

VAASAN AMMATTIKORKEAKOULU

Pasi Vainio

KORKEAN SAATAVUUDEN VERKKOPAL-
VELUT

Liiketalous ja matkailu

2009

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

TIIVISTELMÄ

Tekijä	Pasi Vainio
Opinnäytetyön nimi	Korkean saatavuuden verkkopalvelut
Vuosi	2009
Kieli	Suomi
Sivumäärä	60
Ohjaaja	Jarmo Laasanen

Riippuvuutemme tietoteknisiin järjestelmiin kasvaa jatkuvasti. Tämän myötä järjestelmien toimintavaatimuksille asetetaan enemmän vaatimuksia. Järjestelmien suunnittelu korkean saatavuuden näkökulmasta mahdollistaa järjestelmien luotettavuuden kehittämisen ja mittaamisen. HP BladeCenter -järjestelmällä, virtuaalisella levyjärjestelmällä ja oikeilla sovellusvalinnoilla voidaan saavuttaa yli 99 prosentin käytettävyys verkkopalvelulle. Esimerkkikokoonpanon toteutus on tehty Microsoftin ratkaisulla. Järjestelmä on rakennettu ja sen toimivuus testattu. Kolmen kuukauden tarkastelujaksolla vaatimukseksi asetettu 99 prosentin saatavuus palvelulle saavutettiin.

Asiasanat: verkkopalvelu, klusteri, kuormantasaus, levyjärjestelmä, korttipalvelin

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

ABSTRACT

Author	Pasi Vainio
Topic	High availability network services
Year	2009
Language	Finnish
Pages	60
Name of Supervisor	Jarmo Laasanen

The need for information systems is going to become more and more important in our daily lives. The requirements of these systems are increasing every day. If we design systems to meet high availability requirements, the systems will be more stable and more controlled. By using HP BladeCenter, virtual array disk storage and correct software solutions, we can get more than 99 percent of availability for the systems. The sample configuration for this thesis relied on Microsoft solutions. The system was fully installed and tested to run a high availability network service. During the three months testing period, service availability exceeded the set 99 percent requirement.

Keywords: high availability, network load balancing, cluster, SAN

SISÄLLYS

1. JOHDANTO.....	6
1.1 Työn ajankohtaisuus.....	6
1.2. Tavoitteet ja rajaukset.....	7
2. Korkean saatavuuden verkkopalvelut käytännössä.....	8
3. FYYSSINEN PALVELINYMPÄRISTÖ.....	9
3.1. Korttipalvelinratkaisut.....	9
3.2. Tietoliikenneyhteydet.....	11
3.3. Aktiiviset palomuuriklusterit.....	12
4. VIKASIETOISET LEVYJÄRJESTELMÄT.....	14
4.1. SAN-tallennusverkot.....	14
4.2. HP -levyjärjestelmät.....	14
5. SOVELLUSYMPÄRISTÖ.....	16
5.1. Kuormantasaus palvelinsovelluksissa.....	16
5.2. Failover-klusteroidut tietokantaratkaisut.....	17
5.3. Automaattiset vikailmoituspalvelut.....	18
6. KORKEAN SAATAVUUDEN VERKKOPALVELUN TOTEUTTAMINEN.....	20
6.1. Ympäristön kuvaus.....	20
6.2. Ympäristön suunnittelu.....	21
5.2.1 Verkkosuunnitelmat.....	21
6.2.2 Laitesuunnitelmat.....	23
6.3. Verkkoinfrastruktuurin rakentaminen.....	27
6.3.1 Yhteyksien tilaaminen.....	27
6.3.2 Kytkinten hankinta ja asennus.....	27
6.3.3 Kytkinten asetukset palvelimia varten.....	29

6.4. Palomuurien asentaminen ja käyttöönotto	30
6.4.1 Hallintapalvelin	30
6.4.2 Palomuurien käyttöönotto	31
6.4.3 Palomuurisäännösten luominen	32
6.5. Tallennusverkon rakentaminen	33
6.5.1 Tallennusverkon laitteiden asennus.....	33
6.5.2. SAN-kytkinten esiasennus	34
6.6. Levyjärjestelmän asennus ja käyttöönotto	37
6.6.1 Levyjärjestelmän valinta	37
6.6.2. Hallintapalvelimen asentaminen	38
6.6.3. Levyjärjestelmän asennus.....	39
6.7. Palvelinympäristön asentaminen.....	39
6.3.1. Palvelinkehikon asennus	39
6.3.2. Palvelinten asentaminen.....	40
6.3.3. Virtual Connect -moduulit.....	40
6.3.4. Käyttöönotto.....	40
6.8. Sovellusympäristön asentaminen	43
6.4.1 Hakemistopalvelin.....	44
6.4.2 Verkkosivustopalvelimet.....	44
5.4.3 Tietokantapalvelimet	49
7. TOIMIVUUDEN MITTAAMINEN	58
8. YHTEENVETO	60
LÄHTEET	61

1. JOHDANTO

1.1 Työn ajankohtaisuus

Kun tietotekniikkaa hyödynnetään yhä useammassa jokapäiväiseen elämäämme vaikuttavassa toiminnassa, riippuvuutemme järjestelmiin kasvaa. Jos pankkien, vakuutusyhtiöiden tai tärkeiden julkishallinnollisten tahojen verkkopalvelut menettävät toimintakykynsä, aiheutuu tästä mittavia ongelmia meille kaikille. Järjestelmien käyttöasteen kasvu lisää myös toimimattomuudesta aiheutuvia haittoja. Järjestelmät kuormittuvat suunniteltua nopeammin ja ne muuttuvat epävakaaiksi. Luotettavuus ja sen parantaminen ovat tämän päivän uusia haasteita tietojenkäsittelyssä.

Työssäni tutkin käytännönläheisesti erilaisia ratkaisuja, joiden avulla käytettävyyttä voidaan parantaa. Työn tuloksena luotava tietojärjestelmä voidaan hyväksyä tuotantoon ainoastaan 99 prosentin käytettävyydellä. Tällaiseen käytettävyyteen ei voida päästä ainoastaan sovellusten avulla. Laitteistot on suunniteltava alusta alkaen korkeaa käytettävyyttä silmällä pitäen. Kaikki työn laitteistotutukset on tehty HP:n laitteilla aina, kun sopiva laite on löytynyt valikoimista.

Nykyisessä päivätyössäni tarve suunnitella korkean saatavuuden palveluita näkyy selvänä kehitystarpeena asiakasrajapinnassa. Tietojärjestelmien vaatimukset muissakin kuin tietotekniikka-alan yrityksissä kasvavat jatkuvasti ja asiakkaat osaavat esittää enemmän vaatimuksia ympäristöilleen. Tilausta luotettaville tietojärjestelmille löytyy.

1.2. Tavoitteet ja rajaukset

Korkean saatavuuden palvelut voidaan jakaa useisiin osa-alueisiin, josta työssäni haluan keskittyä erityisesti laitteiston ratkaisuihin. Laitteistoratkaisut sinänsä eivät riitä toimivan ympäristön rakentamiseen, joten työstä ei tulisi yhtenäinen ilman sovellusten käsittelyä. Sovelluksia käsittelen perustasolla, mutta niiden asetukset eivät ole työn painopiste. Ympäristöt voidaan toteuttaa käytännössä millä tahansa käyttöjärjestelmäalustalla, mutta työssäni keskityn Microsoft-pohjaisiin ratkaisuihin.

Yksikään palvelinympäristö ei ole tuotantokelpoinen ilman toimivan fyysisen tietoturvan sekä aktiivisen palomuuriympäristön rakentamista. Fyysisestä tietoturvasta kirjoitan perusteita, palomuuureista käsittelen aktiivista palomuuriklusteria, jolla saavutetaan haluttuja palvelun saatavuusasteita.

Työn toteuttamisessa on käytetty työpaikalta saatua informaatiota ja laitteistoa. Tehtävässä kuvattava ympäristö ei ole todellisessa tuotantokäytössä, vaan käytetty ainoastaan opinnäytetyön testaamiseen. Todellisen ympäristön kuvaaminen ei olisi tietoturvakriteerien kannalta mahdollista, joten testiympäristön avulla pystyin testaamaan mahdollisimman todellista ympäristöä.

Toteutettava ympäristö koostuu verkkosivuston palvelimista, jotka käyttävät hyväkseen tietokantoja sekä käyttäjien hallintaan tarvittavaa aktiivihakemistoa. Palvelinympäristön toteuttamisen perusteet on käsitelty laitteiston toiminnan ymmärtämiseksi.

2. KORKEAN SAATAVUUDEN VERKKOPALVELUT KÄYTÄNNÖSSÄ

Tietojärjestelmiltä edellytetään yhä useammin toimivuutta vuorokauden ympäri vuoden jokaisena päivänä. Järjestelmät kuitenkin vaativat päivitysten asentamista, laitteistokokoonpanon muutoksia ja muita toimenpiteitä, joiden yhteydessä palvelukatkoksia ei voida välttää. Suunniteltujen katkosten lisäksi palveluiden käyttökatkokkien riskiä lisää laitteiden vikatilanteet, sähkökatkokset ja joissain tapauksissa jopa palvelinlaitetilaa koskevat suuremmat ongelmat, kuten tulipalot, vesivahingot tai muut vikatilanteet.

Palvelussa aiheutuva toimintakatkos saattaa aiheuttaa palveluntarjoajalle jopa tuhansien tai kymmenien tuhansien eurojen tappiot tai korvausvaatimukset. Lisäksi palvelutasosopimukseen on alettu kiinnittää enemmän huomiota ja korkeasta saatavuudesta maksetaan ylimääräistä palveluita tarjoaville yrityksille.

Mahdollisia toteutustapoja palvelun korkeamman saatavuuden aikaan saamiseksi on useita. Virtualisointiympäristöt kasvattavat suosiotaan kaikissa palvelintiloissa ympäri maailman tarjoten vikasietoisuuden ohella myös kustannustehokkuutta ja energiankulutuksessa tapahtuvia säästöjä. (VMWare. 2009)

Jos virtualisointi ei sovellu käytettävien sovellusten alustaksi, tai resurssien tarve on niin suuri, ettei virtualisointi ole taloudellisesti kannattavaa, voidaan korkean saatavuuden ympäristöt yhtä hyvin toteuttaa ns. perinteisemmällä ratkaisulla, käyttäen levyjärjestelmiä ja korttipalvelimia.

Korkeaan käytettävyyteen kykenevän järjestelmän suunnittelu on aloitettava täysin eri lähtökohdista kuin verkkopalvelun suunnittelu yleensä. Verkkototeutukset, palvelinten määrä ja laitevalinnat poikkeavat selkeästi ns. perinteisen verkkopalvelun toteutuksesta.

(Shimonski 2003, 316.)

3. FYYSINEN PALVELINYMPÄRISTÖ

3.1. Korttipalvelinratkaisut

Korttipalvelimet kasvattavat markkinaosuuksiaan jatkuvasti korvaten vanhoja räkkipalvelimia. Korttipalvelimien etuja ovat mm. alhaisempi virrankulutus, paremmat kytkentämahdollisuudet sekä mahdollisuus korvata palvelin toisella vastaavalla laitteen vikaantuessa.

Korttipalvelinympäristön laajentaminen ja ylläpito on helppoa verrattuna perinteisen mallisiin palvelimiin. Samoilla verkkokytkennöillä voidaan huolehtia koko palvelinkokonaisuuden yhteyksistä, eikä jokainen palvelin vaadi omaa kaapelointia. Lisäksi palvelinkehikko tarjoaa hyvät mahdollisuudet vikasietoisen verkon rakentamiseksi. Myös virtalähteet on useissa malleissa kahdennettu.

HP BladeCenter C7000 (Kuva 1) mahdollistaa 16 palvelimen käytön yhdessä palvelinkehikossa. Kehikon takaosaan on mahdollista kytkeä yhteensä kahdeksan HP Virtual Connect -moduulia, jotka tarjoavat tietoliikenneyhteydet sekä Ethernet-että SAN-verkon toteutuksiin. Moduulit varmentavat toisiaan, jolloin vasemman puoleinen toimii ensisijaisena moduulina ja oikean puoleinen toimii sen varalaitteena. Vikatilanteessa tai toisen verkkolaitteen yhteyden katkettua, yhteydet siirretään toimivalle moduulille automaattisesti.

Palvelinkehikko tarjoaa oman selainpohjaisen hallintaliittymän, HP Onboard Administratorin. Työkalun avulla voidaan hallita kaikkien palvelinten asetuksia keskitetysti sekä avata etäyhteys palvelimeen ilman erillistä näyttöä ja näppäimistöä palvelinlaitetilassa. Verkkoyhteyksien hallinta onnistuu Onboard Administratorista löytyvällä HP Virtual Connect Managerilla.

Palvelinkehikkoon on saatavilla useita erimallisia palvelimia, jotka vievät yhdestä kahteen laitepaikkaa riippuen laitteen ominaisuuksista. Palvelimet voivat olla AMD x64 -arkkitehtuuriin perustuvia 64-bittisiä järjestelmiä tai vaihtoehtoisesti Intelin Itanium -pohjaisia HP:n HPUX -käyttöjärjestelmään perustuvia tehopalvelimia.

Laadukas mutta edullinen PC-arkkitehtuurin mukainen palvelin on esimerkiksi HP Proliant BL460c, joka toimitetaan yhdellä neliytimisellä Intel Xeon -prosessorilla. Prosessorien määrä on laajennettavissa kahteen ja muistia voidaan liittää aina 64 gigatavuun saakka. Laite vie palvelinkehikosta yhden laitepaikan. Laitteessa on kaksi sisäänrakennettua verkkokorttia, lisäkortilla saadaan kaksi korttia lisää. Lisämoduulin avulla saadaan toteutettua myös SAN-verkon yhteydet.

Tulevissa korttipalvelimissa tullaan käyttämään myös 10 Gbps:n nopeuksiin kykeneviä verkkokortteja ja Virtual Connect -moduuleja, mutta niistä saatava informaatio on vielä vähäistä, eikä tuotteita ole saatu toistaiseksi markkinoille. Tullessaan markkinoille tuotteet mahdollistavat yhä nopeammat tietoliikenneyhteydet sekä entistä helpomman hallinnan. Tuotteet yleistyvät palvelimissa varmasti 2010–2011 vuosien aikana.



Kuva 1: HP Bladecenter C7000 - 16 palvelimen kehikko.

3.2. Tietoliikenneyhteydet

Kahdesta toimipisteestä toimitettavat verkkopalvelut vaativat aina yhteyksien toimittajan tukea toteutukselle. Kahdennetut operaattoriyhteydet molempiin toimipisteisiin on tilattava toimittajalta niin, että ne tukevat useita virtuaalisia verkkoja.

Yhteydet molemmissa palvelintiloissa toteutetaan kahdella valokuidulla, joiden reitit kulkevat operaattorin eri liityntäpisteiden kautta. Yksittäisen valokuidun katkeaminen ei voi vaikuttaa yhteyden toimivuuteen. Samassa yhteydessä on tilattava myös tallennusjärjestelmän verkkoa varten toteutettu verkkojen yhdistäminen, jolloin tallennusverkon varmistaminen etäkohteeseen on mahdollista.

Kaikki yhteydet rakennetaan aktiivisena reititetynä toteutuksena. Toimipisteiden välinen tietoliikenneyhteys täytyy olla nopeudeltaan vähintään 1 Gbps, mutta Internet-yhteyteen riittää 100/100:n Mbps:n yhteys molempiin toimipisteisiin.

Useat palveluntarjoajat kykenevät toimittamaan laittilojen väliset yhteydet aktiivisen DWDM-yhteyden avulla, jolloin operaattori voi valvoa yhteyden tilaa ja ryhtyä korjaustoimenpiteisiin nopeasti. Usein yhteyksiin on saatavilla myös erilaisia palvelutasoja, jolloin vikatilanteisiin reagoidaan peruspalvelua nopeammin.

SAN-verkko tarvitsee omat kytkentänsä WDM-yhteyksien avulla. Uusimmat levyjärjestelmät ja kuitukytkimet vaativat toimiakseen 4 Gbps:n tasoiset yhteydet. SAN-verkon liikennettä ei voida reitittää, joten yhteydet täytyy toteuttaa passiivisia laitteita käyttäen. Jos toimipisteiden väliset reitit on mahdollista toteuttaa kahden eri kautta kulkevan laitteiston avulla, kannattaa tällaista vaihtoehtoa käyttää. Muussa tapauksessa esimerkiksi lähialueella tapahtuvat maansiirtotyöt saattavat aiheuttaa yhteysongelmia, jos yksittäinen väliyhteys katkeaa.

<http://www.tml.tkk.fi/Studies/Tik-110.300/1997/Essays/wdm.html>

3.3. Aktiiviset palomuuriklusterit

Korkeaa saatavuutta vaativan verkkopalvelun toteutuksessa mikään yksittäinen laite ei saa aiheuttaa palvelun toiminnan keskeytymistä. Yhden palomuurin käyttö estäisi kaiken liikenteen laitteen rikkoutumisen yhteydessä. Onneksi markkinoilla on ratkaisuja, joissa käytetään useita laitteita vikatilanteiden ehkäisemiseksi. Kokonaisuuden jäljellä olevat laitteet hoitavat liikennöinnin, yksittäisen laitteen viikaantuessa.

Kahdennetut palomuuriratkaisut perustuvat virtuaalisiin IP-osoitteisiin, jotka vaihtavat paikkaa eri laitteiden välillä tarjoten yhteyden samasta osoitteesta riippumatta kulloinkin käytettävästä laitteesta. Verkkoon kytkeytyvä asiakas ei pysty päättämään, minkä laitteen kautta yhteys todellisuudessa kulkee.

Laitetoimittajasta riippuen laitteista yksi voi olla aktiivinen toiminnassa oleva laite toisen laitteen käynnistyessä, kun ensimmäinen jostain syystä lopettaa toimintansa. Hieman kehittyneemmät laitteet mahdollistavat kuormantasauksen laitteiden välillä. Kuormantasauksessa kaksi tai useammat palomuurit toimivat kaikki

aktiivisina ja niistä vähiten käytössä oleva laite tarjoaa yhteydet asiakkaan ottaessa yhteyttä palveluun.

Kuormaa tasaavat laitteet mahdollistavat myös helpon tavan laitteiden tiedonsiirtomäärän nostamiseen ympäristön kasvaessa alkuperäistä suuremmaksi, koska laitteita ei tarvitse vaihtaa uusiin.

Kun käytössä on useampi toimipiste, molemmissa toimipisteissä tarvitaan vähintään yksi palomuuuri. Palomuuriympäristön kasvattaminen tapahtuu myös pareittain, jotta molemmissa toimipisteissä on aina sama määrä palomuuureja.

4. VIKASIETOISET LEVYJÄRJESTELMÄT

4.1. SAN-tallennusverkot

Useat palvelimet tarvitsevat klustereissa yhtenäisiä levyjä. Levyt voitaisiin toteuttaa NFS-jakojen avulla, mutta nopeampi ja toimintavarmempi tapa on sijoittaa kunnolliseen levyjärjestelmään, joka toimii SAN-verkkona. Toteutuksessa palvelinten levyt jaetaan isosta RAID-levykokonaisuudesta, jossa data tallennetaan useille levyille samanaikaisesti. Järjestelmät ovat erittäin vikasietoisia ja yhden levyn rikkoutuminen järjestelmästä ei aiheuta mitään katkoksia. Useimmissa levyjärjestelmissä levyjen vaihtaminen, lisääminen ja poistaminen onnistuvat ilman järjestelmän alasajoa.

Levyjärjestelmät mahdollistavat usein myös datan peilaamisen levyjärjestelmien välillä. Vikatilanteessa laitteet ohjataan käyttämään toista levyjärjestelmää, eikä asiakas huomaa vian yhteydessä mitään. Jos kaksi levyjärjestelmää on maantieteellisesti hajautettu, turvataso kasvaa entisestään. Lisäksi samoja levyjä voidaan käyttää rajoituksetta molemmissa konesaleissa, eikä laitteiden sijoittaminen riipu levyjen saatavuudesta.

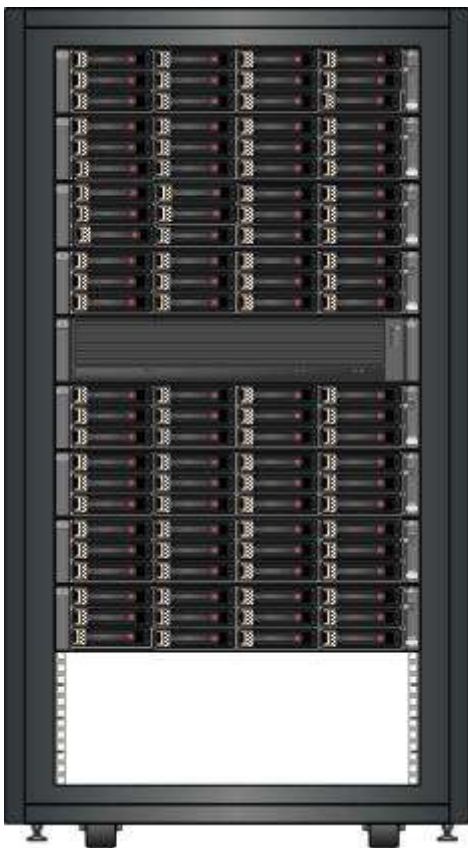
4.2. HP -levyjärjestelmät

HP tarjoaa levyjärjestelmiä monenlaisten yritysten tarpeisiin. Pienimmät MSA-järjestelmät soveltuvat pienten ja keskisuurten yritysten tarpeisiin, jos aiempaa tarvetta levyjärjestelmälle ei ole ollut. Hieman kattavampiin tarpeisiin löytyy Enterprise Virtual Array(EVA) -sarja, joka soveltuu jo erittäin mainiosti korkean saatavuuden ympäristön järjestelmäksi. Suuryritysten järjestelmiä varten voidaan tarvita XP -järjestelmä, joka tukee yli 200 teratavun datamääriä.

Pienikokoisen korkean saatavuuden ympäristön tarpeisiin HP EVA 4400 on hyvin sopiva levyjärjestelmä. Järjestelmä on melko edullinen ja nopeudeltaan riittävä. Tarvittavat 4 gigatavun liittimet löytyvät ja järjestelmää on mahdollista peilata myös isompien järjestelmien kanssa. Yhteen levyhyllyyn pystytään asentamaan

12 kappaletta 400 gigatavun SAS -levyjä. Levyhyllyjen maksimimäärä on 8 kappaletta. Täydellä kokoonpanolla on siis mahdollista saada yli 20 teratavun levy-määrä. EVA4400 on myös sarjan ainoa laite, jonka voi asentaa omatoimisesti ilman valtuutettua HP:n asentajaa.

Enterprise Virtual Array -sarjassa on myös 6400- ja 8400- malliset laitteet, jotka mahdollistavat useampien levyjen asentamisen.



Kuva 2: Eva 4400

5. SOVELLUSYMPÄRISTÖ

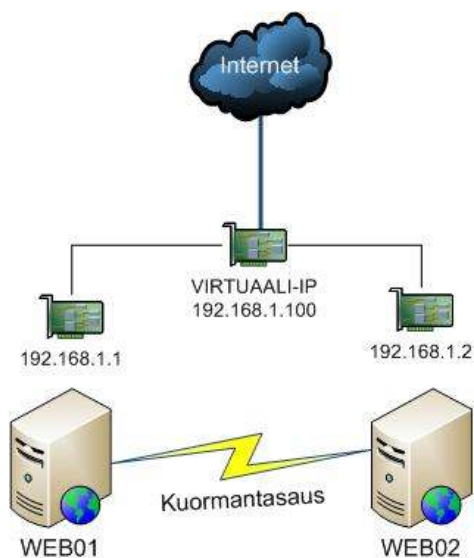
5.1. Kuormantasaus palvelinsovelluksissa

Kuormantasausta käytetään yleisesti paljon kuormittuvissa palveluissa, jolloin kuormaa tasaavat palvelimet jakavat palvelupyynnöt keskenään, lisäten järjestelmän suorituskykyä. Microsoftin palvelinkäyttäjärjestelmien mukana toimitettava kuormantasaussovellus mahdollistaa kuitenkin palvelun toiminnan myös vikatilanteissa. Palvelimen vikaantuessa jäljellä olevat palvelimet huolehtivat palvelun saatavuudesta. Kuormantasaus mahdollistaa luotettavan toiminnan sekä kapasiteetin kasvaessa että mahdollisessa vikatilanteessa.

(Shimonski 2003, 177-182.)

Kuormantasauksen määrittelyssä kaikille palvelimille jaetaan yksi yhteinen virtuaalinen IP-osoite, johon palvelut liitetään palomuurissa. Osoitteesta liikenne ohjataan saatavilla olevalle palvelimelle. Asiakkaan suuntaan näkyy ainoastaan yksi nimi ja kuormantasauksen virtuaalinen IP. Palvelu on toteutettavissa käytännössä melkein minkä tahansa palvelinsovelluksen kanssa, kun asetukset on oikein määritetty. Sovellus hoitaa liikenteen jakamisen aktiivisesti kaikkien klusterissa olevien palvelinten kesken.

(Shimonski 2003, 177-182.)



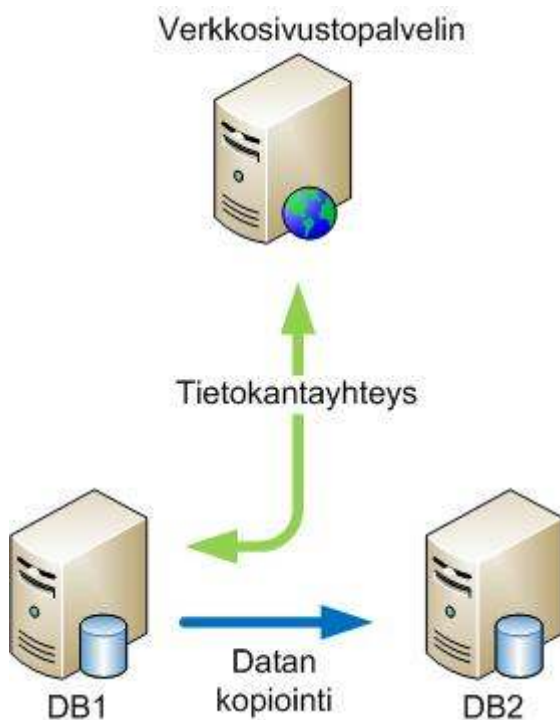
Kuva 3: Kuormantasaus palvelinverkossa

Kuormantasaus voidaan hoitaa käyttäen unicast-, multicast- tai IGMP-multicast-protokollan paketteja verkossa. Luotettavimman toiminnallisuuden saa IGMP-multicast -protokollan avulla, mutta se vaatii tukea laitteistolta. Jos kuormantasaus on toteutettu useiden palvelinsalien välille, on tämä kytkentätapa ainoa toimiva. Tällöin osoitepäivitykset kulkeutuvat verkon läpi oikeaan sijaintiinsa riittävän nopeasti eivätkä aiheuta ylimääräistä verkkoliikennettä, joka hidastaisi liikennettä tai pahimmassa tapauksessa aiheuttaisi palvelukatkoksen.

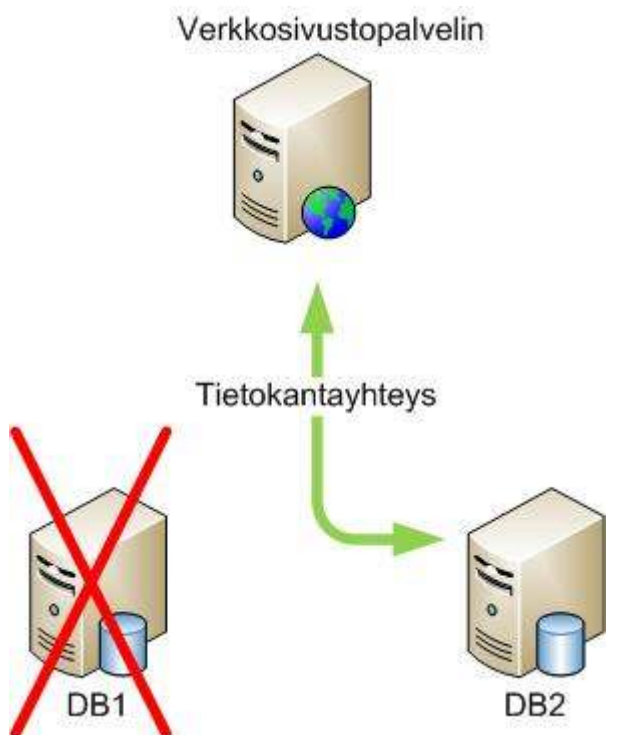
5.2. Failover-klusteroidut tietokantaratkaisut

Klusteroidut tietokantaratkaisut voidaan toteuttaa joustavasti Microsoft SQL Server 2005:n avulla. Windows Server -palvelinkäyttöjärjestelmien mukana toimitetaan Microsoftin klusterointityökalu, jonka määrittelyjen avulla voidaan toteuttaa mm. tietokantaklustereita. Klusteri voi olla toiminnaltaan molempia palvelimia aktiivisesti käyttävä tai vaihtoehtoisesti käyttää ainoastaan toista palvelinta ja sen vikaantuessa siirtyä toisen palvelimen käyttöön. Korkean saatavuuden failover-klusteri sietää hyvin vikatilanteita, mutta ei vaadi lisenssin hankkimista kahdenneulle palvelimelle.

(Gibson 2008, 566-572.)



Kuva 4: Tietokantaklusterin toiminta perustilanteessa



Kuva 5: Tietokantaklusterin toiminta virhetilanteessa

Klusterit vaativat toiminnaltaan yhteiset kiintolevyt, jotka ovat saatavilla molemmilla palvelimilla. Levyjärjestelmän kautta kytkettävät virtuaaliset levyt toimivat erinomaisesti klusteritarkoituksessa. Microsoftin klusterointisovellus huolehtii automaattisesti siitä, kummalle palvelimelle levyt näytetään. Ensimmäisen palvelimen vikatilanteessa levyt siirtyvät näkyviin toisella palvelimella ja tietokantapalvelimen prosessit käynnistetään. Palvelut ovat käytössä toiselta palvelimelta muutaman sekunnin viiveellä.

5.3. Automaattiset vikailmoituspalvelut

Palvelinympäristössä ilmeneviä vikoja ei aina havaita riittävän nopeasti korjaustoimenpiteiden aloittamiseksi. Lisäksi korkean saatavuuden palvelut säilyttävät toimintakykynsä yksittäisen laitteen vikaantumisen yhteydessä, jolloin vian havaitseminen on entistä vaikeampaa. Myös kriittisen ympäristön tilanneilla asiakkailla on usein tarve saada reaaliaikaista tietoa ympäristöidensä toimintakyvystä.

Laitteistojen ja sovellusten valvontaan on saatavilla useita erilaisia ratkaisuja, joiden avulla tieto vikaantuneista osista saadaan lähetettyä ylläpitohenkilökunnalle

sähköpostin tai tekstiviestin välityksellä. Joissain palveluissa valvontajärjestelmät mahdollistavat myös 24 tuntia vuorokaudessa toimivan valvomon ylläpidon, jolloin vikatilanteisiin reagoidaan jokaisena vuorokauden aikana.

Laitteistojen fyysinen valvonta perustuu SNMP -protokollaan, joka lähettää valvontatiedot niitä keräävällä sovellukselle tai sovelluksille. HP tarjoaa omia ratkaisujaan laitteiden valvontaan, jolloin vikailmoitukset lähetetään reaaliajassa HP:n valvomoon, josta asiantuntijat ottavat yhteyttä laitteiden ylläpitäjiin tarvittavien huoltotoimenpiteiden käynnistämiseksi palvelusopimusten mukaisesti. HP:n valvomo huolehtii tarvittavien varaosien ja töiden tilauksista ilman asiakkaalle koituvaa harmia. Huoltohenkilöt vaihtavat osat laitteisiin palvelusopimuksen mukaan usein seuraavana työpäivänä.

HP:n ratkaisu ei sovellu sovellusten valvontaan. Microsoft-ympäristöjen valvontaan on saatavilla tuotteita Microsoft System Center -tuoteperheestä. System Center Operations Manager mahdollistaa tarkan valvonnan Microsoftin käyttöjärjestelmien ja sovellusten välillä.

Microsoft on kehittänyt lukuisia Management Pack -laajennuksia tuotteeseen, joiden avulla sen valvontakykyä voidaan laajentaa. Tuettavia sovelluksia ovat mm. Microsoft Exchange, Microsoft SQL Server sekä Microsoft IIS. Microsoftin sovelluksen huonona puolena voidaan mainita mm. tietokantojen runsas levytilan kasvu, joka saattaa aiheuttaa huomattavia ylimääräisiä kustannuksia suurissa valvontaympäristöissä.

(Piltzecker 2006, 29-35.)

Sovellusten valvontaan voidaan soveltaa myös avoimen lähdekoodin tuotteita, joiden avulla voidaan valvoa erityisesti Linux-palvelimia. Yksi tunnetuista ja toimivaksi havaituista verkonvalvontatuotteista on Nagios, jota julkaistaan GPL-lisenssillä. Tuote kykenee myös verkkotason valvontaan SNMP:n avulla.

(Barth 2005, 71-72.)

6. KORKEAN SAATAVUUDEN VERKKOPALVELUN TO- TEUTTAMINEN

6.1. Ympäristön kuvaus

Toteutettava projekti on konserniyrityksen verkkosivusto-, käyttäjienhallinta- ja tietokantapalvelimista koostuva kokonaisuus, jossa tilaaja edellyttää, että palvelut ovat saatavissa vähintään 99 prosenttia ajasta kuukauden seurantajaksolla. Tilaajan kanssa on sovittu, että vuoden aikana palveluun voidaan tehdä neljä huoltokatkoa, jotka saavat kestää kerrallaan kolme tuntia. Huoltokatkot voidaan suorittaa klo 00–03 välisenä aikana tammikuun, huhtikuun, elokuun ja marraskuun toisen viikon keskiviikkoina.

Lisävaatimuksena asiakkaalla on palveluiden hajauttaminen kahteen konesaliin niin, että palvelu ei keskeydy myöskään suuremmissa yksittäiseen konesaliin kohdistuvissa vahingoissa. Asiakas vaatii myös suunnitelmat suurista vikatilanteista palautumiseen.

Ympäristö toteutetaan Microsoft Windows 2003 R2 Enterprise -version käyttöjärjestelmillä. Tietokantasovellukset toteutetaan Microsoft SQL Server 2005 Enterprise -versiolla ja verkkosivustot vaativat toimiakseen ASP.NET 3.5 -tasoinen rajapinnan Microsoft Internet Information Services 6.0 -verkkosivustopalvelimella.

Asiakas vastaa itse käyttämiensä sovellusten toiminnasta, sisältäen verkkosivustot ja tietokannat. Toimittajan vastuulla on laitteisto-, verkko- ja käyttöjärjestelmätoimitusten lisäksi käyttöjärjestelmien- ja sovellusten ylläpito. Toimittaja omistaa kaikki laitteet ja käyttöjärjestelmät ja vuokraa niitä asiakkaalle sopimuksen mukaisesti.

Asiakkaan asettamat laitteistovaatimukset ovat seuraavat:

- Palvelimet on toteutettu fyysisillä palvelinratkaisuilla, ei virtualisointia.
- Palvelimissa käytetään 64-bittisiä neliydinprosessoreja.
- Kirjautumispalvelimissa ja verkkosivustopalvelimissa on oltava vähintään 8 gigatavua muistia ja tietokantapalvelimissa vähintään 16 gigatavua.
- Käytettävissä 100 Mbps:n tasoinen tietoliikenneyhteys Internet-verkkoon.

6.2. Ympäristön suunnittelu

Ennen toteutuksen aloittamista suunnitelmat ympäristöstä on hyväksyttävä asiakkaalla. Suunnitelmat sisältävät verkkokaavion, kaavion käytetyistä palvelinlaitteista ja niiden asetuksista (muistin määrä, prosessorit) sekä erillisen verkkokaavion tallennusverkosta.

Palvelu on asiakkaalle uusi, joten kaikki toteutettavat osa-alueet ovat uusia. Toimittaja toimittaa kaikki asetukset ympäristöä varten.

5.2.1 Verkkosuunnitelmat

Kaikki palvelimet sijaitsevat toimittajan toimipisteissä. Verkot yhdistetään kahden palvelinlaitetilan välillä operaattorilta tilatuilla yhteyksillä, jotka kulkevat kahta erillistä reittiä. Useat verkot toimitetaan toimipisteisiin VLAN-tekniikan avulla.

AsiakasOy_External1

Asiakkaalle on varattu oma julkinen C-luokan IP-osoitelohko. Osoitteet ovat 83.220.100.x -luokassa (ei todellisia osoitteita). Osoitteet tuodaan VLAN-verkkona molempiin palvelinsaleihin yhtenä verkkototeutuksena. Tämän verkon nimi on AsiakasOy_External1, VLAN-ID: 228.

AsiakasOy_Internall

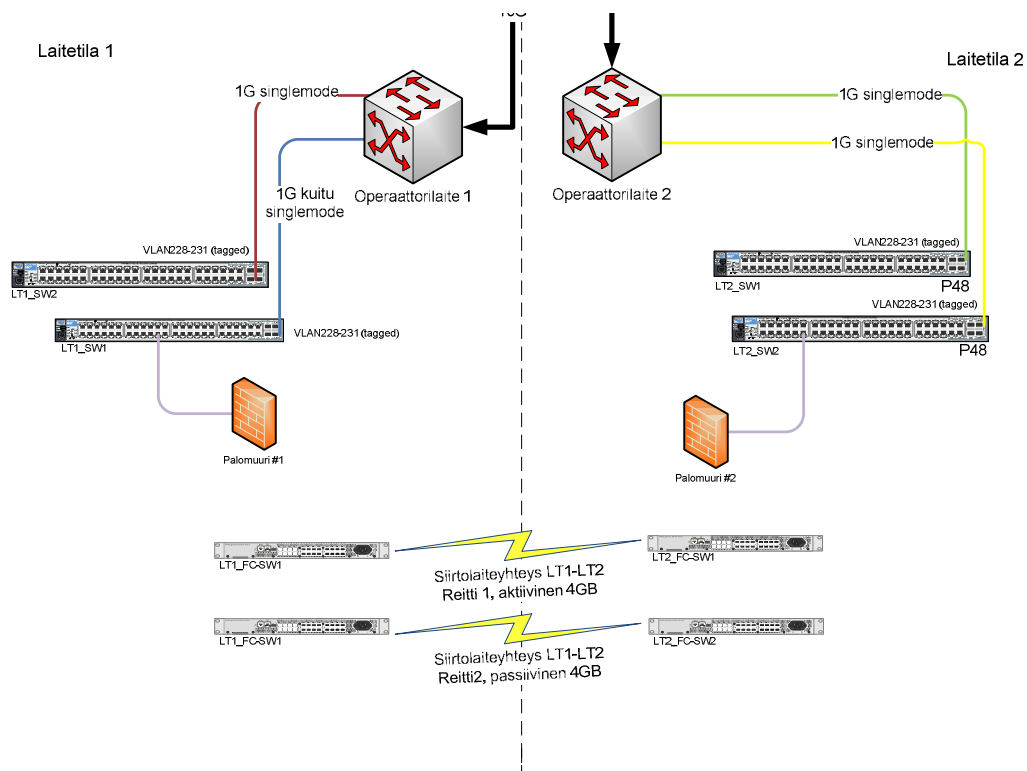
Palvelinten sisäverkkoliikenne hoidetaan omassa verkossaan, jonka kooksi on määritelty C-luokan IP-osoitelohko. Osoitteet ovat 192.168.10.x -luokassa. Osoitteet tuodaan VLAN-verkkoina molempiin konesaleihin yhtenä verkkototeutuksena, lähiverkkojen yhdistämisen avulla. Verkon nimi on AsiakasOy_Internall1, VLAN-ID: 229.

AsiakasOy_Mgmt1

Asiakkaan laitteistojen hallintaosoitteet on jaettu omaan C-luokan osoitelohkoon. Osoitteet ovat 192.168.20.x -luokassa. Osoitteet tuodaan VLAN-verkkoina molempiin konesaleihin yhtenä verkkototeutuksena, lähiverkkojen yhdistämisen avulla. Verkon nimi on AsiakasOy_Mgmt1, VLAN-ID: 230.

AsiakasOy_HBeat1

Tietokantapalvelimet ja palomuurit toimivat klustereissa, joten ne tarvitsevat oman eristetyn verkon palveluiden toimintakyvyn mittaukseen. Tätäkin tarkoitusta varten varattiin C-luokan IP-osoitelohko, jonka osoitteet ovat 192.168.30.x -luokassa. Osoitteet tuodaan VLAN-verkkoina molempiin konesaleihin yhtenä verkkototeutuksena, lähiverkkojen yhdistämisen avulla. Verkon nimi on AsiakasOy_HBeat1, VLAN-ID: 231.



Kuva 6: Laitetilayhteydet

6.2.2 Laitesuunnitelmat

Laitteisto haluttiin pitää mahdollisimman yhtenäisenä kaikilta osin, joten laitemallit eivät voi poiketa toisistaan kovin runsaasti. Kaikissa palvelimissa levyjärjestelmän hallintapalvelinta lukuun ottamatta hyödynnetään nykyaikaista korttipalvelintekniikkaa.

AD01.asiakas.local

Rooli:	Kirjautumispalvelin(Active Directory), DNS-palvelin
Käyttöjärjestelmä:	Windows Server 2003 R2 Enterprise
IP-osoite:	192.168.10.3 (AsiakasOy_Internal1)
Sijainti:	Palvelinsali 1, Korttipalvelin 1
Palvelinlaite:	HP ProLiant BL460c G1
Proessori:	2,5Ghz Intel Xeon Quad
Muistin määrä:	8 gigabittia
Levytilan tarve:	30 gigabittia

AD02.asiakas.local

Rooli: Kirjautumispalvelin(Active Directory), DNS-palvelin
 Käyttöjärjestelmä: Windows Server 2003 R2 Enterprise
 IP-osoite: 192.168.10.4 (AsiakasOy_Internal1)
 Sijainti: Palvelinsali 2, Korttipalvelin 1

 Palvelinlaite: HP ProLiant BL460c G1
 Prosessori: 2,5Ghz Intel Xeon Quad
 Muistin määrä: 8 gigabittiä
 Levytilan tarve: 30 gigabittiä

WEB01.asiakas.local

Rooli: Verkkosivustopalvelin
 Käyttöjärjestelmä: Windows Server 2003 R2 Enterprise
 IP-osoite: 192.168.10.6 (AsiakasOy_Internal1)
 192.168.10.5 (AsiakasOy_Internal1) [LoadBalancer]
 Sijainti: Palvelinsali 1, Korttipalvelin 2

 Palvelinlaite: HP ProLiant BL460c G1
 Prosessori: 2,5Ghz Intel Xeon Quad
 Muistin määrä: 8 gigabittiä
 Levytilan tarve: C: 30 gigabittiä
 D: 100 gigabittiä

WEB02.asiakas.local

Rooli: Verkkosivustopalvelin
 Käyttöjärjestelmä: Windows Server 2003 R2 Enterprise
 IP-osoite: 192.168.10.7 (AsiakasOy_Internal1)
 192.168.10.5 (AsiakasOy_Internal1) [LoadBalancer]
 Sijainti: Palvelinsali 2, Korttipalvelin 2

 Palvelinlaite: HP ProLiant BL460c G1
 Prosessori: 2,5Ghz Intel Xeon Quad
 Muistin määrä: 8 gigabittiä
 Levytilan tarve: C: 30 gigabittiä
 D: 100 gigabittiä

DB01.asiakas.local

Rooli: Tietokantapalvelin, Raportointipalvelin
 Käyttöjärjestelmä: Windows Server 2003 R2 Enterprise
 IP-osoite: 192.168.10.8 (AsiakasOy_Internal1)
 192.168.30.10 (AsiakasOy_HBeat1)
 Sijainti: Palvelinsali 1, Korttipalvelin 3

 Palvelinlaite: HP ProLiant BL460c G1
 Prosessori: 2x 2,5Ghz Intel Xeon Quad
 Muistin määrä: 16 gigabittiä
 Levytilan tarve: C: 30 gigabittiä
 D: 100 gigabittiä
 E: 100 gigabittiä

DB02.asiakas.local

Rooli: Tietokantapalvelin, Raportointipalvelin
 Käyttöjärjestelmä: Windows Server 2003 R2 Enterprise
 IP-osoite: 192.168.10.9 (AsiakasOy_Internal1)
 192.168.30.11 (AsiakasOy_HBeat1)
 Sijainti: Palvelinsali 2, Korttipalvelin 3

 Palvelinlaite: HP ProLiant BL460c G1
 Prosessori: 2x 2,5Ghz Intel Xeon Quad
 Muistin määrä: 16 gigabittiä
 Levytilan tarve: C: 30 gigabittiä
 D: 100 gigabittiä
 E: 100 gigabittiä

BACKUP01.asiakas.mgmt

Rooli: Varmistuspalvelin
 Käyttöjärjestelmä: Debian Linux 4.0
 IP-osoite: 192.168.10.10 (AsiakasOy_Internal1)
 192.168.20.100 (AsiakasOy_Mgmt1)
 Sijainti: Palvelinsali 1, Korttipalvelin 4

 Palvelinlaite: HP ProLiant BL460c G1
 Prosessori: 2,5Ghz Intel Xeon Quad
 Muistin määrä: 4 gigabittiä
 Levytilan tarve: 30 gigabittiä

FWMGMT01.asiakas.mgmt

Rooli: Palomuurien hallinta- ja valvontapalvelin. Käyttöjärjestelmä: Windows Server 2003 R2 Standard

IP-osoite: 192.168.20.101 (AsiakasOy_Mgmt1)

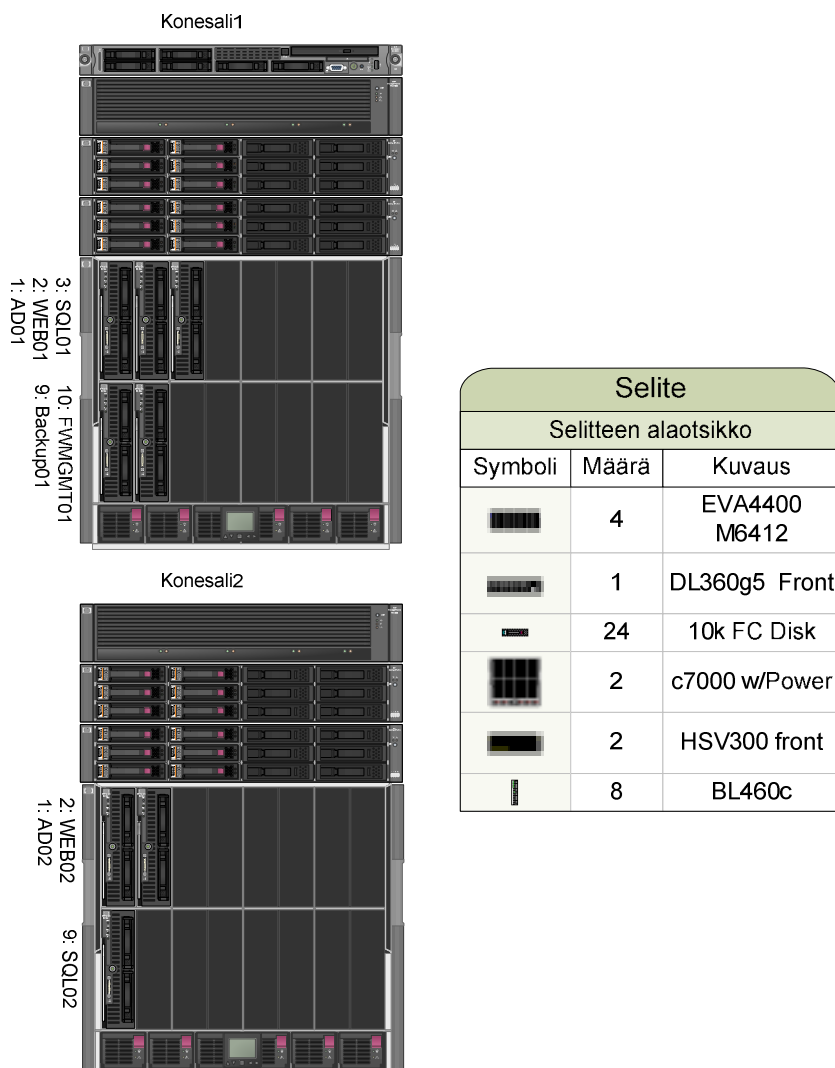
Sijainti: Palvelinsali 1, Korttipalvelin 5

Palvelinlaite: HP ProLiant BL460c G1

Proessori: 2,5Ghz Intel Xeon Quad

Muistin määrä: 4 gigabittia

Levytilan tarve: C: 30 gigabittia
D: 50 gigabittia



Kuva 7: Palvelinlaitteiden dokumentaatio

6.3. Verkkoinfrastruktuurin rakentaminen

6.3.1 Yhteyksien tilaaminen

Verkkoinfrastruktuurin rakentaminen aloitettiin tarvittavien yhteyksien tilaamisella verkkojen toteuttajalta. Toimipisteiden välisille verkoille asetettiin vaatimukseksi, että niiden tulee olla kahdennettuja. Yhden laitteen rikkoutuminen missä tahansa verkon osassa ei saa aiheuttaa katkosta käyttöön. Julkisen Internet -verkon yhteys tilattiin 100/100 Mbps:n nopeudella molempiin toimipisteisiin. Sisäverkot tilattiin verkkosuunnitelman mukaisesti lähiverkkojen yhdistämispalveluna 1 Gbps/1 Gbps:n nopeudella kahta erillistä reittiä pitkin (kahdet yhteydet). Sisäverkot reititettiin julkisen IP-lohkon ensimmäisen vapaan osoitteen taakse, jolloin palomuurilaite toimii näiden verkkojen oletusyhdyskäytävänä. Palomuurin avulla voidaan tällöin rajoittaa sisäverkkoon ja sieltä ulos kulkevaa liikennettä.

6.3.2 Kytkinten hankinta ja asennus

Kun kaikki tarvittavat yhteydet oli tilattu, voitiin hankkia kytkimet sisäverkon toteuttamista varten. HP:n valikoimista löytynyt 48-porttinen ProCurve 2810-48G soveltui tehtävään mainiosti. Valokuituliittimiä ei kytkimissä ollut valmiina, joten hankin vielä erilliset HP:n toimittamat valokuituliittimet. Liittimiä on kahden mallisia, Single-Mode ja Multi-Mode. Toimittaja edellyttää Single-Moden käyttämistä, joten sen mukaiset liittimet hankittiin.

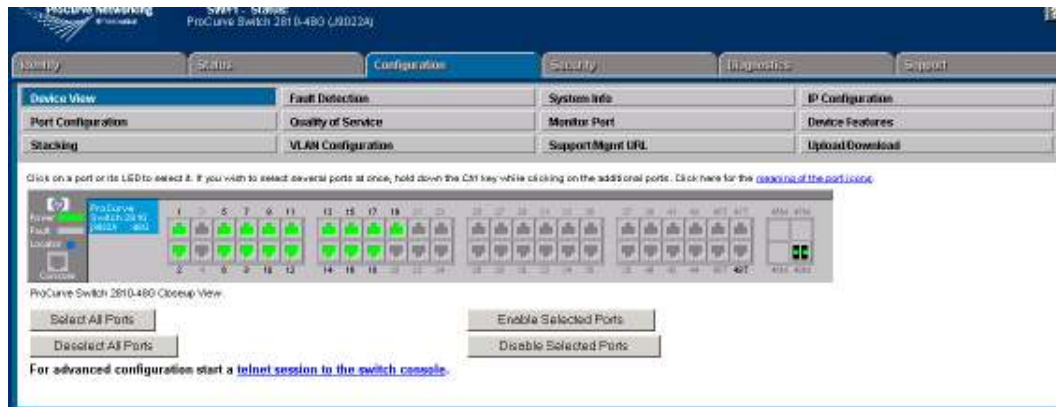


Kuva 8: HP kytkimen Mini-GBIC-liitin

Laitteet asennettiin palvelinsalin asettelusta tehdyn suunnitelman mukaisille paikoille. Laitteet ovat palvelinkaappeihin kiinnitettävää mallia, joten ruuvasin ne paikalleen kaappien takapuolelle. Kytkin laitetoimittajan päätelaitteista kaapelit valokuidulla portteihin 48 kaikissa neljässä kytkimessä. Valokuitujen toimivuuden kannalta on erittäin tärkeää, että kaikki liittimet puhdistetaan ennen asennusta. Tarvittavat puhdistuslaitteet sain lainaksi yhteystoimittajalta, joten liittimet puhdistettiin ennen asennusta.

Kaikki halutut VLAN-verkot määriteltiin 48-portissa tagged-muotoisena, jolloin yhdessä kaapelissa saadaan määriteltyä useita eri verkkoja. Hallintaverkkoon tehtiin IP-osoite jokaista kytkintä varten, jotta hallinta onnistuisi suoraan toimiston puolelta ilman ylimääräisten kaapeleiden liittämistä kytkimiin palvelinsalissa huoltotöiden yhteydessä.

Kun yhteys saatiin avattua uuteen verkkoon, latsin HP:n sivustolta kytkimiin uudet ohjelmistopäivitykset, joiden avulla korjattiin joitain edellisissä versioissa ilmenneitä virheitä. Päivitykset oli helppo asentaa verkkosivupohjaisen hallintaliittymän kautta. Asennuksen jälkeen kytkimet käynnistettiin uudelleen ja ne olivat perusasetuksiltaan käyttövalmiina.



Kuva 9: HP ProCurve 2810-48G hallintakonsoli

6.3.3 Kytinten asetukset palvelimia varten

Kun kytkinten perusasennus oli valmis, määrittelin jokaiseen kytkimeen 8 tagged-porttia korttipalvelinkehikon liikennettä varten. Lisäksi kuituverkon kytkimiä, hallintapalvelinta ja levyjärjestelmää varten tehtiin omat portit. Portit dokumentoitiin huolellisesti verkkodokumentointiin, ja kytkimen asetustiedostosta tehtiin lisäksi merkintä versionhallintaan, josta vanha versio voidaan tarvittaessa palauttaa ongelmatilanteessa.

Kytken konfiguraatio:

; J9022A Configuration Editor; Created on release #N.11.15

```
hostname "ASIAKASOY-SW#1"
snmp-server contact "VAINIO-P"
snmp-server location "ASIAKASOY_KONESALII"
max-vlans 256
time timezone 120
time daylight-time-rule Western-Europe
ip default-gateway 81.xx.xx.xx
ntp server 62.xx.xx.yy
timesync ntp
snmp unicast
snmp-server community "public" Unrestricted
snmp-server community "asiakasoy_valvonta"
vlan 1
name "DEFAULT_VLAN"
untagged 20-47
no ip address
exit
vlan 230
name "AsiakasOy_Mgmt1"
ip address 192.168.20.77 255.255.255.0
tagged 1-8,48
untagged 9-12
exit
vlan 231
name "AsiakasOy_HBeat1"
no ip address
tagged 1-8,48
```

```

untagged 13-14
exit
vlan 229
name "AsiakasOy_Internal1"
tagged 1-8,48
untagged 15-18
no ip address
tagged 48
exit
vlan 228
name "AsiakasOy_External1"
no ip address
tagged 3-4,48
untagged 19-20
exit
password manager

```

6.4. Palomuurien asentaminen ja käyttöönotto

Palomuurien toimintavarmuus projektissa oli tärkeää. Parhaat ominaisuudet löytyivät mielestäni StoneGaten laitteista. Valmistaja on kotimainen, tukea saa tarvittaessa puhelimella tai sähköpostilla vuorokauden ympäri. Laitteen hallinta on poikkeuksellisen helppoa verrattuna muiden toimittajien laitteisiin, kuten WatchGuard Firebox X tai SonicWall PRO-sarjan laitteet.

Palomuuereja hankittiin kaksi kappaletta. Asensin yhden laitteen kumpaankin toimipisteeseen. Stonegaten laitteet tukevat aktiivista kuormantasausta, jolloin molempien laitteiden teho saadaan käyttöön, mutta vikatilanteissa palveluun ei tule katkoksia.

6.4.1 Hallintapalvelin

Palomuuriklusterin asennus aloitetaan hallintapalvelimen asennuksella. Koska korttipalvelinympäristöä ei ollut vielä asennettu, sain lainata toisen projektin käytössä olevaa korttipalvelinta, jolle palvelin voitiin asentaa. Korttipalvelinympäristön valmistuttua voin siirtää palvelimen uuteen ympäristöön pienellä katkoksella. Palvelimelle asensin Windows Server 2003 R2 -käyttäjärjestelmän ja siihen tarvittavat järjestelmäpäivitykset.

Stonegate oli toimittanut aikaisemmin käyttäjätunnuksen ja salasanan, joiden avulla sain ladattua tarvittavat tiedostot hallintapalvelimen asentamiseen. Tiedostot ladattiin palvelimelle ja tavanomainen Windows-asennusohjelma avautui. Pal-

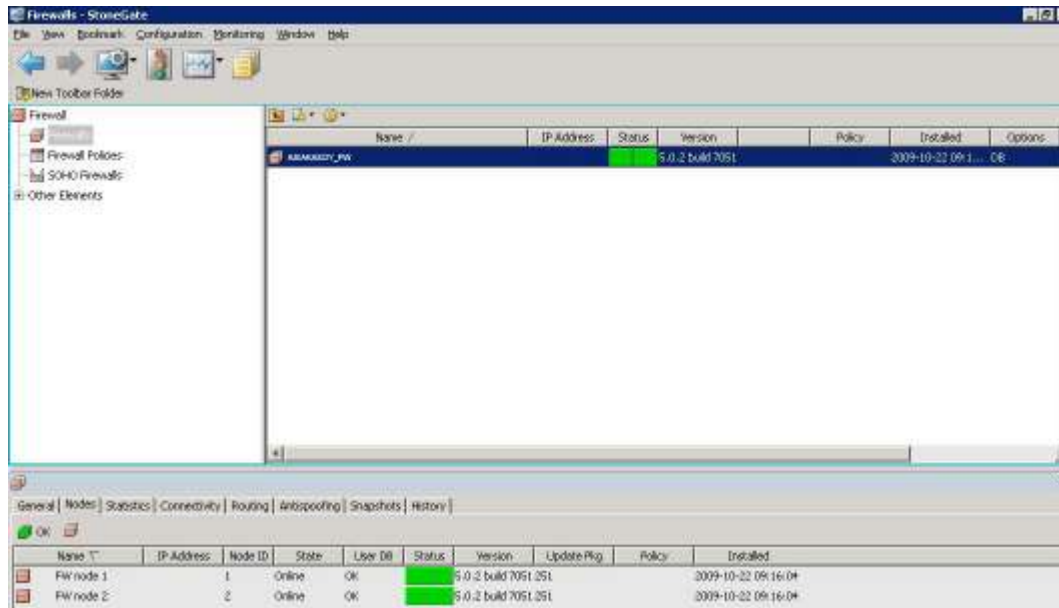
velimelle syötettiin tarvittavat ip-osoitteet palomureja varten ja asennus pyysi käynnistämään palvelimen uudelleen.

Kun hallintapalvelin oli asennettu, määrittelin peruspolitiikan palomureja varten, että laitteet löytävät yhteyden hallintaverkkoon ja klusterin toiminnan kannalta välttämättömään valvontaverkkoon. Kun asetustiedosto oli valmis, siirsin sen USB-muistille palomureille syöttämistä varten.

6.4.2 Palomuurien käyttöönotto

Palomuurilaitteet asennettiin palvelinkaappeihin edellä mainitun suunnitelman mukaisesti. Laitteiden fyysinen asennus oli huomattavasti HP:n kytkimiä hankalampaa, koska kiskot eivät olleet yhtä laadukkaita. Laite kytkettiin CAT5e tason verkkokaapeleilla HP:n kytkimiin ja laitettiin päälle.

Palomuriin kytkettyjen näytön ja näppäimistön avulla valitsin valikosta, että haluan tuoda asetustiedoston USB-muistilta. Asetin muistin kiinni palomuurissa olevaan porttiin ja asetustiedosto siirtyi palomuriin ja laite oli käytettävissä. Samat toimenpiteet tehtiin toisen palomuurilaitteen kanssa toisessa konesalissa. Klusteri oli nyt automaattisesti käytettävissä ja kuormantasausta onnistui laitteiden välillä.



Kuva 10: Stonegate -palomuuriklusterin tilan tarkastelu hallintapalvelimella

6.4.3 Palomuurisäännösten luominen

Oletuksena laitteet kieltävät kaiken liikenteen kaikkialta. Loin palomureille säännön, joka sallii palvelimilta Internetiin muodostettavan liikenteen minne tahansa. Lisäksi NAT-säännösten avulla määriteltiin, että kaikki ulos kulkeva liikenne menee 83.220.100.3 osoitteen kautta.

Sisäverkon liikenne samassa verkossa on oletuksena sallittu kaikkialle, koska palomuri ei voi estää samassa verkossa kulkevaa liikennettä, eikä tätä asiaa ollut tarvetta muuttaa. Julkisen IP-osoitteen 83.220.100.10 taakse määriteltiin kuitenkin reitti porteista 80 (http) ja 443 (https) verkkosivustopalvelimen kuormantasauksen osoitteeseen, jotta asiakkaan verkkosivusto saataisiin näkymään Internetissä.

Yhteys toimistoltani palvelinsaleihin toimii automaattisesti, koska reititys on luotu jo yhteyksien tilaamisen yhteydessä. Palomuri kuitenkin estää kaiken liikenteen, jota ei ole määritetty, joten lisäsin säännön, joka sallii kaiken liikenteen kaikille palvelimille ja hallintaverkkoon toimistoltani.

Palomuurisäännöstö

ID	Source	Destination	Service	Actions	Options	Desc
16.1	ANY	ANY	ANY	Continue	Logging, stored	Tallennetaan kaikki data logiin
16.2	Sisäverkot	Ei_sisäverkot	ANY	Allow		Sallitaan sisäverkoista ulkoverkkoihin kaikki
16.3	MGMT_Net	ANY	ANY	Allow		Sallitaan hallintaverkosta pääsy kaikkiin verkkoihin
16.4	ANY	Web_NLB1	HTTP(80) HTTPS(443)	Allow		Sallitaan HTTP ja HTTPS loadbalancerille
16.5	Discard All					

NAT-säännöstö

ID	Source	Destination	Service	Nat	Desc
18.10	MGMT	Ei_sisäverkot	ANY	Source Dynamic to: 83.220.100.100 on 1024 - 65535	Hallintaverkon koneet näkyvät julkisessa verkossa ip:llä 83.220.100.100
18.11	Internal	Ei_sisäverkot	ANY	Source Dynamic to: 83.220.100.110 on 1024 - 65535	Sisäverkon koneet näkyvät julkisessa verkossa ip:llä 83.220.100.110
18.12	ANY	Web_NLB1	HTTP(80) HTTPS(443)	Destination Web_NLB1 to Web_NLB_Internal1	Ohjataan Web_NLB1 liikenne sisäverkon objektiin Web_NLB_Internal1

6.5. Tallennusverkon rakentaminen

Kuitukanavamuotoisessa tallennusverkossa kaikki tieto palvelimien ja keskitetyn levyjärjestelmän välillä kulkee valokuidulla toteutetussa verkossa. SAN-verkko ei toimi kuten Ethernet, joten sitä ei voida reitittää. Tämän vuoksi toimipisteiden välillä olevat yhteydet tallennusverkkoa varten tilattiin erikseen. Palvelinsalien välille saatiin kaksi toisistaan riippumatonta reittiä. Toinen toteutettiin aktiivisen DWDM-tekniikan avulla ja toinen passiivisen CWDM-yhteyden avulla.

6.5.1 Tallennusverkon laitteiden asennus

HP:n valikoimista löytyi Brocaden valmistamat SAN-kytkimet, joita tilasin kaksi kappaletta molempiin toimipisteisiin. Kytkinten porttien nopeus on 4 Gbps, joka on sama kuin palvelimissa ja levyjärjestelmissä. Kaikkiin laitteiden portteihin tilattiin MiniGBIC-liittimet, joihin valokuidut kytketään. Liittimiä oli kaikissa kytkimissä yhteensä 16 kappaletta, joten laajennusvaraa on reilusti. Myös lisenssit laitteisiin hankittiin heti kaikille 16 portille.



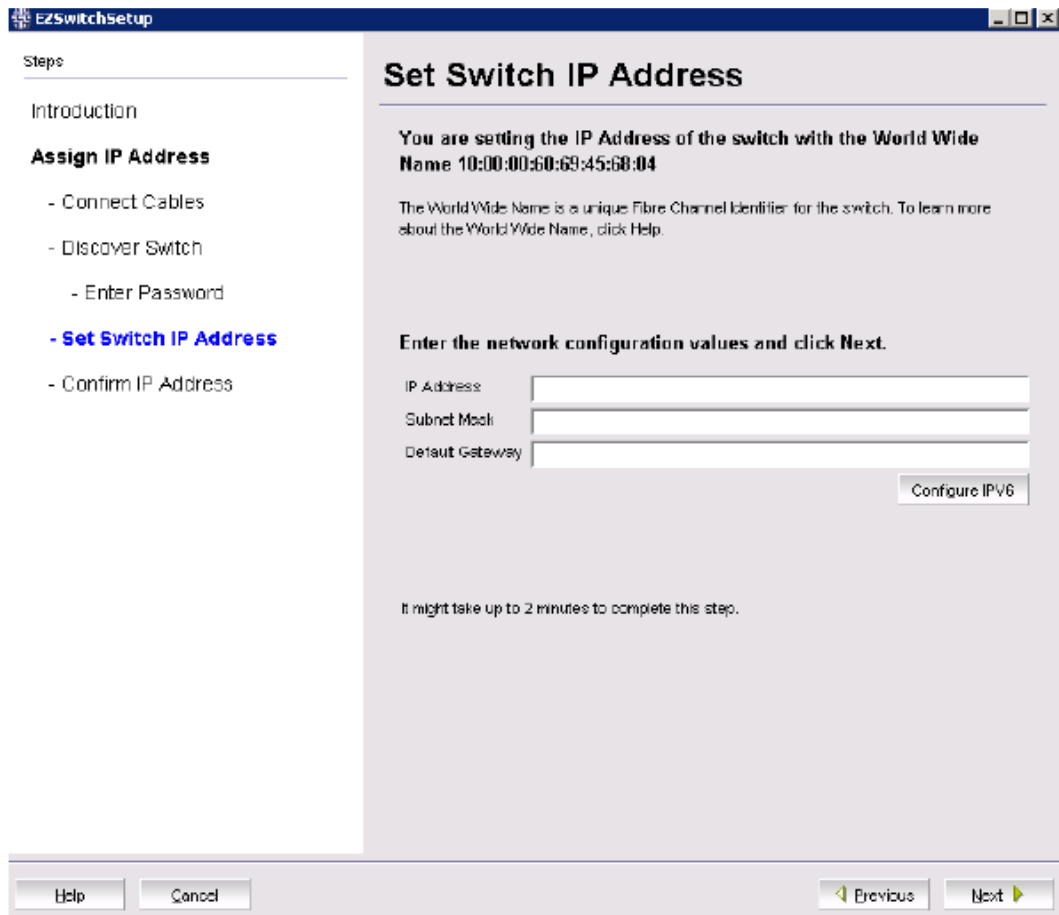
Kuva 11: HP Storageworks 4/8 SAN -kytkin

Laitteet asennettiin suunnitelman mukaisesti mahdollisimman lähelle levyjärjestelmiä niin, että kaapelit voidaan pitää mahdollisimman lyhyinä. SAN-kytkimet yhdistettiin hallintaporttien osalta HP:n Ethernet-kytkimiin, jotta hallinta onnistuisi toimistolta myös näiden kytkinten osalta.

6.5.2. SAN-kytkinten esiasennus

Helpoin tapa SAN-kytkimen asetusten määrittelyyn oli kytkeä se asetuksia varten pieneen 8-porttiseen kytkimeen, joka oli yhdistetty myös kannettavaan tietokoneeseen. Lisäksi kuitukytkimestä liitettiin kaapeli kannettavan sarjaporttiin. Hallintasovellus esiasennusta varten asennettiin työasemalle mukana tulevalta levyltä.

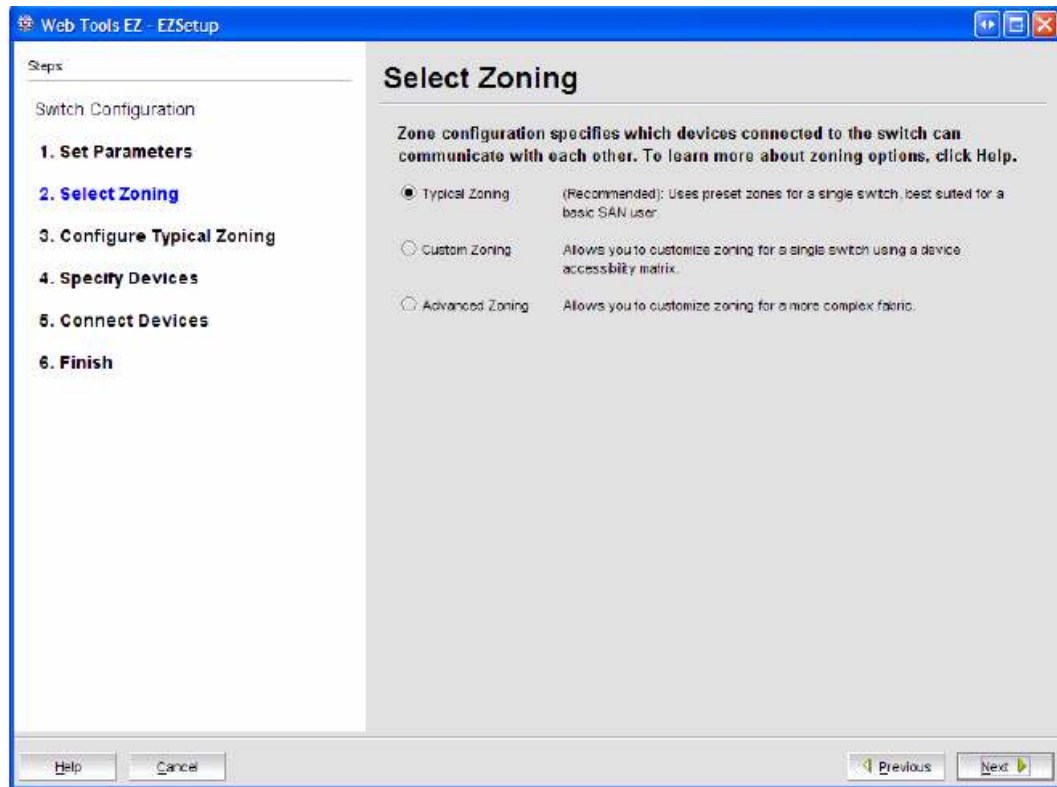
Sovellus etsii asennettavan kytkimen ja pyytää vaihtamaan pääkäyttäjän salasanan. Niiden kirjoittamisen jälkeen määrittelin LAN-asetukset hallintaverkolle, jotta kytkimen hallinta onnistuu myöhemmin Java Webstart -sovelluksen avulla.



Kuva 12: LAN-asetusten määrittely

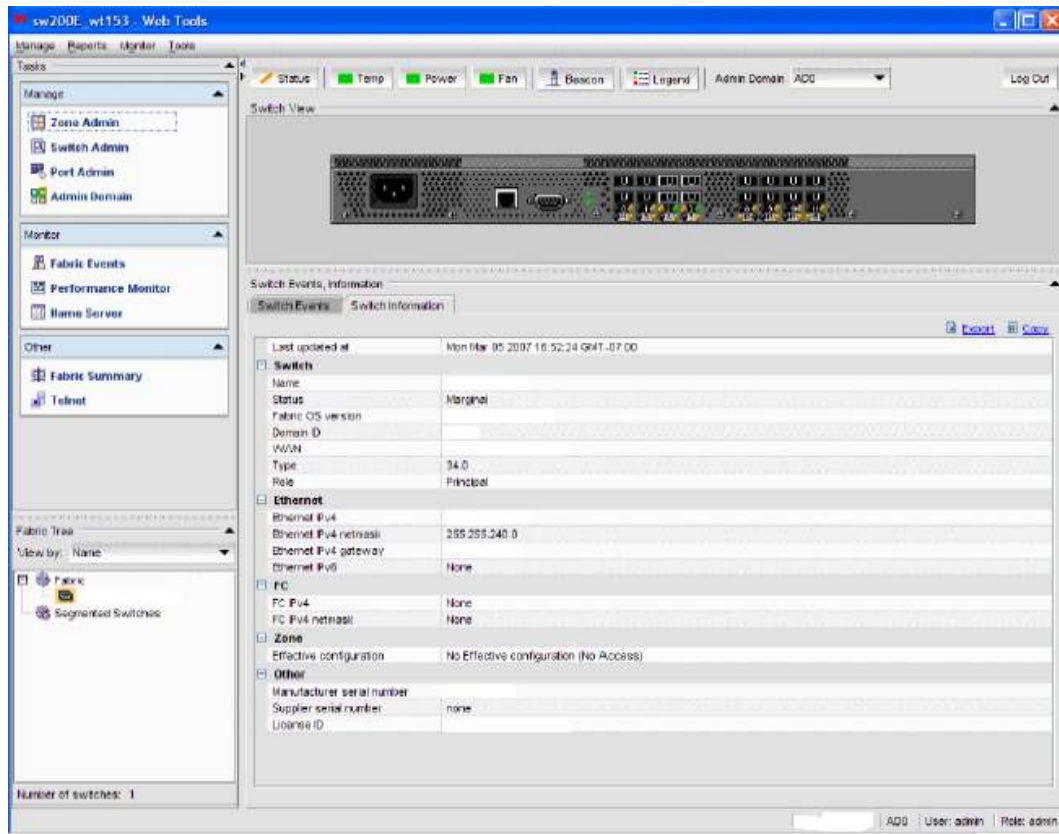
IP-asetusten jälkeen päästään tekemään varsinaista kytkimen asennustyötä. Määritellään kytkimen nimi ja käytettävä aikavyöhyke. Aikatiedot ovat lokitiedostojenkin kannalta erittäin tärkeä asia.

Perustietojen määrittelyn jälkeen voidaan alkaa luoda kytkimen Zone-tietojen käyttötapaa. Zone-tiedot määrittelevät, millä tavoin kytkimeen kytketyt laitteet saavat nähdä toistensa tietoja. Tässä tapauksessa valitsin Typical Zoning -vaihtoehdon, koska mitään erikoisasetuksia ei tarvittu.



Kuva 13: Käytettävän Zone-tilan valinta

Lopulta asensin vielä SFP-modulit laitteen paikkoihin, ja kaapelit Blade-kehikkoon ja toiset levyjärjestelmää varten. Asetukset täytyi tehdä tietenkin molempiin kuitukytkimiin molemmissa konesaleissa. Lisäksi kytkettiin kaapelit, jotka on kytketty konesalien välisiä yhteyksiä varten, jotta molempien konesalien kytkimet saatiin samaan Fabriciin. Jatkokytkennät tehdään levyjärjestelmän asennuksen yhteydessä web-hallinnan kautta.



Kuva 14: SAN-kytkimen web-hallinta

6.6. Levyjärjestelmän asennus ja käyttöönotto

6.6.1 Levyjärjestelmän valinta

HP:lta saatujen tietojen perusteella täytyi valita ympäristön tarkoitusta vastaava levyjärjestelmä. Koska ympäristön toimintavaatimukset vaativat levyjärjestelmän peilausta, MSA-sarjan tuotteita ei voida käyttää. Verkkosivustojen levytilantarve ei arvioiden mukaan tule ylittämään 50 teratavun rajaa, joten EVA-4400 -mallinen levyjärjestelmä riittää käyttöön mainiosti.

Levyjärjestelmän suorituskyvyn vuoksi päätin hankkia molempiin levyjärjestelmiin 2 levykehikkoa, joihin tuli yhteensä 20 kappaletta 450 gigatavun 15 000 kierrosta minuutissa pyöriviä FC-kiintolevyjä. Molempiin levykehikoihin tuli näin ollen 10 levyä. Suorituskyky näillä levyillä riittää arviolta 15 palvelimeen laitetilaa kohti.

Molempiin levyjärjestelmiin hankittiin myös Continuous Access -lisenssit, jotka mahdollistavat reaaliaikaisen levyjärjestelmän peilauksen. Levyn kapasiteettia koskevat lisenssit ostettiin myös koko levyjärjestelmän maksimikapasiteettiin asti yltävinä versioina, jotta lisenssipäivityksiä ei myöhemmin tarvitse enää tehdä.

6.6.2. Hallintapalvelimen asentaminen

Enterprise Virtual Array -levyjärjestelmät vaativat erillisen hallintapalvelimen, joka on kytketty tallennusverkkoon. Palvelimelle asennetaan tarvittavat sovellukset levyjärjestelmän hallintaa varten. Myös valvontasovellukset, joiden avulla vikailmoitukset lähtevät automaattisesti HP:n valvomoon asennetaan levyjärjestelmän hallintapalvelimelle. Luotettavuuden vuoksi asensin molempiin palvelintiloihin oman hallintapalvelimen kyseisen palvelintilan levyjärjestelmää varten.

Hallintapalvelimeksi soveltui mainiosti HP:n Proliant DL-360 G5 -sarjan räkkiin kytkettävä palvelin, johon optiona valittiin myös vikasietoinen virtalähde ja kuituverkon käyttöä varten tarvittava verkkokortti. Käyttöjärjestelmäksi asensin Windows Server 2003 R2:n. Käyttöjärjestelmälle asennettiin tarvittavat päivitykset.

HP:n levyjärjestelmän hallintasovelluksen nimi on Command View. Sovellus asennetaan kuten mikä tahansa Windows-sovellus. Asennuksen jälkeen sovellus etsii saatavilla olevat levyjärjestelmät, ja ne tulevat hallintanäkymässä näkyviin.

The screenshot displays the StorageWorks Command View EVA management interface. The left sidebar shows a tree view of the storage system components, including EVA Storage Network, EVA4100, Virtual Disks, Hosts, Disk Groups, Data Replication, and Hardware. The main window shows the 'Initialized Storage System Properties' for the selected system. The interface includes a 'Refresh' button and tabs for 'General', 'Status Summary', and 'Licensing'. The 'Status Summary' tab is active, showing a table of system components and their status.

Storage	Good	Attention	Failed	Total
Virtual Disks	—	—	—	—
Disk groups	†	—	—	†
DR groups	—	—	—	—

Hosts	Good	Attention	Failed	Total
Hosts	n/a	n/a	n/a	n/a

Hardware	Good	Attention	Failed	Total
Controllers	2	—	—	2
Disk drives	—	—	—	—
ISCSI devices	—	—	—	—

Kuva 15: StorageWorks Command View EVA - hallintasovellus

6.6.3. Levyjärjestelmän asennus

Levyjärjestelmän asennus alkoi laitteiden asentamisella kaappeihin. Levyhyllyt asennetaan päälletysten ja ohjaimet heti levyhyllyjen alapuolelle, jotta mukana toimitettavat lyhyet kaapelit ylettyvät kaikille levyhyllyille. Ohjeistus kaapelointiin löytyy levyjärjestelmän mukana toimitettavasta oppaasta, jonka mukaan asennuksen saa suorittaa itse. 6000- ja 8000-sarjan levyjärjestelmien asentaminen omatoimisesti ei olisi ollut mahdollista, koska niissä vaaditaan tietyn HP:n asennusluokituksen suorittamista.

Kaapelit kulkevat molempien ohjaimien kautta, joten jos toinen ohjaimista tai kaapelista rikkoutuisi, palveluun ei aiheudu katkosta. Kaapeleiden asennuksen jälkeen tarkistin vielä useaan kertaan, että kaikki kaapeloinnit on tehty oikein, jotta toiminnassa ei aiheudu ongelmia myöhemmin. Hyllyjen väärästä kytkennästä aiheutuvat viat voivat olla erittäin hankalia korjata levyjärjestelmän käyttöönoton jälkeen.

Kun kaapelit oli saatu asennettua, käynnistin levyjärjestelmän laitteet. Laitteiden kyljestä saadut SAN-verkon osoitteet määriteltiin näkymään hallintapalvelimelle ja levyjärjestelmälle, jolloin levyjärjestelmä tuli hallittavaksi HP:n sovelluksen kautta hallintapalvelimella.

6.7. Palvelinympäristön asentaminen

6.3.1. Palvelinkehikon asennus

Palvelinkehikot asennettiin molemmissa konesaleissa kaappien alareunoihin, koska ne painavat erittäin paljon. Kiskot ruuvattiin ensimmäisiin kiinnikkeisiin ja kehikko nostettiin niiden päälle. Kehikko oli mallia HP BladeCenter C7000. Kehikon takapuolelle asennettiin lisätuulettimet, jotta tuulettimia olisi yhteensä 12 kappaletta ja jäähdytysteho riittäisi kasvavissakin tarpeissa. Myös virtalähteiden määrä kasvatettiin maksimimäärään eli kuuteen virtalähteeseen. Suuri määrä virtalähteitä mahdollistaa laitteiston toiminnan, vaikka osa olisikin vaurioitunut.

Laitteiston takaosaan kytketään iLO-moduulin verkkokaapeli. Verkkoon tehdään tarvittavat IP-osoiteasetukset, jolloin myös palvelinkehikon ominaisuuksia voidaan hallita suoraan toimistolta. Onboard Administrator -niminen sovellus toimii selaimen välityksellä, joten erillisiä asiakassovelluksia ei tarvita.

6.3.2. Palvelinten asentaminen

HP BL460C G1-malliset korttipalvelimet saapuivat yksittäispakattuina. Laitteet purettiin pakkauksista, niiden kansi avattiin ja lisättiin muistia riittävät 8 gigatavua jokaiseen koneeseen. Lisäksi koneisiin asennettiin valokuituverkkokortit, jotta levyjärjestelmän käyttäminen olisi mahdollista. Tämän jälkeen palvelimet voitiin asentaa kehikkoon kiinni. Asentaminen tapahtui helposti. Kehikosta irrotettiin palvelinpaikan edessä oleva suojamuovi ja palvelin painettiin paikalleen.

6.3.3. Virtual Connect -moduulit

Palvelinkehikon takapuolelle tarvittiin vielä tarvittavat verkkoliittimet, jotta palvelimet voidaan kytkeä toimintaan. Ylimmäiseen riviin asennettiin Ethernet-verkon moduulit, joissa on kahdeksan verkkoliitäntää. Seuraavaan riviin asennettiin valokuituverkkoa varten moduulit, joiden avulla voitiin kytkeytyä levyjärjestelmään.

Ensimmäisestä Ethernet-moduulista kaikki kahdeksan kaapelia kytkettiin ensimmäiseen Ethernet-kytkimeen ja vastaavasti toisesta moduulista toiseen kytkimeen. Varayhteydet verkossa olisivat näin valmiita, koska kehikko osaa automaattisesti siirtää verkkoliikenteen toiselle moduulille, jos ensimmäinen verkko vaurioituu. Valokuitumoduulista kytkettiin neljä kaapelia ensimmäiseen kuitukytkimeen ja toisesta moduulista toiseen kuitukytkimeen, jolloin myös kiintolevyjen liikenne oli kahdennettu.

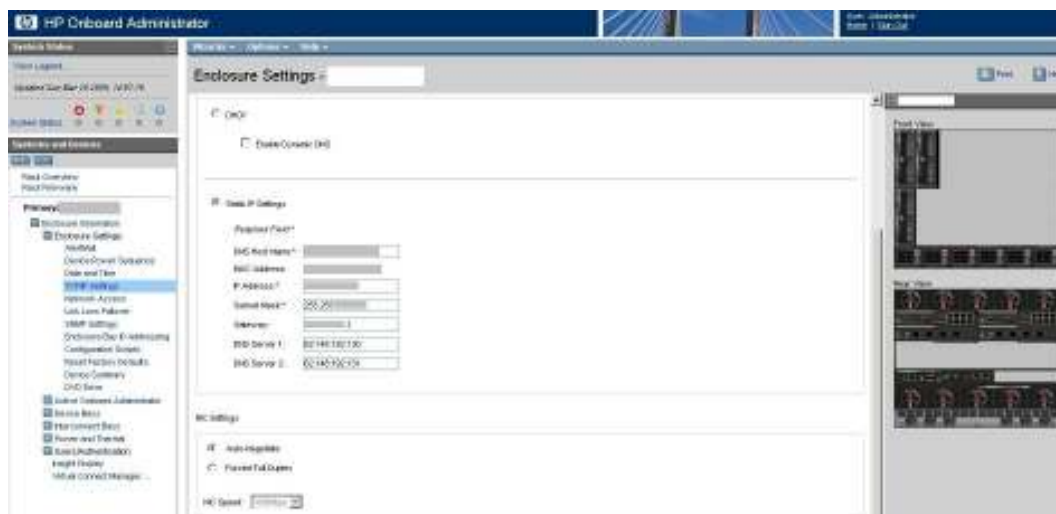
6.3.4. Käyttöönotto

Fyysisten asennusten jälkeen siirryttiin toimistolle ottamaan ympäristöä käyttöön.

Aluksi latusimme HP:n sivustolta tarvittavat päivitykset kaikkiin laitteiston osiin. Onboard Administrator päivitettiin ensimmäisenä. Seuraavaksi päivitettiin kaikki Virtual Connect -moduulit. Kehikon versiot olivat nyt ajan tasalla, ja ongelmilta tultaisiin välttymään. Vanhan version Virtual Connect -moduulit eivät olisi toimineet kahdennetussa ympäristössä toivotulla tavalla.

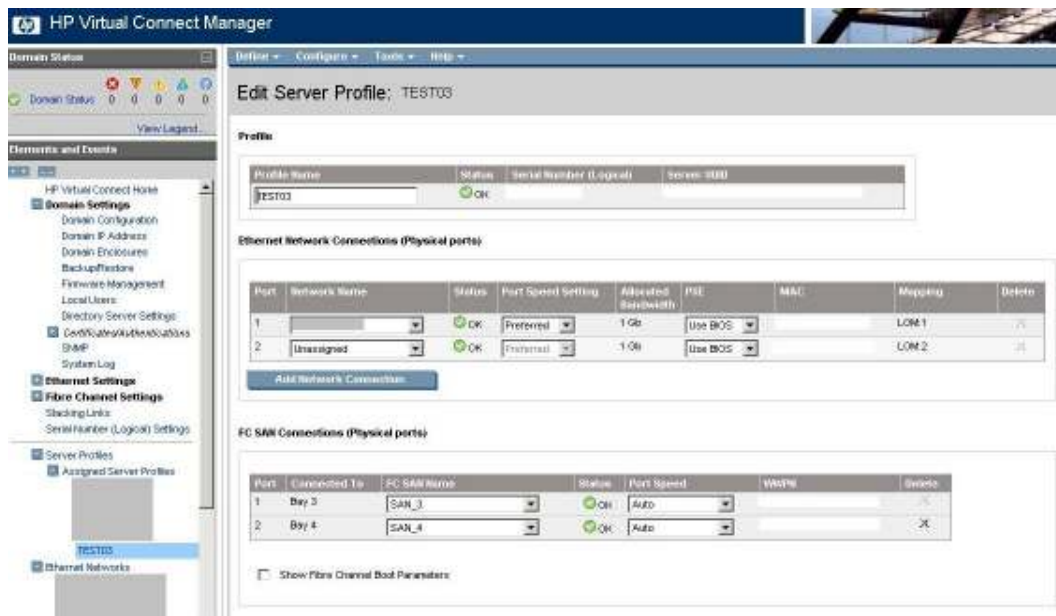
Palvelimet päivitettiin yksi kerrallaan päivityslevyn avulla. CD:n avulla kaikki palvelinten laitekomentit päivittyvät automaattisesti, eikä jotain tiettyä osaa unohdeta. Päivitys onnistui helposti, koska oikeaa levyä ei tarvita. Virtuaaliset mediat palvelimessa mahdollistavat kiintolevyjen että CD/DVD-levyjen jakamisen toimistolta käsin.

Päivitysten jälkeen tehtiin tarvittavat yleisasetukset, jonka jälkeen vasta päästäisiin palvelinten käyttäjärjestelmien ja sovellusten asentamiseen. Palvelinten hallintaverkon IP-osoitteet määriteltiin valmiiksi, kuten myös kehikon valvonta-asetukset, kellonajat sekä virrankulutukseen liittyvät asetukset.



Kuva 16: HP Onboard Administrator

Virtual Connect Managerilla luotiin palvelimille verkkoprofiilit, joiden avulla määrätään, mihin lähiverkkoihin palvelimilla on pääsy.



Kuva 17: HP Virtual Connect Manager

Virtual Connect Managerin avulla määrittelin kaikille palvelimille tarvittavat VLAN-verkot, jotta ne erotellaan toisistaan tietoturva-vaatimuksia vastaavasti. Lisäksi määritellään SAN-asetukset, jotta palvelimet tietävät saatavilla olevan virtuaalisia levyjä. Kun SAN-asetukset on määritetty, käynnistin palvelimet, jotta ne alkavat lähettää WWN-osoitteita SAN-kytkimille.

SAN-kytkinten hallinnan kautta varmistin hakutoiminnolla, että tarvittavat WWN-osoitteet ovat näkyvillä. Tämän jälkeen tein uudet profiilit palvelimille niiden nimen perusteella ja liitin palvelimet samaan ryhmään levyjärjestelmän kautta kunkin palvelimen kohdalla. Tämän jälkeen ryhmä täytyi vielä liittää Zonen konfiguraatioon mukaan. Kuitukytkimen tietojen tallennuksen jälkeen siirryin levyjärjestelmän hallintaan.

Levyjärjestelmän hallinnassa määrittelin uuden host-tiedon, joka löytyi WWN-osoitteen perusteella. Oikeiden laitteiden löytäminen oli helppoa, koska luettelossa näkyy ainoastaan sellaiset laitteet, joille on tehty konfiguraatio kuitukytkimen asetuksiin, ja jotka eivät ole vielä lisättyinä mihinkään host-tietueeseen.

Host -tietojen lisäämisen jälkeen loin palvelimille virtuaalilevyt määriteltyjen kokosuositusten mukaisesti. Palvelinten uudelleenkäynnistyksen jälkeen palvelimet käynnistyvät kuitulevyiltä ja palvelinten sovellusten asentaminen voi vihdoin alkaa.

6.8. Sovellusympäristön asentaminen

Useissa palvelimissa tarvittava käyttöjärjestelmäversio on Windows Server 2003 R2 64-bittisenä versiona. Useiden palvelinten asentaminen yksi kerrallaan samalta levyiltä kestäisi kauan. Tehokkuuden ja palveluiden yhtenäisyyden vuoksi päätin toteuttaa perusasennukset kloonamalla levyt.

Ensiksi valitsin ensimmäisen palvelimen ensimmäisestä konesalista ja asensin siihen Windows Serverin käyttämällä avuksi HP:n SmartStart -levyä, joka sisältää kaikki palvelinten tarvitsemat ajurit ja tukisovellukset. Kun käyttöjärjestelmän asennus oli valmis, etsin HP:n sivustolta tarvittavat levyjärjestelmän MPIO-ajurit, jotka mahdollistavat levyjärjestelmän käynnistyspolkujen muuttamisen koneen ollessa käynnissä.

Palvelimeen ladattiin kaikki uusimmat sovelluspäivitykset update.microsoft.com -sivustolta. Lisäksi tarvittiin Microsoftin sivustolta löytyvä Sysprep-työkalu, jolla palvelinten yhtenäiset ”Computer Security Identifier” (SID) -tiedot, palvelinten nimet ja osoitetiedot voidaan vaihtaa kopioista asennettaessa. Latasin työkalut valmiiksi palvelimelle, jotta niitä ei tarvitse hakea jokaisella palvelimella erikseen.

Lopuksi kopioin Windowsin asennuslevyn sisällön `c:\support`-hakemistoon, jotta levyä ei tarvitse asettaa palvelimen levyasemaan jokaisen Windows-komponentin asennuksen yhteydessä.

Kun palvelin oli asennettu, siirryin levyjärjestelmän hallintasivuston puolelle ja tein levystä kopion. Kopio asetettiin kaikille paikallisille palvelimille, jossa samaa käyttöjärjestelmää käytetään ja tämän jälkeen peilattiin levyt toisen konesalin puolelle Continuos Accessin avulla. Sysprep-työkalun suorittamisen jälkeen palvelimet ovat käytettävissä ja asennettavissa.

6.4.1 Hakemistopalvelin

Hakemistopalvelimet AD01 ja AD02 ovat ensimmäiset palvelimet, jotka vaaditaan ympäristön rakentamisessa, koska muut koneet käyttävät näitä palvelimia kirjautumisen varmentamiseen ja DNS-kyselyiden hakemiseen. Palvelimille määriteltiin IP-asetukset ja DNS-tietueiksi paikalliset palvelinosoitteet. Tämän jälkeen aktiivihakemisto voitiin asentaa käynnistämällä dcpromo-sovellus.

Ensimmäisellä palvelimella määrittelin, että halutaan luoda uusi metsä, johon tehdään ensimmäinen hakemistopalvelin. Nimipalvelut sijoitetaan samalle palvelimelle ja luodaan automaattisesti, koska aikaisempia nimipalvelimia ei ollut määritetty. Toimialuenuimeksi tuli asiakasoy.fi, joka on sama kuin yrityksen julkinen toimialue Internetin puolella.

Ensimmäisen palvelimen asentamisen jälkeen AD02 määriteltiin samaan metsään toiseksi aktiiviseksi toimialuepalvelimeksi. Global Catalog -roolit otettiin käyttöön myös AD02-palvelimella ja toimialueen taso määriteltiin tukemaan ainoastaan Windows 2003 ja sitä uudempia palvelimia.

Palvelinten keskitettyyn päivitysten hallintaan AD01-palvelimelle asensin lisäksi vielä Windows Server Update Services -nimisen sovelluksen, jonka avulla kaikille palvelimille voidaan asentaa käyttöjärjestelmän ja Microsoftin sovellusten päivitykset keskitetysti. Sovellus nopeuttaa ympäristön ylläpitoa jatkossa.

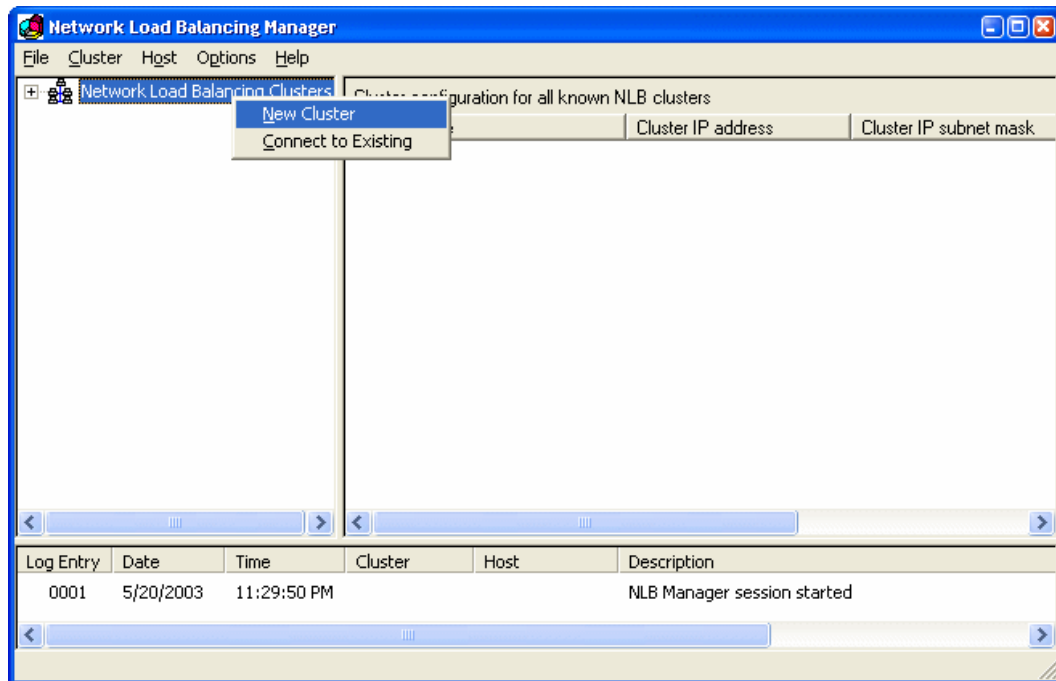
6.4.2 Verkkosivustopalvelimet

Asiakkaan verkkosivustojen toiminnallisuusmäärittelyssä oli mainittu ASP.NET 2.0 -tasoiset sovellukset, joiden perusteella käytettäväksi web-palvelinalustaksi vaadittiin Microsoft IIS v.6.0. Palvelinohjelmisto toimitetaan käyttöjärjestelmän mukana, mutta se täytyy erikseen asentaa käyttöön. IIS asennettiin Windowsin lisää-/poista sovellus -työkalulla.

Koska käytössä on 64-bittiset käyttöjärjestelmät, asensin lisäksi asp.net 2.0 sovellusrajapinnasta 64-bittisen version antamalla komennon:

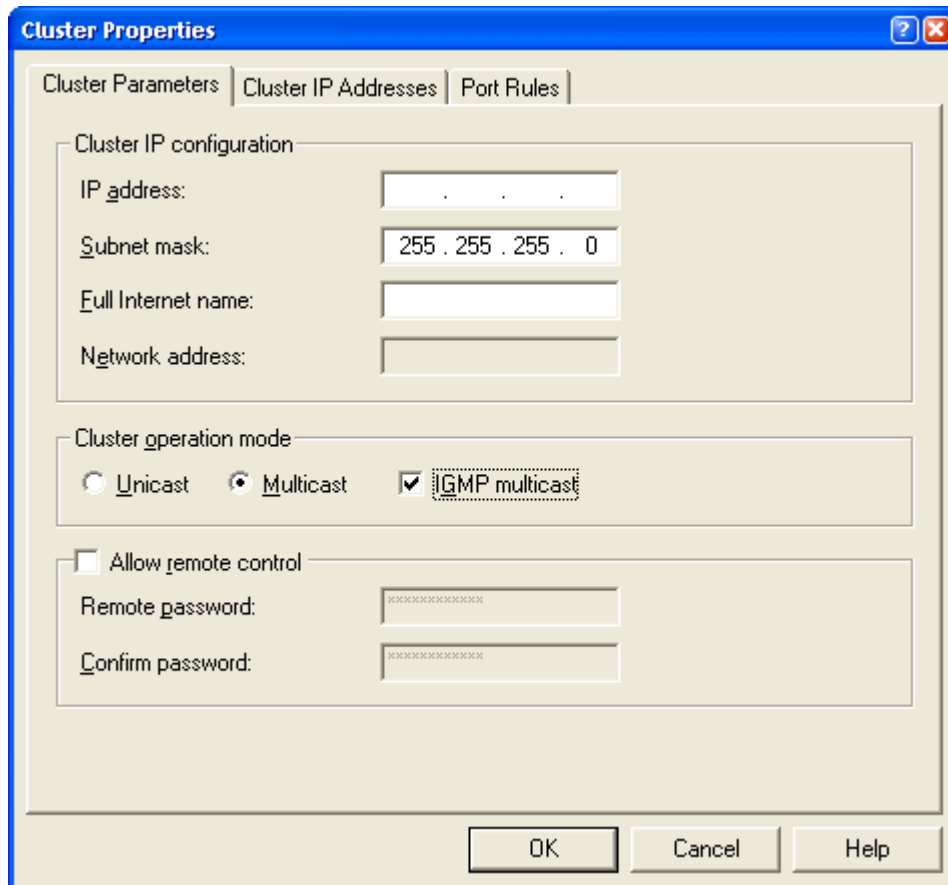
```
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\aspnet_regiis -r
```

Työkalut asennettiin molemmille web-palvelimille. Koska palvelinten välillä on tarkoitus ajaa aktiivista kuormantasausta, tarvittiin vielä määrittymiset Network Load Balancing Manager -sovelluksella. NLB-klusterin rakentaminen aloitetaan valitsemalla Cluster-valikko ja sen alta New Cluster.



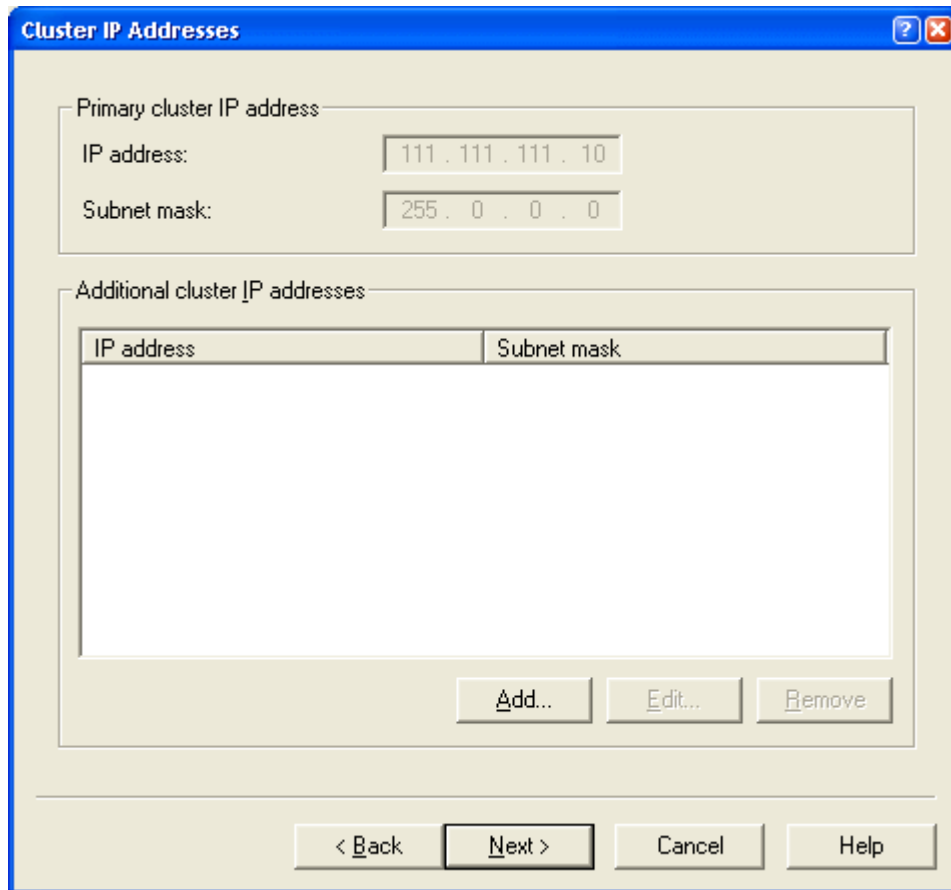
Kuva 18: Network Load Balancing Manager

Klusterin virtuaalinen osoite syötetään IP-osoitekenttään. Lisäksi annetaan Internet-nimi, eli palvelimen lopullinen osoite, tässä tapauksessa www.asiakasoy.fi. Klusterin käytettävä tila määrittyy verkon rakenteen mukaan. Koska halusin saada liikenteen toimimaan palvelintilojen välissä, ainoa mahdollinen tila on IGMP-multicast. Multicast-tilassa ilman IGMP:tä verkko ei toiminut luotettavasti, jolloin IGMP laitettiin päälle ja verkko alkoi toimia.



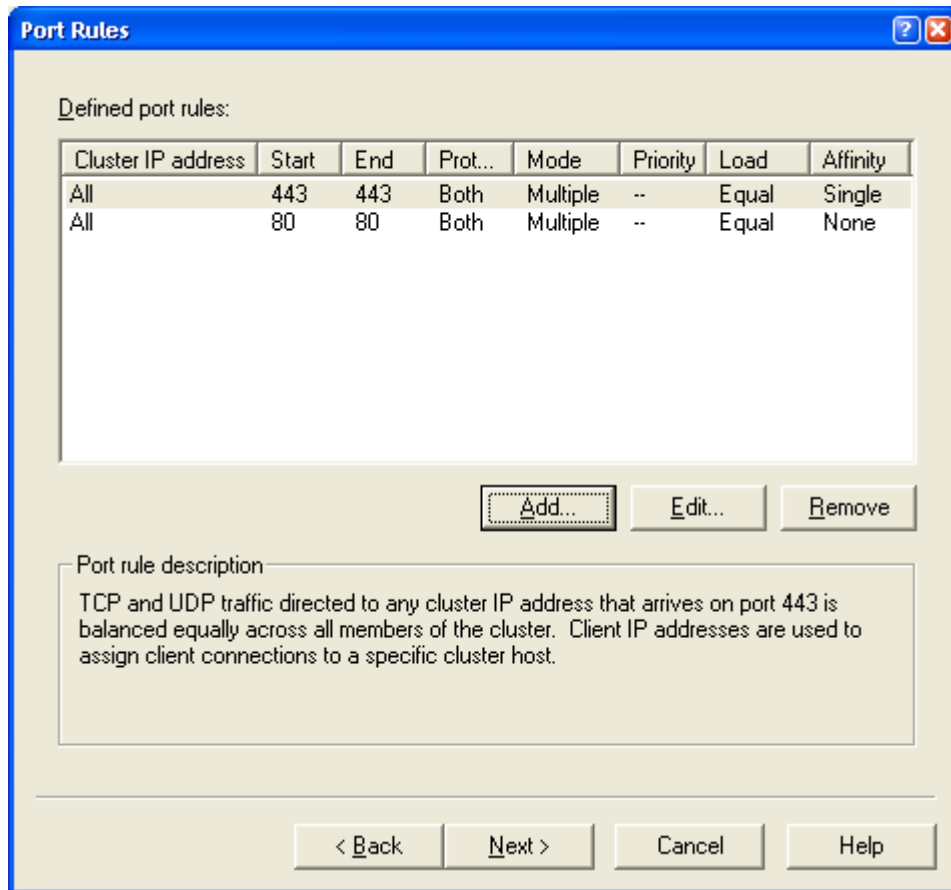
Kuva 19: Uuden NLB-klusterin luonti

Cluster IP Addresses -sivulla voidaan määrittellä klusteriin useampia ip-osoitteita, jos käytetään esimerkiksi IIS 6:n useampia verkkosivustoja, jotka on erotettu toisistaan ip-osoitteen perusteella. Tässä projektissa useammille ip-osoitteille ei kuitenkaan ollut tarvetta, koska erilliset verkkosivustot erotellaan toisistaan host-nimien perusteella.



Kuva 20: Klusterin ylimääräisten ip-osoitteiden määrittely

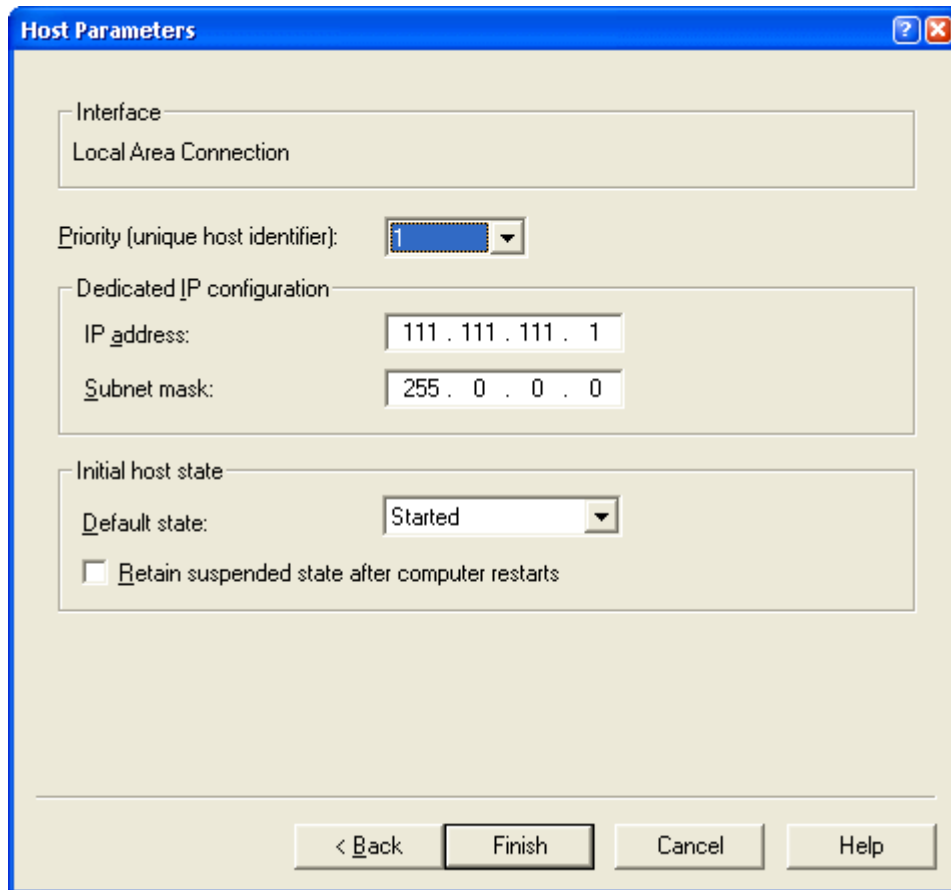
Port Rules -välilehdellä määritellään, mitkä portit kuormantasaus jakaa palvelinten välillä. Lisäksi voidaan määrittellä, millä tavalla tietty portti jaetaan palvelinten kesken. Kaikkien porttien jakaminen toimii useammassa tapauksissa. Jos tietoturvaan halutaan kiinnittää huomiota sisäverkonkin puolella, voidaan määrittellä ainoastaan ne portit, joita käytetään esimerkiksi juuri verkkosivustoille tuleva liikenne 80- ja 443-porteista.



Kuva 21: Kuormantasausta hyödyntävien porttien määrittely

Tässä vaiheessa itse klusteri on luotu, ja voidaan määritellä siihen kuuluvat palvelimet. Kuormantasausta voidaan toteuttaa pelkästään yhdenkin palvelimen avulla, jos halutaan mahdollistaa helppo lisättävyys uusille palvelimille, ja klusteriominaisuuksille ei alkuvaiheessa ole tarvetta.

Tässä tapauksessa tarvittiin heti useampi palvelin, joten määrittelyt tehtiin lisäämällä molemmat palvelimet klusteriin. Aluksi valitaan palvelimen prioriteetti, joka etenee järjestyksessä palvelimesta toiseen. Sitten syötetään palvelimen yksilöllinen IP-osoite, joka on käytössä ainoastaan kyseistä klusterin nodia varten. Oletustilaksi on tärkeää valita Started, koska muuten vikatilanteessa klusterin toiminta ei palaudu normaalisti. Tämä asetus aiheutti itselläni ylimääräistä työtä, koska koneen uudelleenkäynnistyksen aikana palveluun tuli suuria katkoksia. Asetusten tekeminen kuvan näköisellä tavalla mahdollisti kuitenkin toiminnan myös koneiden uudelleenkäynnistyksen jälkeen.



Kuva 22: Yksittäisen palvelimen lisääminen NLB-klusteriin

5.4.3 Tietokantapalvelimet

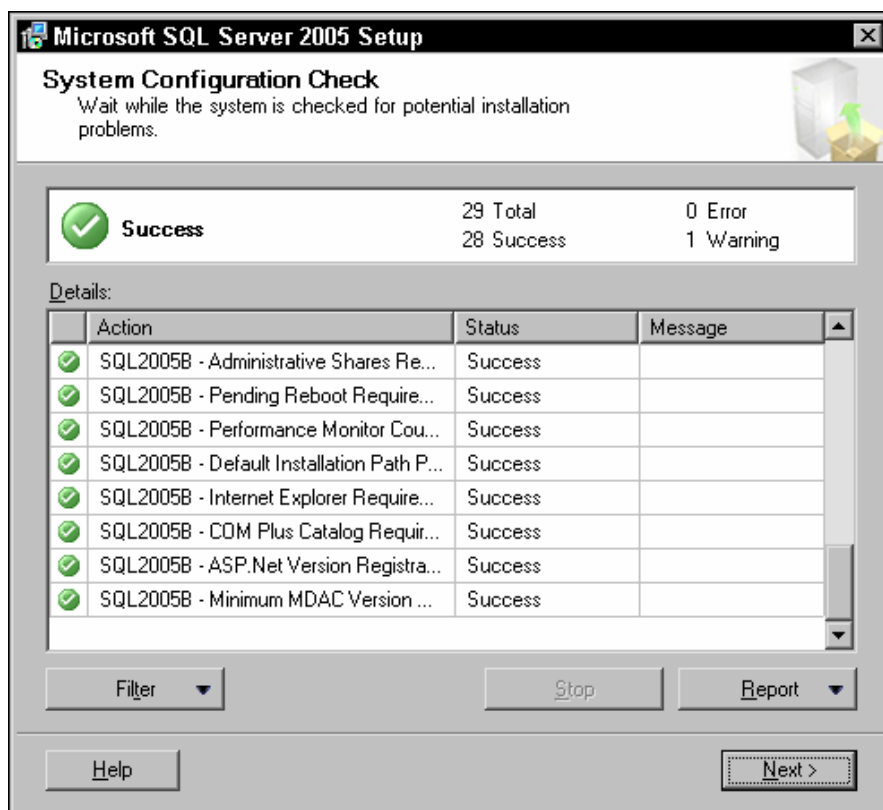
Aloittaessani työn kirjoittamista, minulla oli käsitys että klusteroidun tietokantaratkaisun toteuttaminen olisi vaikea projekti. Lopulta tämä vaihe osoittautui kuitenkin melko helpoksi Sql Server 2005:n valmiiden klusterointitoimenpiteiden vuoksi. Klusterin asentaminen ensimmäiselle palvelimelle alkaa asettamalla sovelluksen dvd koneen virtuaaliseen asemaan.



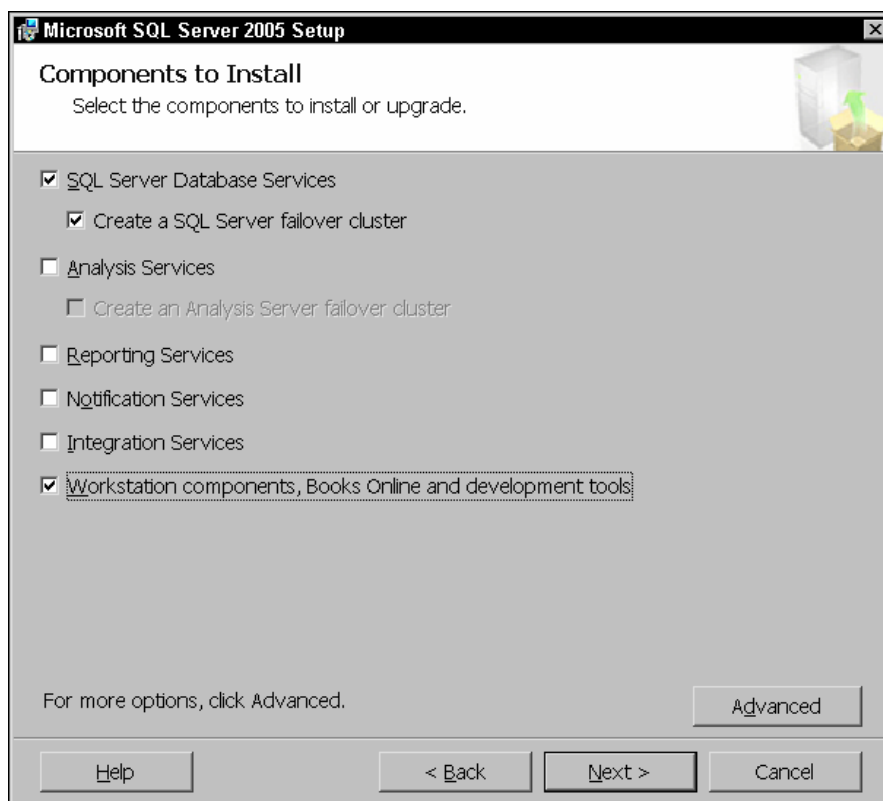
Kuva 23: SQL Server 2005 asennuksen ensimmäinen vaihe

Kun asennus on aloitettu, asennus tarkistaa, että palvelimella vaadittavat komponentit on asennettu, jotta asennus varmasti onnistuu. Vaatimuksia ovat mm. uusimmat käyttöjärjestelmäpäivitykset, asp.net 2.0 asennettuna ja iis 6 asennettuna. Kaikki nämä olin asentanut jo valmiiksi, joten tässä vaiheessa ei tullut ongelmia, valitsin Next.

Seuraavassa valinnassa on tärkeää muistaa valita ”Create a SQL Server failover cluster” -valinta, joka muuttaa olennaisesti asennuksen etenemistä ja mahdollistaa klusterin rakentamisen palvelimelle. Monet toiminnot on automatisoitu, jos tämä valinta on valittu ajoissa.

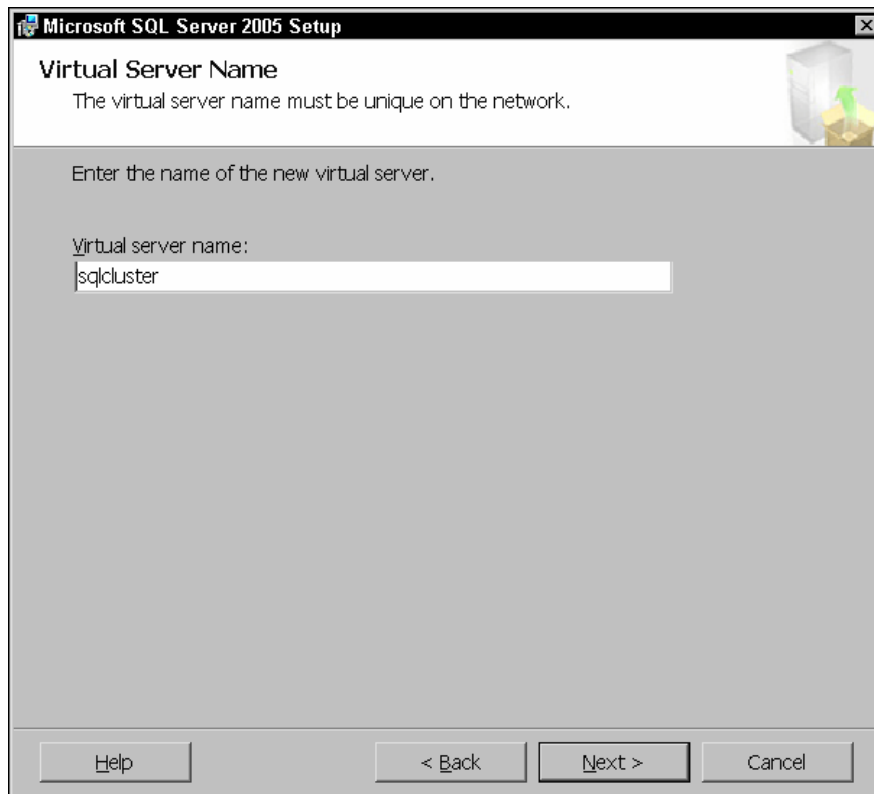


Kuva 24: SQL Server 2005:n asennuksen toinen vaihe. Vaadittavien komponenttien tarkistaminen



Kuva 25: SQL Server 2005 asennus, 3. vaihe. Komponenttien valinta

Seuraavaksi määritellään klusterille sopiva nimi. Klusteri määritellään omalla nimellään ja IP-osoitteellaan, joten näillä tiedoilla on merkitystä sovellusten asennuksen kannalta. Sovellukset käyttävät klusterin osoitteita tietokantapalvelinten osoitteiden sijaan.



Kuva 26: Klusterin nimen määrittäminen

Seuraavalla välilehdellä määritellään verkot, joita klusteri käyttää toiminnassaan. Osoitteiden lisäämisen jälkeen painetaan jälleen Next. Seuraavaksi valitaan klusteriryhmä ja tiedostojen sijainti, johon tietokantapalvelimen tiedostot asennetaan. Klusterin käyttämä levy näkyy molemmille palvelimille levyjärjestelmän kautta, ja klusteri hallitsee sen näkyvyyttä palvelimille. Valitaan SQL Server Group ja sijainniksi tietokannan tiedostoille tehty F-levy.

Microsoft SQL Server 2005 Setup

Virtual Server Configuration

Enter virtual server information.

Enter an IP address for the virtual server. To add IP addresses for additional networks, click Add.

Virtual server name: sqlcluster

Network to use: Public

IP address: 192 . 168 . 1 . 100

Network address: 192.168.1.0

Network subnet: 255.255.255.0

Add Remove

Selected networks and IP addresses:

Help < Back Next > Cancel

Kuva 27: Klusterin osoitteiden määrittely

Microsoft SQL Server 2005 Setup

Cluster Group Selection

Select the cluster group where the virtual server resources will be installed.

Available cluster groups:

- Cluster Group
- SQL Server Group

Unavailable cluster groups:

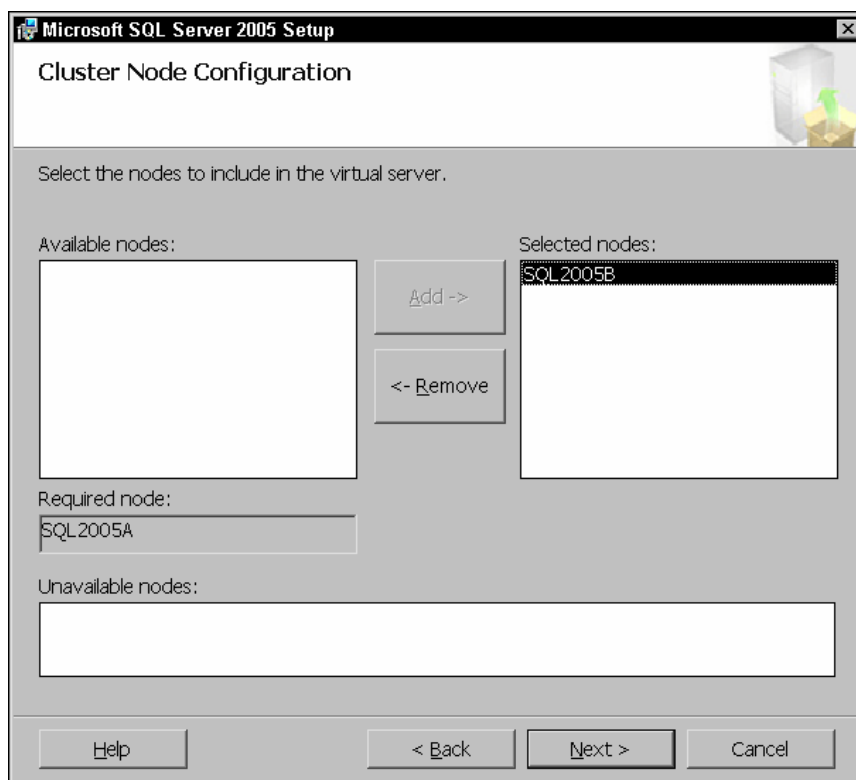
Data files: F:\Microsoft SQL Server\

Help < Back Next > Cancel

Kuva 28: Tiedostojen asennussijainnin määrittely

Kun asennuspolut on määritelty, liitetään asennettavat palvelimet klusteriin. Klusteriin lisätään myös toinen tietokantapalvelin ja jatketaan asennusta. Seuraavassa valinnassa määritellään vielä käytettävä käyttäjätunnus, joka sijaitsee aktiivihakemistossa ja jolla on pääsy molempiin tietokantapalvelimiin pääkäyttäjaoikeuksin. Tässä vaiheessa käytin Administrator-tunnusta.

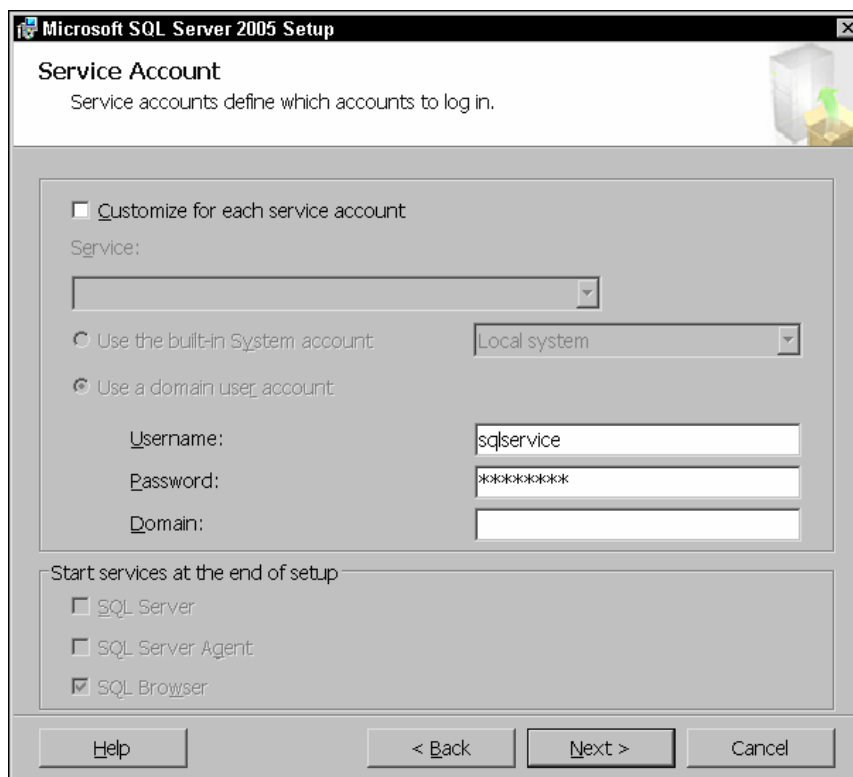
Määritellään myös tietokantapalvelimen käyttämien järjestelmäprosessien ajamisessa käytettävät tunnukset. Tunnus on luotu aktiivihakemistoon ja määritelty molempien palvelinten Local Administrators-ryhmään. Tämän jälkeen painetaan Next.



Kuva 29: Klusteriin liitettävien palvelinten valinta

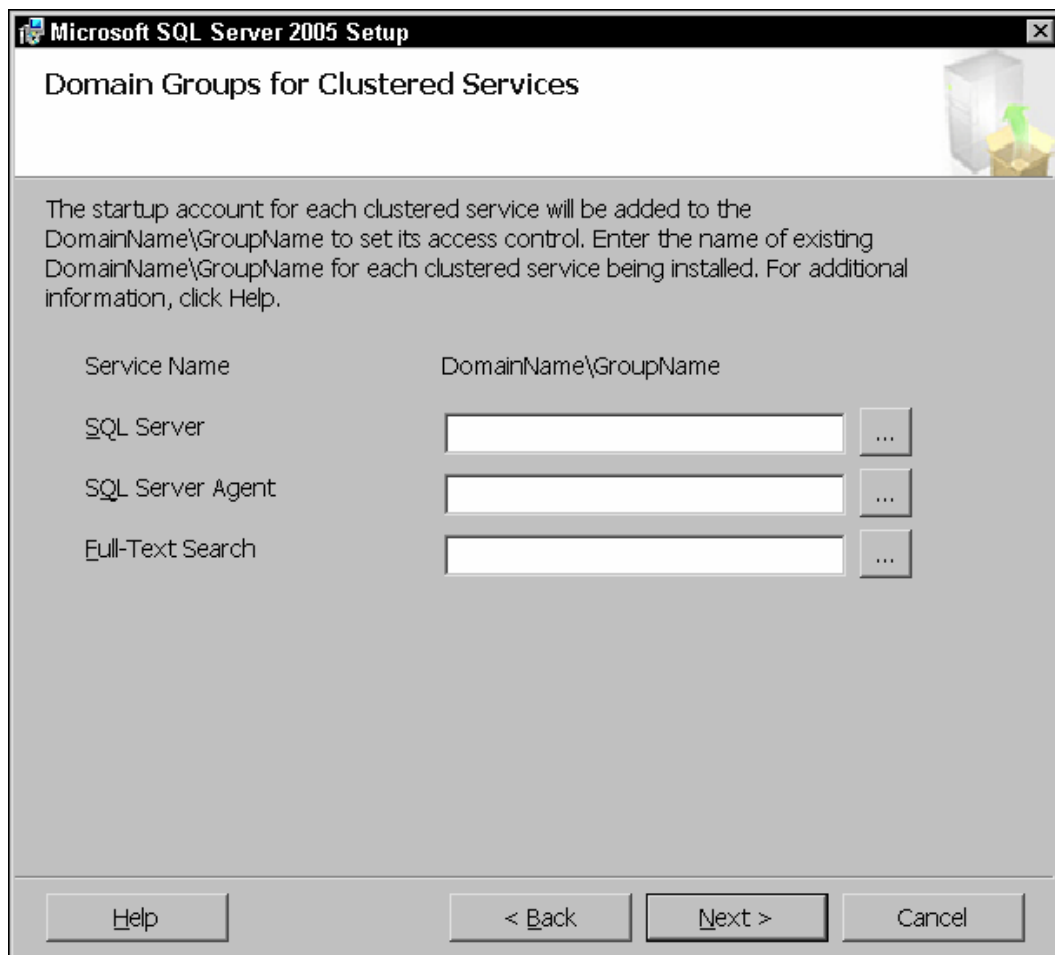


Kuva 30: Pääkäyttäjän salasanan syöttäminen



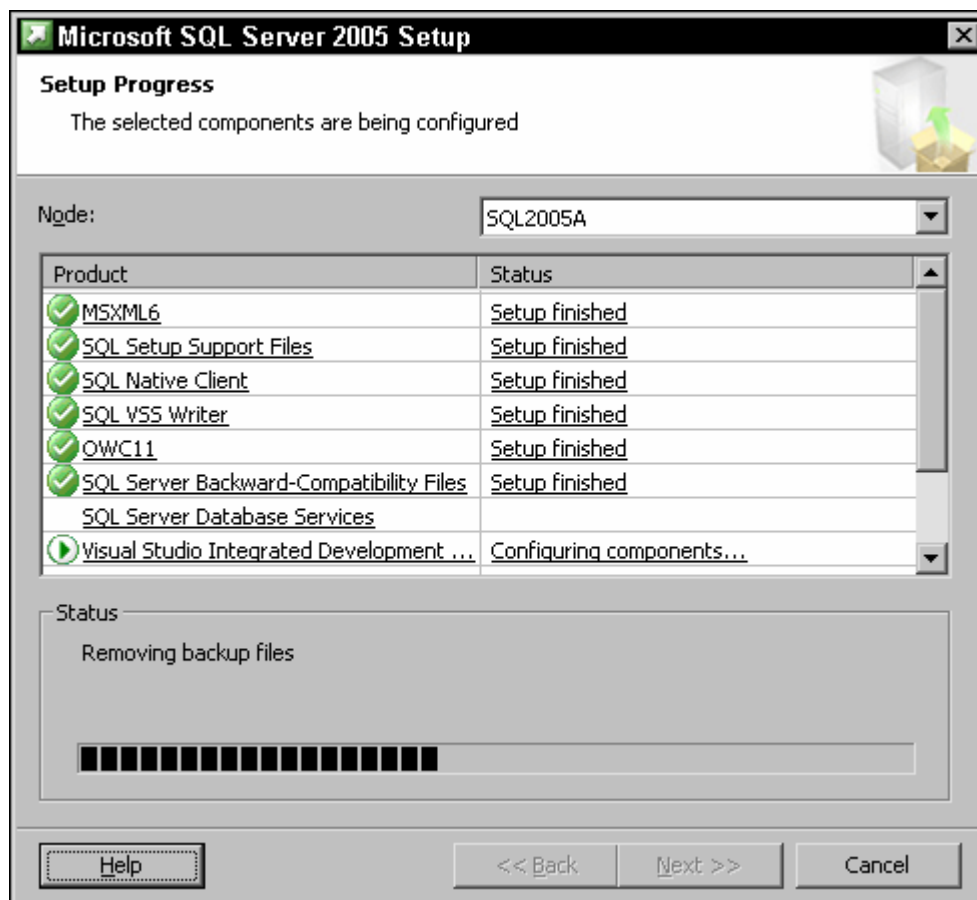
Kuva 31: SQL-palvelimen prosessien ajamisessa tarvittavan tunnuksen määrittely

Seuraavaksi määritellään ryhmät, jotka myöntävät oikeudet tiettyihin tietokantapalvelimen toimintoihin. Kaikki kolme ryhmää voivat olla yhdessä yhteisessä ryhmässä. Ajattelin tämän olevan paras tapa ja lisäsin SQLUsers -nimisen ryhmän aktiivihakemistoon ja määritin sen kaikkiin kuvassa näkyviin kenttiin.



Kuva 32: Tietokantapalvelimen käyttäjätietoryhmien määrittely

Tämän jälkeen klusterin asennus voi alkaa ja palvelut asennetaan palvelimille. Klusteroitu ympäristö on nyt käyttövalmiina. Levyltä saatava versio on kuitenkin Service Pack 1 -tasoinen, joka ei sellaisenaan enää kelpaa useiden palvelinsovel-lusten toiminta-alustaksi. Päivitin Microsoftin päivityssivustolta uusimman Servi-ce Pack 3 -tasoinen version palvelimelle. Tämän jälkeen tietokannat asennettiin palvelimelle asiakkaan toimesta.



Kuva 33: Tietokantapalvelimen asennus

7. TOIMIVUUDEN MITTAAMINEN

Jos palvelun laadulle ja saatavuudelle on asetettu vaatimuksia, täytyy toimintaa kyetä mittaamaan. Mittaamisen avulla voidaan raportoida asiakkaalle toteutuneen palvelutason arvot, joiden avulla asiakas tietää saavansa sopimuksensa tasoista palvelua. Palvelun toimivuutta voidaan mitata sekä 24/7 -valvomon raportoinnin perusteella että erillisillä Disaster Recovery -testauksilla, joiden avulla voidaan varmistua palveluiden saatavuudesta myös laitteiden todella sammussa tai yhteysien katketessa.

Disaster Recovery -testaus tehtiin seuraavan prosessin mukaisesti:

1. Konesali #1:n kaikki laitteet sammutettiin hallitusti. Palvelun saatavuutta mittaavat objektit valvontasovelluksessa eivät havainneet virheitä ja palvelu oli saatavilla konesalin sammuttamisesta huolimatta. Raportoitu viive palveluiden siirtyessä täysin konesali #2:n vastuulle oli alle minuutin pituinen.
2. Konesali #1 otettiin käyttöön ja vastaava testaus suoritettiin sammuttamalla konesali #2:n laitteet. Raportoitu viive oli samaa luokkaa kuin edellisessä testauksessa ja tulos on kiitettävä.
3. Ensisijaisen dataverkon Internet-yhteyden kaapelit irrotettiin. Palomuuriklusteri huomasi välittömästi yhteyden katkeamisen ja yhteys siirtyi alle minuutin viiveellä varaverkon puolelle. Palvelun saatavuus säilytettiin. Sama prosessi toteutettiin sulkemalla varaverkko, jolloin toiminta siirtyi takaisin pääasiallisen yhteyden puolelle.
4. Palvelun toiminta sähkökatkoksien aikana testattiin sulkemalla yhteys valtakunnalliseen sähköverkkoon. Palvelut pysyivät käynnissä akkuvarmennuslaitteiston avulla. Diesel-käyttöiset varavoimalaitteet lähtivät käyntiin ja alkoivat syöttää virtaa akkuvarmennuslaitteistolla. Palvelun toimintaan ei aiheutunut katkoksia.

Testaaminen osoitti, että palvelut kykenevät automaattisesti palautumaan kriittisistä virhetilanteista ympäristössä. Haluttu palvelutaso toteutuu, ellei molemmissa konesaleissa tapahdu laitteiston täydellistä rikkoutumista samaan aikaan. Järjestelmän yksittäisten komponenttien hajoaminen ei aiheuta katkoksia.

Kolmen kuukauden testausjaksolta hankitun raportoinnin mukaan palvelun saatavuus on ollut 99,953 prosenttia, jolloin 99 prosentin kokonaissaatavuus ylittyy selkeästi. Yksittäisten palvelintilojen saatavuudet ovat yli 98 prosenttia.

8. YHTEENVETO

Opinnäytetyön rakentaminen oli pitkä prosessi ja yllätyin asennusten viemästä ajasta. Ympäristön rakentaminen oli kuitenkin kokonaisuutena erittäin kiinnostava projekti, joka opetti uutta sekä verkkoratkaisuista, laitteistoista että sovelluksista ja hieman ohjelmoinnistakin. Rakentaminen näinkin nopealla aikataululla – muutamassa kuukaudessa oli mahdollista käytettävissä olevien sidosryhmien avulla. Laite- ja sovellustoimittajien tukitoimintojen hyödyntäminen mahdollisti projektin.

Järjestelmän fyysiseen rakentamiseen meni muutama viikko, mutta kaiken testaamisen, dokumentoimisen ja pienten korjausten tekemiseen kului yllättävän paljon aikaa. Palvelu on ollut käytössä asennuksen jälkeen kolme kuukautta ja tänä aikana käytettävyys ylitti selvästi 99 prosentin rajan palvelun saatavuudessa. Yksittäisten laitteidenkin käytettävyys oli lähellä 99 prosenttia.

Olen ollut tyytyväinen valittuani tämän projektin toteutettavakseni, ja projekti on opettanut paljon uusia asioita, joista tulee olemaan paljon hyötyä tulevaisuudessa. Kehitettävääkin vastaavanlaisissa järjestelmissä on edelleen. Virtualisointiratkaisut ovat entistä useammin vaihtoehto ympäristöjen toteutukselle. Lisäksi verkkojen nopeudet ovat nousemassa 10 gigabittiä sekunnissa siirtäviin kokonaisuuksiin, joten asia pysyy ajankohtaisena tulevaisuudessakin.

LÄHTEET

VMWare Inc. Server Consolidation [viitattu 17.11.2009]

<URL:<http://www.vmware.com/solutions/consolidation/index.html>>

Shimonski, Robert 2003. Windows Server 2003 Clustering & Load Balancing. McGraw-Hill Osborne.

Gibson, Darril 2008. MCITP SQL Server 2005 Database Developer All-in-One Exam Guide. McGraw-Hill.

Piltzecker, Tony 2006. How to Cheat at Managing Microsoft Operations Manager 2005. Syngress Publishing.

Barth, Wolfgang 2005. Nagios: System and Network Monitoring. No Starch Press, Inc.