

ANKARA ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ



BLM4522 VİZE ÖDEVİ

Ecem Şimşek - 21290553

Latife Süeda Tuğrul -20290297

Github: https://github.com/suedatgrl/SQL_work/

1.Proje- Veritabanı Güvenliği ve Erişim Kontrolü

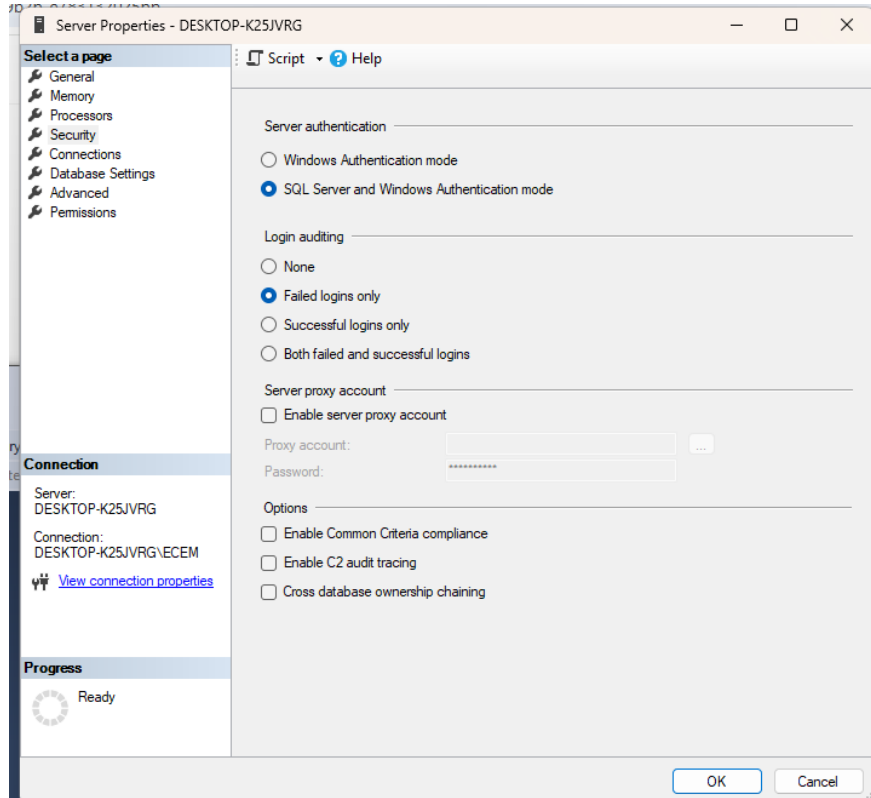
2.Proje- Veritabanı Performans Optimizasyonu ve İzleme

3.Proje- Veritabanı Yedekleme ve Otomasyon Çalışması

1.Proje- Veritabanı Güvenliği ve Erişim Kontrolü

Erişim Yönetimi

1. Sol üstteki **Object Explorer** penceresinde sunucu adına **sağ tıklanır** → **Properties** seçilir.
2. Açılan pencerede soldaki menüden **Security** sekmesini seçilir.
3. **Server authentication** kısmında “**SQL Server and Windows Authentication mode**” seçeneğini işaretlenir.



4. Bu değişikliklerin geçerli olması için sunucuyu yenilenir.
5. SSMS'te Object Explorer'dan: **Security > Logins > sağ tıkla > New Login...** seçilir.
6. Açılan pencerede:
 - **Login name** kısmı doldurulur.
 - **SQL Server authentication** seçili olsun.
 - Güçlü bir şifre girilir.

Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server: DESKTOP-K25JVRG

Connection: DESKTOP-K25JVRG\ECEM

[View connection properties](#)

Progress

Ready

Login name: ecem_user Search...

☐ Windows authentication
☐ Microsoft Entra ID authentication
☒ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy
☒ Enforce password expiration
☒ User must change password at next login

☐ Mapped to certificate
☐ Mapped to asymmetric key
☐ Map to Credential

Mapped Credentials

Credential	Pr...

Add Remove

Default database: master

Default language: <default>

OK Cancel

7. Sol taraftaki **User Mapping** sekmesine gelinir.

- Kullanıcının erişmesini istediğin veritabanını seçilir.
- Altındaki kutulardan db_datareader, db_datawriter rolleri işaretlenir (okuma/yazma yetkisi için).

Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server: DESKTOP-K25JVRG

Connection: DESKTOP-K25JVRG\ECEM

[View connection properties](#)

Progress

Ready

Users mapped to this login:

Map	Database	User	Default Schema
<input checked="" type="checkbox"/>	deneme	ecem_user	...
<input checked="" type="checkbox"/>	master	ecem_user	...
<input type="checkbox"/>	model		
<input type="checkbox"/>	msdb		
<input type="checkbox"/>	tempdb		
<input checked="" type="checkbox"/>	Test1	ecem_user	...
<input type="checkbox"/>	TestDB		

☒ Guest account enabled for: master

Database role membership for: master

<input type="checkbox"/>	db_accessadmin
<input type="checkbox"/>	db_backupoperator
<input checked="" type="checkbox"/>	db_datareader
<input checked="" type="checkbox"/>	db_datawriter
<input type="checkbox"/>	db_dtladmin
<input type="checkbox"/>	db_denydatareader
<input type="checkbox"/>	db_denydatawriter
<input type="checkbox"/>	db_owner
<input type="checkbox"/>	db_securityadmin
<input checked="" type="checkbox"/>	public

OK Cancel

8. Kullanıcı oluşturulmuş olacak.

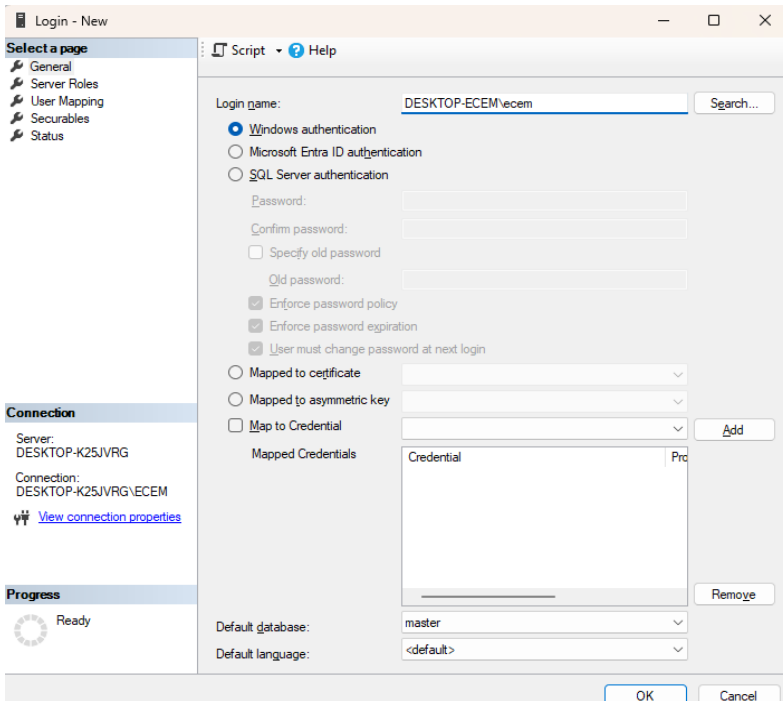
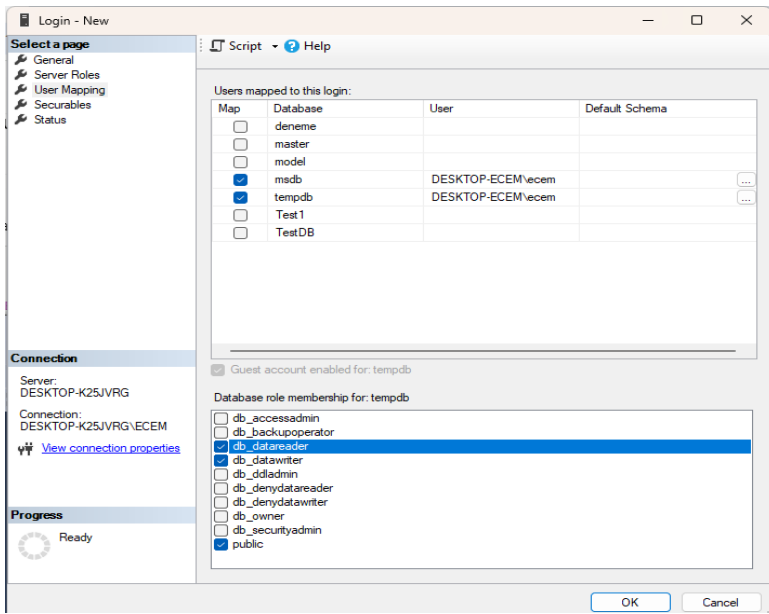
SQL Server Authentication ve Windows Authentication

1. Yine: Security > Logins > **sağ tıkla** > **New Login...**

2. Açılan pencerede:

- **Login name:** Windows kullanıcı adı yazılır.
- Authentication kısmında bir değişiklik yapılmasına gerek yok; çünkü bu bir Windows kullanıcısı olacak.

3. **User Mapping** sekmesinden aynı şekilde veritabanını seçilir ve roller tanımlanır.



Giriş yapılan kullanıcıyı test etmek için şu kod çalıştırılır:

```
SQLQuery1.sql - lo...K25JVRG\ECCEM (54))* X
EXECUTE AS LOGIN = 'ecem_user';
SELECT SYSTEM_USER;
REVERT;
```

121 %

Results Messages

(No column name)
1 ecem_user

Veri Şifreleme

1. TDE'yi etkinleştirmeden önce, **veritabanı şifreleme anahtarı** (Database Encryption Key) için bir **Master Key** oluşturulmalıdır. Master Key, şifreleme anahtarlarını korur.

-Yeni Sorgu penceresini açılır.

-Aşağıdaki komutla Master Key'i oluşturulur:

```
SQLQuery2.sql - lo...K25JVRG\ECCEM (53))* X SQLQuery1.sql - lo...K25JVRG\ECCEM (54))*
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'GüçlüBirParola123';
```

121 %

Messages

Commands completed successfully.

Completion time: 2025-04-24T21:25:50.3402237+03:00

Bu komut, veritabanı şifreleme için gerekli olan Master Key'i oluşturur.

Şimdi **Database Encryption Key (DEK)** oluşturulmalıdır. DEK, veritabanı içindeki verileri şifrelemek için kullanılır.

```
SQLQuery5.sql - lo...K25JVRG\ECCEM (62)))*  SQLQuery3.sql - lo...K25JVRG\ECCEM (55)))*  SQLQuery2.sql - lo...K25JVRG\ECCEM (54)))*
USE TestDB;
GO

CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCPTION BY SERVER CERTIFICATE MyServerCert;
GO
```

Artık TDE'yi etkinleştirebiliriz. Bu, veritabanındaki tüm verileri şifreler ve diske şifrelenmiş olarak yazılır.

- Aşağıdaki komutla **TDE**'yi etkinleştir:

```
SQLQuery7.sql - lo...K25JVRG\ECCEM (52)))*  SQLQuery
ALTER DATABASE TestDB
SET ENCRYPTION ON;
GO
```

TDE'nin başarıyla etkinleşip etkinleşmediğini kontrol etmek için şu komutu çalıştırabiliriz.

```
SQLQuery8.sql - lo...K25JVRG\ECCEM (61)))*  SQLQuery7.sql - lo...K25JVRG\ECCEM (52)))*
SELECT db.name, db.is_encrypted
FROM sys.databases db
WHERE db.name = 'TestDB';
```

	name	is_encrypted
1	TestDB	1

Veritabanının yedeğini alırken, şifrelenmiş veriler de korunur. Aşağıdaki komutla veritabanının yedeğini alabiliriz.

```
SQLQuery8.sql - lo...K25JVRG\ECCEM (61)))*  SQLQuery7.sql - lo...K25JVRG\ECCEM (52)))*  SQL
BACKUP DATABASE [TestDB] TO DISK = 'C:\Backup\TestDB.bak';
```

Artık veritabanındaki hassas bilgiler **TDE ile şifrelenmiş durumda** ve **güvenli bir şekilde korunuyor**.

Bu adımlarla veritabanındaki veriler disk üzerinde şifreli halde saklanacak. Veritabanı şifrelemesi ve yedekleme işlemleri sayesinde verilerin güvenliği artmış olacak.

SQL Injection Testleri

Parametrelili sorgu (özellikle stored procedure) kullanarak SQL Injection'a karşı nasıl korunacağı ele alınacak.

1. İlk olarak, test ortamını kurmak için basit bir veritabanı ve kullanıcılar tablosu oluşturulur. Bu tablonun içine test verisi eklenir.

2. Veritabanı oluşturulduktan sonra, kullanıcılar hakkında bilgi tutacağımız bir tablo oluşturulur. Bu tabloda kullanıcı adı ve şifre bilgilerini tutacağız.

3. Bu tabloya bazı test kullanıcıları eklenir.

```
SQLQuery9.sql - lo...K25JVRG\ECCEM (78)))*  SQLQuery8.sql - lo...K25JVRG\ECCEM (61)))*  SQLQuery7.sql - lo...K25JVRG\ECCEM
CREATE TABLE Users (
    UserID INT PRIMARY KEY IDENTITY,
    Username NVARCHAR(50),
    Password NVARCHAR(50)
);
GO
INSERT INTO Users (Username, Password) VALUES ('admin', 'admin123');
INSERT INTO Users (Username, Password) VALUES ('user1', 'password1');
INSERT INTO Users (Username, Password) VALUES ('guest', 'guest123');
GO

121 %
Messages

(1 row affected)

(1 row affected)

(1 row affected)

Completion time: 2025-04-24T22:10:34.9873919+03:00
```

4. Şimdi, SQL Injection'a açık olan bir sorgu yazalım. Bu sorgu, kullanıcı adı ve şifreyi kontrol etmek için gelen girdileri doğrudan SQL sorgusuna ekler. Bu, SQL Injection'a neden olabilir.

```
SQLQuery10.sql - I...K25JVRG\ECCEM (60)))*  SQLQuery9.sql - lo...K25JVRG\ECCEM (78)))*  SQLQuery8.sql - lo...K25JVRG\ECCEM (61)))*
-- SQL Injection'a açık sorgu
DECLARE @Username NVARCHAR(50);
DECLARE @Password NVARCHAR(50);

SET @Username = 'ecemsmk';
SET @Password = 'ecem2002';

EXEC('SELECT * FROM Users WHERE Username = ''' + @Username + ''' AND Password = ''' + @Password + ''')
GO
```

121 %

Results Messages

UserID	Username	Password
--------	----------	----------

Yukarıdaki kod, **user_input** yerine kullanıcıdan alınan verileri doğrudan sorguya ekler. Eğer bu sorguya kötü niyetli bir giriş yapılırsa, SQL Injection saldırısı gerçekleştirilebilir.

Eğer kullanıcı adı yerine ' OR 1=1 -- girerse, sorgu şu hale gelir:

```
SQLQuery11.sql - I...K25JVRG\ECCEM (56)))*  SQLQuery10.sql - I...K25JVRG\ECCEM (60)))*  SQLQuery9.sql - lo...K25JVRG\ECCEM (78)))*
SELECT * FROM Users WHERE Username = '' OR 1=1 --' AND Password = 'password';
```

121 %

Results Messages

	UserID	Username	Password
1	1	admin	admin123
2	2	user1	password1
3	3	guest	guest123

Bu sorgu, şifre kontrolünü geçersiz kılar ve tüm kullanıcıları geri döndürebilir.

Aşağıda, parametrelili sorgu ile oluşturulmuş bir **Stored Procedure** örneği bulunmaktadır:

```
SQLQuery16.sql - I...K25JVRG\ECCEM (59)))*  SQLQuery15.sql - I...K25JVRG\ECCEM (70)))*  SQLQuery14.sql - I...K25JVRG\ECCEM (61)))*
USE master;
GO
CREATE SERVER AUDIT SPECIFICATION MyAuditSpec
FOR SERVER AUDIT MyAudit
ADD (SUCCESSFUL_LOGIN_GROUP), -- Başarılı girişler
ADD (FAILED_LOGIN_GROUP), -- Başarısız girişler
ADD (LOGOUT_GROUP), -- Çıkışlar
ADD (SQL_STATEMENT_COMPLETED_GROUP); -- SQL komutlarının tamamlanması
GO
```


Bu stored procedure, **Username** ve **Password** parametrelerini alır ve bunları doğrudan SQL sorgusunda kullanır. Ancak bu yöntem, SQL Injection'a karşı güvenlidir, çünkü kullanıcı verileri SQL sorgusuna parametre olarak bağlanır ve veritabanı tarafından güvenli bir şekilde işlenir.

Stored Procedure'u çalıştırmak için aşağıdaki gibi bir sorgu yazabiliriz:

```
EXEC CheckUserCredentials @Username = 'admin', @Password = 'admin123';
GO
```

UserID	Username	Password
1	admin	admin123

Bu komut, **CheckUserCredentials** prosedürünü çalıştırarak, belirtilen kullanıcı adı ve şifreyi sorgular. Ancak bu prosedür, SQL Injection'a karşı korumalıdır çünkü kullanıcı verileri parametre olarak işlenir.

Audit Logları

SQL Server Audit özelliğini kullanabilmek için öncelikle veritabanı denetimini başlatmamız gerekir. SQL Server'da Audit, genellikle bir **Audit** nesnesi ve bunun altına bağlı **Audit Specification** nesnelerinden oluşur.

1. Audit nesnesi, veritabanı üzerinde yapılacak aktivitelerin loglanmasını sağlamak için kullanılır.

```
USE master;
GO

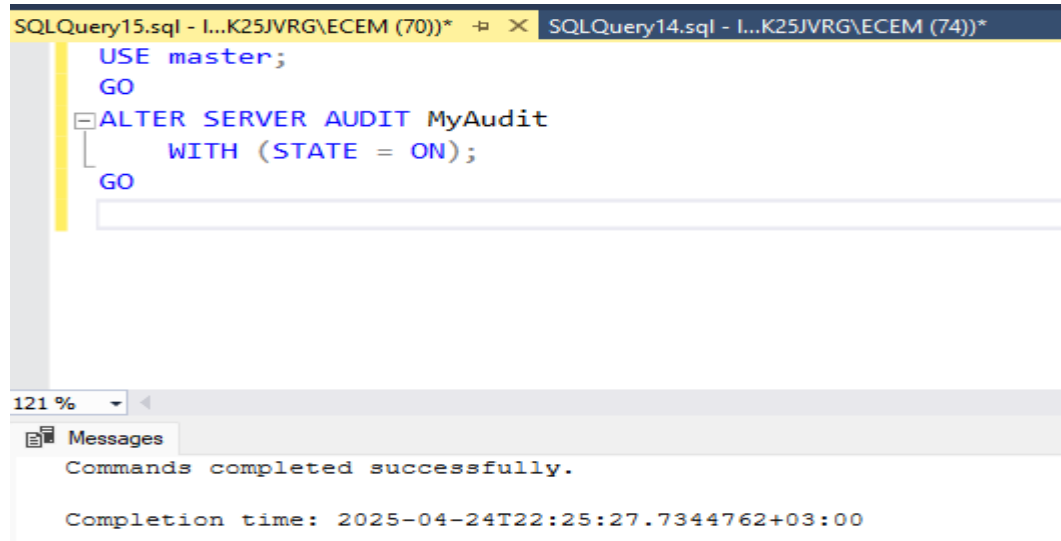
CREATE SERVER AUDIT MyAudit
TO FILE (FILEPATH = 'C:\SQLAuditLogs\'); -- Logların kaydedileceği dosya yolu
GO
```

Commands completed successfully.

Completion time: 2025-04-24T22:24:17.1264869+03:00

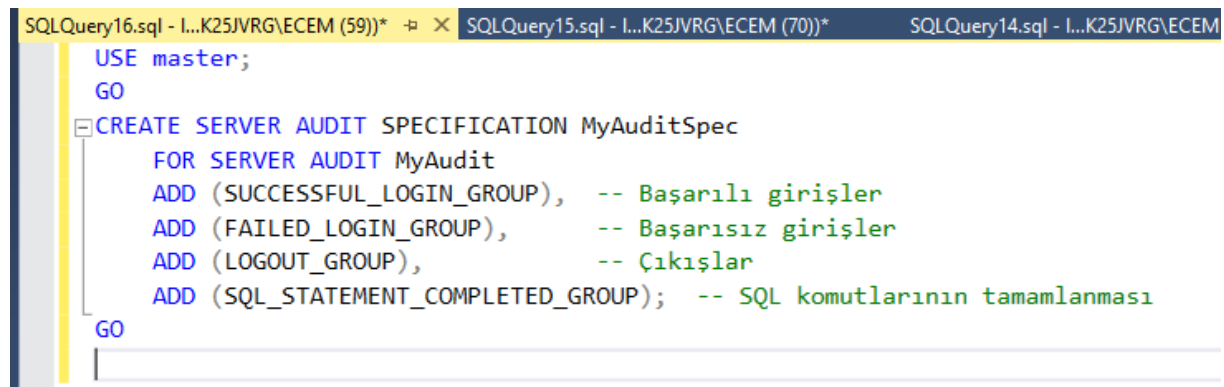
Bu komut, MyAudit adında bir audit nesnesi oluşturur ve logları belirtilen dosya yoluna kaydeder.

2. Audit nesnesini oluşturduktan sonra, onu başlatmamız gerekir.



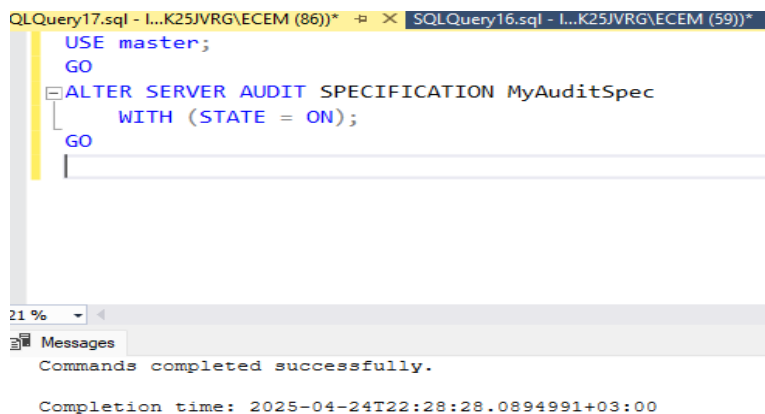
```
SQLQuery15.sql - I...K25JVRG\ECEM (70))*  SQLQuery14.sql - I...K25JVRG\ECEM (74))*  
USE master;  
GO  
ALTER SERVER AUDIT MyAudit  
WITH (STATE = ON);  
GO  
121 %  
Messages  
Commands completed successfully.  
Completion time: 2025-04-24T22:25:27.7344762+03:00
```

3. Audit'i başlatıp, belirli işlemleri izlemek için bir server-level audit specification oluşturabiliriz. Örneğin, bir kullanıcının giriş yaptığı, çıkış yaptığı, veritabanına bağlandığı ve sorgularını çalıştırdığı aktiviteleri izleyelim.



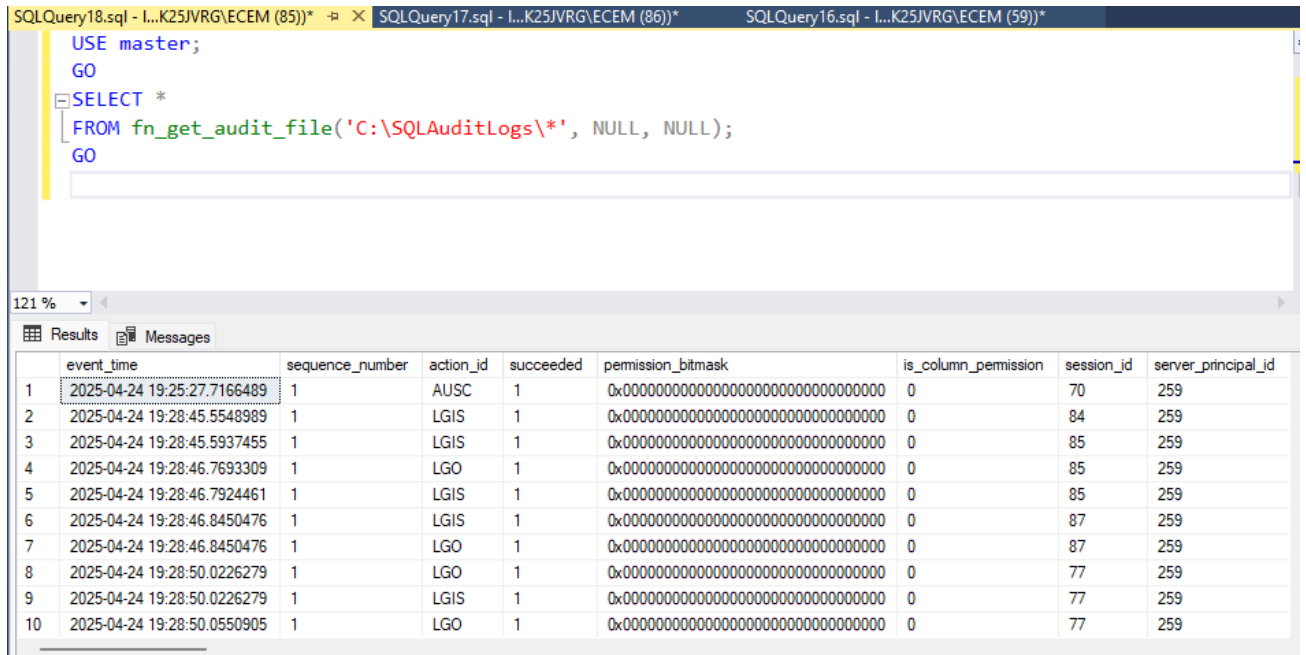
```
SQLQuery16.sql - I...K25JVRG\ECEM (59))*  SQLQuery15.sql - I...K25JVRG\ECEM (70))*  SQLQuery14.sql - I...K25JVRG\ECEM  
USE master;  
GO  
CREATE SERVER AUDIT SPECIFICATION MyAuditSpec  
FOR SERVER AUDIT MyAudit  
ADD (SUCCESSFUL_LOGIN_GROUP), -- Başarılı girişler  
ADD (FAILED_LOGIN_GROUP), -- Başarısız girişler  
ADD (LOGOUT_GROUP), -- Çıkışlar  
ADD (SQL_STATEMENT_COMPLETED_GROUP); -- SQL komutlarının tamamlanması  
GO
```

4. Oluşturduğumuz **audit specification**'i başlatmamız gerekir.



```
QLQuery17.sql - I...K25JVRG\ECEM (86))*  SQLQuery16.sql - I...K25JVRG\ECEM (59))*  
USE master;  
GO  
ALTER SERVER AUDIT SPECIFICATION MyAuditSpec  
WITH (STATE = ON);  
GO  
21 %  
Messages  
Commands completed successfully.  
Completion time: 2025-04-24T22:28:28.0894991+03:00
```

5. Audit logları SQL Server tarafından `fn_get_audit_file` fonksiyonu ile sorgulanabilir. Bu fonksiyon, belirttiğiniz dosya yolundaki logları okuyabilir.



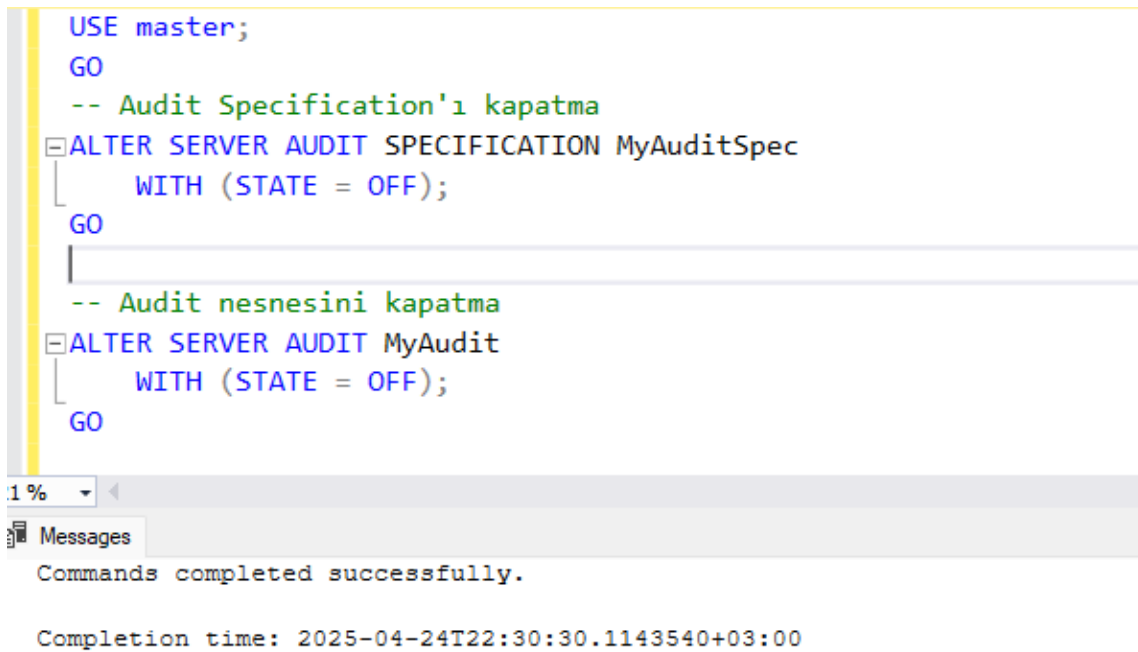
The screenshot shows a SQL Server Enterprise Manager interface. At the top, there are three tabs for SQL queries. The active query window contains the following T-SQL code:

```
USE master;
GO
SELECT *
FROM fn_get_audit_file('C:\SQLAuditLogs\*', NULL, NULL);
GO
```

Below the query window, the 'Results' tab is selected, displaying a table with 10 rows of audit log data. The columns are: event_time, sequence_number, action_id, succeeded, permission_bitmask, is_column_permission, session_id, and server_principal_id.

	event_time	sequence_number	action_id	succeeded	permission_bitmask	is_column_permission	session_id	server_principal_id
1	2025-04-24 19:25:27.7166489	1	AUSC	1	0x00000000000000000000000000000000	0	70	259
2	2025-04-24 19:28:45.5548989	1	LGIS	1	0x00000000000000000000000000000000	0	84	259
3	2025-04-24 19:28:45.5937455	1	LGIS	1	0x00000000000000000000000000000000	0	85	259
4	2025-04-24 19:28:46.7693309	1	LGO	1	0x00000000000000000000000000000000	0	85	259
5	2025-04-24 19:28:46.7924461	1	LGIS	1	0x00000000000000000000000000000000	0	85	259
6	2025-04-24 19:28:46.8450476	1	LGIS	1	0x00000000000000000000000000000000	0	87	259
7	2025-04-24 19:28:46.8450476	1	LGO	1	0x00000000000000000000000000000000	0	87	259
8	2025-04-24 19:28:50.0226279	1	LGO	1	0x00000000000000000000000000000000	0	77	259
9	2025-04-24 19:28:50.0226279	1	LGIS	1	0x00000000000000000000000000000000	0	77	259
10	2025-04-24 19:28:50.0550905	1	LGO	1	0x00000000000000000000000000000000	0	77	259

6. Eğer audit'i kapatmak istenirse, aşağıdaki komutlar kullanılabilir.



The screenshot shows a SQL Server Enterprise Manager interface with a query window containing the following T-SQL code:

```
USE master;
GO
-- Audit Specification'ı kapatma
ALTER SERVER AUDIT SPECIFICATION MyAuditSpec
WITH (STATE = OFF);
GO
-- Audit nesnesini kapatma
ALTER SERVER AUDIT MyAudit
WITH (STATE = OFF);
GO
```

Below the query window, the 'Messages' tab is selected, displaying the following messages:

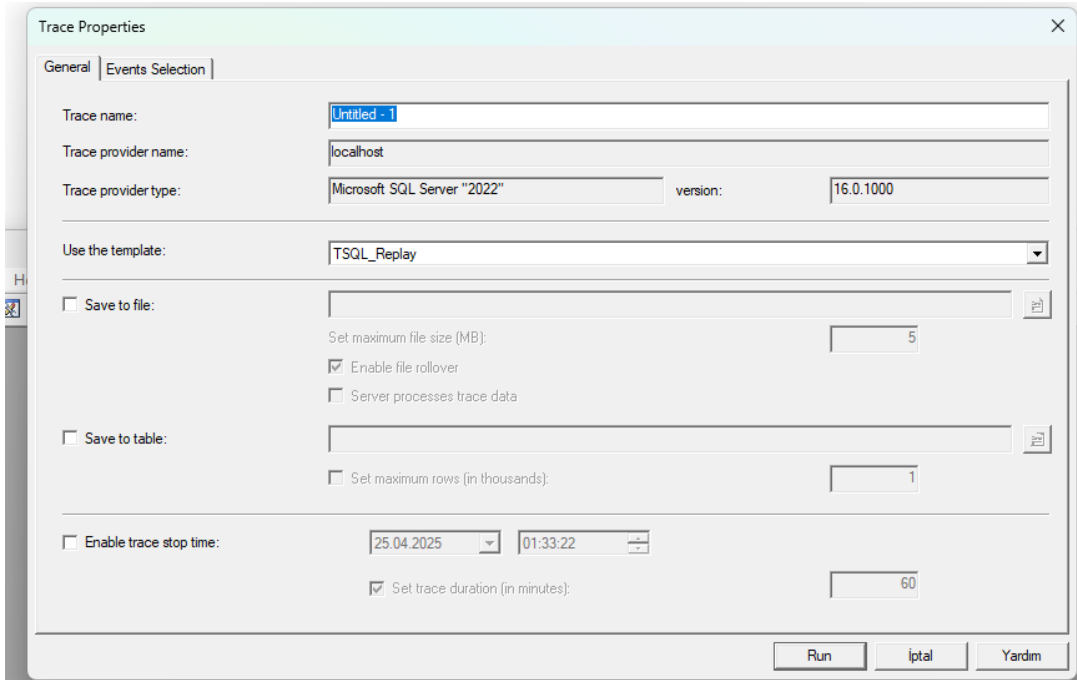
```
Commands completed successfully.

Completion time: 2025-04-24T22:30:30.1143540+03:00
```

2.Proje- Veritabanı Performans Optimizasyonu ve İzleme

Veritabanı İzleme

1. SQL Server Profiler açılır.
2. “File” → “New Trace...” seçilir.
3. SQL Server’a bağlanılır .
4. Bir **Trace Template** seçilir. (örnek: “TSQL_Replay”).
5. “Events Selection” sekmesine gelerek aşağıdaki gibi olaylar eklenir:
 - SQL:BatchCompleted
 - RPC:Completed
 - Showplan XML



- Trace başlatılır.
- Ağır çalışan veya sürekli tekrarlanan sorguları kaydedilir.
- CPU time, Reads, Writes sütunlarına göre analiz edilebilir.
- Trace'i bitirip .trc dosyası olarak kaydedilebilir..

SQL Server Profiler

File Edit View Replay Tools Window Help

Untitled - 1 (localhost)

EventClass	EventSequence	TextData	ApplicationName	LoginName	DatabaseName	DatabaseID	ClientProcessID
SQL:BatchStarting	477	SELECT target_data FROM sy...	SQLServerCEIP	NT SER...	master	1	1280
SQL:BatchCompleted	478	SELECT target_data FROM sy...	SQLServerCEIP	NT SER...	master	1	1280
RPC:Starting	479	exec sp_reset_connection	SQLServerCEIP	NT SER...	master	1	1280
Audit Logout	480		SQLServerCEIP	NT SER...	master	1	1280
RPC:Completed	481	exec sp_reset_connection	SQLServerCEIP	NT SER...	master	1	1280
Audit Login	482	-- network protocol: LPC set quoted...	SQLServerCEIP	NT SER...	master	1	1280
SQL:BatchStarting	483	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	NT SER...	master	1	1280
SQL:BatchCompleted	484	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	NT SER...	master	1	1280
SQL:BatchStarting	485	if not exists (select * from sys.dm...	SQLServerCEIP	NT SER...	master	1	1280
SQL:BatchCompleted	486	if not exists (select * from sys.dm...	SQLServerCEIP	NT SER...	master	1	1280

if not exists (select * from sys.dm_xe_sessions where name = 'telemetry_xe_events')
alter event session telemetry_xe_events on server state=start

Trace is running. Ln 36, Col 1 Rows: 36

DMV'ler, veritabanının iç durumu hakkında canlı bilgiler sağlar.

Bu sorgu, en çok zaman alan sorguları verir.

```

SELECT TOP 10
    qs.total_elapsed_time / qs.execution_count AS [AvgExecTime],
    qs.execution_count,
    qs.total_logical_reads,
    qs.total_logical_writes,
    st.text AS [SQLText]
FROM
    sys.dm_exec_query_stats qs
CROSS APPLY
    sys.dm_exec_sql_text(qs.sql_handle) st
ORDER BY
    [AvgExecTime] DESC;

```

Results Messages

	AvgExecTime	execution_count	total_logical_reads	total_logical_writes	SQLText
1	455695	1	198957	0	(@_msparam_0 nvarchar(4000),@_msparam_1 nvarchar...
2	2811	1	1068	0	(@_msparam_0 nvarchar(4000),@_msparam_1 nvarchar...
3	2006	1	93	0	(@_msparam_0 nvarchar(4000),@_msparam_1 nvarchar...
4	1547	1	37	0	(@_msparam_0 nvarchar(4000),@_msparam_1 nvarchar...
5	1407	1	44	0	SELECT dtb.name AS [Name], CAST(0 AS bit) AS [IsFab...
6	1198	5	265	2	(@_msparam_0 nvarchar(4000),@_msparam_1 nvarchar...
7	1119	1	59	0	(@_msparam_0 nvarchar(4000),@_msparam_1 nvarchar...
8	1070	1	8	0	(@_msparam_0 nvarchar(4000))SELECT dtb.collation_n...

İndeks Yönetimi

1. İlk adımda, veritabanında hangi indekslerin bulunduğunu incelememiz gerekir. Aşağıdaki SQL sorgusu, mevcut tüm indeksleri listeleyecektir.

```

SELECT
    t.name AS Table_Name,
    i.name AS Index_Name,
    i.type_desc AS Index_Type,
    i.is_primary_key AS Is_Primary_Key,
    i.is_unique AS Is_Unique,
    i.fill_factor AS Fill_Factor,
    i.is_disabled AS Is_Disabled,
    i.is_hypothetical AS Is_Hypothetical,
    i.create_date AS Create_Date,
    i.modify_date AS Modify_Date
FROM
    sys.indexes AS i
INNER JOIN
    sys.tables AS t ON i.object_id = t.object_id
WHERE
    t.is_ms_shipped = 0 AND i.type_desc <> 'HEAP' -- 'HEAP' tipi indeks değildir
ORDER BY
    t.name, i.name;

```

2. Bu sorgu, hangi tabloya hangi index'in eklenmesinin faydalı olacağını gösterir. Eksik indeksleri tespit eder.

```
SELECT
    migs.avg_total_user_cost * migs.avg_user_impact * (migs.user_seeks + migs.user_scans) AS [Impact],
    mid.statement AS [TableName],
    mid.equality_columns,
    mid.inequality_columns,
    mid.included_columns
FROM
    sys.dm_db_missing_index_group_stats migs
JOIN
    sys.dm_db_missing_index_groups mig ON migs.group_handle = mig.index_group_handle
JOIN
    sys.dm_db_missing_index_details mid ON mig.index_handle = mid.index_handle
ORDER BY
    [Impact] DESC;
```

21 %

Results Messages

Impact | TableName | equality_columns | inequality_columns | included_columns

3. Gereksiz indeksler, yazma işlemlerini yavaşlatabilir ve disk alanını gereksiz yere doldurabilir. Kullanılmayan veya fazla indeksleri tespit etmek için şu sorguyu kullanabilirsiniz.

```
SELECT
    OBJECT_NAME(ix.object_id) AS TableName,
    ix.name AS IndexName,
    ix.type_desc AS IndexType,
    ix.is_primary_key AS IsPrimaryKey,
    ix.is_unique AS IsUnique,
    ix.user_seeks, -- Kaç kez okuma işlemi yapılmış
    ix.user_scans, -- Kaç kez okuma işlemi tarama ile yapılmış
    ix.user_lookups, -- Kaç kez arama yapılmış
    ix.user_updates -- Kaç kez indeks güncellenmiş
FROM
    sys.indexes ix
WHERE
    OBJECTPROPERTY(ix.object_id, 'IsUserTable') = 1
    AND ix.type_desc IN ('CLUSTERED', 'NONCLUSTERED')
ORDER BY
    ix.user_seeks DESC; -- Kullanılma sıklığına göre sıralama
```

4. Veritabanında en çok kullanılan sorgulara göre yeni indeksler oluşturmak performansı artırabilir. Örneğin, sıkça kullanılan bir sorgu, belirli bir sütuna göre sıralama yapıyorsa, o sütun üzerinde bir indeks oluşturmak faydalı olabilir.

İndeks oluşturma için aşağıdaki komutu kullanılabilir:

```
SQLQuery25.sql - I...K25JVRG\ECM (58))* SQLQuery24.sql - I...K25JVRG\ECM (67))*
CREATE NONCLUSTERED INDEX IX_TableName_ColumnName
ON TableName (ColumnName);
```

Sorgu İyileştirme

1. Uzun süren sorguları analiz etmek için, sorgu planlarını incelemek gerekir. Sorgu planı, SQL Server'ın bir sorguyu nasıl çalıştırdığına dair bilgi sağlar. Aşağıdaki sorguyu çalıştırarak bir sorgunun çalışma planı alınabilir.

```
SQLQuery26.sql - I...25JVRG\ECCEM (104))* X SQLQuery25.sql - I...K25JVRG\ECCEM (5
SET SHOWPLAN_XML ON;
-- Uzun süren sorguyu burada çalıştırılır
SELECT * FROM large_table;
SET SHOWPLAN_XML OFF;
```

2. Yavaş sorguların bir diğer nedeni, çok sayıda tablonun birleştirilmesidir. Bu durumda, doğru JOIN türünü seçmek önemlidir. INNER JOIN, LEFT JOIN, RIGHT JOIN gibi JOIN türleri, sorguların hızını etkileyebilir.

- INNER JOIN: Sadece her iki tabloda da eşleşen kayıtları getirir.
- LEFT JOIN: Sol tablodaki tüm kayıtları getirir, sağ tablodan eşleşmeyenler NULL olur.

Eğer LEFT JOIN gereksiz yere kullanılıyorsa, sorgu süresi artabilir.

3. İyileştirmeleri uyguladıktan sonra, sorgu performansını test etmek önemlidir. Test etmek için aşağıdaki yöntemleri kullanılabilir.

1. **Execution Plan:** SQL Server Management Studio (SSMS) üzerinden, sorguyu çalıştırırken "Include Actual Execution Plan" seçeneğini etkinleştirerek sorgu planını incelenebilir.
2. **Sorgu Süresi:** Sorgu süresi ile yapılan değişikliklerin etkisini görmek için, SET STATISTICS TIME ON komutunu kullanılabilir. Bu, sorgu süresini gösterir.

```
SQLQuery27.sql - I...K25JVRG\ECCEM (96))* X SQLQuery26.
SET STATISTICS TIME ON;
-- Sorguyu çalıştırılır
SELECT * FROM large_table;
SET STATISTICS TIME OFF;
```

Veri Yöneticisi Roller

1. Rolü oluşturduktan sonra, bu role belirli yetkiler atamamız gerekir. Yetkiler, veritabanında hangi işlemleri yapabileceklerini belirler. Aşağıda, bir role veri okuma ve yazma yetkileri verme örneği yer almaktadır.

```
USE [TestDB];
GO
GRANT SELECT, INSERT, UPDATE, DELETE ON [Users] TO [VeriAnalisti];
GO
```

121 %

Messages

Commands completed successfully.

Completion time: 2025-04-25T01:17:03.6587580+03:00

2. Bir rol oluşturduktan ve gerekli yetkileri verdikten sonra, bu rolü bir kullanıcıya atamamız gerekir. Bunun için aşağıdaki komutları kullanılabilir.

```
USE [TestDB];
GO
EXEC sp_addrolemember 'VeriAnalisti', 'ecem'; -- Kullanıcıyı role atama
GO
```

3. Bir kullanıcıyı bir rolden çıkarmak için aşağıdaki komutu kullanılabilir.

```
USE [TestDB];
GO
EXEC sp_droprolemember 'VeriAnalisti', 'ecem'; -- Kullanıcıyı rolden çıkarma
GO
```

4. Bir kullanıcının hangi rollerde olduğunu görmek için aşağıdaki sorguyu çalıştırılabilir.

```
USE [TestDB];
GO
SELECT dp.name AS UserName,
       dp.type_desc AS UserType,
       o.name AS RoleName
FROM sys.database_principals dp
JOIN sys.database_role_members drm ON dp.principal_id = drm.member_principal_id
JOIN sys.database_principals o ON drm.role_principal_id = o.principal_id
WHERE dp.type NOT IN ('A', 'G', 'R', 'X')
AND dp.name = 'ecem';
GO
```


3.Proje- Veritabanı Yedekleme ve Otomasyon Çalışması:

1. Ortam Hazırlığı:

SQL Server Developer Edition ve SSMS yüklendi.

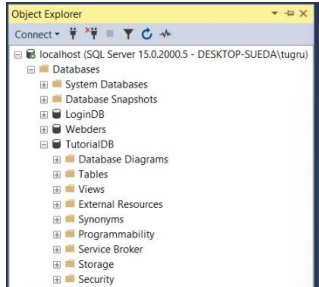
SSMS ile localhost (veya .\SQLEXPRESS) üzerinden "Database Engine"e Windows/sa ile bağlanıldı.

2. Örnek Veritabanı Restore edildi. Burada Db ismimiz TutorialDB olan veritabanımızla çalışmamıza devam edeceğiz.

```
mkdir C:\SQLBackups  
copy "%USERPROFILE%\Downloads\TutorialDB.bak" "C:\SQLBackups\TutorialDB.bak"
```

TutorialDB.bak dosyası C:\SQLBackups yerel klasörüne kopyalandı.

SSMS'te Databases → Restore Database... ile TutorialDB adıyla başarıyla yüklendi.



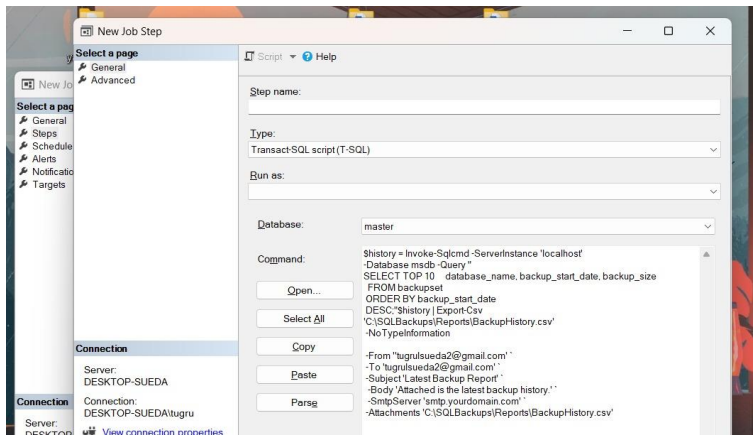
3. Backup Job Oluşturma

SQL Server Agent altında New Job... ile TutorialDB_FullBackup işi tanımlandı.

Steps sekmesinde, TutorialDB için günün tarihini isimde kullanan T-SQL yedekleme script'i eklendi. Database olarak master değil kendi TutorialDB isimli veri tabanımızı ekliyoruz.

T-SQL kodu:

```
DECLARE @bak NVARCHAR(260) =  
N'C:\SQLBackups\TutorialDB_Full_' +  
CONVERT(CHAR(8), GETDATE(), 112) + '.bak';  
  
BACKUP DATABASE [TutorialDB]  
TO DISK = @bak  
WITH INIT, NAME = 'Full backup of TutorialDB ' + CONVERT(VARCHAR, GETDATE(), 120);
```



4. Zamanlama (Schedule)

Job'un Schedules → New... bölümünde, her gece 00:00'da çalışacak şekilde günlük tetikleyici ayarlandı. Böylece yedekleme günlük olarak sağlanacak.

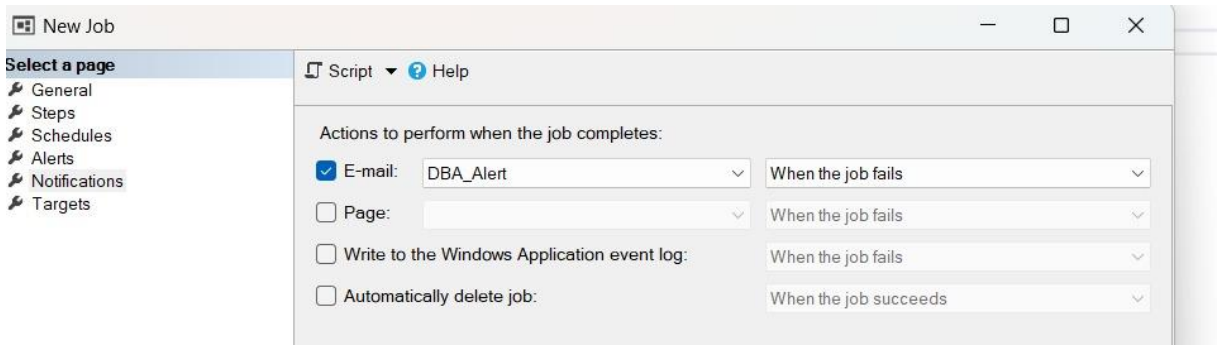
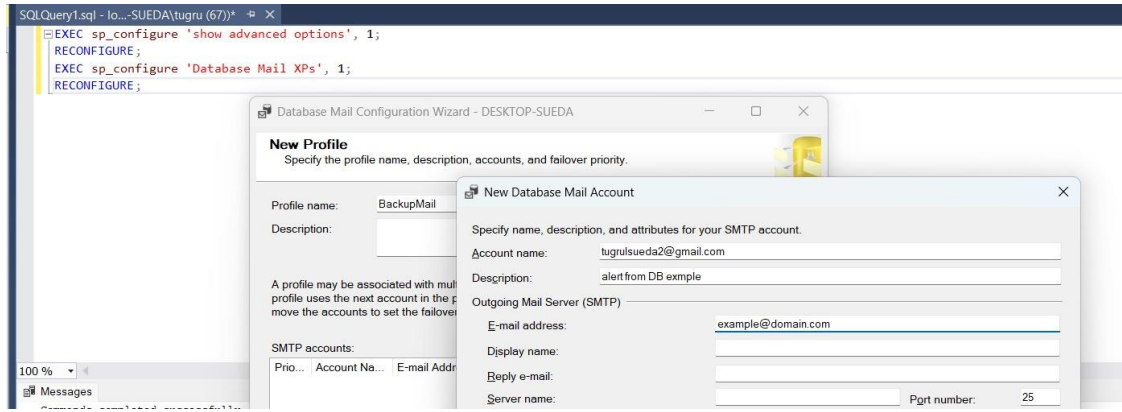
5. E-posta Uyarıları

Management → Database Mail ile BackupMail profili oluşturuldu.

SQL Server Agent Properties'ten bu profil etkinleştirildi.

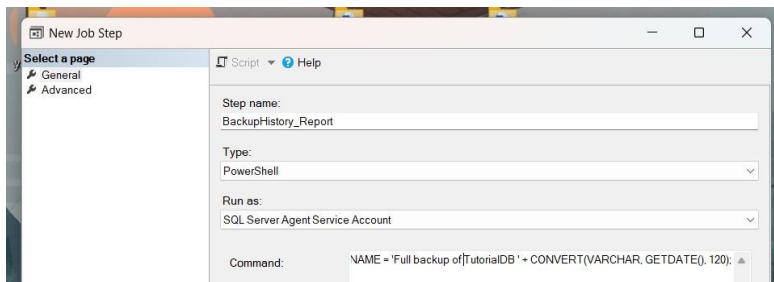
Operators altında DBA_Alert tanımlanıp, Job'un Notifications → If job fails → E-mail kısmına atandı.





6. Raporlama

Yeni bir PowerShell tabanlı job (BackupHistory_Report) eklenip, msdb.backupset'ten son yedek bilgileri CSV'ye yazdırıldı, Oluşan rapor ilgili adrese e-posta ile gönderildi.



```
$history = Invoke-Sqlcmd -ServerInstance 'localhost' -Database msdb -Query "
SELECT TOP 10
    database_name, backup_start_date, backup_size
FROM backupset
ORDER BY backup_start_date DESC;"
$history | Export-Csv 'C:\SQLBackups\Reports\BackupHistory.csv' -NoTypeInformation
```

```
Send-MailMessage -From 'sqladmin@yourdomain.com' `
  -To 'tugrulsueda1@gmail.com' `
  -Subject 'Latest Backup Report' `
  -Body 'Attached is the latest backup history.' `
  -SmtpServer 'smtp.yourdomain.com' `
  -Attachments 'C:\SQLBackups\Reports\BackupHistory.csv'
```