SQL Server Sikkerhed

(Mikael Veistrup-Vetlov)

Contents

[Sikring af Microsoft SQL Server 3](#_Toc88050433)

[Platform og netværkssikkerhed 3](#_Toc88050434)

[Fysisk sikkerhed 3](#_Toc88050435)

[Sikkerhedskopiering 3](#_Toc88050436)

[Operativsystems sikkerhed 3](#_Toc88050437)

[Kun MS SQL Server på en MS SQL Server 3](#_Toc88050438)

[Kryptering og certifikater 3](#_Toc88050439)

[Auditlogning af Data opslag 3](#_Toc88050440)

[Sikkerhed på SQL Serveren 4](#_Toc88050441)

[Brugere og Database sikkerhed 4](#_Toc88050442)

[SQL DBA 4](#_Toc88050443)

[Database Ejere 4](#_Toc88050444)

[Udviklere 4](#_Toc88050445)

[Brugere 4](#_Toc88050446)

[Servicekonti 4](#_Toc88050447)

[Systemfakta 5](#_Toc88050448)

[Fremover vil vi konsolidere MSSQL databaser på fælles SQL Hoteller. 5](#_Toc88050449)

[Fordele ved SQL Server Hotel 5](#_Toc88050450)

[Alternativt kan der oprettes en dedikeret SQL Server til et enkelt System. 5](#_Toc88050451)

[Hvis der er brugere/leverandører der selv har opsat / installeret MSSQL på Server. 6](#_Toc88050452)

[Nedenstående liste er ikke udtømmende men en punktopstilling som man skal være opmærksom på. 6](#_Toc88050453)

[Undtagelser? 6](#_Toc88050454)

[Driftsfakta / Bemærkninger 6](#_Toc88050455)

[Vedligeholdelse Af Database serverne. 7](#_Toc88050456)

[Adgang til databaser 7](#_Toc88050457)

[Udvikling, Test, Preprod, Produktion 8](#_Toc88050458)

[MSSQL Server Versioner. 8](#_Toc88050459)

[Access Databaser. 8](#_Toc88050460)

[Typiske Adgangsproblemer: 9](#_Toc88050461)

[Personhenførbare data. 9](#_Toc88050462)

# Sikring af Microsoft SQL Server

Sikring af SQL Server kan ses som en række trin, der involverer fire områder: platformen, godkendelse, objekter (inklusive data) og applikationer, der har adgang til systemet.

Du kan finde flere oplysninger om SQL Server -sikkerhed på [SQL Server](https://go.microsoft.com/fwlink/?LinkID=31629) -webstedet. Dette inkluderer en guide til bedste praksis og en sikkerhedstjekliste. Dette websted indeholder også de nyeste service pack -oplysninger og downloads.

## Platform og netværkssikkerhed

Platformen til MS SQL Server omfatter den fysiske hardware og netværkssystemer, der forbinder klienter med databaseservere og de binære filer, der bruges til at behandle databaseanmodninger.

### Fysisk sikkerhed

Bedste praksis for fysisk sikkerhed begrænser strengt adgangen til de fysiske server- og hardwarekomponenter.

Alle servere i SDS er i Låste rum med begrænset adgang til (database-) server hardware og netværksenheder.

Der er opsat Firewalls på nettet, og de enkelte servere, der begrænser brugeres adgang til system, netværksressourcer & Data.

Logisk set er en firewall en adskiller eller begrænser af netværkstrafik, som kan konfigureres til at håndhæve SDS datasikkerhedspolitik. Herved øger vi sikkerheden på operativsystemniveau ved at begrænse hvem der kan få adgang til hvad, samt hvorfra de kan tilgå hvilken type data.

Uautoriserede brugere har ikke adgang til netværket.

### Sikkerhedskopiering

Backup foretages krypteret af Externt firma med externe medier.

Restore køres på opfordring efter aftale med Systemansvarlige via Servicenow godkendte sager.

### Operativsystems sikkerhed

Operativsystemerne opgraderes til Nyeste (eller nyeste -1) version, og alle Sikkerhedspakker installeres løbende, efter test, dog evt. begrænset af individuelle krav fra applikationerne om lavere versioner.

Adgang til Servere, SQL Instanser og DataBaser styres af Ad-Sikkerhedsgrupper

### Kun MS SQL Server på en MS SQL Server

Reduktion af grænsefladen er en sikkerhedsforanstaltning, der involverer stop eller deaktivering af ubrugte komponenter. Herved forbedrer vi sikkerheden ved at give færre muligheder for potentielle angreb på et system. Nøglen til at begrænse overfladearealet til SQL Server omfatter kørsel af nødvendige tjenester, der er begrænset til "mindst privilegium" ved kun at give tjenester og brugere de relevante rettigheder.

MS SQL Server bruger operativsystemfiler til drift og datalagring. Bedste fremgangsmåder til filsikkerhed kræver, at vi begrænser adgangen til disse filer til kun MS SQL Serveren!

Vi har IKKE placeret MS SQL Data og Log filer efter Microsoft default, og hvis nogen stjæler en fysisk server følger data & log ikke med, da de er placeret på ekstern Storage.

### Kryptering og certifikater

Kryptering løser ikke adgangskontrolproblemer. Det øger imidlertid sikkerheden ved at begrænse datatab, forbedre adgangskontroller og sikre kommunikationen

### Auditlogning af Data opslag

Da vi har Dataindsamling med personfølsomme data, skal dette altid registreres, og der er opsat Audit-logning, der logger alle relevante aktiviteter, og kan checkes for ulovlige søgninger, via et Syslog projekt, hvor data befinder sig hos ekstern leverandør.

# Sikkerhed på SQL Serveren

## Brugere og Database sikkerhed

Brugere af Databasen omfatter:

### SQL DBA

* Ios Personale der administrerer Servere, Instanser og Databaser.
* De kan installere en Database Server, Instanser, Databaser,
* sikrer at der er opsat Backup af databaserne
* sikrer opdateringer
* giver AD-Grupper privilegier på databaser,
* administrerer SQL Agent jobs.

### Database Ejere

* Systemansvarlige i forretningen der kan administrere den enkelte database
* Kan starte / stoppe, slette databasen
* Kan give avancerede privilegier til database brugere/grupper

### Udviklere

* bruger der kan ændre på opsætningen,
* layout og programmere af de enkelte tabeller og schemaer i databasen

### Brugere

* Slutbrugere der kan læse og/eller skrive data i de opsatte databaser.
* Der kan specificeres yderligere opdeling, så brugere kun har privilegier på dele af data i databasen

### Servicekonti

* Virtuelle anonyme brugere der giver applikationer adgang til data
* Kan være en Web-side, en applikation eller et batch job.
* Må IKKE være en specifik person, og man må ikke logge på databasen for at tilgå data interaktivt.

# Systemfakta

## Fremover vil vi konsolidere MSSQL databaser på fælles SQL Hoteller.

1. Der kan IKKE gives bruger adgang til en SQL Server / Hotel, KUN privilegier på data i databaser!
2. Opsætning af Server, Instans og Databaser foretages af IOS MSSQL afdelingen
3. Adgang til databaser styres via foruddefinerede AD gruppe-par (Global brugergrupper & Lokale Ressourcegrupper) der klargøres af IOS MSSQL afdelingen.
4. Der skal registreres & godkendes Undtagelseserklæring hvis der skal ske adgang udover via AD-grupper.
5. Opsætning & indhold af DataBaser styres og vedligeholdes af Systemejer via foruddefinerede AD grupper.
6. Adgang til data styres af systemernes Dataansvarlige primært for læse & læse/skrive data privilegier.
7. Der må ikke ligge bruger data uden for SQL på denne server, Data skal flyttes til Applikations server eller dedikerede Fil servere
8. Der må ikke startes jobs uden for SQL, og kun godkendte agentjobs, der scheduleres inden for SQL.
9. Der køres hver aften IOS godkendte maintenance jobs, der checker integritet & opdaterer indexes.
10. På et MS SQL Server Hotel, må brugere og udviklere/leverandører IKKE have fjernskrivebords adgang, så databaseadgang kan foretages fra egen udviklings pc, via en Jump host, App. server, eller lignende med f.eks. MS SQL Server Management Studio
11. Kort fortalt indeholder et database hotel flere databaser, og nogle af dem under persondataloven. Vi kan derfor ikke sænke sikkerhedsniveauet bare for en enkelt bruger i et lille øjeblik
12. Hvis installationsprogrammet er en black-box, kan vi ikke sige hvilken ændringer det udfører, så det MÅ ikke køres! Hvis det ikke er en black-box så kan vi se hvilke ændringer der sker og kan derfor udføre dem pr script.
13. På Produktions SQL Hotel må der ikke udvikles, og ikke tildeles rettigheder til administration. Der kan gives temporære privilegier til fejlsøgning
14. Ændringer til Produktion foretages via changes, efter test på test servere & udvikling på udviklings servere.

## Fordele ved SQL Server Hotel

Vi giver IKKE midlertidige SA rettigheder på et SQL Hotel, og det tror vi heller ikke ret mange professionelle SQL afdelinger vil gøre!

Databaserne på et SQL Hotel har

* bruger privilegier tilknyttede via AD grupper, så dataejere styrer hvem der må hvad
* beskyttelse mod adgange til andres databaser
* sikring af data via ugentlig full backup og transaktionslog backup hver time.
* automatiske Maintenance scripts, fra Markedets førende: Ole Hallengreen
* sikring mod spidsbelastning, ved at vi tidsmæssigt styrer hvornår jobs kører,
* auditering osv.

Vi står inde for ovenstående overfor Rigsrevisionen, og kan derfor ikke tillade ”cowboys” uden for vores kontrol får ”gude privilegier”

## Alternativt kan der oprettes en dedikeret SQL Server til et enkelt System.

1. Opsætning af Server, Instans og Databaser foretages af IOS MSSQL afdelingen.
2. Licenser betales af SystemForvalter
3. Adgang til databaser styres via foruddefinerede AD gruppe-par (Global brugergrupper & Lokale Ressourcegrupper) der klargøres af IOS MSSQL afdelingen.
4. Opsætning & indhold af DataBaser styres og vedligeholdes af Systemejer via foruddefinerede AD grupper.
5. Adgang til data styres af systemernes Dataansvarlige primært for læse & læse/skrive data privilegier.
6. Der køres hver aften IOS godkendte maintenance jobs, der checker integritet & opdaterer indexes.
7. Databaseadgang kan foretages fra egen udviklings pc, via en Jump host eller lignende med MS SQLServer Management Studio
8. Systemejer skal sørge for logning og Audirtering via godkendte procedurer.

## Hvis der er brugere/leverandører der selv har opsat / installeret MSSQL på Server.

Ved installation af SQL-servere/express på servere med eller uden IOS's viden skal projektet være opmærksom på at der påligger et krav / ansvar for Backup, Sikkerhed og Opdateringer, der ellers oftest vil være håndteret af den almindelige forretningsgang i IOS.  
Vi gør derfor opmærksom på at IOS er leveringsdygtige i udvikling og test servere, til brug inden produktions fasen, som vil dække langt de fleste behov.  
  
Såfremt at man stadig vælger at benytte egen installation af SQL fraskriver man sig blandt andet mulighed: målepunkter/overvågninger, skalering og høj tilgængelighed samt eventuelt hjælp fra IOS og den ekspertise som IOS råder over, inden for drift.

Det er vigtigt at understrege at en egen installation ikke er undtaget de regler som gælder for Sundhedsdatastyrelsen.

### Nedenstående liste er ikke udtømmende men en punktopstilling som man skal være opmærksom på.

1. SQLExpress versioner må IKKE benyttes i Produktion.
2. Systemforvalter skal sørge for SQL Licenser.
3. Systemejer, skal sikre opsætning og udførsel af Backup & Restore. for at sikre mod pladsproblemer.
4. Systemejer, skal sikre opdatering & patchning af Software.
5. Systemejer, skal sikre Gennemskueligheden af tilgange via AD Brugere og grupper
6. SystemForvalter & Systemejer skal stå for og sikre daglig drift.

Som altid er det systemejers ansvar at installationen overholder gældende lovgivning samt  Sundhedsdatastyrelsens krav på området.

Her under, men ikke kun Logning, GDPR, arkivpligt, revision o.a.

IOS er forpligtiget til foretage audit af de systemer og den kommunikation der residerer i vores netværk, både for licens-, sikkerheds- og data-krav.

Dette sker fra IOS selv eller via samarbejdspartnere.

## Undtagelser?

1. Det er SDS's holdning, at der **ikke** findes nogen haste situationer, som kan berettige tilsidesættelse af grundlæggende sikkerheds forskrifter!
2. Der er **INGEN** Undtagelseserklæring der kan give Lokaladministrator, Sysadm og lignende forhøjede privilegier på et produktions MS SQL hotel
3. Andre undtagelser må tages op med Driftchefen

# Driftsfakta / Bemærkninger

## Vedligeholdelse Af Database serverne.

Vi har analyseret MSSQL Netværket og taget de bedste vedligeholdelses planer med i vores overvejelser.

Vi har automatisk backup af vores databaser via DP for SQL Management ( IBM Spectrum Protect /TSM )der regelmæssigt (hver uge)tager Fuld backup, altereret med mange Transaktions log (T-Log) backup, (prod: hver time, test hver 4 time). Hermed sikrer vi at vi kan genetablere data fra et tidligere tidspunkt.

Derudover har vi allieret med markedets førende maintenance planer Ola Hallengren's scripts ([ola.hallengren.com](https://ola.hallengren.com/)) der sikrer daglig database Integritets check & Index optimisering. Hvormed vi bedst plejer databaserne & Index.

## Adgang til databaser

AL adgang til databaser styres via foruddefinerede AD gruppepar (Global brugergrupper & Lokale Ressourcegrupper) der klargøres af IOS MSSQL afdelingen.

Når der skal oprettes nye Grupper til privilegietildeling skal den ressourceansvarlige (Systemforvalteren) beskrive:

* hvem der er manager for Databasen / Gruppen
* hvem der er befuldmægtiget =  co-manager,
* hvad der skal stå i gruppe noter og beskrivelsen,
* ALLE ressourcerne der gives privilegier til.
* hvem (inkl. domæne) der får privilegier via denne gruppe Seperate Service desk sager.

En co-Manager er en der på den ressource ansvarliges (data-ejers) vegne kan / må styre brugeres adgang til grupperne og ultimativt privilegier på data. Det er co-Managers pligt at holde Manager & den Ressourceansvarlige orienteret om adgange til databasen.

Ligesom Manager, er co-Manager ansvarlig for hvem der må tilgå de pågældende data

Noter og beskrivelse skal angive systemnavn, og klart beskrive hvad medlemsskab af gruppen medfører, hvilke servere, instanser, databaser, rettigheder & privilegier (læs, skriv, udv, dbo mm.), status (Test, Prod, uDvikl.). Hvis gruppen efterfølgende får adgang til mere, skal dette godkendes af gruppe ejer & ressource ansvarlig og noteres på gruppen i AD

Når en bruger vil ansøge om adgang til en database, skal der ansøges via [Forside - Serviceportal (service-now.com)](https://sds.service-now.com/serviceportal?id=frontpage) \ "Anmod om adgang" hvor den dataansvarlige (co)manager skal angive AD-Globalgruppen, samt hvilke brugere der skal meldes ind / ud. Det er IKKE Servicedesk, der er ansvarlig for indhentning af tilladelser.

Hvis der er en eksisterende brugergruppe, der peger på databasen, med de korrekte privilegier, og ansøgningen er godkendt af gruppe ejer / befuldmægtiget, kan servicedesken selv melde bruger ind i gruppen.

Der vil være sammenknyttede Globale: \_g\_ grupper hvor der meldes brugere ind, og Lokale: \_l\_ grupper, hvor der IKKE må være brugere, men som er knyttet til de lokale ressourcer (databaser, folder mm.) med de ønskede privilegier.

Den globale gruppe kan være i andet domæne (hvor brugerne befinder sig) end ressource gruppen. Der kan være flere Globale grupper fra forskellige domæner der er meldt ind i samme ressource gruppe.

Ved oprettelse af ny Database vil MSSQL afdelingen oprette de korrekte Windows AD grupper, på baggrund af ovenstående kriterier, tilknytte Ressource grupperne til sql servere og databaser, melde brugerne ind i \_g\_ gruppen, og melde dette til ressource ejerne.

## Udvikling, Test, Preprod, Produktion

Den optimale metode er at man udvikler et system / applikation mod en udviklings database, indtil dette vurderes fungerende.

Så får man dette kopieret til test, hvor man har test personer (uden udviklings privilegier) til at teste system / applikation mod test data.

Derefter kan man få dette kopieret til Pre-prod, hvor test personer kan teste system / applikation på et udtræk af produktions data.

Til sidst kan man få kopieret system / applikation til Produktion (via Change) hvor der IKKE er nogen der har udvidede privilegier.

At give udviklings privilegier på produktions database kan betragtes som Sikkerhedsbrud.

Øgede privilegier på Produktions versioner bør kun bruges til fejlfinding.

## MSSQL Server Versioner.

Vi har udfaset alle MS SQL server 2008 (og ældre) er ved at gøre det samme med MS SQL Server 2012 & 2014. Vi vedligeholder, MS SQL Server 2016 og MS SQL Server 2019 i produktion.

MS SQL Server 2017 har vi sprunget over / valgt fra.

## Access Databaser.

I MS Access Databaser har du (og kun du) mulighed for at slå op i en lokal database, efter oplysninger gemt der.  
  
Der er så nogle udviklere der kan bruge lidt af Access værktøjet til at lave en "Frontend", dvs en applikation der forbinder til en af vores centrale SQL servere.  
　  
Det betyder at 2 personer SKAL have hver sin access database (frontend) på sin egen maskine, der igen forbinder til en af vores centrale database servere.  
　  
Hvis det er således Jeres Applikation er sat op, er det Jeres udvikler der skal undersøge:  
　  
1) Er I flere, der bruger den samme Access database (det må i Ikke), eller forskellige "frontends", evt. forskellige steder på netværksdrev?

2) Er der brugt forskellige opdaterede Brugerinformationer(konto) (helst med korrekt password) til at forbinde til de centrale databaser, eller er der konflikt, fordi det er samme konto, flere personer bruger?

3) Hvis vi i Ios skal undersøge nærmere, er vi nødt til at vide **hvilke(n) bruger/konto** der forsøger at få adgang til **hvilken Database** på **hvilken MSSQL server(\Instans)**.  
　  
Det er kun Jer og jeres udvikler af Access der kan svare på dette.  
　  
Ios har kun ansvar for drift af DataBase Servere, og vedligeholdelse af dette miljø, men hvis vi kan hjælpe jer med at løse relaterede problemer, vil vi selvfølgelig gøre hvad vi kan.

Vi har i IOS IKKE kompetencer og ansvar for Access udvikling, opsætning og fejlsøgning!

Vi anbefaler til enhver tid at I har en Applikation, der gemmer Data / Informationer på et MS SQL Hotel, Hermed sikres Backup & Maintenance procedurer.

## Typiske Adgangsproblemer:

Den mest sandsynlige fejlårsag er faktisk at brugeren ikke har været logget af efter nyt AD-gruppemedlemsskab.

I Microsoft Windows gives medlemsskab af grupper i forbindelse med logon til domænet, IKKE ved reconnect, så brugeren SKAL være logget af, før de kan komme med i den nye gruppe.

Den næst mest sandsynlige fejlårsag er Access.

Access er en enkeltbruger database IKKE-Multiuser.

Man kan oprette et Access-frontend til en MS SQL database, hvor man behandler Databaseopgaverne i access, der forbinder til MSSQL og henter / gemmer data.

Dette kan kun lade sig gøre hvis hver enkelt bruger har sin egen lokale (IKKE delte) access database, og korrekt opsat ODBC forbindelse til MSSQL Serveren.

Selvom alt dette er sat korrekt op, kan Access stadig låse en bruger, så den ikke kan forbinde, og der er en speciel metode til at låse denne op. (kendes ikke i MSSQL)

Hvis der er forkert version af ODBC eller Access kan dette også give problemer.

Hvis der er synkroniserings problemer mellem passwords i dksund og andet domæne kan dette også give problemer.

## Personhenførbare data.

Da vi har Dataindsamling med personfølsomme data, skal dette altid registreres, og der skal Audit-logges, via et Syslog projekt. Vi skal desuden kunne anonymisere eller Pseudonymisere data.

Alternativt kan udviklerne maskere personhenførbare data i MSSQL, så kun udvalgte brugere må se hele værdien.