windows authentication is integrated with Windows user and group accounts, making it possible to use a local or domain Windows account to log into SQL Server
- When a Windows user connects to a SQL Server instance, the database engine validates the login credentials against the Windows principal token.
- This eliminates the need for separate SQL Server credentials.
- Microsoft recommends that you use Windows Authentication whenever possible.

SQL Server and Windows Authentication

- Sometimes referred to as mixed mode.
- In some cases, however, you might require SQL Server Authentication.
- For example, users might connect from non-trusted domains, or the server on which SQL Server is hosted is not part of a domain.
- in which case, you can use the login mechanisms built into SQL Server, without linking to Windows accounts.
- Under this scenario, the user supplies a username and password to connect to the SQL Server instance, bypassing Windows Authentication altogether.
- You can specify the authentication mode when setting up a SQL Server instance or change it after implementation through the server’s properties.