SAVONIA-AMMATTIKORKEAKOULU

Savonia Business

Windows Server 2008 osana toimintavarmaa ja vikasietoista tietojärjestelmää

Pietu Eronen

Tradenomin opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Lokakuu 2009

SAVONIA-AMMATTIKORKEAKOULU
SAVONIA BUSINESS
Koulutusohjelma, suuntautumisvaihtoehto (jos on)

Tietojenkäsittelyn koulutusohjelma

Tekijä(t)

Pietu Eronen

Työn nimi

Windows Server 2008 osana toimintavarmaa ja vikasietoista tietojärjestelmää

Työn laji	Päiväys	Sivumäärä
Opinnäytetyö	5.10.2009	67 + 1

Työn ohjaaja(t)	Toimeksiantaja
Pekka Granroth	Savonia-ammattikorkeakoulu

Tiivistelmä

Opinnäytetyössä selvitettiin tietojärjestelmien toimintavarmuuden ja vikasietoisuuden merkitystä, miten se määritellään, mitä se käsittää sekä mitä niiden parantamiseksi on tehtävissä niin laitteisto- kuin ohjelmistotasolla.

Työssä kuvataan teoriatasolla niitä toimenpiteitä, joilla tietojärjestelmän palvelujen saatavuutta sekä palvelevuutta voidaan parantaa. Lisäksi kuvataan mihin käytettäviä resursseja on syytä kohdentaa kun tavoitteena on tietojärjestelmän korkea toimintavarmuus.

Käytännön tasolla kuvataan mitä Windows Server 2008-käyttöjärjestelmän toimintoja järjestelmän ylläpitäjällä on käytettävissään kun tavoitellaan palvelujen korkeaa saatavuustasoa tietojärjestelmässä. Työssä kuvataan käytännössä Windows Server 2008:n toimintojen asennus- ja konfigurointivaiheita ja niihin liittyviä seikkoja.

Windows Server 2008 soveltuu puutteistaan huolimatta myös korkeaa luotettavuutta sekä vikasietoisuutta vaativien palvelujen alustaksi tietojärjestelmän palvelinten käyttöjärjestelmänä. Sen vikasietoinen klusterointi sekä verkkoliikenteen kuormantasaus ovat sen tärkeimmät toimintavarmuutta ja vikasietoisuutta parantavat toiminnot.

Asiasanat

Tietojärjestelmä, toimintavarmuus, vikasietoisuus, Windows Server 2008, Failover Clustering, Network Load Balancing

Huomioitavaa

SAVONIA UNIVERSITY OF APPLIED SCIENCES
SAVONIA BUSINESS
Degree Programme, option

Degree Programme in Computer Science

Author(s)

Pietu Eronen

Title of study

Windows Server 2008 As a Part of Reliable and Fault Tolerant Computer System

Type of project	Date	Pages
Thesis	5.10.2009	67 + 1

Supervisor(s) of study	Executive organisation
Pekka Granroth	Savonia University of Applied Sciences

Abstract

This thesis describes the meaning and the definition of a reliable and a fault tolerant computer system, how it is constructed and what measures there can be taken both hardware-wise and software-wise to improve the system's ability to operate in a reliable way.

The thesis expresses in theory the means by which the system's ability to provide services and the availability of the services can be improved. Additionally the thesis pinpoints the targets on which to focus when aiming for a highly reliable computer system.

At a practical level the thesis introduces the tools a systems administrator has access to when focusing on highly available services in a computer system based on Windows Server 2008. The details relating to the installation and configuration of Windows Server 2008 tools are also described from a practical viewpoint.

Despite its limitations, Windows Server 2008 is well suited for computer systems where a high level of reliability and fault tolerance are required. Its Failover Clustering and Network Load Balancing are the main tools when providing reliable and fault tolerant services.

Keywords

Computer system, reliability, fault tolerance, Windows Server 2008, Failover Clustering, Network Load Balancing

Note

SISÄLLYS

SANASTO

DFS	Distributed File System. Hajautettu tiedostojärjestelmä.
Domain Controller	Windows-toimialueen ohjauspalvelin.
EEC-muisti	Error Correcting Code. Palvelimissa käytetty muistitekniikka.
Feature	Windows Server 2008:n ominaisuus, vrt. palvelinrooli (role).
Heartbeat	Laitteen tai palvelimen lähettämä signaali, joka viestittää sen olevan toimintakuntoinen.
Hot pluggable	Mahdollistaa järjestelmän vaihto-osan kytkemisen laitteen ollessa käytössä.
Hot swap	Mahdollistaa esimerkiksi palvelimen komponenttien vaihtamisen laitteen ollessa käytössä keskeyttämättä sen toimintaa.
HTTP	Hypertext Transfer Protocol. Selainten ja www-palvelinten tiedonsiirtoprotokolla.
IEEE 1394	FireWire-väylä. Ulkoisten lisälaiteiden (kuten kiintolevyjen) liitäntästandardi.
IIS	Internet Information Services. Microsoftin www-palvelinohjelmisto.
Image tai image-tiedosto	Järjestelmän tilasta otettu levykuva, jota käytetään esim. varmuuskopiontityökaluissa.
IP-protokolla	Internet Protocol. TCP/IP-mallin verkkokerroksen protokolla. Toimittaa tietoliikennepaketit hallitusti kohdeosoitteeseen varmistaen niiden perille menon.
iSCSI	Internet Small Computer System Interface. Nopea IP-protokollaan perustuva lähi- ja kaukoverkkojen verkkostandardi. Käytetään mm. SAN-verkkojen tiedonsiirrossa.
Load	Verkkokuormitus.
NLB	Network Load Balancing. Verkkoliikenteen kuormantasaus.
Node	Klusterin jäsenkone esimerkiksi NLB- tai Failover Clustering-kokoonpanossa.
RAID	Redundant Array of Independent Disks. Vikasietoinen kiintolevyjen asennuskonfiguraatio.
SAN	Storage Area Network. Suurien organisaatioiden verkkoresurssiratkaisu. Mahdollistaa suuren tallennuskapasiteetin lähiverkossa verkkoliikenteen yli.

SLA	Service Level Agreement. Asiakkaan ja palveluntarjoajan välinen kirjallisesti laadittu sopimus tai muu lupaus palvelun saatavuustasosta.
UDP	User Datagram Protocol. TCP/IP-mallin kuljetuskerroksen protokolla. Sovellusten ja tietokoneiden välinen viestienvälityskäytäntö, jossa tietoliikennepakettien perille menoa ei varmisteta.
UPS	Uninterruptible Power Supply. Varavirtalähde sähkökatkosten varalle. Tasaa myös sähköverkon jännitepiikkejä.
Validation	Soveltuvuus, tässä soveltuvuus vikasietoiseen klusterointikonfiguraatioon.
WAN	Wide Area Network. Maantieteellisesti laajan alueen tiedonsiirtoverkko.

1 JOHDANTO

Tietojärjestelmien toimintavarmuus on edellytys nyky-yhteiskunnan palveluille. Toiminnaltaan varmojen ja vikatilanteessa toimintakykynsä säilyttävien palvelujen tarjoaminen asettaa organisaatiolle omat vaatimuksensa niin taloudellisesti kuin teknisen osaamisen ja sen toimintaa ohjaavien päätöstenkin osalta.

Opinnäytetyöni selventää mitä toiminnaltaan varma ja vikasietoinen tietojärjestelmä käytännössä tarkoittaa, mitä se niin laitteisto- kuin ohjelmistotasolla edellyttää ja kuinka kohdeorganisaation muut ratkaisut vaikuttavat sen tietojärjestelmien käyttöön.

Opinnäytetyöni jakautuu käytännössä kolmeen eri osioon. Ensimmäinen osio keskittyy teoriatasolla tietojärjestelmien luotettavuuden merkityksen ja mahdollisimman korkean luotettavuuden saavuttamiseksi tarvittavien menetelmien kuvaamisesta. Osio kuvaa ne kohteet, joita kokonaistoimintavarmuutta parannettaessa on järkevä tarkastella ja joihin resursseja on syytä kohdentaa sekä yleisimmät käytettävissä olevat tekniset ratkaisut, joilla järjestelmän kriittisten laitteiden toimintavarmuutta ja palvelujen käytettävyyttä voidaan parantaa.

Toinen osio alaotsikoineen kuvaa käytännön tasolla, mitä toimintoja ja ominaisuuksia suositun Windows-tuoteperheen uusin palvelinkäyttöjärjestelmä Windows Server 2008 tarjoaa tietojärjestelmän palvelujen korkean luotettavuustason ja vikasietoisuuden saavuttamiseksi. Kuvaan ko. ohjelmiston toimintojen asennus- ja konfigurointivaiheiden seikkoja omassa testiympäristössäni tehtyihin havaintoihin perustuen. Osio on kirjoitettu käyttöohjemaisella otteella osittain siitä syystä, että käyttämäni lähdemateriaali ja käsiteltävän asian luonne siihen ohjaavat.

Kolmannessa osiossa esitetään loppupäätelmät ja työn tekemiseen vaikuttaneita seikkoja sekä muita huomioita koko opinnäytetyöprosessista.

Työn lukijalta edellytetään osaamista palvelinten ja palvelinohjelmistojen toiminnoista sekä tuntemusta IT-alan termeistä.

2 TIETOJÄRJESTELMIEN TOIMINTAVARMUUDEN JA VIKASIETOISUUDEN MERKITYS

2.1 Yleistä

Tietojärjestelmien toimivuus ja niiden tarjoamien resurssien saatavuus ovat ehdoton edellytys nykypäivän tietoyhteiskunnassa niin valtion ja kuntien, yritysten kuin yksityishenkilöidenkin tarpeita ajatellen. Terveydenhuolto, koulutuspalvelut, kuntien ja valtion rekisterit, päivittäistavara- ja verkkokauppa ja lähestulkoon jokainen kuviteltavissa oleva elinympäristöömme kuuluva palvelu vaatii toimiakseen toiminnaltaan varmaa ja luotettavaa tietojärjestelmää.

Tietojärjestelmän luotettavuuden ja toimintavarmuuden parantamiseksi järjestelmän ylläpitäjällä on käytettävissään laaja kirjo toimenpiteitä niin järjestelmän suunnittelu-, rakennus- kuin käyttövaiheessakin. Alkaen järjestelmän keskeisimpien palvelinten peilauksesta sekä niiden komponenteista, toimintavarmuuden kannalta tarkasteltavia kohteita ovat lisäksi niin organisaation tietoturvapolitiikka, kulunvalvonta kuin itse palvelinkäyttöjärjestelmätkin.

Nykyaikaiset palvelinohjelmistot tarjoavat yhdessä teknisten ratkaisujen kanssa monipuoliset työkalut, jotka mahdollistavat organisaation tietojärjestelmien palvelujen mahdollisimman korkean käyttöasteen ja ylläpitotoimien aiheuttamien palvelukatkosten vähentämisen minimiin. Lisäksi yllättävien laiterikkojen tai muiden ongelmien aiheuttamien suoranaisten toimintahäiriöiden vaikutusten pienentämiseksi palvelinohjelmistot voidaan määrittää vikasietoisiin tilanteisiin automaattisesti reagoiviksi, jolloin edes palvelimen toiminnan täydellinen häiriintyminen ei estä tietyn palvelun käyttöä tietojärjestelmässä.

Tietojärjestelmät ovat kuitenkin hyvin laajoja. Jaakohuhta (2003) toteaa, että tietojärjestelmien luotettavuus on käsitteenä hyvin laaja ja sitä on sen vuoksi tarkasteltava osa-alueittain pienemmissä osissa ja eri näkökulmista. Lisäksi hän kuitenkin muistuttaa, että pelkästään yhteen tiettyyn seikkaan keskittyminen voi vääristää kokonaisuuden ja sen sijaan tärkeintä onkin kokonaisuuden hahmottaminen.

Erikseen tarkasteltavia seikkoja Jaakohuhdan mukaan ovat tietojärjestelmän tietokoneet, verkot, ohjelmistot, käytettävät mediat, järjestelmän dokumentaatio, ympäristö, järjestelmän data sekä ihmiset, jotka tietojärjestelmää käyttävät, rakentavat ja ylläpitävät. Näiden lisäksi on huomioitava myös sopimukset, lainsäädäntö, takuuasiat, vakuutukset sekä organisaation oma toiminta-ajatus. (Jaakohuhta 2003.)

2.2 Käsitteitä

Tietojärjestelmiä on syytä tarkastella osissa niiden laajuuden ja monimutkaisuuden vuoksi. Lisäksi niitä kuvailtaessa eri käsitteet auttavat ymmärtämään laajaa kokonaisuutta. Jaakohuhdan (2003) mukaan tällaisia käsitteitä ovat:

Luotettavuus ja toimintavarmuus kuvaavat kohteen kykyä suorittaa vaaditut toiminnat määritetyissä olosuhteissa määritettynä ajanjaksona.

Käyttövarmuus on usein peruste sille, miksi tiettyä järjestelmää käytetään ja siihen turvaudutaan. Se on laaja käsite, jolla tarkoitetaan usein myös muita luotettavuustekijöitä **luotettavuus**, **palvelevuus**, **ylläpitovarmuus**, **turvallisuus** ja **testattavuus.**

Palvelevuus ja **saatavuus** kuvaavat järjestelmän ja sen osien kykyä tarjota siltä vaadittuja palveluja mahdollisimman vähäisin keskeytyksin ja häiriöin halutulla ajanhetkenä.

Käytettävyys kuvaa tietyn käyttäjäryhmän kykyä käyttää tuotetta (tässä tietojärjestelmää) tehokkaasta, tuottavasti ja miellyttävästi määriteltyjen tavoitteiden täyttämiseksi tietyssä käyttöympäristössä. Tietojärjestelmien kohdalla hyvä käytettävyys kuvaa erityisesti ohjelmistojen käyttöliittymien selkeyttä ja helppokäyttöisyyttä, toimintojen loogisuutta sekä ergonomiaa.

Tietoturvallisuus tarkoittaa toimia, joilla pyritään turvaamaan tietojen **luottamuksellisuutta**, **eheyttä** ja **saatavuutta** niin laitteisto- kuin ohjelmistovikojen, luonnontapahtumien kuin tapaturmienkin uhilta ja niiden aiheuttamilta vahingoilta.

Lisäksi Hakala ym. (2006) laajentaa tietoturvallisuuden määritelmää käsitteillä **kiistämättömyys** ja **pääsynvalvonta**. Näistä ensin mainitulla tarkoitetaan tietojärjestelmän kykyä tunnistaa ja tallentaa järjestelmää käyttävän henkilön tiedot luotettavasti. Siihen pyritään pääasiassa kahdesta syystä. Yhtäältä halusta varmistaa tiedon alkuperä ja toisaalta halusta ja tarpeesta todistaa tietojen luvaton käyttö sellaisessa tilanteessa, jossa joudutaan harkitsemaan oikeudellisia toimia järjestelmän käyttäjää vastaan. Käsitteistä jälkimmäisellä tarkoitetaan yhteisesti niitä menetelmiä, joilla voidaan rajoittaa tietojärjestelmän käyttöä kokonaan ulkopuolisilta tai tarvittaessa oman organisaation sisällä omiin tarkoituksiinsa. Pääsynvalvonta pyrkii täten minimoimaan luvattoman käytön aiheuttamia ongelmia kuten tarpeetonta verkon ja laitteistojen kuormitusta sekä haittaohjelmien leviämistä. (Hakala ym. 2006.)

2.3 Luotettavuuden merkitys

Kuten edellä on ilmennyt, tietojärjestelmien luotettavuus ja toimivuus ovat edellytyksiä yhteiskunnan eri palveluiden toiminnalle. Käyttövarmuus on perusteena tietyn järjestelmän käytölle ja sen ongelmat heijastuvat laajalle alueelle. Järjestelmän luotettavuutta arvioitaessa puhutaan yleisesti esimerkiksi viiden yhdeksikön (*Five Nines*) luotettavuustasosta (ks. mm. Continuity Central 2009). Tämä tarkoittaa 99,999 prosentin luvattua käyttöastetta ja vuositasolla ainoastaan vähän yli viiden minuutin käyttökatkosta, mikäli tietojärjestelmän oletetaan toimivan ympäri vuorokauden vuoden jokaisena päivänä. Yleisesti ottaen järjestelmää voidaan sanoa luotettavaksi vasta kun sen luotettavuus on viiden yhdeksikön tasolla, sillä alle sen olevien järjestelmien tai sen osien ei katsota olevan soveltuvia korkeaa luotettavuutta vaativien operaatioiden suorittamiseen juuri pitkien käyttökatkosten vuoksi.

Pelkästään prosenttilukuina tarkasteltuna asiakkaalle luvattu saatavuusaste saattaa siis antaa väärän kuvan palvelun varmuudesta ja luvatun toiminta-ajan ulkopuolelle jäävä osuus voi osoittautua yllättävän pitkäksi, ks. kuva 1.

Myös Jaakohuhta (2003) esittää, että prosenttilukuina tarkasteluna 99,95 % varmuudella toimiva palvelu on vuodessa yli 4 tunnin ajan pois käytöstä, mikäli laskentaperusteena käytetään vuoden jokaisen päivän jokaista tuntia. Katkos on pitkä,

mikäli se on suunnittelematon ja ajoittuu liiketoiminnan kannalta kiireiseen aikaan. (Jaakohuhta 2003.)

Jaakohuhta (2003) toteaa myös, että tietojärjestelmäongelmista aiheutunut keskeytys vaikuttaa kaikkialle yrityksen liiketoimintaan ja sen syitä on tarkasteltava koko liiketoiminnan kannalta yksittäisen toiminnon sijaan. Yrityksen liiketoiminnan kannalta hyvin arvokas tieto muuttuu arvottomaksi, mikäli se ei ole tarvittaessa käytettävissä. Usein käyttökatkoksen syynä on jokin muu kuin ylläpito- tai huoltotoimien vaatima suunniteltu palveluiden alasajo. (Jaakohuhta 2003.)

Organisaatiosta ja sen koosta riippuen hyväksyttävän käyttökatkoksen pituus voi vaihdella suuresti. Yritysmaailmassa pienyritykset eivät välttämättä menetä toimintakykyään edes tuntien käyttökatkoksen aikana kun taas ympärivuorokautista ja -vuotista liiketoimintaa harjoittaville yrityksille, kuten verkkokauppa- tai pankkipalveluja tuottaville organisaatioille, jo minuuttien käyttökatkoksella on todella suuri merkitys sen toimintakykyyn ja ennen kaikkea sen asiakkaille.

Käyttökatkosten pituutta ja sitä kautta niiden vaikutusta organisaation toimintaan pyritään minimoimaan. Kuva 1 kuvaa tietojärjestelmän käyttökatkoksen (*downtime*) pituutta kun laskenta perustuu 24 tuntiin vuorokaudessa vuoden jokaisena päivänä.

Availability (%)	Downtime in a Year (24×7×365) for 24-Hour Operation
99.9999	32 seconds
99.999	5 minutes, 15 seconds
99.99%	52 minutes, 36 seconds
99.95%	4 hours, 23 minutes
99.9%	8 hours, 46 minutes
99.5%	1 day, 19 hours, 48 minutes
99%	3 days, 15 hours, 40 minutes
95%	18.25 days
90%	36.5 days

Kuva 1 Palvelun saatavuustaso ja käyttökatkoksen pituus vuodessa (Shapiro & Polich 2004).

Merkittäväksi edellä kuvatut prosenttiluvut tulevat silloin, kun yritys tai muu taho lupaa asiakkaalleen tietyn palvelutason, esimerkiksi edellä mainitun viiden yhdeksikön luotettavuustason niin sanotussa SLA-sopimuksessa. Sopimuksessa

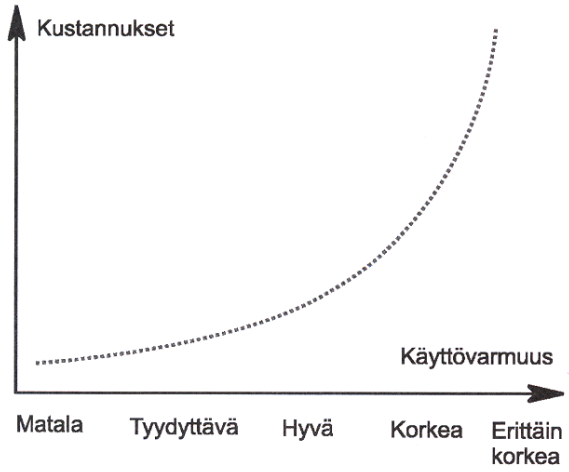
luvatun palvelutason ylläpitäminen on ehdottoman kriittinen esimerkiksi verkkokaupoille ja muille sähköiseen kaupankäyntiin erikoistuneille tahoille. Sovitusta palvelutasosta poikkeaminen voi johtaa korvausvaatimuksiin.

Esimerkiksi verkkokaupastaan paremmin tunnettu Amazon tarjoaa myös palvelinkapasiteettia it-palvelunsa ulkoistaneille asiakkailleen ja se lupaa SLA-sopimuksessa vuositasolla 99,95 prosentin saatavuustason esimerkiksi www-palvelimelle. Mikäli tätä tasoa ei saavuteta, lupaa Amazon asiakkaalleen rahallisen hyvityksen. (Amazon EC2 2009.)

2.4 Toimintavarmuuden parantamiseen käytettävien resurssien kohdistaminen

Luvussa 2.3 kuvatut prosentuaaliset toimintavarmuusasteet kuvaavat realistisia varmuusodotuksia tietojärjestelmiä ja niiden luotettavuutta kohtaan. Vaadittuun käyttövarmuustasoon vaikuttaa muun muassa organisaation koko ja sen toiminnan luonne. Täysin sataprosenttista toimintavarmuutta ei ole järkevää tavoitella sen vaatimien teknisten järjestelmien ja niiden kustannusten vuoksi. Lisäksi Shapiro ym. muistuttaa, että toiminnaltaan sataprosenttisen varmaa järjestelmää ei ole olemassakaan (Shapiro & Polich 2004).

Toiminta- ja käyttövarmuuden kasvattaminen kasvattaa Jaakohuhdan (2003) mukaan siihen liittyviä kustannuksia eksponentiaalisesti, ks. kuva 2. Käyttövarmuusasteen nostaminen korkeasta erittäin korkeaksi vaatii isoja rahallisia panoksia.



Kuva 2 Käyttövarmuuden kasvattaminen kasvattaa kustannuksia eksponentiaalisesti (Jaakohuhta 2003).

Lisäksi Jaakohuhta (2003) muistuttaa, että kaikkien toimintavarmuuden parantamiseen käytettyjen rahallisten ja henkilöstöresurssien tulee olla suhteessa arvioituun riskiin. Käytännössä tämä tarkoittaa sitä, että jokaisessa organisaatiossa tulee arvioida sen toimintaan liittyvät riskit ja niiden aiheuttamien vaikutusten suuruus sen toimintaan ja tietojärjestelmien luotettavuuteen ja verrata niitä vaadittuun palvelujen saatavuustasoon. Siinä missä yhdelle organisaatiolle riittää, että tietojärjestelmän palvelut ovat käytössä ”vain” 99,9 % toiminta-ajastaan ja sen ulkopuolelle jäävä käyttökatkos (8 h 46 min vuodessa, kun laskentaperusteena 24/7/365) on täysin hyväksyttävissä, sallii toinen taho korkeintaan joidenkin minuuttien mittaisen käyttökatkon omassa toiminnassaan vuoden aikana. Tällöin on selvää, että jälkimmäisenä mainitun tahon rahalliset ja henkilöstöresursseja vaativat panostukset tietojärjestelmiensä luotettavuuteen ovat aivan eri tasolla kuin pidemmän käyttökatkon hyväksyvällä organisaatiolla.

Toimintavarmuutta parannettaessa onkin edellä kuvatuista syistä johtuen keskityttävä järjestelmän kannalta kaikkien oleellisimpiin kohteisiin, joiden toiminnan turvaamiseen käytössä olevia resursseja kohdistetaan. Pelkästään yksittäisten työasemien luotettavuuteen keskittyminen ei ole taloudellisesti tai edes teknisessä mielessä järkevää järjestelmän luotettavuutta kokonaisuutena ajatellen vaan sen sijaan tulee keskittyä palvelinten ja verkon keskeisimpien aktiivilaitteiden vikasietoisuuden ja toimintavarmuuden tarkasteluun ja niiden riskien tunnistamiseen ja niistä aiheutuvien vaikutusten minimoimiseen. Luvussa 3 esitetään mihin tietojärjestelmän osa-alueisiin organisaation resursseja on mielekästä toimintavarmuuden parantamistarkoituksessa kohdentaa.

3 YLEISIMMÄT MENETELMÄT

Tietojärjestelmän palvelujen toimintavarmuuden ja vikasietoisuuden parantamiseksi on olemassa niin teknisiä kuin inhimillisiä ratkaisuja, joilla pyritään turvaamaan palveluiden mahdollisimman korkea käytettävyys- ja saatavuusaste. Palvelinten tekniikka on jo lähtökohdiltaan luotettavaa ja sitä voidaan entisestään parantaa teknisten ratkaisujen avulla. Organisaatio tarvitsee kuitenkin aina niiden lisäksi johtotasolla tehtyjä toimintaa ohjaavia päätöksiä turvallisuus- ja tietoturvapolitiikkaan liittyen.

3.1 Palvelinten peilaus

Palvelinten peilaus *(server mirroring*) kahdentaa reaaliajassa koko palvelimen ja sen toiminnot toiselle palvelimelle, joka voi fyysisesti sijaita kokonaan eri tilassa. Erillään pitämisen perusteena on tulipalojen tai muiden suurien ympäristön uhkien aiheuttamien riskien minimointi. Peilattavien palvelinten välillä on oltava nopea tiedonsiirtoverkko (1 Gb/s tai nopeampi), jonka välityksellä peilausliikenne välitetään. Palvelimen vikaantuessa toinen täysin identtinen peilauspalvelin jatkaa tietojärjestelmän palvelujen tarjoamista lähes reaaliajassa, jolloin viasta aiheutuneen käyttökatkoksen pituus jää hyvin lyhyeksi.

3.2 Vikasietoiset komponentit

Palvelinkoneet eroavat merkittävästi perustyöasemasta komponenttiensa osalta. Palvelinten toimintavarmuuden odotetaan olevan korkea, joten palvelimissa käytetyt komponentit ovat jo lähtökohdiltaan luotettavuuden osalta varmoja. Sen lisäksi eri komponenttien vikasietoisuutta voidaan parantaa teknisin ratkaisuin. Toimintavarmuuden parantamisen pääajatuksena on vähentää riippuvuutta yksittäisen laitteen tai muun kohteen toiminnasta. Usein käytetty termi *Single Point of Failure* (ks. esim. TechNet NLBa 2009) kuvaa tällaista kriittistä kohdetta järjestelmässä ja niiden lukumäärän vähentäminen on tehokas tapa kasvattaa järjestelmän kokonaisluotettavuutta ja toimintavarmuutta.

3.2.1 Kiintolevyt

Palvelimen tärkeimpiin yksittäisiin komponentteihin lukeutuvat kiintolevyt ovat kulutustavaraa niiden sisältämien lukuisten liikkuvien osien ja suuren käyttöasteen vuoksi. Niiden sisältämät tiedot ovat kuitenkin elintärkeitä niin itse palvelinkäyttöjärjestelmän kuin organisaation toiminnan kannalta. Yksittäinen kiintolevy onkin luotettavuuden kannalta niin epävarma, että vikasietoinen järjestelmä käyttää useita levyjä massamuistinaan. Levyt ovat RAID-konfiguroituja siten, että yhtenä loogisena kokonaisuutena näkyvä usean levyn järjestelmä kirjoittaa datan usealle levylle yhden sijaan. Tällöin yhden tai välttämättä edes useamman levyn yhtäaikainen rikkoutuminen ei vaikuta heikentävästi järjestelmän toimintavarmuuteen. RAID on mahdollista toteuttaa joko ohjelmistotasolla tai erillisellä fyysisellä RAID-ohjaimella. Luotettavuuden kannalta erillinen ohjain on luonnollisesti toimintavarmempi, mutta sen toiminnan häiriintyessä koko RAID-järjestelmän toiminta häiriintyy. Ideaalitilanteessa koko RAID-järjestelmä onkin kahdennettu.

3.2.2 Muisti

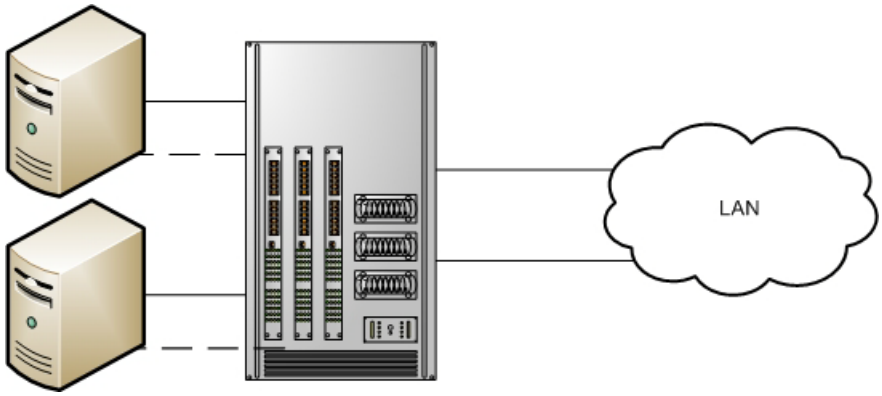
Palvelimen muistilla on suuri merkitys sen toimintaan. Toimintakyvyn kannalta oleellista on muistin määrän lisäksi sen toimivuus. Palvelimissa käytetään muistivirheen korjaavaa muistia. Hakalan ym. (2006) mukaan ns. EEC-muisti tarkistaa muistiin tallennetun tiedon eheyden ja osaa korjata pienimmät yhden bitin virheet. Tämä vähentää muistivirheistä johtuvia häiriöitä palvelimen toiminnassa.

3.2.3 Virtalähteet

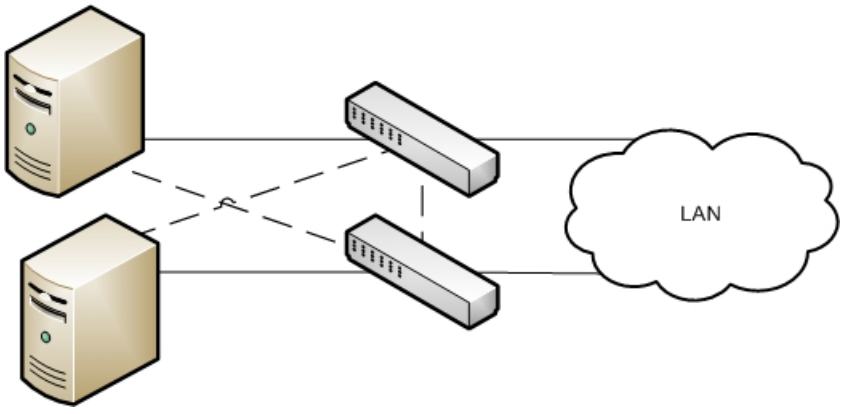
Palvelimen virrantarve on suuri ja vikasietoisessa palvelimessa on useita virtalähteitä. Usealla virtalähteellä saavutettu kuormantasaus vähentää virtalähteen hajoamisen riskiä ja yhden hajottua muut hoitavat edelleen virran jakamista palvelimelle ja sen komponenteille. Täydellisen sähkökatkoksen varalle järjestelmä vaatii kuitenkin toimiakseen lisäksi varavirta- eli UPS-järjestelmän, joka tarjoaa virtaa katkoksen ajan akkujensa avulla. Lisäksi UPS suojaa palvelimia lyhyiltä jännitteen vaihteluilta ja jännitepiikeiltä.

3.3 Vikasietoiset verkot

Työasemat, palvelimet ja muut verkkoresurssit yhdistävän lähiverkon palveluiden hajauttamisella saavutetaan parantunut vikasietoisuus, kun keskeisimpien palvelinten ja aktiivilaitteiden väliset yhteydet on toteutettu siten, että käytettävissä on aina varsinaisen yhteyden varmistava varayhteys, joka vikatilanteessa otetaan automaattisesti käyttöön. Verkkoyhteyksien kahdennus voidaan toteuttaa joko yhden vikasietoisen, tässä luvussa jäljempänä esiteltyjä ominaisuuksia tukevan aktiivilaitteen (kuva 3) tai kahden erillisen aktiivilaitteen avulla (kuva 4).

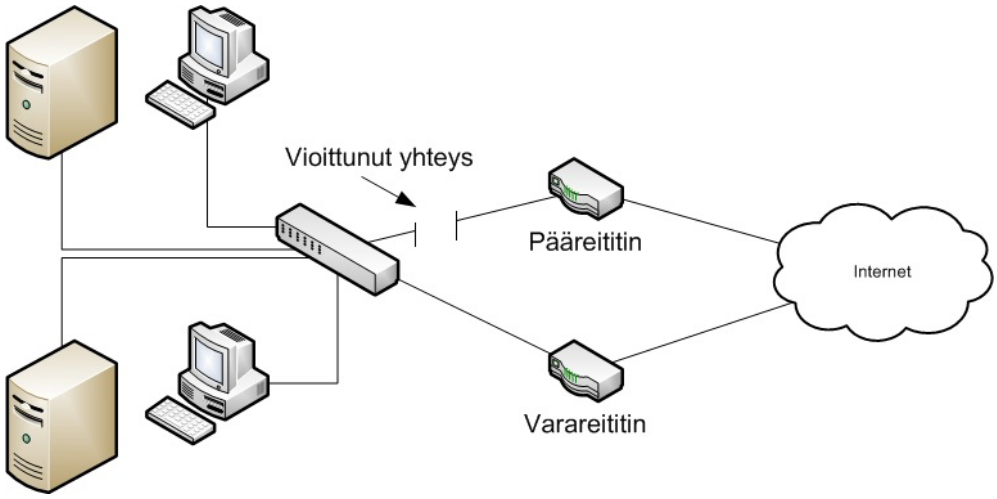


Kuva 3 LAN-verkko modulaarisella kytkimellä (mukailtu Jaakohuhta 2003).



Kuva 4 LAN-verkko kahdella kytkimellä (mukailtu Jaakohuhta 2003).

Yhteydet lähiverkosta ulospäin WAN-verkkoon tai Internetiin toteutetaan mahdollisuuksien mukaan kahden tai useamman reitittimen kautta, ks. kuva 5. Reitittimet lähettävät toisilleen signaaleja, joiden perusteella kunkin laitteen oletetaan toimivan häiriöttä. Mikäli ko. signaali häviää vikaantumisen seurauksena, ohjataan verkkoliikenne pääreitittimeltä varareitittimelle ja siitä edelleen Internetiin.



Kuva 5 Vikasietoinen WAN-verkko (Jaakohuhta 2003).

Verkkojen toiminnaltaan varmoilla aktiivilaitteilla kuten reitittimillä ja kytkimillä on keskeinen rooli vikasietoisessa verkossa. Verkon keskeisimpien laitteiden vikasietoisuuden parantamiseksi aktiivilaitteiden on Jaakohuhdan (2003) mukaan tuettava seuraavia ominaisuuksia:

- kaksi tai useampia virtalähteitä ja virransyötön varmistus UPS-laitteistolla
- kaksi tai useampia tuulettimia
- osien vaihtomahdollisuus laitteen toimiessa (*hot pluggable* ja *hot swap*)
- varaliitäntäkortit
- kahdennetut kytkinmatriisit
- hallittu alasajo-ominaisuus lämpötilan noustessa
- lämpötilaltaan sopiva, pölytön ja lukittava asennuspaikka
- säännöllinen huoltosuunnitelma

3.4 Varmuuskopiointiratkaisut

Yleisesti ottaen tietojärjestelmän tiedostot varmistetaan aina, kun niiden mahdollinen katoaminen tai vioittuminen voi aiheuttaa taloudellisia tai muita menetyksiä. Tiedostojen varmuuskopiointiratkaisuja on lukuisia. Kannettavat mediat muistitikuista DVD-levyihin soveltuvat yksittäisen käyttäjän tarpeisiin, mutta varmuuskopioitavan tiedostomassan kasvaessa tilantarve ja sitä kautta varmuuskopiointijärjestelmälle asetetut vaatimukset kasvavat jatkuvasti suuremmaksi. Suurimmillaan organisaatioiden tilantarve on nykypäivänä teratavujen luokkaa ja se kasvaa jatkuvasti. Nauhavarmistus puoltaa edelleen paikkansa varmuuskopiointimediana edullisen hintansa vuoksi vaikkakin kiintolevyt kasvattavat suosiotaan yhä enenevässä määrin. SAN-verkot mahdollistavat keskitetyt varmuuskopiointiratkaisut suurissa organisaatiossa ja online-varmuuskopiointipalveluja tarjoavat yritykset mahdollistavat varmuuskopiointipalvelun ulkoistamisen.

3.5 Inhimilliset ratkaisut

Käytössä olevien vikasietoisten laitteiden ja toiminnoiltaan varmatoimisten palvelinkäyttöjärjestelmien lisäksi tietojärjestelmien toimivuus edellyttää myös muita kuin teknisiä keinoja, joilla palvelujen toimintaa organisaation tietojärjestelmän osana tehostetaan entisestään.

3.5.1 Tietoturvapolitiikka ja -suunnitelma

Osana toimivaa tietojärjestelmää on aina organisaation tietoturvapolitiikka. Se sisältää koko organisaatiota koskevat ohjeet, vaatimukset ja käytänteet liittyen tietojärjestelmän ja sen osien käyttöön.

Tietoturvapolitiikka on osa koko organisaation turvallisuuspolitiikkaa ja se muodostuu organisaation johdon hyväksymistä käytänteistä. Se kuvaa yleisellä tasolla organisaatiossa vaadittavaa tiedon turvaamisastetta, millä menetelmillä haluttu turvataso saavutetaan sekä miten tietoturvallisuutta hallinnoidaan ja kehitetään. Tietoturvapolitiikka ohjaa lisäksi tietojärjestelmien suunnittelijoiden ja esimiesten toimintaa ja se laaditaan yleensä keskipitkälle (5 vuotta) ja pitkälle (10 vuotta) aikavälille. (Hakala ym. 2006.)

Tietoturvasuunnitelma muotoutuu tietoturvapolitiikassa määriteltyjen linjausten ja reunaehtojen mukaiseksi ja sen avulla pyritään tietoturvapolitiikassa määritettyyn tietoturvallisuuden tasoon. Siinä dokumentoidaan konkreettisesti ja yksityiskohtaisesti kunkin tietojärjestelmän käyttöön liittyvät työmenetelmät ja tekniset ratkaisut. Tietoturvasuunnitelma laaditaan yleensä keskipitkälle aikavälille (2-5 vuotta), mutta sitä on syytä tarkentaa vuosittain tai kun tietojärjestelmissä tapahtuu muutoksia. (Hakala ym. 2006.)

3.5.2 Varmuuskopiointisuunnitelma

Tietojärjestelmiin on tallennettu liike- tai muun toiminnan kannalta hyvin tärkeätä tietoa. Tietojen turvaaminen varmuuskopioimalla on ehdottomasti tärkeimpiä yksittäisiä toimenpiteitä tietojärjestelmän palvelujen toimintavarmuuden ylläpitämisen kannalta. Yksittäisten tiedostojen lisäksi kaikki muukin data ohjelmistoasetuksista kokonaisiin käyttöjärjestelmiin on varmuuskopioitavissa.

Varmuuskopioiden säilyttäminen vaatii tallennuskapasiteettia, joten varmuuskopiointityyppi on mietittävä varmennettavan kohteen mukaan. Harvoin muuttuvia tiedostoja, kuten käyttöjärjestelmän asennustiedostoja ei ole mielekästä kopioida joka päivä ja toisaalta kriittisistä tiedostoista harvemmin kuin kerran päivässä otettu varmuuskopio voi olla liian vanha. Tämän lisäksi varmuuskopiointiajankohta on valittava kulloinkin kyseessä olevan organisaation vaatimusten mukaisesti siten, että tärkeimmistä tiedostoista on mahdollisimman tuore varmuuskopio, mutta varmuuskopiointi haittaa esimerkiksi lähiverkkoliikennettä mahdollisimman vähän.

Varmuuskopiointisuunnitelmassa edellä mainittujen seikkojen lisäksi otetaan kantaa myös siihen, millaiselle tallennusmedialle varmuuskopiot tallennetaan ja miten niiden kierto toteutetaan, kuka varmuuskopioinnista vastaa ja kuinka tiedot palautetaan tarpeen tullessa.

3.5.3 Kulunvalvonta

Osana organisaation turvallisuuspolitiikkaa kulunvalvonta turvaa tietojärjestelmien toimintaa estämällä asiattomien liikkumisen palvelintiloissa tai niiden lähistöllä. Ainoastaan palvelinten ja verkkojen aktiivilaitteiden huollon ja ylläpidon kanssa tekemisissä olevilla tulee olla pääsy konesalin kaltaisiin tiloihin. Jokaisella järjestelmänvalvojalla ei ole tarvetta päästä fyysisesti samaan tilaan palvelinten kanssa.

3.6 Palvelinohjelmistojen toiminnot

Palvelinten toimintavarmuudesta puhuttaessa vikasietoisten komponenttien tarjoama toimintavarmuus on ainoastaan yksi osa varmatoimista palvelinympäristöä. Palvelimen varmatoiminen käyttöjärjestelmä on vankka pohja tietojärjestelmän palveluille ja sitä kautta organisaation toiminnalle. Luotettavuus palvelinohjelmistoissa on itsestäänselvyys, josta ei tingitä. Palvelinohjelmistojen tarjoamilla ominaisuuksilla palvelujen kokonaistoimintavarmuutta voidaan parantaa entisestään.

3.6.1 Yleisimmät palvelinohjelmistot

Yleisimmät yritysmaailmassa käytössä olevat palvelinkäyttöjärjestelmät ovat Microsoft Windows Server-tuoteperheen sekä Linux-jakeluiden eri versiot kuten Red Hat Enterprise Linux, SuSE Linux Enterprise ja Debian. Lisäksi erilaisia Unix-pohjaisia käyttöjärjestelmiä käytetään muun muassa pankkien ja muissa äärimmäistä luotettavuutta vaativissa suurissa palvelimissa ja palvelinsaleissa.

Muita palvelimissa käytettyjä käyttöjärjestelmiä ovat muun muassa Mac OS X Server, Novell Open Enterprise Server ja Sun Solaris.

3.6.2 Palvelinohjelmistojen yleisimmät toimintavarmuutta parantavat toiminnot

Puhtaasti laitteistotason verkko- ja palvelinteknisten ratkaisujen lisäksi osana palvelimen toimintaa niiden käyttöjärjestelmät tarjoavat joukon erilaisia toimintoja ja työkaluja tietojärjestelmän kokonaistoimintavarmuuden ja palvelujen saatavuuden parantamiseksi.

3.6.2.1 Palveluiden hajauttaminen ja replikointi

Palveluiden hajauttamisella useiden palvelinten suoritettavaksi saavutetaan monia etuja. Tietoturvallisuuden ja toimintavarmuuden vuoksi tietojärjestelmässä on täysin perusteltua olla omat palvelimensa esimerkiksi toimialueen ohjauskoneille (*Domain Controller*), www- ja tiedostopalvelimille. Organisaation tietoverkko voi olla maantieteellisestikin niin laajalle levittäytynyt, että pitkien vasteaikojen ja hitaampien WAN-yhteyksien vuoksi tiettyjen palvelujen hajauttaminen ja erillään olevien palvelinten välinen tehokas tiedonvälitys tehostavat suorituskykyä, toimintavarmuutta ja siten niiden tarjoaminen palvelujen saatavuutta.

Tietojärjestelmän palvelut kuten sähköposti, tulostus, tiedostojärjestelmän palvelut, tietokannat, hakemisto- ja kirjautumispalvelut, multimedia ja suurta laskentatehoa vaativat operaatiot ovat hajautettavissa useiden palvelinten suoritettavaksi (Crichlow 2001).

Luku 5.5 kuvaa, miten hajautettu tiedostojärjestelmä (DFS) ja siihen liittyvä replikointi rakentuu Windows Server 2008-palvelinympäristössä.

3.6.2.2 Klusterointi

Klusterointi eli ryvästys on toimintavarmuutta ja vikasietoisuutta parannettaessa tyypillinen ratkaisu. Klusteri koostuu kahdesta tai useammasta jäsenkoneesta, jotka jatkuvasti tarkkailevat toistensa toimintaa. Määrättyä palvelua suorittaa kulloinkin yksi palvelin kerrallaan. Virhetilanteesta aiheutunut häiriö tunnistetaan ja sen palvelut siirretään klusterissa toisen jäsenen suoritettavaksi.

Luku 5.2 kuvaa klusteroinnin ominaisuuksia tarkemmin Windows Server 2008-ympäristössä.

3.6.2.3 Verkkoliikenteen tasaus

Lisääntynyt kuormitus saattaa aiheuttaa häiriöitä esimerkiksi verkkosivuston käytettävyydessä tai muissa verkon palveluissa. Www-palvelimiin kohdistunutta kuormitusta voidaan tasoittaa lisäämällä verkkosivustoa samanaikaisesti tarjoavien palvelinten määrää ja jakamalla sivuston sivupyynnöt näiden palvelinten kesken.

Luku 5.3 kuvaa verkkokuormituksen tasaamisominaisuuksia Windows Server 2008-ympäristössä.

3.6.2.4 Varmuuskopiointi ja tietojen palautus

Varmuuskopiointi ja tietojen palautus mahdollistavat tiedostojen ja jopa täydellisten tietokoneiden saatavuuden ja nopean palautettavuuden laiterikkojen tai inhimillisten erehdysten aiheuttamien häiriöiden aiheuttamissa häiriötilanteissa.

Luvussa 5.4 kuvataan Windows Server 2008:n varmuuskopiointiominaisuuksia.

3.6.2.5 Virtualisointi

Virtualisoinnilla tarkoitetaan useamman käyttöjärjestelmän ajamista yhdessä fyysisessä tietokoneessa samanaikaisesti. Jokainen käyttöjärjestelmä toimii itsenäisesti muista riippumatta ja omien määritystensä mukaisesti. Tällä voidaan tehostaa palvelinkoneiden käyttöastetta ja siten kustannus- ja energiatehokkuutta. Lisäksi virtualisointi mahdollistaa joustavasti uusien palvelujen käyttöönottamisen osaksi jo olemassa olevaa tietojärjestelmää.

Toimintavarmuuden kannalta tarkasteltuna virtuaalikoneet ja virtualisointi mahdollistavat tietyn palvelun tai sovelluksen suorittamisen virtuaalikoneessa, jolloin siihen kohdistuvat päivitys- ja huoltotoimenpiteet vaikuttavat ainoastaan yhteen virtuaalikoneeseen. Myös mahdollisuus virtualisoidun palvelun siirtämiseen fyysiseltä palvelimelta toiselle huoltotöiden ajaksi vähentää palvelun käyttökatkosten pituutta ja täten parantaa sen palvelevuutta. Palvelinohjelmistoista muun muassa Windows Server, FreeBSD (Unix), Mac OS X Server, Sun Solaris, Red Hat Enterprise Linux ja SuSE Linux Enterprise sisältävät uusimmissa versioissaan tuen virtualisoinnille.

4 TESTAUSYMPÄRISTÖN KUVAUS

Opinnäytetyössäni esiteltyjen toimintojen asennus- ja testaustoimien ympäristönä toimi Windows Server 2008 Enterprise. Testiympäristö koostuu yhdestä fyysisestä palvelimesta *PEONTS1H* ja siinä omina virtuaalikoneinaan toimivista virtuaalisista palvelimista *PEONTS2V* ja *PEONTS3V*. Jokainen kolmesta palvelimesta käyttää samaa käyttöjärjestelmäversiota.

Palvelimet ovat samassa toimialueessa *ont.local*. Toimialueen ohjauskoneena toimii *PEONTS1H* ja muut kaksi ovat toimialueessa jäsenkoneina. Palvelimet keskustelevat virtuaalisen lähiverkon välityksellä. Palvelimet on eristetty muista verkoista eikä niillä ole pääsyä Internetiin.

Palvelinten IP-osoitteet on määritetty manuaalisesti ilman DHCP-palvelinta. Lisäksi virtuaalipalvelimille *PEONTS2V* ja *PEONTS3V* on määritetty kaksi verkkokorttia, joista toinen on normaalia lähiverkko- ja toinen verkkoliikenteen kuormantasausliikennöintiä varten, koska NLB tarvitsee toimiakseen oman erillisen lähiverkkonsa.

Palvelimiin asennetut palvelinroolit ja ominaisuudet jakautuvat seuraavasti:

PEONTS1H	*PEONTS2V*	*PEONTS3V*
Domain Controller	IIS 7	IIS 7
Network Load	Network Load	Network Load
Balancing	Balancing	Balancing
DNS	Windows Server	Windows Server
DFS	Backup	Backup
Windows Server		DFS
Backup		
Hyper-V		

Opinnäytetyön testausympäristön rakennekuva on esitetty liitteessä 1.

5 MICROSOFT WINDOWS SERVER 2008

Tämä kappale keskittyy kokonaisuudessaan palvelinkäyttöjärjestelminä yleisten Windows-ohjelmistojen ja erityisesti niistä uusimman Windows Server 2008 Enterprise-version toimintojen ja ominaisuuksien esittelyyn. Toimintoja ja ominaisuuksia kuvataan toimintavarmuuden ja vikasietoisuuden näkökulmasta, eikä sen muita toimintoja tai palvelinrooleja käsitellä sen enempää kuin kulloinkin käsittelyssä olevan aihepiirin tarkastelun kannalta on olennaista. Kirjoitushetkellä sen seuraajaa Windows Server 2008 R2:a ei ole vielä julkaistu. Microsoft on ilmoittanut sen tulevan markkinoille lokakuun lopussa 2009 (Windows Server 2008 R2 2009).

5.1 Windows-palvelinohjelmistojen historiaa

Windows-palvelinohjelmistojen historian voidaan katsoa alkaneen jo vuonna 1993, jolloin Microsoft julkaisi Windows NT 3.1 Server:n. Sen kehitystä jatkettiin aina vuoteen 1998 saakka, jolloin viimeisin versio 4.0 Terminal Server julkaistiin. (Windows Products and Technologies History 2009.) Vuonna 2000 Microsoft julkaisi Windows Server 2000:n, jonka ominaisuuksiin kuuluvat muun muassa uutena toimintona esitelty aktiivihakemistorakenne, DFS ja kiintolevyjen RAID-konfigurointi (TechNet Windows 2000 Server 2009).

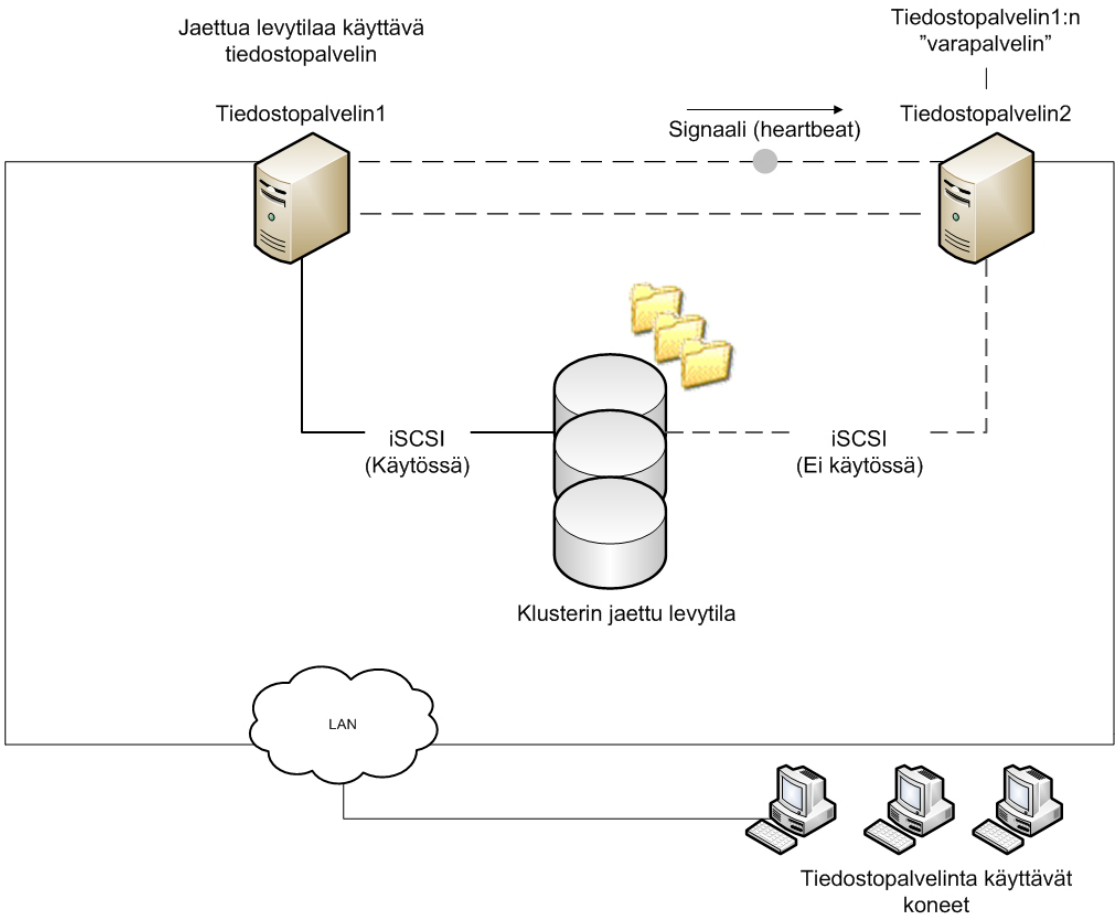
Vuonna 2003 markkinoille tuotu Windows Server 2003 oli kehitysaskel Windows-palvelinohjelmistojen saralla ja toi parannuksia muun muassa aktiivihakemiston toimintaan. Windows Server 2003 tukee verkkokuormantasausta (NLB) ja sen *Enterprise*- ja *Datacenter*-versiot tarjosivat lisäksi työkalut vikasietoisen klusterin perustamiseen ja hallintaan. (TechNet Server 2003 Product Overview 2009.)

Viimeisin Microsoft-palvelinohjelmisto Windows Server 2008 julkaistiin alkuvuodesta 2008. Parannuksina edeltäjiinsä se tarjoaa muun muassa helpommin hallittavat palvelinroolien toiminnot, uusimman version www-palvelimestaan (IIS 7) sekä parantuneet turvallisuusominaisuudet käyttäjien autentikoinnista parantuneeseen tiedonsiirron turvallisuuteen (Matthews 2008).

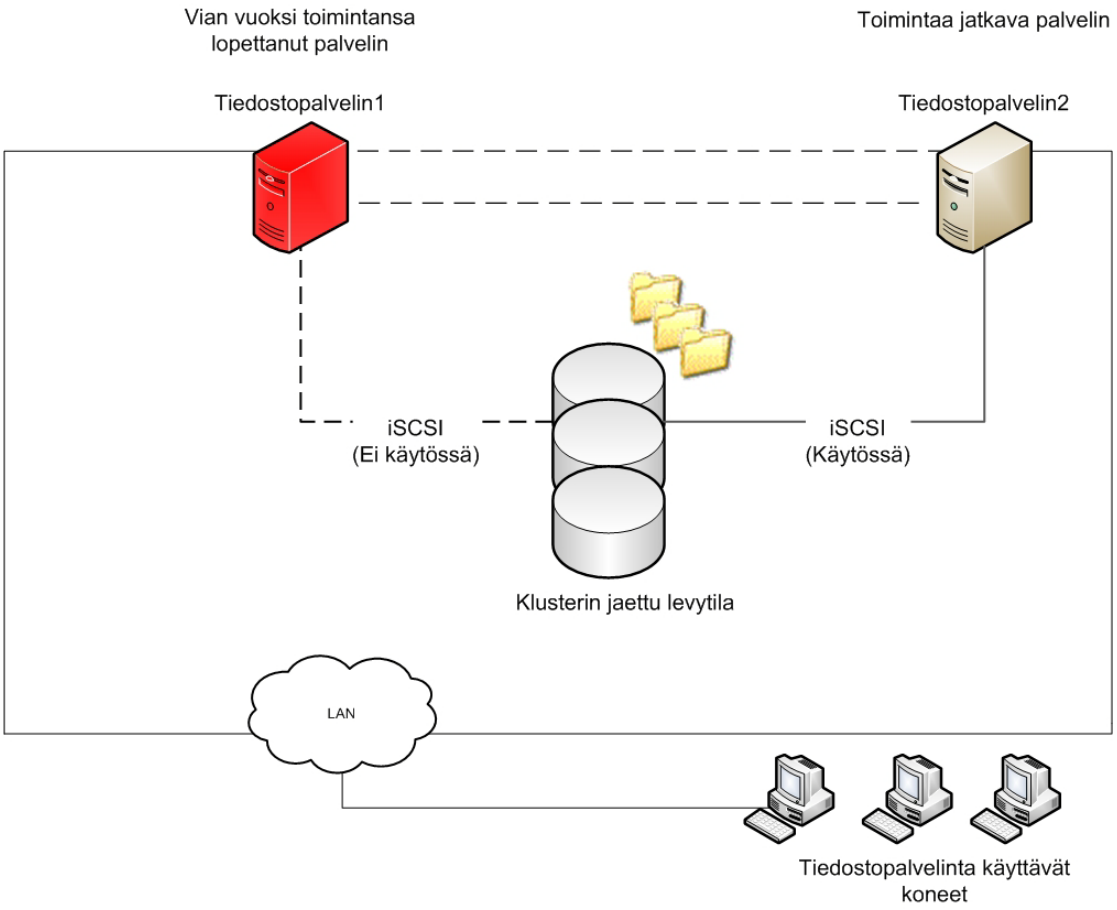
5.2 Vikasietoinen klusteri (Failover Clustering)

Vikasietoinen klusteri varmistaa toiminnoiltaan ehdottaman kriittisten sovellusten käytettävyyden myös silloin, kun niitä tarjoava palvelin lopettaa toimintansa toimintahäiriön tai laitevian seurauksena. Klusteri muodostuu kahdesta tai useammasta kokoonpanoltaan täysin identtisestä palvelimesta. Klusterin jäsenkoneet (*node*) ovat identtisiä myös toiminnoiltaan joko palvelinrooliensa tai niiden tarjoamien sovellusten osalta. Vaikka klusterissa on useampi jäsen, se käyttäytyy yhden palvelimen tavoin ja näyttäytyy verkkoympäristössä yhtenä itsenäisenä kokonaisuutena. Klusteroitavaa palvelua tai sovellusta suoritetaan ainoastaan yhdessä palvelimessa kerrallaan. (Zacker 2009.)

Klusterin jäsenkoneet lähettävät normaalitilassa toisilleen omasta toimintakunnostaan ilmaisevia signaaleja (*heartbeat*), ks. kuva 6. Mikäli jokin klusterin jäsenistä lakkaa lähettämästä näitä signaaleja esimerkiksi laitevian tai muun ongelman seurauksena, siirretään kyseisen jäsenen tarjoamat palvelut klusterissa edelleen toimintakuntoisen palvelimen hoidettavaksi. Kuvassa esitetyllä Tiedostopalvelin1:llä on aktiivinen iSCSI-väylää käyttävä yhteys jaettuun levytilaan, eli käytännössä tiedostopalvelimen tiedostoihin. Se lähettää omasta toimintakunnostaan ilmaisevaa signaalia klusterin toiselle jäsenelle Tiedostopalvelin2:lle, joka ei käytä klusterin yhteistä levytilaa kunnes Tiedostopalvelin1:n lähettämät signaalit lakkaavat. Tällöin Tiedostopalvelin2 muodostaa yhteyden jaettuun levytilaan ja lähiverkosta tulevat tiedostopalvelimen tiedostoihin kohdistuvat pyynnöt ohjautuvat nyt sen kautta edelleen lähiverkon käyttäjille, ks. kuva 7. Klusteroitavan palvelun käyttäjille tästä aiheutuva katkos palvelujen käytettävyydessä on hyvin lyhyt (TechNet Example, Clustered File or Print Server 2009).



Kuva 6 Klusteroitu tiedostopalvelin normaalitilassa (mukailtu TechNet Example, Clustered File or Print Server 2009).



Kuva 7 Klusteroitu tiedostopalvelin vikatilanteessa (mukailtu TechNet Example, Clustered File or Print Server 2009).

5.2.1 Laitteistoon ja käyttöjärjestelmään kohdistuvat vaatimukset

Windows Server 2008-ympäristössä vikasietoisen klusterin jäsenten ja käytettävän verkkoinfran laitteistovaatimukset Zackerin (2009) mukaan ovat

- komponenteiltaan identtiset palvelimet
- jaettu levytila, jossa kriittiset tiedot sijaitsevat
- vikasietoinen verkko, ks. luku 3.3

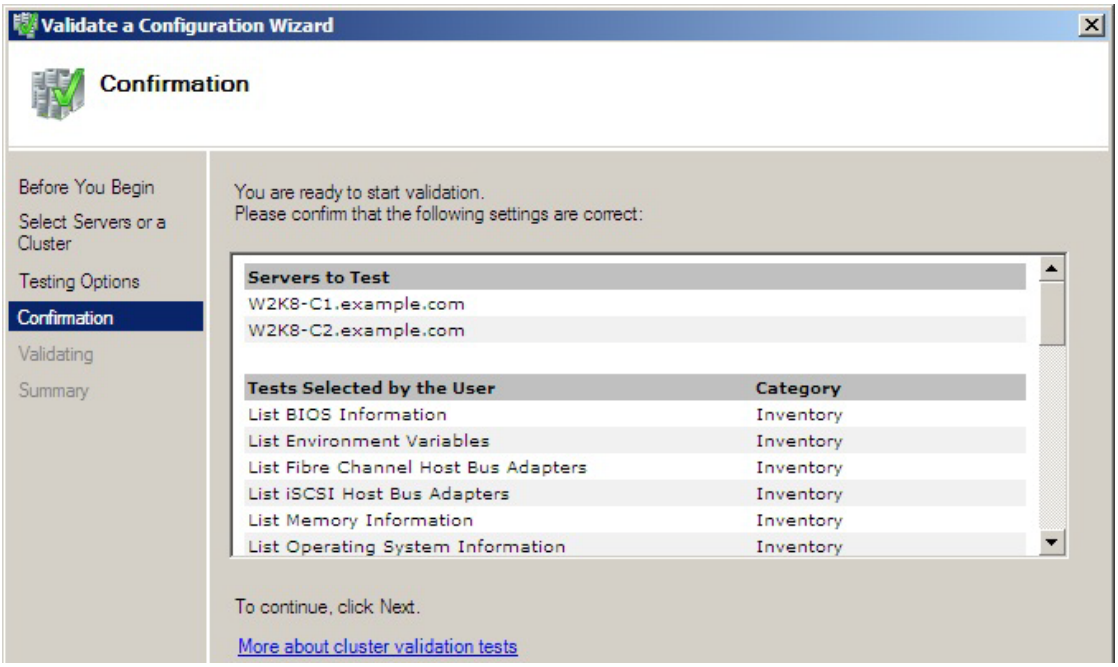
Zackerin (2009) mukaan jaettu levytila on klusterin toiminnan kannalta oleellisin yksittäinen tekijä, siellä sijaitsee kaikki klusteroitavan palvelun tai sovelluksen data. Jokaisen klusterin jäsenkoneista tulee saada yhteys tähän levyyn toimiakseen oikein. On kuitenkin huomioitava, että tiedon eheyden säilymisen vuoksi ainoastaan yksi jäsenistä voi käsitellä sovellusdataa kerrallaan. (Zacker 2009.)

Lisäksi klusterin jäsenten tulee olla identtisiä niin käyttöjärjestelmän version, klusteroitavan sovelluksen kuin asennettujen päivitystenkin osalta. Jokaisen jäsenen on lisäksi kuuluttava samaan toimialueeseen (*Domain*) ja on suositeltavaa, että ne ovat toimialueessa ainoastaan jäseniä, eivät toimialueen ohjauskoneita (*Domain Controller*). (Zacker 2009.)

Windows Server 2008-versioista ainoastaan *Datacenter* ja *Enterprise* tukevat vikasietoisen klusterin ominaisuuksia (Zacker 2009).

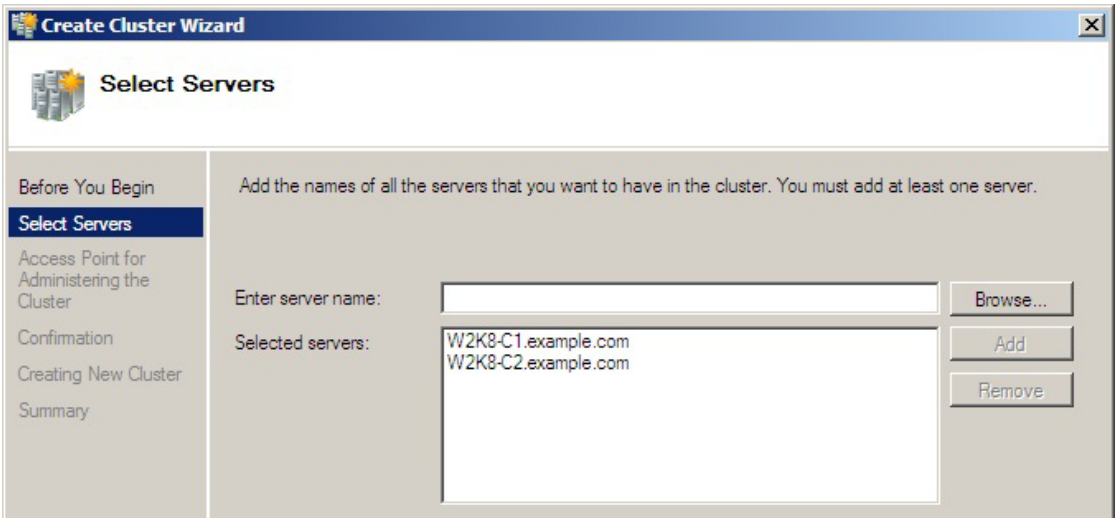
5.2.2 Vikasietoisen klusterin luominen ja konfigurointi

Windows Server 2008:ssa Failover Clustering on asennettava ominaisuus (*feature*) ja sen tulee olla asennettuna jokaisessa klusteriin kuuluvassa palvelimessa. Windows Server 2008:n klusterointi eroaa edeltäjänsä Windows Server 2003:n ominaisuuksista. Muun muassa klusterin luomiseen, sen hallintakäyttöliittymään ja toimintavarmuuteen on tehty parannuksia. Uutena ominaisuutena siinä on klusterin jäsenten testaustyökalu, joka testaa niiden soveltuvuuden (*validation*) klusterissa toimimiseen. (TechNet Failover Clusters 2009.) Kyseinen validointitesti testaa muun muassa jokaisen jäsenen BIOSin, verkkokorttien, käyttöjärjestelmän ja sen version soveltuvuuden klusterointikonfiguraatioon (kuva 8). Tämän lisäksi jäsenten laitteistokokoonpanoja verrataan toisiinsa ja testataan, onko jokaisella jäsenellä pääsy jaettuun levytilaan. Testin tulos ilmoittaa, onko käytettävä konekanta ja verkon rakenne soveltuva klusterin luomiseen, ja erittelee tulokset testattujen osa-alueiden osalta. Mikäli testi havaitsee klusterointiin soveltumattomia laitteisto- tai käyttöjärjestelmäkokoonpanoja, voi osa klusterin toiminnoista olla mahdotonta toteuttaa. Testin antama raportti on syytä tutkia tarkkaan ja tarvittaessa korjata siinä havaitut puutteet.

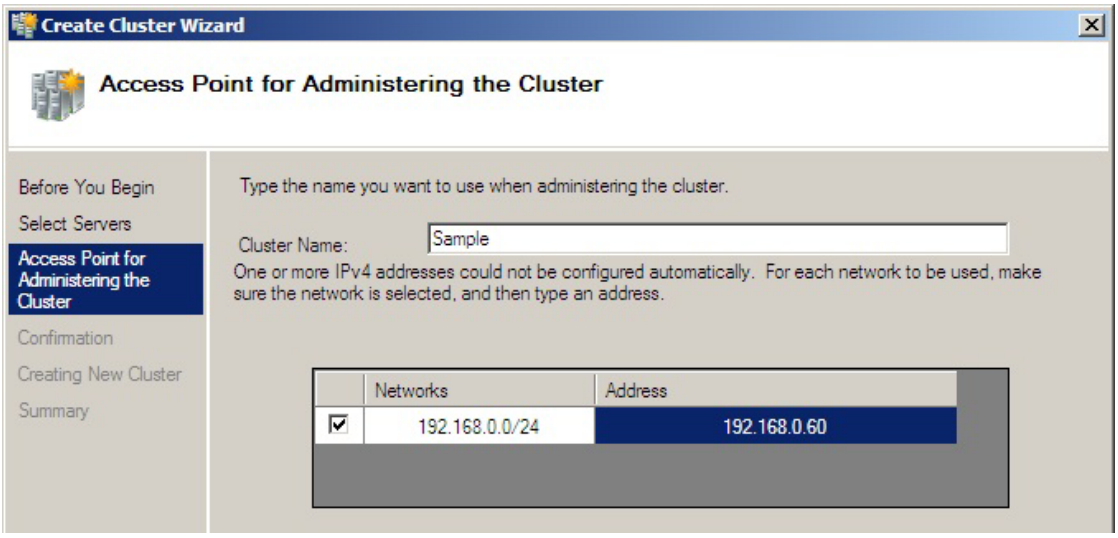


Kuva 8 Klusteroinnin soveltuvuustestin testattavat kohteet (TechRepublic 2009).

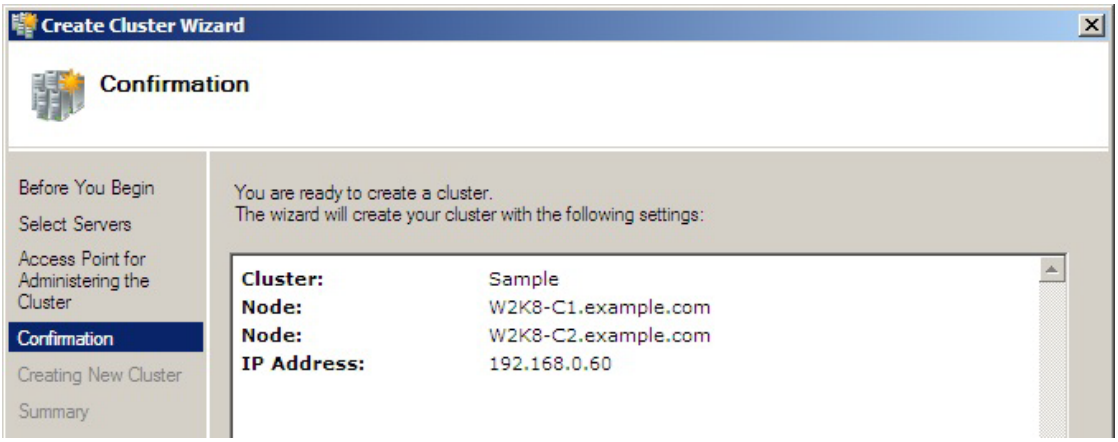
Jäsenten testauksen ja mahdollisten muutosten jälkeen luontivaiheessa klusterille määritetään siihen kuuluvat jäsenkoneet, klusterin nimi ja IP-osoite, ks. kuvat 9, 10 ja 11.



Kuva 9 Klusterin jäsenkoneiden valinta (TechRepublic 2009).

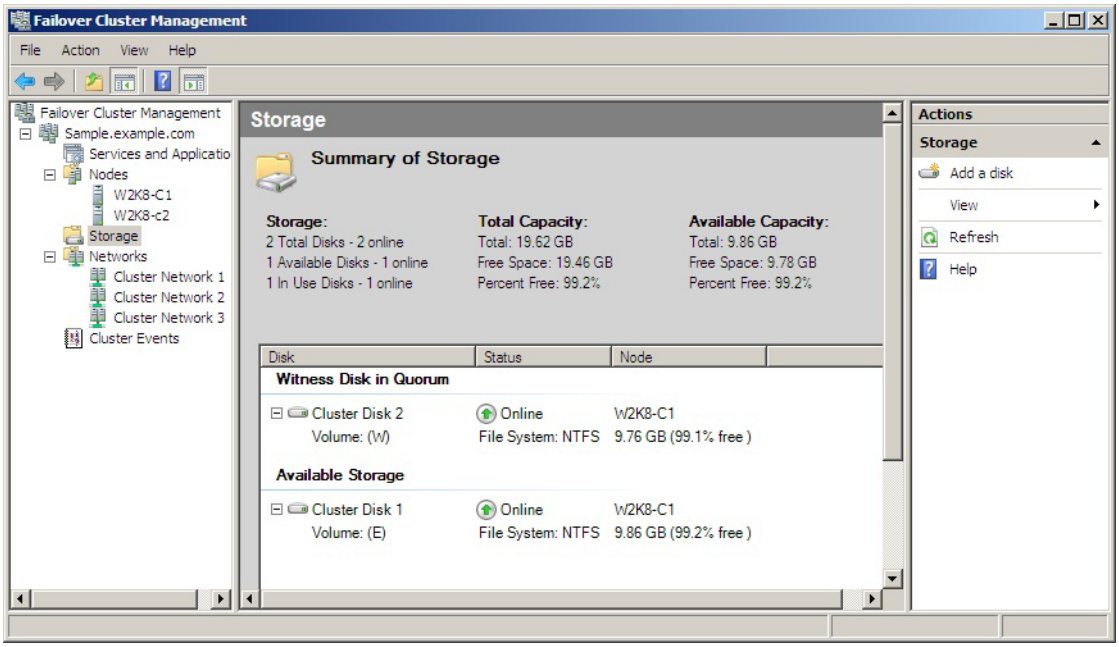


Kuva 10 Klusterin nimen ja IP-osoitteen määritys (TechRepublic 2009).



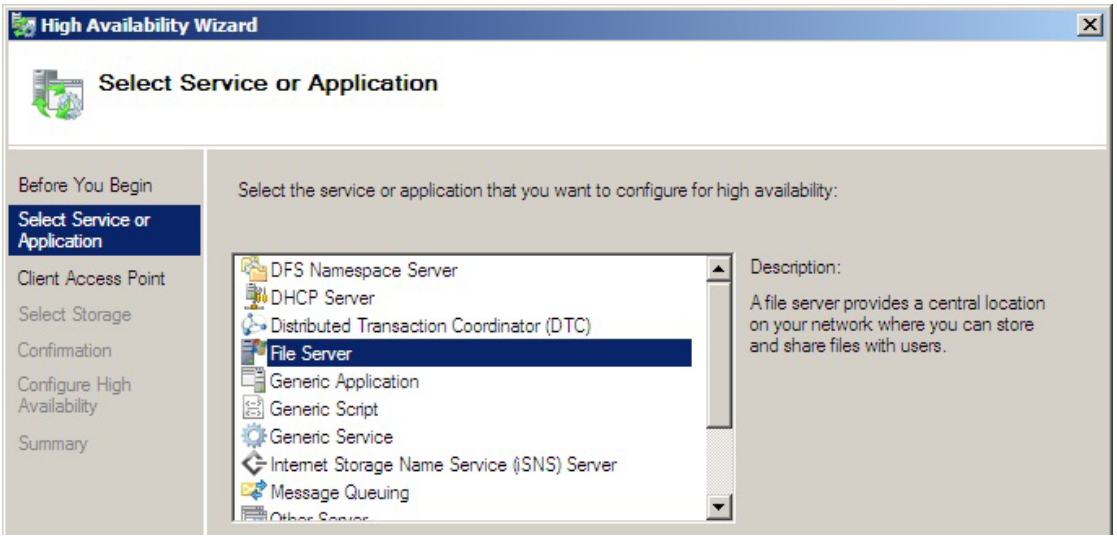
Kuva 11 Klusterin luonnin vahvistaminen (TechRepublic 2009).

Klusterin palvelujen, jäsenten, klusterin käyttämän tallennustilan ja klusterointiin käytettävien verkkojen asetuksia ja toimintoja hallitaan klusterin hallintanäkymässä, ks. kuva 12.



Kuva 12 Klusterin hallintanäkymä (TechRepublic 2009).

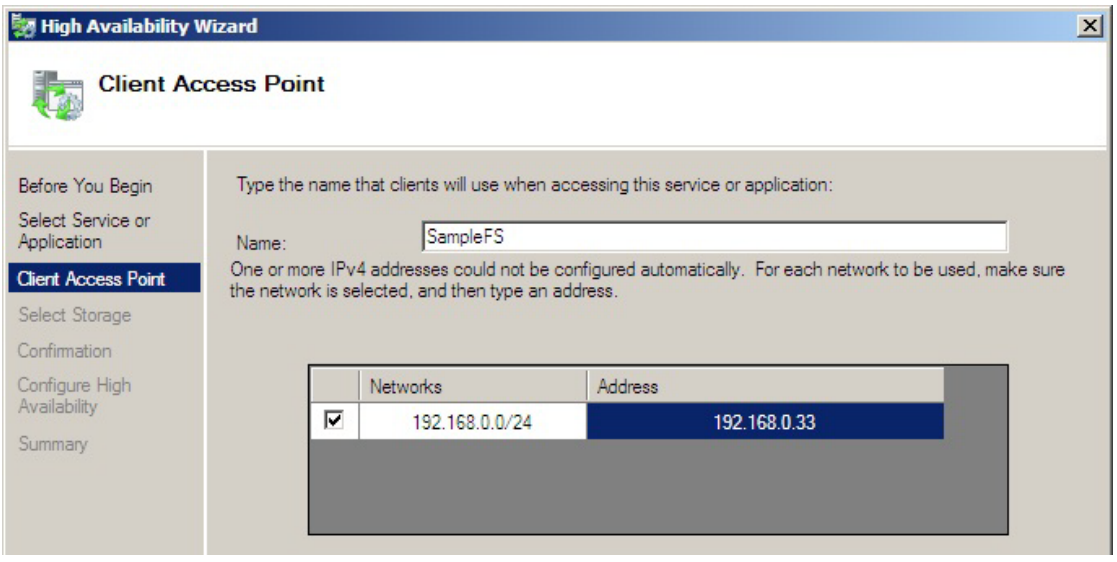
Klusterin tarjoaminen palvelujen konfigurointivaiheessa valitaan se palvelinrooli tai tietojärjestelmän palvelu, jonka toimintavarmuus on kriittisen tärkeää ja jonka saatavuus klusteroinnilla siis turvataan, ks. kuva 13. Klusteroitava palvelu voi olla esimerkiksi tietokantasovellus tai palvelimen rooli kuten virtualisointi-, tulostus-, tiedosto-, DHCP-, DFS- tai DNS-palvelin.



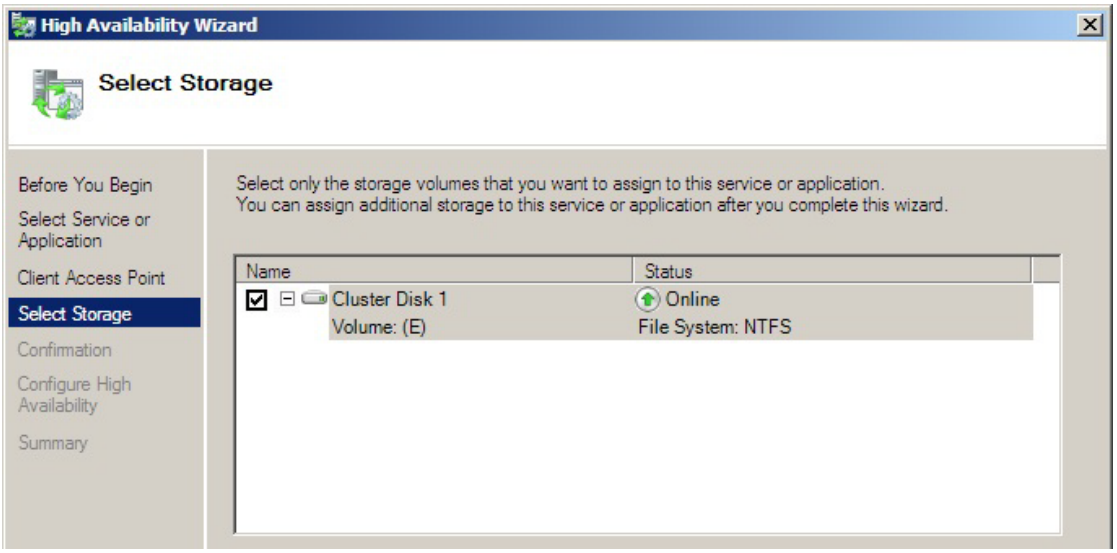
Kuva 13 Klusteroitavan palvelinroolin valinta (TechRepublic 2009).

5.2.2.1 Vikasietoisen tiedostopalvelimen asennus klusterikonfiguraatioon

Toteutettaessa tiedostopalvelinta osana klusterointikokoonpanoa sille määritetään jakonimi, jolla se lähiverkossa näkyy, yksilöllinen IP-osoite sekä tiedostoille osoitettu tallennustila, joka käytännössä sijaitsee jäsenkoneiden (*node*) fyysisillä kiintolevyillä, ks. kuvat 14 ja 15.

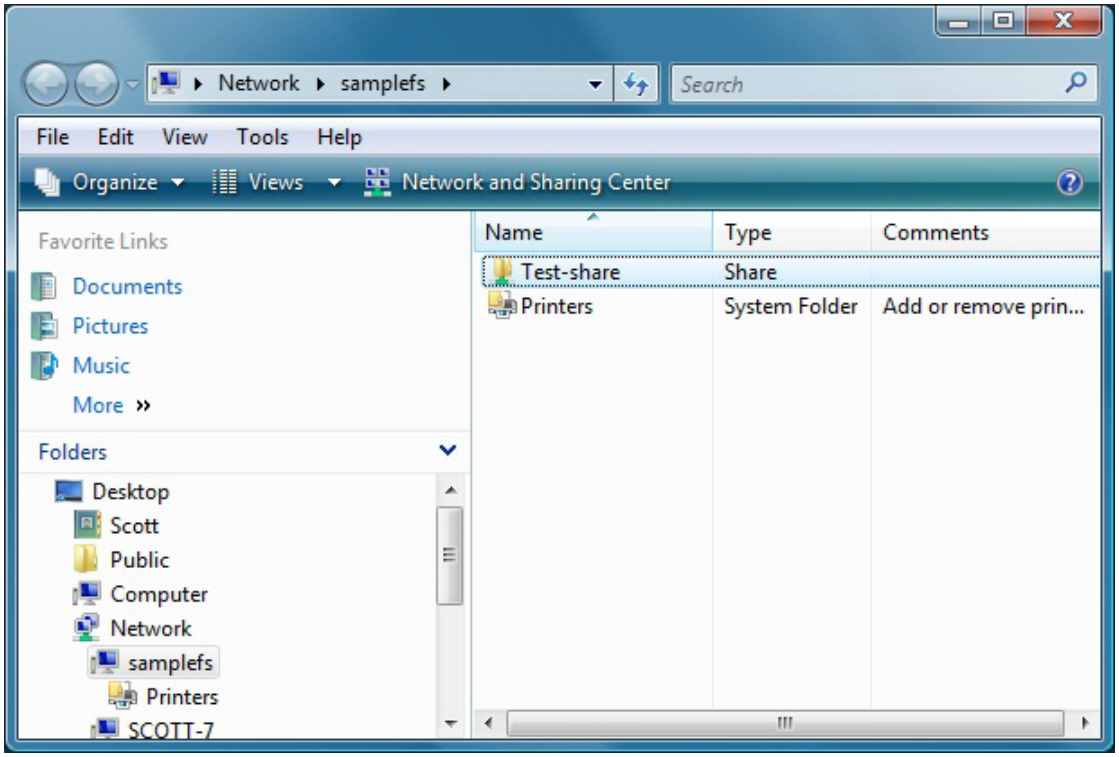


Kuva 14 Palvelulle määritetään nimi ja IP-osoite (TechRepublic 2009).



Kuva 15 Tiedostopalvelimen käyttämän tallennustilan valinta (TechRepublic 2009).

Kuvassa 16 on esitetty käyttäjän näkymä klusteroituun verkkojakoon. Olennaista on, että peruskäyttäjälle kyseinen verkkojako näkyy ainoastaan yhtenä kokonaisuutena, eikä sen käytettävyys eroa tavallisesta verkossa sijaitsevasta tiedostojaosta.



Kuva 16 Klusteroidun verkkojaon käyttäjän näkymä (TechRepublic 2009).

5.3 Verkkoliikenteen tasaus (Network Load Balancing)

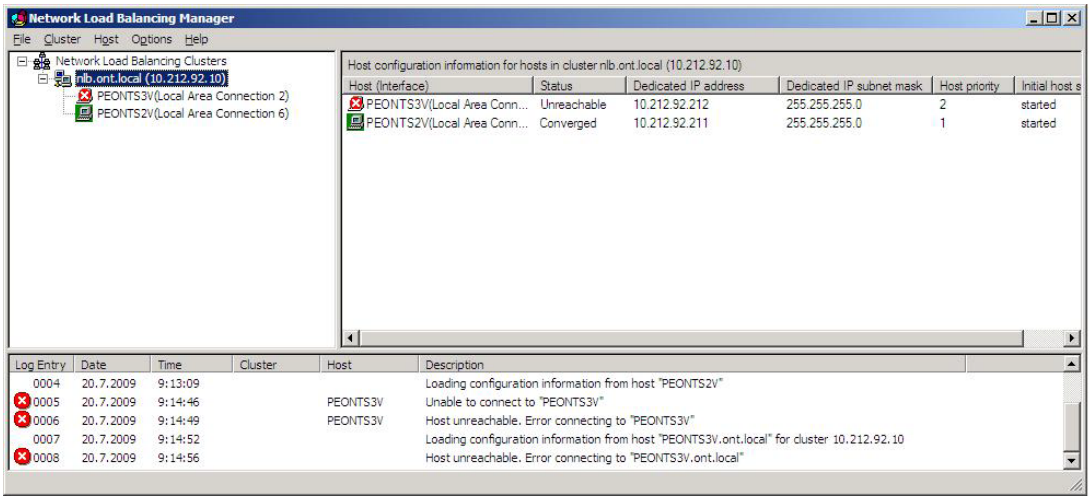
Windows Server 2008:ssa Network Load Balancing on nimensä mukaisesti pääasiassa väline, jolla tasataan verkkoliikennettä jakautumaan eri palvelimille. NLB on asennettava ominaisuus (*feature*) ja se soveltuu hyvin esimerkiksi staattisten www-sivustojen sekä FTP- ja Telnet-palvelinten kuormantasaamiseen. (TechNet NLBb 2009.) Sen sijaan se ei sovellu sähköposti- ja tietokantasovellusten kuormituksen tasaamiseen, koska klusterin tietokantakäsittelyyn liittyy tiettyjä rajoituksia, ks. luku 5.3.2 (Zacker 2009).

NLB:n tyypillisin käyttökohde on www-palvelinten kuormituksen tasaaminen. NLB:n avulla voidaan varmistaa verkkosivuston saatavuus myös lisääntyneen kävijämäärän ja sitä kautta www-palvelimeen kohdistuvan lisäkuormituksen mahdollisesti mukanaan tuomista ongelmista huolimatta. Lisäksi NLB:n avulla www-palvelinten toimintavarmuus voidaan pitää vaaditulla tasolla ja tarvittavia ylläpitotöitä voidaan tehdä ilman pitkiä katkoksia sivuston palveluissa. Tällöin ylläpidon kohteena olevan palvelimen tarjoamat palvelut voidaan siirtää muiden palvelinten suoritettavaksi huoltotyön ajaksi.

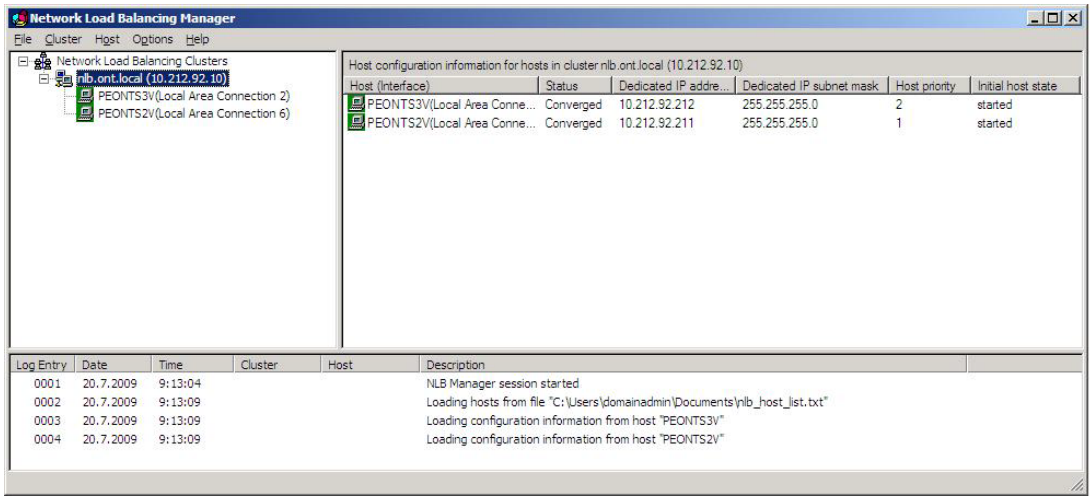
NLB yhdistää useamman yksittäisen palvelimen omaksi itsenäiseksi kokonaisuudeksi, joka on toiminnaltaan samankaltainen kuin vikasietoinen klusteri, ks. luku 5.2. Yhtäläisyyksistään huolimatta se ei pääasiallisesti kuitenkaan ole tarkoitettu parantamaan www-palvelinten vikasietoisuutta. NLB-klusterin jäsenet lähettävät toisilleen signaaleja, joita tarkkailemalla seurataan klusterin jäsenten toimintaa. Tilanteessa, jossa jonkin jäsenen signaalit lakkaavat palvelimen lopetettua toimintansa, ohjaa klusteri ko. jäsenen verkkoliikenteen muille jäsenille. (TechNet Edge 2009.) Yhteen kuormitusta tasaavaan NLB-klusteriin voidaan liittää 32 palvelinta (TechNet NLBa 2009).

NLB-klusterilla on oma nimensä ja IP-osoitteensa. Kaikki klusterin jäsenkoneet toimivat, vikasietoisesta klusterista poiketen, yhtäaikaisesti NLB-klusterin kokonaissuorituskyvyn parantamiseksi ja esimerkiksi verkkosivuston ollessa kyseessä jokainen klusterin jäsenkoneista www-palvelimena toimiva palvelee sivustolla kävijöitä sille tehtyjen määritysten mukaisesti, ks. luku 5.3.2. (Zacker 2009.)

Vaikka NLB:n pääasiallinen tehtävä ei olekaan vikasietoisuuden parantaminen, voi klusteri jatkaa toimintaansa huolimatta siitä, että yksi sen jäsenkoneista lopettaa toimintansa virheen tai toimintahäiriön vuoksi (kuva 17). Tällöin verkkosivun liikenne ohjautuu edelleen klusterin muiden jäsenkoneiden www-palvelimiin klusterin määritysten mukaisesti, mutta koska tässä vaiheessa jäljellä olevia verkkokuormaa tasaavia jäseniä on vähemmän, kasvaa niihin kohdistuva kuormitus. Tästä johtuen ihanteellista onkin huolehtia toimintansa lopettaneen palvelimen toimintakuntoon saattamisesta mahdollisimman pikaisesti. Tarvittavien huoltotoimenpiteiden jälkeen palvelin palautetaan takaisin klusterin jäseneksi ja se voi jatkaa osallistumistaan verkkokuormituksen jakamiseen (kuva 18).



Kuva 17 Kun yksi klusterin jäsenistä lakkaa toimimasta, muut jatkavat.



Kuva 18 Kaikki klusterin jäsenet jälleen toiminnassa.

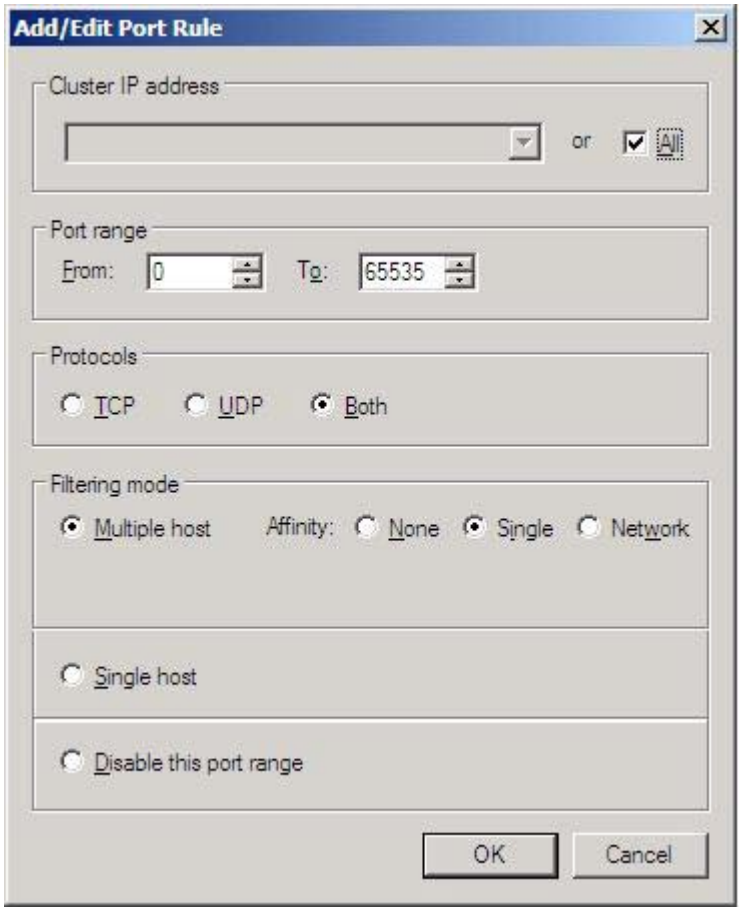
5.3.1 NLB-klusterin luominen

Klusterin asennusvaiheessa sille määritetään muun muassa nimi, IP-osoite ja porttienohjaussäännöt, joilla kuormantasausta ohjataan porttikohtaisesti IP - ja UDP-protokollilla ts. miten haluttu liikenne ohjataan jakautumaan klusterin jäsenten kesken. Esimerkiksi portin 80 (*HTTP*-liikenne) liikenne voidaan ohjata yksinomaan tietylle jäsenelle tai vaihtoehtoisesti jakautumaan tasaisesti kaikkien klusterin jäsenten kesken.

Kun klusteri on luotu, siihen lisätään haluttu määrä jäseniä. NLB-klusterissa voi olla 2-32 jäsentä ja niiden lisääminen klusteriin on tehty helpoksi. Klusterin luomiseksi jokaisessa jäsenkoneessa on oltava asennettuna Network Load Balancing -ominaisuus. Jäsenkonetta lisättäessä määritetään verkkokortti, jota jäsen kuormantasausliikenteessään käyttää sekä yksilöivä tunniste-ID. Uuden jäsenen tiedot päivittyvät klusteriin ja jäsen on toimintavalmiudessa lähes välittömästi ja osallistuu verkkokuorman tasaamiseen klusterin määritysten mukaisesti.

5.3.2 NLB-klusterin asetukset

Tärkeimmät klusterin asetuksista ovat sen verkkoliikenteen *Filtering Mode* ja *Affinity*. NLB ohjaa porttikohtaisesti tulevan verkkoliikenteen joko aina samalle klusterin jäsenelle (*Filtering Mode = Single*) tai jakaa sen kaikkien jäsenten kesken (*Filtering Mode = Multiple*) (kuva 19). Liikenne voidaan jakaa tasaisesti kaikkien jäsenten kesken eli verkkosivuston käyttäjää voi palvella useampi kuin yksi www-palvelin asiakasistunnon (*session*) aikana. Tällä ei staattisen sivuston ollessa kyseessä käyttäjän kannalta ole juuri merkitystä, mutta esimerkiksi verkkokaupassa asioinnin sujuvuuden kannalta on tärkeää, että ainoastaan yksi klusterin jäsenistä käsittelee tietyn asiakkaan sivupyyntöjä ja esimerkiksi ostoskorin tilatietoja tietyn asiakasistunnon aikana. Jos asiakasta palveleva www-palvelin (eli tässä yhteydessä klusterin jäsen) vaihtuu kesken asiakasistunnon aikana, tilatiedot eivät siirry uudelle jäsenelle. Tämän vuoksi on tärkeää, että verkkokauppojen ja vastaavien asiakasistuntoon ja sen tilatietoja vaativien verkkosivustojen ollessa kyseessä NLB:n asetukset on määritetty ohjaamaan tietystä IP-osoitteesta (*Affinity = Single*) tai -osoitealueesta (*Affinity = Network*) tulevat sivupyynnöt aina samalla klusterin jäsenelle. (Techotopia 2009.)

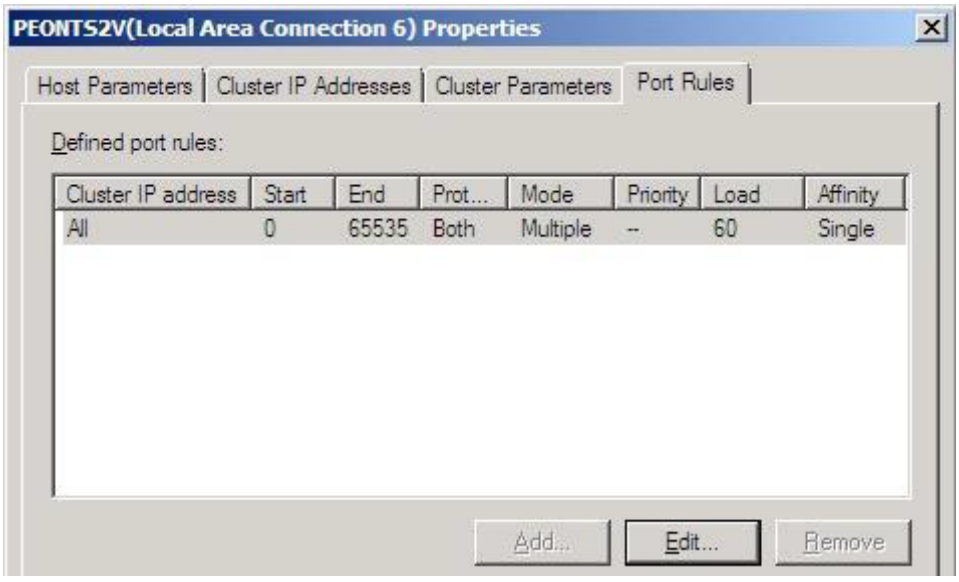


Kuva 19 NLB-klusterin asetukset.

5.3.3 NLB-klusterin toiminnot

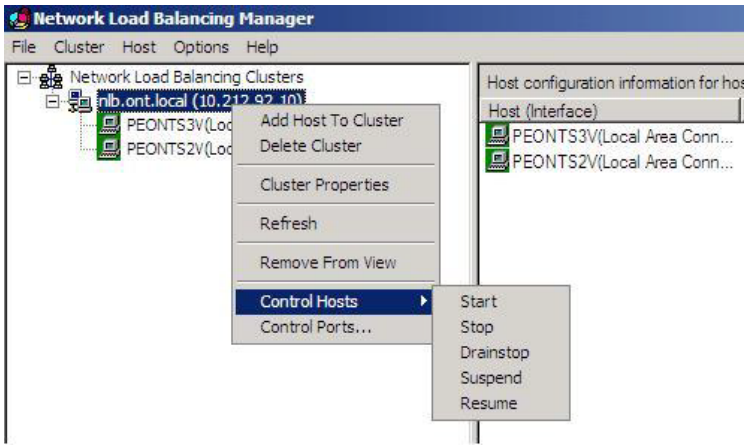
Klusterin luomisen jälkeen se toimii oletusasetuksilla automaattisesti. Sen toimintaa ohjataan NLB Manager -hallintaohjelman avulla. Klusteria hallitaan joko kokonaisuutena tai jokaista sen jäsentä yksitellen.

Olennaisin osa klusterin toimintaa on sen verkkoliikennekuorman tasaus jäsenten välillä. Oletusasetuksilla klusteri tasaa liikenteen tasan kaikille jäsenille kaikkiin TCP- ja UDP-protokollien portteihin tulevan verkkoliikenteen osalta. Porttienohjaussääntöjen avulla verkkokuorma (*load*) voidaan tarvittaessa jakaa kuitenkin porttikohtaisesti halutuissa suhteissa jäsenten kesken, esimerkiksi kahden jäsenen klusterissa suhteessa 40/60 %, jolloin toiseen jäseneen voidaan sen paremman suorituskyvyn tai muun syyn vuoksi ohjata suurin osa kokonaisliikenteestä (kuva 20). Tällainen konfiguraatio on voimassa, kun kaikki klusterin jäsenet ovat toimintakuntoisia eli lähettävät toiminnastaan ilmaisevia sydämenlyöntejä klusterin muille jäsenille. Jos jokin jäsenistä lopettaa toimintansa, ohjautuu liikenne luonnollisesti kokonaisuudessaan toimintaansa jatkavien käsiteltäväksi. Kahden jäsenen klusterissa toimintaansa normaalisti jatkava jäsen hoitaa tällöin kaiken (100 %) klusteriin tulevan verkkoliikenteen.



Kuva 20 Porttienohjaussäännöillä ohjataan verkkoliikenteen jakautumista jäsenten kesken.

NLB Manager -hallintaohjelman kautta koko klusteri tai sen yksittäinen jäsen voidaan tarvittaessa ajaa hallitusti alas esimerkiksi huolto- ja ylläpitotöiden vuoksi. Klusterin verkkoliikenne voidaan lopettaa joko kerralla siten, että kaikki klusterin verkkoliikenne keskeytetään sekä sillä hetkellä avoinna olevien että uusien yhteyksienkin osalta (*stop*) tai siten, että nykyiset yhteydet säilytetään, mutta uusia ei sallita (*drainstop*), ks. kuva 21. Näiden lisäksi verkkoliikenne voidaan ajaa hallitusti alas myös porttikohtaisesti portinohjaussääntöjen mukaisesti. (TechNet NLBc 2009.)



Kuva 21 NLB-klusterin liikenne voidaan ajaa alas hallitusti.

5.3.4 Muut huomioitavat seikat

NLB-klusterin käyttöönoton jälkeen on huomioitava se, että klusterilla on oma IP-osoitteensa ja nimensä, ja että klusteri ohjaa sen jäsenkoneiden verkkoliikennettä. Näin ollen DNS-palvelimen tietueisiin on päivitettävä nimenomaan klusterin IP-osoite vastaamaan haluttua palvelua, esimerkiksi verkkosivustoa, sen sijaan, että ko. tietue viittaisi sitä tarjoavan www-palvelimen IP-osoitteeseen. (Zacker 2009.)

Tämän lisäksi Zacker (2009) muistuttaa, että muutokset ja päivitykset haluttuun sovellukseen tai palveluun on tehtävä kaikkiin klusteriin kuuluviin palvelimiin samanlaisina. Esimerkiksi verkkosivustolle uutta sivua lisättäessä sama sisältö tulee päivittää kaikille ko. sivustoa tarjoaville www-palvelimille. (Zacker 2009.)

5.4 Windows Server-varmuuskopiointi (Windows Server Backup)

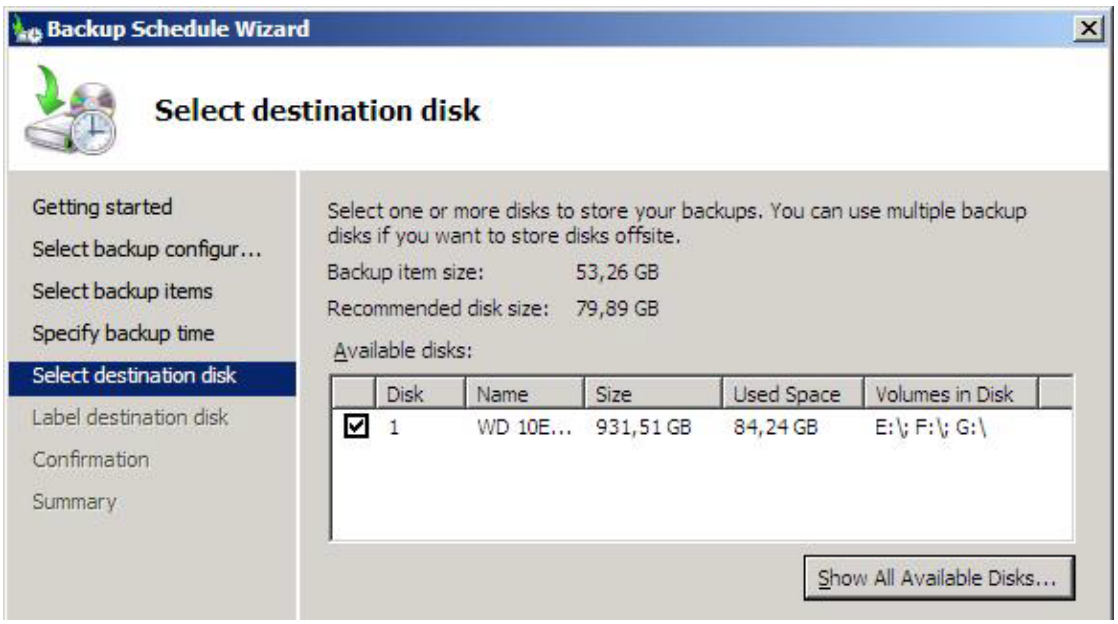
Windows Server 2008 sisältää työkalut perustason varmuuskopiointiin ja varmuuskopioiden palauttamiseen. Käyttöjärjestelmän omalla Windows Server Backup:lla on mahdollista ottaa varmuuskopio palvelinjärjestelmästä kertaluontoisena ja ajastettuna toimintona. Eroavaisuuksia ja suoranaisia puutteita aikaisempiin Windows-palvelinkäyttöjärjestelmäversioiden varmuuskopiointityökaluihin verrattuna kuitenkin on.

5.4.1 Ajastettu (Scheduled Backup) ja kertaluontoinen (Backup Once) varmuuskopiointi

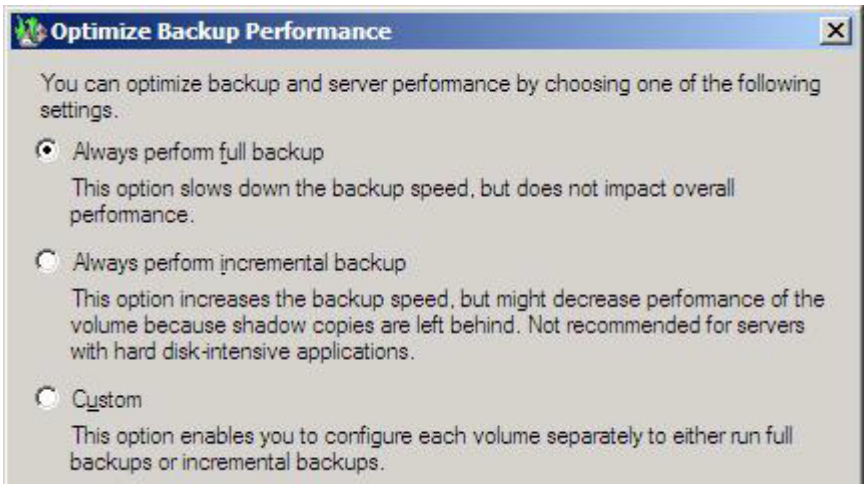
Windows Server Backup on toiminnoiltaan ja ominaisuuksiltaan kolmansien osapuolten kaupallisia varmuuskopiointiohjelmistoja huomattavasti rajoittuneempi. Lisäksi sen tarjoamat varmuuskopiointitoiminnot eroavat merkittävästi Windows Server -käyttöjärjestelmien aikaisempien versioiden toiminnoista muun muassa käyttöliittymän ja ennen kaikkea käyttämänsä vhd-tiedostomuodon (*Virtual Hard Disk*) osalta, sillä Windows Server Backup:lla ei ole mahdollista palauttaa tietoja Windows Server 2003:n Ntbackup.exe-ohjelmalla tehdyistä varmuuskopioista. Kyseinen ohjelma on kuitenkin saatavissa Windows Server 2008:an erikseen ladattavana, mikä mahdollistaa aikaisempien Windows-versioiden varmuuskopioiden palauttamisen. Huomioitavaa kuitenkin on, että sillä ei voi luoda uusia varmuuskopioita Windows Server 2008 -ympäristössä. (Zacker 2009.)

Windows Server Backup onkin suunniteltu pääasiassa loogisten levyjen ja osioiden varmuuskopiointiin siten, että kopiointi tehdään ulkoiselle kiintolevylle käyttäen joko USB- tai IEEE 1394 -väylää (kuva 22). Se ei Windows Server 2003:sta poiketen tue enää nauhavarmistusta, vaan sitä varten tarvitaan kolmannen osapuolen ohjelmisto (Zacker 2009). Lisäksi sen ajastettua varmuuskopiointia (*Scheduled Backup*) ei voida tehdä optiselle levylle tai verkkojakoon ja varmuuskopiointi tehdään aina levy tai osio kerrallaan sen sijaan, että varmuuskopioitavaksi voisi valita haluamansa tiedostot ja kansiot. Käytettävissä on tällöin joko täydellinen (*Full Backup*) tai pelkästään edellisen varmuuskopion jälkeen muuttuneiden tiedostojen varmuuskopiointi (*Incremental Backup*) (kuva 23). Myös koko palvelin (mukaan lukien käyttöjärjestelmä, sovellukset ja järjestelmän asetukset) on mahdollista ajastaa

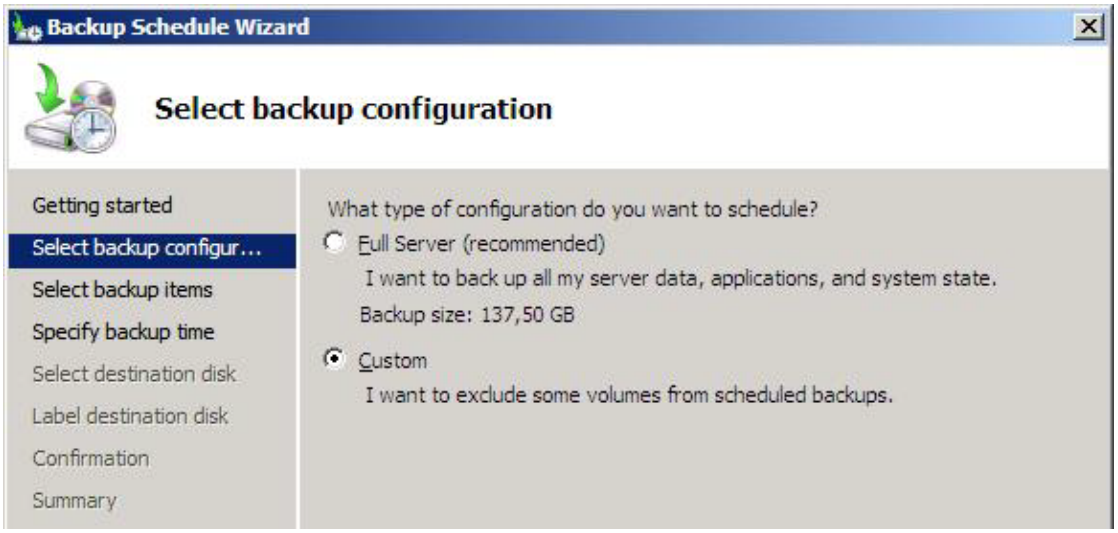
varmuuskopioitavaksi (kuva 24). Tällöin kannattaa kiinnittää huomioita varmuuskopioitavien tiedostojen tiedostokokoon.



Kuva 22 Ajastettu varmuuskopio on otettavissa ainoastaan ulkoiselle kiintolevylle.

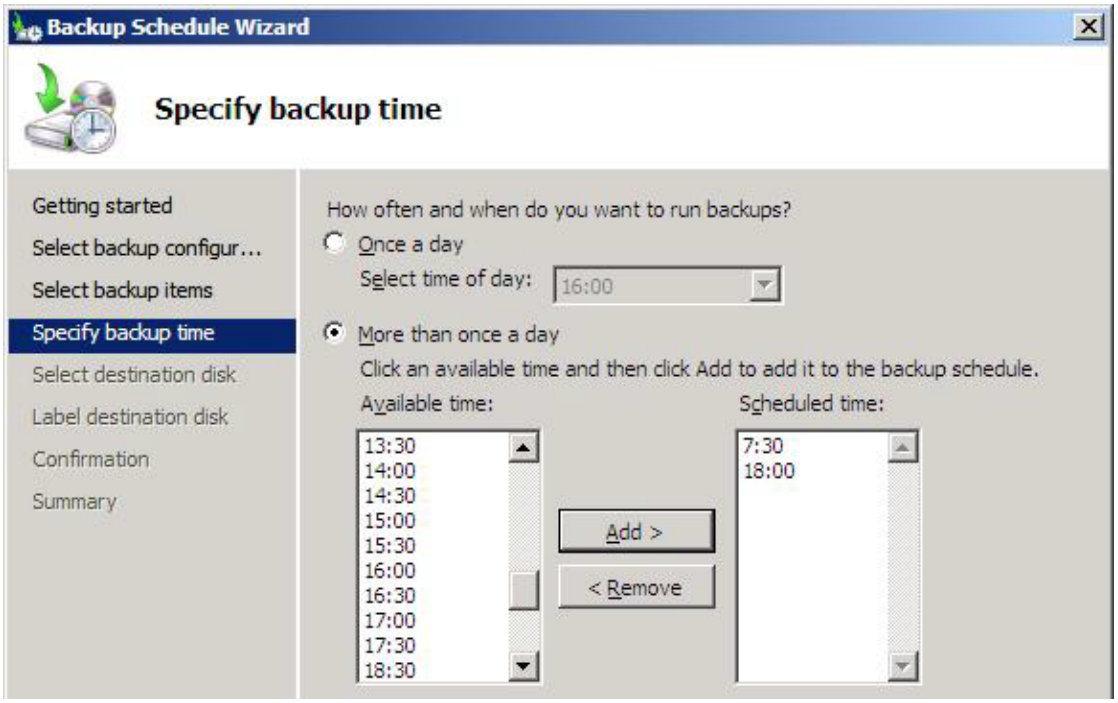


Kuva 23 Varmuuskopiointityypin valinta.



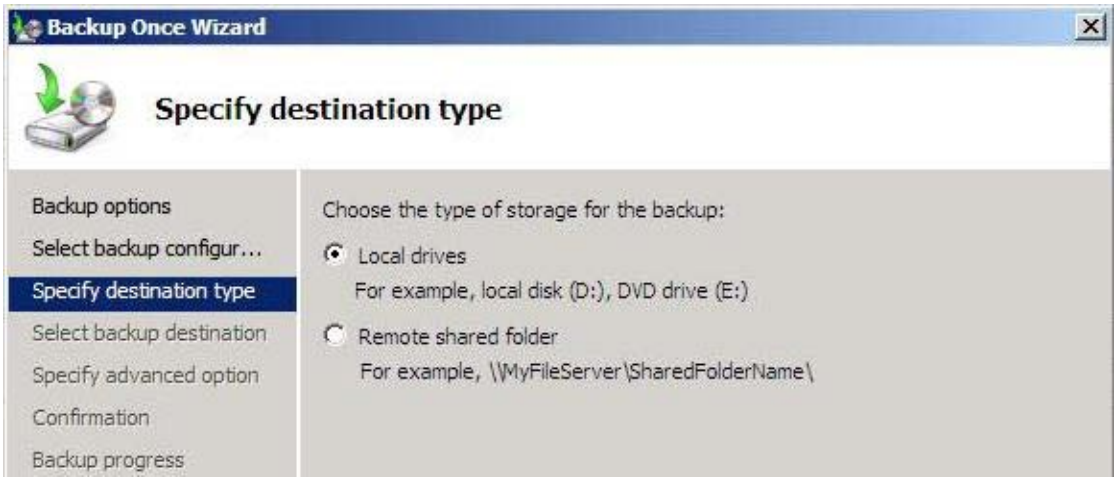
Kuva 24 Varmuuskopioitavien kohteiden valinta.

Ajastetun varmuuskopion voi ajastaa otettavaksi joko kerran tai useita kertoja päivässä ja ajankohta on valittavissa puolen tunnin välein (kuva 25). Kaupallisista varmuuskopiointiratkaisuista poiketen ajastuksia ei kuitenkaan voi määrittää otettavaksi eri viikonpäiville eri tavoin tai kerran kuussa täydellisenä ja muutoin ainoastaan muuttuneet tiedostot kopioivana tehtäväksi.



Kuva 25 Varmuuskopiointiajankohdan valinta.

Tehtäessä kertaluontoista varmuuskopiointia (*Backup Once*) palvelimesta ja sen tilasta optinen asema ja verkkojako ovat kuitenkin käytettävissä varmuuskopion tallennuspaikkana (kuva 26). Kertaluontoisen varmuuskopion kohteiksi on valittava niin ikään joko osio tai koko levy, yksittäisten kansioiden valinta ei ole mahdollista. Myös täydellinen järjestelmän varmuuskopiointi on mahdollista.



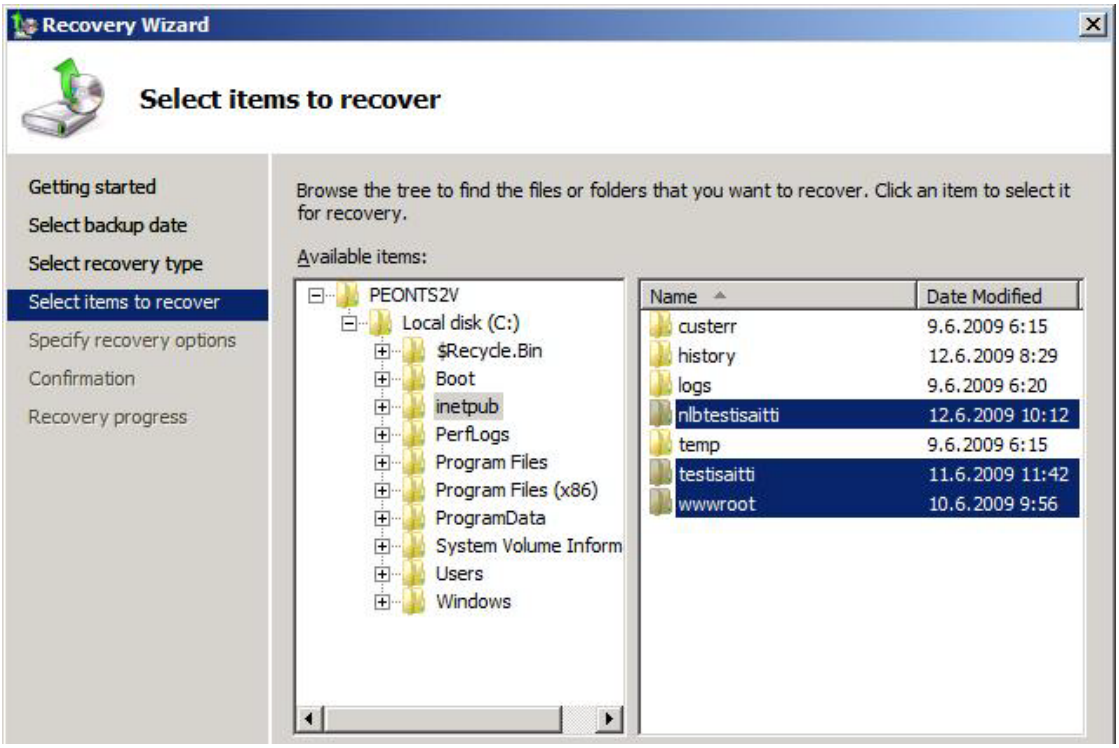
Kuva 26 Kertaluontoinen varmuuskopio voidaan tallentaa myös verkkojakoon.

Puutteistaan huolimatta Windows Server Backup on toimiva perustason varmuuskopiointiratkaisu, vaikkakin sen ominaisuudet voivat tuntua rajoittuneilta. Sillä tehdyt ulkoiselle kiintolevylle otetut ajastetut varmuuskopiot toimivat sekä täydessä että muuttuneiden tiedostojen varmuuskopioinnissa pienen tietojärjestelmän tarpeisiin nähden hyvin. Windows Server Backup:sta puuttuvat ominaisuudet on saatavilla Microsoftin tuotteesta Microsoft System Center Data Protection Manager (Zacker 2009).

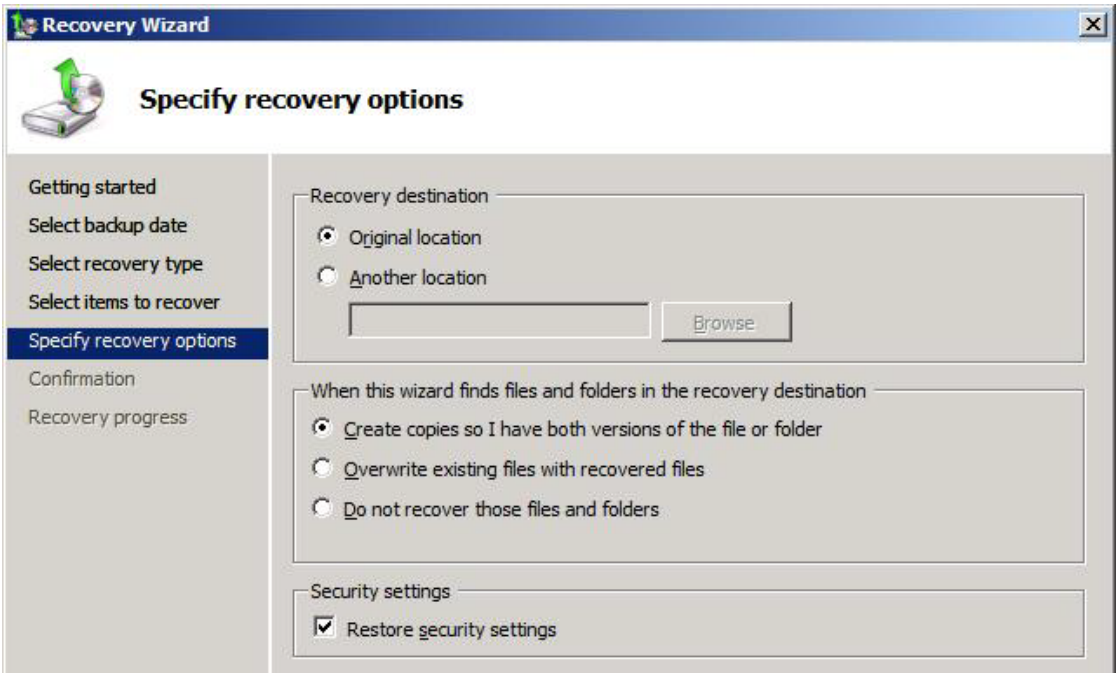
Kirjoitushetkellä käytössä olleen version seuraaja Windows Server 2008 R2 sisältää uusina ominaisuuksina muun muassa mahdollisuuden käyttää verkkojakoa ajastettujen varmuuskopioiden tallentamiseen sekä mahdollisuuden valita varmuuskopioitavat kansiot ja tiedostot koko osion sijaan. Nauhavarmistusta se ei kuitenkaan edelleenkään tue. (TechNet Backup and Recovery 2009.)

5.4.2 Varmuuskopioiden palauttaminen (Recovery)

Windows Server Backup -ohjelman Recover-toiminto on työkalu luotujen varmuuskopioiden palauttamiseen. Sen avulla on mahdollista palauttaa haluamansa osio (esimerkiksi koko C:\-asema) tai yksittäisiä kansioita ja tiedostoja (kuva 27) sekä sovelluksia. Palautustyökalu (kuva 28) mahdollistaa palautettavien tiedostojen ja kansioiden kopioimisen joko niiden alkuperäiseen tai käyttäjän määrittelemään uuteen sijaintiin ja siten, että palautettavat tiedot tarvittaessa korvaavat ennen palautusta luodut samannimiset tiedostot ja kansiot. Tällöin palautettava versio samannimisestä tiedostosta korvaa ko. sijainnissa jo olevan kirjoittamalla sen päälle. Palautus on mahdollista tehdä myös niin, että sekä palautettava että ennen palautusta olemassa oleva tiedosto ovat käytettävissä palautuksen jälkeen. Palautusvaiheessa on mahdollista säilyttää palautettavien tietojen käyttöoikeusmääritykset, joten niitä ei tarvitse enää palautuksen jälkeen manuaalisesti määrittää.



Kuva 27 Palautettavien kansioiden valinta.

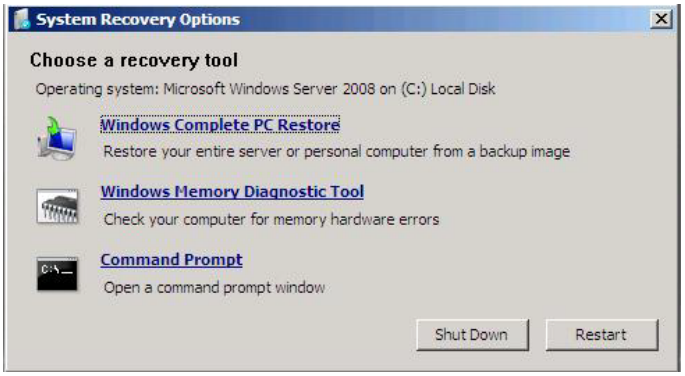


Kuva 28 Palautusvaiheessa tehtävät valinnat.

5.4.3 Palautusympäristö (Recovery Environment)

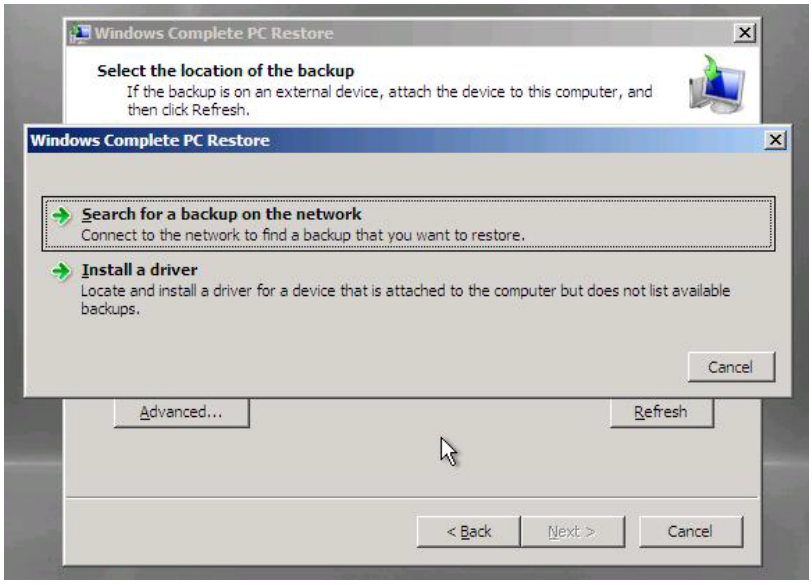
Edellä kuvattujen varmuuskopioiden palauttamistapojen lisäksi Server 2008:ssa on kokonaan oman tilansa tilanteisiin, joissa itse käyttöjärjestelmä ei enää käynnisty ollenkaan käyttöjärjestelmän vakavien virheiden tai muiden vastaavien ongelmien seurauksena. Tällaisessa tilanteessa ei ole esimerkiksi mahdollista käynnistää Windows Server Backup -ohjelmaa ja palauttaa tietoja ja tiedostoja käyttöjärjestelmän sisäisiä työkaluja käyttäen. Palvelimen uudelleenasennuksen ohella ainoa mahdollisuus järjestelmän toimintakunnon palauttamiseksi on Windows RE:ksi (*Recovery Environment*) kutsuttu tila, johon pääsemiseksi palvelin käynnistetään asennuslevyltä ja valitaan *Repair your computer* (kuva 29). Tämä avaa ohjatun toiminnon, jonka avulla koko palvelinkäyttöjärjestelmä voidaan palauttaa varmuuskopiosta toimivaan tilaan. Muut RE:n tarjoamat työkalut ovat muistin diagnosointi- ja komentokehotetyökalut, ks. kuva 30.

Kuva 29 RE:n käynnistäminen asennuslevyltä.

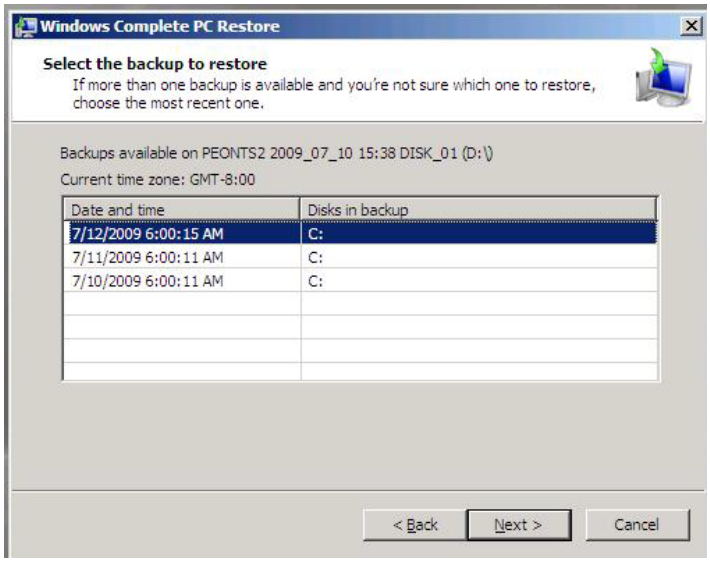


Kuva 30 RE:n toiminnot.

Valitsemalla palautustyökalun (*Windows Complete PC Restore*) ja etenemällä vaiheittain määritetään käytettävän varmuuskopion sijainti joko ulkoiselta kiintolevyltä tai verkkosijainnista (kuva 31). Valittavissa ovat kaikki valittuun tallennuspaikkaan tallennetut varmuuskopiot, ks. kuva 32.

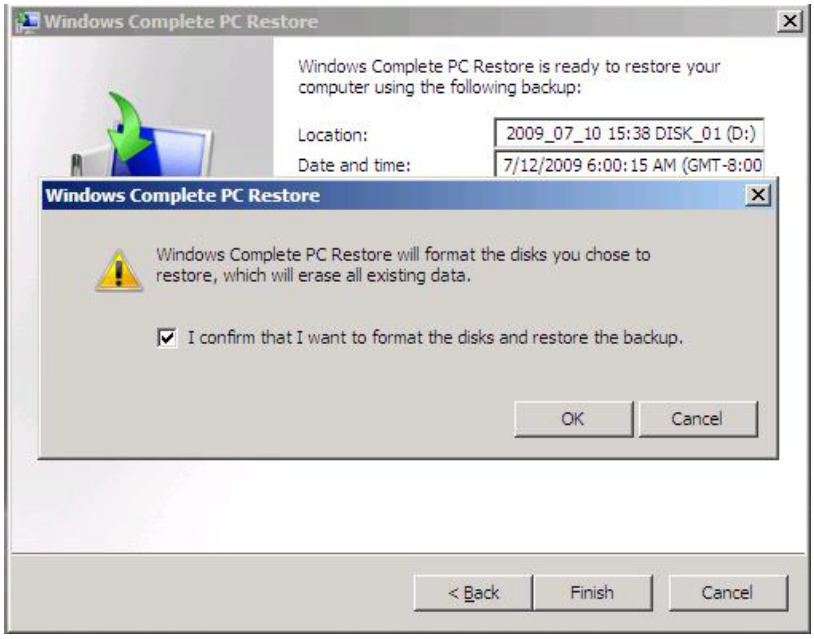


Kuva 31 Varmuuskopion sijainnin valinta.

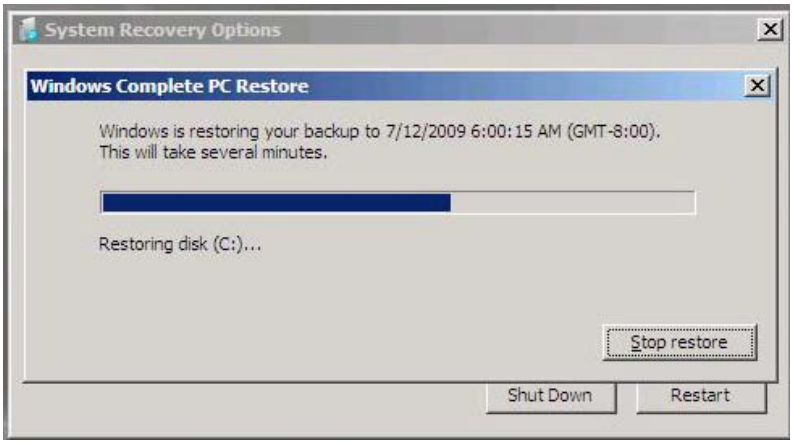


Kuva 32 Käytettävissä olevat varmuuskopiot.

Järjestelmän palautusvaiheessa kaikki kiintolevylle oleva tieto kirjoitetaan yli varmuuskopio-levykuvan (*image*) tiedoilla (kuva 33), kiintolevy osioidaan ja järjestelmä palautetaan varmuuskopiota vastaavaan tilaan (kuva 34).



Kuva 33 Tietojen ylikirjoittamisen varmistus.



Kuva 34 Järjestelmää palautetaan.

5.5 Hajautettu tiedostojärjestelmä (DFS)

Työskentelyorganisaation tietojärjestelmässä tiedostojen saatavuus ja käytettävyys ovat tehokkaan työskentelyn edellytys. Tietoverkossa voi olla useita verkkosijainteja, joissa tärkeät tiedostot ja tietokannat sijaitsevat ja joihin on oltava esteetön pääsy kaikille niitä tarvitseville mistä päin verkkoa tahansa. Verkkosijainteja on helppo lisätä kasvavien tiedostomassojen ja muiden tarpeiden mukaan, mutta verkossa sijaitsevien verkkojakojen lukumäärän kasvaessa tietyn tiedoston paikallistaminen voi käyttäjän näkökulmasta katsottuna tulla vaikeammaksi. Lisäksi ainoastaan yhdessä verkkosijainnissa sijaitsevan tiedoston käyttäminen on mahdotonta verkon tai sitä tarjoavan tiedostopalvelimen toiminnan häiriintyessä.

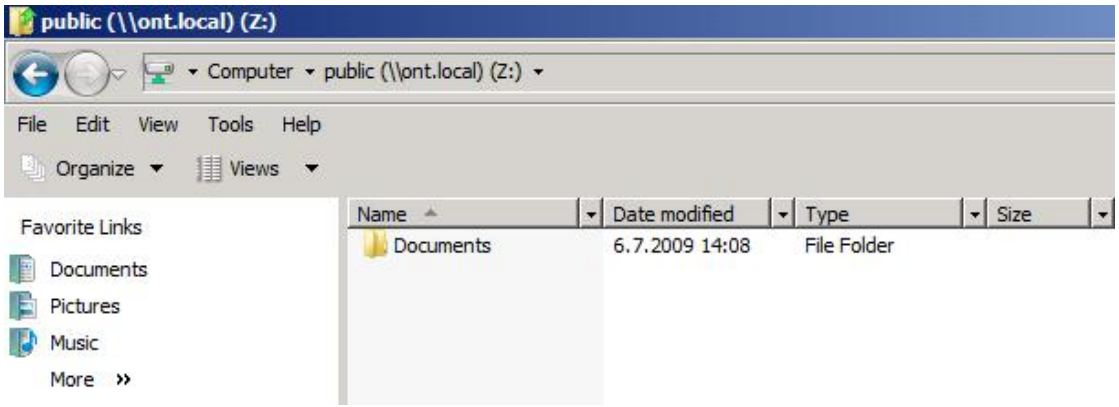
Windows-palvelinkäyttöjärjestelmissä usean verkkojaon yhdistäminen yhdeksi loogiseksi kokonaisuudeksi ja hajautettujen verkkojakojen käyttäminen on mahdollista. Perusteluna tiedostojärjestelmän hajauttamiseen voidaan nähdä esimerkiksi helpompi ylläpidettävyys ja verkkoliikenteen kuormituksen tasaaminen siten, että käyttäjä ohjataan käyttämään lähimmän toimipaikan (*site*) verkkojakoa sen sijaan, että käytettäisiin kauempana saman toimialueen sisällä sijaitsevia (TechNet DFS 2009).

Hajautettu tiedostojärjestelmä (DFS) muodostaa käyttäjälle yhtenä kokonaisuutena näyttäytyvän tiedostojärjestelmän, jonka tiedostot ja kansiot voivat sijaita usealla erillisellä tiedostopalvelimella. Käyttäjän ei tarvitse muistaa tai selata eri tiedostopalvelimien kansioita etsiessään haluamaansa tiedostoa. Ylläpitäjälle DFS mahdollistaa lisäksi tiedostojen varmuuskopioinnin verkon kautta keskitettyyn varmuuskopiointijärjestelmään (Zacker 2009).

Lisäksi Kivimäen (2005) mukaan ylläpito- tai huoltotehtäviä varten alas ajettavan palvelimen jaetut kansiot voidaan ohjata DFS:n avulla toiselle palvelimelle, jolloin käyttäjälle tiedostojen käytettävyys pysyy kaiken aikaa samanlaisena ilman niiden etsimistä erillisiltä palvelimilta.

5.5.1 Nimiavaruus

Nimiavaruus (*Namespace*) on käyttäjille yksi näkymä, joka kattaa DFS:n piirissä jaossa olevat kansio. Se on esimerkiksi muotoa *\\domain\Public* (kuva 35) , ja sen alikansiot ja tiedostot voivat sijaita fyysisesti useilla palvelimilla. (TechNet DFS Management 2009.) Nimiavaruus voidaan mieltää kokoelmana viittauksia eri tiedostopalvelimilla sijaitseviin kansioihin. Kun käyttäjä käyttää ko. resursseja, DFS-palvelin ohjaa hänet viittauksen mukaiselle tiedostopalvelimelle. (Zacker 2009.)



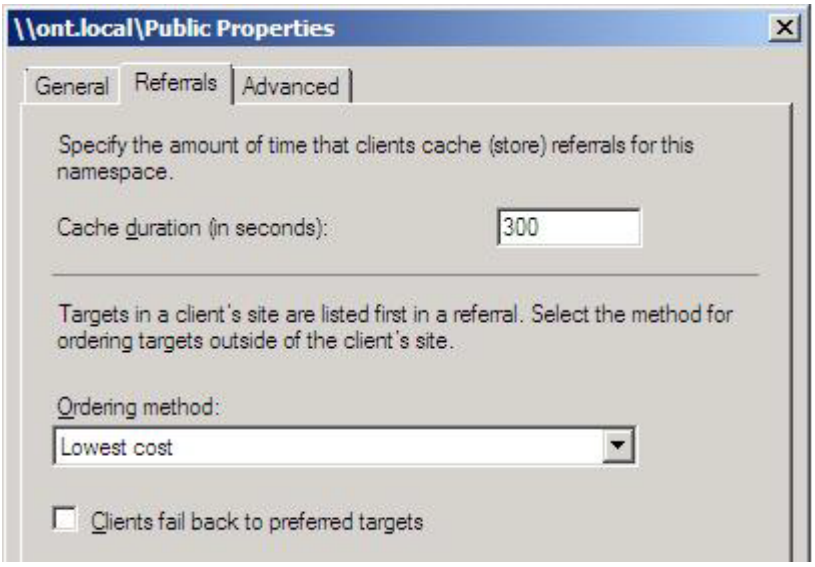
Kuva 35 Verkkoasema käyttäjän näkökulmasta.

5.5.2 Replikointi

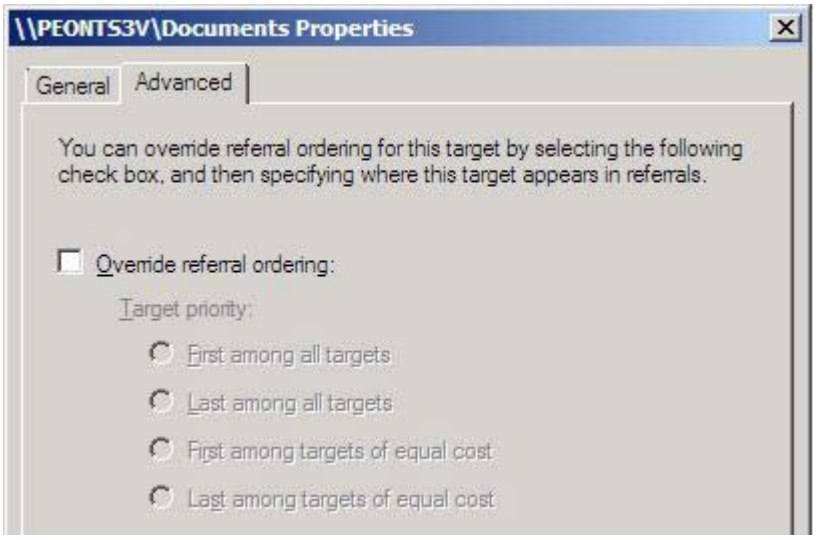
DFS-konfiguraatiossa replikoinnilla tarkoitetaan tiedostojen kopioimista eri tiedostopalvelimille ja kopioiden samanlaisiksi synkronoituna pitämistä. Replikoinnin suurimmat hyödyt liittyvät tiedostojen käytettävyyden parantamiseen ja verkkokuormituksen tasaamiseen. Suurissa organisaatioissa toimipaikat voivat olla erillään toisistaan ja organisaation yhteisten verkkoresurssien käyttämisessä voi olla verkkoviiveitä, mikäli tiedostot sijaitsevat ainoastaan yhdessä tietyssä verkon osassa. Lisäksi tällaisessa tilanteessa yhden ainoan tiedostopalvelimen toimintakyky voi häiriintyä suuren käyttäjämäärän vuoksi.

Replikointi ohjaa tiettyä tiedostoa pyytävän käyttäjän käyttämään verkossa lähimpänä sijaitsevan replikointipalvelimen tiedostoja. Näin käyttäjän kokema verkkoviive pysyy mahdollisimman pienenä ja verkkoliikenteen kuormitus jakautuu useille tiedostopalvelimille. (Zacker 2009.)

Ohjaus haluttuun replikointipalvelimeen määräytyy nimiavaruuden ja replikointiryhmän jäsenkoneiden *referral*-asetusten mukaisesti. Se määrittää järjestyksen, jossa replikointipalvelimia käytetään ja täten tehostaa verkon käyttöä. Tietyn resurssin käyttämistä edellyttävän verkon kuormittavuusastetta kuvataan termillä *cost* ja mitä pienempi *cost*-arvo on, sitä vähemmän kyseisen verkkoresurssin käyttäminen verkkoa kuormittaa. Käyttäjä ohjataan lähtökohtaisesti käyttämään lähimmän toimipaikan (*site*) verkkoresursseja. Mikäli sitä ei kuitenkaan haluta käyttää tai se ei ole ollenkaan käytettävissä, käyttäjä ohjataan helpoiten saatavilla olevalle (*lowest cost*) replikointipalvelimelle, ks. kuva 36. Vaihtoehtoisesti verkkoliikenne voidaan, huolimatta lähimmän palvelimen saatavuudesta, aina ohjata tietylle replikointipalvelimelle (kuva 37). Tällöin *referral*-asetus ohitetaan (*override*) ja tietty palvelin asetetaan etusijalle. (TechNet DFS Management 2009.) Perusteluna tälle voidaan nähdä tietyn palvelimen parempi suorituskyky ja palvelevuus.

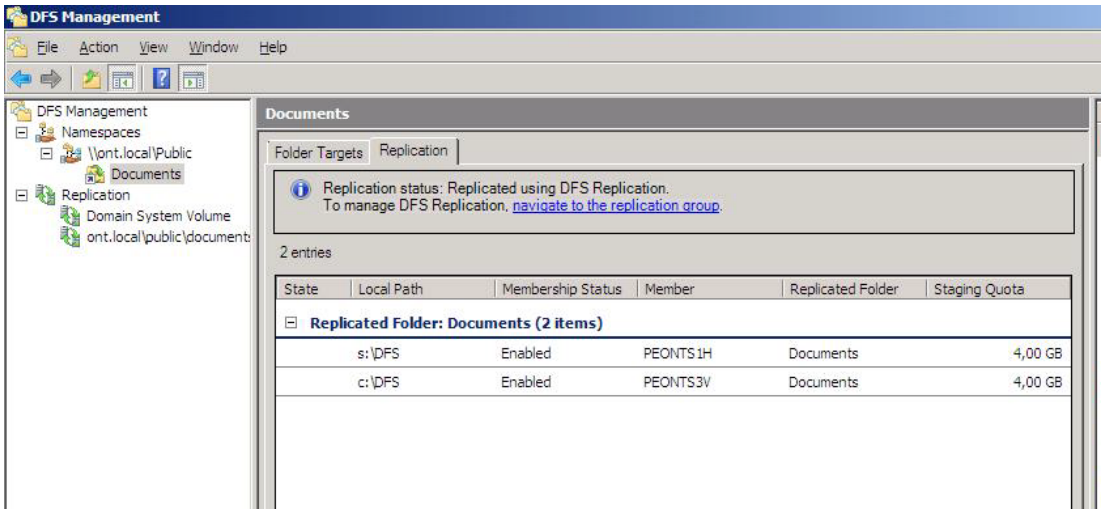


Kuva 36 Käytettävän replikointipalvelimen valinta.



Kuva 37 Haluttu replikointipalvelin voidaan asettaa ensisijaisesti käytettäväksi.

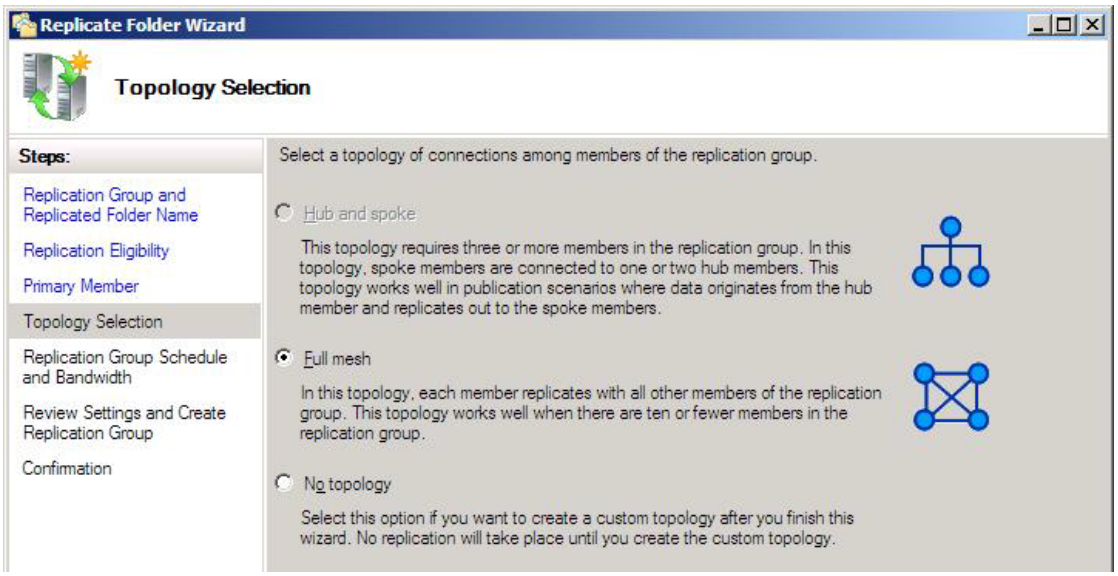
Tiedostopalvelinten välillä tapahtuva replikointi synkronoi jaossa olevien kansioiden tiedostot replikointiin osallistuvien palvelinten muodostaman replikointiryhmän (*Replication Group*) välillä. Kuvassa 38 nimiavaruuden jäsenkoneet *PEONTS1H* ja *PEONTS3V* muodostavat kahden jäsenen replikointiryhmän, joiden välillä nimiavaruuden kansio *ont.local\Public\Documents* replikoidaan. Molempien jäsenten paikallisilla levyillä on kopio ko. kansiosta ja johon tehdyt muutokset päivittyvät jatkuvasti lähiverkon yli ts. muutokset kopioidaan jäsenkoneelta toiselle. Vaihtoehtoisesti replikointi on myös mahdollista ajastaa halutun aikataulun mukaan tapahtuvaksi (kuva 39).



Kuva 38 Replikointiryhmän jäsenkoneet.

Kuva 39 Replikoinnin ajankohdan valinta.

Replikointi skaalautuu organisaation koon mukaan. Windows Server 2008:n replikointiryhmässä voi olla jopa 256 jäsentä ja 256 replikoitua kansiota ja jokainen tiedostopalvelin voi olla jäsenenä 256 eri replikointiryhmässä. Replikointiryhmän jäsenten välillä tapahtuva verkkoliikenne noudattaa ryhmän luontivaiheessa valittua topologiamallia. Vaihtoehdoista *Full Mesh* replikoi jaettuja resursseja kaikilta kaikille, ks. kuva 40. Suuriin organisaatioihin paremmin soveltuva topologiamalli *Hub and Spoke* replikoi kansioita yhdeltä monelle ja siten kuormittaa vähemmän verkkoa. (Zacker 2009.)

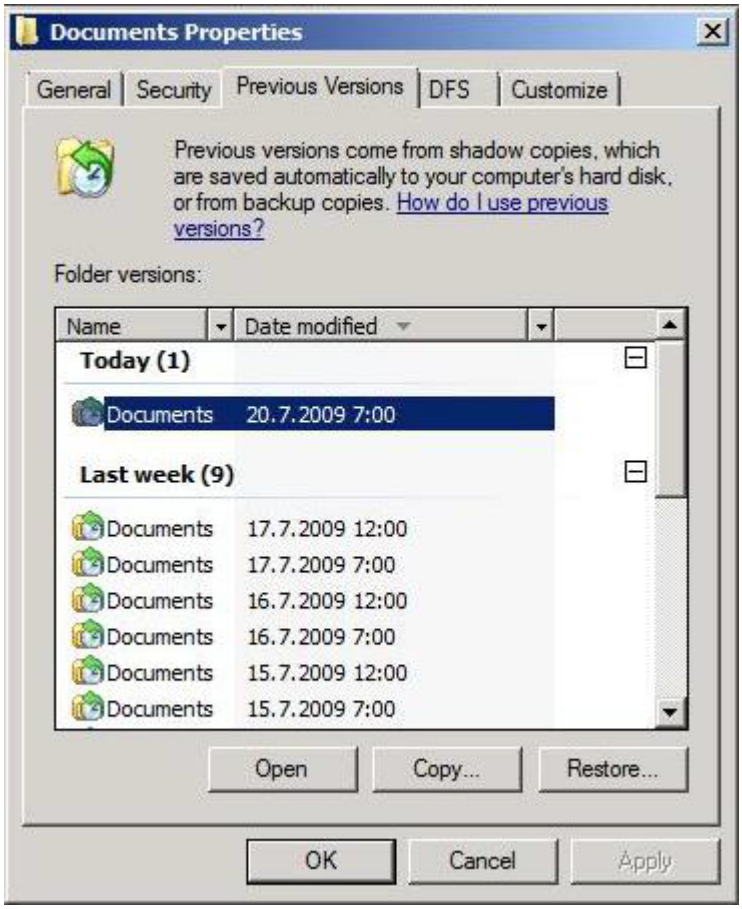


Kuva 40 Replikoinnin topologiamalli.

5.6 Varjokopiot (Shadow Copies)

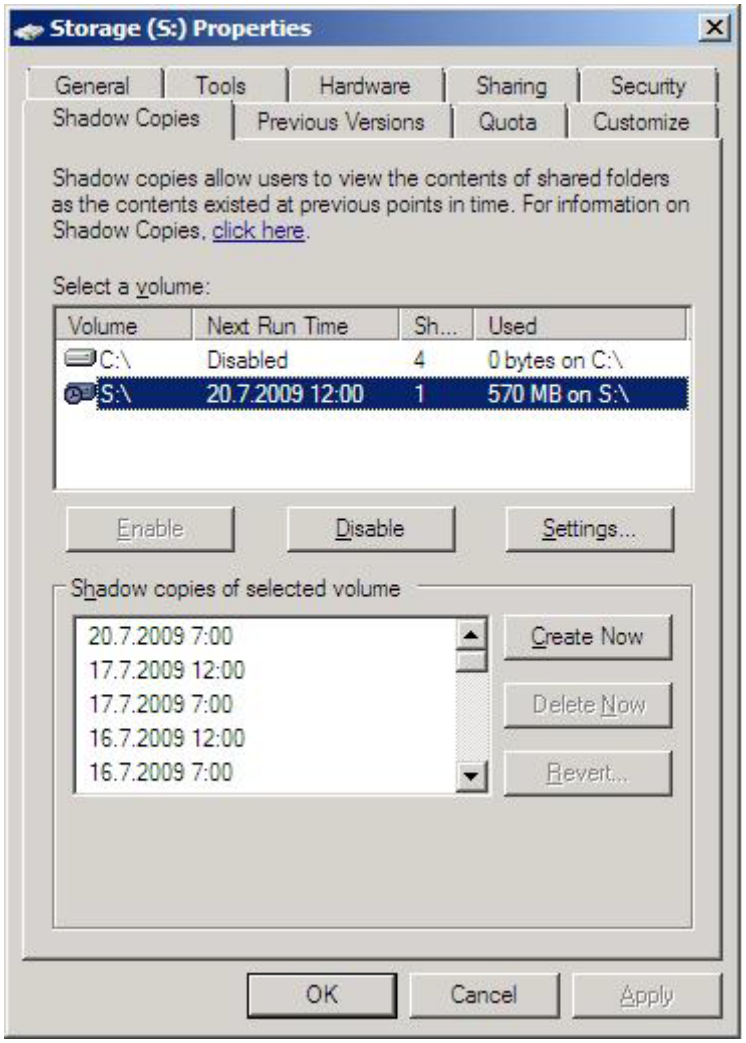
Olennaisena osana tietojärjestelmän toimintaa ovat sen käyttäjien omat tiedostot. Koska jokaisella käyttäjällä on yleensä omiin tiedostoihinsa täydet käyttöoikeudet, vahingossa tehtyjä poistoja ja virheellisiä muokkauksia tapahtuu. Näiden tiedostojen aikaisempien versioiden palauttaminen varmuuskopiointimedioilta on järjestelmänvalvojien työtaakkaa turhaan kasvattava tehtävä. Käyttäjän vahingossa poistaman tiedoston palauttamiseen käytettynä aikana tiedosto ei ole saatavissa, mikä heikentää työskentelyn tehokkuutta.

Windows Server 2008:n Shadow Copies eli varjokopiot mahdollistavat tiedostojen ja kansioiden aikaisempien versioiden (*Previous Versions*) tehokkaan ja käyttäjäystävällisen hallinnan. Varjokopiot ovat tietyllä ajanhetkellä automaattisesti otettuja kopioita määritetyistä tiedostoista. Ajankohdat ja kopiointipalvelun aikataulu ovat tarvittaessa muokattavissa. Otetut kopiot tallennetaan verkkoon esimerkiksi tiedostopalvelimelle, josta niiden keskitetty hallinta on mahdollista. Versionhallinnan avulla ylläpitäjä tai yleensä käyttäjä itse voi palauttaa haluamansa tiedoston tai kansion aikaisempaan versioon vahingossa tapahtuneen poistamisen tai virheellisen muokkauksen vuoksi. Lisäksi versioiden välisten muutosten vertailu on varjokopioita käyttäen mahdollista. Kuvassa 41 käyttäjän näkymä testausympäristön kansion *Documents* varjokopioista.



Kuva 41 Varjokopiot käyttäjän näkökulmasta.

Windows Server 2008:ssa varjokopioiden käyttämisessä on kuitenkin tiettyjä rajoitteita. Kuten kuva 42 osoittaa, niitä otetaan aina kokonaisista levyistä tai levyosioista yksittäisten tiedostojen tai kansioiden sijaan. Varjokopiointi ei saa korvata säännöllisten varmuuskopioiden ottamista, sillä tallennettuja versioita voi olla korkeintaan 64 kappaletta ja niille osoitetun tilan loputtua aikaisempia versioita poistetaan vanhimmasta alkaen tilan vapauttamiseksi uusia varten. (TechNet Shadow Copies 2009.)



Kuva 42 Varjokopioita otetaan aina levy- tai osiokohtaisesti.

6 POHDINTA

Opinnäytetyössäni selvitettiin yleisellä tasolla mitä tietojärjestelmän luotettavuus ja toimintavarmuus tarkoittaa, mitä se edellyttää ja millaisin teknisin ja inhimillisin ratkaisuin sitä voidaan parantaa. Käytännön osiossa kuvataan millaisia työkaluja edellä mainittuihin tarpeisiin Windows Server 2008 tarjoaa. Lisäksi esitellään niiden asentamiseen ja konfigurointiin liittyviä seikkoja ja omia työn tekemisen aikana ilmi tulleita omakohtaisia huomioita ja havaintoja.

Työn käytännön osio on kirjoitettu osin käyttöohjemaisella otteella johtuen lähdemateriaalien tyylistä ja siitä, että käsitellyt asiat ovat monilta osin itselleni ennestään tuntemattomia. Työssä esiteltyjen toimintojen dokumentointi on edellyttänyt perusteellista pohjatyötä niin lähdemateriaaliin perehtymisen kuin testausympäristössä tehtyjen asennusten muodossa. Windows Server 2008 sisältää toimintoja ja konfigurointivaihtoehtoja, joiden ymmärtäminen ja toimintakuntoon asentaminen omassa testausympäristössä on oma lukunsa, eikä niiden testaaminen sujunut täysin ongelmitta. Testausympäristön laitteisto rajoitti vikasietoisen klusterikonfiguraation toteuttamista käytännössä siinä määrin, että sen omakohtainen testaaminen ei onnistunut, joten ko. toimintoa käsittelevä luku pohjautuu pääosin www-lähteisiin. Muiden esiteltyjen toimintojen asennukset ja toiminnallisuus on todennettu omassa testausympäristössä.

Asennus- ja testausvaiheessa käytössä ollut periaate ottaa kuvankaappaus jokaisesta työvaiheesta osoittautui hyväksi ratkaisuksi, sillä kuvilla havainnollistetut asennus- ja konfigurointivaiheet ovat auttaneet laajojen asiakokonaisuuksien hahmottamista ja asian sisäistämistä. Kuvien pariin on lisäksi helppo palata myöhemmin kun jokin seikka kaipaa tarkempaa tutkimista. Tämä selittää omalta osaltaan myös lopulliseen työhön päätyneiden kuvien runsaan lukumäärän ja tukee entisestään työn käyttöohjemaista tyyliä.

Myös se, että opinnäytetyössä käsiteltyjä toimintoja ja ominaisuuksia on useita ohjaa siihen, että kulloinkin käsillä olevaa asiaa kuvataan enemmän yleisimpien toiminnallisuuksien kannalta kuin hyvin tarkkoja teknisiä seikkoja painottaen. Lisäksi asennusvaiheiden pienimpien yksityiskohtien kuvaaminen jätetään pääsääntöisesti

pois. Työn lukijalta odotetaan siis perusymmärrystä palvelinten ja palvelinroolien toiminnoista sekä yleiskäsitystä IT-alan termeistä.

Työn lopputuloksena todettakoon, että Windows Server 2008 sopii hyvin tietojärjestelmän palvelinten käyttöjärjestelmäksi myös silloin, kun edellytyksinä ovat korkean luotettavuuden kriteerit ja soveltuvuus vikasietoiseen palvelinkokoonpanoon. Sen tarjoamista työkaluista erityisesti verkkokuorman tasaaminen ja vikasietoinen klusterointi soveltuvat hyvin tietojärjestelmän palveluiden vikasietoisuuden ja toimintavarmuuden parantamiseen. Myös muut tässä työssä esitellyt ominaisuudet mahdollistavat palvelujen korkean käytettävyyden ja saatavuuden tietojärjestelmän käyttäjille ja ylläpitäjille. Ainoastaan käytettävissä olleen käyttöjärjestelmäversion varmuuskopiointityökalu (Windows Server Backup) on selvästi puutteellinen ja toiminnoiltaan rajoittunut.

Kirjoitushetkellä käytettävissä ollut Windows Server:n versio saa seuraajan vuoden 2009 lokakuun lopussa, kun Windows Server 2008 R2 julkaistaan. Se tuo mukanaan joitain uusia ominaisuuksia, jotka liittyvät myös tässä opinnäytetyössä käsiteltyihin ominaisuuksiin, mukaan lukien parannukset Windows Server Backup -toiminnoissa. Aikataulusyistä johtuen R2:n ominaisuuksia ei tässä työssä kuitenkaan esitellä.

Opinnäytetyön tekemisen aikana olen saanut ja joutunut käyttämään kaikkea opintojeni ja ennen kaikkea työharjoitteluni aikana oppimaani laitteistotekniikasta palvelinten toimintaan ja lähiverkkotekniikan kautta suunnittelutyökalujen käyttöön. Lisäksi omatoimisen opiskelun osuus opinnäytetyön aikana on korostunut aivan eri tavoin kuin perusopetuksen aikana. Sain työskennellä omana esimiehenäni koko opinnäytetyöprosessin ajan, mikä näkyi niin hyvässä kuin pahassakin. Tein itsenäistä työskentelyä, jolloin vastuu projektin etenemisestä oli koko ajan itselläni. Lopputulokseen voin sanoa olevani tyytyväinen siitäkin syystä, että Windows Server 2008 tulee hyvin todennäköisesti olemaan käytössäni työelämässä seuraavien vuosien aikana ja koko opinnäytetyöprosessi on ollut erinomaista harjoitusta sen uusien toiminnallisuuksien opetteluun ja sisäistämiseen.

LÄHTEET

Amazon EC2 2009

Verkkodokumentti. Luettu 6.8.2009. Amazon Web Services. http://aws.amazon.com/ec2-sla/.

Crichlow, J. 2001

Hajautetut tietojärjestelmät. Suomentanut Erkki Huru. IT Press. Helsinki.

Continuity Central 2009

Verkkodokumentti. Luettu 1.9.2009. Continuity Central. http://www.continuitycentral.com/feature0267.htm.

Hakala, M., Vainio, M. & Vuorinen, O.2006

Tietoturvallisuuden käsikirja. Docendo. Jyväskylä.

Jaakohuhta, H. 2003

Tietojärjestelmien luotettavuus. IT Press. Helsinki.

Kivimäki, J. 2005

Windows Server 2003 Tehokas hallinta. Readme. Helsinki.

Matthews, M. 2008

Microsoft Windows Server 2008: A Beginner's Guide. McGraw-Hill. USA.

TechNet Backup and Recovery 2009

Verkkodokumentti. Luettu 15.7.2009. Microsoft. http://technet.microsoft.com/en-us/library/dd979562(WS.10).aspx#BKMK_Windows_Server_Backup_overview.

TechNet DFS 2009

Verkkodokumentti. Luettu 16.7.2009. Microsoft.
http://technet.microsoft.com/en-us/library/cc753479(WS.10).aspx.

TechNet DFS Management 2009

Verkkodokumentti. Luettu 16.7.2009. Microsoft.
http://technet.microsoft.com/en-us/library/cc732006(WS.10).aspx.

TechNet Edge 2009

Verkkodokumentti. Luettu 15.7.2009. Microsoft
http://edge.technet.com/Media/Network-Load-Balancing-NLB-in-Windows-Server-2008.

TechNet Example, Clustered File or Print Server 2009

Verkkodokumentti. Luettu 17.8.2009. Microsoft
http://technet.microsoft.com/en-us/library/dd197557(WS.10).aspx.

TechNet Failover Clusters 2009

Verkkodokumentti. Luettu 20.7.2009. Microsoft
http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx.

TechNet NLBa 2009

Verkkodokumentti. Luettu 14.8.2009. Microsoft
http://technet.microsoft.com/en-us/library/cc757731(WS.10).aspx.

TechNet NLBb 2009

Verkkodokumentti. Luettu 14.7.2009. Microsoft.
http://technet.microsoft.com/en-us/library/cc786264(WS.10).aspx.

TechNet NLBc 2009

Verkkodokumentti. Luettu 15.7.2009. Microsoft.
http://technet.microsoft.com/en-us/library/cc770870.aspx.

TechNet Server 2003 Product Overview 2009

Verkkodokumentti. Luettu 3.8.2009. Microsoft.
http://technet.microsoft.com/fi-fi/windowsserver/bb429524(en-us).aspx.

TechNet Shadow Copies 2009

Verkkodokumentti. Luettu 16.7.2009. Microsoft.
http://technet.microsoft.com/en-us/library/cc771305(WS.10).aspx.

TechNet Windows 2000 Server 2009

Verkkodokumentti. Luettu 3.8.2009. Microsoft.
http://technet.microsoft.com/en-us/library/bb727159.aspx.

Techotopia 2009

Verkkodokumentti. Luettu 12.6.2009.Techotopia.
http://www.techotopia.com/index.php/Building_a_Windows_Server_2008_Network_Load_Balancing_Cluster.

TechRepublic 2009

Verkko-opas. Luettu 2.9.2009. TechRepublic.
http://content.techrepublic.com.com/2346-10878_11-251086-1.html.

Shapiro, J. & Polich, M. 2004

Building High Availability Windows Server 2003 Solutions. Addison-Wesley. USA.

Stanek, W. 2003

Microsoft Windows Server 2003. Asiantuntijan käsikirja. Suomentanut Tapani Lahtinen. IT Press. Helsinki.

Windows Products and Technologies History 2009

Verkkodokumentti. Luettu 3.8.2009. Microsoft.
http://www.microsoft.com/windows/WinHistoryServer.mspx.

Windows Server 2008 R2 2009

Verkkodokumentti. Luettu 17.8.2009. Microsoft.

http://www.microsoft.com/windowsserver2008/en/us/R2.aspx.

Zacker, G. 2009

Microsoft Official Academic Course, Windows Server 2008 Administrator, Microsoft Certified IT Professional Exam 70-646. Wiley. USA.

LIITE 1 Testausympäristön rakennekuva