



SQL SERVER AYARLARI

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.

- TCP 1433 ve TCP 1434 numaralı portlar Sql server'ın default portları olduğundan değiştirilmeli
- Named instancelar için Dynamic port numarası **verilmemeli**
- Dinamik port, SQL Server servisi başladığında 1433 numaralı port başka bir uygulama tarafından kullanılıyor ise clientların erişiminde problem yaşanmaması için dinamik port atamasına dayanan bir mimariye dayanır
- Fakat kurumsal yapılarda SQL Server sunucu adanmış makine olacağından dinamik portalar ihtiyaç olmaz

- Sql Server sunucusu Güvenlik Duvarı ile korunmalı
- Veritabanı sunucusu DMZ yerine iç ağa konulabilir.
- İç ağda da sunucu güvenlik duvarı ile korunmalıdır
 - Bu güvenlik duvarı sadece uygulama sunucusundan gelen(veya orta katman) trafiğe izin vermeli
- Toplam 3 adet Güvenlik duvarı kullanımı idealdir
 1. DMZ önündeki Güvenlik Duvarı
 2. İç ağın önündeki Güvenlik Duvarı(Veritabanı sunucusu da bunun arkasında)
 3. Sadece veritabanı sunucularını koruyan Güvenlik Duvarı

- 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.

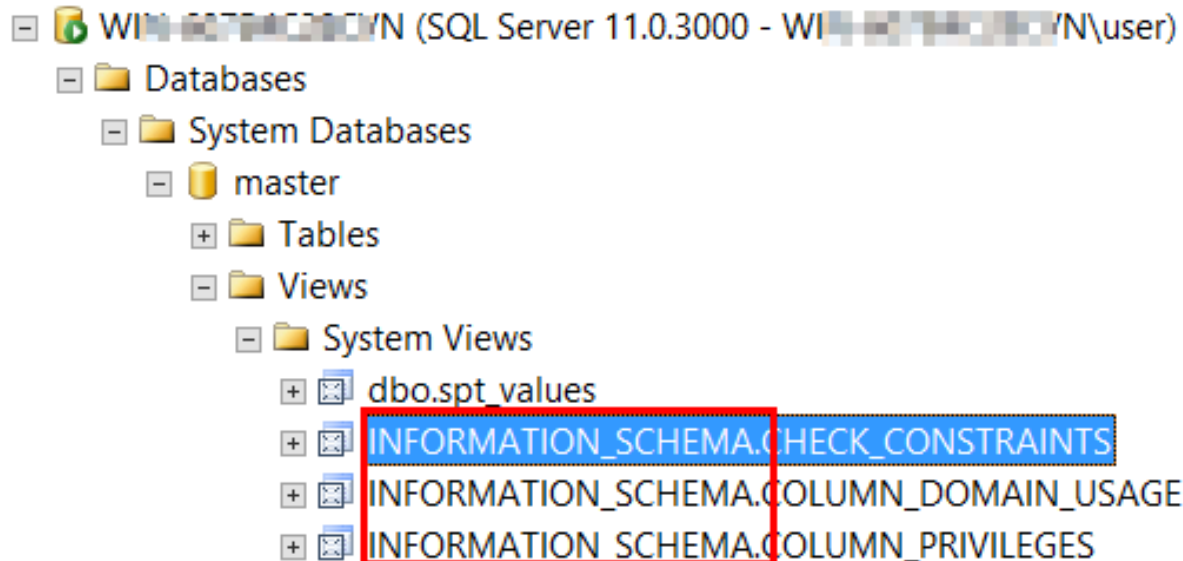
TÜBİTAK
BİLGEM
SİBER GÜVENLİK
ENSTİTÜSÜ

Özet

- Desteklenen network protokollerini sınırlayın
- Gerekmedikçe network protokollerini enable etmeyin
- SQL Server çalışan bir sunucuyu doğrudan internete açmayın
- Named instancelar için TCP/IP için dinamik port yerine belirli port kullanımını sağlayın.

- Veritabanları, tablolar ve diğer objeler için bilgi(metadata) sistem kataloglarında saklanır.
- Bu metadata master veritabanında ve kullanıcı veritabanlarında bulunur.
- Bu metadata tablolarını görmek için metadata viewları bulunmaktadır.
- SQL Server 2000'de bu sistem metadata tabloları public olarak okunabilir idi. İstenirse bu tablolar yazılabilir olacak şekilde de ayarlanabilir.
- SQL Server 2005'ten sonra bu sistem metadata tabloları readonly dir ve yapıları değişmiştir.
- SQL Server 2005'ten sonra bu metadataalar sys şemasının altında toplanmıştır.
- Geçmişe yönelik uyumluluk için de bazı tabloların yapısı korunmuştur.

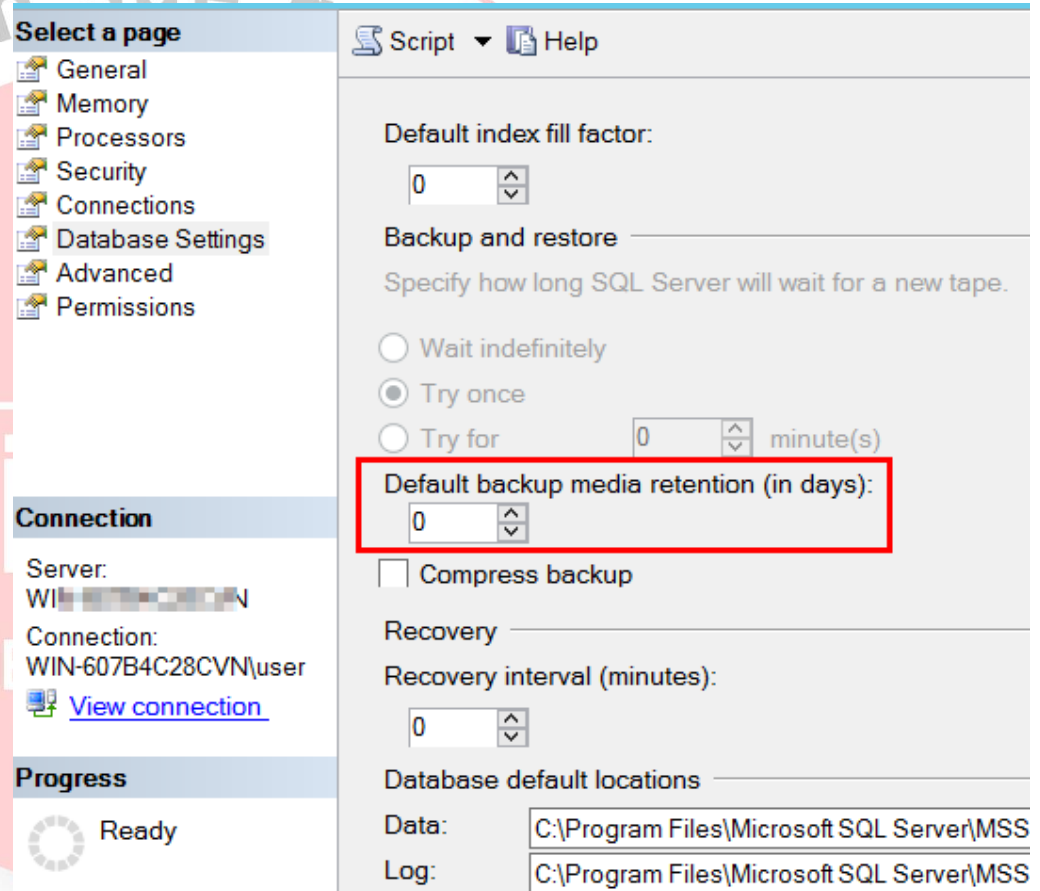
- SQL Server metadata master veritabanı altında bulunan sistem viewlarında bulunur.
- Bu kataloğa Information_Schema denir.



- SQL Server 2005 ve sonrasında tüm metada viewları default'ta güvenlidir. Gerekmedikçe ayarları değiştirilmemelidir;
 - Yeni metadata viewları(örnek sys.tables, sys.procedures)
 - INFORMATION SCHEMA Viewları
- Sistem metadata viewlarındaki bilgiye erişim row bazlı yetkilendirilmiştir.
- Yani bir kullanıcının bir objenin metadatasını görebilmesi için, kullanıcının o obje üzerinde bazı haklara sahip olması gerekmektedir.
- Örnek: dbo.authors tablosunun metadatasını görebilmek için tablo üzerinde select hakkı verilmesi gereklidir.

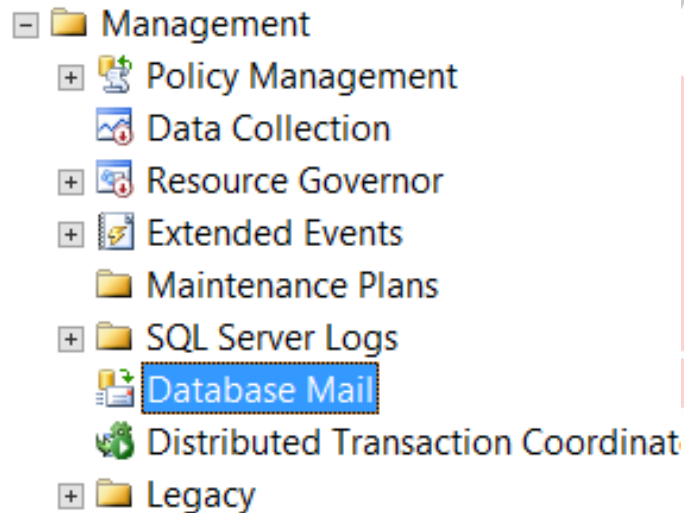
Medyaların Tutulması (Media Retention)

- Backup medyasını elde tutma süresi, elde full backupı bulunduracak en az güne ayarlanmalı
- İdeali, kaynaklar izin verdiği ölçüde yüksek olmasıdır.
- Yedeklerin tutulması ayarı bakım planlamasında kurulması gerekir. Varsayılanda veritabanı yedekleri silinmez.



The screenshot shows the SQL Server Enterprise Manager interface. On the left, the 'Select a page' menu is open, showing options like General, Memory, Processors, Security, Connections, Database Settings, Advanced, and Permissions. The 'Connection' page is selected, showing the server name 'WIN-607B4C28CVN' and the connection path 'WIN-607B4C28CVN\user'. The 'Progress' section shows a 'Ready' status. On the right, the 'Script' and 'Help' tabs are visible. The 'Default index fill factor' is set to 0. The 'Backup and restore' section is expanded, showing the 'Default backup media retention (in days)' setting, which is currently set to 0 and is highlighted with a red box. Other settings include 'Wait indefinitely', 'Try once', 'Try for 0 minute(s)', 'Compress backup' (unchecked), 'Recovery interval (minutes)' set to 0, and 'Database default locations' for Data and Log, both pointing to 'C:\Program Files\Microsoft SQL Server\MSS'.

- Mesajlaşma gerekmiyorsa “Database Mail” kapatılmalı
- Database Mail, SQL Mail’in yeni versiyonudur.



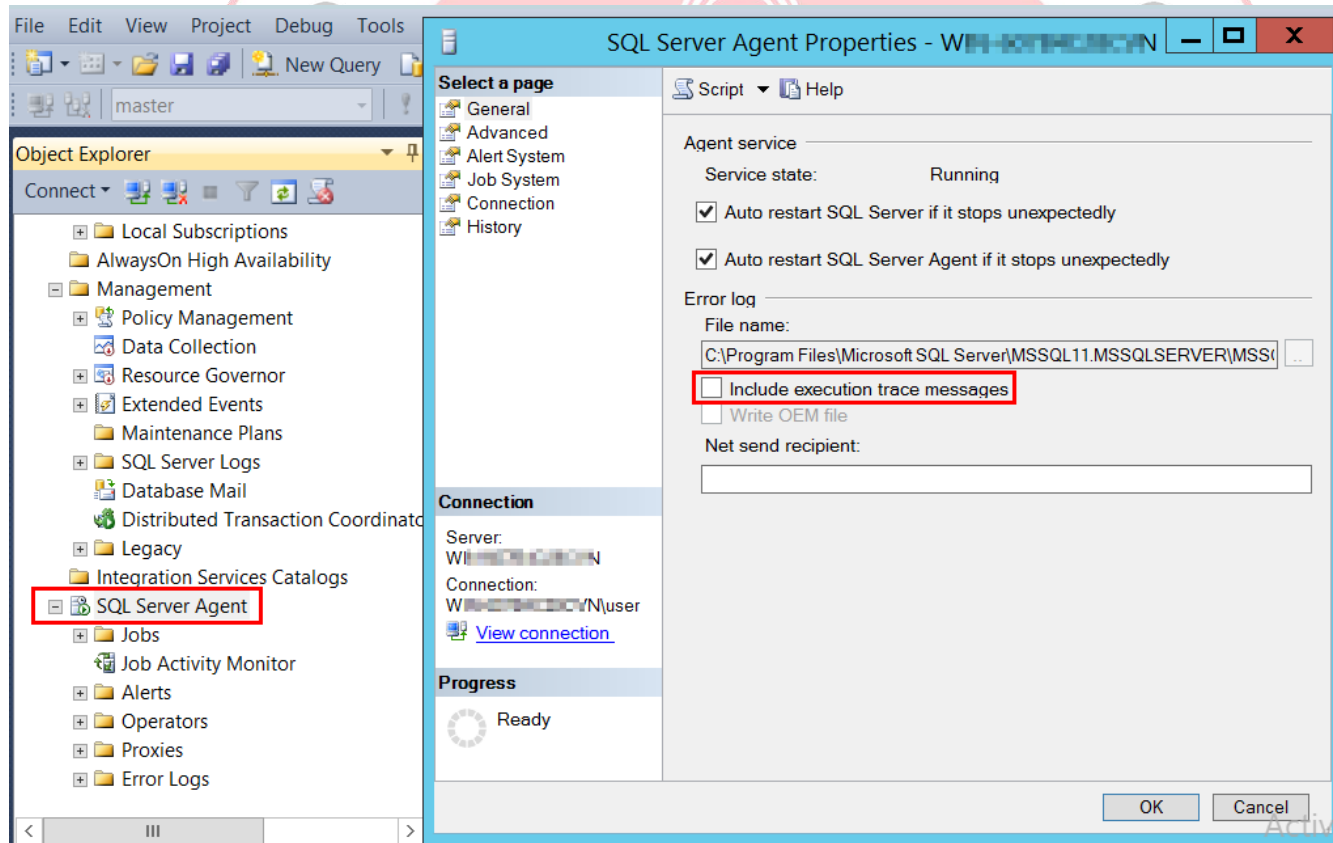
- Varsayılanda kapalıdır.
- Veritabanı posta etkin olup olmadığını belirlemek için;

```
2 EXECUTE sp_configure 'Database Mail XPs';
```

Results					
	name	minimum	maximum	config_value	run_value
1	Database Mail XPs	0	1	0	0

Trace Messages

- Error Log/Include execution trace messages = off olmalı
- Diski doldurmayı hedefleyen Servis Dışı Bırakma(DOS) saldırıları için bir önlemdir.



- Kritik olan kullanıcı tanımlı(User-defined) stored prosedürleri encrypt edilmelidir.
- Hassas bilgi içerebilirler
- **CREATE PROCEDURE #EncryptSP WITH ENCRYPTION**
 - Execution Plan oluşturmaz

SQLQuery1.sql - WI...4C28CVN\user (52))* x

```
1 SELECT
2 IsEncrypted = OBJECTPROPERTY(OBJECT_ID, 'IsEncrypted'),
3 ObjectName = OBJECT_NAME(OBJECT_ID)
4 FROM sys.sql_modules;
```

100 %

Results

Messages

	IsEncrypt...	ObjectName
1	0	sp_MSrepl_startup
2	0	sp_MScleanupmergepublisher
3	0	spt_values

- SQL Server bazı yönetimsel task'lar için **xp_** veya **sp_** önekle sistem stored procedure'leri kullanır;
 - Mail gönderme ve COM component call edilmesi gibi.
 - SQL Server instance'ı dışındaki kaynaklara erişmek.
- Sistem SP (Stored Procedure)'leri;
 - Prosedürün içinde bazı güvenlik kontrolleri yapar.
 - Görevini yerine getirmek için login olunan Windows kullanıcıasını taklit ederek (impersonate) işlem yapar.
 - Alt seviye işletim sistemi fonksiyonlarını kullanır.
- Bazı SP'ler, işletim sistemi ile etkileşerek ve SQL Server permissionları dışında kod çalıştırabildiğinden risklidir.

- Kapatılırken uygulamaların ihtiyaçları gözetilmelidir.
- Bazı uygulamalar veri import ve export işlemleri için bazı extended stored procedure'lere ihtiyaç duyar.
- Kapatılmayan stored procedureleri dökümanite edilmeli ve exception olarak not edilmelidir.

TÜBİTAK
BİLGEM
SİBER GÜVENLİK
ENSTİTÜSÜ

Kapatılacak Ext. Stored Procedure'ler

- **xp_cmdshell** en kritik extended stored procedure
- Varsayılanda kapalıdır.
- SQL Server içinden, işletim sistemi fonksiyonlarını çalıştırır.
- İşletim sistemine erişme ve ağ saldırıları potansiyeline sahiptir.

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

100 % < |||

Results Messages

	name	minimum	maximum	config_value	run_value
1	xp_cmdshell	0	1	0	0

Kapatılacak Ext. Stored Procedure'ler

Extended Stored Procedure Adı	
xp_available_media	xp_getnetname
xp_dirtree	xp_logevent
xp_dsninfo	xp_loginconfig
xp_enumdsn	xp_msver
xp_enumerrorlogs	xp_readererrorlog
xp_enumgroups	xp_servicecontrol
xp_eventlog	xp_sprintf
xp_fixeddrives	xp_sscaf
xp_getfiledetails	xp_subdirs

REVOKE EXECUTE ON <Extended_Stored_Procedure_Adi> TO PUBLIC;

Varsayılanda hepsi kapalıdır.

Extended Stored Procedure Adı	
xp_deletemail	
xp_findnextmsg	
xp_get_mapi_default_profile	
xp_get_mapi_profiles	
xp_readmail	
xp_sendmail	
xp_startmail	
xp_stopmail	

```
EXECUTE sp_configure 'show advanced options',1
RECONFIGURE WITH OVERRIDE
EXECUTE sp_configure 'SQL Mail XPs',0
RECONFIGURE WITH OVERRIDE
```

Varsayılanda hepsi kapalıdır.

Extended Stored Procedure Adı	
xp_cleanupwebtask	
xp_convertwebtask	
xp_dropwebtask	
xp_enumcodepages	
xp_makewebtask	
xp_readwebtask	
xp_runwebtask	

*EXECUTE sp_configure 'show advanced options',1
RECONFIGURE WITH OVERRIDE
EXECUTE sp_configure 'web assistant procedures',0
RECONFIGURE WITH OVERRIDE*

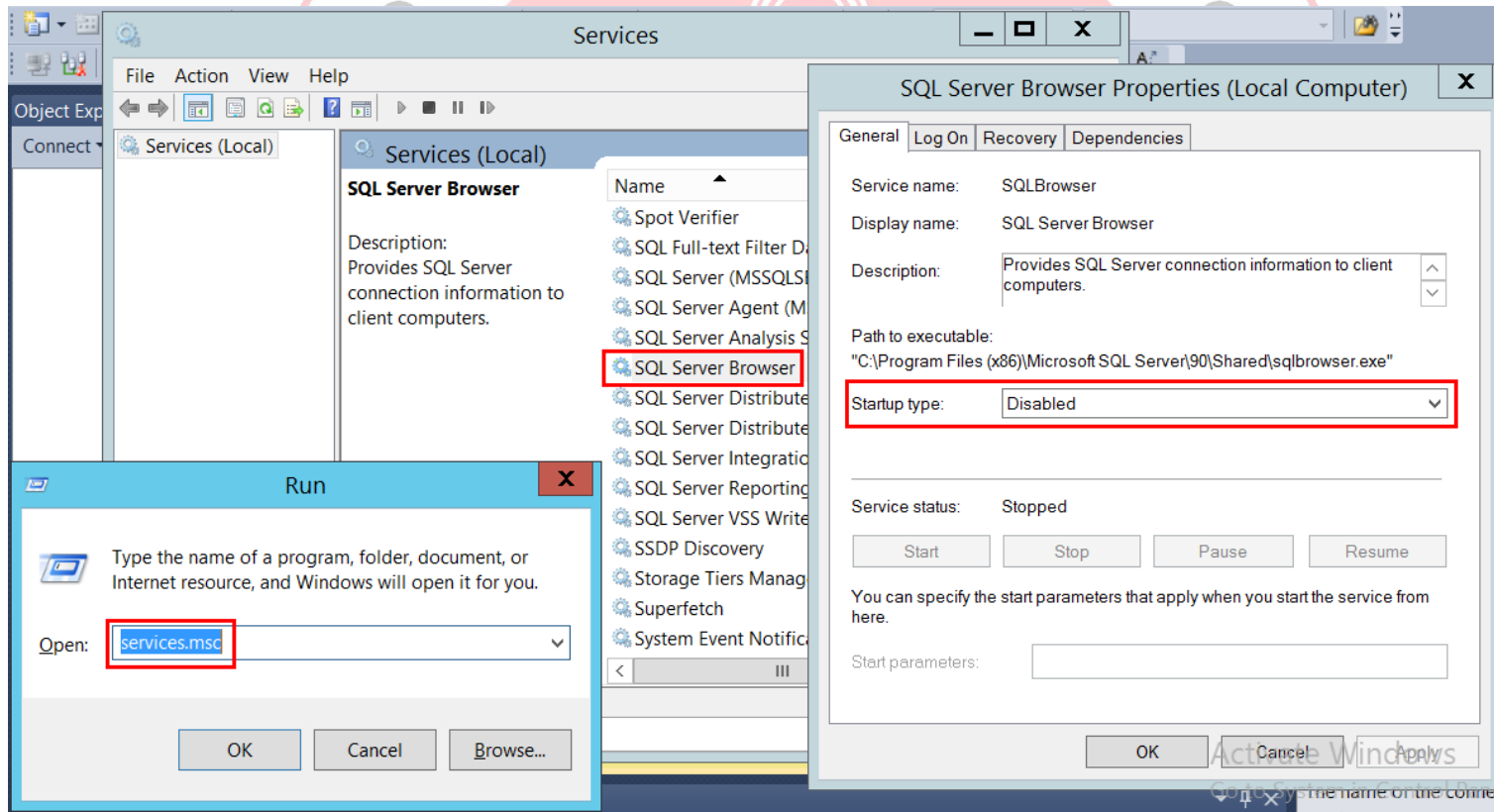
- Varsayılanda tümü kapalıdır.

Extended Stored Procedure Adı	
xp_regaddmultistring	
xp_regdeletekey	
xp_deletevalue	
xp_enumvalues	
xp_regremovemultistring	
xp_regwrite	

REVOKE EXECUTE ON <Extended_Stored_Procedure_Adi> TO PUBLIC;

SQL Server Tarayıcı Servisi

- SQL Server Browser servisi kapatılmalı
- Varsayılanda kapalıdır.
- SQL Server Browser kapatıldığında clientlara bağlantı için port sağlanmalıdır.



- İlk kurulumda 'default instance' üzerinde sql server tarayıcı servisi kapalı olmakta. Yalnız 'named instance' kurulduğunda başlangıçta otomatik ayarlanabilmektedir.
- Bu servisin kullanılması tavsiye edilmemekte.

