TÜBİTAK

MSSQL Veritabanı Güvenliği Eğitimi

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

İşletim Sistemi ve Ağ İle ilgili Konular

MODÜL 1

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Fiziksel Güvenlik

- SQL Server sunucusu fiziksel olarak güvenli bir yerde konumlandırılmalıdır.
  - Kilitli Odalar
  - Kamera Sistemleri
  - Giriş Çıkış Kayıtları…
- Sadece yetkisi olan personel erişim sağlamalı

Etki Alanı Ortamı

- SQL Server, diğer etki alanları tarafından güvenilen bir etki alanında ise;
  - Güvenilen etki alanlarına verilen erişim hakları kontrol edilmelidir
- Güvenilen etki alanından SQL Server'a ve içerdiği veritabanlarına sınırlı yetki verilmelidir
- Verilen yetkiler ve hakların dokümantasyonunun yapılması gerekmektedir

İnternet Üzerinden Erişilen SQL Server

- SQL Server bir uygulamaya kaynak sağlıyorsa (web server gibi)
  - internet erişimi SQL Server, WEB Server ile beraber DMZ'e konulmalı
- Bu SQL Server'ın veritabanının içeriği sadece public olarak yayınlanabilecek veriler için olmalıdır.

İnternet Üzerinden Erişilen SQL Server

- Özellikle internete açık bir SQL Server güvenlik duvarı arkasında konuşlandırılmalıdır.
- TCP-1433 ve UDP 1434 portları bloke edilmeli
- Named Instance'lar ek olarak diğer portları dinliyorsa bu portlar da ayrıca bloke edilmeli
- Multi-tier ortamlarda çoklu firewall kullanarak denetimli altağlar oluşturulmalı
- Web logic ve bussiness logic farklı makinelere dağıtılmalı

Test ve Geliştirme Sunucuları

- Test ve geliştirme sunucuları, canlı sistem sunucuları ile farklı ağ segmentlerinde konuşlandırılmalıdır
- Yamalar, canlı sistem sunucularına uygulanmadan önce dikkatlice test edilmelidir

Veritabanı İçin Adanmış Sunucu

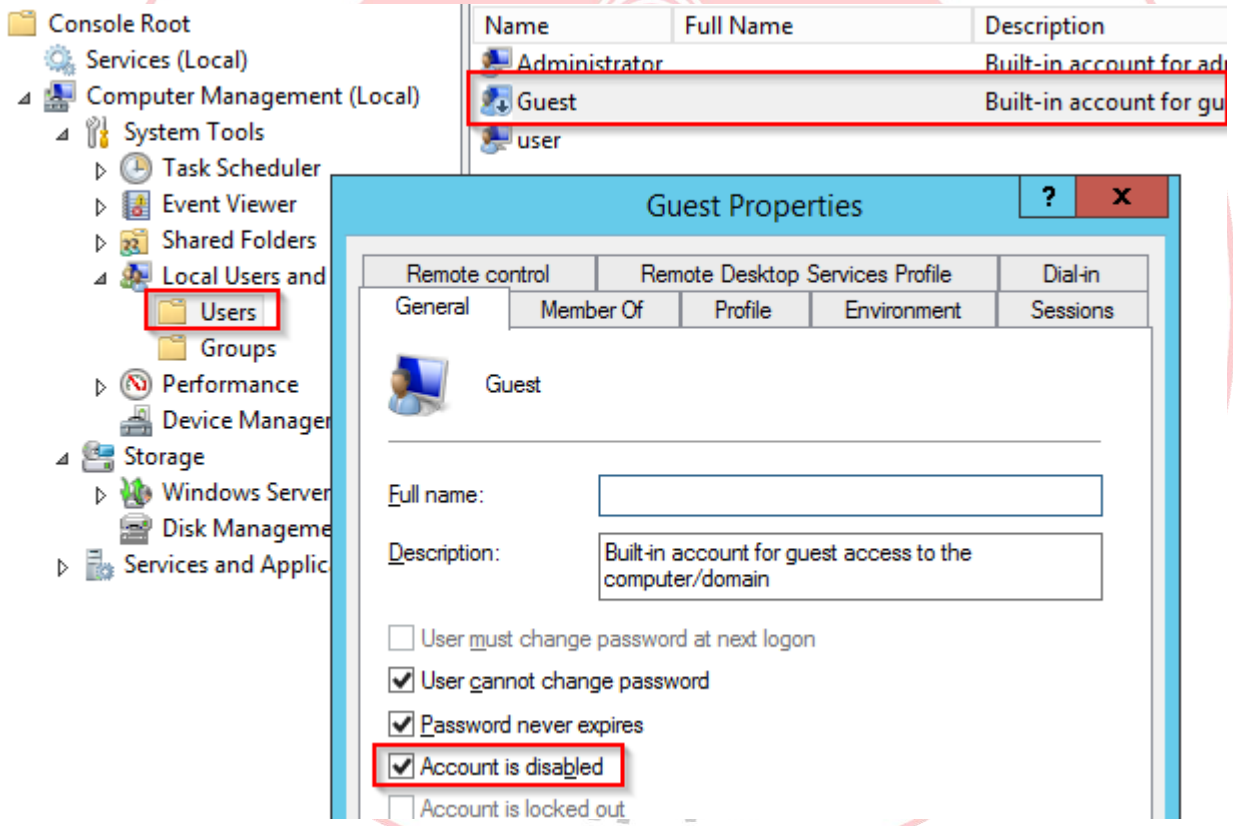
- SQL Server, üzerinde başka servislerin çalışmadığı bir sunucu üzerine kurulmalıdır.
  - Web servisleri
  - Mail servisleri kurulmamalı
- Diğer servislerdeki açıklıklar SQL Server sunucusunda güvenlik açıklıklarına neden olabilir
- Anti virüs yüklü ise data/log dosyaları tarama dışı bırakılmalı

İşletim Sistemi Güvenlik Ayarları

- SQL Server 2012'in üzerinde çalıştığı Windows İşletim sisteminin kritik güvenlik ayarları yapılmalıdır
- Bu yapılandırmalar için aşağıdaki kaynaklardan faydalanılabilir.
  - www.bilgiguvenligi.gov.tr
  - www.cis.security.com
  - www.sans.org/reading-room/

Windows Kullanıcı Hesapları

- Windows sistem üzerinde Guest hesaplarının kapatılması gerekmektedir.



Windows Servisleri

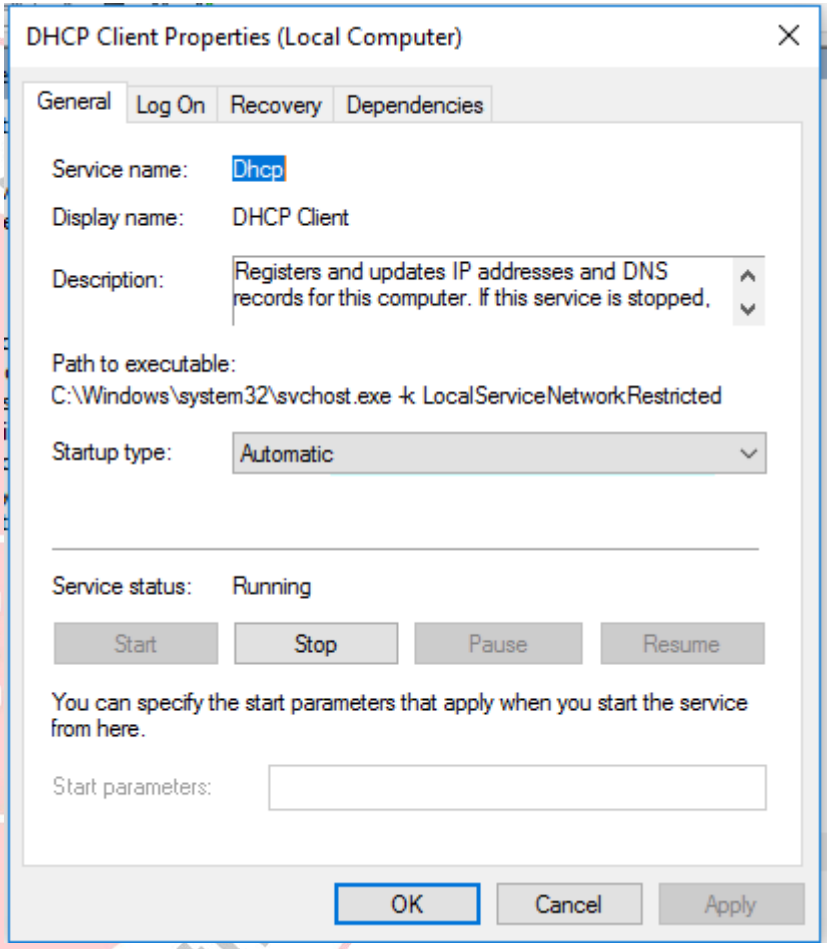
- SQL Server sunucusu üzerinde kullanılmayan servisler kapatılmalıdır
- Kapatılırken uygulamaların ihtiyaçları gözetilmelidir
- Alternatif yaklaşım hangi servislerin açık kalacağını belirlemektir

Kapatılacak Windows Servisleri

Windows Servisleri	
Alerter	Network DDE
Clipbook Server	Network DDE DSDM
Computer Browser	Print Spooler
DHCP Client	Remote Access Connection Manager
Distributed File System	Remote Registery
Distributed Transaction Coordinator	Removable Storage
Fax Service	RunAs Service
Internet Connection Sharing	Smart Card
IPSec policy agent	Smart Card Helper
License Logging	Task Scheduler
Logical Disk Maneger Administrative Service	Telephony
Windows Messenger	Telnet
Netmeeting Remote Desktop Sharing	Windows Installer

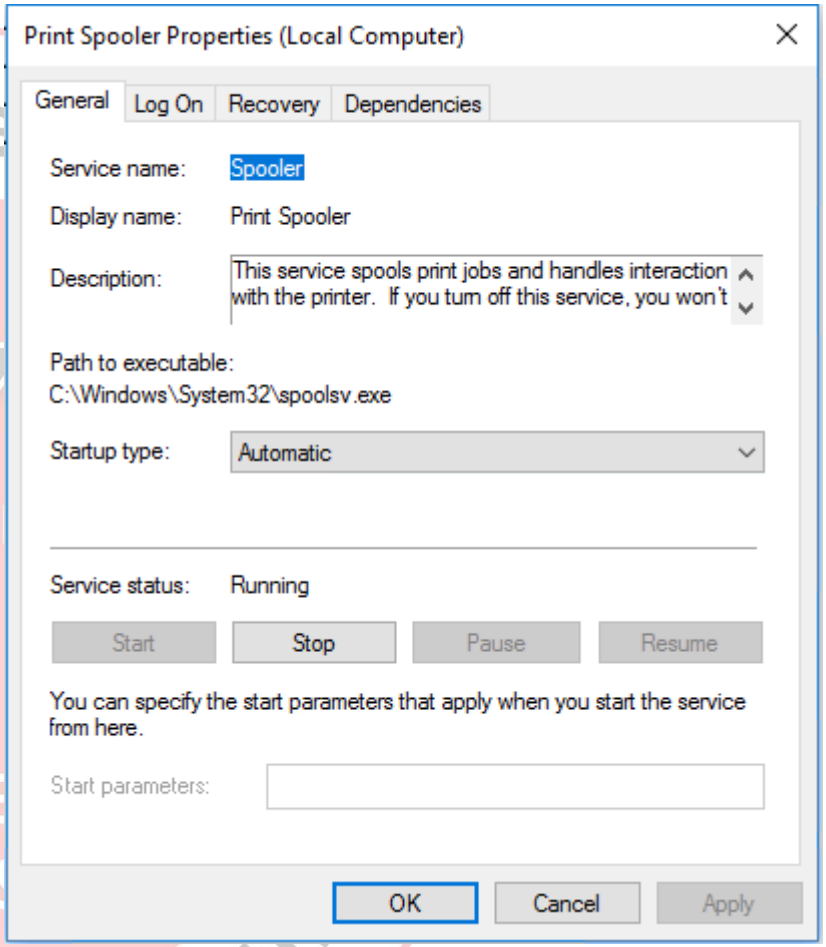
DHCP Client Servisi

- TCP / IP özelliklerinde «otomatik IP adresi al» seçilirse, bilgisayar DHCP istemcisi haline gelir.
- İstemci bilgisayar DHCP kullanacak şekilde ayarlandığında katıldığı ağ için geçerli olduğu bilinen bir IP adresi alır.



Print Spooler Servisi

- **Print Spooler**, her bilgisayarda yazdırma işlemi için çalışan bir hizmettir.



Windows Servisleri

- Remote Registry,
  - Uzak kullanıcıların gerekli izinlere sahip olması koşuluyla, bilgisayarınızdaki kayıt defteri ayarlarını değiştirmesini sağlar.
- Task Scheduler,
  - SQL Server Agent veya işletim sistemi üzerinde zamanlanmış görevler yoksa kapatılabilir

Windows Servisleri Listeleme

```
PS C:\Users\oracle> Get-Service | Where-Object { $_.Status -eq "Running" }

Status   Name               DisplayName
------   ----               -----------
Running  AeLookupSvc        Application Experience
Running  Appinfo            Application Information
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  AudioSrv           Windows Audio
Running  BFE                Base Filtering Engine
Running  BITS               Background Intelligent Transfer Ser...
Running  CertPropSvc        Certificate Propagation
Running  CryptSvc           Cryptographic Services
Running  CscService         Offline Files
Running  DcomLaunch         DCOM Server Process Launcher
Running  Dhcp               DHCP Client
Running  Dnscache           DNS Client
Running  DPS                Diagnostic Policy Service
Running  eventlog           Windows Event Log
Running  EventSystem        COM+ Event System
Running  FontCache          Windows Font Cache Service
Running  gpsvc              Group Policy Client
Running  hidserv            Human Interface Device Access
Running  Intel(R) PROSet... Intel(R) PROSet Monitoring Service
Running  iphlpsvc           IP Helper
Running  LanmanServer       Server
Running  LanmanWorkstation  Workstation
Running  lmhosts            TCP/IP NetBIOS Helper
Running  MMCSS              Multimedia Class Scheduler
Running  MpsSvc             Windows Firewall
Running  Netman             Network Connections
Running  netprofm           Network List Service
Running  NlaSvc             Network Location Awareness
Running  nsi                Network Store Interface Service
Running  PcaSvc             Program Compatibility Assistant Ser...
Running  PlugPlay           Plug and Play
Running  Power              Power
Running  ProfSvc            User Profile Service
```

Servis Hesablarının Seçimi ve Yönetilmesi

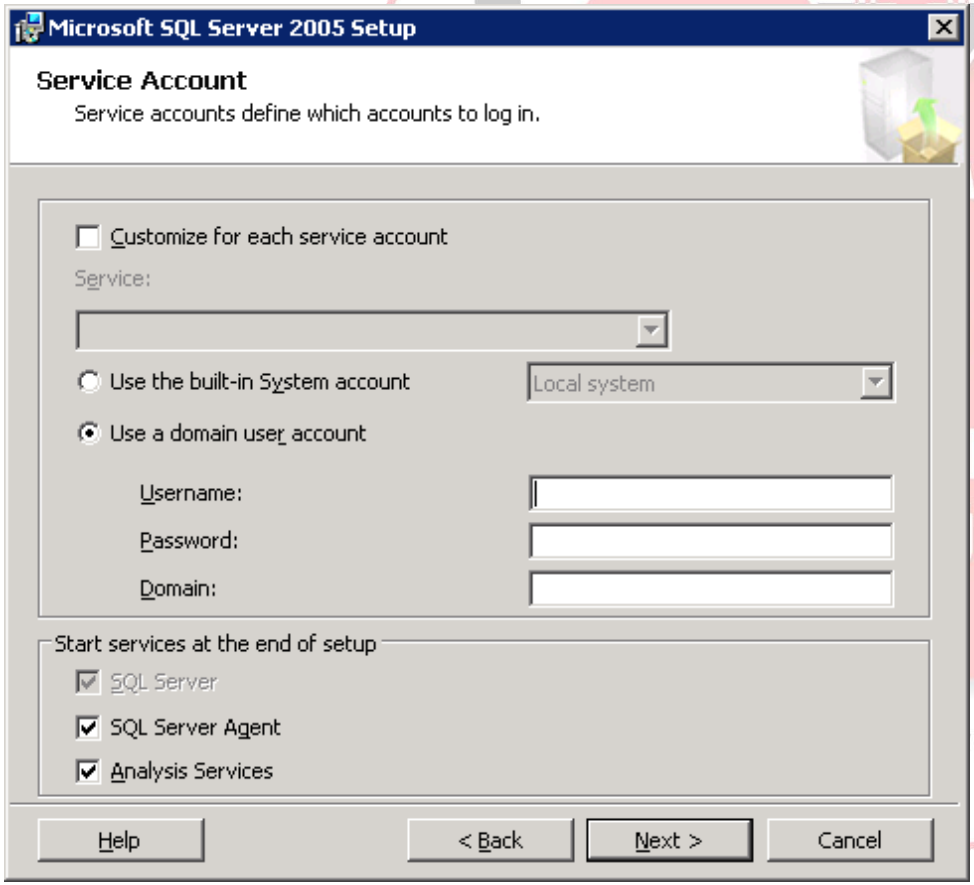
- SQL Server 2012, bir Windows servisi şeklinde çalışmaktadır.
- Kurulum sırasında / sonrasında:
  - Tüm servisler aynı servis hesabını kullanabilir
  - Veya Her bir servis kendi servis hesabını kullanacak şekilde yapılandırılabilir
- Servis hesapları izole edilmelidir; her bir servisin servis hesabı farklı olmalı

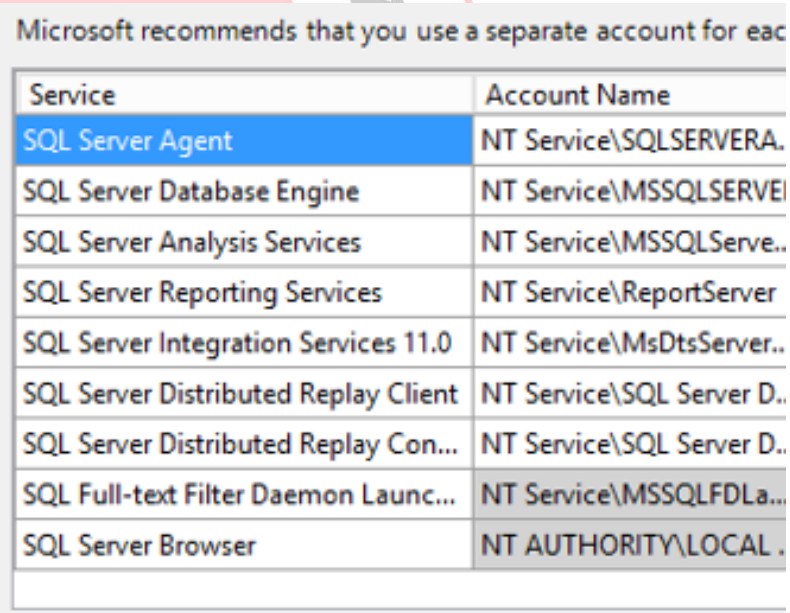
- Hesaplar SQL Server Configuration Manager ile yönetilebilir
- https://msdn.microsoft.com/en-us/library/ms144228.aspx

Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server Integration Services 11.0	Running	Automatic	NT Service\MsDtsServer110	1056	
SQL Full-text Filter Daemon Launcher (MSSQLSERVER)	Running	Manual	NT Service\MSSQLFDLauncher	2400	
SQL Server (MSSQLSERVER)	Running	Automatic	NT Service\MSSQLSERVER	1448	SQL Server
SQL Server Analysis Services (MSSQLSERVER)	Running	Automatic	NT Service\MSSQLServerOLAPService	1508	Analysis Server
SQL Server Reporting Services (MSSQLSERVER)	Running	Automatic	NT Service\ReportServer	1592	Report Server
SQL Server Browser	Stopped	Other (Bo...	NT AUTHORITY\LOCALSERVICE	0	
SQL Server Agent (MSSQLSERVER)	Stopped	Manual	NT Service\SQLSERVERAGENT	0	SQL Agent

Servis Hesablarının Seçimi ve Yönetilmesi

- Her bir servis ayrı ayrı yapılandırılabilmektedir
- Built-In sistem hesapları veya domain hesapları kullanılabilir.





Varsayılan Kullanıcı ve Gruplar

- Grupların bazıları, ilgili modüller kurulunca oluşturulur
- Bazı kullanıcılar standart kurulumda gelmeyebilir.

Lokal Kullanıcılar	
1.	Administrator
2.	Guest
3.	HelpAssistant

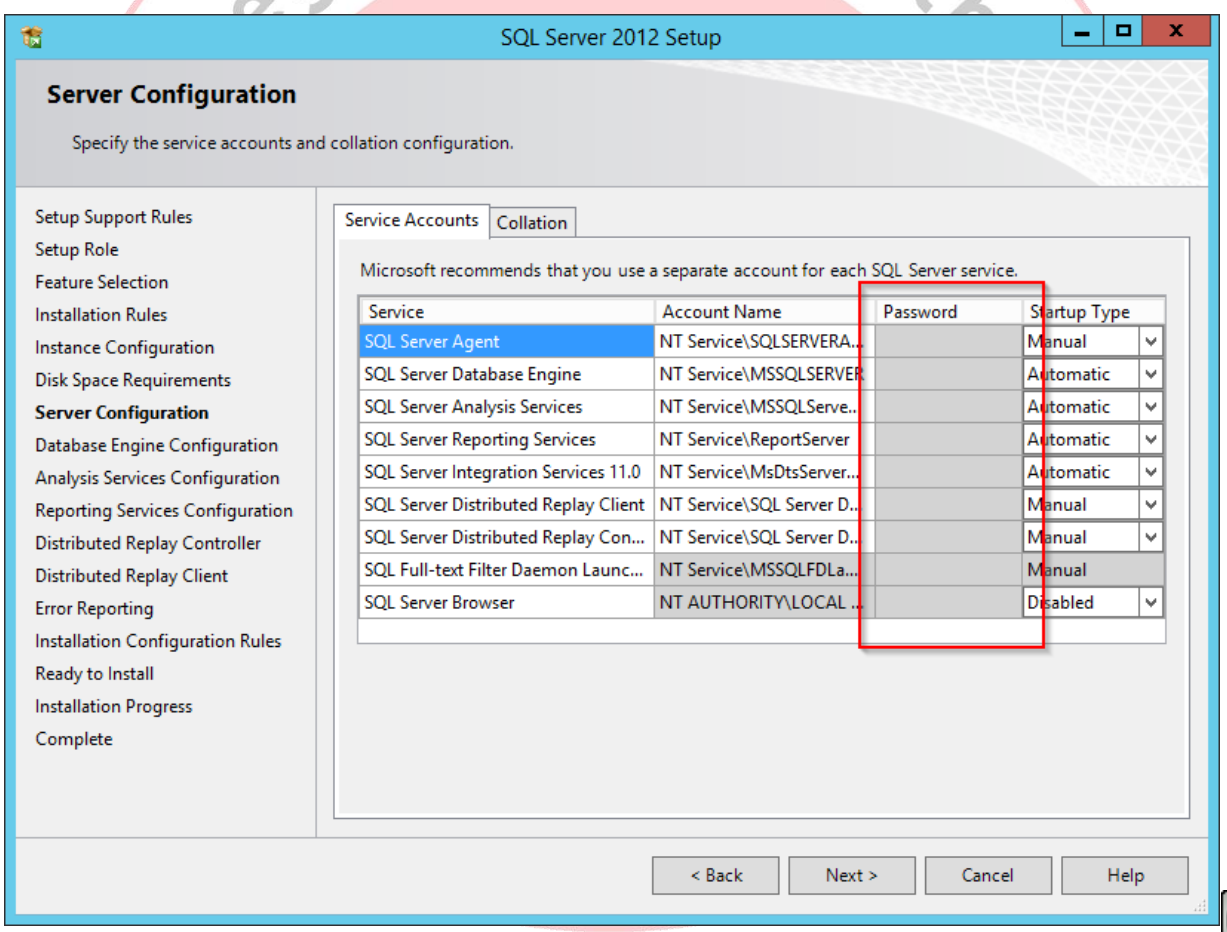
Lokal Gruplar	
Administrators	Performance Log Users
Backup Operators	Power Users
DHCP Administrators	Print Operators
DHCP Users	Remote Desktop Users
Guests	Replicator
HelpServicesGroup	Terminal Server Users
Network Configuration Operators	Users
Performance Monitor Users	WINS Users

MS SQL Servis Hesabı

- Düşük haklara sahip Local veya Domain hesabı kullanılmalı
- SQL Server, uzak işlemlere ihtiyaç duyuyorsa
  - Örnek; Network üzerinden yedekleniyorsa, Domain hesabı kullanılmalı
- Aksi takdirde lokal kullanıcı hesapları kullanılmalı
- Servis hesapları için paylaşılan hesap kullanılmamalı
- Yetkilendirmeler servis hesaplarına değil, hesapların bağlı olduğu gruba verilmeli

MS SQL Servis Hesabı

- SQL Server servis hesabı kurulum sırasında tanımlanır



MS SQL Servis Hesabı Değiştirilmesi

- Kurulum sonrası servis hesabı Windows services.msc veya SQL Server Configuration Manager ile değiştirilebilir.
- Servis hesabı, Windows üzerinden değiştirilmemeli
- Configuration Manager kullanılarak değiştirilmeli. Böylece:
  - Değiştirilen hesaba önceki hesabın yetki ve haklarının aynen yansıtılır
  - Yeni hesabın olması gereken grupta olması garantilenir
  - Servisi çalıştırabilmesi için doğru haklar verilmiş olur

Servis Hesabı Seçimi

Seçilebilecek Olası Hesaplar		
Hesap	Problemi	Tercih
Administrator olmayan domain kullanıcısı		√
Administrator olmayan lokal kullanıcı		√
Network Service hesabı	Paylaşılan hesap	X
Local System hesabı	- Gereksiz yetkiler - Paylaşılan hesap	X
Administrator olan lokal kullanıcı	Gereksiz yetkiler	X
Administrator olan domain kullanıcısı	Gereksiz yetkiler	X

Servis Hesabı Seçimi

- Etki alanındaki SQL Server
  - Domain kaynaklarına erişmesi gerekiyorsa,
  - Sql Server çalışan diğer makinelere linked server bağlantısı yapması gerekecekse bir domain hesabı tercih edilebilir
- Etki alanında olmayan SQL Server (Örneğin:DMZ'de ise)
  - Domain kaynaklarına erişim ihtiyacı yoksa Administrator olmayan bir lokal kullanıcı tercih edilir
  - SQL Server, kurulumda her bir SQL Server servisi için bir Windows grubu oluşturur.
    - Ve her bir servis hesabı uygun gruba koyulur.

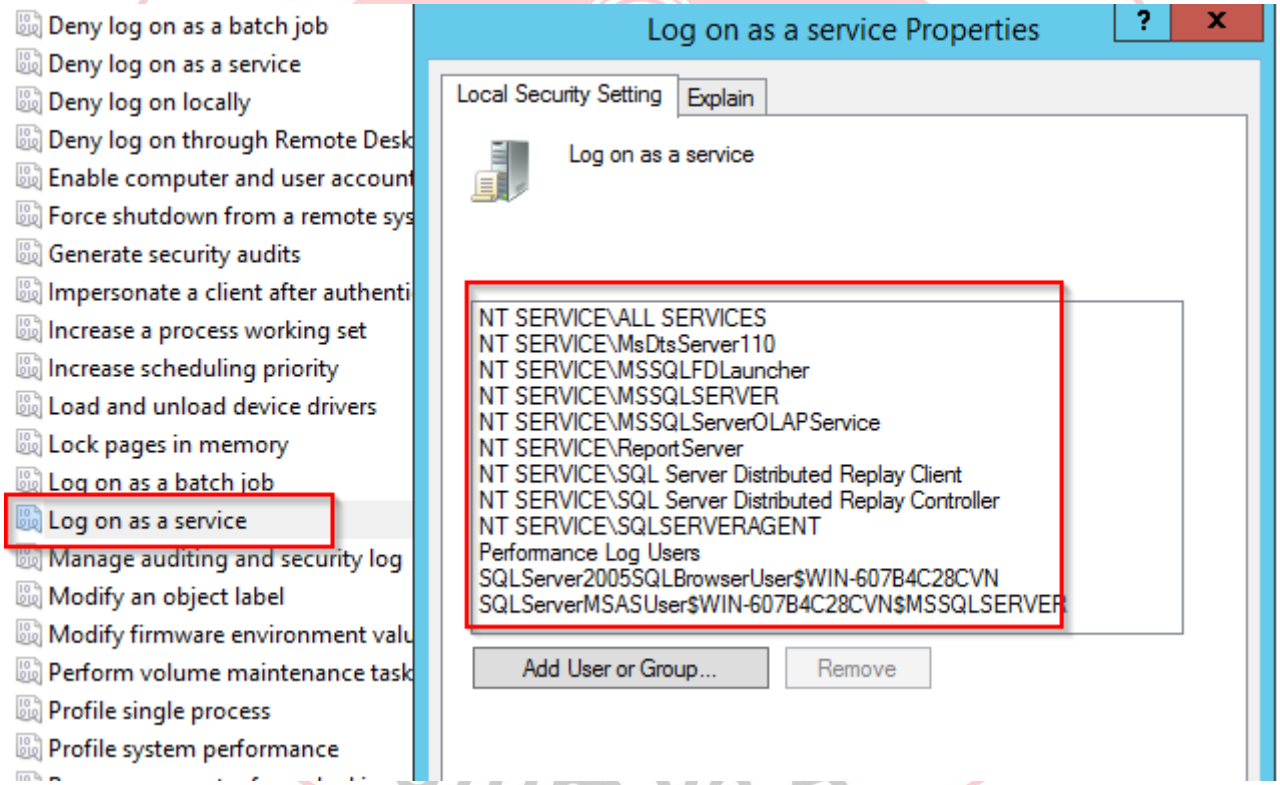
SQL Server Servis Hesabı Hakları

Configure Windows Service Accounts and Permissions
https://msdn.microsoft.com/en-us/library/ms143504.aspx

Servis Hesabına Verilmesi Gereken Hak	Açıklama
Log on as a service	Servis olarak logon olma
Act as the part of the operating system	İşletim sisteminin parçası olarak çalışabilme
Log on as a batch job	Batch işlemi içinde veya job içinde login olabilme. İnteraktif olmayan kullanıcı modu
Replace a process-level token	"CreateProcessAsUser()" API'ni çağırarak başka bir servisi başlatabilme
Bypass traverse checking	Kullanıcının yetkisi olmasa bile bir directory ağacında ileri geriye hareket edebilmesi
Adjust memory quotas for a process	Prosesler için bellek kotası uygulanması
Permission to start SQL Server Active Directory Helper	SQL Server Active Directory Helper'ı başlatabilme
Permission to start SQL Writer	SQL Writer'ı başlatabilme

SQL Server Servis Hesabı Hakları

- Servis hesabına “Local Security Settings” den haklar verilebilir.



SQL Server Servis Hesabı Hakları

- Servis hesabına açıkça "Log on locally" hakkı deny edilmeli
  - Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment
  - Determine which users can log on at the computer.
- Servis hesabının log on olmasına ihtiyaç yoktur
- Böylece veritabanı sunucusuna erişim elde etmek için yapılacak olan kaba-kuvvet saldırıları önlenmiş olur

SQL Server Servis Hesabı Hakları

- Eğer servis hesabı bir domain hesabı ise, bu hesabın sadece veritabanı sunucusu üzerinde "Log on To" Windows hakkı olacak şekilde ayarlanmalı
- Böylece bu servis hesabı ile herhangi bir domain bilgisayarında oturum açması önlenmiş olur.

SQLServer Agent Servis Hesabı

- SQLServerAgent Servis hesabı için, eğer;
  - Replikasyon varsa
  - DTS kullanılıyorsa(DTS'in yeni versiyonu SSIS)
  - Serverlar arası bağlantıya ihtiyaç duyuyorsa
  - Domain hesabı olması gerekir
- Bu hesaba düşük yetkiler verilmeli
- SQL Server Agent servisi, Windows Administrator grubuna üye olan bir hesap altında çalıştırılmamalıdır

SQL Server Agent Servis Hesabı Hakları

- SQL Server Agent servis hesap veya hesaplarına aşağıdaki haklar verilmelidir:
- Bu haklar varsayılanda ilgili servis hesabına verilmektedir.

Servis Hesabına Verilmesi Gereken Hak	Açıklama
Log on as a service	Servis olarak logon olma
Act as the part of the operating system	İşletim sisteminin parçası olarak çalışabilme
Log on as a batch job	Batch işlemi içinde veya job içinde login olabilme. İnteraktif olmayan kullanıcı modu
Replace a process-level token	"CreateProcessAsUser()" API'ni çağırarark başka bir servisi başlatabilme
Bypass traverse checking	Kullanıcının yetkisi olmasa bile bir directory ağacında ileri geriye hareket edebilmesi
Adjust memory quotas for a process	Prosesler için bellek kotası uygulanması