MS SQLServer ylläpitosuunnitelman teko-ohje

- Palvelin tietokoneiden sijoituspaikka, varajärjestelmät, tietoturva:
  - Onko laitteiden sijoituspaikka sopiva?
    Ilmastointi? Kulunvalvonta? Varmistusnauhojen sijoitus muualla kuin palvelin tietokoneet? Vai käytetäänkö verkkolevyjä varmistukseen, ja onko ne sijoitettu muihin toimitiloihin esimerkiksi tulipalon vuoksi. Entä jos jotain menetetään niin miten toimitaan, kun palvelin rikkoutuu, konehuone vaurioituu tulipalossa tms?
  - Tarvitaanko vara järjestelmät?
    Onko vara järjestelmät kyllin kaukana varsinaisista järjestelmistä?
    (Maanjäristykset, tulipalot, tulvat tms.)
  - Virran syöttö palvelin tietokoneisiin ja muihin kriittisiin laitteisiin?
    UPS? (mitä laitetaan ups:eihin?)
    Onko oma virran syöttö laitteisiin, joka on eri kuin toimitilan muihin käytetty virran syöttö?
    Miten ilmastointi on järjestetty?
  - Palvelin tietokoneen käyttöjärjestelmän ylläpito?
    Varmistukset? Jos salausavaimia käytetään tietoturvan aikaan saamiseksi, onko avainten varmistus kunnossa? (Tässä tarkoitetaan lähinna MS Windows Server 2003:n ja 2008:n Windows autentikoinnin salakirjoitus avaimia, mutta muissakin tilanne on samankaltainen).
  - Kuinka kauan aikaa kestää rakentaa järjestelmä uudelleen jos tarve tulee?
    Tarvittavat laitteistot (palvelin tietokone, tietoliikenne verkko ja aktiivilaitteet)?
    Käyttöjärjestelmä (lisenssinumerot, verkkoyhteys asennuksen aikana)?
  - Tietoturva?
    Onko tietoliikenneverkon tietoturva kunnossa?
    Päivitys tiheys ja miten se tehdään? (automaattisesti ehkä suoraan verkosta?)
    Virustorjunta? (päivitykset?)
    Käyttäjä politiikka? (autentikointi, authorisointi - asiaa käsitelty alla)

- Tietokantojen ylläpito:
  - Tietokanta kannattaa olla omalla kiintolevyllään.
    Ja käyttöjärjestelmä ja muut järjestelmät omalla levyllään.
    Loki myös voisi olla omalla levyllään.
  - Varmistus:
    Otetaan tietokannoista alkuun `Full` backup ja varmistetaan että onnistuu aina virheettömästi.
    Myöhemmin kun dat nauha tai varmistus verkkolevy alkaa täyttyä, ryhdytään ottamaan sopivalla frekvenssillä: `full backup`, `diff backup`, `diff backup`,...,`full backup` (esim. viikon tai kuukauden tms.)
    Ennen kuin varmistus otetaan, on aina tarkistettava, että tietokannat ovat kunnossa (eivät ole liikaa fragmentoituneet tai pahimmassa tapauksessa korruptoituneet).
    Vasta sen jälkeen tehdään varmistus `verifyonly` ja `checksum` päällä kiintolevylle, josta vasta kopioidaan varmistus nauhalle. Jokaisen varmistuksen jälkeen on tarkistettava varmistusloki.
  - Varmistetaan seuraavat systeemin tietokannat:
    `master.mdf`
    `msdb.mdf`
    `model.mdf`
    `temp` (normaalisti tätä tietokantaa ei tarvitse varmistaa – mutta tapauskohtaisesti voi tarvetta olla)
    data tietokannat tietysti myös,
    ja transaktio loki varmistetaan myös
    Kuka hoitaa varmistuksen?
  - Millainen käyttäjäryhmä ja käyttäjäpolitiikka otetaan käyttöön?
  - Single user tyyppinen hätäkäynnistys on pystyttävä tekemään. Harjoittele siis sitä, että osaa hätätilanteessa.
  - Mikä Recovery Model on eri palvelinten tietokannoissa käytössä (`Full`, `Simple`,...)
  - `sa` –käyttäjän salasana pitää olla tiedossa. Tarvitaan single user tyyppisessä hätäkäynnistyksessä.

- MS SQL Server:ssä mielellään vain yksi instanssi. Jos useampia niin per instanssi jää tätä vastaava murto osa keskusmuistista käyttöön, mikä ei ole hyvä asia. Keskusmuistia halutaan tavallisesti varata mahdollisimman paljon tietokanta instanssin käyttöön, jolloin sen toiminta on nopeutuu.
- Kun tietokanta on pystyssä, on tehtävä tehomittaukset MS SQLServer palvelimesta.
  (Counter: transaction/sec
  (Counter: …
- Miten schemoja on käytetty?
  Mielellään on oltava tietokannassa omat käyttäjät ja mielellään myös käyttäjäryhmät omine turvallisuus politiikkoineen.
- Millaista autentikointia käytetään MS SQL Server:ssä.
  Windows Authentication (tällöin MS SQL Serverin käyttäjät on oltava myös käyttöjärjestelmässä) vai onko käytössä Mixed Authentication eli Windows Authencation ja SQL Server Authentication ovat käytössä yhtäaikaa.
- Mille kiintolevylle ja mihin hakemistoon `mdf`:t ja `ldf`:t on tallennettu.
- Millä merkistöllä (collotation) tietokanta on luotu.
  Ehkä `Finnish_Swedish_CI_AS`?
  Tärkeä tietää hätäkäynnistyksessä ja data tietokantoja importattaessa (siis kun tietokannan datat importataan toiselle palvelintietokoneelle).
- Ylläpidon työasema pitää varustaa siten, että sillä voi etäylläpitää tietokantapalvelinta (pitää olla Management Studio, Performance Monitor, jossa tarvittavat counter:t tietokannan seurantaan.
- Onko MS SQLServer:ssä raportointi asennettuna (edellyttään IIS ja ASP.NET:iä).
- Onko MS SQLServer:n käyttämä portti 1433 vapaana SQL Server:lle, ja onko se asian mukaisesti otettu huomioon palomuurissa? Siis tukittu. Tosin Standalone UI tarvinnee tämän auki (jos tällaisia ohjelmia on käytössä).
- Testaa ettei vain pysty hyökkäämään MS SQLServeriä vastaan tyyliin:
  Käyttöliittymän kirjoittaa vain:
  `' OR 1=1 – xp_cmdshell`
- Alert:it käyttöön.
  Performance Monitoriin päälle hälytykset error level:lle 19…25. Ja näistä hälytyksistä email ylläpidon postiin.
  Myös kirjautumisten seuranta trace properties seurantaan.
- Database Engine Tuning
  Onko siis tietokantojen indeksoinnit riittävän hyvät ja kunnossa (eli eivät ole liian fragmentoituneet).
  Onko kyseessä päivitys vai raportointi tietokanta – tästä riippuen indeksointi voi olla hyvinkin erilainen.
- Varmista että `guest` käyttäjä on ainakin `disable` tilassa.
- Indeksien pirstoutumista (fragmentoitumista) pitää ylläpidon seurata säännöllisesti.
  Ja jos on pirstaleisia, niin pitää ajaa:
  `alter index … reorganize` tai `rebuild` riippuen kuinka fragmentoituneita ovat.
  Indeksit muuten kannattaa tallentaa mielellään omalle kiintolevylle. Nopeuttaa tietokannan toimintaa.
- Onko data levyn koko riittävä.
  `kanta.mdf`:n inkrementti mielellään n. 10MB – ei missään tapauksessa prosenttilukuna.
  Mikä on levyn maksimi koko?
  Looginen nimi?
- Indeksit luotu mielellään 70…95 fillfactor:ia käyttäen (siis tällöin olisi kyseessä päivitystyyppinen tietokanta – raportointi tyyppiselle tietokannalle arvo on eri).
  Ja muistetaan tehdä defragmentointi myös tietokannalle jos < 30 %:ia.
  -> reorganize
- Tietysti aina ennen varmistusta on tarkistettava, että varmistettavat tietokannat ovat virheettömiä ja ehyitä.
- Onko varmistusnauhuri itse palvelintietokoneessa (ei siis mielellään niin, että joutuu tekemään varmistusnauhoituksen yli verkon! Tosin nykyään on alettu yhä enemmän käyttää verkkolevyjä varmistukseen).
- Mikä on pisin aika mikä voidaan varmistuksen takia menettää dataa?
  Mikä aika siedetään?
  Koko päivän työ vai halutaanko että varmistus tehdään niin tiheästi että ei menetetään niin paljon?
- Tarvitaanko ns. Standby tyyppinen palvelin (esim. raportoinnin nopeuttamiseksi)?
- Miten `grant`:ia on käytetty käyttäjäryhmä ja käyttäjätunnus tasolla oikeuksissa?

- SQL Server:in lisenssinumero (ja cd-levy jos on asennettu siltä alunperin)?
  Muiden tässä yhteydessä tarvittavien sovellusten lisenssinumero (ja myös asennus cd-levy jos on)?
- Kannattaako replikointia käyttää?

- Siis ylläpidon tehtäviin kuuluu jatkuvasti (päivittäin):
  - Ottaa tietokantojen varmistukset
    (voi automatisoida, mutta aina on varmistettava että varmistus on onnistunut)
  - Pitää indeksejä yllä
    (ovatko pirstoutuneet eli fragmentoituneet – jos ovat, niin rakentaa ne uudelleen)
  - Tehdä säännöllisesti sopivin väliajoin tilastointiajoja.
    (niiden perusteella voi suunnitella tarvittavat hankinnat, keskusmuistin, prosessoreiden, kiintolevyjen, verkkokortin kapasiteetin alkaessa pikku hiljaa loppumaan).
  - Seurata kiintolevyjen täyttymisastetta.
  - Seurata palvelimen suoritusastetta laskureiden avulla.
  - Seurata täytyykö loki
    (riittääkö levytila lokitiedostojen tarpeisiin).
  - Sekä seurata ettei palvelimen muistinkäyttö aste nouse yli 90%:ia.