SQL Teknikker Håndbog

(Mikael Veistrup-Vetlov)

Indhold

[System Oversigt 7](#_Toc89350116)

[AD Domæner og DMZ 7](#_Toc89350117)

[Dokumentation 8](#_Toc89350118)

[Datalagring: 8](#_Toc89350119)

[Linux / Windows 8](#_Toc89350120)

[Virtualisering. 8](#_Toc89350121)

[Overvågning. 8](#_Toc89350122)

[Personhenførbare data. 8](#_Toc89350123)

[MSSQL Servere. 8](#_Toc89350124)

[SQL Server Collection og Rapporter 8](#_Toc89350125)

[Firefox Konfiguration Autologon mtime 9](#_Toc89350126)

[ToDo Liste: 10](#_Toc89350127)

[Planlagte nye SQL Servere 10](#_Toc89350128)

[SQL Servere der skal analyseres og Nedlukkes 10](#_Toc89350129)

[Changes til kommende Servicevindue (Prefiks Servicevindue -) 10](#_Toc89350130)

[Udført 10](#_Toc89350131)

[Andet: 10](#_Toc89350132)

[Fremtidig Ad Struktur: 11](#_Toc89350133)

[Ou oversigt: 11](#_Toc89350134)

[Planlægning af Ny SQL Server 12](#_Toc89350135)

[Fremover vil vi konsolidere MSSQL databaser på fælles SQL Hoteller. 12](#_Toc89350136)

[Alternativt kan der oprettes en dedikeret SQL Server til et enkelt System. 12](#_Toc89350137)

[Adgang til databaser 12](#_Toc89350138)

[Planlægning af ny SQL Database 13](#_Toc89350139)

[Krav: 13](#_Toc89350140)

[Installation: 14](#_Toc89350141)

[Adgang til databaser. 14](#_Toc89350142)

[Service konti findes i 3 typer: 14](#_Toc89350143)

[Nedlægning af SQL Server 15](#_Toc89350144)

[Stop Backup af SQL Server 15](#_Toc89350145)

[Opret Change I ServiceNow, Server Nedlagt 15](#_Toc89350146)

[Gem evt. Databaser på Data Gravpladsen 16](#_Toc89350147)

[Afinstaller SQL fra Server 16](#_Toc89350148)

[Marker server I ServiceNow, som Nedlagt 16](#_Toc89350149)

[Marker server I Check\_MK, som Nedlagt 16](#_Toc89350150)

[Marker server I Systemkataloget, som Nedlagt 16](#_Toc89350151)

[Marker server I SQL Collect, som Nedlagt 16](#_Toc89350152)

[Marker server I AD, som Nedlagt 16](#_Toc89350153)

[Marker server I Logpoint, som Nedlagt 16](#_Toc89350154)

[Marker server I s-logdb01-p, som Nedlagt 16](#_Toc89350155)

[Odbc forbindelse til SQL Server. 17](#_Toc89350156)

[Powershell I MSSQL, Server, Arbejdsplads. 20](#_Toc89350157)

[Maintenance scripts 20](#_Toc89350158)

[Anbefalinger: 20](#_Toc89350159)

[Kontrol af fragmentering: Page\_count & frag i % 20](#_Toc89350160)

[Check om der er kommet en ny version. 21](#_Toc89350161)

[Installation af Maintenance plan på server 22](#_Toc89350162)

[SQL LOG dir 23](#_Toc89350163)

[Batch/Transaktions Service Konti 24](#_Toc89350164)

[Logon as Batch, logon as Service 26](#_Toc89350165)

[Change Security Policy SecPol 26](#_Toc89350166)

[Lokal Service Konti 26](#_Toc89350167)

[Klargør job via Task Scheduler (bør IKKE bruges, brug SQL Agent job) 27](#_Toc89350168)

[Active Directory and Kerberos SPNs Made Easy! 28](#_Toc89350169)

[Server-ServiceAccounts: 29](#_Toc89350170)

[ServicePrincipalName (SPN) (SETSPN) 29](#_Toc89350171)

[Årsag: Kerberos Authentificering 29](#_Toc89350172)

[Server-ServiceAccounts og opstart: 31](#_Toc89350173)

[SetSPN (Service Principal Name) 31](#_Toc89350174)

[MS GroupManaged ServiceAccounts: 31](#_Toc89350175)

[TCP-IP Opsætning MSSQL Server 34](#_Toc89350176)

[Auditing / Logning på MSSQL Server til Logpoint 36](#_Toc89350177)

[Opsætning af Audit på MSSQL Instans. 36](#_Toc89350178)

[Oprettelse af Audit Logfile 37](#_Toc89350179)

[Konverteringsjob fra audit format til csv format. 38](#_Toc89350180)

[Forbered Automatisk kørsel. 38](#_Toc89350181)

[Konverteringsjob via Task Scheduler (Skal IKKE bruges) 40](#_Toc89350182)

[Logpoint opsætning: 41](#_Toc89350183)

[Regler 42](#_Toc89350184)

[Registerregistrering 42](#_Toc89350185)

[Systemregistrering 42](#_Toc89350186)

[Systemer og Brugere: 43](#_Toc89350187)

[AD: 43](#_Toc89350188)

[SAP: (bestilling af ressourcer) 43](#_Toc89350189)

[Nilex (til sagsstyring): 43](#_Toc89350190)

[Check\_MK (Server / system monitorering): 43](#_Toc89350191)

[Exchange / Outlook / Skype: 43](#_Toc89350192)

[HP / IMC: http://imc.ssi.ad:8080 43](#_Toc89350193)

[VmWare: 43](#_Toc89350194)

[Citrix: 43](#_Toc89350195)

[Siemz: 43](#_Toc89350196)

[SecretServer: https://secretserver.dksund.dk/Login.aspx 43](#_Toc89350197)

[Sas Analyse: 43](#_Toc89350198)

[System Opsætning 44](#_Toc89350199)

[Service Vinduer 44](#_Toc89350200)

[Service Vindue tids registrering 44](#_Toc89350201)

[Tilføj printere og scannere 45](#_Toc89350202)

[Printer Spool problemer 45](#_Toc89350203)

[Fil lokationer: 45](#_Toc89350204)

[Bestilling af Ekstern Konsulent id / oprettelse af Bruger 46](#_Toc89350205)

[Krævede oplysninger: 46](#_Toc89350206)

[Procedure: 46](#_Toc89350207)

[Ekstern Bruger login via Citrix 49](#_Toc89350208)

[MSSQL Server Opsætning 49](#_Toc89350209)

[Lokal Brugere 49](#_Toc89350210)

[Administrators group 49](#_Toc89350211)

[Instance Logins 49](#_Toc89350212)

[Mail opsætning på SQL Server 49](#_Toc89350213)

[SQL Principals 49](#_Toc89350214)

[SQL Server-level principals 50](#_Toc89350215)

[sa Login 50](#_Toc89350216)

[public Server Role and Database Role 50](#_Toc89350217)

[INFORMATION\_SCHEMA and sys Users and Schemas 50](#_Toc89350218)

[The guest User 51](#_Toc89350219)

[Login 51](#_Toc89350220)

[Credential 51](#_Toc89350221)

[User 51](#_Toc89350222)

[Brug af Login 51](#_Toc89350223)

[Use of credentials 51](#_Toc89350224)

[Gruppe login & individual DataBase User. 51](#_Toc89350225)

[Analyse af server 52](#_Toc89350226)

[PSTOOLS 52](#_Toc89350227)

[Check\_MK Serverovervågning 53](#_Toc89350228)

[Check\_MK Klient til Server og Registrering I Check\_MK 53](#_Toc89350229)

[Check\_MK Overvågning 54](#_Toc89350230)

[Typiske Alarmer 54](#_Toc89350231)

[SQL Funktioner 56](#_Toc89350232)

[Log Check / Syslog-Analyse 56](#_Toc89350233)

[Adgang til Syslog 56](#_Toc89350234)

[Auditing / Logning på MSSQL Server 59](#_Toc89350235)

[MSSQLer her i SDS: 59](#_Toc89350236)

[Kontaktpersoner: 60](#_Toc89350237)

[Licenser 64](#_Toc89350238)

[Indkøb 64](#_Toc89350239)

[Core Licenser 64](#_Toc89350240)

[Licensierede Produktions servere, MSDN TEST Servere 64](#_Toc89350241)

[Leverandør / Support. 64](#_Toc89350242)

[Oversigt 64](#_Toc89350243)

[Opret Microsoft Support sag: 67](#_Toc89350244)

[Opret SQL Standard Change (forhåndsgodkendt change) 73](#_Toc89350245)

[Servicevindue: 73](#_Toc89350246)

[Opret Nilex RFC (Request For Change) / Normal Change 74](#_Toc89350247)

[Dekomissionering af SQL Server 76](#_Toc89350248)

[Opret Test Server 77](#_Toc89350249)

[Migrering af database til nyere SQL 83](#_Toc89350250)

[Tools / Utilities. 86](#_Toc89350251)

[SHRINK DATABASE / FILE 86](#_Toc89350252)

[Disk plads forbrug check med windirstat 86](#_Toc89350253)

[Powershell scripts. 86](#_Toc89350254)

[AD-GroupUser.ps1 - Gruppe Bruger Action 86](#_Toc89350255)

[AD-Users.ps1 – søgeord 86](#_Toc89350256)

[AD-Groups.ps1 – søgeord 86](#_Toc89350257)

[AD-ChkUser.ps1 – AD-brugerlogon 86](#_Toc89350258)

[disk-size.ps1 – fqServernavn 86](#_Toc89350259)

[Make\_group.ps1 86](#_Toc89350260)

[SQL Server Backup / Restore 88](#_Toc89350261)

[Check af schedulering 88](#_Toc89350262)

[Systemer 89](#_Toc89350263)

[Opsætning af nyt system <Systemnavn> 89](#_Toc89350264)

[Nedlægning af system <Systemnavn> 89](#_Toc89350265)

[MTIME – kommende tidsregistrerings system. 89](#_Toc89350266)

[Anonymiset kopi af XXXX-test/prod databasen, lagt op på TMS's FTP-site. 89](#_Toc89350267)

[Venteinfo: 91](#_Toc89350268)

[MitSygehusvalg (afløseren for Venteinfo) 91](#_Toc89350269)

[SOR - Sundhedsvæsenets Organisationsregister 91](#_Toc89350270)

[Kopier SOR fra imkit 🡪 pubdmz 91](#_Toc89350271)

[SOR database (db2) 91](#_Toc89350272)

[Nulstilling af brugernes password for SOR-EDI & SOREDI-DEMO 92](#_Toc89350273)

[Vejledning: 92](#_Toc89350274)

[BioNumerics Databasesystem 92](#_Toc89350275)

[CRM ( XRM ) Formålet med CRM-systemet (Customer Relationship Management) er at understøtte de forskellige arbejdsområder samt samle og effektivisere de processer der relaterer sig til Sundhedsdatastyrelsens kundekreds. 93](#_Toc89350276)

[Udviklet /administreret af Netcompany 93](#_Toc89350277)

[Spoop 94](#_Toc89350278)

[SPOOP-data er klar for <måned> 20xx efter 26/3/2020 94](#_Toc89350279)

[~~SPOOP-data er klar for <måned> 20xx~~ 95](#_Toc89350280)

[Dsdn 96](#_Toc89350281)

[KOES 96](#_Toc89350282)

[TAS 96](#_Toc89350283)

[MRSA 96](#_Toc89350284)

[Snit5, snit8, snit11 97](#_Toc89350285)

[FSK Forskerservice 98](#_Toc89350286)

[Nilex Spørgeskemaer 98](#_Toc89350287)

# System Oversigt

## AD Domæner og DMZ

Sundhedsdatastyrelsen er oprettet for at hjælpe en samling af styrelser, med at administrere deres systemer og data.

Dette har medføre en del kompromisser med flere sideløbende AD, DMZ, Servere, Databaser og systemer.

Vi prøver at samle systemdokumentationen på SharePoint servere.

Vi har oprettet 2 nye AD, for at samle de tidligere systemer, og få ensartet procedurer, regler og sammenhænge.

DKSUND.DK ( dks 0x)

Dette er vores nye hoveddomæne, hvor vi vil konsolidere brugere og kommende systemer, og få samling.

Vi har vores mail(Exchange) og de skrappeste regler i dette domain.

DKSUNDTEST.DK ( dkt 9x)

Dette er pendanten for test og udvikling, og reglerne er: der må ikke køre test i dksund.dk, og der må ikke være produktion i dksundtest.dk

SSI.AD (ssi 1x)

Dette var samlenetværket før dksund.dk, og var første stadie i samme. Disse 4 netværk er samlet i samme forest, så man kan opsætte og administrere alle 4 domæner fra samme konsol.

SST.DK ( sst 2x)

Dette er oprindeligt domæne for Statens Serum Institut, og en del af forskningen foregår i dette domæne.

På sigt bliver funktioner og systemer porteret til DKSUND, med testversioner i DKSUNDTEST.

SDSP.DK

Det nye udviklingsnetværk SundDataPlatformen (SDP) hostet hos DXC Technology. Hvis der er en der skal have oprettet en Udviklingsdatabase på SDP mssql-serveren: sdsdbscop901: eller håndteret brugere på SDP, skal man vurdere, om det lyder fornuftigt, og sender egen vurdering med, når man sender sagen videre til systemforvalteren for SDPen, nemlig Jacques Holm Villaume Johansen (JHVJ) fra KOS.

På DMZ siden har vi en stribe ad, der ikke er så langt fremme opsætningsmæssigt, som på indersiden.

INTDMZ.DK (dmz 4x)

Er den indadrettede DMZ med interne servere der betjener partneren Pubdmz med bl.a. databaseservere.

Der er ingen Web-applikationer i Intdmz

PUBDMZ.DK (dmz 5x)

Er den udadrettede partner, med webservere, mm, der betjener ”befolkningen”, og i samarbejde med Intdmz henter og afleverer oplysninger.

Pubdmz & Intdmz hænger sammen ved at Webapplikationer i Pubdmz har adgang til MSSQL databaseservere i Intdmz. Der er ingen Database servere i Pubdmz.

SSIDMZ01.LOCAL (dmz 6x)

Dette er blevet vedtaget som det kommende DMZ hvor alle fremtidige dmz ressourcer skal placeres.

IMKIT.DK (dmz 7x)

NSIDSDN.DK (dmz 8x) (eSundhed?)

Lige pt. kræves der forskellige brugere og kodeord på de forskellige domæner; serverstruktur, ad-struktur mm. er forskellige, men på sigt skal der samkøres og kopieres, så administrationen bliver mere ensartet og enkel.

Vi vil på sigt have den samme AD-OU struktur, så man ved hvor man skal oprette en privilegie gruppe, en service konto eller lignende.

Der satses på Tier0 til Tier2 modellen, og sikkerheden øges, hvilket betyder at der kræves Kerberos for at forbinde mellem servere, se senere.

Dokumentation:

Vores dokumentation findes primært i Sharepoint.

Vi har et Systemkatalog: <https://sektornet/nsi/systemkatalog/SitePages/Startside.aspx> hvor vores systemer er beskrevet, og der er links til drift-dokumentation, servere, databaser, host notes og andre interessante dokumenter

### Datalagring:

Udover Filer på filservere, har SDS en stribe Database servere.

De 3 store systemer er ORACLE, DB2 og MSSQL, men vi har enkelte POSTGRESQL, MYSQL og lignende.

### Linux / Windows

Oracle er primært Linux baserede (RedHat Enterprise), Db2 kan være begge dele, og Mssql er pt. udelukkende Windows baseret.

### Virtualisering.

Servere bliver VMWare baserede.

### Overvågning.

Vi bruger Check\_MK til at overvåge servere, netværk og enheder, og der installeres agenter med plugins på serverne der samler informationerne, og videresender til central Check\_MK server

### 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.

## MSSQL Servere.

Vi har udfaset alle MS SQL server 2005 (og ældre) skal til at gøre det samme med MS SQL Server2008(r2), har 2012 og 2014, og 2 stk. MS SQL Server 2016 i produktion & 2 i test.

Vi foretrækker 1 server 1 instans politikken, prøver at konsolidere Databaser på SQL hoteller, og alle nye tiltag SKAL være AD-gruppe baseret, dvs. ingen brugere tilknyttet databaserne.

Der skal ligeledes give så minimale rettigheder som muligt.

Service konti skal defineres i AD, og komplicerede kodeord SKAL gemmes i Thycotic Secret server, og må IKKE sendes via mail.

Vi kan benytte gMSA til at definere servicekonti, med automatisk password styring.

## SQL Server Collection og Rapporter

Da vi bruger SCCM til at administrere og opdatere software og patches, er alle servere (og workstations) registreret her. Derfor kan vi hente opsamlede data herfra og viderebehandle andetsteds.

Dette kræver at der, på den enkelte server, registreret en del WMI klasser relateret til SQL Server. Man kan registrere "sqlmgmproviderxpsp2up.mof" på en ikke registreret SQL server med følgende kommando:

mofcomp "C:\Program Files (x86)\Microsoft SQL Server\XXX\Shared\sqlmgmproviderxpsp2up.mof"

Vigtigt! SCCM Server: srv-inf-sccm.ssi.ad skal IKKE administreres af MSSQL DBA!

<SCCM Admin> administrerer den, holder den opdateret, SQL licensen blever dækket af Configmgr licensen, så den skal IKKE med i licens optælling mv.

Men vi vil selvfølgelig være behjælpelig hvis <SCCM Admin> har behov derfor.

## Firefox Konfiguration Autologon mtime

Åbn Firefox, skriv about:config

Tryk ”Jeg lover at være forsigtig!”

Søg i søgefelt på auth

Dobbeltklik på

Network.automatic-ntlm-auth.allow-non-fqdn - for at skifte til værdien true

Network.automatic-ntlm-auth.trusted-urls - for at indtaste urls:

Skriv f.eks. 4 url’s komma separeret:

https://sundhedsdata.mtime.dksund.dk,https://s-adm02-p.dksund.dk,https://dksund.sharepoint.com, https://s-mssqlrs03-p.dksund.dk

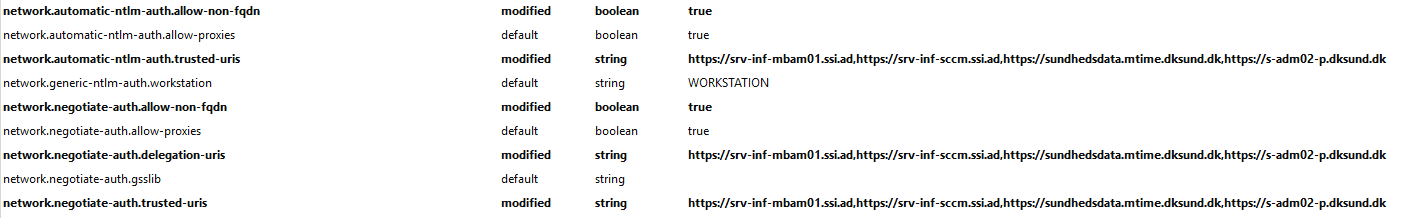
Network.negotiate-auth.allow-non-fqdn - for at skifte til værdien true

Network.negotiate-auth.delegation-urls - for at indtaste urls:

Skriv samme 4 Urls

Network.negotiate-auth.trusted-urls - for at indtaste urls:

Skriv samme 4 Urls



Luk og genstart, så er der autologon til mtime mm.

# ToDo Liste:

## Planlagte nye SQL Servere

s-mssql11-p.ssi.ad SQL Server 2016 Enterprise Produktions Hotel

s-mssql12-t.ssi.ad SQL Server 2016 Enterprise Test / udv. Hotel (2 Instanser)

s-mssql22-p.sst.dk SQL Server 2016 Enterprise Produktions Hotel

s-mssqlrs03-p.dksund.dk SQL Server 2016 Reporting Services.

s-mssqlasis04-p.dksund.dk SQL Server 2016 Analysis & Integration services

## SQL Servere der skal analyseres og Nedlukkes

Sqlserver02.ssi.ad

Sqlserver04.ssi.ad

Srv-sql-test02.ssi.ad

Lanmssql1udv.sst.dk

Lanmssql2.sst.dk

Alle 2008, 2008R2 og 2012 SQL servere

Alle SQLexpress

ADMOEK.sst.dk Patchning? (spoop ny version skal planlægges, derefter kan denne måske nedlægges)

## Changes til kommende Servicevindue (Prefiks Servicevindue -)

SD 346761 MSSQL 2014 SP3 på 9 servere.

#Check\_MK kontrol af Ola Hallengreen maintenance jobs

#Check\_MK SQL 2-trin udtræk via blob

#Check sa konto for alle SQL instanser og ret til hvis sa konto ikke svarer til Secret Server sa konto.

## Udført

## Andet:

MSSQL Audit opsætning, Check\_MK MSSQL Plugin på s-fmsql21-p.sst.dk og s-mssql02-p.dksund.dk

Begræns MSSQL Auditing Output

Check\_MK VB-script deles op til lokal udførsel.

# Fremtidig Ad Struktur:

## Ou oversigt:

Dksund.dk = Domænet

∟Tier0 = Domæne & Enterprise ressourcer

| ∟Service Administrators

| ∟T0Groups

| ∟T0Servere

| ∟T0ServiceKonti

∟Tier1 = Overordnet System niveau

| ∟Data Administrators --- adm\_mive

| ∟T1Groups

| ∟MSSQL --- G-ORG-MSSQL-Sysadmin = sysadm brugere på alle mssql db

L-ORG-MSSQL-Sysadmin = sysadm logon på alle mssql db

G-ORG-MSSQL-AdmWinOS = Lokaladm brugere på alle mssql Servere

L-ORG-MSSQL-AdmWinOS = medlemskab Lokaladm (administrators) gruppe på alle Servere

Grupper der skal have adgang til mssql servere i domænet: brugere 🡪 Global 🡪 Lokal 🡪 Ressource

| ∟T1Servere

| ∟T1ServiceKonti

| ∟MSSQL --- svd-sql-agent03 = svd der skal bruges til at starte services

svd-sql-de03 ! her skal sættes Kerberos via Attribute editor: servicePrincipalName

svd-sql-agentApp02

svd-sql-deApp02

svt\_sql\_report03 = svt der skal bruges til reporting services

| ∟<applikation/system> --- svd-sql-agent03 = svd der skal bruges til at starte services

∟Tier2 = Applikations niveau

| ∟T2Groups

| ∟T2ServiceKonti

∟Users = Bruger niveau

# Planlægning af Ny SQL Server

Hotel / Eksklusiv maskine:

Nyt Jern / Virtuel:

Standard SQL / Enterprise:

Antal kerner / CPU:

Ram:

Hvem skal betale Licensen:

Diskopsætning:

C: (system incl pagefil)

R: SQLData

S: SQLLog

T: SQLTempDb

U: SQLBackup

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

1. Opsætning af Server, Instans og Databaser foretages af IOS MSSQL afdelingen
2. Adgang til databaser styres via foruddefinerede AD gruppe-par (Global brugergrupper & Lokale Ressourcegrupper) der klargøres af IOS MSSQL afdelingen.
3. Der skal registreres & godkendes Undtagelseserklæring hvis der skal ske adgang udover via AD-grupper.
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 må ikke ligge bruger data uden for SQL på denne server, Data skal flyttes til Applikations server eller dedikerede Fil servere
7. Der må ikke startes jobs uden for SQL, og kun godkendte agentjobs, der scheduleres inden for SQL.
8. Der køres hver aften IOS godkendte maintenance jobs, der checker integritet & opdaterer indexes.
9. På et MS SQL Server Hotel, må brugere IKKE have fjernskrivebords adgang, så databaseadgang kan foretages fra egen udviklings pc, via en Jump host eller lignende med MS SQLServer Management Studio
10. På Produktions SQL Hotel må der ikke udvikles, og ikke tildeles rettigheder til administration. Der kan gives temporære privilegier til fejlsøgning
11. Ændringer til Produktion foretages via changes, efter test på test servere & udvikling på udviklings servere.

## 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 Systemejer
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

## 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 godkende hvem der er manager & befuldmægtiget til at tildele privilegier via denne gruppe, hvad der skal stå i gruppe noter og beskrivelsen, hvem (inkl. domæne) der får privilegier via denne gruppe, samt ALLE ressourcerne der gives privilegier til.

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

Når en bruger vil ansøge om adgang til en database, skal ansøgningen (typisk en eMail med liste af brugere, databaser, privilegieønske og en god begrundelse)godkendes af den data / ressource ansvarlige for det pågældende system før den videresendes til Servicedesk, der IKKE 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.

Alternativt kan MSSQL afdelingen oprette de korrekte Windows AD grupper, på baggrund af ovenstående kriterier, tilknytte grupperne til databaserne, 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 veersioner bør kun bruges til fejlfinding.

## Planlægning af ny SQL Database

### Krav:

SQL Version?

Hotel / Eksklusiv maskine

Forventet størrelse / ressourcebehov

Specielle Backup / 24-7 krav?

System i Systemkataloget.

Hvem er overordnet Systemejer af databasen?

For hver gruppe der giver adgang til databasen, skal der være defineret en Ressource ansvarlig?

Hvad er databasens formål?

Hvilken slags data vil blive gemt i databasen? Er det kun "tekst" eller fx. også billeder?

Hvor skal data tilgås fra? Klienter, anden server, Webserver eller flere typer? Hvilke klienter; hvor er de placeret?

Enterprise / standard version:

Er der personfølsom data i databasen? Hvis ja, hvilke?

Er der personhenførbar data i databasen? Hvis ja, hvilke?

Er der data af personer/steder i anonymiseret form i databasen?

Hvordan tilgås databasen; hvilke værktøjer bruges?

### Installation:

Højreklik Databases – New Database

Angiv Navn & Owner = sa

Start ”DP for SQL Management Console,

vælg Tivoli Storage Manager\Dashboard\Protect and Recover Data

vælg den aktuelle instans

Vælg den nye database

Vælg Action (til højre) \Full Backup

Når backup er færdig, luk Tivoli Flashcopymanager ned

Opret evt. nye logins på ad-Lokal gruppen, med default db som ny db, og User Mappings på ny db med privilegier

Check Security under database at brugergruppe har dbo som default schema

Hvis man glemmer at bruge korrekt owner:

exec sp\_helpdb

viser hvilke brugere der er owner på databaserne - derefter

Use Dbnavn

Exec sp\_changedbowner @loginame = 'sa'

### Adgang til databaser.

Al fremtidig adgang til databaser skal styres af grupper

Grupper sættes op i AD i bestemte ou, hvor MSSQL har adgang.

På p:\SQLDBA\ps1\ad kan man tilrettet de første linier i Make-group.ps1

### Service konti findes i 3 typer:

svb​ Batch-konto (servicekonto)

Anvendes til at overføre særlige datamængder på særlige (skedulerede) tidspunkter.

svt​ ​Transaktions-konto (servicekonto)

Anvendes til at forespørge én service på vegne af en anden; anvendes fx af en web-frontend til at forespørge en database-backend.

​svd Installations/service/daemon-konto (servicekonto)​

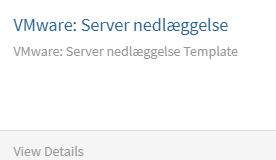
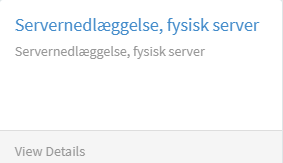
Dette er den typiske service-konto; en konto, som afvikler en service/proces lokalt på en maskine. Bruges til at isolere software i særlige sikkerhedskontekster.

# Nedlægning af SQL Server

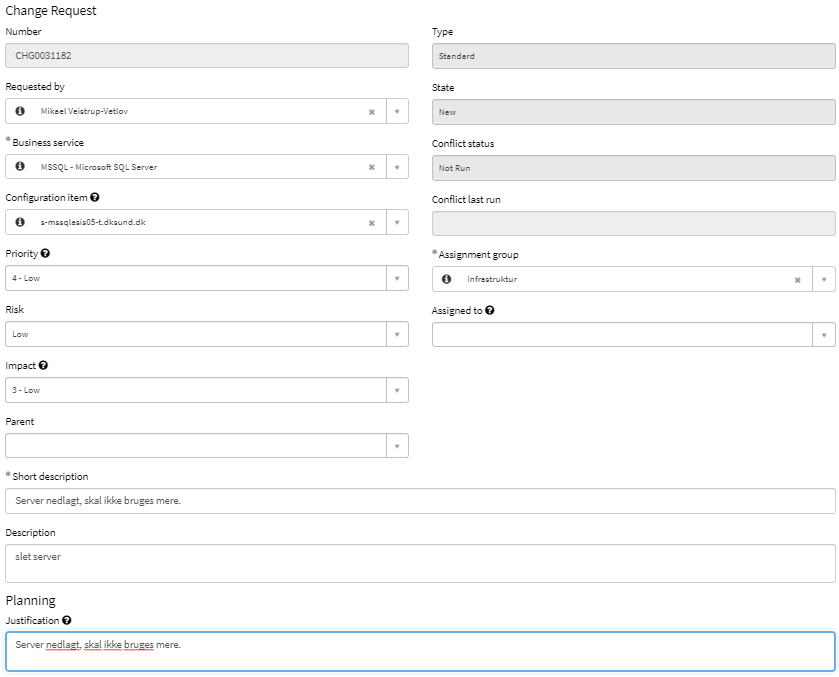
### Stop Backup af SQL Server

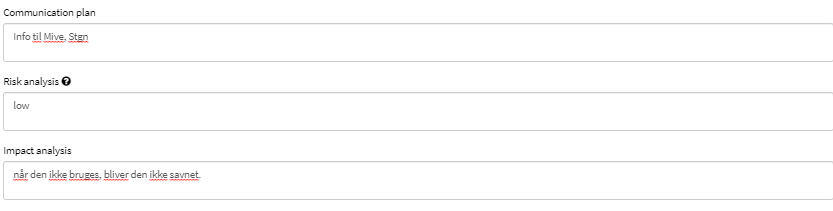
### Opret Change I ServiceNow, Server Nedlagt

[Catalog - Browse - Serviceportal (service-now.com)](https://sds.service-now.com/serviceportal?id=sc_category&sys_id=b0fdfb01932002009ca87a75e57ffbe9&catalog_id=-1)



Submit





### Gem evt. Databaser på Data Gravpladsen

### Afinstaller SQL fra Server

### Marker server I ServiceNow, som Nedlagt

### Marker server I Check\_MK, som Nedlagt

### Marker server I Systemkataloget, som Nedlagt

### Marker server I SQL Collect, som Nedlagt

### Marker server I AD, som Nedlagt

### Marker server I Logpoint, som Nedlagt

### Marker server I s-logdb01-p, som Nedlagt

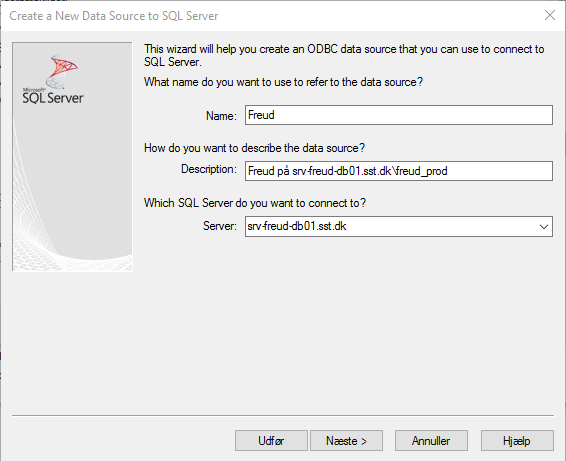
# Odbc forbindelse til SQL Server.

Start Kontrolpanel\Administration\ODBC-Datakildeadministrator (f.eks. 64-bit)

I bruger-DSN tryk tilføj.

Vælg Driver:

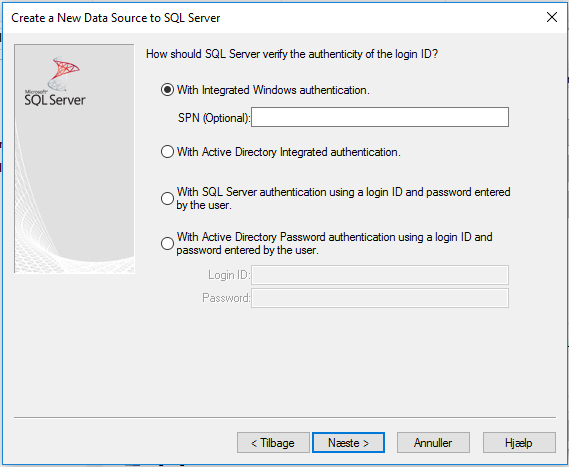
”ODBC Driver 13 for SQL Server” eller ”SQL Server” og tryk Udfør.



Angiv navn og beskrivelse,

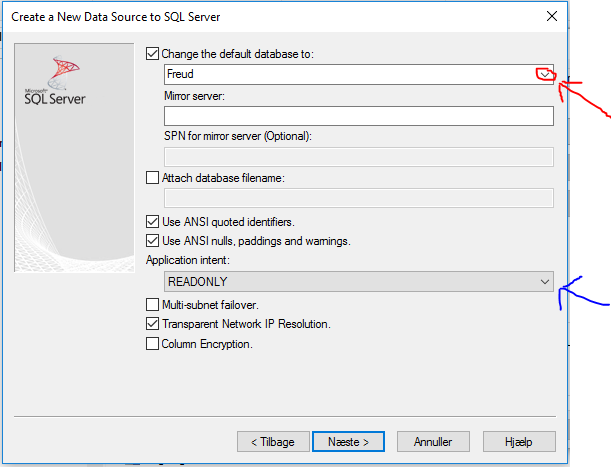
og skriv Servernavn

Tryk Næste



Vælg With Integrated Windows …

Tryk Næste



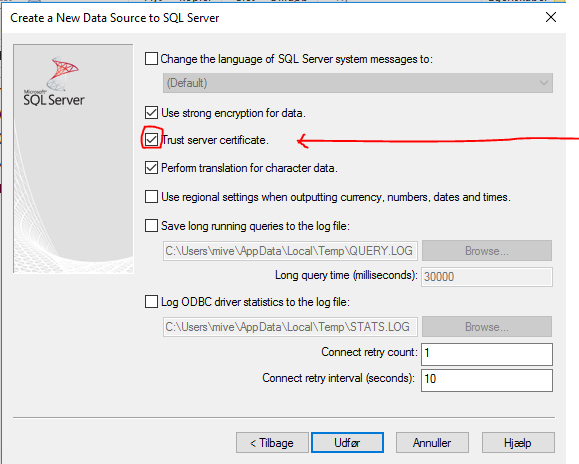
Vælg: Change default db to:

Klik  og vælg den ønskede database.

Herved kan du se at du har adgang til SQL Serveren.

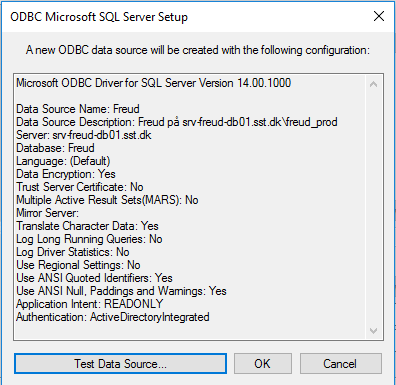
Vælg privilegie (læs / skriv)

Tryk Næste

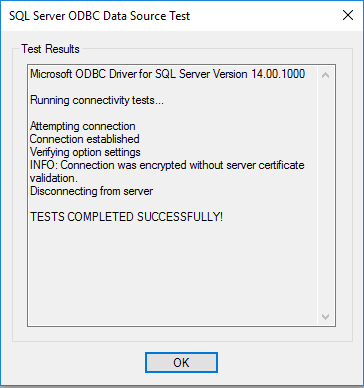


Vælg Trust server Certificate

Tryk Udfør



Test Datakilde / Data Source



Tryk Ok nogle gange

Luk ODBC, Administrations vindue & Kontrolpanel.

# Powershell I MSSQL, Server, Arbejdsplads.

# Maintenance scripts

## Anbefalinger:

Det er Best Practice & De-facto Standard for MSSQL Installationer over hele verden.

MSSQL Community anbefaler:

>>You should intelligently do index reorg and rebuilds. As a general (widely accepted) rule of thumb is

>>If your indexes are fragmented :

* If index has less than 1000 pages - do not perform any index maintenance operation.
* Less than 10% - then do nothing
* between 10% and 30% - then do a reorg
* more than 30% - then rebuild them.

>>I would highly recommend to use Ola's maintenance solution (index and checkdb)

Dette er præcis hvad vi gør.

Der er mange der anbefaler indeks reorganiseringen hver 2-3 måneder, og for hyppig genopbygning vil faktisk belaste serveren meget mere end det gavner.

Desuden vil der ofte gå nogle timer -> et par dage før statistikker er faldet på plads efter en genopbygning, hvilket igen modvirker den gavn man kan have af en reorganisering.

### Kontrol af fragmentering: Page\_count & frag i %

use <database>;

SELECT

t.NAME 'Table name',

i.NAME 'Index name',

ips.index\_type\_desc,

ips.alloc\_unit\_type\_desc,

ips.index\_depth,

ips.index\_level,

ips.avg\_fragmentation\_in\_percent,

ips.fragment\_count,

ips.avg\_fragment\_size\_in\_pages,

ips.page\_count,

ips.avg\_page\_space\_used\_in\_percent,

ips.record\_count,

ips.ghost\_record\_count,

ips.Version\_ghost\_record\_count,

ips.min\_record\_size\_in\_bytes,

ips.max\_record\_size\_in\_bytes,

ips.avg\_record\_size\_in\_bytes,

ips.forwarded\_record\_count

FROM

sys.dm\_db\_index\_physical\_stats(DB\_ID(), NULL, NULL, NULL, 'DETAILED') ips

INNER JOIN

sys.tables t ON ips.OBJECT\_ID = t.Object\_ID

INNER JOIN

sys.indexes i ON ips.index\_id = i.index\_id AND ips.OBJECT\_ID = i.object\_id

WHERE

AVG\_FRAGMENTATION\_IN\_PERCENT > 0.0

ORDER BY

AVG\_FRAGMENTATION\_IN\_PERCENT, fragment\_count

## Check om der er kommet en ny version.

Vi bruger Ola Hallengrens Maintenance scripts på alle MSSQL Servere.

På <https://ola.hallengren.com/> findes og downloades: <https://ola.hallengren.com/scripts/MaintenanceSolution.sql>

Der checkes om det er en nyere version end den med tisdsstempel: f.eks: Last updated 7 October, 2016.

Hvis det er, downloades script til P:\sqldba\dba\MaintenanceScripts med dato i navn.

Og der tilrettes:

Der appendes i toppen:

/\*

PRE SCRIPT, Mive 20200229

Slet job til kontrol 'DatabaseBackup - USER\_DATABASES - DIFF'

\*/

Use msdb

DECLARE @jobId0 binary(16);

SELECT @jobId0 = job\_id FROM msdb.dbo.sysjobs WHERE (name = N'DatabaseBackup - USER\_DATABASES - DIFF')

IF (@jobId0 IS NOT NULL)

BEGIN

EXEC msdb.dbo.sp\_delete\_job @jobId0, @delete\_unused\_schedule=1

END

/\* Slut PRE SCRIPT \*/

Set @cleanuptime --sættes til = 504 eller

DECLARE @CleanupTime int --sættes til = 504

Og der appendes i bunden:

/\*

POST SCRIPT, eks\_arjo Rettet Mive 20210104

CREATE AND ASSIGN SCHEDULE

DISABLE BACKUP JOBS

\*/

USE [msdb]

--If exists (select 1 from msdb.dbo.sysschedules where name = 'SQLDBA\_Nightly\_01:00')

--Begin

-- DECLARE @Schedid1 binary(16)

-- SELECT @Schedid1 = schedule\_id FROM msdb.dbo.sysschedules WHERE (name = N'SQLDBA\_Nightly\_01:00')

-- IF (@Schedid1 IS NOT NULL)

-- EXEC msdb.dbo.sp\_delete\_schedule @Schedid1

--END

USE [msdb]

If NOT exists (select 1 from msdb.dbo.sysschedules where name = 'SQLDBA\_Nightly\_01:00')

Begin

EXEC msdb.dbo.sp\_add\_schedule

@schedule\_name = N'SQLDBA\_Nightly\_01:00' ,

@freq\_type = 4,

@freq\_interval = 1,

@active\_start\_time = 010000

END

og

If NOT exists (select 1 from msdb.dbo.sysschedules where name = 'SQLDBA\_Nightly\_03:00')

Begin

EXEC msdb.dbo.sp\_add\_schedule

@schedule\_name = N'SQLDBA\_Nightly\_03:00' ,

@freq\_type = 4,

@freq\_interval = 1,

@active\_start\_time = 030000

END

If NOT exists (select 1 from msdb.dbo.sysschedules where name = 'SQLDBA\_Nightly\_23:00')

Begin

EXEC msdb.dbo.sp\_add\_schedule

@schedule\_name = N'SQLDBA\_Nightly\_23:00' ,

@freq\_type = 4, -- 4=daily, 8=weekly

@freq\_interval = 1,

@active\_start\_time = 230000

END

*--DatabaseIntegrityCheck - USER\_DATABASES*

*EXEC msdb.dbo.sp\_attach\_schedule*

*@job\_name = N'DatabaseIntegrityCheck - USER\_DATABASES',*

*@schedule\_name = N'SQLDBA\_Nightly\_03:00' ;*

*GO*

*--DatabaseIntegrityCheck - SYSTEM\_DATABASES*

*EXEC msdb.dbo.sp\_attach\_schedule*

*@job\_name = N'DatabaseIntegrityCheck - SYSTEM\_DATABASES',*

*@schedule\_name = N'SQLDBA\_Nightly\_03:00' ;*

*GO*

*--IndexOptimize - USER\_DATABASES*

*EXEC msdb.dbo.sp\_attach\_schedule*

*@job\_name = N'IndexOptimize - USER\_DATABASES',*

*@schedule\_name = N'SQLDBA\_Nightly\_01:00' ;*

*GO*

*--disable backup jobs*

*EXEC msdb.dbo.sp\_update\_job @job\_name=N'DatabaseBackup - SYSTEM\_DATABASES - FULL',*

*@enabled=0*

*GO*

*EXEC msdb.dbo.sp\_update\_job @job\_name=N'DatabaseBackup - USER\_DATABASES - DIFF',*

*@enabled=0*

*GO*

*EXEC msdb.dbo.sp\_update\_job @job\_name=N'DatabaseBackup - USER\_DATABASES - FULL',*

*@enabled=0*

*GO*

*EXEC msdb.dbo.sp\_update\_job @job\_name=N'DatabaseBackup - USER\_DATABASES - LOG',*

*@enabled=0*

*GO*

*/\* Slut POST SCRIPT \*/*

## Installation af Maintenance plan på server

Der checkes på server om der er 4 disablede backup jobs med navn:

'DatabaseBackup - SYSTEM\_DATABASES - FULL',

'DatabaseBackup - USER\_DATABASES - DIFF',

'DatabaseBackup - USER\_DATABASES - FULL',

'DatabaseBackup - USER\_DATABASES - LOG'

Hvis de findes er Ola Hallengrens maintenance jobs allerede installeret

Hvis ikke, kopieres indholdet af P:\sqldba\dba\MaintenanceScript\MaintenanceSolution\_Inkl\_PostScript.sql med nyeste dato i navn.

På SQL Instansen startes Query, ola’ scriptet pastes ind og køres, og der checkes at bl.a. ovenstående disablede jobs nu optræder

Hvis de skal geninstalleres skal der checkes om der er en schedulering der skal fjernes først.

select \* from sysschedules where name like 'SQLDBA%'

Disse kan slettes på navn ved

USE [msdb];

EXEC msdb.dbo.sp\_delete\_schedule

@schedule\_name = N'SQLDBA\_Nightly\_03:00' ,

@force\_delete = 1;

GO

EXEC msdb.dbo.sp\_delete\_schedule

@schedule\_name = N'SQLDBA\_Nightly\_01:00' ,

@force\_delete = 1;

GO

Eller ved Schedule\_id:

USE [msdb]

EXEC msdb.dbo.sp\_delete\_schedule

@schedule\_id = 11 ,

@force\_delete = 1;

GO

## SQL LOG dir

For at se SQLLogdir, opret SQLAgentjob, med step:

print '$(ESCAPE\_SQUOTE(SQLLOGDIR))'

kør det og se resultat, f.eks.:

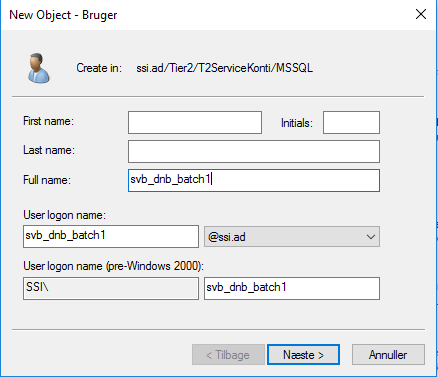
Executed as user: SSI\svd\_sqla09t$. R:\MSSQL12.MSSQLSERVER\_TEST\MSSQL\Log

# Batch/Transaktions Service Konti

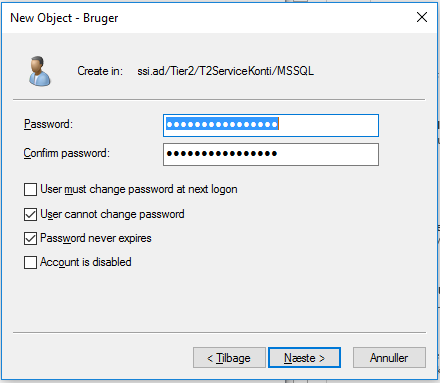
Bruges til at forbinde til SQL fra applikation, Task Scheduler eller batch job.

I aktuel AD oprettes ny bruger:

Højreklik ssi.ad\Tier2\T2Servicekonti\MSSQL - - > Ny Bruger



Angiv User Logon Name: og kopier dette til Full Name, Tryk Næste.



Vælg kun: User cannot Change pw &

Password never expires.

Angiv password fra f.eks.

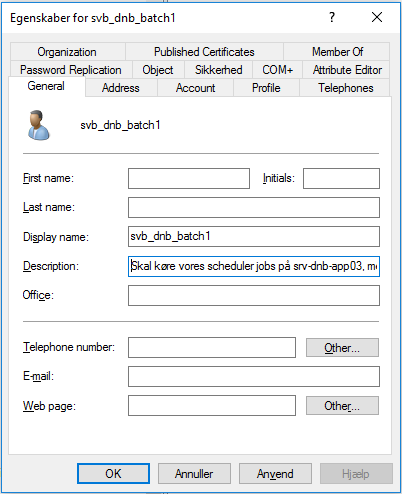
http://passwordsgenerator.net/

med 16 char. Specialtegn, tal, store & små bogstaver.

Password skal gives videre til Bruger & Secret Server

Tryk Næste

Åbn den nyoprettede Service konto



Angiv beskrivelse.

Tryk Ok

Åbn Secret Server i Browser.

https://secretserver.dksund.dk/login.aspx

login med dksund konto (skal have adgang)

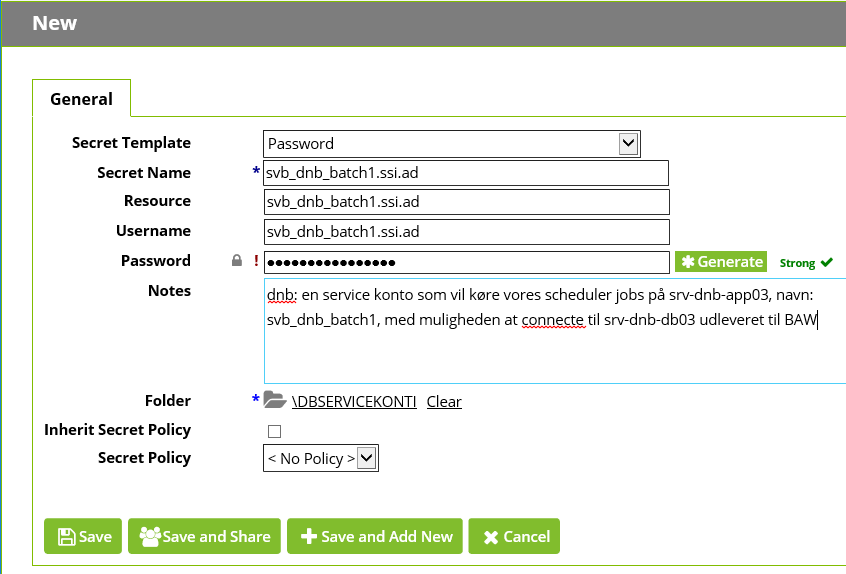
Create Secret – Create New Password

Angiv Secret Name, Ressource & Username  
Giv password der blev angivet i AD

Giv kort beskrivelse

Vælg folder dbservicekonti

Tryk save



På Server hvor service konto skal bruges åbnes Local Group Policy Editor: gpedit.msc

\Local Computer Policy\Windows Settings\Local Policies\User Rights

Her tilføjes kontoen til “Log on as a batch job” eller “Log on as a service” afhængig af formålet.

Hvis der allerede er AD konto defineret, skal kontoen meldes ind i denne.

# Logon as Batch, logon as Service

På server startes gpedit.msc

Der vælges:

Computer\windows\Security Settings\local Policies\user rights Assignments\log on as a batch job.

eller

Computer\windows\ Security Settings\local Policies\user rights\log on as a Service.

Derudover sættes gruppen i

Computer\windows\ Security Settings\local Policies\user rights\Deny log on locally

Computer\windows\ Security Settings\local Policies\user rights\Deny log on through Remote Desktop Services

## Change Security Policy SecPol

Hvis der ikke er gui adgang til server, har jeg et PowerShell Script:

[\\s-inf-fil-05-p.ssi.ad\pvl\INSTALL\SQLDBA\ps1\u\Chg-SecPol.ps1](file:///\\s-inf-fil-05-p.ssi.ad\pvl\INSTALL\SQLDBA\ps1\u\Chg-SecPol.ps1) <AdAccount> <cmd>

Hvor man kan give kommandoer til at liste, fjerne & tilføje konto til SecPol

# Lokal Service Konti

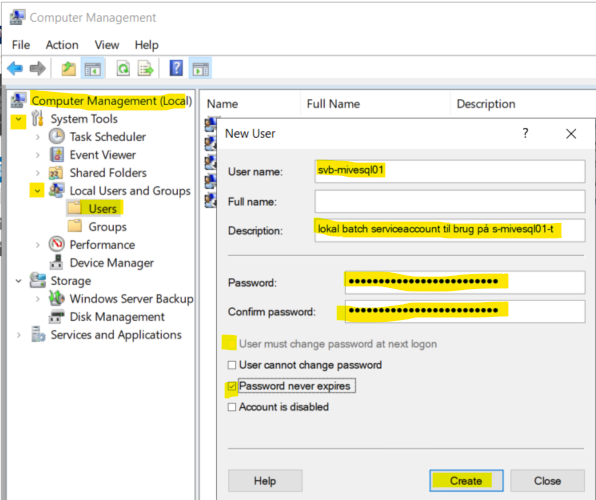
Som alternativ til ”Batch/Transaktions Service Konti” kan man oprette en lokal service konto.

Denne kan kun bruges på denne ene maskine, og man skal selv have styr på password og password skift.

Åbn Computer Management(local)\system Tools\Local users and groups\users og opret en ny bruger.

Giv denne konto et langt sikkert password, da det ikke bliver skiftet så tit som andre kodeord. F.eks.:

Dette kodeord skal gemmes på et sikkert sted, og der skal noteres ALLE steder denne servicekonto bruges, da password ikke tvinges skiftet som almindelige kodeord.



Angiv Bruger:

Description:

Password & gentag:

Fjern markering for at bruger skal skifte password næste logon.

Sæt markering om at password aldrig udløber.

Tryk Create for at oprette servicekonto.

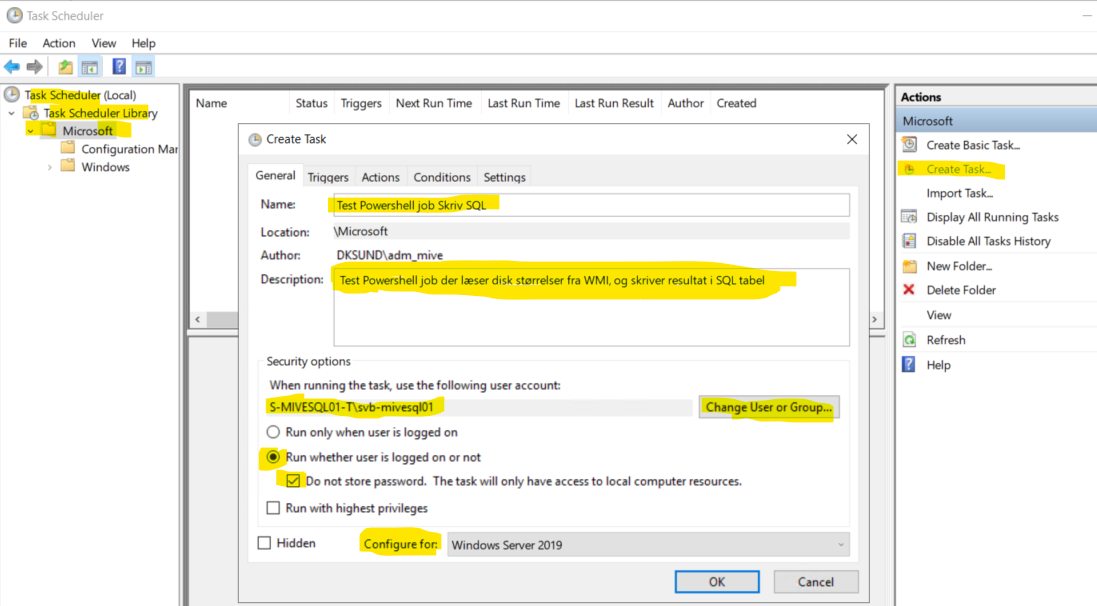
### Klargør job via Task Scheduler (bør IKKE bruges, brug SQL Agent job)

Forbered Automatisk kørsel.

Start Task scheduler

\Task Scheduler library \Microsoft

Actions: Create task:



General: Name=<JobNavn>

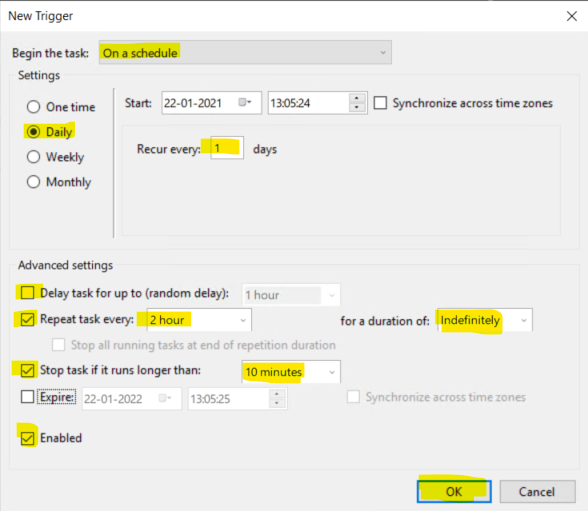
General: Description:<Beskrivelse>

General: Vælg servicekonto fra ad- eller lokalt

General: check Run whether user is logged in or not

General: check Do not store password, hvis job kun arbejder lokalt.

Vælg Trigger faneblad, vælg New..



Vælg Begin the task: on a schedule

Daily

Startid

Recur 1 days

Repeat task every 2 hour

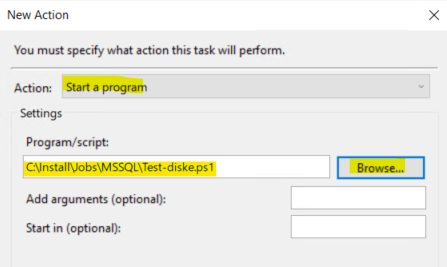
for duration of Indefinitely

Stop task if it runs longer than 10 min

Enabled

Tryk Ok

Vælg Actions faneblad, vælg New..



Action: Start a program

Program: Browse til scriptet

Udfyld evt parameter.

Tryk Ok

(

– Powershell

Add arguments: -noprofile -file u:\<path>\Audit\auditexport.ps1

Settings: "if already running......" Stop the existing instance

General: Change user or Group: --> svd\_sql\_xxxx

Tryk ok for password (from Secret Server)

Test Task ved at trytkke Run. (f5 eller højreklik task)

)

# Active Directory and Kerberos SPNs Made Easy!

By [RhysGoodwin](https://blog.rhysgoodwin.com/author/admin/) on April 7, 2009 in [Windows Admin](https://blog.rhysgoodwin.com/category/windows-admin/)

There are a lot of articles out there on setting up Kerberos **S**ervice **P**rincipal **N**ames but today I’m going to make it simple. Bear with me as I start off with the basics; by the end of the post it will all be very clear.

Throughout this post I’ll make reference to a scenario of a client computer connecting to an SQL server called **sql1.domain.com** however the same applies for any service, for example a web server where the client connects via HTTP.

The SQL server service is running under a domain service account called “**domain\SQLSVC**“. No SPNs have been set yet.

**The Basics**

Active directory user and computer accounts are objects in the active directory database. These objects have attributes. Attributes like *Name* and *Description.*

Computer and User accounts are actually very similar in the way they operate on a Windows domain and they both share an attribute called **ServicePrincipalName**. An account object can have multiple **ServicePrincipalName** attributes defined**.**

The setspn.exe tool manipulates this attribute. That’s all it does.

**The Failure**

The client wants to access the SQL server so he asks his domain controller: *“Please may I have a ticket for accessing* ***MSSQLSvc/sql1.domain.com”***

Now the domain controller asks the active directory database: “*Give me the name of the account object who’s ServicePrincipalName is* ***MSSQLSvc/sql1.domain.com****“*

The active directory database replies: *“Sorry, there are no account objects with that ServicePrincipalName”*

So the domain controller asks the active directory database again: *“Ok then, give me the account object who’s ServicePrincipalName is* ***HOST/sql1.domain.com****“*

**All** computer accounts have, by default ServicePinciaplName attributes set to:  
**HOST/*[computername]*** and **HOST/*[computername].[domain]***

So the active directory database replies to the domain controller: *“The account object that has that ServicePrincipalName is sql1.domain.com’s* ***computer account****“*

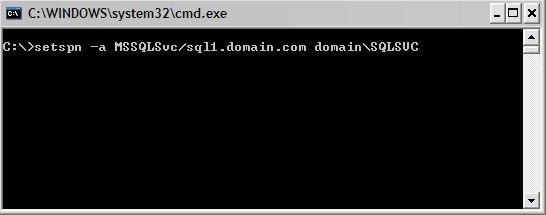
The domain controller now creates a ticket that only the computer account of **sql1.domain.com** can read. He gives the ticket to the client.

The client goes to the SQL service on sql1.domain.com and says “*here is my ticket, may I come in?”*

The SQL service will attempt to read the ticket. The problem is, the SQL service is not running under the computer account; it is running under a domain service account. It can not read the ticket; the ticket is only intended for the computer account of sql1.domain.com. Authentication fails (falls backto NTLM).

**The Fix**

Now lets run the **setspn.exe** tool to manipulate the **ServicePrincipalName** attribute of the SQL service account.

[](https://blog.rhysgoodwin.com/wp-content/uploads/2009/04/setspncmd.jpg)

setspn -a MSSQLSvc/sql1.domain.com domain\SQLSVC

We will also add **sql1** (without the domain name) in case we want to access the the server without the domain name appended.

setspn -a MSSQLSvc/sql1 **domain\SQLSVC**

Now run  through the scenario again and this time notice that the domain controller will return a ticket that the SQL server service account can read.

Obviously this is heavily paraphrased but hopefully it helps you understand the reason for setting the SPN attribute on the account that runs a given service.  Of course if the service runs under the local **NetworkService** or **LocalSystem** account then everything will just work because these local accounts represent the computer account in active directory.

-use kerbtray on the client to see what tickets you’re getting

-use wirshark to look at kerberos errors, first at the client then at any other box involved. E.g. app server etc.

https://devcentral.f5.com/questions/kerberos-authenication-cross-multiple-domains

# Server-ServiceAccounts:

## ServicePrincipalName (SPN) (SETSPN)

### Årsag: Kerberos Authentificering

Hvis det drejer sig om forbindelse fra anden server til SQL Server, så har Windows gruppen hærdet sikkerheden i domænerne, så man SKAL bruge Kerberos Authentificering.

Dette kræver at der er de korrekte servicekonti der starter SQL serveren, dette kræver også at der er sat de korrekte SetSPN parametre på server & servicekontoen.

Servicekontoen kan med fordel være en groupManagedServiceAccount(gMSA)

Hvis dette ikke er opfyldt, vil forbindelses forsøg resultere i "Login failed. Login is from an untrusted domain, and cannot be used with Windows Authentification.

Når SetSPN er sat op, skal SQL instansen genstartes, for at give de korrekte godkendte Kerberos adresse.

For at sikre at det kun er godkendte konti/brugere, og ikke konti med hengemte passwords fra NTLM, skal forbindelserne til serverne Kerberous authentificeres.

I en perfekt verden ville servere og service konti have rettighederne til at oprette de nødvendige forbindelser automatisk, men vi er nødt til at hjælpe dem på vej ved at angive nogle servicePrincipalNames, dvs navne der må forbindes til.

Der er forskel på opsætningen af SQL serverne og instanser, hvor mange og hvilke SPN der skal oprettes.

#### 1 instans, default instans.

Her skal der ikke sættes port på SPN, men der skal oprettes 1 servicekonto med 2 SPN, 1 med servernavn, og 1 med FQDN. Format: MSSQLSvc/SnameFqdn og MSSQLSvc/Sname

f.eks. SetSPN -S MSSQLSvc/s-mssql61-t.ssidmz01.local ssidmz01.local\svd\_sqle\_sql61t

#### 1 instans Navngiven instans.

Her skal der vælges en ubrugt port i tcp-range 50000-65000, SQL Config manager, tcpip opsætningen kan komme med et forslag (dynamisk port) der kan sættes som fast port. Her skal oprettes 1 servicekonto med 2 SPN, 1 med servernavn, og 1 med FQDN, begge med portnr., fra SQL Config manager, tcpip opsætningen nederst.

Format: MSSQLSvc/SnameFqdn:port og MSSQLSvc/Sname:port

Det skal også sikres at SQL Server Browseren er startet, og der skal på serveren (fqdn) laves (sikres) 1 SPN.

Format: MSOLAPDisco.3/SnameFqdn

#### 2 instanser, 1 default, og 1 eller flere Navngivne instanser.

Her skal oprettes 1 servicekonto med 2 SPN uden portnummer , + 1 servicekonto med 2 SPN med portnummer (for hver navngiven instans), se ovenfor.

Det skal igen sikres at SQL Server Browseren er startet, og der skal på serveren (fqdn) laves (sikres) 1 SPN.

#### 2 eller flere Navngivne instanser.

Her skal oprettes 1 servicekonto med 2 SPN med portnumre (for hver instans), der hver koordineres med SQL Config manager, tcpip opsætningen se ovenfor.

Det skal igen sikres at SQL Server Browseren er startet, og der skal på serveren (fqdn) laves (sikres) 1 SPN.

#### 1 eller flere SSAS instanser.

Her skal oprettes 1 servicekonto med 2 SPN (1 med servernavn, 1 med fqdn) ,med instansnavn (for hver instans).

Format: MSOLAPSvc.3/SnameFqdn:Instansnavn og MSOLAPSvc.3/Sname:Instansnavn

Det skal igen sikres at SQL Server Browseren er startet, og der skal på serveren (fqdn) laves (sikres) 1 SPN.

#### DNS alias til sql server / Instans

Der tilføjes spn for hver instans efter samme regler som ovenfor, men med alias navn i stedet for servernavn.

## Server-ServiceAccounts og opstart:

I mange tilfælde er SQL serveren installeret med en lokal konto til opstart

Denne skal udskiftes med en AD service konto, af sikkerhedsmæssige årsager.

Opret en service konto til at starte serveren under f.eks.: dksund.dk\Tier1\T1ServiceKonto\SQL\svd-sql-de03

Der er valgt navnestd: svd\_xxxx\_Servershort

Hvor:

Xxxx kan være: sqle,ssis,ssas,ssrs,sqla

Servershort er en entydig del af servernavnet barberet for mssql osv.

### SetSPN (Service Principal Name)

Start med at undersøg SPN afhængigheder:

setspn -l dksund.dk\s-mssql-db-02p for serveren

Registered ServicePrincipalNames for CN=S-MSSQL-DB-02P,OU=MSSQL,OU=Servere,DC=dksund,DC=dk:

CmRcService/S-MSSQL-DB-02P

CmRcService/S-MSSQL-DB-02P.dksund.dk

WSMAN/S-MSSQL-DB-02P.dksund.dk

TERMSRV/S-MSSQL-DB-02P.dksund.dk

RestrictedKrbHost/S-MSSQL-DB-02P.dksund.dk

HOST/S-MSSQL-DB-02P.dksund.dk

WSMAN/S-MSSQL-DB-02P

TERMSRV/S-MSSQL-DB-02P

RestrictedKrbHost/S-MSSQL-DB-02P

HOST/S-MSSQL-DB-02P

setspn -l dksund.dk\svd-sql-de02 for Servicekontoen (der starter sql instansen)

Registered ServicePrincipalNames for CN=svd-sql-de02,OU=SQL,OU=T1ServiceKonti,OU=Tier1,DC=dksund,DC=dk:

MSSQLSvc/idmdb02p

MSSQLSvc/idmdb02p.dksund.dk

MSSQLSvc/idmdb02p.dksund.dk:1433

MSSQLSvc/idmdb02p:1433

MSSQLSvc/s-mssql-db-02p:1433

MSSQLSvc/s-mssql-db-02p

MSSQLSvc/s-mssql-db-02p.dksund.dk:1433

MSSQLSvc/s-mssql-db-02p.dksund.dk

I P:\SQLDBA\ps1\spn er der et testværktøj, ”Find-SpnHost.ps1” der kan søge om der kan være andre servere / servicekonti der er bundet op med det aktuelle SPN eller server navn.

Kan køres i powershell på det aktuelle domæne med fqdn som parameter.

Dette kan også sættes i AD under den nye servicekonto (I properties\Attribute editor vælges servicePrincipalName og editeres.)

Her tilføjes alle nødvendige kombinationer af server navn, fqdn, instancenavn og portnummer, der skal kunne bruges til at kommunikere med Instansen.

Disse kan først gemmes, når service med nuværende lokal konto er stoppet

## MS GroupManaged ServiceAccounts:

Det anbefales at benytte gMSA til sqlopstart, da det er mere sikkert, systemet går ikke ned hver gang et password udløber, og man skal ikke tildele kryptiske (umulige) passwords via secretserver.

Man giver en server, eller gruppe af servere adgang til gMSA password, der styres af OS.

[Det kræver at man har adgang til MS AD Powershell modulerne](#_Check_AD-Powershell_modulerne:).

#### Forbered en gMSA ServiceAccount, Gem ad-server-identity i variabel.

$com = Get-ADComputer -Identity s-mssql-db-01p

#### Opret en gMSA ServiceAccount

new-ADServiceAccount -Name Test\_Mive -DNSHostName Test\_mive.dksund.dk

-PrincipalsAllowedToRetrieveManagedPassword $com

#### Opret en gMSA ServiceAccount med spn

new-ADServiceAccount -Name Test\_Mive -DNSHostName Test\_mive.dksund.dk

-PrincipalsAllowedToRetrieveManagedPassword $com -ServicePrincipalNames "MSSQLSvc/s-mssql-db-11q", "MSSQLSvc/s-mssql-db-11q.dksund.dk"

#### Opret en gMSA ServiceAccount med spn og portnr

new-ADServiceAccount -Name Test\_Mive -DNSHostName Test\_mive.dksund.dk

-PrincipalsAllowedToRetrieveManagedPassword $com -ServicePrincipalNames "MSSQLSvc/s-mssql-db-11q:54321", "MSSQLSvc/s-mssql-db-11q.dksund.dk:54321"

#### Slet en gMSA ServiceAccount

Remove-ADServiceAccount -Identity Test\_Mive$

>Confirm

>Are you sure you want to perform this action?

>Performing the operation "Remove" on target "CN=Test\_Mive,CN=Managed Service Accounts,DC=dksund,DC=dk".

>[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y

#### Test om denne server kan tilgå gMSA

PS> Test-ADServiceAccount -Identity test\_mive$

Hvis den svarer True må pågældende server gerne tilgå gMSA password.

Hvis False

>WARNING: Test failed for Managed Service Account Test\_Mive. If standalone Managed Service Account, the >account is linked to another computer object in the Active Directory. If group Managed Service Account, either this >computer does not have permission to use the group MSA or this computer does not support all the Kerberos >encryption types required for the gMSA. See the MSA operational log for more information.

#### Fjern gMSA fra host / server

Remove-ADServiceAccount -Identity svd\_sqlefreuEsu$

#### Find gMSA forbundet til en server

Fra p:\SQLDBA\ps1\spn: Find-SpnHost.ps1 srv-mssql-09t

#### Find alle SQL gMSA I et domæne

Get-ADServiceAccount –Filter 'Name -like "svd\_s\*"' | FT Name, DistinguishedName, ObjectClass -A

Tilknyt gMSA til host / server

Add-ADComputerServiceAccount -Identity Fabrikam-SRV1 -ServiceAccount IIS-SRV1

#### Link:

[Group Managed Service Accounts | IT Connect (uw.edu)](https://itconnect.uw.edu/wares/msinf/ous/guide/gmsa/)

#### Eksempler:

MSSQLSvc/S-MSSQL-DB-03P.dksund.dk

MSSQLSvc/S-MSSQL-DB-03P

MSSQLSvc/S-MSSQL-DB-03P.dksund.dk:1433

MSSQLSvc/S-MSSQL-DB-03P:1433

MSSQLSvc/S-SPE-DB-02P.dksund.dk:2433

MSSQLSvc/S-SPE-DB-02P:2433

MSSQLSvc/S-SPE-DB-02P.dksund.dk:SPECIMENGATE

MSSQLSvc/S-SPE-DB-02P: SPECIMENGATE

MSSQLSvc/S-MSSQL-DB-03P.dksund.dk:SPECIMENGATE

MSSQLSvc/S-MSSQL-DB-03P:SPECIMENGATE

MSSQLSvc/S-MSSQL-DB-03P.dksund.dk:2433

MSSQLSvc/S-MSSQL-DB-03P:2433

MSSQLSvc/SRV-MSSQL-07P.ssi.ad:2433

MSSQLSvc/SRV-MSSQL-07P.ssi.ad:MGMT

MSSQLSvc/SRV-MSSQL-07P:2433

MSSQLSvc/SRV-MSSQL-07P:MGMT

Setspn –s MSSQLSvc/SRV-MSSQL-07P.ssi.ad:1433 ssi.ad\svd-sql-de02

Setspn –s MSSQLSvc/DBHOTEL01.ssi.ad:1433 ssi.ad\svd-sql-de02

Setspn –s MSSQLSvc/SRV-MSSQL-07P:1433 ssi.ad\svd-sql-de02

Setspn –s MSSQLSvc/DBHOTEL01:1433 ssi.ad\svd-sql-de02

Setspn –s MSSQLSvc/SRV-MSSQL-07P.ssi.ad ssi.ad\svd-sql-de02

Setspn –s MSSQLSvc/DBHOTEL01.ssi.ad ssi.ad\svd-sql-de02

Setspn –s MSSQLSvc/SRV-MSSQL-07P ssi.ad\svd-sql-de02

Setspn –s MSSQLSvc/DBHOTEL01 ssi.ad\svd-sql-de02

MSSQLSvc/SRV-MSSQL-07P.ssi.ad:1433

MSSQLSvc/DBHOTEL01.ssi.ad:1433

MSSQLSvc/SRV-MSSQL-07P:1433

MSSQLSvc/DBHOTEL01:1433

MSSQLSvc/SRV-MSSQL-07P.ssi.ad

MSSQLSvc/DBHOTEL01.ssi.ad

MSSQLSvc/SRV-MSSQL-07P

MSSQLSvc/DBHOTEL01

MSSQLSvc/SRV-MSSQL-07P.ssi.ad

MSSQLSvc/SRV-MSSQL-07P.ssi.ad:1433

CmRcService/SRV-MSSQL-07P

CmRcService/SRV-MSSQL-07P.ssi.ad

WSMAN/SRV-MSSQL-07P.ssi.ad

WSMAN/SRV-MSSQL-07P

TERMSRV/SRV-MSSQL-07P

TERMSRV/SRV-MSSQL-07P.ssi.ad

RestrictedKrbHost/SRV-MSSQL-07P

HOST/SRV-MSSQL-07P

RestrictedKrbHost/SRV-MSSQL-07P.ssi.ad

HOST/SRV-MSSQL-07P.ssi.ad

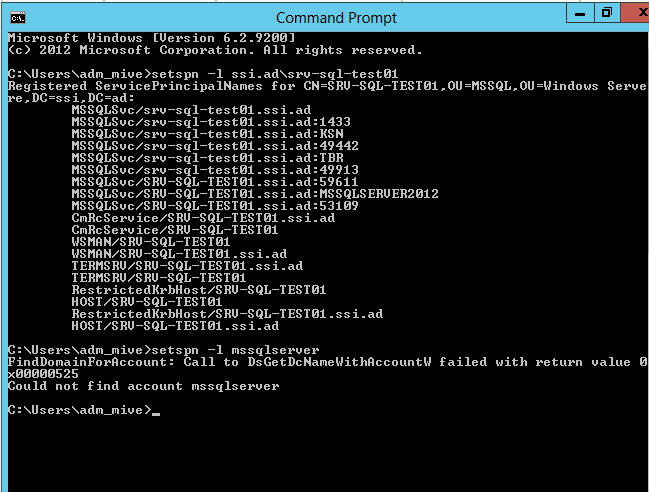
MSSQLSvc/SRV-MSSQL-09T.ssi.ad:1433

MSSQLSvc/SRV-MSSQL-09T:1433

MSSQLSvc/SRV-MSSQL-09T.ssi.ad

MSSQLSvc/SRV-MSSQL-09T

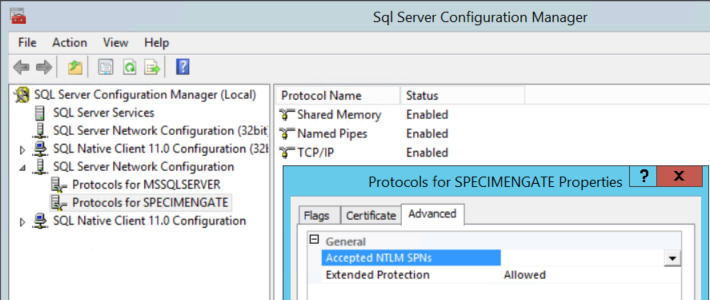
MSSQLSvc/srv-mssql-06t.sst.dk

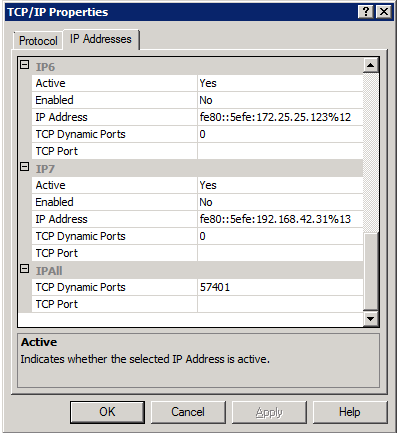


## TCP-IP Opsætning MSSQL Server

Vær sikker på i nedenstående, at Configuration Manager er den der passer til SQL Server instansen!!!

På serveren – I SQL Server Configuration manager\Network Configuration\Protocols for “instansnavn” vælges properties og Advanced\Extended Protection “Allowed”



Så vælges der TCP/IP Properties\Protocol: Listen All=Yes hvis kun 1 IP-adresse, ( og evt. =No hvis der er flere Ip-adresser og DNS der peger på dem).

Under IP Adresser vælges Active:Yes og Enabled :Yes for de aktive, port 1433 for default instans.

Gå til bunden

Ved dynamisk tildelt port:

Noter den dynamiske port som systemet har tildelt til den pågældende Named Instance for ALLip (her 57401)

Slet denne og tildel den faste port den samme nu frie port

Tildel denne port til fast ip, hvis det kun er specifikke ip der må bruges.

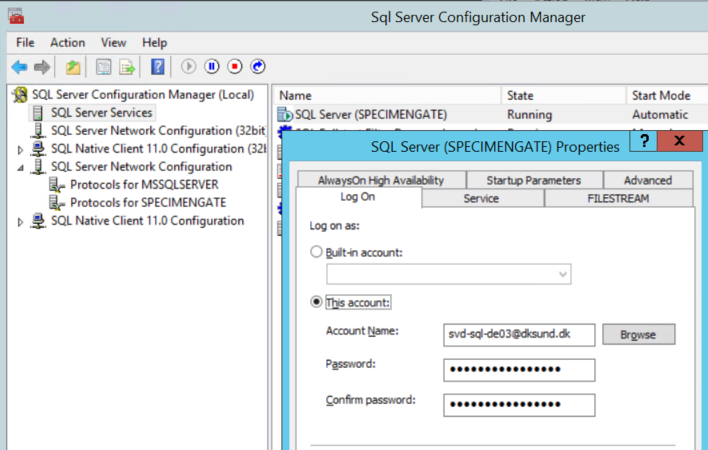
(Der kan også sættes 0 i dynamisk port (og blank i TCP port) for at bruge dynamiske porte for efterfølgende instanser.

IKKE ved kerberos)

I SQL Server Configuration manager\SQL Server Services\SQL Server(instans) Properties angives gMSA

Service account & Password (fra secret server)

NB Det anbefales at bruge gMSA, hvor man kun skal angive navnet på gMSA, og ikke password.



Og gå I Windows Services og controller at den samme service konto er sat her.

Derefter genstart SQL Server service (fra Windows Services)

Så kan man tilgå instans fra anden server:

S-SPE-DB-02P\SPECIMENGATE,2433

# Auditing / Logning på MSSQL Server til Logpoint

Alle Enterprise MSSQL servere skal auditlogge, logfilen skal konverteres til csv fil, og forberedes til afhentning af Logpoint. Logpoint skal opbevare logs i 5 år.

På instans niveau sættes log specifikationerne, der er valgt, og der logges til MSSQL audit log filer.

Da logpoint ikke kan modtage MSSQL formaterede audit logfiler, har vi et Powershell script, der skal scheduleres til at køre hver 10 min, der konverterer logfilerne til csv logfiler.

Logpoint henter disse filer og opbevarer dem.

Tilgang til disse audit logfiler foregår via en hjemmeside som tilgås via nedenstående simple link. Det anbefales at man kopierer link til en browser.

https://192.168.39.16/#Logs/searchLogs?query%3Dlabel%253D%2522Account%2522%2520label%253D%2522Create%2522%2520-target\_user%2520in%2520NAMING\_STD\_ACCOUNT\_FILTER%2520%257C%2520fields%2520col\_ts%252C%2520caller\_user%252C%2520caller\_domain%252C%2520target\_user%26time\_range%3D2017%252F01%252F02%252013%253A00%253A00%2520To%25202017%252F01%252F03%252014%253A00%253A00%26repos%3D%255B%2527127.0.0.1%253A5504/WindowsAD%2527%255D

Her angives ssi-brugernavn, password og domæne: ssi.ad vælges.

## Opsætning af Audit på MSSQL Instans.

1. Opret svd-sqla<servershort> (gMSA til at starte SQL agent) som sysadmin login på SQL Server instans
2. gpedit.msc Computer\windows\security\local Policies\user rights\log on as a batch job. Tilføj svd-sqla<servershort>

På MSSQL serverens logdisk S: (/T:) skal der være en Auditlog folder under Instansnavn, hvor auditlogs fra MSSQL lægges.

På MSSQL serverens Backupdisk (U:) skal der være en Audit folder under Instansnavn, her skal PowerShell konverterings scriptet være.

På MSSQL serverens Backupdisk (U:) skal der være en Logpoint folder under Instansnavn\Audit, hvor de til csv konverterede auditlogs placeres, og hentes af Logpoint programmet: nxlog (se senere)

Alle 3 må kun have følgende Security Permissions:

System: Full Control

Domæne\MSSQLServerAdms: Full Control (på dksund\ L-ORG-MSSQL-Sysadmin)

Domæne\ svd-sqla<servershort> : Full Control (SQL agenten starter)

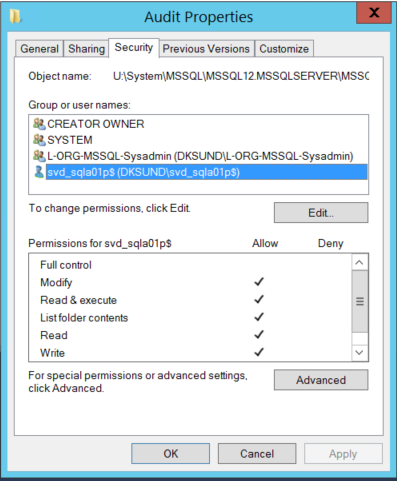
(Domæne\ svd-sqle<servershort> : Full Control) kun audit folder (SQL engine starter)

Alle andre brugere skal fjernes via:

Properties\Security\Advanced

Replace all child object….. Disable inheritance Convert inherited….

* Vælg og remove andre brugere.
* Add \ Select a principal \object types (tilføj service account)
* \ svd-sqla<servershort>; svd-sqle<servershort>
* Check Names
* Basic Permissions Full Control
* Ok



Oversigt

### Oprettelse af Audit Logfile

i SQL\<instans>\Security\Audits:

Opret Auditlog og parameter til samme, Maxsize X Max Rollover angiver max størrelse på disk, Filepath tilrettes så den peger på auditlog folder.:

USE [master]

GO

CREATE SERVER AUDIT [AuditLog]

TO FILE

( FILEPATH = N'S:\System\MSSQL12.MSSQLSERVER\Auditlog'

,MAXSIZE = 50 MB

,MAX\_ROLLOVER\_FILES = 400

,RESERVE\_DISK\_SPACE = OFF

)

WITH

( QUEUE\_DELAY = 1000

,ON\_FAILURE = CONTINUE

)

ALTER SERVER AUDIT [AuditLog] WITH (STATE = ON)

GO

Angiv Parametre til logning:

NB. Hvis der ændres på hvad der logges, SKAL Logpoint have besked, da de skal normaliseres (opsamlings checkes)

CREATE SERVER AUDIT SPECIFICATION [AuditLogSpec]

FOR SERVER AUDIT [AuditLog]

ADD (SCHEMA\_OBJECT\_ACCESS\_GROUP),

ADD (DATABASE\_ROLE\_MEMBER\_CHANGE\_GROUP),

ADD (SERVER\_ROLE\_MEMBER\_CHANGE\_GROUP),

ADD (BACKUP\_RESTORE\_GROUP),

ADD (AUDIT\_CHANGE\_GROUP),

ADD (DATABASE\_PERMISSION\_CHANGE\_GROUP),

ADD (DATABASE\_OBJECT\_PERMISSION\_CHANGE\_GROUP),

ADD (SCHEMA\_OBJECT\_PERMISSION\_CHANGE\_GROUP),

ADD (SERVER\_OBJECT\_PERMISSION\_CHANGE\_GROUP),

ADD (SERVER\_PERMISSION\_CHANGE\_GROUP),

ADD (FAILED\_LOGIN\_GROUP),

ADD (SUCCESSFUL\_LOGIN\_GROUP),

ADD (DATABASE\_PRINCIPAL\_CHANGE\_GROUP),

ADD (SCHEMA\_OBJECT\_CHANGE\_GROUP),

ADD (SERVER\_PRINCIPAL\_CHANGE\_GROUP),

ADD (DATABASE\_OWNERSHIP\_CHANGE\_GROUP),

ADD (DATABASE\_OBJECT\_OWNERSHIP\_CHANGE\_GROUP),

ADD (SCHEMA\_OBJECT\_OWNERSHIP\_CHANGE\_GROUP),

ADD (SERVER\_OBJECT\_OWNERSHIP\_CHANGE\_GROUP)

WITH (STATE = ON)

GO

(Højreklik Security\Audits\Auditlog og Enable Auditlog.) hvis det ikke kører

Herefter checkes om der kommer audit logs i auditlog folder:

## Konverteringsjob fra audit format til csv format.

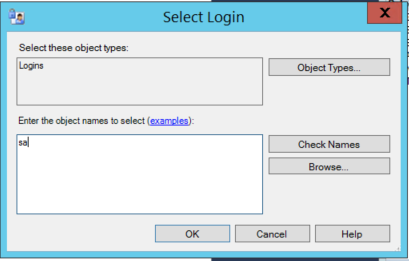
Kopier p:\SQLDBA\logpoint\auditexport.ps1 til Backupdisk (U:) Instansnavn\Audit folder: og ret til:

# ret AuditSourcedir (s:\.....\auditlog) & AuditExportdir (u:\......\audit\Logpoint) til lokale disk navne.

# ret maxfilePerRun efter performance test.

## Forbered Automatisk kørsel.

I SQL Server: \SQL Server Agent\Jobs Start New Job:



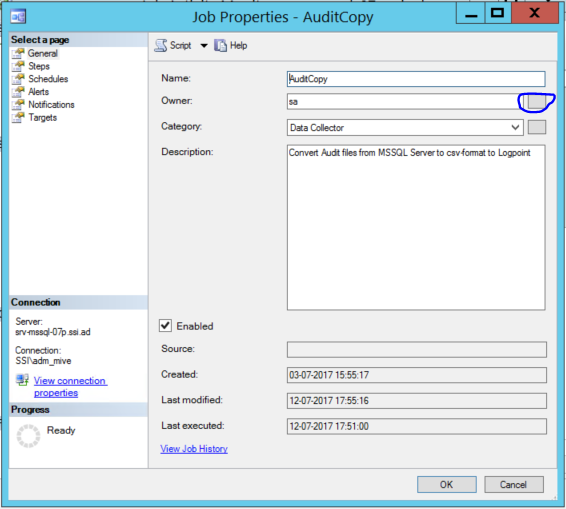
Owner:

(klik for select login,

skriv sa,

Check Names,

OK)



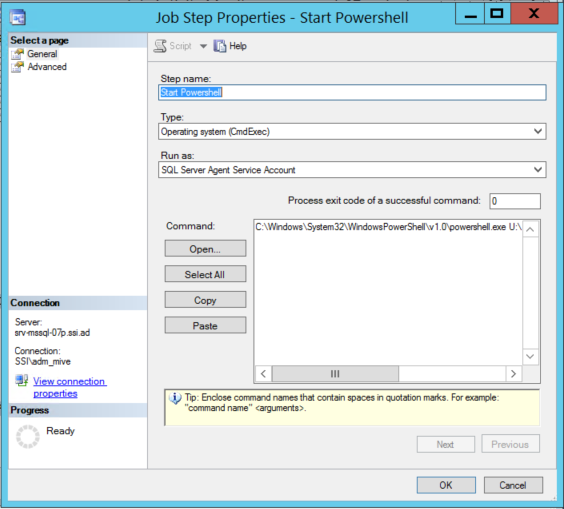
Name: AuditCopy

Category:

Data Collector

Description: Convert Audit files from MSSQL Server to csv-format to Logpoint

Steps: New



Step Name:

Start PowerShell

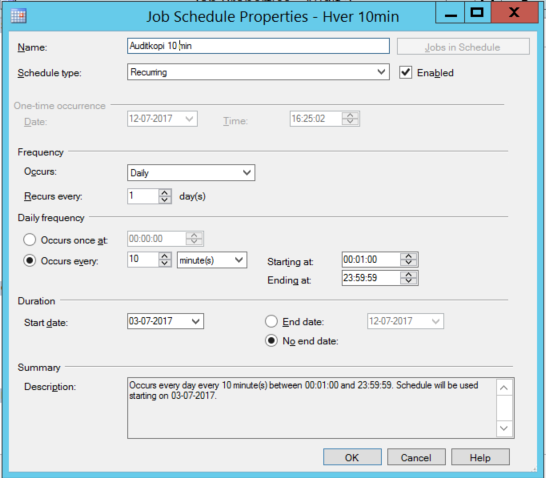
Type: Operating system (CmdExec)

Run as: SQL Server Agent Service Account

Command: (ombyt stien til -.ps1 filen med den aktuelle og indsæt under command som 1 linie)

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe U:\System\MSSQL\MSSQL11.MSSQLSERVER\MSSQL\Audit\auditexport.ps1

Tryk Ok



Schedules: New

Navn:

Auditkopi 10 min

Occours: Daily

Recours every 1 Days

Daily Frequency:

Occours every: 10 min.

Starting at 00:01:00

Start date: nu

No end date

Ok

### Konverteringsjob via Task Scheduler (Skal IKKE bruges)

Forbered Automatisk kørsel.

Start Task scheduler

\Task Scheduler library \Microsoft

Actions: Create task:

General: Name=Description: MSSQL Audit log export til Logpoint

General: check Run whether user is logged in or not

Triggers: new, start 00:04:33 daily, Recur 1 days, repeat task every 10 min. for duration 1 day

Actions: New

Start a program – Powershell

Add arguments: -noprofile -file u:\<path>\Audit\auditexport.ps1

Settings: "if already running......" Stop the existing instance

General: Change user or Group: --> svd\_sql\_xxxx

Tryk ok for password (from Secret Server)

Test Task ved at trytkke Run. (f5 eller højreklik task)

### Logpoint opsætning:

NB.: man kan ikke redigere ”.conf” med notepad. (Kopier evt. til skrivebord, og åbn med wordpad)

1. Tilret C:\Program Files (x86)\nxlog\conf\nxlog.conf

Tilføj nederste linie:

include %CONFDIR%\Custom\_mssql.conf

<Output logcontents> sektion og <Output agentlog> sektion

Host logpoint rettes til ip-adresse se nedenfor

1. Tilret C:\Program Files (x86)\nxlog\conf\Custom\_mssql.conf

Basedir skal pege på u:…\audit\logpoint folderen

<Output out\_mssql> sektion

Host 192.168.39.16 rettes til nyeste (09t: Host 192.168.33.12)

1. Genstart nxlog service

Kontroller ved at åbne C:\Program Files (x86)\nxlog\data\nxlog (dobbeltklik)

Skal gerne slutte med noget der ligner:

2017-06-27 11:21:51 INFO nxlog-3.0.1714 started

2017-06-27 11:21:51 INFO connecting to 192.168.33.12:514

1. Hvis problem med nxlog service

Under installation: kontakt tskj

I drift: mail: [Support@logpoint.com](mailto:Support@logpoint.com)

1. Kan testes med ”telnet 192.168.33.12 514” fra cmd
2. På logpoint kan søges med device\_name="forskermssql" | chart count() by device\_name, label order by label efter valg af “Last 7 days” og evt. audit\_db repository

På systemkataloget \servere\<servernavn> tilrettes Siemz overskrift til ”audit-logs, oper-logs” når disse virker.

# Regler

## Registerregistrering

Jeg er dog nødt til, i henhold til de nye regler, at spørge om der er personfølsomme data i Influenza\_2013\_2014 og i den nye database: BN\_RSV, og om der er en registerregistrering overfor Datatilsynet af disse?

## Systemregistrering

Jeg vil anbefale at du opretter dit system som system i systemkataloget, så vi fremover ikke behøver at lede efter ejerskab, og det vil samtidigt gøre det lettere for dig at få hjælp fra servicedesken.

For at få oprettet et system i systemkataloget, skal systemforvalter sende en mail til Servicedesk der indeholder følgende:

* Systemnavn (Det navn flest mennesker kender systemet under): f.eks. Bedre sundhed i generationer
* Kort navn / alias f.eks. BSIG
* Systemkategori f.eks. Sundheds-it
* Systemejer (Endelig beslutningstager)
* Systemforvalter (daglig administration)
* Teknisk ansvarlig / udvikler
* Data / Ressource ansvarlig, (kan tildele adgange, og bemyndige rettelser.):
* Kort beskrivelse af systemets formål (til brug for oversigten)
* Kunder
* Evt. baggrund og tilhørsforhold.
* Evt. servere, applikationer & databaser der hører til under systemet.

Følgende kategorier kan anvendes:

• Sundheds-it

• Forvaltnings-it

• Produktions-it

• Basis-it

Hvis du har spørgsmål, forslag eller kommentarer, er du velkommen til at kontakte os.

Du kan også grund-registrere dit system, og så tilføje yderligere oplysninger på et senere tidspunkt.

Roller kan skiftes efter behov.

# Systemer og Brugere:

## AD:

Ssi.ad\MiVe Normal bruger der ikke må have systemadgang

dksund.dk\MiVe Normal bruger Ssi.ad\MiVe repliceret til dksund.dk

dksund.dk\adm\_mive Administrator 0 bruger med udvidede privilegier på DKSUND domænet.

Ssi.ad\adm\_mive Administrator 1 bruger med udvidede privilegier på SSI domænet.

Sst.dk\adm\_mive Administrator 2 bruger med udvidede privilegier på SST domænet.

intdmz.dk\adm\_mive Administrator 4 bruger med udvidede privilegier på intdmz domænet.

pubdmz.dk\adm\_mive Administrator 5 bruger med udvidede privilegier på pubdmz domænet.

Ssidmz01.local\adm\_mive Administrator 6 bruger med udvidede privilegier på Ssidmz01.local domænet.

imkit.dk\adm\_mive Administrator 7 bruger med udvidede privilegier på imkit domænet.

nsidsdn.dk\adm\_mive Administrator 8 bruger med udvidede privilegier på nsidsdn domænet.

dksundtest.dk\adm\_mive Administrator 9 bruger med udvidede privilegier på DKSUNDTEST domænet.

## SAP: (bestilling af ressourcer)

## Nilex (til sagsstyring):

MIVE

## Check\_MK (Server / system monitorering):

MIVE

## Exchange / Outlook / Skype:

< dksund.dk\MiVe>

[mive@sundhedsdata.dk](mailto:mive@sundhedsdata.dk) Mail bruger i postsystemet.

IoS – Infrastruktur og Support Mailingliste.

## HP / IMC: http://imc.ssi.ad:8080

Adm\_mive Bruger til Styring / overvågning af netværket

## VmWare:

adm\_mive@ssi.ad Vmware administrator på https://vcenter01.ssi.ad/ui

## Citrix:

## Siemz:

Ssi\mive

## SecretServer: https://secretserver.dksund.dk/Login.aspx

Ssi\mive

## Sas Analyse:

mive@saspw Bruger til management console sasanalyse.sst.dk

mive@saspw Bruger Til Management console sasprod01.sst.dk

# System Opsætning

### Service Vinduer

Ændring af eksisterende servere foretages bedst i aftalt servicevindue.

Link til service vindue liste: https://srv-inf-sccm.ssi.ad/Reports/report/SCCM/\_Custom%20Reports/Maintenance%20Window%20Overview

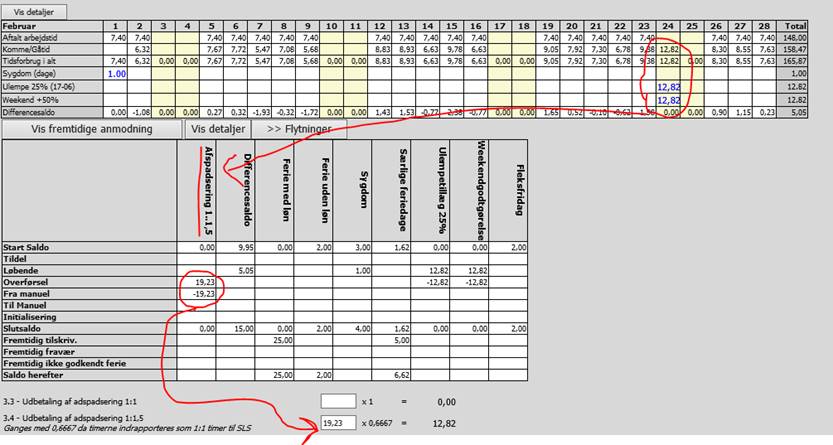
Specielle aftaler kan aftales med berørte systemejere.

### Service Vindue tids registrering

MABZ var i tvivl om hvordan han registrerede servicevinduet i mTime.

Han har kontaktet HR og de sagde følgende:

1. Registrer komme/gå tid som ”*Beordret overarbejde”*
2. I opgørelsen kan i se jeres timer i tabellen med dagene. De bliver omregnet og vist i ”*Afspadsering 1..1,5”*



Når I skal godkende måneden, skal der nederst i 3.4, skrives et svarende beløb ind som der er repræsenteret i ”*Afspadsering 1..1,5”* Dette fjernes fra puljen og sendes til udbetaling.

1. Godkend som i plejer.

### Tilføj printere og scannere

Vælg Den printer jeg søger efter findes ikke på listen

Vælg Søg efter printer i kataloget, baseret på placering eller funktion

Navn = printernummer. Printer i IOS ved AO er 446

Check placering, og tryk ok

Evt. sæt som standardprinter.

### Printer Spool problemer

1)

net stop spooler

del %systemroot%\System32\spool\printers\\* /Q /F /S

net start spooler

2)

start Services.msc

find ”Print Spooler” - højreklik – vælg Properties.

General: Startup type Automatic

Recovery: First Failure + Second failure + Subsequent failures = Restart the service

General: Apply , Start , Ok

3)

Stop Spooler service (via services)

Start Kontrolpanel\Devices & Printers

Find, og højreklik på printeren:

Remove Printer

Start Spooler service (via services)

4)

Regedit

For 32 Bit PC:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Environments\Windows NT x86\Print Processors

For 64 bit PC:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Environments\Windows x64\Print Processors

Slet alle nøgler undtagen Winprint

Luk regedit

Genstart PC

## Fil lokationer:

G: hjemmedrev

H: hvl

I: Ios Afdelingsdrev

P: Installations filer & Diske

S: svl

U: uvl

## Bestilling af Ekstern Konsulent id / oprettelse af Bruger

### Krævede oplysninger:

Fornavn

Efternavn

Firma

Mobilnr.

eMail

Konsulentansvarlig

Afdelingschef

Adgang til h:, g:, SDS-email,Citrix

Begrundelse

Adm- Privilegier.

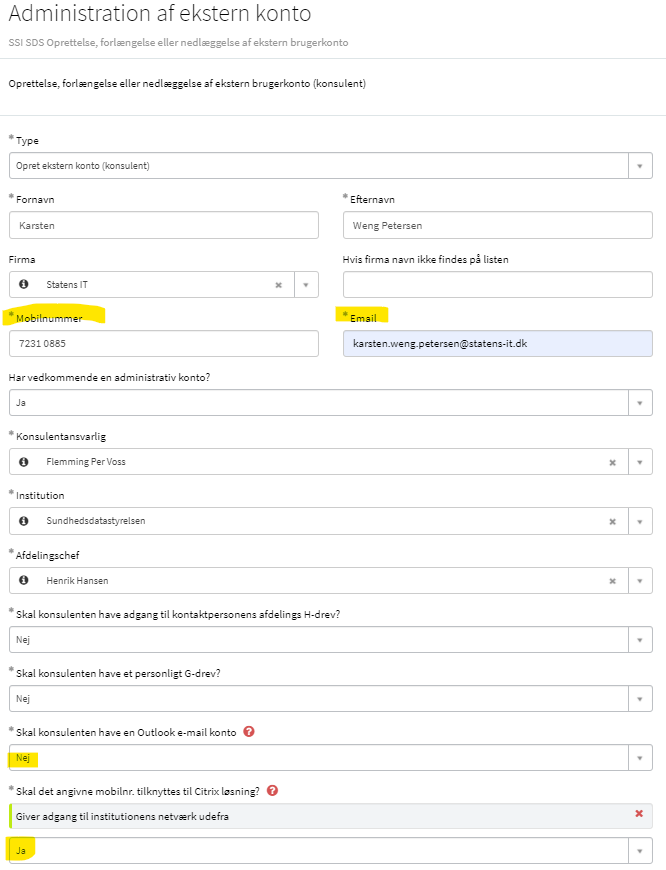
Underskrift fortrolighedsaftale

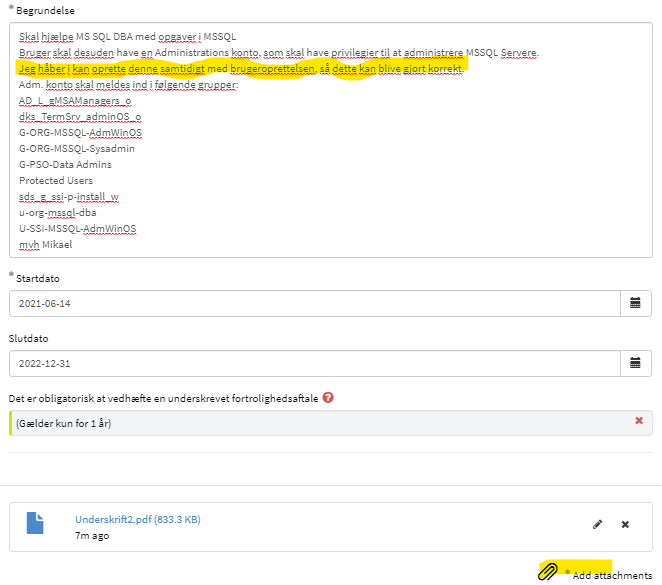
### Procedure:

[Forside - Serviceportal (service-now.com)](https://sds.service-now.com/serviceportal)

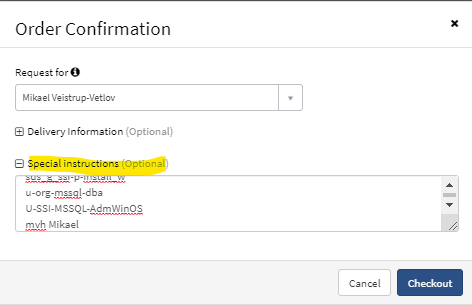
Anmod om adgang:

Administration af ekstern konto:





Tryk Order Now



jeg ved godt at Administrations konto, kan oprettes seperat, men for helhedens skyld ville det være rart at få denne oprettet samtidigt.

og Adm. konto skal meldes ind i følgende grupper:

AD\_L\_gMSAManagers\_o

dks\_TermSrv\_adminOS\_o

G-ORG-MSSQL-AdmWinOS

G-ORG-MSSQL-Sysadmin

G-PSO-Data Admins

Protected Users

sds\_g\_ssi-p-install\_w

u-org-mssql-dba

U-SSI-MSSQL-AdmWinOS

mvh Mikael

Tryk Checkout

Noter Req / ritm nr til opfølgning.

Efter oprettelsen skal du aktivt ind i Servicenow, og hente oplysninger om brugerid & Password, og sende til bruger.

### Ekstern Bruger login via Citrix

Du skal så logge på med din normale <eks\_> bruger via en browser, hvor du angiver adressen login.dksund.dk

Du bliver bedt om at skifte password 1. gang.

Her får du adgang til en stribe Citrix Applikationer, bl.a. MS SQL Server Management Studio

De fleste applikationer skal startes som en anden bruger; din adx\_ bruger.

Da vi ikke har single logon, skal du første gang, skifte password på din adx\_bruger evt. via Change Password app.

De fleste servere kan tilgås direkte via citrix applikationer (run as different user: <adx\_> bruger) nogle få skal der bruges jumphost, nærmere detaljer aftales senere.

## MSSQL Server Opsætning

### Lokal Brugere

Tsmoperator ?

### Administrators group

SSI\Domain Admins

SSI\GRP-RGH-SCCMClientPush

SST.dk\GRP-360-AdminOgRemoteAdgang ?

SSI\GRP-RGH-TSMOperator

SSI\L-SSI-MSSQL-AdmWinOS

SSI\L-WinSRV-AdmOS

SSI\LyncMonitorService ?

SSI\MSSQLServerAdms

SSI\ TSMOperator ?

Tsmoperator ?

### Instance Logins

NT AUTHORITY\SYSTEM Sysadmin (/ Public?)

NT SERVICE\MSSQLSERVER Sysadmin

NT SERVICE\SQLSERVERAGENT Sysadmin

SSI\check\_mk Public vSphere\_VC\_DB

SSI\MSSQLServerAdms Sysadmin

SST.DK\TSMoperator Sysadmin

NT SERVICE\ReportServer Public Master(RSExecRole), msdb(RSExecRole, SQLAgentOperatorRole, SQLAgentReaderRole, SQLAgentUserRole)

NT SERVICE\SQLWriter Sysadmin

NT SERVICE\Winmgmt Sysadmin

NT SERVICE\MSSQLServerOLAPService ? Public BI\_xxxxxx datareader

## Mail opsætning på SQL Server

Opret profil

Opret agent

Bruger skal være medlem i rollen:

EXEC msdb.dbo.sp\_addrolemember @rolename = 'DatabaseMailUserRole'

,@membername = 'ssi\tbr';

GO

## SQL Principals

Principals are entities that can request SQL Server resources. Like other components of the SQL Server authorization model, principals can be arranged in a hierarchy. The scope of influence of a principal depends on the scope of the definition of the principal: Windows, server, database; and whether the principal is indivisible or a collection. A Windows Login is an example of an indivisible principal, and a Windows Group is an example of a principal that is a collection. Every principal has a security identifier (SID). This topic applies to all version of SQL Server, but there are some restictions on server-level principals in SQL Database or SQL Data Warehouse.

### SQL Server-level principals

SQL Server authentication Login

Windows authentication login for a Windows user

Windows authentication login for a Windows group

Azure Active Directory authentication login for an AD user

Azure Active Directory authentication login for an AD group

Server Role

Database-level principals

Database User (There are 11 types of users. For more information, see CREATE USER.)

Database Role

Application Role

### sa Login

The SQL Server sa log in is a server-level principal. By default, it is created when an instance is installed. Beginning in SQL Server 2005, the default database of sa is master. This is a change of behavior from earlier versions of SQL Server. The sa login is a member of the sysadmin fixed database role. The sa login has all permissions on the server and cannot be limited. The sa login cannot be dropped, but it can be disabled so that no one can use it.

dbo User and dbo Schema

The dbo user is a special user principal in each database. All SQL Server administrators, members of the sysadmin fixed server role, sa login, and owners of the database, enter databases as the dbo user. The dbo user has all permissions in the database and cannot be limited or dropped. dbo stands for database owner, but the dbouser account is not the same as the db\_owner fixed database role, and the db\_owner fixed database role is not the same as the user account that is recorded as the owner of the database.

The dbo user owns the dbo schema. The dbo schema is the default schema for all users, unless some other schema is specified. The dbo schema cannot be dropped.

### public Server Role and Database Role

Every login belongs to the public fixed server role, and every database user belongs to the public database role. When a login or user has not been granted or denied specific permissions on a securable, the login or user inherits the permissions granted to public on that securable. The public fixed server role and the public fixed database role cannot be dropped. However you can revoke permissions from the public roles. There are many permissions that are assigned to the public roles by default. Most of these permissions are needed for routine operations in the database; the type of things that everyone should be able to do. Be careful when revoking permissions from the public login or user, as it will affect all logins/users. Generally you should not deny permissions to public, because the deny statement overrides any grant statements you might make to individuals.

### INFORMATION\_SCHEMA and sys Users and Schemas

Every database includes two entities that appear as users in catalog views: INFORMATION\_SCHEMA and sys. These entities are required for internal use by the Database Engine. They cannot be modified or dropped.

Certificate-based SQL Server Logins

Server principals with names enclosed by double hash marks (##) are for internal system use only. The following principals are created from certificates when SQL Server is installed, and should not be deleted.

##MS\_SQLResourceSigningCertificate##

##MS\_SQLReplicationSigningCertificate##

##MS\_SQLAuthenticatorCertificate##

##MS\_AgentSigningCertificate##

##MS\_PolicyEventProcessingLogin##

##MS\_PolicySigningCertificate##

##MS\_PolicyTsqlExecutionLogin##

These principal accounts do not have passwords that can be changed by administrators as they are based on certificates issued to Microsoft.

### The guest User

Each database includes a guest. Permissions granted to the guest user are inherited by users who have access to the database, but who do not have a user account in the database. The guest user cannot be dropped, but it can be disabled by revoking it's CONNECT permission. The CONNECT permission can be revoked by executing REVOKE CONNECT FROM GUEST; within any database other than master or tempdb.

### Login

Et login er defineret på Instans niveau, og givere adgang til og privilegier på hele instansen. Her gives de overordnede privilegier, samt opsætningsmæssige parametre.

Adgangen kan tildeles lokale brugere, Domæne brugere, Domæne grupper og SQL Server authenticated konti.

Vi foretrækker AD grupper til burger logins.

### Credential

A credential provides a mechanism to store login information for a domain account within SQL Server. The credential can then be used to pass that authentication information into another login or a proxy to grant it permissions to resources external to SQL Server.

### User

En bruger (User) oprettes på database og giver privilegier & roller til databasen & til data i denne. Vi opretter typisk data læsnings grupper (\_r) læsning & skrivnings grupper (\_w), udviklings grupper ((\_d) og ejer grupper (\_o) til en database. Ejeren må alt, inkl. at slette databasen, men IKKE genoprette denne. Udvikleren har ddladmin & execute rettigheder, og kan derved ændre struktur og opsætning af databasen, men ikke slette den.

### Brug af Login

Hvis du vil tilgå en MS SQL Instans \ Database, har du brug for et Login til SQL Server Instansen, via en AD Gruppe. Dette login bliver knyttet til en eller flere Databaser, hvor den samme bruger (User) er defineret.

Dette er vejen, hvis du skal tilgå data og database.

### Use of credentials

Credentials get brought in when permissions from domain users need to be granted to accounts or services that wouldn’t usually have those permissions. For instance, if an assembly required EXTERNAL\_ACCESS, those permissions could be granted through the use of a credential. Credentials can also be used to grant SQL Authentication accounts access to external resources.

### Gruppe login & individual DataBase User.

Der er en speciel situation hvis du skal tilgå en database via en gruppe, men med ekstra / anderledes privilegier I forhold til resten af gruppen.

Login til gruppen oprettes normalt, bruger privilegier til gruppen oprettes normalt, du meldes ind i gruppen, og efter en logoff & logon (disconnect virker ikke, da AD-gruppeprivilegier træder i kraft ved windows logon) kan du tilgå databasen med samme privilegier som resten af gruppen.

Nu opretter vi en individuel database-bruger der giver anderledes privilegier, f.eks. db\_ddladmin.

Denne ekstra privilegie virker når bruger har disconnectet fra databasen og connectet igen (eller næste afsluttede kørsel) da der ikke er tale om ad-tilknytninger.

Denne bruger SKAL oprettes via t-sql, da der ikke er nogen login med samme navn, kun gruppe login. F.eks.

USE [db-navn]

GO

CREATE USER [dksund\mive] FOR LOGIN [DKSUND\MIVE] WITH DEFAULT\_SCHEMA=[dbo]

GO --Husk schema=dbo for ikke at rydde op I ekstra schemaer.

--ALTER ROLE [db\_datareader] ADD MEMBER [dksund\mive] -- ikke nødvendig, har fra gruppen

--GO

--ALTER ROLE [db\_datawriter] ADD MEMBER [dksund\mive] -- ikke nødvendig, har fra gruppen

--GO

ALTER ROLE [db\_ddladmin] ADD MEMBER [dksund\mive]

GO

Husk at DENY privilegier er destruktive, og forhindrer uanset hvilke andre privilegier der er aktive, mens ALLOW er positive og supplerer andre privilegier

Dette virker også ved f.eks. ”Grant create table” eller ”Grant Execute”

# Analyse af server

## PSTOOLS

[\\tsclient\P\SQLDBA\PsTools.zip](file://tsclient/P/anjeT2/PsTools.zip)

Udpakkes til lokaldrev, f.eks. c:\install

Open File lokation af SQL management studie

Åbn Powershell som administrator

Skift til udpakningssted: cd \install\pstools\pstools

**.\psexec -i -s "D:\MSSQLSERVERx86\120\Tools\Binn\ManagementStudio\Ssms.exe" #eller**

**.\psexec -i -s "R:\Systemx86\110\Tools\Binn\ManagementStudio\Ssms.exe"**

Tryk Agree

# Check\_MK Serverovervågning

## Check\_MK Klient til Server og Registrering I Check\_MK

Åbn Check\_MK \ Hosts \ New Host

Skriv Host navn

Oftest anvendt \ Agent type: check MK Agent ( + SNMP hvis fysisk)

\Serverrum Artillerivej 5 anywhere (hvis virtuel), ellers direkte

\OS famillie: Windows

Server Karakteristika: Prod/test System

Save and go to Services

* Discovery failed, ingen Check\_MK agent installeret eller firewall eller stavefejl.

Log på Server

Check Services ingen Check\_MK agent

[\\tsclient\P\check\_mk\client\windows](file://tsclient/P/check_mk/client/windows)

Kopier klient til desktop

Installer, next agree mm.

Check Firewall \inbound rules agent skal findes.

Check\_MK retry discovery

Save manual check Configuration

Changes

Activate Changes

Vent

Quick

## Check\_MK Overvågning

### Typiske Alarmer

Fix – det

Lav Sag til

1. Haiba Kuben er for gammel: Sag til Systemforvalter MLH (Malene Haahr), abonnenent til KSN & KRM, sagstype: Fejlhåndtering, Kategori: fagsystem – Haiba, Pri:3;

Hvis der ikke er nogen der kan kontaktes, Ring til den Kundeansvarlige: JETC og spørg hvordan vi kommer videre

Check\_MK: Server\ Service\  Kommentar: Sag oprettet til sagsforvalter, tryk Acknowledge, godkend

1. Fejlede workflows på srv-cap-sumin1.sst.dk: Søg / find server i systemkatalog (hele navnet –uden domæne) Sag til Systemforvalter KIAP, sagstype: Fejlhåndtering, Kategori: fagsystem – ?, Pri:3;

Check\_MK: Server\ Service\ 🛠 Kommentar: Sag oprettet til sagsforvalter, tryk Acknowledge, godkend

Sag til Systemforvalter:

1. Hvis man modtager en sag med beskrivelse som: Services of Host <sql server navn>

Der er en masse alarmer på div. Databaser

Der er typisk et Check\_MK link med der viser en Check\_MK side med rene Grønne ikoner:

Her kan svares:

Jeg kan desværre ikke gøre noget, Det hele er i grønt igen, og det er nogle alarmer, der ALTID går i sig selv igen.

Det drejer sig om Check\_MK der ikke venter længe nok på at SQL skal svare tilbage, og derefter sender en ny forespørgsel afsted til SQL så flere forespørgsler snubler over hinanden, og spænder ben for hinanden, så der kommer nye fejl.

Jeg har spurgt Check\_MK gruppen om der er noget de kan gøre, men ikke fået nogen løsning, så jeg lukker desværre denne sag.

mvh xxxxx

Reboot af Windows server

Før

0. opret Standard Change ”Reboot af Windows server.docx”

1. Check serveren i Server-listen (Servertype, AD/Workgroup, Afhængige systemer,…)

2. Find evt. Local Administrator login i LAPS eller Secretserver

3. Check om andre medarbejder er logget på serveren i ”Task Manager”

4. Planlæg Reboot med driftansvarlig eller Systemforvalter i ”Afhængige systemer”

5. Check status i Check\_MK – alerts

6. Giv besked til Check\_MK vagten at server genstartes.

Under

1. Restart serveren

2. Ping serveren: [ping servernavn -t]

3. Check status i Check\_MK indtil alle målepunkter bliver grønne

Efter

1. Check status i Check\_MK

2. Check Server Manager at alle Services er i luften

3. Hvis noget driller, så check detaljer i ”Event Loggen”

4. Informer evt. Systemforvalter at reboot er succesfuld

5. opret Emergency change

Ved punkt 0 før, eller 5. efter:

Standard Change: "Reboot af Windows server.docx"

[https://sektornet/nsi/systemkatalog/Lists/Standard%20Changes/DispForm.aspx?ID=96&Source=https%3A%2F%2Fsektornet%2Fnsi%2Fsystemkatalog%2FLists%2FStandard%2520Changes%2FAllItems%2Easpx%23InplviewHashe0ac79e7%2Dcae2%2D4c35%2D8a94%2Dd3b37f827beb%3DFilterField1%253DAuthor%2DFilterValue1%253DSteen%252520N%2525C3%2525B8rgaard%252520Thomsen&ContentTypeId=0x0100C21019E2EEB20F4C83996A5AFE743F90](https://sektornet/nsi/systemkatalog/Lists/Standard%20Changes/DispForm.aspx?ID=96&Source=https://sektornet/nsi/systemkatalog/Lists/Standard%2520Changes/AllItems.aspx%23InplviewHashe0ac79e7-cae2-4c35-8a94-d3b37f827beb%3DFilterField1%253DAuthor-FilterValue1%253DSteen%252520N%2525C3%2525B8rgaard%252520Thomsen&ContentTypeId=0x0100C21019E2EEB20F4C83996A5AFE743F90)

# SQL Funktioner

## Log Check / Syslog-Analyse

### Adgang til Syslog

Brug en SSH-klient (såsom Putty) til at logge på serveren "syslog". Brugernavn: Éns normale (ikke-administrator) SSI.AD brugernavn. Kodeord: Éns normale SSI.AD kodeord. Hvis man bliver afvist, kan det være fordi, at man mangler at være medlem af en relevant AD-gruppe (se adgangsregler til serveren sis på host notes for srv-mon2).

Serveren gemmer syslog-beskeder i /var/log/messages; denne fil omdøbes en gang ugentligt. Derfor vil /var/log/messages nogle gange være ret lille; andre gange meget stor. Ældre filer findes også i /var/log kataloget og hedder noget i stil med messages-20150824.gz (roteret 24. august 2015 og gzip-komprimeret).

SNMP-traps konverteres til syslog-beskeder og findes dermed også i /var/log/messages.

Søgninger i syslog

Om "grep"

Når man søger i tekstfiler, er en afart af grep-værktøjet næsten altid i spil. To vigtige afarter:

•fgrep: En variant, hvor søgestrengen opfattes helt bogstaveligt. Således er der ingen tegn, som har særlig betydning. God (og ekstra hurtig) til simple søgninger.

•egrep: En variant, hvor søgestrengen opfattes som et udvidet regulært udtryk (extended regular expression), dvs. hvor visse tegn har særlig betydning. God til mere avancerede søgninger.

For alle varianter gælder, at man kan give argumentet "-i", hvorefter de vil søge på case insensitive facon.

Linjeformatet i /var/log/messages

På syslog-serveren er det konfigureret således, at hver syslog-besked afføder en linje såsom flg:

2015-08-24T11:42:42.333656+02:00 2015-08-24T11:42:42+02:00 sisp2 192.168.43.12 sshd[3713]: Accepted publickey for trar from 10.30.7.44 port 49466 ssh2

Hver linje består af et antal felter adskildt af et mellemrum:

|  |  |  |
| --- | --- | --- |
| **Element​** | **​Eksempel** | **​Betydning** |
| ​1 | ​2015-08-24T11:42:42.333656+02:00 | ​Tidsstempel i følge syslog-serveren. |
| ​2 | ​2015-08-24T11:42:42+02:00 | ​Tidsstempel i følge afsendende host (bør normalt tilsvare det andet tidsstempel; men der kan være ure på udstyr, som går forkert). |
| ​3 | ​sisp2 | Hostnavn for afsendende host. Hvis dette ikke indikeres af afsendende system, vil der blot stå en IP-adresse (dvs. ligesom efterfølgende kolonne).​ |
| ​4 | ​192.168.43.12 | ​IP-adresse for afsendende host. |
| ​Resten | sshd[3713]: Accepted publickey for trar from 10.30.7.44 port 49466 ssh2 | Syslog-besked i varierende format. Hvis der er tale om en SNMP-trap, vil dette felt starte med strengen "snmptrapd".  Nederst på formularen |
|  |  |  |

Eksempler

•Find beskeder, som indeholder strengen "10.200.30.170":

fgrep 10.200.30.170 /var/log/messages

•Find beskeder, som omhandler captiadb11-serveren:

egrep -i 'captiadb11|192\.168\.208\.43' /var/log/messages

Bemærk pipe-tegnet (|), som i regulære udtryk betyder "eller". Bemærk også, at punktummerne er escaped med backslash, fordi punktum i regulære udtryk ellers har en særlig betydning (som joker-tegn).

Her er valgt at søge på både hostnavn ("captiadb11") og dennes IP-adresse (192.168.208.43), fordi vores DNS-setup desværre har nogle huller, som kan forstyrre navne-/adresseopslag.

•Ovennævnte giver desværre en del uinteressant støj, som nogen egentlig burde undersøge og få fjernet grunden til, men som vi nu og her gerne vil se bort fra:

egrep -i 'captiadb11|192\.168\.208\.43' /var/log/messages | egrep -v 'ICMP echo request|AUDIT\_FAILURE An account failed to log on|The COM\+ Event System failed'

Bemærk de to grep-kommandoer, som er knyttet sammen af en pipe (|). "-v" betyder omvendt match, dvs. at vi gerne vil se ting, som ikke match'er.

Bemærk også, at plus-tegnet i anden grep-kommando er escaped, fordi plus-tegnet i regulære udtryk har særlig betydning ("ét eller flere af foregående tegn").

•Se første linjer i messages-filen (giver indtryk af, hvor mange dage tilbage, filen dækker):

head /var/log/messages

•Vi vil se, hvilket IP-adresser, som firewalls har set sig gale på og derfor har blokeret (shunned) i en periode:

fgrep -i shunned /var/log/messages

Hvilket fx. giver en linje såsom:

2015-08-25T16:03:22.506461+02:00 2015-08-25T16:03:22+02:00 10.100.0.1 10.100.0.1 %ASA-4-401004: Shunned packet: 10.10.7.69 ==> 191.232.139.254 on interface inside

•Ovenstående giver i skrivende stund desværre mange hits (hvilket nogen burde gøre noget ved). Vi vil derfor gerne se, hvilket adresser, som ofte bliver shunned:

fgrep -i shunned /var/log/messages | cut -d ' ' -f 8 | sort | uniq -c | sort -r -n

Ovennævnte indeholder 5 kommandoer; kommentarer til visse af disse:

cut -d ' ' -f 8: Giv mig 8. kolonne, hvor kolonner adskilles af et mellemrum

uniq -c: Optæl antal unikke strenge; kræver, at det indkommende er sorteret

sort -r -n: Sortér teksten i omvendt rækkefølge (-r); sorteringen skal ske numerisk (-n)

Resultat:

1030 10.10.7.69

73 192.168.69.23

Hvilket betyder, at 10.10.7.69 blev shunned 1030 gange, mens 192.168.69.23 blev shunned 73 gange.

•Find tekst i en roteret+komprimeret messages-fil:

zcat /var/log/messages-20150816.gz | egrep -i 'malware|virus|worm' | egrep -v 'WMI instance|Endpoint Protection client is up and running in a healthy state'

I ovennævnte er tre kommandoer pipe'et sammen; nogle kommentarer hertil:

- zcat betyder dekomprimér og "spyt ud"

- første egrep isolerer potentielt interessante ord

- anden egrep fjerner noget irriterende støj

Andre muligheder

Man kan et "live feed" fra syslog vha. flg. kommando:

tail -f /var/log/messages

- Men dét vil give voldsomme mængder meddelelser, som antagelig vil være værdiløst. Og filtre bliver her interessante. Man kan selv skrive filtre, hvis man vil, men man kan også gøre brug af et eksisterende filter:

Eksisterende filtre

•Bortfiltrerer de fleste kendte underligheder:

tail -f -n 500000 /var/log/messages | /usr/local/bin/syslog-filters/trar-general-1

"tail -f -n 500000" betyder "spyt de sidste 500000 linjer fra filen ud og følg derefter nye linjer".

•Et mere specifikt filter kigger efter tegn på malware:

cat /var/log/messages | /usr/local/bin/syslog-filters/trar-malware-1

"cat" betyder "udspyt indholdet af filen".

Hvis man vil se, hvad nævnte filtre gør, kan man fx. kigge i dem med følgende kommando:

mcedit /usr/local/bin/syslog-filters/trar-general-1

(Man hopper ud af mcedit igen ved at trykke to gange på escape-knappen.)

## Auditing / Logning på MSSQL Server

### MSSQLer her i SDS:

Alle Enterprise MSSQL server kan auditlogge, og jeg har et script der kan sætte det op så de logger korrekt; og jeg har et testscript der afvikler de basale hændelser der er krav til hvad der skal logges og et review script viser at auditeventsne kommer i loggen.

Opsætning af Auditlog:

Gå på SQL server instans

Åbn Security\Audit

Hadoop (aka. Sundheddatasplatformen):

Bagved softwaren ligger en et par MSSQL servere og en Postgress database.

Postgress har fine auditlogningsmuligheder (af hvad jeg har hørt) og MSSQL’en (som vi har købt som en service der kan logge; så vi stiller ikke yderligere krav) tester vi på bagkant når de siger de er parat til at lukke os ind med det ovennævnte testscript og review script at logningen virker. Hvordan det så skal samles op og overføres til logpoint er jeg ved jeg ikke om.

I MSSQL auditlogning serverauditspecification kan bindvariable kaldte værdier og storedprocedurekalds parametre fanges med SCHEMA\_OBJECT\_ACCESS\_GROUP og SCHEMA\_OBJECT\_CHANGE\_GROUP.

Microsofts overview af ServerAUDITSpecification kan finds her; om end googling på de specifike emner andre steder end MS giver meget bedre information. https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions

## Kontaktpersoner:

|  |  |  |  |
| --- | --- | --- | --- |
| **EMNE** | **ANSVARLIG MEDARBEJDER** | **MAIL** | **INITIALER PÅ AFSNITSLEDER** |
| Abortregister | Christian Theodor Ulrich | CHTU@ssi.dk | HEMH |
| Afregning | Anne Bernth | ANNB@ssi.dk |  |
|  | Lars Falsted Karlsen | LAFK@ssi.dk |  |
| Beskæftigelse på sundhedsområdet | Ditte Trier-Poulsen | DTP@ssi.dk | ANNB |
| Børnedatabase | Thomas Tjørnelunde Nielsen | THTN@ssi.dk |  |
| Cancerregister | Maya Christel Milter | MACH@ssi.dk | HEMH |
|  | Margit Rasted | MACR@ssi.dk |  |
|  | Milan Fajber | , MIFA@ssi.dk |  |
| CPR-register | Thomas Tjørnelunde Nielsen | THTN@ssi.dk | HEMH |
| Diabetesregister | Katrine Facius | KAFA@ssi.dk | ANNB |
| DREAM - Beskæftigelsesministeriets forløbsdatabase | Christian Theodor Ulrich | CHTU@ssi.dk | HEMH |
| Dødsårsagsregister - Legalisering | Claudia Ranneries, | CLRA@ssi.dk, | HEMH |
| - Kopi af dødsattest - Danskere | Lis Lykke Warner, | LLW@ssi.dk |  |
| døde i udlandet - Udlændinge | Kirsten Stahr, | KIAS@ssi.dk, |  |
| døde i DK - Forsikringssager | Milan Fajber | MIFA@ssi.dk, |  |
|  |  | d-attest@sst.dk |  |
| DRG-takster | Sanne Blenstrup Raun Østergaard | DRGtakster@ssi.dk | ANAN |
| EOJ - elektronisk omsorgsjournal | Christian Theodor Ulrich | CHTU@ssi.dk | HEMH |
| Sundhed.dk/ eSundhed - data på | Anne Bernth | eSundhed@ssi.dk | LARH |
| eSundhed (spørgsmål af mere |  |  |  |
| generel karakter) Private skal |  |  |  |
| have standardsvar |  |  |  |
| Egenaccess - køb af medicin | Lene Kokholm | medicindata@ssi.dk | JAKP |
| Fordelingsregnskab | Sanne Blenstrup Raun Østergaard | SBRO@ssi.dk | ANAN |
| Fremadrettede ventetider (indberetning - NIV) | Emil Nygaard Jørgensen (EMNJ) | venteinfo@ssi.dk | ANNB |
| Fællesindhold (for | Anne Reuss | anre@ssi.dk | ANAN |
| basisregistrering af sygehuspatienter) |  |  |  |
| Fødselsregister | Christian Theodor Ulrich | CHTU@ssi.dk |  |
|  |  |  |  |
| Grupperingslogik | Annsofie Kocemba | kliniskvalidering@ssi.dk | ANAN |
|  | Katarina Bjerg-Holm, |  |  |
|  | Elisabeth Faber Weinreich |  |  |
| Datagrundlag til afregning | Anne Bernth, | ANNB@ssi.dk, | ANNB |
|  | Lars Falsted Karlsen, | LAFK@ssi.dk |  |
| Hårdest belastede stofmisbrugere | Claudia Ranneries | CLRA@ssi.dk | HEMH |
| (HBS) - projekt |  |  |  |
| Implantatregister | Sanne Blenstrup Raun Østergaard | SBRO@ssi.dk | ANAN |
| Interaktiv DRG | Annsofie Kocemba |  | ANAN |
|  | Katarina Bjerg-Holm, | kliniskvalidering@ssi.dk |  |
|  | Elisabeth Faber Weinreich |  |  |
| Injicer bar heroin og metadon | Claudia Ranneries | CLRA@ssi.dk | HEMH |
| (IHM-databasen) |  |  |  |
| IVF-register (kunstig befrugtning) | Maya Christel Milter | MACH@ssi.dk | HEMH |
| Kronikerregister | Katrine Facius | KAFA@ssi.dk | ANNB |
| Kritisk sygdom | Lise Kristine Højsgaard Schmidt | LIHS@ssi.dk | HEMH |
| Landspatientregister (LPR) - | Kristian Nielsen, | KRNI@ssi.dk, | ANNB |
| aktivitet på sygehuse | Erik Villadsen | ERV@ssi.dk |  |
| - Dusas | Kristian Nielsen | KRNI@ssi.dk | ANNB |
| - private sygehuse - MiniPas | Erik Villadsen | ERV@ssi.dk | ANNB |
| - psykiatri | Emil Nygaard Jørgensen | EMNJ@ssi.dk | ANNB |
| National alkoholbehandling (NAB) | Claudia Ranneries | CLRA@ssi.dk | HEMH |
| Omkostningsdatabasen | Sanne Blenstrup Raun Østergaard | SBRO@ssi.dk, | ANAN |
| Patientregistrering | Anne Reuss, | patientregistrering@ssi.dk | ANAN |
|  | Ole B. Larsen |  |  |
| Patologi-register | Milan Fajber | MIFA@ssi.dk | HEMH |
| Register over genoptræning | Thomas Tjørnelunde Nielsen | THTN@ssi.dk | HEMH |
| SEB nedlæggelser | Sundhedsdokumentation | Servicedesk |  |
| SEI - Sundhedsstyrelsens | Christian Theodor Ulrich | Chtu@ssi.dk | HEMH |
| Elektroniske indberetning | Helle Rejnhold Sørensen | HERS@ssi.dk |  |
| Stofmisbrugere i behandling (SIB) | Claudia Ranneries | CLRA@ssi.dk | HEMH |
| Sygesikringsregister | Lars Falsted Karlsen | LAFK@ssi.dk | ANNB |
| Tvang i psykiatrien | Emil Nygaard Jørgensen | EMNJ@ssi.dk | ANNB |
|  | Linda Saabye Kongerslev | LISK@ssi.dk |  |
| Vakanceregisteret (Esvat ) | Ditte Trier-Poulsen | DTP@ssi.dk | ANNB |
| Venteinfo |  | venteinfo@ssi.dk | HEMH |
|  | Christian Theodor Ulrich | CHTU@ssi.dk |  |
|  | Martin Barney Møller-Ern | MABM@ssi.dk |  |
| Visual DRG | Annsofie Kocemba | kliniskvalidering@ssi.dk | ANAN |
|  | Katarina Bjerg-Holm, |  |  |
|  | Elisabeth Faber Weinreich |  |  |
| Vævsanvendelsesregister | Linda Saabye Kongerslev | LISK@ssi.dk | ANNB |
| Yderregister | Ditte Trier-Poulsen | DTP@ssi.dk | ANNB |
| Forskerservice – generelle | SAF | forskerservice@ssi.dk | BIDR |
| henvendelser ifht forskerservice |  |  |  |
| Forskerservice – mere specifikke | SAF | Udtraek.forskerservice@sst.dk | BIDR |
| henvendelser vedr. registerudtræk |  |  |  |
| ifht Forskerservice |  |  |  |
| Fælles medicinkort/FMK | LEAR og HBAL | Servicedesk ATT: FMK | ABRA |
| Håndkøbsmedicin, | Peter Plinius Thomsen | PPT@ssi.dk | KAMG |
| indberetning/LMS detail | Dataleverancer & lægemiddelstatistik |  |  |
| Kodeønsker (Fx SKS kodeønske), | SOA/NSI- SOA | soaafdelingspost@ssi.dk | ABRA/BIDR |
| locationsnr.,klassifikation | afdelingspostkasse |  |  |
| Kritisk sygdom | Sundhedsdokumentation, |  | HEMH |
|  | Lise Kristine Højsgaard Schmidt | LIHS@ssi.dk |  |
| KØS | Lars Ryslander Holm | larh@ssi.dk | LARH |
|  | Stine Holm | stho@ssi.dk |  |
|  | Dataleverancer og Lægemiddelstatistik |  |  |
| eKommune/Tilfredshedsportalen | Hans Christian Riis | hacr@ssi.dk | LARH |
|  | Dataleverancer og Lægemiddelstatistik |  |  |
| Lægemiddelstatistik | Dataleverancer og Lægemiddelstatistik | medicindata@ssi.dk | KAMG |
| MEDSTAT.dk | Dataleverancer og Lægemiddelstatistik | medicindata@ssi.dk | KAMG |
| SDS Institutionspostkasse | NSI Institutionspostkasse | Kontakt@sundhedsdata.dk |  |
| (henvendelser til SDS) | (DIS kontaktperson) |  |  |
| SKS koder | SOA/NSI- SOA | soaafdelingspost@ssi.dk | ABRA/BIDR |
| afdelingspostkasse |  |  |  |
| Sundhedsanalyser (henvendelser | Sundhedsanalyser (HEJO | NSFsundhedsanalyser@sum.dk | MERH |
| til Sundhedsanalyser) | kontaktperson) |  |  |
| eSundhed (Ikke private – her | Dataleverancer og | esundhed@ssi.dk | LARH |
| gives standardsvar) | Lægemiddelstatistik |  |  |
| Virus på edb-systemer | IOS | servicedesk@ssi.dk | MIHA |
| Sundhedsdatastyrelsen | Sundhedsdatastyrelsen | kontakt@sundhedsdata.dk |  |
| Servicedesk | IT-servicemanagement- | miha@ssi.dk | MIHA |
|  | /processer |  |  |
| Infrastruktur | Netværk, | vara@ssi.dk | VARA |
|  | - Storage, |  |  |
|  | - Vitualisering |  |  |
|  | - Databaser, |  |  |
|  | - Entreprisearkitektur |  |  |
| Vidensplatforme | Microsoft, pc-platforme, | sbt@ssi.dk | SBT |
| WHO-FIC (Family og | Solvejg Bang | soaafdelingspost@ssi.dk | BIDR |
| International Classifications) |  |  |  |
| SNOMED CT | Palle G. Petersen | snomedct@ssi.dk | BIDR |
|  | Camilla Wiberg Danielsen |  |  |
| Begrebsbasen/Nationalt | Camilla Wiberg Danielsen | begrebssekretariatet@ssi.dk | BIDR |
| Begrebsarbejde for |  |  |  |
| Sundhedsvæsenet |  |  |  |
| IHE metadataprofil | Thor Schliemann | soaafdelingspost@ssi.dk | BIDR |
| Projektmodel, portefølje, | Mette Frimann Poulsen | mfp@ssi.dk | ABRA |
| projektledelse, PMO |  |  |  |
| FMK – trust/ | Marchen Lyngby | MCLY@ssi.dk | BIDR |
| Uberettigede opslag på FMK |  |  |  |
| SOR, Sundhedsvæsenets | SOA/NSI- SOA afdelings | soaafdelingspost@ssi.dk | BIDR |
| OrganisationsRegister, SOR-koder | postkasse Palle G. Petersen |  |  |
| Laboratoriedata, NPU koder, | Ulla Magdal Petersen, | labterm@ssi.dk | BIDR |
| Nationale kortnavne (NKN) | Helle Møller Johannessen, |  |  |
| Måleenheder generelt | Young Bae Lee Hansen |  |  |
| Lægemiddelterminologi | Kell Greibe | keg@ssi.dk | BIDR |
| Standardkatalog | Diana Reerman standarder@nsi.dk | BIDR |  |
| Referencearkitektur | Esben Dalsgaard soaafdelingspost@ssi.dk BIDR |  |  |
| Rådgivende udvalg for standarder | Pia Jespersen | soaafdelingspost@ssi.dk | BIDR |
| og arkitektur (RUSA) |  |  |  |
| Myndighedsspørgsmål vedr. |  | soaafdelingspost@ssi.dk | BIDR |
| standardanvendelse |  |  |  |
| Sundhedsdatastyrelsen | Sundhedsdatastyrelsen | kontakt@sundhedsdata.dk |  |
|  |  |  |  |

## Licenser

Kontakt Person:

Licens manager Søren Tøpholm

### Indkøb

Crayon Licens leverandør /konsulent / Sælger.

### Core Licenser

Hurtige CPU- få cores.

Kun udfyld ram slots 2/3 dele af performance hensyn

Server med SQL check antal core licenser

Bestil server, bestil også licens. oprettelse og 3 år licensiering og support

Hvis personhenførbare data kræver Enterprise server.

Pris ca. 125.000,- pr 2 kerner

Standard server ca. 60.000,-

Begge Min. 4 kerner på en server

Skal betale for alle kerner i maskinen (til rådighed for OS)

Datacenter licens betal for alle kerner på alle maskiner

VMWare

Kun processorer:

Tæl Processorer (= 1 core)

### Licensierede Produktions servere, MSDN TEST Servere

1. Der betales fuld licens for Produktions servere efter MS licens regler
2. Licens for Test, Udvikling og Preprod dækkes af at udviklerne SKAL have en Personlig MSDN Licens for at bruge en Server hvor licensen IKKE skal indrapporteres, da den dækkes af MSDN Licensen.
3. Developer edition er gratis, og kan downloades til egen pc.

Test / udviklings servere må kun benyttes af folk med MSDN Licens, og er så herved gratis.

Afdelingerne SKAL sørge for MSDN Licens til egne folk der logger på og arbejder med SQL Test servere, både udviklerer og driftsfolk (ios), dvs. alle der skal have adgang til test og udviklings servere.

Konsulenter udefra forventes at være MSDN certificerede.

Og projekterne SKAL sørge for at kontrollere dette.

## Leverandør / Support.

### Oversigt

SQL Server leveres af Microsoft, og vi har Microsoft Unified Support Advanced, så vi (IOS) kan oprette sager hos Microsoft, og få Premium Support. Kræver Access id og MSDN full medlemsskab.

https://support.microsoft.com/da-dk/premier

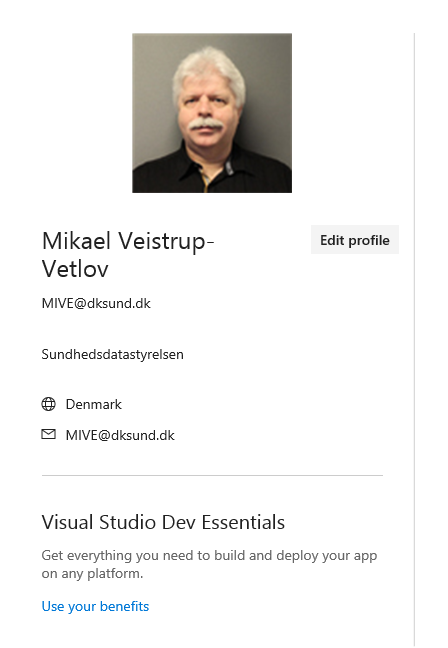
Kræver Fuld MSDN & bruger oprettet.

Ved alvorlige problemer

Hvis dit problem kræver øjeblikkelig handling, kan du ringe til kontoret i dit område:

+45 82 33 32 54

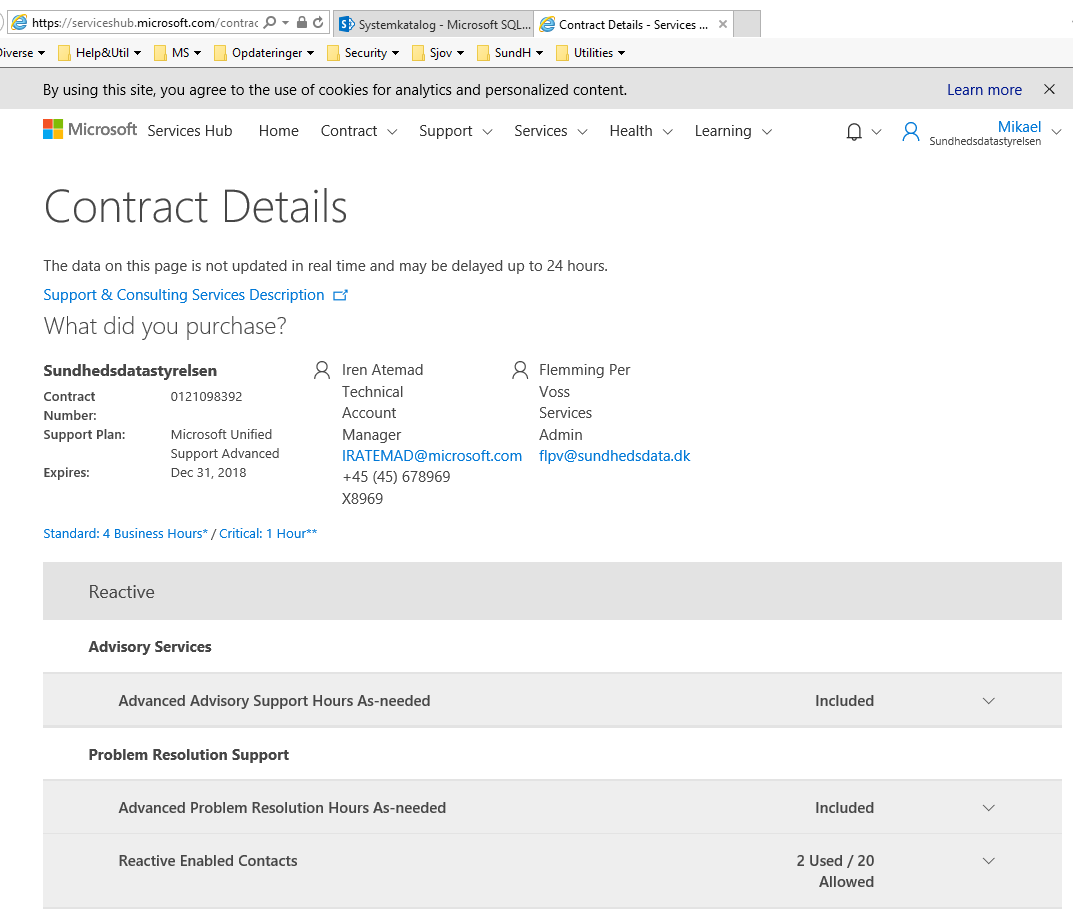
https://app.vsaex.visualstudio.com/me?mkt=en-US



https://serviceshub.microsoft.com/contractdetails/70ac4e3e-b298-41d9-b2d1-b48025b490e4

https://click.email.microsoftemail.com/?qs=e76f0bef09f2deae834a9505c966f57a41d812832d07878cac70b6404009bd52bfa48ef4bb435f7307e72a94bd8cea066285de7ea282cc45

for the Microsoft Services Hub registration



## Opret Microsoft Support sag:

Log på MS hub: [xxx@sundhedsdata.dk](mailto:xxx@sundhedsdata.dk) eller [xxx@dksund.dk](mailto:xxx@dksund.dk)

https://serviceshub.microsoft.com/databoard

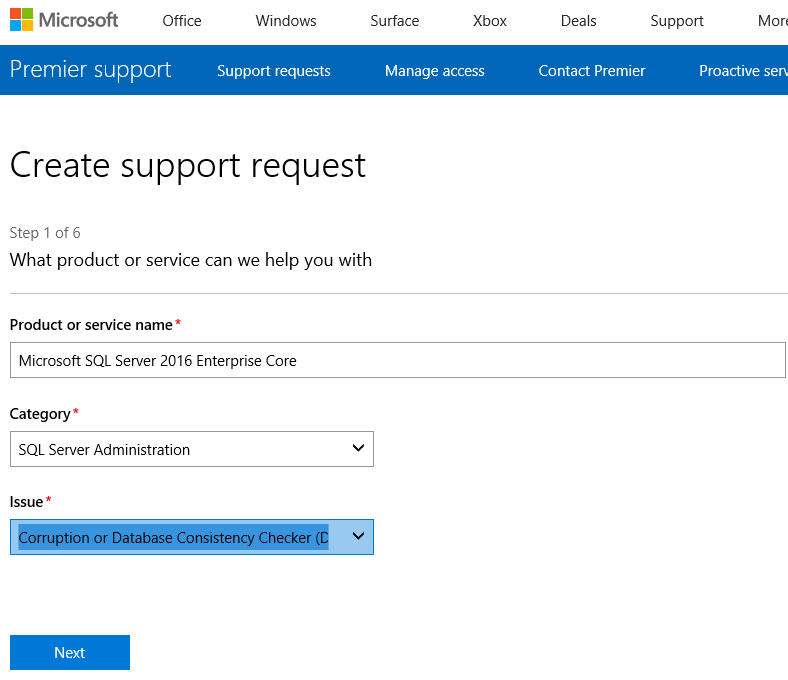
vælg Support \ Support Requests

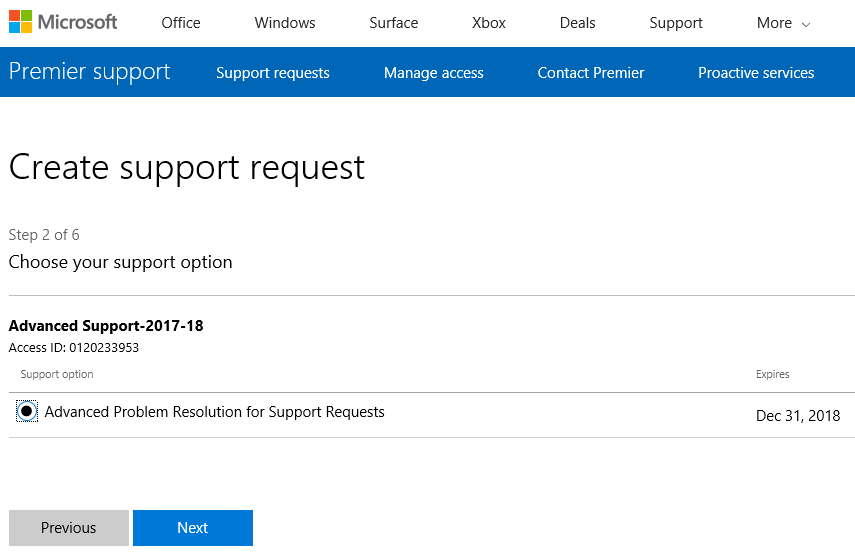
+New support request

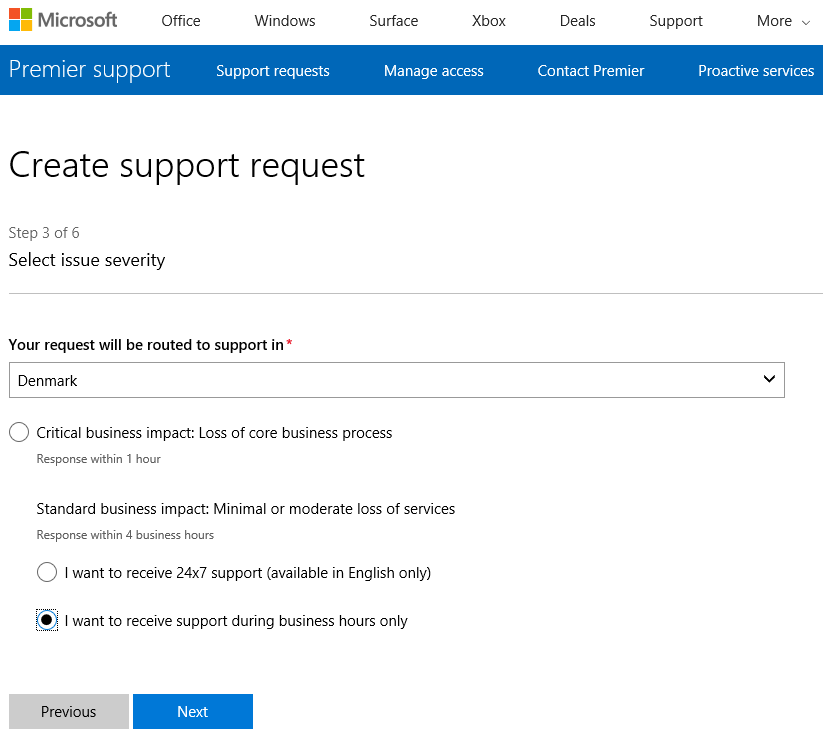
Product

Category

Issue







Create Support request

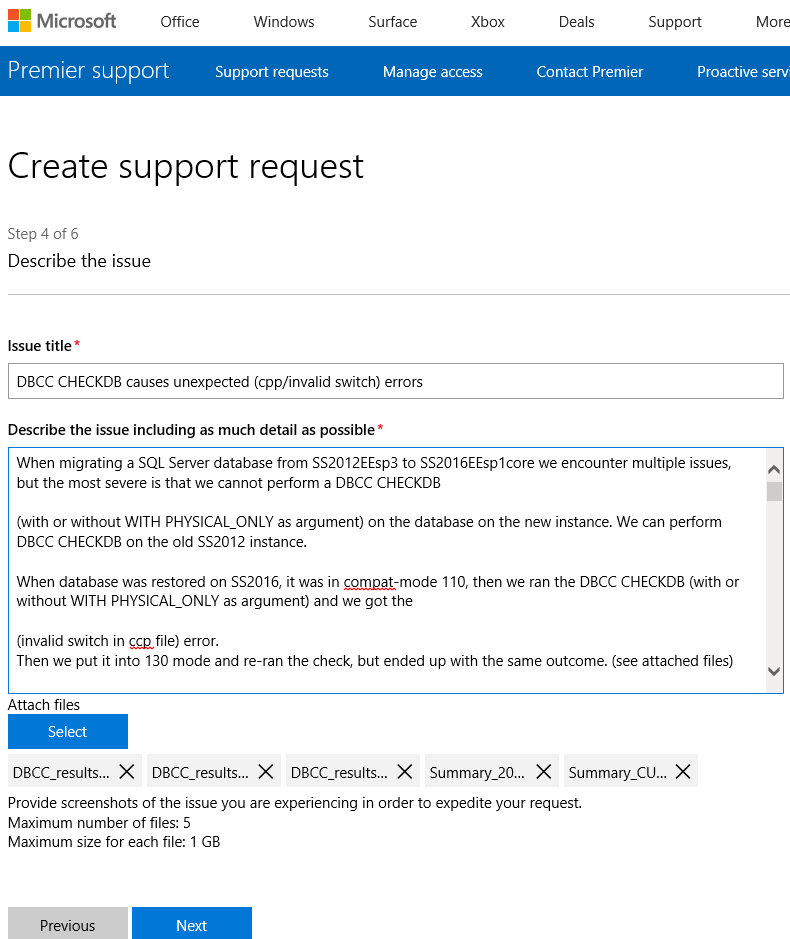
Issue title

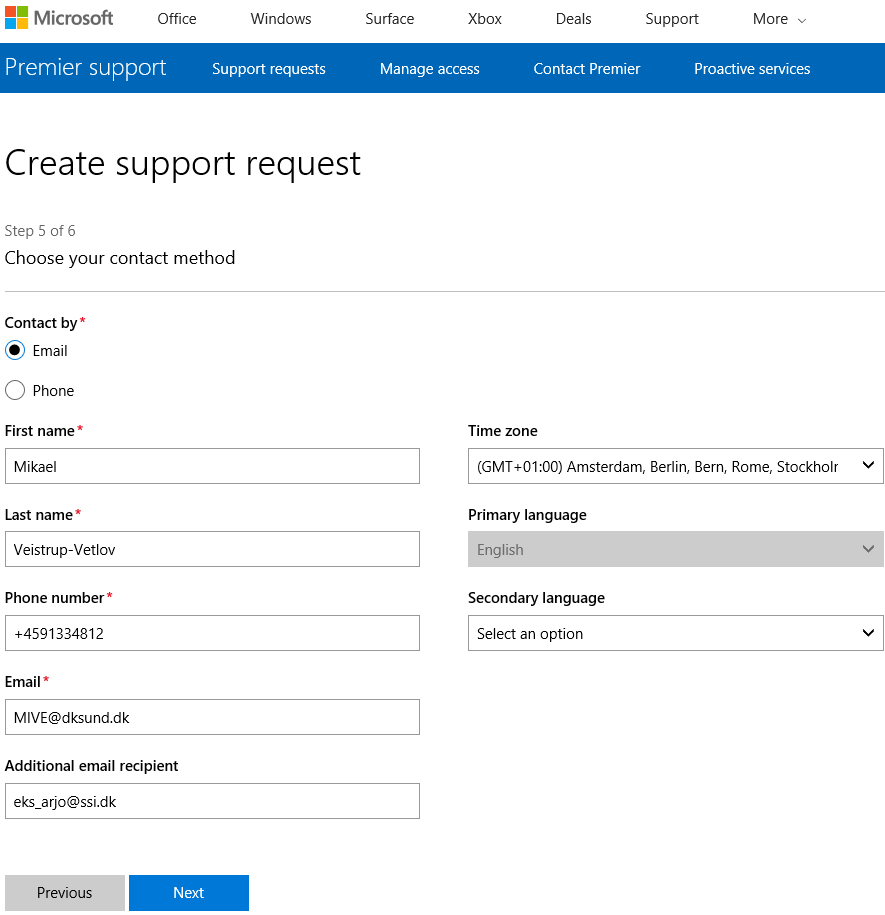
DBCC CHECKDB causes unexpected ccp errors

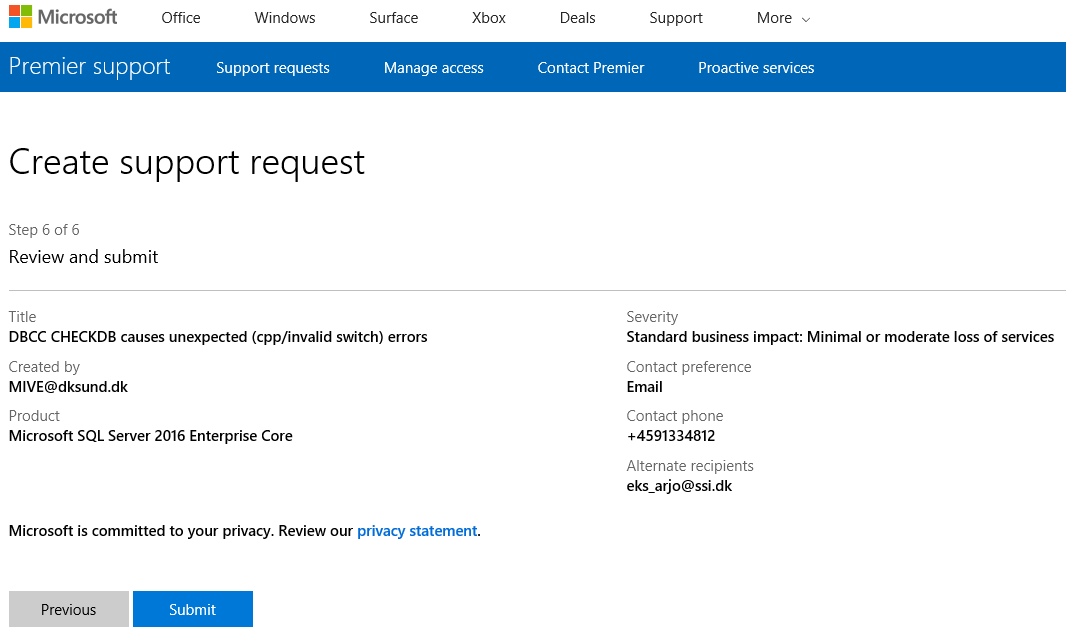
Describe issue with detail.

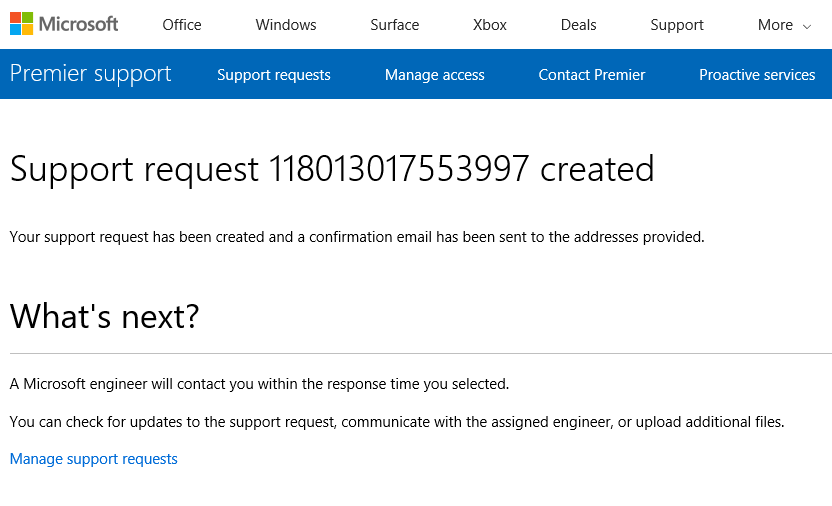
Attach files

Advisory Support = Proaktiv, Unified Support = Reaktiv.









## Opret SQL Standard Change (forhåndsgodkendt change)

Hvis en bruger har brug for at få lavet en ændring i Produktionen (ændring af data og/eller parametre inden for et system, hvor IOS ikke er ansvarlig for indholdet, men for strukturen.) eller hvis der er behov for ændring der kan påvirke flere systemer eller serverens driftfunktion, skal der oprettes en change.

Hvis det er en gentagen ændring, der er lige ud af landevejen / efter bogen, kan man oprette en Standard Change, der kan genbruges næste gang.

Dette kræver at Bruger / IOS kan dokumentere

1. Hvilke Systemer der er omfattet af changen.
2. Hvad der skal rettes,
3. Hvor det skal rettes,
4. Hvilken indflydelse ændringen har på Systemet,
5. Hvordan resultatet kan testes/måles,
6. Samt hvordan man kan lave rollback.

Og det skal godkendes af en Systemansvarlig indenfor pågældende System

I systemkataloget er der en sektion: Standard Changes.

https://sektornet/nsi/systemkatalog/Lists/Standard%20Changes/AllItems.aspx

Her skal pågældende Standard change findes, og hvis den ikke findes her skal dokumentationen oprettes som Word dokument, der vedhæftes en Standard Change, begge med relevant navn.

Første gang skal changen godkendes af Change Management.

Opret Sag i Nilex:

Gruppe: Change Management

Sagstype: Standard Change

Sagsbehandler: <MSSQL DBA>

Emne: <Relevant Beskrivelse>

Kategori: Server..Databaseserver / Databaser..MS SQL

Status: Tildelt

Risikovurdering: 3

Bruger: mive (tryk f7) mssql medarbejder

Eller Bruger <Projektleder/Systemansvarlig> Anmelder: <mssql medarbejder> (tryk f8)

Sagsbeskrivelse:

<Udvidet Relevant Beskrivelse>

I systemkatalog ”\Standard Changes\< relevant navn se ovenfor>” kopieres link til sagsbeskrivelsen (se under std-Change) eller Teknisk løsning

Vedhæftede filer gennemgås, der oprettes lokal kopi med rettelser.

I Nilex Changen trækkes den lokale kopi til punktet Sagsmenu: \Øvrige\Dokumenter\Dokument.

### Servicevindue:

Hvis changen skal med i kvartals service vindue, skal emnet starte med ordet: Servicevindue –

Når changen er åben:

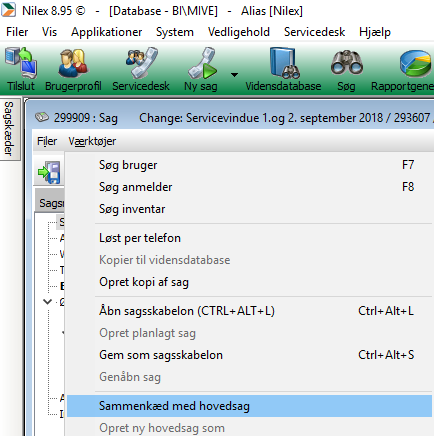
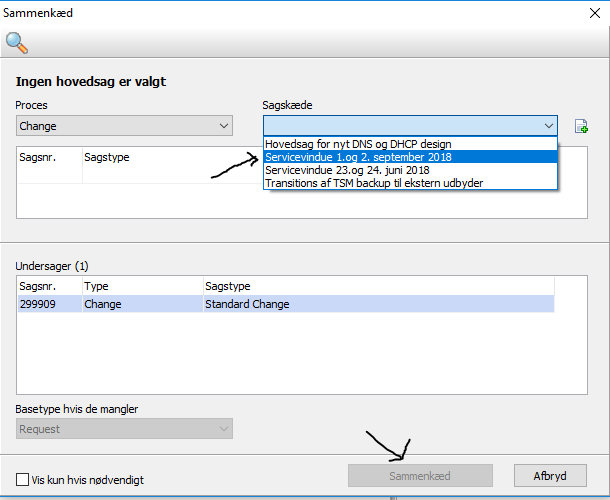
Tryk Værktøjer

Vælg Sammenkæd med hovedsag

Proces=Change

Sagskæde=<Relevant Service Vindue Sag>

Tryk Sammenkæd



## Opret Nilex RFC (Request For Change) / Normal Change

Hvis IOS skal udføre en større ændring i eksisterende miljø, skal der oprettes en Change.

I systemkataloget er der en sektion: Standard Changes.

https://sektornet/nsi/systemkatalog/Lists/Standard%20Changes/AllItems.aspx

Her skal ønskede Standard change IKKE findes, dvs. hvis det er en ny type change, skal der først oprettes en

Request For Change(RFC), hvor man spørger om lov til at lave en ændring, dette tages op på en Change Advisory Board (CAB), hvor der skal høres om forslaget, og det kan afvises hvis der ikke er tilstrækkeligt grundlag eller Rollback plan, eller hvis løsningen ikke er sikkert nok.

Et positivt resultat af dette CAB møde vil være en Normal Change, der skal udføres.

En normal change kan godkendes om til en standard change, der ikke kræver så omfattende behandling, hver gang.

Dette kræver at Bruger / IOS kan dokumentere

1. Hvilke Systemer der er omfattet af changen.
2. Hvad der skal rettes,
3. Hvor det skal rettes,
4. Hvilken indflydelse ændringen har på Systemet,
5. Hvordan resultatet kam testes/måles,
6. Samt hvordan man kan lave rollback.

Og det skal godkendes af en Systemansvarlig indenfor pågældende System

Opret Sag i Nilex:

Gruppe: Change Management

Sagstype: RFC

Sagsbehandler: <MSSQL DBA>

Emne: <Relevant Beskrivelse>

(Hvis changen skal med i kvartals service vindue, skal emnet starte med ordet: Servicevindue )

Kategori: Server..Databaseserver / Databaser..MS SQL

Status: Tildelt

Risikovurdering: 3

Bruger: mive (tryk f7) mssql medarbejder

Eller Bruger <Projektleder/Systemansvarlig> Anmelder: <mssql medarbejder> (tryk f8)

Husk relevante Abonnenter

Sagsbeskrivelse:

<Udvidet Relevant Beskrivelse>

I systemkatalog: https://sektornet/nsi/itilprocesser/Sider/Change%20Management/Change%20Management%20for%20intern%20drift.aspx

kopieres RfC skabelon.docx til lokal kopi, der rettes med relevante informationer.

I Nilex Changen trækkes den lokale kopi til punktet Sagsmenu: \Øvrige\Dokumenter\Dokument.

# 

## Dekomissionering af SQL Server

Check om Fysisk / Virtuel server. Kontroller at der ikke er aktivitet på SQL Server, tag alle SQL databaser offline, stop og disable alle SQL Services, stop alle meddelelser i Check\_MK, og efter 1 md uden problemer, opret change.

Opret Sag i Nilex:

Gruppe: Change Management

Sagstype: Standard Change

Sagsbehandler: Martin Buntzen evt.

Emne: Dekomissionering af server: <servernavn.domæne> beskrivelse

Kategori: Server..Databaseserver

Status: Tildelt

Risikovurdering: 3

Bruger: vara (tryk f7) mssql Chef

Anmelder: mive (tryk f8) mssql medarbejder

Sagsbeskrivelse:

Hej

Da <servernavn.domæne> ikke bruges mere, og SQL har været testlukket, vil jeg gerne have den lukket med henblik på at blive dekommissioneret.

Følgende SQL Databaser er taget offline

<dbnavn>

<dbnavn2>

…

Jeg har ikke nærmere oplysninger om systemerne der hører til.

/eller

Jeg har aftalt med ejere af databaserne at de bliver lukket ned

Med henblik på at lukke serveren helt ned.

navn: <servernavn.domæne>

[Venligt sæt | Jeg har sat] serveren til ikke at blive monitoreret i Check\_MK.

Jeg vil gerne have besked hvis der er nogen der alligevel henvender sig i servicedesk, i en periode på 1 måned for at sikre at der ikke er nogen der benytter serveren & databaserne.

Jeg kan enable databaser mm. hvis der opstår problemer, men det vil være med henblik på at få flyttet til anden server.

mvh Mikael

Udfyld og vedhæft change dokument & regneark fra:

Systemkatalog \ Standard Changes \ Dekommisionering af fysisk / virtuel server

Til Sagsmenu\Øvrige\Dokumenter

## 

## Opret Test Server

Planlæg domæne, system, ip, adgange, version, gui/core mm.

Opret Sag i Nilex:

Gruppe: Change Management

Sagstype: Standard Change

Sagsbehandler: Nikou Negerhend evt.

Emne: Har brug for test SQL server i 2-3 uger. beskrivelse

Kategori: Server..Databaseserver

Status: Tildelt

Risikovurdering: 3

Bruger: mive (tryk f7) mssql medarbejder

Sagsbeskrivelse:

Hej

Jeg vil gerne bestille en test virtuel windows server 2016 med gui

navn: s-mivesql21-t.sst.dk

ip: normal i sst

firewall: normal i sst

GPO: normal i sst

bestykning:

2 core

8 Gb ram

c: 100Gb

r: 50Gb

s: 50Gb

t: 50Gb

u: 50Gb

Std-Change

https://sektornet/nsi/systemkatalog/Lists/Standard%20Changes/DispForm.aspx?ID=2&Source=https%3A%2F%2Fsektornet%2Fnsi%2Fsystemkatalog%2FLists%2FStandard%2520Changes%2FAllItems%2Easpx%23InplviewHashe0ac79e7%2Dcae2%2D4c35%2D8a94%2Dd3b37f827beb%3D&ContentTypeId=0x0100C21019E2EEB20F4C83996A5AFE743F90

poso & std-change vedhæftet.

Page/swap placeres på systemdisk c:

Diske r,s,t u formatteres som bedst for MSSQL db dvs. 64Kb

Når WmVare installatione er på plads, skal server overleveres til Office Backend for normal Windows tilpasning.

Derefter overleveres til MiVe/StGn (MSSQL) for SQL Installation & Backup

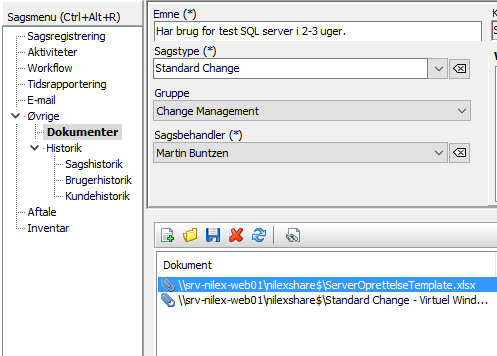
Mvh MIkael

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

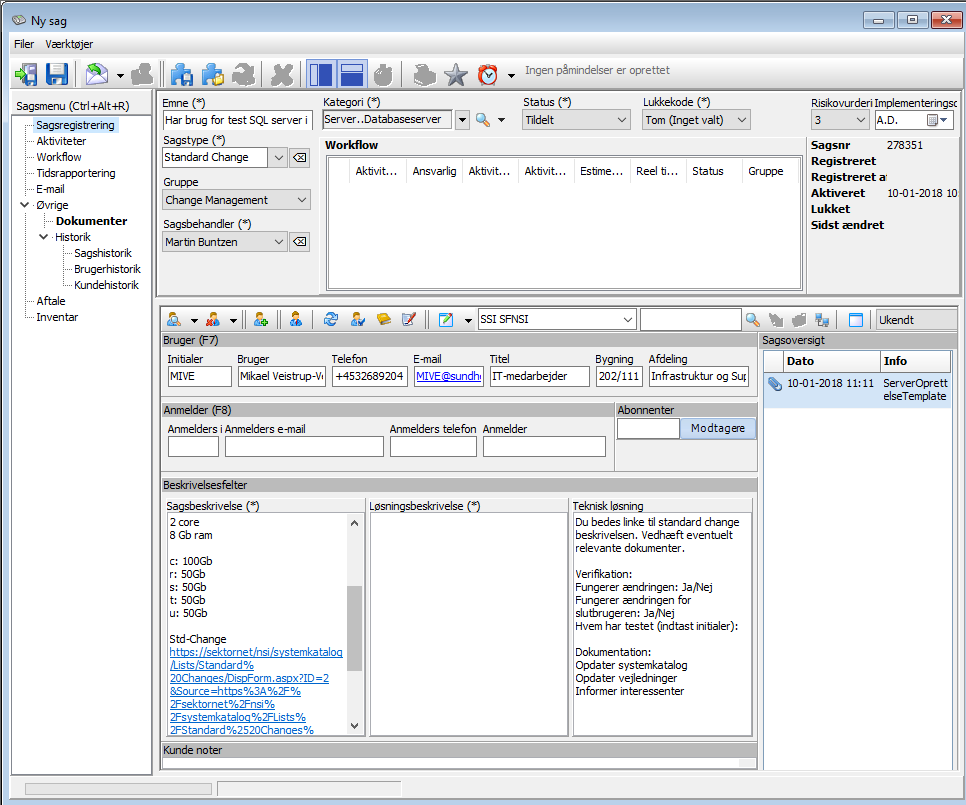
I systemkatalog ”\Standard Changes\Opret Virtuel Windows Server 2012R2” kopieres link til sagsbeskrivelsen (se under std-Change)

Vedhæftede filer gennemgås, der oprettes lokal kopi med rettelser.

I Nilex Changen trækkes den lokale kopi til punktet Sagsmenu: \Øvrige\Dokumenter\Dokument.



Med Resultatet: Der submittes via Gem og Luk:



EurekaLog 6.1.04

Application:

-------------------------------------------------------

1.1 Start Date : Wed, 10 Jan 2018 09:19:02 +0100

1.2 Name/Description: plus.exe - (Nilex 8.94)

1.3 Version Number : 8.94.3006.5

1.5 Compilation Date: Fri, 3 Feb 2017 08:23:13 +0100

1.6 Up Time : 2 hours, 36 minutes, 14 seconds

Exception:

-----------------------------------------------------

2.1 Date : Wed, 10 Jan 2018 11:55:16 +0100

2.2 Address : 00458C91

2.3 Module Name : plus.exe - (Nilex 8.94)

2.4 Module Version: 8.94.3006.5

2.5 Type : EReadError

2.6 Message : Stream read error.

2.7 ID : 2F10

2.8 Count : 1

2.9 Status : New

2.10 Note :

Active Controls:

--------------------------------------------------------------------------------

4.1 Form Class : TfrmMain

4.2 Form Text : Nilex 8.94 © - [Database - BI\MIVE] - Alias [Nilex]

4.3 Control Class: TPanel

4.4 Control Text :

Computer:

-----------------------------------------------------------------------------------

5.1 Name : WXU004361

5.2 Total Memory : 8048 Mb

5.3 Free Memory : 4160 Mb

5.4 Total Disk : 118,33 Gb

5.5 Free Disk : 8,96 Gb

5.6 System Up Time: 4 days, 21 hours, 16 minutes, 35 seconds

5.7 Processor : Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz

5.8 Display Mode : 1920 x 1080, 32 bit

5.9 Display DPI : 96

5.10 Video Card : Intel(R) HD Graphics 520 (driver 22.20.16.4749 - RAM 1024 MB)

5.11 Printer : Xerox Global Print Driver PCL6 (driver 10.0.14393.953)

Operating System:

----------------------------------------------

6.1 Type : Microsoft Windows 6.2 (64 bit)

6.2 Build # : 9200

6.3 Update :

6.4 Language: Danish

6.5 Charset : 0

Custom Information:

----------------------------------------------------------------------------------------------------------------------------------------------------

8.1 Plus Application Path : C:\Program Files (x86)\Nilex AB\Nilex Enterprise\plus.exe

8.2 Plus Application Parameters :

8.3 Nilex UserName : MIVE

8.4 Eurekalogs created in this session : 2

8.5 Database Type : MSSQL (DevartSQLServer 7.1.2.0)

8.6 Database Version : Microsoft SQL Server 2008 R2 (SP3) - 10.50.6220.0 (X64)

Mar 19 2015 12:32:14

Copyright (c) Microsoft Corporation

Standard Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601:\_Service Pack 1) (Hypervisor)

8.7 Database Name (Quoted) : "nilex"

8.8 Database UserId : SSI\MIVE

8.9 Database Authentication : KERBEROS

8.10 Database Collation : Danish\_Norwegian\_CI\_AS

8.11 Database VendorLib : sqloledb.dll (MSSQL OLE-DB)

8.12 DbCon1/dbExpress ConnectionTimeout : Default

8.13 DbCon1/dbExpress CommandTimeout : Default

8.14 DbCon2/ADO.Net ConnectionTimeout : Default

8.15 DbCon2/ADO.Net CommandTimeout : Default

8.16 Licensed Modules : WFM, SLA, ReleaseCalendar, Knowledgebase

8.17 Modules not used (no license) : ComAround, ResourceCalendar

8.18 DocSafe : No

8.19 Boxed Application : Yes

8.20 Remote Session (Citrix/RDS) : No

8.21 Nilex RC Assembly Version :

8.22 Nilex Shared Assembly Version : 8.94.3001.1001

8.23 Nilex WFM Assembly Version : 1.28.1.2

8.24 Nilex DecodeLicense Assembly Version : 1.0.0.1009

8.25 WFM DB ConnectionString (Initial value, Quoted): "Server=srv-mssql-db01.ssi.ad;Database=nilex;Integrated Security=SSPI"

8.26 WFM/nxSA Application Context : Loaded in memory

8.27 #50777 Except Counter : 0

8.28 WFM Assembly ErrorInfo : Assembly Error structure not loaded.

Call Stack Information:

--------------------------------------------------------------------------------------------------------

|Address |Module |Unit |Class |Procedure/Method |Line |

--------------------------------------------------------------------------------------------------------

|\*Exception Thread: ID=916; Priority=0; Class=; [Main] |

|------------------------------------------------------------------------------------------------------|

|00458C91|plus.exe |Classes.pas |TReader |ReadBuffer | |

|00458C64|plus.exe |Classes.pas |TReader |ReadBuffer | |

|00458C2D|plus.exe |Classes.pas |TReader |Read | |

|00458C18|plus.exe |Classes.pas |TReader |Read | |

|0045AA24|plus.exe |Classes.pas |TReader |ReadValue | |

|0045AA1C|plus.exe |Classes.pas |TReader |ReadValue | |

|004587DD|plus.exe |Classes.pas |TReader |EndOfList | |

|004587D8|plus.exe |Classes.pas |TReader |EndOfList | |

|00458DEC|plus.exe |Classes.pas |TReader |ReadCollection | |

|00458D84|plus.exe |Classes.pas |TReader |ReadCollection | |

|0061CE39|plus.exe |ComCtrls.pas | |ReadCols | |

|0061CDCC|plus.exe |ComCtrls.pas | |ReadCols | |

|0061CF93|plus.exe |ComCtrls.pas |TCustomListView|CreateWnd | |

|0058CE07|plus.exe |Controls.pas |TWinControl |CreateHandle | |

|00590B99|plus.exe |Controls.pas |TWinControl |HandleNeeded | |

|00590B7C|plus.exe |Controls.pas |TWinControl |HandleNeeded | |

|00590BA5|plus.exe |Controls.pas |TWinControl |GetHandle | |

|00590BA0|plus.exe |Controls.pas |TWinControl |GetHandle | |

|0061B8EF|plus.exe |ComCtrls.pas |TListItems |GetHandle | |

|0061B8EC|plus.exe |ComCtrls.pas |TListItems |GetHandle | |

|0061BAA7|plus.exe |ComCtrls.pas |TListItems |SetUpdateState | |

|0061BA24|plus.exe |ComCtrls.pas |TListItems |SetUpdateState | |

|0061BA19|plus.exe |ComCtrls.pas |TListItems |BeginUpdate | |

|0061BA0C|plus.exe |ComCtrls.pas |TListItems |BeginUpdate | |

|0167794B|plus.exe |fmeInvent.pas|TfmeInventarier|LoadChainedInvents |1115[5] |

|016778E0|plus.exe |fmeInvent.pas|TfmeInventarier|LoadChainedInvents |1110[0] |

|01C3B888|plus.exe |hdprop.pas |TfrmHdProp |saveRecord |4847[817]|

|01C38BDC|plus.exe |hdprop.pas |TfrmHdProp |saveRecord |4030[0] |

|01C3D52A|plus.exe |hdprop.pas |TfrmHdProp |SaveCase |5258[339]|

|01C3C938|plus.exe |hdprop.pas |TfrmHdProp |SaveCase |4919[0] |

|01C51DDC|plus.exe |hdprop.pas |TfrmHdProp |Action2Execute |10512[54]|

|01C51BA0|plus.exe |hdprop.pas |TfrmHdProp |Action2Execute |10458[0] |

|01C67AB0|plus.exe |hdprop.pas |TfrmHdProp |SaveClose |17446[19]|

|01C67A20|plus.exe |hdprop.pas |TfrmHdProp |SaveClose |17427[0] |

|01C67A18|plus.exe |hdprop.pas |TfrmHdProp |btnSaveAndCloseClick |17423[1] |

|005899C4|plus.exe |Controls.pas |TControl |Click | |

|00589954|plus.exe |Controls.pas |TControl |Click | |

|00622D64|plus.exe |ComCtrls.pas |TToolButton |Click | |

|00406B24|plus.exe |System.pas | |\_CallDynaInst | |

|00589E69|plus.exe |Controls.pas |TControl |WMLButtonUp | |

|00589458|plus.exe |Controls.pas |TControl |WndProc | |

|778D35DB|ntdll.dll | | |RtlDeactivateActivationContextUnsafeFast| |

|0058907C|plus.exe |Controls.pas |TControl |Perform | |

|00589058|plus.exe |Controls.pas |TControl |Perform | |

|0058D4B4|plus.exe |Controls.pas | |GetControlAtPos | |

|0058D408|plus.exe |Controls.pas | |GetControlAtPos | |

|0058D57E|plus.exe |Controls.pas |TWinControl |ControlAtPos | |

|0058907C|plus.exe |Controls.pas |TControl |Perform | |

|00589058|plus.exe |Controls.pas |TControl |Perform | |

|0058D648|plus.exe |Controls.pas |TWinControl |IsControlMouseMsg | |

|0058D59C|plus.exe |Controls.pas |TWinControl |IsControlMouseMsg | |

|0058DB98|plus.exe |Controls.pas |TWinControl |WndProc | |

|00589058|plus.exe |Controls.pas |TControl |Perform | |

|00624DE5|plus.exe |ComCtrls.pas |TToolBar |UpdateButtonState | |

|00624D94|plus.exe |ComCtrls.pas |TToolBar |UpdateButtonState | |

|00624E26|plus.exe |ComCtrls.pas |TToolBar |UpdateButtonStates | |

|0058D7B4|plus.exe |Controls.pas |TWinControl |WndProc | |

|006277B4|plus.exe |ComCtrls.pas |TToolBar |WndProc | |

|0058D3BC|plus.exe |Controls.pas |TWinControl |MainWndProc | |

|0046223C|plus.exe |Classes.pas | |StdWndProc | |

|777482B0|user32.dll | | |GetKeyState | |

|0168CE42|plus.exe |fmeReg.pas |TfmeAnkReg |aplctnvntsRichPasteEventsMessage |2286[13] |

|7773DF9B|user32.dll | | |DispatchMessageW | |

|7773DF90|user32.dll | | |DispatchMessageW | |

|006515EB|plus.exe |Forms.pas |TApplication |ProcessMessage | |

|006514F8|plus.exe |Forms.pas |TApplication |ProcessMessage | |

|0065162E|plus.exe |Forms.pas |TApplication |HandleMessage | |

|00651624|plus.exe |Forms.pas |TApplication |HandleMessage | |

|00651959|plus.exe |Forms.pas |TApplication |Run | |

|00651890|plus.exe |Forms.pas |TApplication |Run | |

|022ED7E8|plus.exe |plus.dpr | |Initialization |1048[66] |

|751662C2|KERNEL32.DLL| | |BaseThreadInitThunk | |

--------------------------------------------------------------------------------------------------------

Modules Information:

--------------------

Processes Information:

----------------------

Assembler Information:

----------------------

Registers:

----------

## Migrering af database til nyere SQL

Check Database med https://www.microsoft.com/en-us/download/details.aspx?id=53595

P:\SQLDBA\SQLDataMigrationAssistant

https://www.mssqltips.com/sqlservertip/1936/sql-server-database-migration-checklist/

Backup database copyonly

Restore database new server / disk

1. DBCC WITH DATA\_PURITY

2. DBCC UPDATEUSAGE

3. UPDATE STATS with FULLSCAN

4. IF needed rebuild all indexes (This should have happened with UDPATE STATS)

These steps must be taken when moving a database from one server to another to ensure metadata is correct as well as the IAM and GAM map to be corrected for the new storage. If not we can expect to see these issues.

1. DBCC with Data Purity

-- Generate commands on tables in any databases and schema. Prints commands to Console, Will execute

-- commands if EXE is activated.

-- Script outputs a time difference clocking the execution time for the entire process (useful full for test migration).

DECLARE @StartTimer datetime2

DECLARE @Database VARCHAR(255)

DECLARE @Table VARCHAR(255)

DECLARE @cmd NVARCHAR(500)

SET @StartTimer = SYSDATETIME()

DECLARE DatabaseCursor CURSOR FOR

SELECT name FROM master.dbo.sysdatabases

WHERE name NOT IN ('master','msdb','tempdb','model' ,'ForskerTest')

ORDER BY 1

OPEN DatabaseCursor

FETCH NEXT FROM DatabaseCursor INTO @Database

WHILE @@FETCH\_STATUS = 0

BEGIN

SET @cmd = 'DECLARE TableCursor CURSOR FOR SELECT ''['' + table\_catalog + ''].['' + table\_schema + ''].['' +

table\_name + '']'' as tableName FROM [' + @Database + '].INFORMATION\_SCHEMA.TABLES

WHERE table\_type = ''BASE TABLE'''

-- create table cursor

EXEC (@cmd)

OPEN TableCursor

FETCH NEXT FROM TableCursor INTO @Table

WHILE @@FETCH\_STATUS = 0

BEGIN

-- SQL 2005 or higher command

SET @cmd = 'dbcc checktable (' + @Table + ') WITH DATA\_PURITY;';

SET @cmd =REPLACE(@cmd,'([','(''')

SET @cmd =REPLACE(@cmd,'])',''')')

SET @cmd =REPLACE(@cmd,'].[','.')

print @cmd ;

-- EXEC (@cmd) ;

FETCH NEXT FROM TableCursor INTO @Table

END

CLOSE TableCursor

DEALLOCATE TableCursor

FETCH NEXT FROM DatabaseCursor INTO @Database

END

CLOSE DatabaseCursor

DEALLOCATE DatabaseCursor

-- Change measures to: millisecond, second, minute, hour, day .....

print 'Execution time in seconds : ';

print DATEDIFF(second, @StartTimer, SYSDATETIME()) ;

1. DBCC UPDATEUSAGE (<dbnavn>)

-- DBCC execution completed. If DBCC printed error messages, contact your system administrator.

1. Brug update statistics i 1)

SET @cmd = ' UPDATE STATISTICS ' + @Table + ' WITH FULLSCAN;'; -- (uden replace linier)

1. Brug Rebuild Indexes I 1)

SET @cmd = 'ALTER INDEX ALL ON ' + @Table + ' REBUILD;'; -- (uden replace linier)

1. Drop & Create COLUMNSTORE index on [LMS].[DS\_EkoKur]

--(højreklik på db\tabel\index - script “drop& create to”)

USE [Forsker];

/\*\*\*\*\*\* Object: Index [cstoreidx\_DS\_EkoKur] Script Date: 03-05-2018 13:36:17 \*\*\*\*\*\*/

DROP INDEX [cstoreidx\_DS\_EkoKur] ON [LMS].[DS\_EkoKur];

SET ANSI\_PADDING ON;

/\*\*\*\*\*\* Object: Index [cstoreidx\_DS\_EkoKur] Script Date: 03-05-2018 13:36:17 \*\*\*\*\*\*/

CREATE NONCLUSTERED COLUMNSTORE INDEX [cstoreidx\_DS\_EkoKur] ON [LMS].[DS\_EkoKur]

(

[EKSD],

[VNR],

[APK],

[TARD],

[EKSP],

[PTP],

[PATT],

[RGLA],

[IBGP],

[TSKA],

[AREF],

[TSK3],

[KOM],

[RGL1],

[TSK1],

[RGL2],

[TSK2],

[EJS],

[RAMT],

[OVNR],

[UDLV],

[KOEN],

[ALDR],

[TAKD],

[KORR],

[TILPRIS],

[AIP],

[AUP],

[ABC],

[PKSUBGR],

[PPRS],

[RIMB],

[CPR\_REG],

[CPR\_KOM],

[EncryptionID]

)WITH (DROP\_EXISTING = OFF, COMPRESSION\_DELAY = 0);

GO

1. Sæt db-owner til sa & compat level 130

USE [Forsker]

EXEC sp\_changedbowner 'sa';

ALTER DATABASE forsker SET COMPATIBILITY\_LEVEL = 130;

1. Kør script til sletning af Orphaned users, og til at oprette de Logins & users der skal bruges.

# Tools / Utilities.

## SHRINK DATABASE / FILE

Når man oplever at SQL\_Logfil (transaktions log) løber løbsk, og ikke kan blive større, da disken er ved at være fyldt, så skal der ryddes op i logfil. Dette forekommer når Databasen er sat til Full.

T-log indeholder de database transaktioner, der er foretaget siden sidste T-log backup (i klumper). For at rydde op inden for den eksisterende t-log kan der køres en (eller flere) T-log backup, og shrink.

(BS) For at BrandSlukke kan man definere en ekstra t-log på en anden disk, der så bør ryddes op efter nedenstående shrink.

(BS) Hvis der er brug for den pågældende log-størrelse, så bør log disken udvides. (nemt hvis virtuel disk.)

## Disk plads forbrug check med windirstat

Hvis windirstat ikke findes på serveren, installer evt. fra P:\SQLDBA\windirstat1\_1\_2\_setup.exe med default settings.

Start, vælg disk og analyser.

Brug af Remote Desktop Manager

## Powershell scripts.

### AD-GroupUser.ps1 - Gruppe Bruger Action

- PowerShell script til at checke bruger og gruppe sammenhænge.

└-Angiv parametre: Gruppe Bruger Action

└-Hvor:

└-Gruppe: her skal angives sAMAccountName for en eksisterende AD-Gruppe.

└-(Gruppe: lst for at liste AD-grupper for efterfølgende bruger.)

└-Bruger: her skal angives sAMAccountName for en eksisterende AD-bruger.

└-Action: kan angive

└- - add for at tilføje bruger til gruppen.

└- - del for at fjerne bruger fra gruppen.

└- - lst lister brugere der er medlem i gruppen.

└- - lsu lister brugere der er medlem i gruppen. Udvidet visning

└- - vis eller alt andet for at vise om bruger er medlem i gruppen.

### AD-Users.ps1 – søgeord

- PowerShell script til at liste brugere der har søgeordet som del af navnet

### AD-Groups.ps1 – søgeord

- PowerShell script til at liste grupper der har søgeordet som del af navnet

### AD-ChkUser.ps1 – AD-brugerlogon

- PowerShell script til at liste brugeren i dksundtest, dksund, sst & ssi

### disk-size.ps1 – fqServernavn

- PowerShell script til at liste diskstørrelser for en remote disk

### Make\_group.ps1

- PowerShell script til at definere ad-grupper til MsSql adgang

man redigerer Make\_group.ps1, tilretter:

$System="SDPudv"

$DBname="DocxPress"

$DBshort="DocxPress"

$ServiceDeskNummer="257345"

$Ressourceejer="SOTH"

$befuldmaegtiget="THBH" # initialer komma adskilt

$sqlserver="srv-mssql-07p.ssi.ad (dbhotel01)”

$mssqldba="MiVe"

$domRes="ssi.ad"

$domUser="ssi.ad"

Med de aktuelle oplysninger og køre scriptet.

Scriptet vil vise notepad hvor t-sql kommandoerne til at oprette grupperne med korrekte parametre klargøres.

Herefter kan man kopiere de enkelte linier og køre i de korrekte domæner, og derved oprette grupperne.

Der gemmes log over hvilke grupper der er oprettet i Total-MkGrp.log

Der klargøres ligeledes T-SQL kommandoer til at oprette Databasen & SQL instans logins & database brugere & knytter disse sammen. Disse kommandoer skal ligeledes kopieres til SQL query vinduet på den pågældende server, og køres.

Der klargøres ligeledes nogle linier der kan bruges for at beskrive Gruppe sammenhængene i servicedesk sagen.

Disse kan kopieres ind i Løsningsbeskrivelsen.

Is-Sql.ps1

Checker om PowerShell SQLserver modulerne er installeret, og gør det hvis de ikke er.

Kræves for at køre invoke-sqlcmd

Is-Ntfs.ps1

Checker om Powershell NTFSSecurity er installeret, og gør det hvis de ikke er.

Kræves for at sætte ntfs rettigheder.

Call-Sql.ps1

Laver PowerShell opkald til SQL database og udfører et tsql kald

# SQL Server Backup / Restore

Installation på Gui

Installation på Core

## Check af schedulering

get-service TSM\_SQL

c:\tsm\log

scite sql\_schedlog.log

CD 'C:\Program Files\Tivoli\TSM\TDPSql'

.\tdpsqlc.exe q tsm

scite dsm.opt

indsæt SCHEDLOGRETENTION 30 D

for 30 dages schedulerings log retention

# Systemer

## Opsætning af nyt system <Systemnavn>

Beskrivelse af systemet

Servicenow opretBusiness Service <Systemnavn>

Kontaktpersoner & ansvarlige.

App-Servere

Databaser

Ad-grupper

Brugere

Servicekonti

Passwords: Secret Server

TSM Backup

Firewall Regler

Licensiering

DNS & Cname(alias)

## Nedlægning af system <Systemnavn>

Gem Backup af Server & DB

Nedlæg:

Server <Servernavn>

Databaser: <DBnavne>

AD & SQL Serviceaccounts:

Passwords: i Secret Server

AD-Grupper: List og nedlæg

Stop tsm-backup:

Afbestil Firewall regler:

Afbestil Licens:

Fjern appl fra sw

Fjern cname fra dns

Marker system i Sharepoint & ServiceNow som nedlagt

## MTIME – kommende tidsregistrerings system.

Kontakt person Charlotte Herbst. & Kirsten Vester Skov

2 app (web) servere:

srv-mt-web01p.ssi.ad og srv-mt-web01t.ssi.ad

her er 4-5 versioner på

Konsulentfirmaet MTIME SYSTEMS har fuld adgang.

SQL på DBHOTEL01(srv-mssql-07p.ssi.ad) og srv-mssql-09t.ssi.ad

Her er 6 forskellige databaser:

MTIME\_(afdeling)\_Prod

MTIME\_Historik

…….\_ANONYM der er kopi med anonymiserede data.

XDB\_PROD

MSYNC\_PROD

### Anonymiset kopi af XXXX-test/prod databasen, lagt op på TMS's FTP-site.

Det er som regel Charlotte Harbst der bestiller, i forenklet form som ovenstående.

Der kopieres en db til db\_ANONYM (bk + rest) f.eks. via: GenBkRstScript.sql

Hvorefter der køres et script. Sletcpr.sql

Derefter køres en ny backup til FTP

NB. Husk at bruge compression!!!!!!!!

Kopier produktionsdatabase til ”prodnavn”\_anonym database

Kør det relevante anonymiserings statement på ”prodnavn”\_anonym database (IKKE PRODUKTION)

Backup ”prodnavn”\_anonym database (f.eks. til \\srv-mssql-09t.ssi.ad\MiveTemp) og ftp upload til mtime

Brug Stifinder: (Server: ftp.timemsystem.com, user: Client\_SST, pass: Se Secret server mTimeFTP i sektion DB)

https://secretserver.dksund.dk/SecretView.aspx?secretid=1754

26-10-2017 12:02/MIVE

Hej Charlotte

Databasen: mTIME\_STPS\_PROD på srv-mssql-07p.ssi.ad er kopieret til mTIME\_STPS\_PROD\_ANONYM

derefter Anoymiseret, backup til mTIME\_STPS\_PROD\_ANONYM\_20171109.bak der er kopieret til TMS' ftp-site.

Alle de anonyme database kopier er herefter slettet.

mvh Mikael

På test har de bruger

a\_mtime – og

ssi\MTIME\_KRUE (KRVE?)

t\_mtime =dbo

logfil af ftp ruller.

Property Owner is not available for Database ‘[DBName]’.

exec sp\_helpdb 'zero\_d'

sp\_changedbowner @loginame = 'sa'

## Venteinfo:

Offentligt system til ventetider på behandlinger.

App på PubDmz

Mssql db på intdmz:

idmzmssql2.intdmz.dk

Venteinfo\_prod

Venteinfo\_test

Prod skal flyttes til srv-mssql-05p.intdmz.dk

Test skal flyttes til srv-mssql-06t.sst.dk

## MitSygehusvalg (afløseren for Venteinfo)

Test db på srv-mssql-06t.sst.dk

Prod db på srv-mssql04p.sst.sk

Job: Mitsygehusvalg.Orkestrering (SSIS pakke) henter data fra DB: mitsygehusvalg og uploader til Webside hver 10 min.

Hvis jobbet ikke nulstiller temp overførsels område får systemet ikke de rigtige data med over.

Der køres Stort job hver morgen (varighed 1 time +) , samme job, men hvis rundate er ny, køres stort job.

Dette kan tvinges igennem ved at rette rundate tilbage:

USE mitsygehusvalg;

UPDATE dbo.Fritvalg\_rundate

SET Run\_date = DateAdd(d,-1,GETDATE());

I samarbejde med PMNI & JHVJ

## SOR - Sundhedsvæsenets Organisationsregister

Systemejer: KMLY, PGP

Befuldmægtet: BDA

Teknisk ansvarlige: DRI

Servere fundet i NSIDSDN.dk:

s-sor2-app1-p.nsidsdn.dk

s-sor2-app3-t.nsidsdn.dk

s-sor3-web1-p.nsidsdn.dk

s-sor3-web3-t.nsidsdn.dk

Fejllogs fundet:

SRV-SOR2-PROD.imkit.dk: E:\websites\_log\_files\edi\edi.log

### Kopier SOR fra imkit 🡪 pubdmz

Hver nat genererer SOR nogle filer 🡪 srv-sor2-prod.imkit.dk - E:\filersstdk\sor

som et job på srv-fil-06.sst.dk - c:\sor\winscp\_tosorserver via ftp: c:\sor\wftp\_command

sender til Pubwww.pubdmz.dk

Kræver at firewall er åbnet for ftp

Task Scheduler\

### SOR database (db2)

Backup & restore procedurer er beskrevet i hostnotes til srv-ldb3.nsidsdn.dk

https://sektornet/nsi/systemkatalog/HostNotes/srv-ldb3.nsidsdn.dk.aspx

Fra Driftdok:

## Nulstilling af brugernes password for SOR-EDI & SOREDI-DEMO

### Vejledning:

Passwords for SOR-EDI skal nulstilles direkte i databasen, da selve funktionen ikke virker i SOR-EDI. SOR-brugerne i SOA skal involveres for at verificere brugeren.

DB-server: ” SRV-SQL-BIS1”

For SOR-EDI er det databasen: ”SOREDI”

For SOREDI-DEMO er det databasen: ”SOREDIDEMO”

Passwords er gemt i tabellen ”Users” og selve feltet kan direkte opdateres med det nye password.

Password 8 char; nXx

Rettes f.eks.:

Declare @User AS Nvarchar(20)

Set @User = 'complimenta'

Declare @NewPW AS Nvarchar(8) --Max 8 char "xnX" alfanum

Set @NewPW = 'rlZnUpyv'

Select \* from SOREDI.dbo.Users

where Username like @User

-- efterfulgt af

If exists (Select \* from SOREDI.dbo.Users where Username = @User)

Begin

update SOREDI.dbo.Users

set Password =@NewPW

where Username = @User

End

If exists (Select \* from SOREDIDEMO.dbo.Users where Username = @User)

Begin

update SOREDIDEMO.dbo.Users

set Password =@NewPW

where Username = @User

End

Select \* from SOREDI.dbo.Users where Username = @User

Select \* from SOREDIDEMO.dbo.Users where Username = @User

Det nye kodeord skal sendes til: "kunde@email\_adr" med Cc til: [sorpost@sundhedsdata.dk](mailto:sorpost@sundhedsdata.dk) = bda

Kære xxxx

Jeg har genereret et nyt password til dig/jer

Xxxxx

d. 28/2 kl 10:00

Ios kundeansvarlige: mive

Nilex sag kan lukkes med:

10-03-2020 14:47/MIVE

Der er genereret nyt kodeord til <kunde> (<bruger>)

og sendt mail om dette til brugeren <email>

med cc til sorpost.

både prod & demo

Sagen lukkes herefter

mvh Mikael

## BioNumerics Databasesystem

When a SQL Server database is used for data storage, BioNumerics employs a stored procedure called usp\_GETAUTONM to auto-number all new database objects (e.g. entries, attachments, ...). The error occurs because the SQL Server User that is connecting to the database via BioNumerics does not have the rights to execute this stored procedure. You can grant this permission by executing following SQL statement in e.g. SQL Server Management Studio:

Use FBI\_BN\_Clostridium\_surv -- dbnavn

GRANT EXECUTE ON OBJECT::[dbo].[usp\_GETAUTONM] TO [ssi\bionum\_l\_fbi\_bn\_db\_o] --gruppenavn

## CRM ( XRM ) Formålet med CRM-systemet (Customer Relationship Management) er at understøtte de forskellige arbejdsområder samt samle og effektivisere de processer der relaterer sig til Sundhedsdatastyrelsens kundekreds.

## Udviklet /administreret af Netcompany

Sd: Jeg opretter denne sag da jeg har en konsulent fra Netcompany som skal have administrator rettigheder til nedenstående servere.

autregweb.sst.dk ( skal have adgang til Aut dbérne)

Captia1.sst.dk

Captia2.sst.dk

crmprod.sst.dk

crmprod02.sst.dk

DMZSQL2005.sst.dk

crmpint01.sst.dk

crmscribe.sst.dk

lanmssql2.sst.dk ( skal have adgang til crm dbérne)

captiatest.sst.dk

CRMTEST.sst.dk

crmitest.sst.dk

sql1test.sst.dk ( skal have adgang til crm dbérne)

sstdemocms.sst.dk

BYGUDV01.sst.dk

CRMUDV01.sst.dk

crmiudv01.sst.dk

lanmssql1udv.sst.dk ( skal have adgang til crm dbérne)

crmsqludv01.sst.dk

udvikling01.sst.dk

udvikling02.sst.dk

udvikling03.sst.dk

udvikling04.sst.dk

udvikling05.sst.dk

samt database adgang til NaviStatProxyTest og findes på lanmssql1udv

NaviStatProxyProd og findes på lanmssql2

Dette skal de have for at kunne udvikle , teste og drifte CRM systemet

## Spoop

Kontrollerer at læger ikke skriver for meget medicin ud.

SPOOP skal også håndtere medicin ordineret på et sygehus afsnit?

Tillægs db på AUT stamdata ift. datakilden (på LanMSSQL2) og på db2: YDR & YDR2 db (på SST3/ OSLO)

Det er Thomas Tjørnelund Nielsen (THTN) der har styr på Yderregisteret, og som kan hjælpe med opslag.

Det viser sig at der er det gamle register: YDR, der i 2012 blev afløst af det nye YDR2, der dog er i et lidt anderledes format.

Man kan søge i vSOP. Stamdata efter Anders:

SELECT navnekode, cpr,navn1,navn2,adresse1,adresse2,adresse3,postnr,autid,koen,kommunenr,fagkode

,f.v\_fagkodenavn, tilsyn

FROM [BI\_SST\_Baseline].[Aut].[vSOP\_Stamdata] s

join [BI\_SST\_Baseline].[Aut].[vSOP\_Faggruppeliste] f

on s.fagkode = f.c\_fagkode

where --fagkode not in (5433,7170) and

navn1 like 'Ander%'

and navn2 like 'nørg%'

Grunden til vi ikke fik mere end 1 Anders i første forsøg skyldes at han har forskellig autorisationskode for hver arbejdstype.

Gl Version i prod.

### SPOOP-data er klar for <måned> 20xx efter 26/3/2020

Grundet manglende opdatering (lanmssql2.sst.dk kan IKKE opdateres, ved at blive udfaset.) Ny Procedure:

Vi har aftalt at vi er nødt til at lave et workaround de sidste 2 måneder af Lanmssql serverens liv.  
  
Til det formål har jeg som aftalt oprettet grupperne:  
sst\spoop\_g\_lms\_import\_w   der via   sst\spoop\_l\_lms\_import\_w har contributer privilegier på share lanmssql2.sst.dk\SOP\_LMS\_Import hvor sst\pptadmin er meldt ind.  
og   
sst\spoop\_g\_lms\_import\_r   der via   sst\spoop\_l\_lms\_import\_r har læse privilegier på share lanmssql2.sst.dk\SOP\_LMS\_Import hvor sst\adm-pesp er meldt ind.  
  
hermed har pesp læse adgang og ppt skrive adgang på det share hvor SPOOP data skal afleveres, da det er her SPOOP systemet (Effektor / det gamle) henter data. (efter næste logoff & logon)

Fremover procedure bliver:  
1) ppt henter analysedata fra LAR-databasen  i 2 stk .csv filer, der afleveres til oslo.dksund.dk  -  mappen: ”home/dksund.dk/svb\_rbtbi\_spo\_upl/incoming"  
  
2)  ppt henter analysedata fra LAR-databasen  i 2 andre .csv filer, der afleveres til   
[\\lanmssql2.sst.dk\SOP\_LMS\_Import](file:///\\lanmssql2.sst.dk\SOP_LMS_Import)

*ls F:\ImportData\SOP\_LMS\_Import*

3) SPOOP/Effektor henter så data direkte fra [\\lanmssql2.sst.dk\SOP\_LMS\_Import](file:///\\lanmssql2.sst.dk\SOP_LMS_Import)  
  
4) rbtbi (Ny SPOOP) henter så data direkte fra oslo.dksund.dk  -  mappen:   
”home/dksund.dk/svb\_rbtbi\_spo\_upl/incoming"

IOS skal IKKE blandes ind i ovenstående, da vi ikke har indflydelse på flowet.

Vi kan rdp til lanmssql2

checke F:\ImportData\SOP\_LMS\_Import se nedenfor

Her vises f.eks. april & maj måneds data klar til at blive hentet af effektor.

PS M:\ps1> f:

PS F:\> cd .\ImportData\SOP\_LMS\_Import

PS F:\ImportData\SOP\_LMS\_Import> ls

Directory: F:\ImportData\SOP\_LMS\_Import

Mode LastWriteTime Length Name

---- ------------- ------ ----

-a--- 19-05-2020 09:45 48386 adrlist\_202004.csv

-a--- 05-06-2020 17:12 48333 adrlist\_202005.csv

-a--- 19-05-2020 09:45 59118413 ap4dat\_202004.csv

-a--- 05-06-2020 17:12 61484033 ap4dat\_202005.csv

Når PPT sender Servicerequest, går vi ned på serveren og checker F:\ImportData\SOP\_LMS\_Import, og hvis alt er ok, svarer Vi:

” Kontrolleret data for 202005, ligger klar på F:\ImportData\SOP\_LMS\_Import og venter på effektor

Dato: <dato for csv-filer>

Sag lukket

Mvh Mikael”

Og lukke sagen.

Vi kan IKKE kontrollere om effektor har hentet data.

### ~~SPOOP-data er klar for <måned> 20xx~~

Peter Plinieus leverer data til ftp.LMSdetail.dk (ekstern) mail/ sag i nilex

Svar på forespørgsel: ”Vi checker IKKE leveringen automatisk.

Til gengæld kører det hele pr. automatik, så når Spoop data ankommer, bliver de automatisk processeret i PowerShell der kører hver morgen kl. ca. 03:30.

Derefter kører der et Jams-Job ca. kl: 06:00 hver morgen, der processerer data videre, (jeg ved desværre ikke hvorhen), men data kommer umiddelbart til rigtige destination.

Når PPT sender Servicerequest, går vi ned på serveren og checker output fra powershell jobbet, og hvis alt er ok, svarer Vi:

” Kontrolleret i log, kørt ok d. <dato for kørsel>

og lukker sagen

Hvis der opstår problemer, kan vi bruge denne sag til at kontrollere hvornår ppt har sendt SPOOP data, vi checker loggen for at kontrollere at alt er gået godt, og at logdato svarer til den dag ppt har angivet, og så må vi checke Jams-Log for at se hvad der så kan være gået galt

Og ppt kan så bruge disse sager for at se at vi har sagt god for modtagelsen.”

#### LanMssql2.sst.dk

Indenfor de næste par dage hentes data til LanMssql2.sst.dk (der køres PowerShell script: E:\Import\SOP\sshfileretriever.ps1 der sender mail til ([mive@ssi.ad](mailto:mive@ssi.ad)) rettet til: [mon.sop@sundhedsdata.dk](mailto:mon.sop@sundhedsdata.dk) om vellykket kørsel.

Csv. Fil kan forefindes i E:\Import\SOP\dl, E:\Import\SOP\work og E:\Import\SOP\new foldere

Næste morgen kl 04:00 køres JAMS job der viderebehandler .csv filen

Log over kørsler appendes til: E:\Import\SOP\logs\ sshfileretriever.txt

>

2017-11-25 03:30:03 Starting script

2017-11-25 03:30:03 Logging on to ftp.LMSdetail.dk to retrieve files

2017-11-25 03:31:28 Files transferred 2

2017-11-25 03:31:28 work\adrlist\_201710.csv

2017-11-25 03:31:28 File converted, made ready for import in New and archived in dl folder

2017-11-25 03:31:28 work\ap4dat\_201710.csv

2017-11-25 03:32:37 File converted, made ready for import in New and archived in dl folder

2017-11-25 03:32:37 Finished run without errors

>

Herefter kan SPOOP sagen markeres som løst.

”Kontrolleret i log, kørt ok d. 6/11/2019

mvh Mikael”

hvis den ikke skriver tilsvarende; kontaktes BIDR & CIBF

Javascript har ikke koden.

Kube brænding

Db: D3\_SOP,K5451\_SST\_SOP\_STAGE,SOP\_LOG

Rehfeldt (Susanne Søger, Birgitte Smidt Holm, Theis Romose, programmør: Natacha Amuah)laver ny version til overtagelse.

Spørg Charlotte om der er nogen hos Rehfeldt der kan hjælpe os, hvis der er noget galt.

Dsdn = Sundhedsdata nettet.

KOES = Økonomisk dmz mellem os og kommuner

Lars Ryslander

Ny på lanmssql2

TAS – Tilskudssystem

System som Departementet bruger til at registrerer og styre ansøgninger og bevillinger omkring tilskud.

Test sql: s-mssql-db-03t.dksundtest.dk\MSSQLSERVER\SUMTAS\_Test

Prod sql: s-wdb4-p.dksund.dk\MSSQLSERVER\SUMTAS

DB Bruger oprettes af tas systemet, og Login skal oprettes af MSSQL DBA. Har aftalt at der skal prøves med SQL/AD Brugertilgangs & Ressource grupper

Systemforvalter ATSN

Leverandør kontakt: FormPipe Software, Fatih Öksüz tlf: +4572208321

## MRSA

Jeg er projektleder på elektronisk MRSA-indeberetning, som firmaet HyperLead v. Lars Anker Steen og Kenneth Agerskov arbejder i.

Anders Koch

Senior Researcher, MD, PhD, MPH

Professor in Infectious Diseases, Ilisimatusarfik, University of Greenland

Specialist in Infectious Diseases and Tropical Medicine

Department of Infectious Disease Epidemiology and Prevention

T +45 3268 3964 | M +45 2986 8802 | E ako@ssi.dk

Eks.keag bedes gives dbo adgang til følgende sql databaser:

· sql server mrsaapptestdb.dksundtest.dk som er et alias for S-MSSQL-01T

o e\_mrsa

o mrsaApp

· Sqlssqlserver mrsaappdb.dksund.dk som er et alias for S-MSSQL-DB-01P

o e\_mrsa\_test

o mrsaapp\_test

## Snit5, snit8, snit11

databaserne Snit5-betalingsoplysninger og Snit11-afregningsdatabasen.

## FSK Forskerservice

Kontaktperson LSL ved fejl

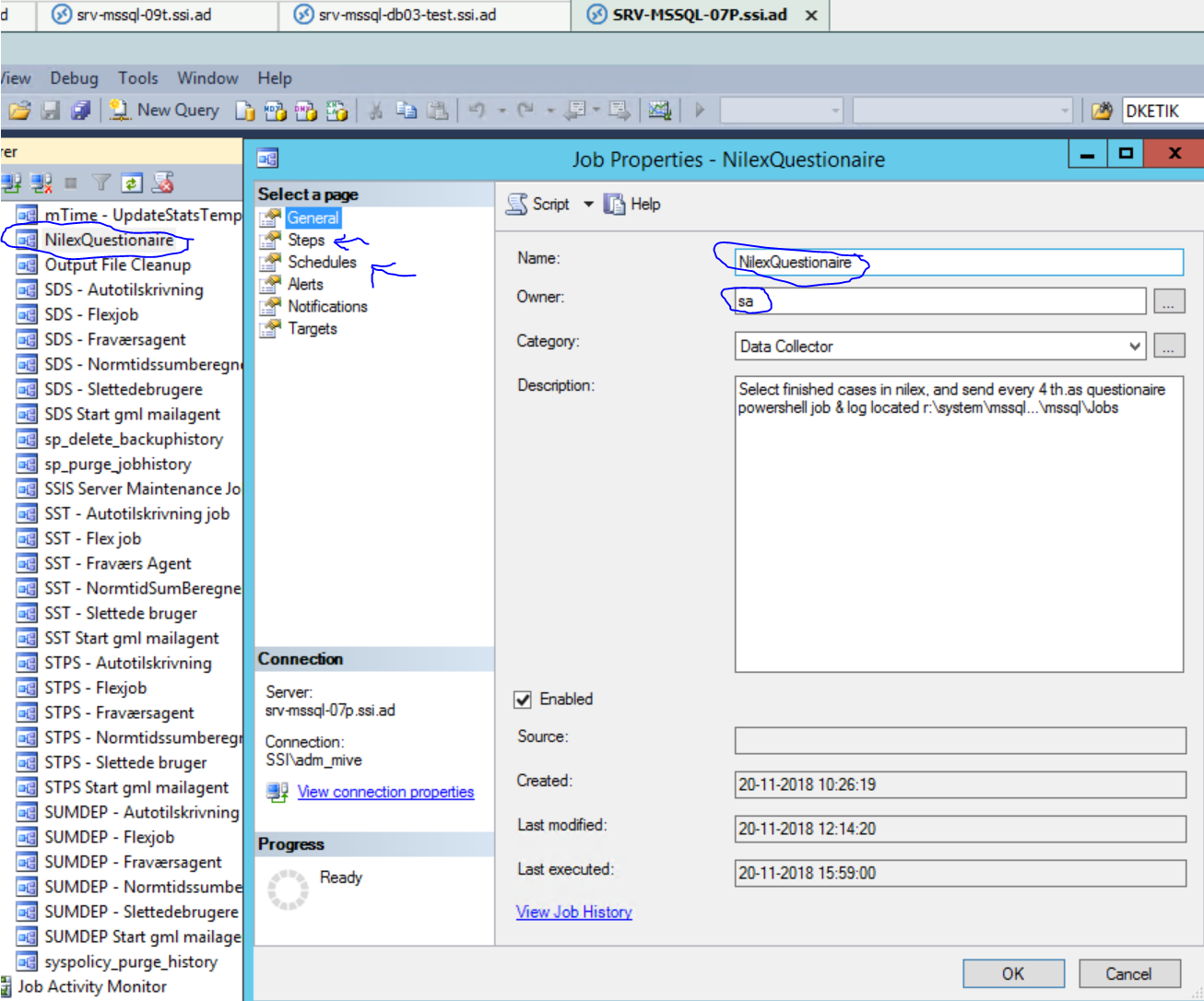
De administrerer selv

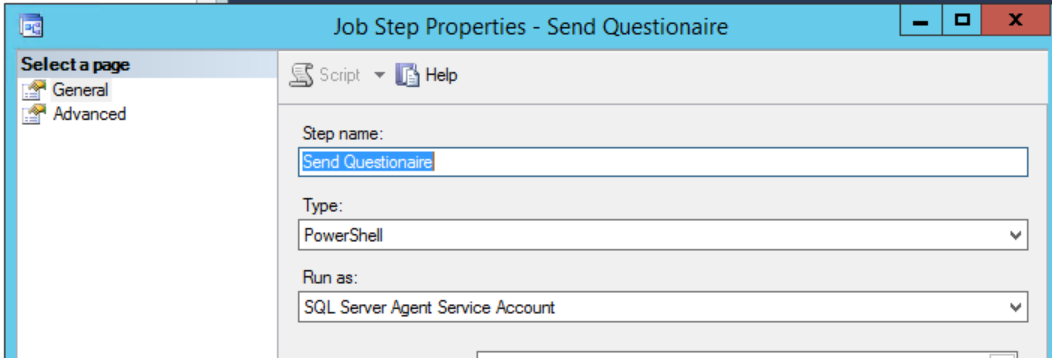
SQL og andre licenser -75%

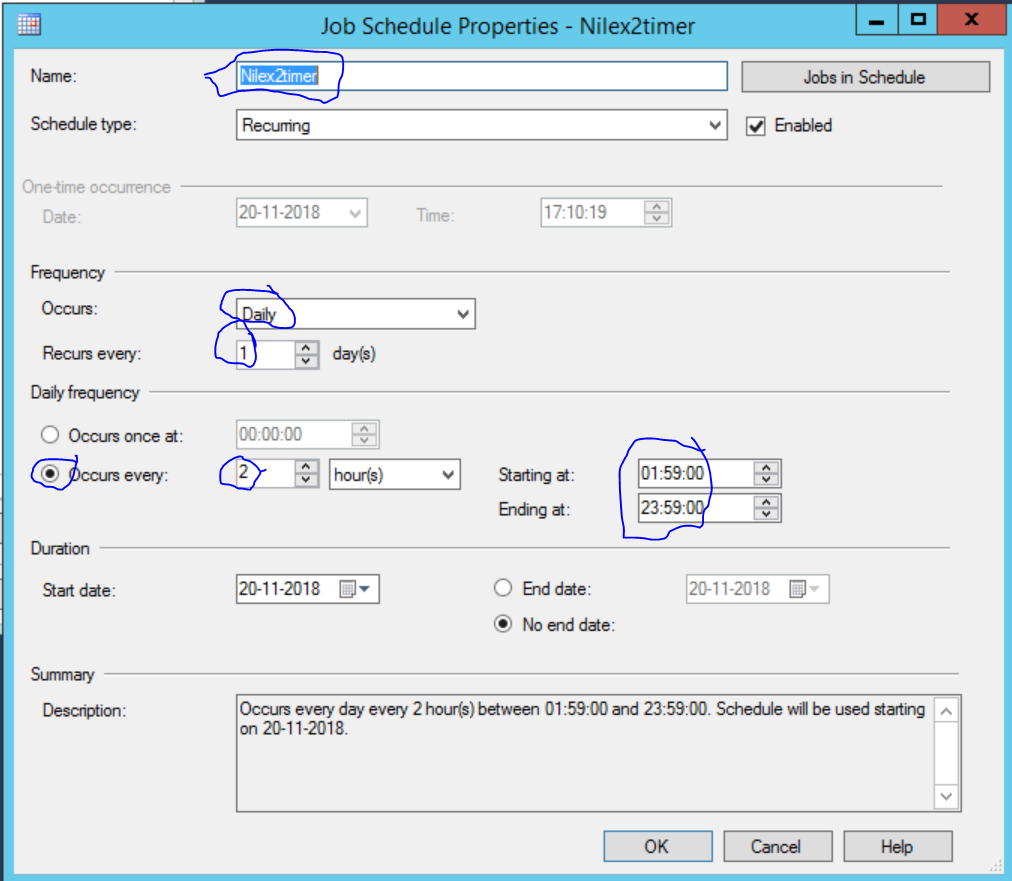
## Nilex Spørgeskemaer

På server srv-mssql-07p.ssi.ad

SQL Agent Job: NilexQuestionaire

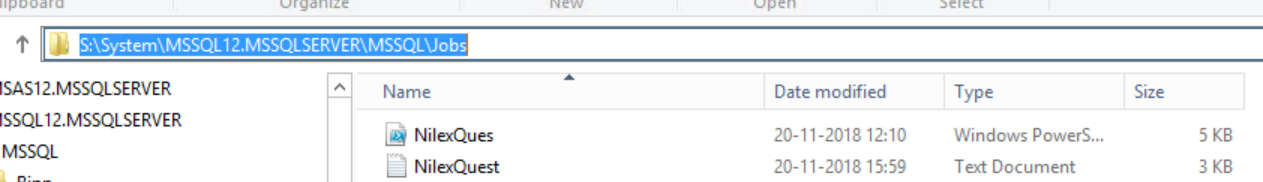




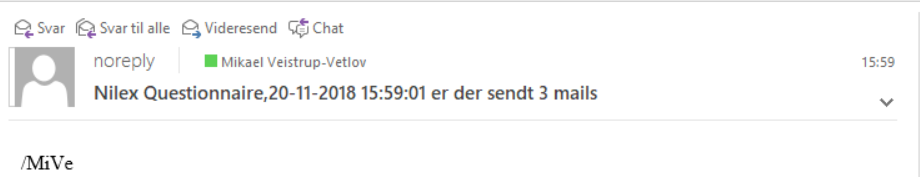


Job er gemt på S:\System\MSSQL12.MSSQLSERVER\MSSQL\Jobs

Hvor loggen også bliver gemt.



Der sendes status log besked hver gang jobbet kører og der har været sendt spørgeskema ud.



Jeg har sat jobbet til at køre hver 2 timer hver dag fra 1:59 til 23:59  
  
den vælger hver 4 lukkede sag, og skulle gerne være sikret mod at få sendt dubletter.  
  
Mail der sendes til de udvalgte slutbrugerne ser ud som nedenstående

>>

Jeg har sat jobbet til at køre hver 2 timer hver dag fra 1:59 til 23:59  
  
den vælger hver 4 lukkede sag, og skulle gerne være sikret mod at få sendt dubletter.  
  
Mail der sendes til de udvalgte slutbrugerne ser ud som nedenstående

>>

>>