



ERİŞİM KONTROLÜ ve YETKİLENDİRME

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü



Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabılır ancak değiştirilemez ve ticari amaçla kullanılamaz. Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

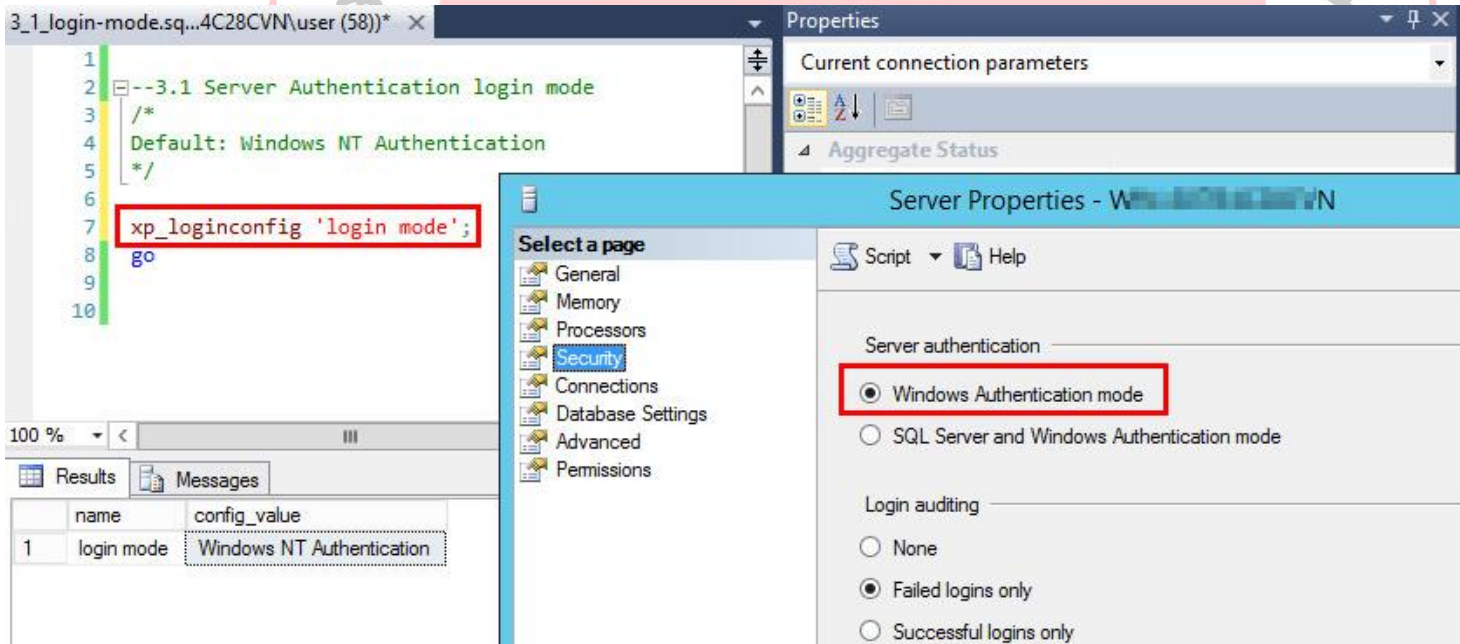
'Server Authentication' Özelliği

- Sunucu Erişim kontrolü için 'Windows kimlik doğrulama modu' özelliği seçilmeli
- Windows, SQL Server'dan daha kuvvetli bir kimlik doğrulama mekanizması sunmaktadır.
- Varsayılan olarak Windows Kimlik Doğrulama Modu seçilidir.
- Aşağıdaki sorguyu çalıştırarak denetimi sağlayabilirsiniz.

```
xp_loginconfig 'login mode';
```

'Server Authentication' Özelliği

- Eğer varsayılan değeri değiştirilmişse;
 - SQL Server Management Studio aracı açılır.
 - Object Explorer sekmesi açılır ve ilgili veritabanı instance'a bağlanılır.
 - Instance name üzerinde sağ tıklayıp özelliklere gelinir.
 - Güvenlik sayfasında sunucu kimlik doğrulama ayarlarından 'Windows Authentication' modu seçilir.



The screenshot displays the SQL Server Management Studio interface. In the top-left pane, a query window shows the following SQL code:

```
1
2 --3.1 Server Authentication login mode
3 /*
4 Default: Windows NT Authentication
5 */
6
7 xp_loginconfig 'login mode';
8 go
9
10
```

The query 'xp_loginconfig 'login mode';' is highlighted with a red box. Below the query window, the 'Results' pane shows a table with the following data:

	name	config_value
1	login mode	Windows NT Authentication

In the top-right pane, the 'Properties' window is open, showing 'Current connection parameters'. In the bottom-right pane, the 'Server Properties - W...' window is open, with the 'Security' page selected. Under 'Server authentication', the 'Windows Authentication mode' radio button is selected and highlighted with a red box. The 'Login auditing' section shows 'Failed logins only' selected.

- Hem Windows hem de SQL Server hesapları (SQL login'leri) kullanılır.
- SQL login şifreleri network üzerinden iletildiği için (encrypted gönderilmesine rağmen) daha güvensizdir.
- Mümkün olan her yerde Windows authentication tercih edilmelidir. Böylece **single sign on** sağlanmış ve login yönetimi basitleşmiş olur.

Eğer Mixed Mod gerekli ise;

- SQL Server hesaplarının password özellikleri ve kilitleme özellikleri (lock, expire ...) lokal veya domain grup politikaları ile düzenlenmeli
- Mixed Mode Authentication seçilirse sa kullanıcısı için bir password verilmeli
- Bu şifrenin de yeteri kadar güçlü bir şifre olması gerekmektedir (Her iki modda da).
- Password policy force seçilmişse zayıf şifreleri kabul etmeyecektir.

- master, msdb ve tempdb hariç tüm SQL Server veritabanlarına misafir kullanıcı (guest user) hesapları üzerinden erişim izinlerini iptal edilmelidir.
- Aşağıdaki sorgu intance'daki her veri tabanı için çalıştırılmalı, sonuç dönmemelidir.

```
USE [database_name];
GO
SELECT DB_NAME() AS DBName, dpr.name,
dpe.permission_name
FROM sys.database_permissions dpe
JOIN sys.database_principals dpr
ON dpe.grantee_principal_id=dpr.principal_id
WHERE dpr.name='guest'
AND dpe.permission_name='CONNECT';
```

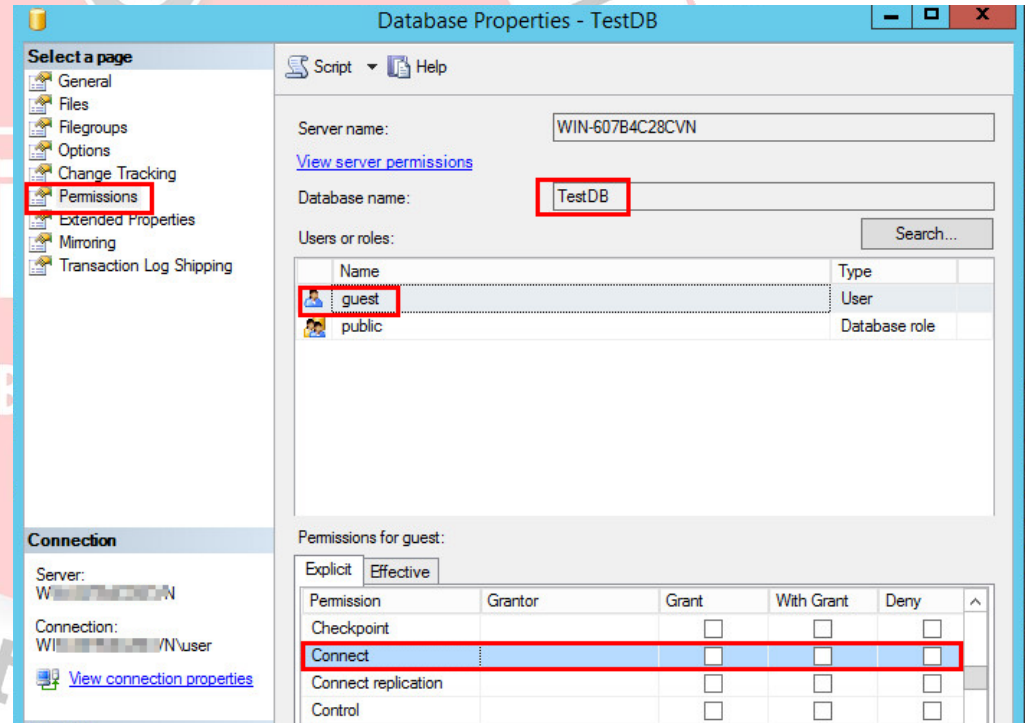

- Sorgu cevap dönerse ilgili veritabanına misafir kullanıcı erişimini (CONNECT hakkı) kaldırmak için;

```
USE [database_name];
```

```
GO
```

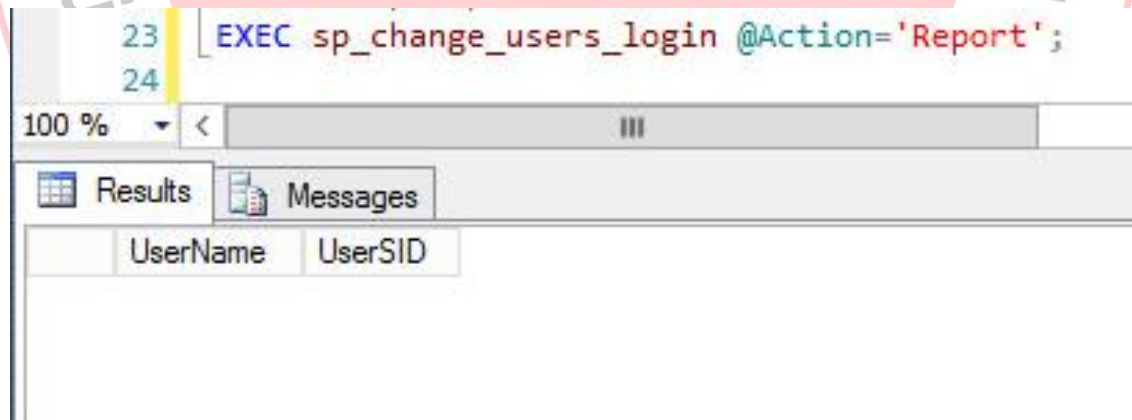
```
REVOKE CONNECT FROM guest;
```

- Varsayılan olarak her yeni eklenen veritabanında misafir kullanıcı hesabı var ama 'CONNECT' hakkı yok.



- Yanlış bir şekilde kullanılmalarını önlemek için potansiyel risk olan Sahipsiz (Orphan) kullanıcılar SQL Server veritabanlarından kaldırılmalı.
- Bu tarz kullanıcıların tespiti için aşağıdaki T-Sql sorgusu kullanılabilir. Hiçbir sonuç dönmemelidir.

```
EXEC sp_change_users_login @Action='Report';
```



- Sorgu sonrası bulunan Sahipsiz Kullanıcıların kaldırılabilmesi için;

TÜBİTAK
DROP USER <username>;

BİLGEM

SİBER GÜVENLİK
ENSTİTÜSÜ



PAROLA POLİTİKALARI

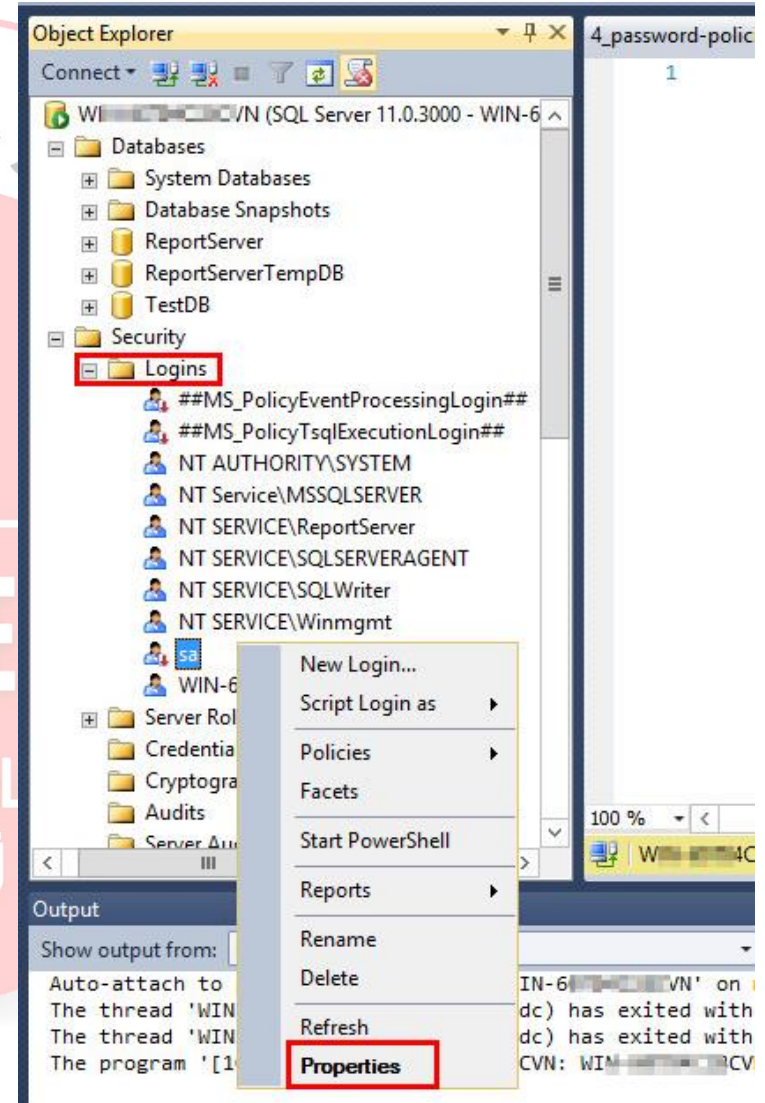
TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü



Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabılır ancak değiştirilemez ve ticari amaçla kullanılamaz. Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

İlk Parolanın Değiştirilmesi

- Parolası güncellenen kullanıcı ilk oturum açtığında SQL Server tarafından verilen parolanın değiştirilmesi istenmeli
- Parola değiştirilmeye zorlanır ve böylece yönetici veya başka birisi tarafından hesaba erişimi engellenmiş olur.



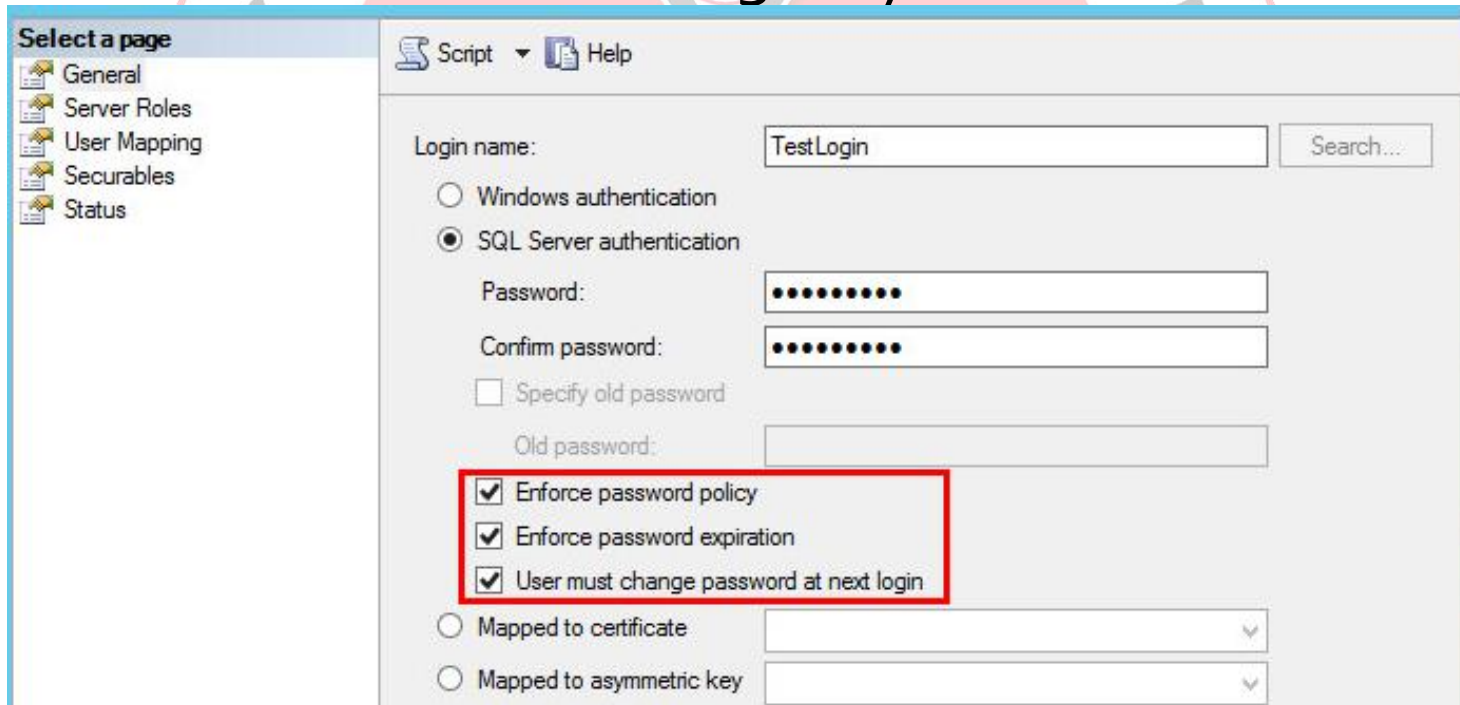
- 'MUST_CHANGE' opsiyonu bütün Sql Erişim Kontrolü login'leri için 'ON' olmalı.
- Bu konfigürasyonu ilgili kullanıcıya atamak için;

```
ALTER LOGIN Kullanici WITH PASSWORD = 'geciciparola123'  
MUST_CHANGE;
```

- Varsayılanda 'ON' şeklindedir.
- Ayrıca 'CHECK_POLICY' ve 'CHECK_EXPIRATION' opsiyonları da etkinleştirilmiş olmalıdır.

İlk Parolanın Değiştirilmesi

- SQL Server Management Studio aracı üzerinden Object Explorer açılır ve hedef instance'a bağlanılır.
- 'Logins' sekmesine gidilir, istenilen login'inin özellikleri bölümünde ilgili ayarlar atanır.



Select a page

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

Script Help

Login name: TestLogin Search...

☐ Windows 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

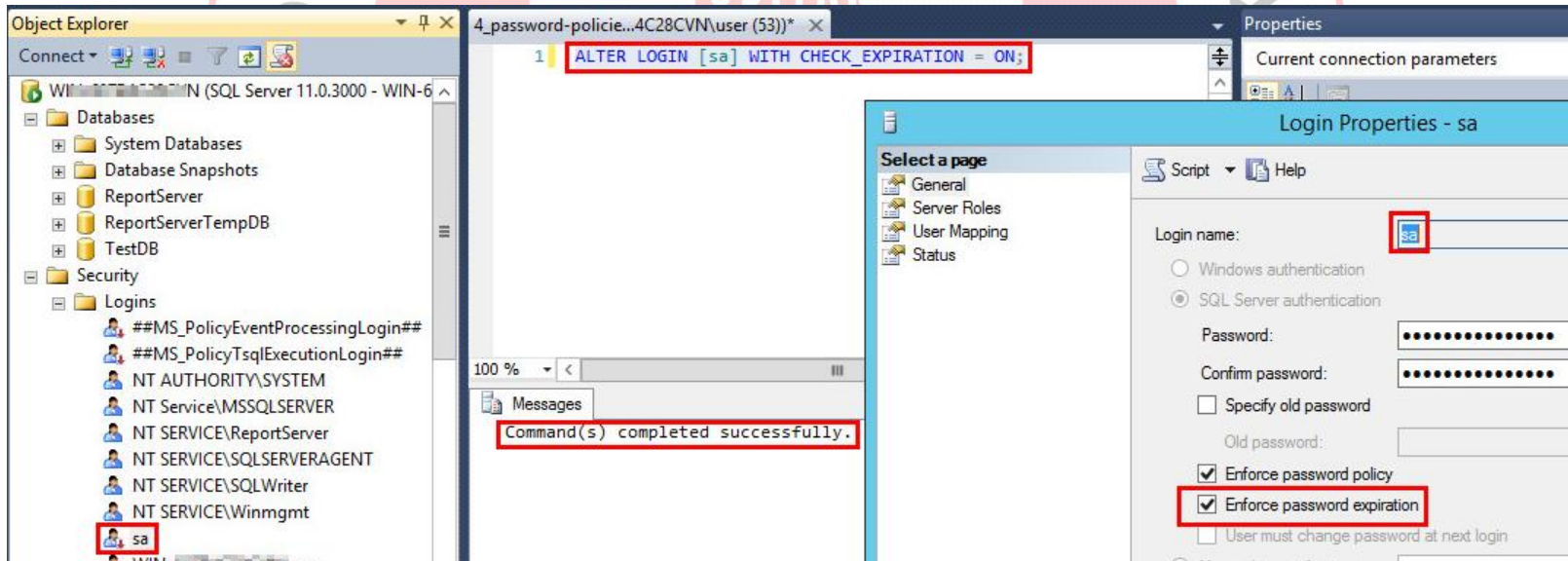
- Kaba kuvvet saldırılarına karşı sysadmin haklarıyla gerçekleştirilen login'lere parola değiştirme sıklığı ayarı girilmelidir.
- Aşağıdaki T-Sql sorgusu ile 'CHECK_EXPIRATION' parametresi 'off' olan sysadmin login'leri bulabiliriz;

```
SELECT l.[name], 'sysadmin membership' AS 'Access_Method'
FROM sys.sql_logins AS l
WHERE IS_SRVROLEMEMBER('sysadmin',name) = 1
AND l.is_expiration_checked <> 1
UNION ALL
SELECT l.[name], 'CONTROL SERVER' AS 'Access_Method'
FROM sys.sql_logins AS l
JOIN sys.server_permissions AS p
ON l.principal_id = p.grantee_principal_id
WHERE p.type = 'CL' AND p.state IN ('G', 'W')
AND l.is_expiration_checked <> 1;
```

- Sonucu 'off' olanları tavsiye edilen şekilde 'on' yapmak için;

```
ALTER LOGIN [login_name] WITH CHECK_EXPIRATION = ON;
```

- Bir SQL, SSMS ile oluşturulduysa 'CHECK_EXPIRATION' değeri varsayılanda 'on' değerindedir.



- Bütün SQL kimlik doğrulama girişleri için 'CHECK_POLICY' değeri 'on' olmalı.
- Karmaşık parola kullanıma zorlanması kaba kuvvet saldırılarının önlenmesinde önemlidir.
- Aşağıdaki sorguda sıfır değeri 'off', bir değeri 'on' manasına gelir.
 - Hiçbir satır döndürmezse ya hiç SQL kimlik doğrulama girişi oluşturulmamıştır ya da hepsi 'on' değerindedir.

```
SELECT name, is_disabled  
FROM sys.sql_logins  
WHERE is_policy_checked = 0;
```

- 'CHECK_POLICY' değerini 'on' yapmak için;

```
ALTER LOGIN [login_name] WITH CHECK_POLICY = ON;
```

- Bu ayar varolan zayıf parolalar üzerinde bir değişiklik yapılması için zorlama yapmıyor.
- Varsayılanda bu değer 'on' değerindedir.

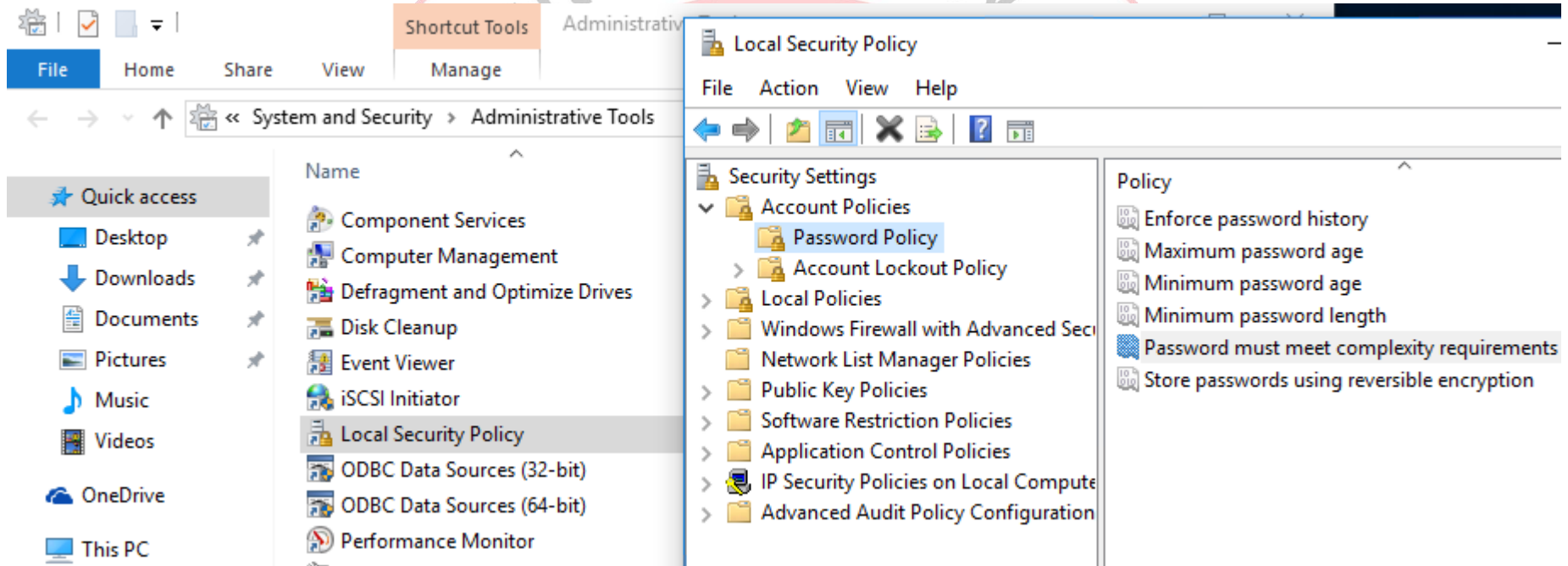
```
4 --Check_password complexity policy
5 SELECT name, is_disabled
6 FROM sys.sql_logins
7 WHERE is_policy_checked = 0;
8
```

100 % < |||

Results Messages

name	is_disabled
Hiçbir değer döndürmedi	

Karmaşık Parola





DENETİM ve LOGLAMA

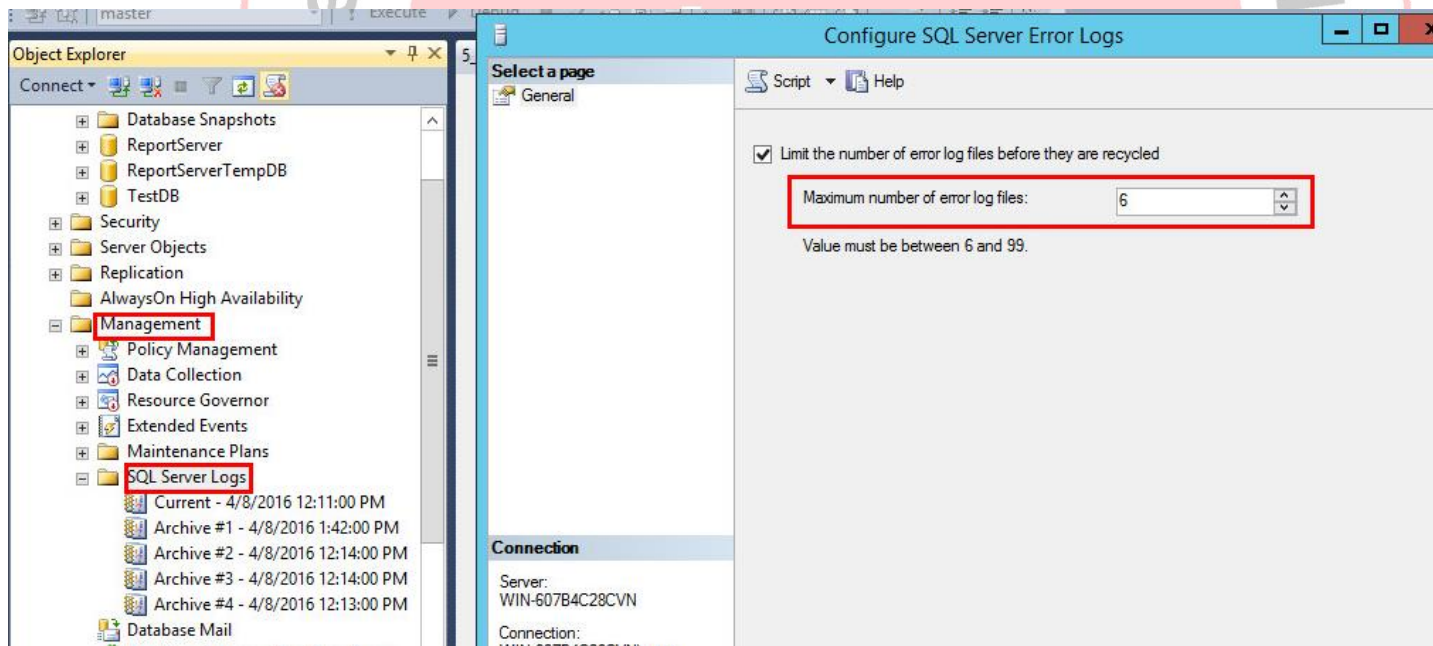
TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü



Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabılır ancak değiştirilemez ve ticari amaçla kullanılamaz. Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

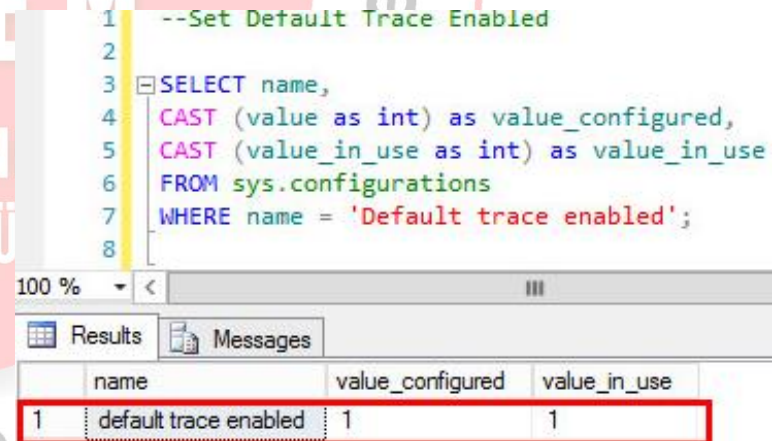
- SQL Server hata log dosyaları sayısı 12 ve üzeri olmalıdır.
 - Varsayılanda bu değer 6 dır.
- Log sayısının artırımı ile üzerine yazma işlemi azaltılmış olur.
- Ayrıca login olamama kayıtları daha fazla tutulmuş olur.

- Varsayılan 6 değerini tavsiye edilen 12 değerine çıkarmak için;
 - SSMS üzerinden Object Explorer açılır ve hedef instance'ye bağlanılır.
 - Sql Server Log'lar üzerinde sağ tıklayıp konfigürasyonlar seçilir ve gerekli değişiklikler yapılır.



- Veritabanı üzerinde hesap oluşturma hak yükseltme ve Database Console Commands (DBCC) komutları çalıştırma aktivitelerinin kayıt altına alınması
- 'Default trace enabled' değeri '1' olmalıdır.
 - Varsayılan değeri '1' dir.
- Aşağıdaki T-SQL sorgusu sonucu bütün sütunlar '1' değerini göstermelidir.

```
SELECT name,  
CAST(value as int) as value_configured,  
CAST(value_in_use as int)  
as value_in_use  
FROM sys.configurations  
WHERE name = 'Default trace enabled';
```



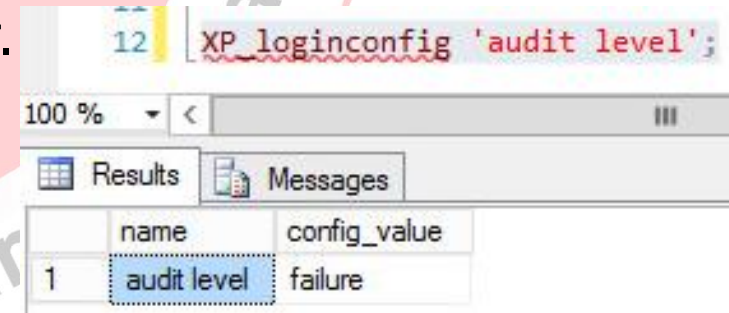
	name	value_configured	value_in_use
1	default trace enabled	1	1

- Aşağıdaki T-SQL komutu ile de ayar yapılmış olur;

```
EXECUTE sp_configure 'show advanced options', 1;  
RECONFIGURE;  
EXECUTE sp_configure 'Default trace enabled', 1;  
RECONFIGURE;  
GO  
EXECUTE sp_configure 'show advanced options', 0;  
RECONFIGURE;
```


- 'Login Denetimi' olarak hatalı login seçilmeli ve yanlış parola denemeleri kayıt altına alınmalı.
 - Varsayılanda bu ayar vardır.
- Böylece parola tahmini saldırıları tespit edilmiş olur.
- Bu konfigürasyona erişebilmek için;
 - SSMS aracı üzerinden hedef instance üzerinde sağ tıklayıp özellikler sonra güvenlik sekmesi seçilir.
 - İlgili instance restart edilmelidir.

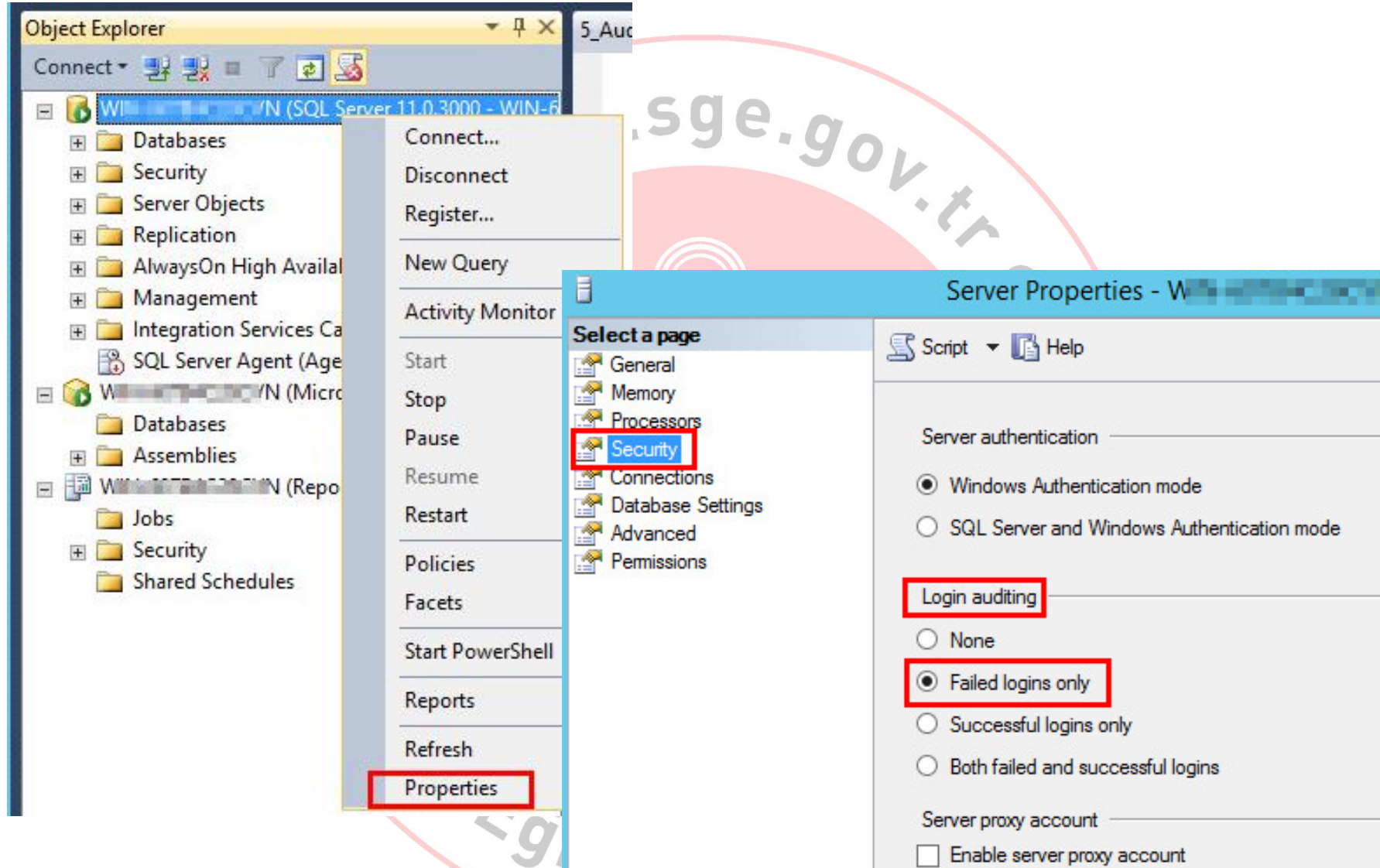
XP_loginconfig 'audit level';



The screenshot shows the 'audit level' configuration in SQL Server Enterprise Manager. The 'name' column is 'audit level' and the 'config_value' column is 'failure'.

	name	config_value
1	audit level	failure

Hatalı Login Kaydı



The screenshot illustrates the steps to configure login auditing in SQL Server. The Object Explorer on the left shows the tree structure: Databases, Security, Server Objects, Replication, AlwaysOn High Availability, Management, Integration Services Catalog, SQL Server Agent (Alerts, Jobs, Operators, Subscriptions, Tasks), and a specific server instance. The 'Security' folder is expanded, showing 'Logins'. The 'Properties' window for a login is open, with the 'Security' tab selected. The 'Login auditing' section is highlighted, showing the 'Failed logins only' option selected.

Object Explorer

- Connect
- Disconnect
- Register...
- New Query
- Activity Monitor
- Start
- Stop
- Pause
- Resume
- Restart
- Policies
- Facets
- Start PowerShell
- Reports
- Refresh
- Properties

Server Properties - W

Select a page

- General
- Memory
- Processors
- Security
- Connections
- Database Settings
- Advanced
- Permissions

Script Help

Server authentication

- ☒ Windows Authentication mode
- ☐ SQL Server and Windows Authentication mode

Login auditing

- ☐ None
- ☒ Failed logins only
- ☐ Successful logins only
- ☐ Both failed and successful logins

Server proxy account

- ☐ Enable server proxy account

- Sql Server Denetimi, hem başarılı hem de hatalı kullanıcı girişlerini tespiti ve denetim politikalarını değiştirme girişimlerini log'lamaktadır.
- 'ERRORLOG' ların azaltılması ile DBA'lar için daha okunur hale getirmektedir.
- SIEM ürünleri için de uyumlu çıktı sağlamaktadır.
- 3 farklı yerden birisine kaydeder.
 - Uygulama olayları kayıtına
 - Güvenlik olayları kayıtına
 - Dosya sistemine

- Sql Server Denetimi ayarına ulaşabilmek için;
 - SSMS üzerinden Sql Server, sonra Güvenlik Dosyasına gelinir.
 - Denetim dosyasından sağ tıklayıp Yeni Denetim seçilir.
 - Server Denetimi için isim verilir, ayarlar sonrası kaydedilir.
 - Server Denetimi üzerinde sağ tıklayıp yeni Server Denetimi Özellikleri seçilir ve isimlendirilir.
 - Denetim içinde sadece Server Denetimi oluşturulması seçilir.
 - Denetim Aksiyon Tiplerinde AUDIT_CHANGE_GROUP, FAILED_LOGIN_GROUP ve SUCCESSFUL_LOGIN_GROUP seçilir.
 - Yeni Server Denetim Özellikleri üzerinde sağ tıklayıp etkinleştirilir.
 - Yeni Server Denetimi üzerinde sağ tıklayıp etkinleştirilir.

SQL Server Denetimi

Object Explorer (SQL Server 11.0.3000 - WIN-6)

- Databases
- Security
 - Logins
 - Server Roles
 - Credentials
 - Cryptographic Providers
 - Audits
 - Audit-Test
 - Server Audit Specifications
 - ServerAuditSpecification-Testtest
 - Server Objects
 - Replication
 - AlwaysOn High Availability
 - Management
 - Integration Services Catalogs
 - SQL Server Agent (Agent XPs disabled)

Create Server Audit Specification

Name: ServerAuditSpecification-Testtest

Audit: Audit-Test

Actions:

	Audit Action Type	Object Class
1	AUDIT_CHANGE_GROUP	
2	FAILED_LOGIN_GROUP	
3	SUCCESSFUL_LOGIN_GROUP	
* 4		

Object Explorer (SQL Server 11.0.3000 - WIN-6)

- Databases
- Security
 - Logins
 - Server Roles
 - Credentials
 - Cryptographic Providers
 - Audits
 - Audit-Test
 - Server Audit Specifications
 - ServerAuditSpecification-Testtest
 - Server Objects
 - Replication
 - AlwaysOn High Availability
 - Management
 - Integration Services Catalogs
 - SQL Server Agent (Agent XPs disabled)

5_Audit-and-loggi...4C28CVN\user (57))*

```
--5.4 Sql Server Audit
SELECT
  S.name AS 'Audit Name'
  , CASE S.is_state_enabled
    WHEN 1 THEN 'Y'
    WHEN 0 THEN 'N' END AS 'Audit Enabled'
  , S.type_desc AS 'Write Location'
  , SA.name AS 'Audit Specification Name'
  , CASE SA.is_state_enabled
    WHEN 1 THEN 'Y'
    WHEN 0 THEN 'N' END AS 'Audit Specification Enabled'
  , SAD.audit_action_name
  , SAD.audited_result
FROM sys.server_audit_specification_details AS SAD
JOIN sys.server_audit_specifications AS SA
ON SAD.server_specification_id = SA.server_specification_id
JOIN sys.server_audits AS S
ON SA.audit_guid = S.audit_guid
WHERE SAD.audit_action_id IN ('CNAU', 'LGFL', 'LGSD');
```

Results

	Audit Name	A.	Writ...	Audit Specification Name	Audit Specification Enabled	audit_action_name	audited_result
1	Audit-Test	N	FILE	ServerAuditSpecification-Testtest	Y	AUDIT_CHANGE_GROUP	SUCCESS AND FAILURE
2	Audit-Test	N	FILE	ServerAuditSpecification-Testtest	Y	FAILED_LOGIN_GROUP	SUCCESS AND FAILURE
3	Audit-Test	N	FILE	ServerAuditSpecification-Testtest	Y	SUCCESSFUL_LOGIN_GROUP	SUCCESS AND FAILURE



UYGULAMA GELİŞTİRME

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü



Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabılır ancak değiştirilemez ve ticari amaçla kullanılamaz. Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

- Veritabanı ve Uygulama kullanıcı girişleri olası 'sql injection' saldırılarına karşı temizlenmesi/filtrelenmesi
 - SQL Injection Prevention Cheat Sheet
https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
- T-SQL ve uygulama kodları incelenmeli/teftiş edilmeli
- Sunucuya kullanıcı girişi göndermek için sadece minimum ayrıcalıklı hesaba izin verilmeli
- Saldırıları minimuma indirmek için parametrelili komutlar (parameterized commands) ve saklı prosedürler (stored procedures) kullanılmalı.

- Kullanıcı girişleri her zaman doğrulanmalı ve kesinlikle doğrudan sql cümlecikleri (sql statements) olarak kullanılmamalı
- Aşağıdaki türdeki kullanıcı girişleri içeriyorsa reddedilmeli:
 - İkili veri (binary data)
 - Özel karakterler (escape sequences)
 - Komut karakterleri



ŞİFRELEME

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü



Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabılır ancak değiştirilemez ve ticari amaçla kullanılamaz. Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

- Simetrik anahtar şifreleme algoritması olarak sadece AES-128 bit şifreleme ve üzeri kullanılmalıdır.
- RC₂, RC₄, RC_{4_128}, TRIPLE_DES_3KEY (DESX) ve TRIPLE_DES algoritmaları zayıf oldukları için önerilmemektedir.
- Varsayılanda şifreleme bulunmamaktadır.
- Eğer veritabanlarında sıkıştırma kullanılıyorsa önce sıkıştırılıp sonra şifrelenmelidir. Çünkü şifrelenmiş veri sıkıştırılamaz.

- Her kullanıcı veritabanı için aşağıdaki denetim yapılabilir;

```
USE [dbname]
GO
SELECT db_name() AS Database_Name, name AS Key_Name
FROM sys.symmetric_keys
WHERE algorithm_desc NOT IN
('AES_128', 'AES_192', 'AES_256')
AND db_id() > 4;
GO
```

- Denetim sonucu hiçbir satır döndürmemelidir.

- Sol Server asimetrik şifreleme algoritması olarak RSA, şifreleme anahtarı olarak güvenli olmasından dolayı 2048 bit tavsiye edilmektedir.
- Varsayılanda şifreleme ayarlanmamıştır.
- Her kullanıcı veritabanı için aşağıdaki denetim yapılabilir;

```
USE [dbname]
GO
SELECT db_name() AS Database_Name, name AS Key_Name
FROM sys.asymmetric_keys
WHERE key_length < 2048
AND db_id() > 4;
GO
```



TÜBİTAK

Teşekkürler