



# GENEL YAPILANDIRMALAR

**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.

- Ad Hoc dağıtık sorgular kullanıcıların harici veri kaynakları üzerinden sorgu ve çalıştırma istekleri gönderilmesine izin veren bir yapılandırmadır.
- Bu kullanımın sistemde kapalı durumda olması gerekmektedir.
- Bu özellik sayesinde SQL Server üzerinde
  - Uzaktan erişim sağlanması ve Exploit çalıştırılması
  - Uygulama fonksiyonları için güvensiz visualbasic kodlarının çalıştırılması gerçekleştirilebilmektedir

- AdHoc dağıtık yapılandırmasını kontrol etmek amacı ile aşağıdaki T-SQL komutu çalıştırılmalıdır.
- Burada gerçekleştirilen sorguda gelen iki sütun değeri de sıfır (0) olmalıdır.

```
SELECT name, CAST(value as int) as value_configured,  
CAST(value_in_use as int) as  
value_in_use  
FROM sys.configurations  
WHERE name = 'ad hoc distributed queries';
```

- AdHoc dağıtık yapılandırmasını yapılandırmak için ise aşağıdaki T-SQL komutları çalıştırılmalıdır.

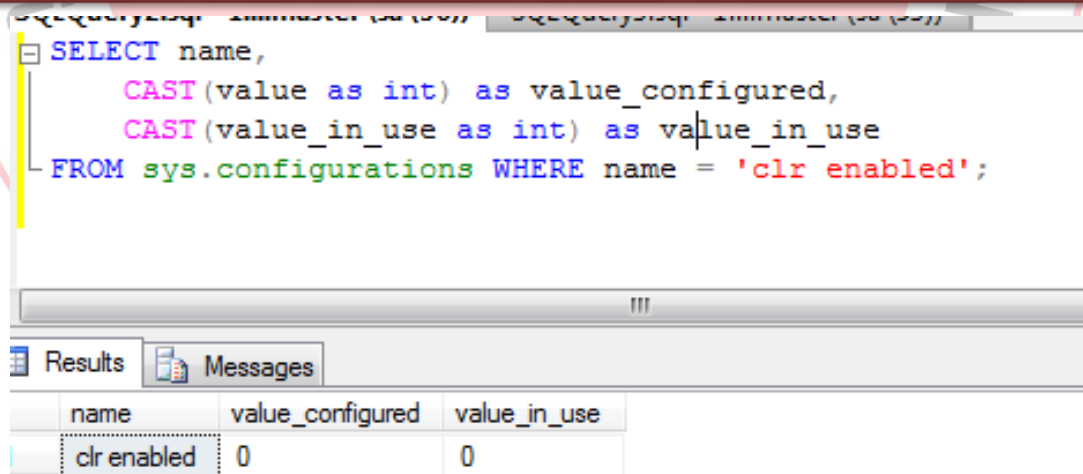
```
EXECUTE sp_configure 'show advanced options', 1;  
RECONFIGURE;  
EXECUTE sp_configure 'Ad Hoc Distributed Queries', 0;  
RECONFIGURE;  
GO  
EXECUTE sp_configure 'show advanced options', 0;  
RECONFIGURE;
```

- Common language runtime (CLR) özelliği ile kullanıcıları kodlarının SQL Server tarafından çalıştırılması sağlar.
- Bu özelliğin açık olması ile SQL Serverin saldırı yüzeyini artırır
- Yanlışlıkla veya zararlı kodların çalışmasına da olanak sağladığı için büyük risk oluşturmaktadır.

TÜBİTAK  
BİLGEM  
SİBER GÜVENLİK  
ENSTİTÜSÜ

- CLR Enabled özelliğinin sistemdeki durumunu kontrol etmek için aşağıdaki T-SQL sorgusu gerçekleştirilir
- Bu sorgu sonucunda elde edilen iki veri de sıfır olmalıdır.

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



The screenshot shows a SQL Server Enterprise Manager window with a query executed. The query is the same as the one in the red box. The results pane shows a single row with the following data:

| name        | value_configured | value_in_use |
|-------------|------------------|--------------|
| clr enabled | 0                | 0            |

- CLR Enabled özelliği eğer sıfıran farklı bir değere atanmış ise o zaman aşağıdaki T-SQL sorgusu ile bu özellik kapatılmalıdır.

```
EXECUTE sp_configure 'clr enabled', 0;  
RECONFIGURE;
```

**BİLGEM**

SİBER GÜVENLİK  
ENSTİTÜSÜ



- «cross-database ownership chaining» özelliği ile tüm veritabanları seviyesinde kontrol gerçekleştirilmesine olanak vermektedir.
  - Bir kullanıcının erişim izni olmadığı başka bir vt'de yer alan nesneye dolaylı erişim izni verilmesi
  - Kullanıcı A vt de yer alan A view'ına select yetkisi olsun. Eğer bu özellik enable edilirse, A view üzerinden yetkisi olmadığı B vt de yeralan B view'ına erişim sağlar.
- Bu özelliğin aktif edilmesi ile kullanıcının Veritabanı içindeki db\_owner rolü ile diğer veritabanlarına ve Veritabanı gerekli olmamasına rağmen erişim gerçekleştirilmektedir.
- Gerekli olduğu zaman ise «cross-database ownership chaining» özelliği sadece bir Veritabanı için aktif hale getirilmelidir.
- Bu Veritabanı özelliği master, test veya production veritabanlarından hiçbirisinde değiştirilmemelidir.



- «cross-database ownership chaining» özelliğinin sistemdeki durumunu kontrol etmek için aşağıdaki T-SQL sorgusu gerçekleştirilir
- Bu sorgu sonucunda elde edilen iki veri de sıfır olmalıdır.

```
SELECT name,  
CAST(value as int) as value_configured,  
CAST(value_in_use as int) as value_in_use  
FROM sys.configurations  
WHERE name = 'Cross db ownership chaining';
```

- «cross-database ownership chaining» özelliği eğer sıfıran farklı bir değere atanmış ise o zaman aşağıdaki T-SQL sorgusu ile bu özellik kapatılmalıdır.

```
EXECUTE sp_configure 'Cross db ownership chaining', 0;  
RECONFIGURE;  
GO
```

SİBER GÜVENLİK  
ENSTİTÜSÜ

- SQL Server tarafından mail oluşturma ve gönderme özelliğinin sistem üzerinde kapalı olması gerekmektedir.
- Bu yapılandırma için 'Database Mail XPs' seçeneği üzerinde değişiklikler yapılmaktadır.
- Veritabanı mail sisteminin kapatılması saldırı yüzeyinin azaltılmaktadır.
- DDOS saldırı yüzeyi ve saldırı kanalını da kapatmaktadır.

TÜBİTAK  
**BİLGEM**

SİBER GÜVENLİK  
ENSTİTÜSÜ

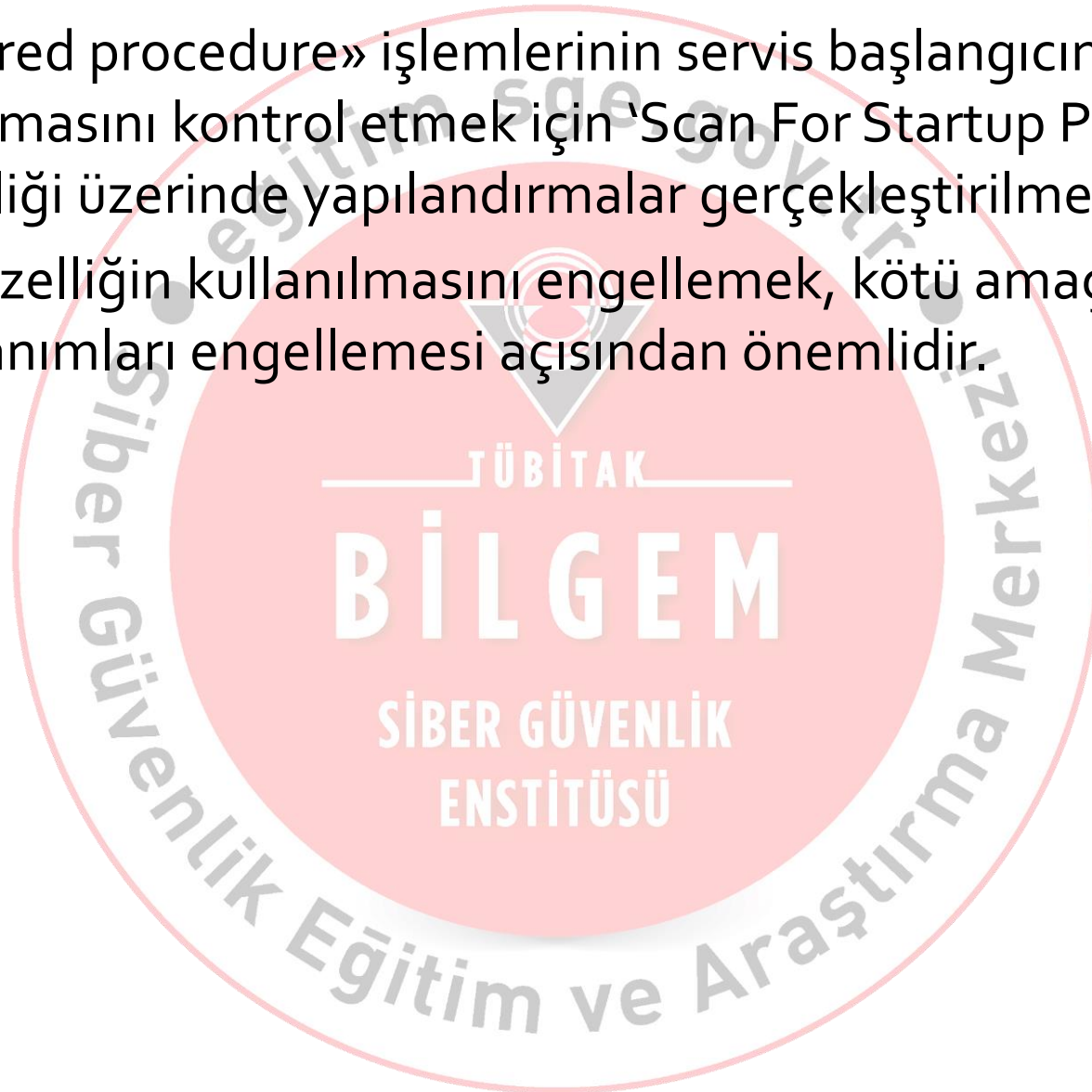
- 'Database Mail XPs' özelliğinin sistemdeki durumunu kontrol etmek için aşağıdaki T-SQL sorgusu gerçekleştirilir
- Bu sorgu sonucunda elde edilen iki veri de sıfır olmalıdır.

```
SELECT name,  
CAST(value as int) as value_configured,  
CAST(value_in_use as int) as value_in_use  
FROM sys.configurations  
WHERE name = 'Database Mail XPs';
```

- 'Database Mail XPs' özelliği eğer sıfıran farklı bir değere atanmış ise o zaman aşağıdaki T-SQL sorgusu ile bu özellik kapatılmalıdır.

```
EXECUTE sp_configure 'show advanced options', 1;  
RECONFIGURE;  
EXECUTE sp_configure 'Database Mail XPs', 0;  
RECONFIGURE;  
GO  
EXECUTE sp_configure 'show advanced options', 0;  
RECONFIGURE;
```

- «stored procedure» işlemlerinin servis başlangıcında çalışmasını kontrol etmek için 'Scan For Startup Procs' özelliği üzerinde yapılandırmalar gerçekleştirilmektedir.
- Bu özelliğin kullanılmasını engellemek, kötü amaçlı kullanımları engellemesi açısından önemlidir.



- 'Scan For Startup Procs' özelliğinin sistemdeki durumunu kontrol etmek için aşağıdaki T-SQL sorgusu gerçekleştirilir
- Bu sorgu sonucunda elde edilen iki veri de sıfır olmalıdır.

```
SELECT name,  
CAST(value as int) as value_configured,  
CAST(value_in_use as int) as value_in_use  
FROM sys.configurations  
WHERE name = 'Scan for startup procs';
```

SİBER GÜVENLİK  
ENSTİTÜSÜ



- 'Scan For Startup Procs' özelliği eğer sıfırdan farklı bir değere atanmış ise o zaman aşağıdaki T-SQL sorgusu ile bu özellik kapatılmalıdır.

```
EXECUTE sp_configure 'show advanced options', 1;  
RECONFIGURE;  
EXECUTE sp_configure 'Scan for startup procs', 0;  
RECONFIGURE;  
GO  
EXECUTE sp_configure 'show advanced options', 0;  
RECONFIGURE;
```

- Veritabanındaki TRUSTWORTHY özelliği, Veritabanı nesnelerinin farklı bir Veritabanı veya durumdaki Veritabanı nesnelerine erişimi sağlamaya izin verir.
- Bu özelliğin kapatılması ile zararlı komut veya prosedürlere karşı koruma sağlanmış olur.

**BİLGEM**

SİBER GÜVENLİK  
ENSTİTÜSÜ

- 'Remote Access' özelliğinin sistemdeki durumunu kontrol etmek için aşağıdaki T-SQL sorgusu gerçekleştirilir
- Bu sorgu sonucunda bir değer geri dönmesi beklenmez.

```
SELECT name  
FROM sys.databases  
WHERE is_trustworthy_on = 1  
AND name != 'msdb'  
AND state = 0;
```

- Bu özelliğin kapatılması için, aşağıdaki komutun çalıştırılması gerekmektedir.

```
ALTER DATABASE <dbname>  
SET TRUSTWORTHY OFF;
```



- MS SQL Server birçok protokole destek sağlamaktadır.
  - Shared Memory
  - Named Pipes
  - TCP/IP
  - VIA
- Kullanılan protokol seviyesi ihtiyaca göre minimum seviyede tutulmalıdır.
- Az sayıda protokol kullanımı SQL sunucu üzerindeki saldırı yüzeyini azaltır
- Uzak saldırılara karşı koruma sağlar

- SQL Server Configuration Manager içerisinde, SQL Server Network Configuration Özellikleri gerekli olanların aktif halde tutulması gerekmektedir
- Gerekli olmayan protokoller kapatılmalı
- Database engine, değişikliklerin aktif hale gelebilmesi için yeniden başlatılmalıdır.

TÜBİTAK  
BİLGEM  
SİBER GÜVENLİK  
ENSTİTÜSÜ



- Kurulum sırasında gelen varsayılan port TCP/1433'dür
- Bu porta yapılan otomatik saldırılarının engellenmesi için yönetici tarafından değiştirilmelidir.

TÜBİTAK  
**BİLGEM**  
SİBER GÜVENLİK  
ENSTİTÜSÜ



- Kullanılan portun denetlenmesi için aşağıdaki powershell komutu çalıştırılmalıdır.

```
PS C:\>netstat -ano |select-string 1433.+listening
```

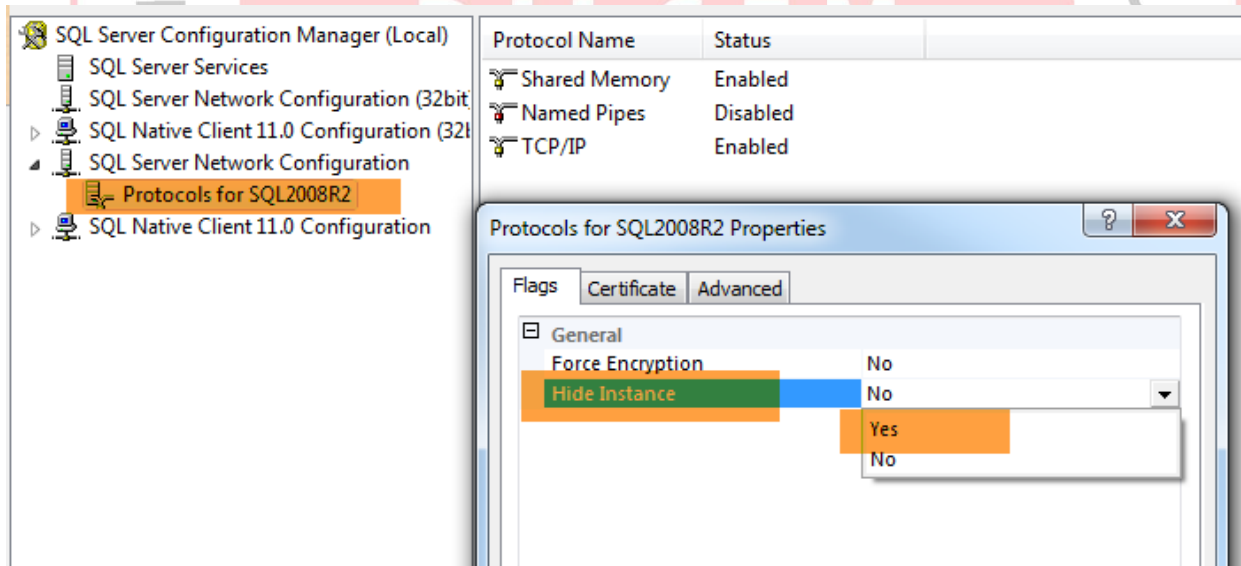
- Bu komut sonucunda bir değer dönmemesi beklenmektedir.
- Eğer bir sonuç döner ise, SQL server varsayılan portlarda kullanılıyor demektir
- SQL Server Configuration Manager Üzerinden yapılandırmalar yapılmalıdır.

- Port değişiminden etkilenecek tüm yapılandırmaların değiştirilmesi
- Firewall ve Router yapılandırmaları
- Client yapılandırmaları



# «Hide Instance» Yapılandırması

- Yayında olan ve cluster yapıda olmayan SQL server instance'ları gizli olacak şekilde tasarlanmalıdır.
  - SQL Browser çalışabilir, ama vt görünmez
- Gizli olarak yapılandırılan instance'ler güvenli kurulum yapmaya olanak sağlar



- SQL Server konfigurasyon manager, SQL Server Network configuration içerisinde
- Bayrak yapılandırmalarında bulunan «Hide instance» yapılandırmasının seçili olması gerekmektedir.
- «Hide Instance» Yapılandırması aktif değil ise aktif hale getirmek için yukarıda bahsedilen seçenek evet olarak işaretlenmelidir.
- SQL Server içinde instance'ler varsayılan olarak hidden olarak tanımlı değildir.

- sa kullanıcısı SQL server üzerinde sysadmin hakları ile tanımlanmış bir kullanıcıdır
- Saldırganların kaba kuvvet saldırılarına mağrus kalmaması için bu hesabın pasif hale getirilmesi gerekmektedir.

TÜBİTAK  
**BİLGEM**  
SİBER GÜVENLİK  
ENSTİTÜSÜ

- Aşağıdaki sorgu ile sa kullanıcısının durumu denetlenebilmektedir.

```
SELECT name, is_disabled  
FROM sys.server_principals  
WHERE sid = 0x01;
```

- Bu sorgu sonucunda is\_disabled değeri 1 olarak döner ise bu sa kullanıcısının pasif durumda olduğunu göstermektedir.
- sa kullanıcısını pasif hale getirmek için aşağıdaki sorgu çalıştırılmalıdır.

```
ALTER LOGIN sa DISABLE;
```



- Özellikle yazılım ve betiklerin kullanılmasında sa hesabının kullanılması güvensiz bir yaklaşımdır.
- Bu hesabın pasif hale getirilmesi ile sa hesabını kullanan uygulama ve betikler çalışmaz.
- Uygulama ve betik tasarımı gerçekleştirilirken bu durum göz önünde bulundurulmalıdır.

**BİLGEM**

SİBER GÜVENLİK  
ENSTİTÜSÜ



- xp\_cmdshell prosedürü, SQL server kullanıcısının işletim sistemi komutu çalıştırması ve sonuçları okumasına olanak sağlar.
- xp\_cmdshell ile saldırganlar eriştikleri SQL server sunucusunda işletim sistemi komutu çalıştırabiliyorlar.
- Büyük bir güvenlik riski oluşturuyor

**BİLGEM**  
SİBER GÜVENLİK  
ENSTİTÜSÜ

- Sistemdeki xp\_cmdshell yapılandırmasının durumunu öğrenebilmek için aşağıdaki sorgu çalıştırılabilir.

```
EXECUTE sp_configure 'show advanced options',1;  
RECONFIGURE WITH OVERRIDE;  
EXECUTE sp_configure 'xp_cmdshell';
```

- Bu sorgunun geri dönüş değeri sıfır ise bu özellik kapalı olarak yapılandırılmıştır.

- xp\_cmdshell yapılandırmasını kapatmak için aşağıdaki T-SQL sorgusu çalıştırılmalıdır.

```
EXECUTE sp_configure 'show advanced options', 1;  
RECONFIGURE;  
EXECUTE sp_configure 'Xp_cmdshell', 0;  
RECONFIGURE; GO EXECUTE sp_configure 'show advanced  
options', 0;  
RECONFIGURE;
```

SİBER GÜVENLİK  
ENSTİTÜSÜ