
# Konfiguraationhallintajärjestelmän reaaliaikainen varmuuskopiointijärjestelmä

Heini Porri-Henttinen

Valvoja: Prof. Jorma Virtamo
Ohjaaja: DI Ari-Pekka Virta, Digia Oyj

# Sisältö

- Työn tausta
- Tietokannat ja varmuuskopiointi
- Katastrofitilanteesta toipuminen (Disaster Recovery)
- Digia Oyj:n konfiguraationhallintaympäristö
- Työssä käytetyt metodit
- Nykyisen varmuuskopiointijärjestelmän epäkohdat
- Mahdolliset ratkaisuvaihtoehdot
- Johtopäätökset

# Työn tausta

- Liiketoiminnalle kriittinen data on yleensä varastoitu tietokantapalvelimilla sijaitseviin tietokantoihin.
- Varmuuskopiointijärjestelmän kehittämiselle varataan harvoin tarpeeksi resursseja.
- Puutteellisen varmuuskopioinnin riskejä ei osata hahmottaa.
- Digia Oyj:n konfiguraationhallintaympäristön varmuuskopiointijärjestelmän nykytilaa ei ole kartoitettu.
- Liiketoiminnallinen jatkuvuus halutaan taata myös katastrofitilanteissa.

# Tietokannat ja varmuuskopiointi

- Tietokannoista voidaan ottaa sekä loogisia että fyysisiä varmistuksia.

  - Loogisia varmistuksia otettaessa tallennetaan vain data, ei sijaintia. Loogisia varmistuksia käytetään esimerkiksi objektien siirtämiseen tietokantojen välillä.

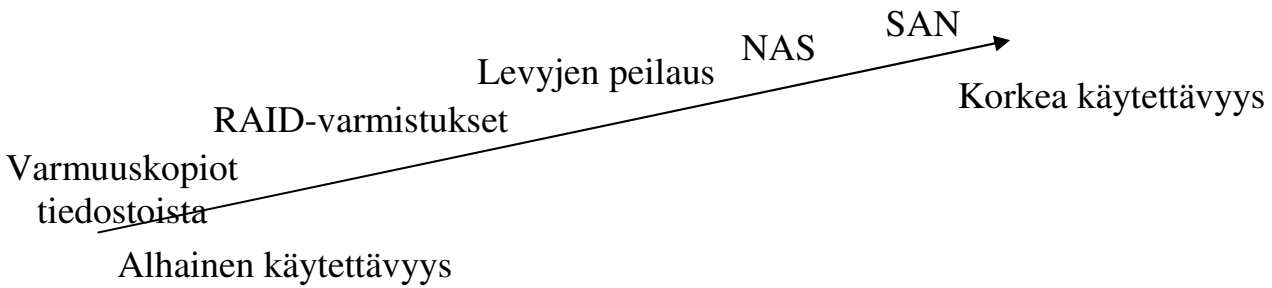
  - Fyysisiä varmistuksia otettaessa kopioidaan datatiedostot ja sijainti. Fyysiset varmistukset voivat olla erillisvarmistuksia (offline backup), jolloin tietokanta on alhaalla varmistuksen ja palautuksen ajan tai suoria varmistuksia (online backup), jolloin tietokanta on ylhäällä ja käytettävissä koko varmuuskopiointitoiminnon ajan.

# Tietokannat ja varmuuskopiointi: varmistus-strategia

- Varmistusmetodit voidaan jakaa kolmeen pääluokkaan:
  - Täydellinen varmuuskopiointi (Full Backup)
    - Kopioidaan kaikki data.
  - Asteittainen varmuuskopiointi (Incremental Backup)
    - Tehdään täydellisten varmistusten välissä, jolloin kopioidaan edellisen varmistuksen jälkeen muuttunut data.
  - Eroavuuskopiointi (Differential Backup)
    - Tehdään täydellisten varmistusten välissä, jolloin kopioidaan data, joka on muuttunut edellisen täydellisen varmistuksen jälkeen.

# Tietokannat ja varmuuskopiointi: reaali-aikaisuutta ja käytettävyysastetta parantavat menetelmät

- Levyjen peilaus (mirroring)
- RAID-varmistukset (Redundant Array of Inexpensive Disk)
- NAS (Network Attached Storage)
- SAN (Storage Area Network)



# Katastrofitilanteesta toipuminen

- Toipumista tilanteesta, jossa järjestelmä on tuhoutunut käyttökelvottomaksi, kutsutaan nimellä Disaster Recovery.
- Tuho voi saada alkunsa esimerkiksi luonnonmullistuksesta, onnettomuudesta tai tahallisesta vahingonteosta.
- Tuhosta selviytymiseen on varauduttava etukäteen tehtävällä suunnitelmalla (Disaster Recovery plan):
    - Suunnittelu
    - Kriittisen datan tunnistaminen
    - Sopivan politiikan ja proseduurien luominen
    - Varmuuskopiointityyppien määritteleminen
    - Suunnitelman testaaminen ja ylläpito

# Digia Oyj:n konfiguraationhallintaympäristö

- Viisi Solaris 9 –palvelinta sijoitettuna eri sijaintipaikoille (Helsinki, Kuopio, Lappeenranta, Oulu, Pori)
- Jokaisella palvelimella on toiminnassa Telelogic Synergy/CM 6.4 ja Informix Dynamic Server 9.4
- Kokonaistietokantakoko eri sijaintipaikoilla vaihtelee 30 megatavusta 55 gigatavuun
- Objektien (kuten projektit, kansiot, taskit) jakaminen tietokantojen välillä on mahdollistettu hajautetulla konfiguraationhallinan työkalulla, DCM:llä (Distributed Configuration Management)
- DCM-palvelin toimii asiakasrajapintana. Eri sijaintipaikoilla olevat palvelimet toimivat keskenään DCM-klusterina.

# Digia Oyj:n konfiguraationhallintaympäristö: varmuuskopioiminen

- Synergy/CM –palvelimien  tietokannoista otetaan täydellisen varmistuksen varmuuskopiot synergyn *ccmdb backup* –metodilla arkiöisin.
- Varmuuskopioinnin ajaksi tietokannat ajetaan alas.
- Tiedostojärjestelmän tarkistus ja väliaikaismuistin tyhjennys ajetaan viikonloppuisin.
- Varmuuskopioitu data siirretään FTP-yhteydellä Windows-palvelimella sijaitsevaan tietokantavarastoon.
- Tietokantavaraston varmuuskopioiminen on suoritettu kolmannen osapuolen toimesta.
- Varmuuskopiointi ja FTP-siirto on automatisoitu skriptein.

# Työssä käytetyt metodit

- Kartoitettiin konfiguraationhallintajärjestelmän varmuuskopiointijärjestelmä.
- Toimivuutta tutkittiin päivittäisen käytön yhteydessä sekä työtä varten asennetun testipalvelimen avulla.
- Web-sivustoilta etsityn tiedon perusteella vertailtiin kolmen ennalta määrätyn varmuuskopiointijärjestelmiä tuottavan yrityksen (HP, EMC, Veritas) varmuuskopiointi ratkaisuvaihtoehtoja.

# Nykyisen varmuuskopiointijärjestelmän epäkohdat 1/2

- Varmuuskopioiminen vie aikaa; projektikantojen vaihtelevasta koosta johtuen varmuuskopioiminen kestää 10 minuutista seitsemään tuntiin.
- Varmuuskopioinnin aikana ei voi työskennellä; varmuuskopioinnin ajaksi projektien tietokannat ajetaan alas, jolloin kaikki sillä hetkellä käynnissä olevat yhteydet tietokantaan katkeavat.
- Siirrot vievät aikaa ja resursseja; isojen tietokantojen FTP-siirrot kuormittavat verkkoa.

# Nykyisen varmuuskopiointijärjestelmän epäkohdat 2/2

- DCM-siirrot voivat keskeytyä tai varmuuskopioita voi jäädä ottamatta isojen DCM-siirtojen johdosta, koska
  - DCM-siirrot vaativat resursseja,
  - pakettien siirtoon ja tietokantaan purkuun voi yhteensä kulua aikaa kahdeksankin tuntia,
  - isot siirrot aloitetaan pääasiassa työajan jälkeen,
  - mikäli siirto on päällä varmuuskopioinnin alkaessa, se katkeaa.
- Mahdolliseen katastrofitilanteeseen ei ole varauduttu.
- Nykyisessä varmuuskopiointijärjestelmässä ei ole reaaliaikaisuutta eikä tiettyyn ajanhetken palautusta.

# Mahdolliset ratkaisuvaihtoehdot 1/4

- Haettiin järjestelmää,
  - joka pystytään helposti ja vähäisin kustannuksin sisällyttämään tämän hetkiseen ympäristöön,
  - joka lisää järjestelmän reaaliaikaisuutta,
  - jolla pystytään parantamaan työskentelytehokkuutta ja vähentämään tietokannan alhaalla oloaikaa,
  - jolla pystytään varmistamaan kriittinen data sekä normaali- että katastrofitilanteissa.

# Mahdolliset ratkaisuvaihtoehdot 2/4

- Tutkitut ratkaisuvaihtoehdot:
  - HP Data Protector –varmistusohjelmisto ja EVA-levyjärjestelmä
    - Virtuaalinen levyjärjestelmä on varustettu kuituliitännöillä.
    - Suurin osa varmistusohjelmiston ominaisuuksista vaatii toimiakseen SAN-ympäristön.
    - Pää varmistusominaisuudet:
      - tilannevedokset (snapshot),
      - kohdistuskopiot (snapclone),
      - välitön toipuminen (Instant Recovery)
      - ZDB (Zero Downtime Backup) –ominaisuus
      - tiettyyn ajanhetkeen palautuminen (point-in-time-recovery)
      - Bare-Metal –palautus

# Mahdolliset ratkaisuvaihtoehdot 3/4

- EMC:n Legato NetWorker –varmistusohjelmisto ja CLARiiON CX -tallennusjärjestelmä
  - CLARiiON CX –tallennusjärjestelmä on varustettu sekä kuitu- että ATA-liitännöillä
  - Varmistusohjelmisto ja tallennusjärjestelmä toimivat sekä SAN- että LAN-ympäristössä.
  - Pää varmistusominaisuudet
    - Tilannevedokset (snapshot),
    - toipumisen hallinta (Recovery Manager) katastrofitilanteita varten
    - tietokantamoduuleilla suora varmuuskopiointi eri tietokantaohjelmistoille
    - tiettyyn ajanhetkeen palautuminen (point-in-time recovery)

# Mahdolliset ratkaisuvaihtoehdot 4/4

- Veritas NetBackup
  - Yhteensopiva CLARiiON CX –tallennusjärjestelmän kanssa
  - Pää varmistusominaisuudet
    - Tilannevedokset (snapshot)
    - välitön toipuminen (Instant Recovery)
    - tiettyyn ajanhetkeen palautuminen (point-in-time recovery)
    - synteettinen varmuuskopiointi
    - Bare-Metal –palautus kovoon, jonka ei tarvitse olla alkuperäinen.

# Johtopäätökset 1/2

- Nykyinen varmuuskopiointijärjestelmä ei ole riittävä, jotta liiketoiminnallinen jatkuvuus pystyttäisiin takaamaan myös katastrofitilanteessa.
- Varmuuskopiointijärjestelmän reaaliaikaisuuden puute kasvattaa datan häviämisprosenttia tilanteissa, joissa varmuuskopioitu data on palautettava järjestelmään.
- Erillisvarmistuksena suoritettava varmuuskopiointi haittaa DCM-siirtoja.
- Täydellisinä varmistuksina otettavat varmuuskopiot kuormittavat verkkoa.

# Johtopäätökset 2/2

- Työn tuloksena käyttöön otettavaksi suositellaan Veritaksen NetBackup –ohjelmistoa ja CLARiiON CX –tallennusjärjestelmä, koska
  - varmistusohjelmiston kloonaus- ja tilannevedosominaisuuksien avulla pystytään lisäämään reaaliaikaisuutta ja
  - varmistusohjelmiston synteettisillä varmuuskopioilla pystytään alentamaan varmistuksen oton ja siirron aikaista verkkokuormitusta,
  - katastrofitilanteista palautumista nopeutetaan Bare-Metal –palautuksella, jota ei välttämättä tarvitse tehdä alkuperäiseen kovoon.
  - CLARiiON CX –tallennusjärjestelmä tarjoaa vaadittavan levykapasiteetin ja se pystytään helposti sisällyttämään nykyiseen ympäristöön vaihtoehtoisten ATA-liitäntöjen johdosta.