HAAGA-HELIA
ammattikorkeakoulu

Hajautetun sovelluksen suunnittelu ja mallinnus System Center Operations Manager 2007 R2 avulla

Antti Toivanen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2011

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

Tekijä tai tekijät Antti Toivanen	**Ryhmätunnus tai aloitusvuosi** HETI10SIM3
Raportin nimi Hajautetun sovelluksen suunnittelu ja mallinnus System Center Operations Manager 2007 R2 avulla	**Sivu- ja liitesivumäärä** 44 + 6
Opettajat tai ohjaajat Ahti Kare	

Yritysten ydinliiketoiminta on nykypäivänä yhä riippuvaisempaa tietojärjestelmien ja tietoteknisten palveluiden toiminnasta. Tietotekniset palvelut ovat suuntautumassa entistä enemmän suoraan kriittisten liiketoimintojen valvontaan. Palvelukatkosten välttäminen ongelmatilanteita ennakoimalla sekä jo syntyneisiin ongelmiin nopeasti reagoiminen ovat avainasemassa.

Tämä opinnäytetyö tehtiin osana monivaiheista projektia suoraan kohdeyrityksen verkkoympäristöön. Sen tarkoituksena oli määritellä ja mallintaa hajautettu sovellus. Hajautettu sovellus ei ole yksittäinen ohjelma tai palvelu, vaan useammassa järjestelmän koneessa olevien ohjelmakomponenttien yhteistoiminnallinen sovellus. Palvelutarpeiden vaihdellessa sen komponentteja on voitava ladata dynaamisesti eri koneille.

Opinnäytetyön tutkimusosuudessa käsiteltiin palveluiden hallintaa tietotekniikkayksikön sekä liiketoiminnan näkökulmasta ja Case-osuudessa suunniteltiin ja mallinnettiin hajautettu sovellus Extranet-ympäristöstä, joka jatkossa otetaan mukaan keskitetyn hallinnan ja monitoroinnin piiriin. Hallintaohjelmistona on Microsoftin System Center Operations Manager 2007 R2.

Hallintaohjelmistoilla haetaan automatiikkaa ja kokonaisvaltaisuutta, jossa useampaa verkon kriittistä komponenttia hallitaan keskitetysti. Operations Managerin käyttämä tekniikka sisältää parhaita käytäntöjä palvelunhallintaan. Suurimmat edut ovat ongelmien ennaltaehkäisyn parantuminen sekä henkilöstöresurssien käytön tehostuminen.

Tutkimuksen, määrittelyn ja mallinnuksen avulla todettiin, että Microsoftin System Center Operations Manager 2007 R2 on hyvä valinta palveluiden hallinnan automatisointiin ja valvontaan. Sen avulla saadaan merkittäviä etuja siirryttäessä reaktiivisesta toiminnasta kohti proaktiivista toimintaa, mutta se vaatii huolellista suunnittelua ja testaustyötä. Tämän työn jälkeinen vaihe projektissa tulee olemaan valvontaprosessien testaaminen ja mallinnetun sovelluksen ottaminen monitoroinnin alaisuuteen.

Asiasanat
Järjestelmänhallinta, Verkonhallinta, Palvelimet, Tietokannat, ATK-ohjelmat

HAAGA-HELIA
University of Applied Sciences

Abstract

Authors Antti Toivanen	**Group or year of entry** HETI10SIM3
The title of thesis Designing and modeling of distributed application with System Center Operations Manager 2007 R2	**Number of pages and appendices** 44 + 6
Supervisor(s) Ahti Kare	

Companies' core business today are increasingly dependent activities of information systems and IT-services, which are more and more focused on critical business issues. The key roles are to avoid service interruptions by anticipating problem situations and taking care of existing problems as quickly as possible.

The purpose of this thesis was to process service management from IT and business perspective and also define and model a distributed application into company's veritable network environment. A distributed application is not a single program or service, but a co-operative application which runs on several machines at the same time.

In this thesis there were two main subjects processed: the service management from IT and business perspective and how to design and model a distributed application of the extranet environment, which will be controlled and monitored later. The management software is Microsoft System Center Operations Manager 2007 R2.

Operations Manager provides a reliable and versatile solution for centralized management and for anticipating network problems. The techniques used by Operations Manager will bring the pieces of IT-infrastructure together and control them as a whole.

After researching, defining and modeling the conclusion of this thesis was that Microsoft System Center Operations Manager 2007 is an excellent choice for service management automation and monitoring. A company can achieve many instant benefits in a short period of time, but a transition from reactive activity to proactive needs studious planning and testing.

Key words
System management, Network management, Servers, Databases, Software

Sisällys

1 Johdanto

Informaatioteknologian hallinta yrityksissä on suuntautunut viime vuosina entistä enemmän yksittäisten palveluiden ja laitteiden hallinnasta moninaisten hajautettujen ympäristöjen hallintaan. Tällaiseen ympäristöön voi kuulua kymmeniä eri laitteita ja sovelluksia, fyysisiä tai virtuaalisia, jotka kommunikoivat keskenään tai ovat jotenkin riippuvaisia toisistaan. Samalla laitekannat kasvavat ja palvelinten ylläpito sekä palveluiden valvonta vie kasvavassa määrin resursseja.

Tällöin syntyy tarve laajentuneen IT-infrastruktuurin keskitetylle hallinnalle. Eräs tärkeimmistä seikoista on mahdollisten vikatilanteiden ennakoiminen jo ennen niiden toteutumista. Tällainen valvonta on työlästä ja aikaa vievää ilman asiaan kuuluvaa ohjelmistoa. Tämän opinnäytetyön projektissa ohjelmistoksi on valittu Microsoftin System Center Operations Manager 2007 R2. Valinta oli luonteva, kun käytössä on jo ennestään järjestelmänhallintatuotteena System Center Configuration Manager.

Opinnäytetyössä selvitetään, mitä palveluiden hallinnalla tarkoitetaan liiketoiminnassa ja miksi sen tehostaminen on tärkeää. Aina ei ymmärretä IT-palvelunhallinnan tärkeyttä osana kokonaisvaltaista liiketoimintaa, mutta sen pitäisi olla nimenomaan räätälöity tuottamaan ja tukemaan palveluita, jotka vaikuttavat suoraan jokapäiväisiin organisaation ydinliiketoiminnan vaatimuksiin. Lisäksi selvitetään mikä on hajautettu sovellus ja miten sellaisen määritys ja mallinnus toteutetaan, kun käytössä on Operation Manager -hallintaohjelmisto. Hallintaohjelmistosta käydään läpi olennaisimmat seikat sekä niitä ominaisuuksia, jotka liittyvät työn Case osuuteen.

Kohdeyritys tarjoaa palveluita Suomessa seitsemällä eri toimialalla. Nämä ovat energia ja ilmasto, infra ja liikenne, rakennukset ja rakenteet, teollisuus ja öljy/kaasu, vesi ja ympäristö, IT ja tietotekniikka sekä johdon konsultointi. Sen liikevaihto oli vuonna 2009 noin 90 miljoonaa euroa. Yrityksellä on Suomessa 25 toimipistettä, joissa on palvelimia noin 100 ja työasemia yhteensä lähes 1500. Palvelimissa on mukana muun muassa nimi-, tiedosto-, tulostin-, sekä lisenssipalvelimia.

1.1 Opinnäytetyön tavoitteet ja tarkoitus

Idea opinnäytetyölle lähti yrityksen tarpeesta hyödyntää laajemmin System Center Operations Manager 2007 R2 hallintatyökalua. Lähtötilanteessa ohjelmisto oli asennettu omalle palvelimelleen ja otettu tuotantokäyttöön niin, että sen avulla valvottiin yksittäisiä palvelimia ja verkon aktiivilaitteita. Työn tavoitteeksi asetettiin hajautetun sovelluksen määrittely ja mallinnus, joka voitaisiin jatkossa ottaa loogisena kokonaisuutena Operations Manager:n monitoroinnin piiriin. Tällä lähdettiin hakemaan syvemmin proaktiivisuutta, joka pitkällä aikavälillä vapauttaa IT-yksikön resursseja muuhun toimintaan sekä nostaa liiketoimintakriittisten palveluiden valvonnan tason korkeammalle.

Opinnäytetyö perustuu kohdeyrityksen todelliseen tarpeeseen saada ulotettua valvonta hajautetulle sovellukselle, jota käyttävät sekä yrityksen henkilöstö kuin myös asiakkaat. Työ on kieliasultaan melko teknistä ja sisältää paljon tietoteknisiä termejä, joiden ymmärtäminen on oleellista kokonaisuuden hahmottamiseksi. Keskeisimmät termit ovat selitetty lyhyesti liitteessä yksi ja kaikista oleellisimmat termit kappaleessa 1.4.

Opinnäytetyön tarkoitus on antaa lukijalle käsitys IT-palveluidenhallinnan merkityksestä liiketoiminnalle sekä Operations Managerin mahdollisuuksista hajautetun sovelluksen valvonnassa. Työ soveltuu parhaiten esimerkkinä henkilöille, jotka työskentelevät tietoteknisellä alalla ja joilla on jo hieman kokemusta IT-järjestelmien hallinnasta.

1.2 Työn rajaus

Opinnäytetyössä keskitytään teoriatasolla palvelunhallintaan sekä perustasolla hallintaohjelmiston toimintaan. Käytännön produktiin kuuluu hajautetun sovelluksen (distributed application) määrittely ja mallinnus. Työssä ei esitellä kaikkia Operations Managerin ominaisuuksia ja mahdollisuuksia, eikä siinä käsitellä sen asennusprosessia palvelimelle. Ohjelmiston kokonaisvaltaista käyttöönottoa ei myöskään esitellä yksityiskohtaisesti, koska vaatimukset ovat erilaisia eri ympäristöissä. Työssä käsitellään IT-palveluiden hallintaa pohjautuen ITIL-, ja MOF-kehyksiin (kappaleet 2.1 ja 2.2), koska Operations Managerin toimintalogiikka on rakennettu niiden pohjalta. Lisäksi esitellään Operations Manager yleisesti sekä tutkitaan sen sopivuutta yrityksen kriittisten palveluiden valvon-

nan työvälineeksi. Työstä on jätetty pois myös kilpailevien tuotteiden vertailu, koska Operations Manager oli valittu jo aiemmin hankittavaksi yhteensopivuuden ja lisenssisopimusten vuoksi.

1.3 Aineisto ja tutkimusmenetelmät

Tutkimuksen teoria-aineisto ja lähdemateriaalit ovat pääosin englanninkielisiä. Lisäksi lähes kaikki materiaali on tuotekohtaista, manuaalityyppistä materiaalia, jota on vaikea kyseenalaistaa tai kritisoida muihin lähteisiin vedoten. Tämä onnistuisi esimerkiksi vertailemalla kilpailevia tuotteita valitun ohjelmiston kanssa, mutta tässä projektissa se ei tullut kyseeseen. Aiheesta ei ole koulutusyritysten materiaaleja lukuun ottamatta juurikaan saatavilla suomenkielistä kirjallisuutta. Lähdemateriaali koostuu pääosin verkkojulkaisuista ja Microsoftin tuottamista materiaaleista, koska niitä on runsaasti tarjolla ja ne ovat usein hyvin yksityiskohtaisia. Tämänkaltaisessa aiheessa on luonnollista, että verkkomateriaali on hallitsevassa roolissa, koska se on helposti päivitettävissä. Ongelmaksi voi koitua linkkien poistuminen tai sijainnin vaihtuminen ja sitä kautta niiden toimimattomuus. Työskentely tapahtuu tietokoneympäristössä, joten ohjeita sekä vinkkejä on nopeaa etsiä verkosta.

Tässä työssä tutkimusongelmana oli hajautetun sovelluksen määrittelyn ja mallinnuksen toteuttaminen System Center Operations Manager hallintaohjelmistoa hyödyntäen niin, että sovellus olisi käytännössä valmis otettavaksi valvonnan piiriin. Ohjelmiston asetusten ja määritysten saaminen halutunlaiseksi ei mene ennalta määrätyllä ”step-by-step” -periaatteella, vaan se vaatii aina tapauskohtaisen suunnittelun ja paljon erilaisia testaustoimenpiteitä.

1.4 Keskeisimmät termit

IT	Information Technology, Informaatioteknologia, globaali termi tietotekniikalle
ITIL	Information Technology Infrastructure Library. Prosessikehys. Kokoelma parhaiksi havaittuja käytäntöjä IT-palveluiden johtamiseen ja hallintaan.
MOF	Microsoft Operations Framework, laajennettu ITIL joka tarjoaa kokonaisvaltaisen näkemyksen ja konseptin palveluiden hallintaan. (Microsoftin kehittämä)
OpsMgr / SCOM	(System Center) Operations Manager, järjestelmänhallintaohjelmisto (kappale 3). Työssä käytetään yleisesti myös lyhennettä OpsMgr

2 Palveluiden hallinnan määritelmä

Tietotekniset palvelut voidaan määrittää joukoksi prosesseja ja teknologioita, jotka toimivat yhdessä jonkin päämäärän saavuttamiseksi. Esimerkiksi web-selain, verkko ja tietokanta toimivat yhdessä ja pyörittävät osto- ja myyntiprosessiin liittyviä tapahtumia sekä liikuttavat rahavirtoja elektronisessa muodossa. Tätä ryhmää voidaan kutsua IT-palveluksi, jossa yhdenkin lenkin pettäminen johtaa yleensä tapahtuman keskeytymiseen. IT-ylläpitäjän tulisi hallita järjestelmää palveluiden kontekstin mukaisesti pitääkseen toiminnan tehokkaana. (End-to-end Whitepaper, 2007, 4)

Palveluiden ja järjestelmien hallinta ei ole pelkästään hallintaohjelmiston hyödyntämistä IT-yksikön toiminnassa. Se on laaja kokonaisuus, jolla pyritään kehittämään toimintavarmuutta ja saatavuutta tietotekniikan palveluiden ja sovellusten osalta. Palveluiden hallinnassa yhdistyvät ihmiset, proseduurit (liite 1) ja työkalut. Näistä yhdenkin vajavainen toiminta voi vaarantaa jokapäiväisen liiketoiminnan onnistumisen halutulla tasolla. Palvelunhallinnan määritelmä IT-yksikön näkökulmasta on epäoleellisten ja mahdollisesti haitallisten tapahtumien ennakoimista sekä oikeiden ja tarpeellisten asioiden haravoimista ja hyödyntämistä.

Se on samalla myös resurssien säästämistä automatisoimalla sellaisia tapahtumia, jotka voidaan hoitaa käyttämättä siihen IT-henkilön työaikaa. Jos henkilö hallinnoi useaa eri työkalua ja usein yhtä kerrallaan, käytetty aika on pois muusta toiminnasta. Hallintaohjelmisto mahdollistaa resurssien käytön muuhun ottaessaan usean eri prosessin hallintaansa. Tällöin IT-henkilön panosta tarvitaan ainoastaan määrittelemään, miten automatiikan on tarkoitus toimia ja millaista tietoa halutaan mahdollisista ongelmatilanteista. Tämän jälkeen jäljelle jää kokonaisuuksien valvonta.

Yrityksen IT-infrastruktuuri saattaa paisua yllättävän nopeasti. Aiemmin riittävällä henkilöstöllä ei välttämättä enää pystytä hoitamaan vaadittavia tehtäviä ja tällöin riskit palveluiden toiminnan ja saatavuuden osalta kasvavat. Palvelunhallinta vastaa suoraan liiketoiminnan kysyntään tavoitteista: kuinka kasvattaa tuottavuutta, kuinka laskea kustannuksia ja kuinka tarjota parempi tietoturvataso kriittisille toiminnoille.

Alemmat kustannukset ja korkeampi tuottavuus ovat välttämättömiä, koska epäonnistunut järjestelmänhallinta ja laskenut palvelun taso voivat olla tuhoisia, jos aikaa menee hukkaan ja asiakkuudet karkaavat kilpailijoille. Tällöin saamatta jääneet tulot ovat pois myös IT-yksikön budjetista ja edelleen palveluiden toiminnan kehittämisestä. (Meyler, Fuller, Joyner, Dominey, 2007, 20)

2.1 ITILv3 palveluiden hallinnassa

ITIL (Information Technology Infrastructure Library) on maailman laajimmin käyttöönotettu lähestymistapa IT-palveluiden hallinnalle. Se koostuu käytännössä viidestä eri kirjasta, joista on koottu parhaiksi havaitut käytännöt, joiden pohjalta koko yrityksen palvelustrategiaa tulisi lähteä rakentamaan. ITIL tarjoaa käytännönläheisen ja asiapitoisen rungon tunnistamaan, suunnittelemaan, tuottamaan ja tukemaan IT-palveluita liiketoiminnalle. Siinä tarkastellaan palvelun elinkaarta kokonaisuutena asiakkaan tarpeiden tunnistamisesta valvontaan ja kehitysvaiheisiin. ITIL puolesta puhuu palveluiden suuntaamisesta yrityksen liiketoiminnan ydinalueisiin. Se antaa myös ohjeistusta organisaatioille, kuinka käyttää IT:a työkaluna helpottamaan liiketoiminnan kasvua ja muodonmuutosta. (OGC: ITIL. 2011)

Tietotekniikka on perinteisesti keskittynyt infrastruktuurin palveluihin ja teknologian hallinnointiin. ITIL:n ohjeistus End-to-End -palveluiden (kappale 2.4) hallinnalle suosittelee kokonaisvaltaisempaa lähestymistapaa. Hallinnoitaessa koko liiketoimintakehyksen palveluita sen omilla komponenteilla taataan se, että kaikki palvelun tekijät tulee huomioitua eikä vain yksittäisiä teknologiahaaroja. Lisäksi tällä varmistetaan se, että tuotetaan tarvittavat toiminnot sekä ylläpidetään vaadittu palvelun taso. Palvelutasolla tarkoitetaan palvelun tuottamista tietyn aikajakson puitteissa, asianmukaisten turvatasojen saavuttamista sekä palvelun jatkuvan saatavuuden varmistamista.

Hyvin suunniteltu IT-palvelu tarjoaa toiminnallisuudet, jotka sopivat liiketoiminnan tarkoitukseen tukemaan ihmisiä, prosesseja sekä infrastruktuuria. Sen tulee olla myös yrityksen oman laatuvaatimuksen mukainen. Tärkeää on myös mahdollisuus joustavaan käytöstä poistoon tarpeen loppuessa ilman suurempia kustannuksia tai häiriövaikutuk-

sia. Keskittyminen pelkkään toiminnallisuuteen käytettävyyden jäädessä taka-alalle voi aiheuttaa tappioita ja vaikeuttaa palveluetujen hyödyntämistä.

ITIL on organisoitu palvelun elinkaaren ympärille. Elinkaareen kuuluvat palvelustrategia, palvelusuunnittelu, palvelumuutos, palvelun toiminta sekä sen jatkuva kehittäminen. Elinkaari alkaa asiakkaan palvelutarpeiden ymmärtämisestä sekä siihen kuuluvista vaatimuksista. Onnistuneen strategian läpiviemiseksi IT:n täytyy aina yrittää taata yhdenmukaiset toimituskustannukset suhteessa asiakkaan saaman käyttöarvon kanssa.

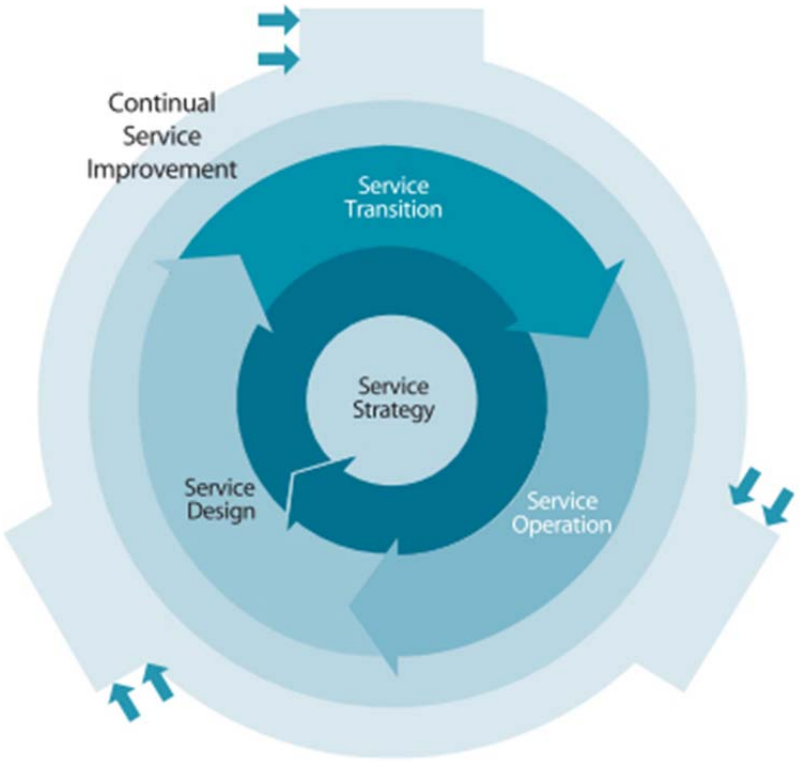
Palvelun mallinnus osana elinkaarta takaa sen, että palvelut ovat suunniteltu tehokkaasti vastaamaan asiakkaan odotuksia. Teknologia ja arkkitehtuuri ovat avainasemassa palvelusuunnittelussa haettaessa asiakkaalle kustannustehokkuutta. Palveluiden hallintaan tarvittavat prosessit ovat myös osa mallinnusvaihetta. Monitorointiin ja palveluiden tukemiseen tarvittavat järjestelmät ja työkalut tulisi ajatella myös prosessien ja palvelutasojen tehokkuuden mittareina.

Palvelun muutosvaiheen aikana sen mallinnus on testattu ja implementoitu (suunnitelman toteuttaminen käytäntöön) tuotteeseen, jotta laadun taso saadaan asiakkaan odottamalle tasolle. Tämä vaihe käsittää muutosten hallinnoinnin, vahvuuksien ja konfiguraatioon (asetusten määritys) kuuluvien osasten hallinnan (muun muassa laitteistot ja-ohjelmistot), palvelun validoinnin (tiettyjen kriteerien täyttäminen) ja testauksen sekä siirtymän suunnittelun. Tällä varmistetaan se, että käyttäjät, tukihenkilöt ja tuoteympäristö ovat valmistautuneet julkaisuun.

Varmistuksen jälkeen palvelu siirtyy päivittäiseen tuotantokäyttöön ja sen yleistä tilaa aletaan valvoa päivittäin. Tähän kuuluu palvelun häiriöiden käsittely, ongelmien alkuperän löytäminen, toistuvien tapausten havainnointi ja loppukäyttäjien toiveiden ja oikeuksien hallinnointi. Palvelun elinkaaren mukana kulkee jatkuva kehittäminen (Continual Service Improvement, CSI), jossa mitataan ja kehitetään palvelutasoja, teknologiaa sekä tehokkuutta toiminnasta ja käyttökokemuksista saadun palautteen ja kokemuksen pohjalta. (Arraj, V. ITIL. 2010, 3-4)

ITIL käytäntöjä ei voida omaksua pelkällä suppealla henkilöstön koulutuksella tai hankkimalla sen käytäntöjä hyödyntävä ohjelmisto. Se vaatii muutosta koko IT:n liiketoimintaan, jotta tuotettavat palvelut suuntautuvat ydinliiketoiminnan tarpeisiin ja vaatimuksiin. ITIL sopeuttaminen voi vaatia investointeja ihmisiin ja työvälineisiin, mutta tärkeämpi vaatimus on palvelukulttuuri, joka tulisi mallintaa tarkkaan harkiten kokeneiden osaajien avulla. (Kneller, M. 2010. 8-9)

Kuviossa 1 on yksinkertaistettu ITIL:n periaatteen mukainen palvelunhallinnan toiminta. Palvelustrategian (Service Strategy) mukaisesti toteutetaan suunnitelmat (Service Design), siirtymät (Service Transition) sekä operoinnit (Service Operation) käytettäville IT-palveluille. Samalla kerätään kokemusta koko elinkaaren ajalta (Continual Service Improvement), jonka mukaan tehdään kehitystyötä jokaiselle osa-alueelle saadun kokemuksen ja palautteen mukaisesti.



Kuvio 1. ITIL ydin ja palvelunhallinnan periaate.

2.2 MOF palveluiden hallinnassa

MOF tulee sanoista Microsoft Operations Framework ja se on edellisessä kappaleessa kuvatun ITIL:n pohjalta luotu prosessikehys. System Center Operations Managerin toiminta perustuu tähän konseptiin, joka on suunniteltu ITIL:n pohjalta valikoidusti ja joka sisältää parhaat käytännöt palveluiden hallinnalle sekä niiden tuottamiselle liiketoiminnan tarpeita varten. Siinä keskitytään yksinkertaistettuna itse palveluun, kun taas ITIL on suuremman kokonaisuuden viitekehys. Microsoft määrittelee ITIL:n kuvailevana mallinnuksena ja MOF:n puolestaan ohjailevana mallinnuksena, joka keskittyy siihen, miten jokin prosessi palvelunhallinnassa toimii.

MOF jaotellaan elinkaarensa kuvailemiseksi karkeasti kahteen malliin, tiimimalli ja prosessimalli. Tiimimalli luotiin kaventamaan eroavaisuutta ITIL käytäntöihin ja siihen kuuluvat seuraavat roolit: palvelu, infrastruktuuri, tuki, toiminnot, partneri, turva sekä julkaisu. Näillä jokaisella on oma vastuualueensa kattamaan elinkaaren toiminnot. Prosessimallissa jaottelu tapahtuu neljään ryhmään (quadrant): muutos, toiminta, tuki ja optimointi. Nämä sisältävät 21 eri palvelunhallinnan funktiota, kuten ongelmien hallinta tukiryhmässä, verkon hallinta toimintaryhmässä, palveluntason hallinta optimointiryhmässä ja muutosten hallinta muutosryhmässä. Käytännössä tällaisella menettelyllä halutaan jakaa tehtäviä ja vastuita loogisiin ryhmiin. Tällöin suuri kokonaisuus saadaan pilkottua palasiksi ja jaoteltua vastuualueet oikeille tahoille. Jokin taho voi määrittää, mitä muutoksia tarvitaan palveluiden valvonnan osalta. Ylläpitohenkilö suorittaa tarpeelliset toimintojen sekä asetusten määritykset ja muokkaukset, ja valvovat tahot varmistavat, että muutokset vastaavat tarpeita. Vastuiden erittely ei tarkoita sitä, että tarvittaisiin eri henkilö hoitamaan jokaista tehtävää erikseen. Pienellä henkilöstöllä voidaan delegoida enemmän tehtäviä yhdelle henkilölle, jolloin vastuita kannattaa jakaa MOF:n prosessimallin quadranttien mukaisesti.
(Price, B., Mueller, J., P., Fenstermacher, S. 2007, 8-13)

2.3 ISO/IEC 20000 standardi

ISO/IEC 20000 on ensimmäinen kansainvälinen standardi IT-palveluiden hallinnalle. Se on suunniteltu vuonna 2005 ja sen oli tarkoitus korvata aiempi dokumentointi BS 15000. Standardista on kaksi osaa, joista ensimmäinen tukee integroitujen prosessien

lähestymistavan hyväksymistä tehokkaaseen hallinnoitujen palveluiden tuottamiseen ja asiakkaiden vaatimusten täyttämiseen. Toinen osa, ISO/IEC 20000-2, pohjautuu täysin ensimmäiseen osaan ja kuvaa parhaita käytäntöjä palveluiden hallintaan. Jälkimmäisessä osassa on sivuutettu hallintajärjestelmän vaatimusten osuus kokonaan. Standardi sisältää ITIL:n kehyksen ja sisällön sekä tukee tasavertaisesti muita palvelunhallinnan kehyksiä, mukaan lukien Microsoft Operations Framework. (ISO, 2011)

2.4 End-to-End palvelun periaate

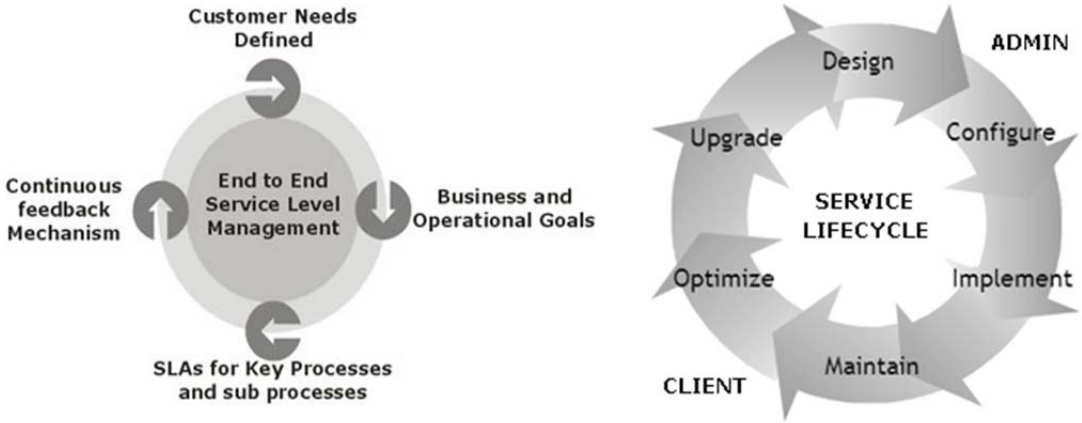
End-to-end -palvelunvalvonta tarkoittaa useasta teknologisesta komponentista (muun muassa ohjelmisto, palvelin ja tietokanta) koostuvan palvelun kokonaisvaltaista valvontaprosessia. Näitä korkean tason objekteja kutsutaan myös hajautetuiksi sovelluksiksi. Niitä käsitellään tarkemmin kappaleissa 4 ja 5. Palvelulähtöiset näkymät ja saatavuusraportoinnit mahdollistavat ylläpidon tunnistamaan ja ratkaisemaan esille tulevia ongelmatilanteita, jotka vaikuttavat palvelutasoon.

Käytännössä palvelu tulee ensin mallintaa. Kaikki siihen liittyvät alikomponentit on tunnistettava ja niihin vaikuttavat relaatiot täytyy tiedostaa. Tämä voi olla joskus prosessin hankalin vaihe, mutta puutteellisesti tehtynä palvelun toiminta voi häiriintyä. Palvelun kannalta välttämättömät komponentit voidaan jättää pois mallinnuksesta. (End-to-end Whitepaper, 2007, 5)

Palvelun tai sovelluksen suunnitteluun kuuluu kaksi tärkeää asiaa. Toteutukseen ei saa tulla riippuvaisuuksia, jotka voisivat jotenkin vahingoittaa end-to-end -periaatetta. Toisekseen palvelusta tulee tunnistaa kaikki sen päätepisteet johdonmukaisella tavalla. Ongelmia voi syntyä esimerkiksi lisättäessä uusia objekteja hajautettuun sovellukseen tai luotaessa jokin riippuvaisuus väärällä tavalla, mikä tekee tiedonkulun mahdottomaksi. Jos ongelmia ei ole, saadaan tuloksena hajautettu sovellus, jonka objektien päätepisteistä kulkee tieto toisiinsa dynaamisesti ilman katkoja. (Kempf, J., Austein, R. 2004. Internet requests for comments, 4.2)

Kuviossa 2 vasemmalla on End-to-End palvelunhallinnan peruspilarit. Palvelua kehiteltäessä tulee määrittää asiakkaan tarpeet (Customer Needs Defined). Tämän jälkeen selvitetään kaikki mahdolliset liiketoiminnan ja muun toiminnan tavoitteet ja määränpäät (Business and Operational Goals). Seuraavaksi on tarpeen sopia ja määrittää asianmukaiset palvelutason yksityiskohdat ja vaatimukset pää -ja aliprosesseille (Service Level Agreements for Key Processes and sub processes), kuten sallitut palvelunkatkosajat tai viiveet palveluissa. Tähän voidaan katsoa kuuluvaksi myös ylläpidolliset palvelun tason tavoitteet. Koko toimintaa kehitetään ja valvotaan jatkuvalla palautteen keräämisellä (Continuous feedback Mechanism) eri lähteistä, pääasiassa palvelun käyttäjien puolelta.

Oikeanpuoleinen kuvio kuvaa uuden palvelun elinkaarta. Admin eli järjestelmästä vastaava henkilö aloittaa ensimmäisellä vaiheella, eli suunnittelulla (Design) ja määrittelyllä (Configuration). Käyttöönoton (Implement) jälkeen kerätään kokemuksia ja hoidetaan ylläpitotehtäviä (Maintain), joiden pohjalta optimoidaan (Optimize) sekä päivitetään mahdollisia korjauksia ja muutoksia (Upgrade). Palvelun tuottaja (IT-osasto, helpdesk, ulkoinen palveluntarjoaja tai vastaava) osallistuu käytännössä jokaiseen elinkaaren vaiheeseen, kun taas asiakaspuolen käyttäjätaho (Client) lähinnä vain itse käyttöön sekä palautteen antamiseen.



Kuvio 2. End-to-end palvelutason hallinta ja elinkaaren vaiheet

2.5 Dynaaminen ja proaktiivinen IT ympäristö

Proaktiivisella toiminnalla tarkoitetaan eteenpäin suuntautuvaa toimintaa ja asennetta. Käytännössä tämä tarkoittaa toimintaa sekä henkilöstötasolla että tietoteknisellä tasolla. Proaktiivisessa ympäristössä muutosvaatimuksiin vastataan joustavasti, tarkoituksenmukaisesti ja jopa ennakoivasti. Henkilöstötasolla tämä tarkoittaa sitä, että työntekijöiden vastuu ja oma-aloitteisuus kasvavat selvästi aiempaan ”ylhäältä johdettuun” malliin verrattuna. Samalla kun organisaation rakenne muuttuu muutosten myötä proaktiivisemmaksi, niin myös IT-ympäristön rakenne muuttuu dynaamisemmaksi esimerkiksi hallintaohjelmistoja käyttöönotettaessa. (Antila J., Ylöstalo P. 2002. 11)

Optimointi on tärkeä osa IT-infrastruktuurin viennissä dynaamiseen suuntaan. Mahdollisuudet, vahvuudet, uhat ja haitat tulee kartoittaa nelikenttäanalyysin mukaisesti. Lisäksi vaatimukset täytyy olla tiedossa, jotta voidaan laatia etenemissuunnitelma. Optimoinnilla avataan mahdollisuudet nähdä IT-infrastruktuurin ja sen investointien arvo liiketoiminnan silmin. Samalla yritetään vakiinnuttaa tietotekniset toiminnot koko liiketoiminnan vahvistukseksi vastaamaan muutosten haasteisiin.

Dynaamisen infrastruktuurin omaavat yritykset ovat tietoisia omista vahvuuksistaan ja mahdollisuuksistaan. Näitä hyödyntämällä etu kilpailijoihin näkyy liiketoiminnan kriittisimmissä elimissä, kun IT-tiimissä on pidetty huoli omien toimintojen vakaudesta ja tehokkuudesta. Kulut, tietovirrat, palvelimet ja työasemat ovat hallinnassa ja yhteistyö on sujuvaa IT-henkilöiden ja liiketoimintapäättäjien välillä. Dynaamisen kokonaisuuden saavuttaminen vaatii niin taloudellista pääomaa kuin myös henkilöstön oma-aloitteisuutta koko organisaatiolta, mutta proaktiivisuus nähdään pitkällä aikavälillä palvelutason ja kilpailukyvyn nousuna sekä mahdollisuuksina ottaa vastaan suurempia liiketoiminnallisia haasteita. (Microsoft Webcast: Optimizing Application Platform Infrastructure to Advance Business, 2007)

Microsoft on rakentanut System Center -perheen hallintaohjelmistot ITIL:n ja MOF:n ympärille. Näiden lisäksi se on kehittänyt vastaavan tavan hahmottaa ja käsitellä suurempaa kokonaisuutta. Usein pienestä ja yksinkertaisesta ohjelmasta voi kasvaa laajempi, useiden käyttäjien hajautettu sovellus (distributed application, tarkemmin kappalees-

sa 4). Tällöin sen ylläpito voi vaatia yhden ihmisen sijaan useamman tiimin panosta. Tällöin voidaan puhua hajautetusta järjestelmästä, joka vaatii keskitettyä hallintaa. Tähän tarpeeseen Microsoft on suunnitellut ratkaisukehyksen nimeltään The Dynamic System Initiative (DSI). Siinä on tarkoituksena suunnitella ohjelmistoratkaisu, joka sisällyttää IT-palvelunhallinnan mahdollisuudet sekä MOF:n parhaat käytännöt ohjelmiston avulla (tässä tapauksessa OpsMgr) täyttämään liiketoiminnan vaatimuksia IT-palveluille. DSI auttaa IT-organisaatiota luomaan end-to-end -palveluita, jotka tuovat yksinkertaisuutta ja automatisaatiota. Käytännössä ne muun muassa parantavat tuottavuutta ja vähentävät juoksevia kuluja, vähentävät ylläpitoon ja ongelmanratkaisuun tarvittavaa aikaa sekä työmäärää, nostavat valmiutta vastata ydinliiketoiminnan tarpeisiin sekä kehittävät järjestelmän toimintaa IT-politiikan mukaisesti. Pitkällä aikavälillä näillä on selkeä proaktiivinen merkitys.

Tällä hetkellä DSI:n päämäärät saavutetaan OpsMgr:n hallintapakettien (Management Pack, tarkemmin kappaleessa 3.2) avulla. Jatkossa niitä hallitaan prosessin nimeltä System Definition Model (SDM) avulla. Se on DSI-tuotteiden ja komponenttien ytimessä ja rakentuu XML-pohjaisesta mallista. Sitä käytetään luomaan erilaisia mallinnuksia koko IT-järjestelmästä. SDM toimii ikään kuin aivoina manipuloiden luomiaan malleja järjestelmästä. Tällöin se osaa hyödyntää eri paikoista hankkimaansa dataa luodakseen end-to-end ratkaisuja, jotka ovat integroituneet sovelluksiin, käyttöjärjestelmiin, laitteistoihin sekä hallintatyökaluihin. Näillä saadaan kustannustehokkuutta sekä luotettavuutta IT-palveluiden elinkaareen.
(Price, B. ym. 2007. 14-15)

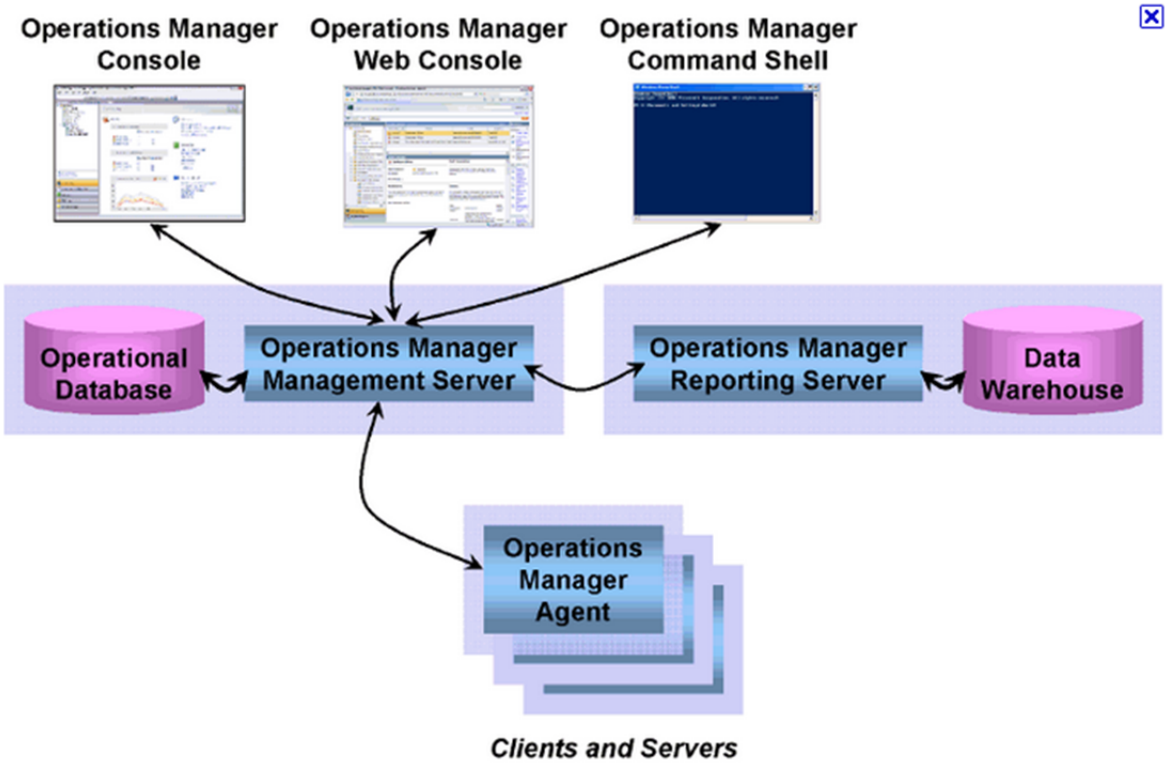
3 Microsoft System Center Operations Manager 2007 R2

Tämän opinnäytetyön hallintatyökaluksi valittu System Center Operations Manager 2007 R2 on ohjelmisto, jolla tarjotaan ratkaisuja end-to-end palveluiden valvontaan yrityksen IT-ympäristöön. Sen edeltäjänä toimi Microsoft Operations Manager (MOM), jossa valvonta rajoittui pääosin yksittäisiin palvelimiin. Uudempaan versioon on tuotu mahdollisuuksia monitoroida yksityiskohtaisemmin verkon eri komponentteja ja nähdä niiden ”terveyden tila”. Käytännössä hyvinkin laajaa, tuhansia palvelimia ja ohjelmistoja kattavaa ympäristöä saadaan valvottua yhdeltä näytöltä, riippuen mitä ylläpitäjä haluaa sisällyttää hallintasovellukseensa. (End-to-end Whitepaper, 2007, 4)

Suunniteltaessa OpsMgr:n käyttöönottoa on oman IT-ympäristön vaatimusten tunnistaminen tärkeässä roolissa. Tunnistettavia seikkoja ovat paitsi tarvittavat komponentit ja niiden käytön soveltuvuus omiin tarpeisiin, niin myös tarvittavat ominaisuudet ja niiden käyttö. Vaatimukset voidaan karkeasti jakaa kolmeen kategoriaan: liiketoiminta-vaatimukset, IT:n vaatimukset ja optimoinnin tavoitteet. Voidaan asettaa kysymyksiä, kuten halutaanko sähköposti, jos tulostinpalvelimen prosessorin kuormitus ylittää viisi prosenttia, halutaanko välitön hälytys, jos varayhteyden reititin ei ole toiminnassa, kuinka tarkasti halutaan raportoida yrityksen johdolle tiettyjen kokonaisuuksien toiminnasta. Kun näistä on selkeä kuva, on hallintaympäristöstä helpompi rakentaa odotuksia vastaava kokonaisuus. (SCOM documentation design guide, 16-18)

Organisaation IT-infrastruktuurista tulee monimutkainen heti, kun siinä on useampia ohjelmistoja ja laitteistoja, jotka ovat erilaisissa relaatioissa keskenään tai muiden tietolähteiden kanssa. Operations Managerin tarkoituksena on vastata kahteen syntyvään haasteeseen. Toinen niistä on tarjota IT-ylläpitäjälle selkeä ja kokonaisvaltainen kuva ohjelmistojen saatavuudesta aina levyjen käyttöasteeseen. Toinen haaste on kyky vastata älykkäästi valvonnan tuottamaan informaatioon. Näiden haasteiden tulisi kattaa myös ongelmien ennakoinnin onnistuminen ennen kuin jokin oleellinen osa-alue pettää. (Operations Manager Overview, 2010, 3)

Kuviossa 3 on havainnollistettu Operations Managerin pääkomponentit ja niiden keskenäisiä riippuvuussuhteita. Hallintapalvelin (Operations Manager Management Server) on ikään kuin isäntä, johon kaikki osaset liittyvät suoraan tai välillisesti ja sillä on aina myös oma tietokanta (Operational Database). Erillislaitteissa (Clients and Servers) olevat agentit (Operations Manager Agent) ottavat yhteyttä automaattisesti isäntään säännöllisin väliajoin. Raportointipalvelin (Reporting Server) käsittelee ja arkistoi omaan tietokantaansa (Data Warehouse) isännältä tulevaa tietoa palveluiden ja laitteiden tilasta. Hallintakonsoli (Operations Manager Console) on useimmiten sijoitettu hallintapalvelimelle, mutta joskus myös erilliselle palvelimelle. Web-konsoli (Web-console) ei tarvitse välttämättä omaa palvelinta, mutta palvelutason varmistamiseksi sellainen on suositeltavaa asentaa. Command Shell on komentorivipohjainen työkalu, josta voidaan antaa satoja erilaisia suoria käskyjä palveluiden hallinnointiin ja ylläpitoon. (Operations Manager Overview, 2010, 5)



Kuvio 3. OpsMgr:n pelkistetty rakennekaavio

3.1 Monitoroinnin ja hallinnan haasteet

System Center Operations Manager on jo sen suunnittelusta asti pyrkinyt vastaamaan palvelunhallinnan keskeisimpiin haasteisiin. Mitä suurempi yritys ja mitä enemmän sillä on hallittavia objekteja, sitä haastavammaksi käy myös palveluiden ja laitteiden valvonta. Haastavan siitä tekee se, että monitoroinnin tulisi olla tehokasta ja sen tulisi kattaa mahdollisimman suuri osa ympäristöstä. Tuhansien työasemien ja palvelinten viidakkoon mahtuu lukemattomia ohjelmistoja, tietokantoja ja verkkopalveluita, joiden odotetaan palvelevan käyttäjiä katkotta. Näistä syntyvä tietomäärä on valtava käsiteltäväksi. Siihen tarvitaan ohjelmistollista apua muuttamaan se ymmärrettävään, selkokieliseen muotoon ja ennen kaikkea tunnistamaan olennainen ja tarpeellinen tieto epäolennaisesta.

Mahdollisuus monipuolisille toiminnoille on usein tarpeen, kuten pääsy tarkistamaan hälytyksiä mistä tahansa verkosta (Web Console), luomaan ja ajamaan scriptejä (liite 1) (Command Shell) tai tulostamaan raportteja, mitä kaikkea on tapahtunut tai mitä on tehty aiemmin (Reporting Services). Jos näitä mahdollisuuksia ei ole, saattaa se aiheuttaa pitkällä aikavälillä ongelmia seurannan ja kehitystyön osalta. Ajantasainen tieto auttaa nykyhetkessä, mutta historia auttaa kehityksessä ja trendien havainnoinnissa. Ei myöskään ole mahdollista, että yksi henkilö hallitsisi laajan yrityksen tuhansien objektien monimutkaisen valvonnan täydellisesti. Ohjelmistolta tarvitaan avoimuutta ja ominaisuuksia kolmansien osapuolten (kuten laitevalmistajat) hallintapakettien hyväksymiseen ja hyödyntämiseen. Lisäksi ydinliiketoiminta ja maksavat asiakkaat, usein myös yritysjohto, näkevät palvelut kuten ne ovat määritelty ITIL:ssä ja MOF:ssa, joten haasteena on paitsi ohjelmiston myös yrityksen toimintatapojen saaminen näiden kehysten mukaisiksi. (Chappell, D. Introducing SCOM 2007, 3)

3.2 OpsMgr:n komponentit

Operations Managerin hallintaympäristöön kuuluu ryhmä komponentteja, joista muutamat ovat välttämättömiä perustoimintojen ylläpitämiseksi ja osa on tarpeen mukaan asennettavia lisäosia. Keskeisin vaadituista komponenteista on ***Operations Manager Database (OMDB)***. Se on aina ensimmäinen asennettava komponentti kaikissa hallin-

taryhmissä. Sen alustana tulee olla Microsoft SQL Server 2005 tai sitä uudempi versio. Tähän tietokantaan sisältyy kaikki hallittava tieto ja siihen varastoituu myös kaikki agenttien keräämä informaatio. Sen huolellinen ylläpito on varsin tärkeää, sillä sen suorituskyky voi laskea koko hallintaympäristön suorituskykyä. Tärkeimmät ylläpidolliset toimenpiteet ovat sen koon pitäminen tarpeeksi pienenä (alle 50 gigatavua) sekä mahdollinen klusterointi (kahdennus, jos pääpalvelin hajoaa, niin toinen identtinen kopio jatkaa sen tehtäviä).

Toinen keskeinen ja välttämätön komponentti on erityinen juuripalvelin, ***Root Management Server*** (RMS). Hallintaryhmässä voi olla vain yksi aktiivinen juuripalvelin kerrallaan. Se on päähallintatyökalu, joka sisältää kaikki toiminnallisuudet asetusten hallinnointiin, ylläpitoon sekä kommunikointiin tietokantojen ja valvottavien työasemien kanssa. Juuripalvelimelle asennetaan hallintakonsoli ja siitä tulee myös kohdepalvelin verkkopohjaiselle valvontakonsolille. Juuripalvelin ylläpitää kaikkia olennaisimpia palveluja, joten sen toimintavarmuus on taattava. Se voidaan myös kahdentaa tai jokin toinen tavallinen hallintapalvelin voidaan tarpeen tullen määrittää toimimaan juuripalvelimen roolissa. (SCOM documentation design guide, 8-9)

Agentti on valvottavalle kohdetyöasemalle laitettava palvelu, joka valvoo sen toimintaa ja ”terveyden tilaa”. Jokaiselle agentille on kohdennettu oma hallintapalvelin, jonne se lähettää keräämänsä reaaliaikaista tietoa sen perusteella, miten sen on määritelty toimivan. Jos valvottavan aseman tila muuttuu selkeästi verrattuna agentille annettuihin arvoihin, agentti voi generoida hälytyksen, joka lähetetään hallintapalvelimelle ja edelleen ylläpitäjän tiedoksi. Vaikka mikään ei olennaisesti muuttuisi, lähettää agentti säännöllisin väliajoin tilannetietoa palvelimelle ajantasaisen kokonaiskuvan rakentamiseksi hallintaympäristöstä. Kaikille laitteille ei tarvitse tai ei voida laittaa agenttia, kuten verkon aktiivilaitteille, esimerkiksi kytkimelle. Tällöin valvonta tapahtuu etäagentin välityksellä suoraan hallintapalvelimelta (tarkemmin kappaleessa 3.4).

Operations console, hallintakonsoli, on päähallintatyökalu ja siinä on käyttöliittymä kaikkien Operations Manager -ympäristöön kuuluvien komponenttien hallintaan. Jotta ylläpitäjä voi päästä käsiksi konsoliin, täytyy hänen roolinsa olla erikseen luvitettu Active Directory:ssa (liite 1). Tällä rooli-pohjaisella menettelyllä voidaan jaotella ylläpitäjille

(operaattoreille) eriasteisia oikeuksia OpsMgr:n toimintoihin. Hallintakonsolia käsitellään myös kappaleessa 3.5.

Management Pack, jota voidaan kutsua hallintapaketiksi tai määrittelypaketiksi, sisältää sovelluksen kehittäjän luomat määrittelyt ja säännöt siitä, miten OpsMgr valvoo ja monitoroi sovellusta. Suurimmalle osalle sovelluksista on olemassa valmis paketti määrittelyineen, joka vain otetaan käyttöön kun sovelluksen tai vastaavan komponentin monitorointi halutaan aloittaa. Management Pack:iin on määritelty lähtökohtaisesti muun muassa valvottavat osat, hälytyssäännöt ja hälytysrajat, automaattiset korjaustoimenpiteet sekä sääntelyt siitä, mitä tietoa ja koska agentti lähettää hallintapalvelimelle raportoitavaksi. Objektien monitorointi ei käytännössä ole mahdollista ilman asiankuuluvaa hallintapakettia, lukuun ottamatta esimerkiksi verkon aktiivilaitteita.

Management Packit (MP) ovat OpsMgr:n komponentteja, joiden avulla voidaan kerätä ja hyödyntää laajasti informaatiota monesta lähteestä. Ne ovat XML-dokumentteja (rakenteellinen kuvauskieli, joka auttaa jäsentämään laajoja tietomassoja selkeämmin) ja tarjoavat perusrakenteen tietyn laitteen, ohjelmiston tai palvelun valvonnalle. Ne sisältävät eri rakenneosasten määritelmät ja informaation, jota ylläpitäjä tarvitsee käyttäessään tiettyä ohjelmaa, laitetta tai palvelua. Tässä yhteydessä voimme kutsua näitä objekteiksi. Management Pack sisältää tiedot muun muassa objektin rakenteesta, havainnoinnista, monitoroinnista sekä siitä mitä tehdä, kun sovellukseen tai laitteeseen tulee vika. Se toimii havaitsemalla ja valvomalla kyseisiä objekteja. Kun objekti on havaittu, sitä monitoroidaan MP:iin määritellyn mallin mukaisesti. OpsMgr käyttää malleja monitoroinnin perustana. Malleilla mahdollistetaan objektien semanttisuuden (liite 1) määritys sekä niiden terveydentilan seuraaminen. Malleihin sisällytetään objektien määrittelyt sekä niiden väliset vaikutussuhteet toisiin objekteihin. Mallipohjainen hallinta edellyttää, että objektit ovat mallinnettu Management Packissa.

Management Packit ovat joko Microsoftin, jonkin kolmannen osapuolen tai käyttäjän itsensä toteuttamia. Usein sama taho, joka on tuottanut jonkin tietyn sovelluksen tai palvelun, on tehnyt myös siihen kuuluvan hallintapaketin. Tämä takaa paremman luotettavuuden oikean informaation saamiseen monitoroitaessa järjestelmän tilaa. Valmiit paketit ovat usein niin sanotusti sinetöityjä eikä alkuperäistä pakettia voi editoida. Niis-

sä olevien esiasetusten muokkaaminen vaatii MP:n ”syrjäyttämisen” (Override) ja uudeksi paketiksi tallentamisen. Suositeltavaa on, että yhtä sinetöityä hallintapakettia kohden tehtäisiin vain yksi uusi Management Pack. (Meyler ym., 2007, 593-595)

Management Server, eli hallintapalvelin, ei ole välttämätön lisäkomponentti, varsinkaan jos verkkoympäristö on suppea. Hallintapalvelin poikkeaa toiminnaltaan juuripalvelimesta siinä, että se ei suorita juuripalvelimen toimintoja oletuksena, ellei niin erikseen määritellä. Hallintapalvelimia voidaan pystyttää useampia tukemaan agenteilta tulevan tiedon käsittelyä ja vakauttamaan ympäristöä mahdollisen vikatilanteen sattuessa. Yleinen hyväksi havaittu käytäntö on asentaa ainakin yksi hallintapalvelin juuripalvelimen rinnalle, joka on valjastettu toimimaan vikatilanteessa juuripalvelimena. Suositeltavaa on myös laittaa toinen palvelin, joka keskittyy muihin toimintoihin, kuten ylläpitämään tietoturvaa lisäävää valvonnan keruu palvelua (Audit Collection Service, ACS). Tämä voitaisiin sisällyttää myös juuripalvelimen toiminnoksi, mutta hallinnan selkeyttämiseksi sen on parempi toimia erillisenä. ACS palvelin itsessään kerää tietoa valvottavien työasemien tietoturvalokeista ja sisällyttää ne omaan tietokantaansa, joka voidaan luoda samalle palvelimelle. ACS raportointikomponentilla voidaan puolestaan määritellä, mitä kaikkea tietoa halutaan saada lokeista koostetusti ulos, koska osa tiedosta on aina tarpeetonta, mutta osa voi olla toiminnan kannalta kriittistä.

Gateway Server, yhdyskäytäväpalvelin, ei ole välttämätön, jos kaikki valvonnan alaiset työasemat ovat sille osoitetun hallintapalvelimen kanssa samassa toimialueessa. Tällöin ne eivät tarvitse erillistä tunnistautumiskanavaa tiedonkulkuun agentin ja palvelimen välillä. Muussa tapauksessa yhdyskäytäväpalvelin on tarpeen, jos esimerkiksi useita monitoroitavia objekteja on toisen verkon toimialueessa. Työläitä ongelmia voi tulla muun muassa tilanteessa, jossa palomuuri on sijoitettu agenttien ja hallintapalvelimien väliin, eikä yhdyskäytävää ole. Lisäämällä yhdyskäytävä verkkoympäristöön riittää tunnistautumiseen yhteneväiset sertifikaatit sekä yhdyskäytäväpalvelimelle ja hallintapalvelimelle. (SCOM documentation design guide, 9-11)

3.3 Keskeisten konseptien hyödyntäminen

Riippuen yrityksen verkkoympäristöstä ja tarpeesta, Operations Manager tarjoaa useampia vaihtoehtoja ja lisäominaisuuksia, jotka eivät ole välttämättömiä, mutta joista voi olla suurta apua hallinnassa. Seuraavassa on käsitelty muutama ominaisuus, joita kannattaa harkita omaan ympäristöön käyttöönotettavaksi.

Yksi niistä, ***Agentless Exception Monitoring***, on jo olemassa olevan tekniikan hyödyntämistä OpsMgr:n ympäristössä. Windows -käyttöjärjestelmässä oleva sisäinen viankaappausominaisuus voidaan ottaa myös keskitetyn hallinnan piiriin. Tällöin kohdeobjekti määritellään lähettämään tietoa hallintapalvelimelle esimerkiksi silloin, kun jokin sovellus kaatuu. Kohdeasema luo niin sanotun virheraportin, joka ohjautuu hallintapalvelimen käsittelyyn, jossa taas voidaan suorittaa haluttua analysointia ja diagnosointia. Tällä voidaan mahdollisesti havaita ja ennaltaehkäistä usein toistuvia ongelmia niin työasemien kuin palvelintenkin osalta. (SCOM documentation design guide, 14)

Simple Network Management Protocol (SNMPv2). Tämä käytäntö ei ole uusi keksintö. Se tarjoaa monitoroinnin mahdollisuuden hyödynnettäväksi sellaisissa tapauksissa, joissa varsinaisen agentin käyttö ei ole jostain syystä mahdollista. Esimerkiksi ilman varsinaista käyttöjärjestelmää olevat verkon aktiivilaitteet, kuten reititin, kytkin tai palomuuri, saadaan valvonnan piiriin käytännössä pelkkien verkko-osoitteiden avulla. Ne määritellään hallintapalvelimelle niin sanotun etävalvonnan alaisuuteen, kun SNMP optio on ensin otettu käyttöön hallintapalvelimella. Saatava informaatio on suppeammassa muodossa kuin agenttien antama tieto, mutta yleensä tieto laitteen toimimattomuudesta tai katkonaisesta toiminnasta riittää. (Microsoft TechNet, SNMP, 2011)

Kun verkkoympäristössä on aktiivilaitteita, jotka eivät käytä Windows -käyttöjärjestelmää ja joihin ei ole mahdollista laittaa agenttia, tarvitaan edellisen lisäksi myös ***Proxy Agent***-ominaisuutta. Tämä tarkoittaa käytännössä sitä, että jokin normaali työasema tai muu objekti, jossa on agentti, valjastetaan monitoroimaan laitetta, jossa agenttia ei ole. Tämä tulee sallia ja määritellä erikseen jokaisessa tapauksessa. Valvottavalle laitteelle

nimetään siis ikään kuin sijaishuoltaja, joka katsoo sen perään koska sillä itsellään ei ole siihen resursseja. (SCOM documentation design guide, 12-13)

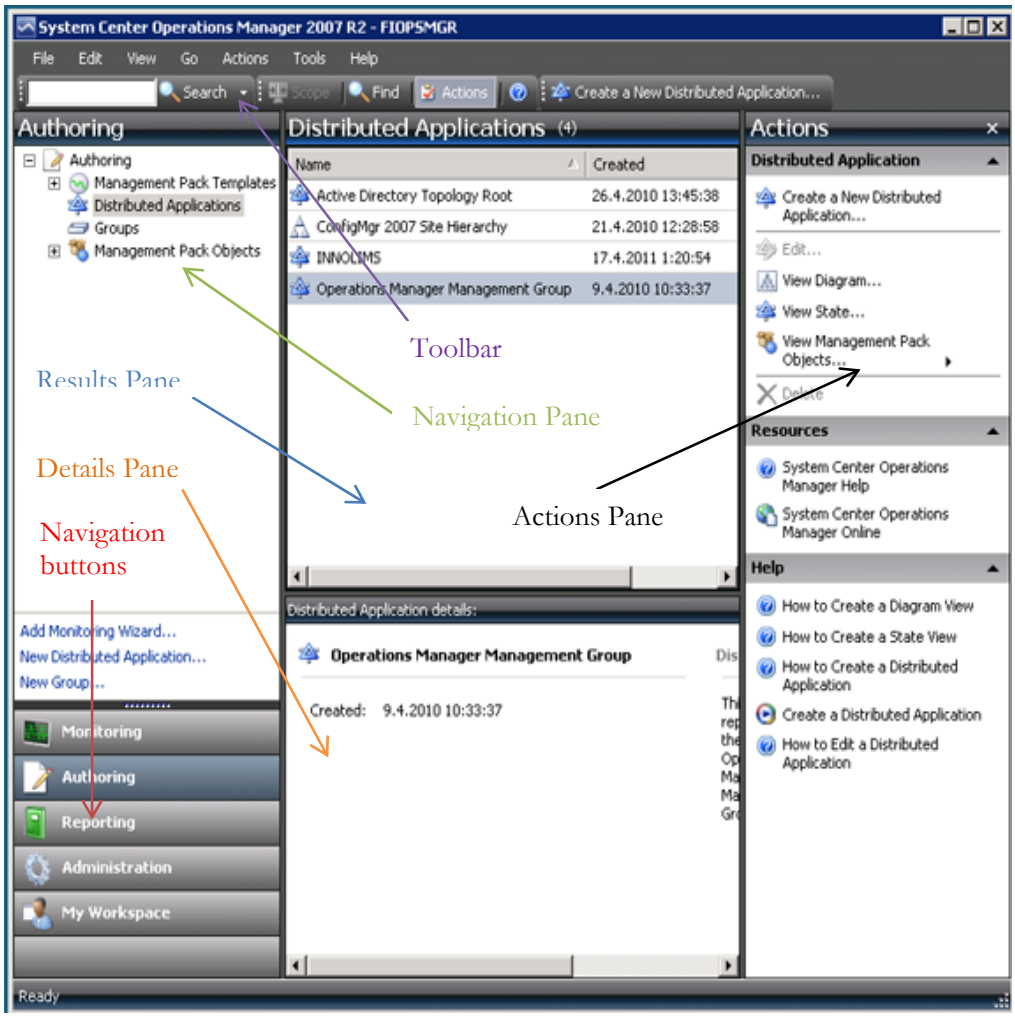
Toinen mainittava ominaisuus, jota voidaan suositella riippumatta IT-infran koosta, on ***Audit Collection Services*** (ACS). Se on erillinen turvaratkaisu, jossa kerätään ja varastoidaan monitoroitavien objektien tietoturvalokeista. Tieto tallennetaan MS SQL Server -tietokantaan, joka on hyvä olla erillään juuripalvelimen tietokannasta. Työaseman agenteissa on sisäänrakennettu ominaisuus kerätä ja lähettää edelleen informaatio ACS-palvelimelle, joten käyttöönotto on kohtuullisen vaivatonta. Ehkä tärkein huomioitava asia on se, että lähes kaikki data kerätään oletuksena talteen ja sitä on yleensä valtava määrä. Suurin osa siitä on tarpeetonta, mutta suodatusmekanismin avulla voidaan valita yksityiskohtaisesti haluttu informaatio. ACS raportointitietokanta on suositeltavaa perustaa omaksi kannaksi erilleen Operations Managerin raportoinnista, jotta tiedon käsittely helpottuu ja vastuutehtävien jakaminen eri henkilöille helpottuu.

3.4 Hallintakonsoli ja web-pohjainen konsoli

Web-konsoli on hyvin samankaltainen kuin itse hallintakonsoli. Se vaatii toimiakseen ActiveX-komponentin (liite 1) selaimeen, joka asentuu ensimmäisellä avauskerralla. Verkkoversiota on mahdollista käyttää myös älypuhelimella, jossa on internet-yhteys. Käyttäjä voi tällöin tehdä RSS-uutisvirtoja (liite 1) OpsMgr:n valvontaan puhelinlaitteellaan. (Meyler, Fuller, Joyner, Dominey, 2007, 130-134)

Web-konsoli on suunniteltu operaattorin tai vain luku-oikeuksin varustetun operaattorin rooleille. Web-konsolissa on mahdollista käyttää vain Monitoring- (valvonta sekä monitorointi) ja My Workspace (omat valitut valvottavat komponentit) -ikkunaruutuja. Se on tarkoitettu lähinnä toimijoille, jotka tarkastelevat seurantatietoja, suorittavat valvontatehtäviä ja ratkovat hälytyksiä. Siinä ei voida kuitenkaan käyttää ”Suorita nimellä..” -toimintoa, koska se ei ole sallittu. Kaikki tehtävät ajetaan hakemistopalvelimelta (AD) määräytyvien käyttäjäoikeustietojen perusteella. Web-konsoli ei vaadi erityistä laitteistoa tai käyttöjärjestelmää. Jos käyttäjän tarvitsee päästä luomaan uusia valvontasääntöjä, tulee hänen käyttää hallintakonsolia. (SCOM documentation, operations guide, 22)

Hallintakonsoli (kuviossa 4) muistuttaa Microsoftin hallintakonsolin (MMC) liitännäistä, mutta se on itsenäinen sovellus, joka asennetaan hallintapalvelimelle. Sen käyttöliittymä ja ulkoasu on selkeä ja muistuttaa jonkin verran Office Outlookia. Hallintakonsoli koostuu erilaisista ikkunoista. Niiden avulla voidaan operoida kaikkia tärkeimpiä ja yleisimpiä toimintoja sekä seurata monitoroitavilta työasemilta ja muilta laitteilta tulevia ilmoituksia palveluiden tilasta. Konsolissa voidaan tehdä myös mukautettuja näkymiä ja monimutkaisempia hakuja (My Workspace Pane), jotka kohdistuvat tiettyihin osa-alueisiin.



Kuvio 4. Hallintakonsolin perusnäkymä ja sen moduulit

3.5 Roolipohjaiset käyttöoikeudet

Operations Manager mahdollistaa käytännössä pääsyn lähes kaikkeen, mitä valvottavassa verkkoympäristössä on. Usein ei kuitenkaan haluta, että jokainen ylläpitohenkilö pääsee aivan kaikkeen käsiksi. Tämä on ratkaistu roolipohjaisella käyttäjäoikeuksien hallinnalla. Roolilla käsitetään sekä profiili (mitä toimintoja roolissa olevan operaattorin on mahdollista käyttää) ja ulottuvuus (kuinka laajasti nämä toiminnot ovat käytössä). OpsMgr:ssa on sisäänrakennettuna kolme profiilia, jotka ovat administrator (ylläpitäjä), author (alkuunpanija) ja operator (operaattori). Näistä ensin mainitussa on kaikki oikeudet kaikkeen, joten tarkkaa harkintaa tulee noudattaa. Author -profiili omaa myös laajat oikeudet, kuten asennettujen hallintapakettien sääntöjen luonti ja muokkaus. Operaattorit ovat yleensä keskittyneet valvontaan muutosten tekemisen sijaan.

Käyttäjät voidaan sijoittaa suoraan sisäänrakennettuihin profiileihin, jos heille ei ole tarvetta tarkentaa pääsyn kohteita. Roolille voidaan kuitenkin määrittää tarkemmin, mihin kaikkeen profiilin oikeudet kohdistuvat. Esimerkiksi sähköpostipalveluiden valvontaan keskittyvä henkilö voidaan laittaa operaattoriryhmään ja sallia näkyvyys vain Exchange -palveluille. Rooleja voidaan perustaa niin paljon kuin on tarve ja muokata niitä tarpeiden mukaan. Tällöin käyttäjähallintaa on helppo valvoa ja tarvittaessa muokata. Myös vastuidenjako ja ongelmatilanteiden ratkonta on vaivattomampaa. (Chappell, D. Introducing SCOM 2007, 23)

4 Hajautetut sovellukset (distributed applications)

Tämän opinnäytetyön pääteemana on hajautettu sovellus ja sen mallintaminen Operations Managerilla. Näitä asioita käsitellään tässä kappaleessa pääpiirteittäin ja kerrotaan mitä ne ovat, mistä ne koostuvat ja mikä on niiden asema verkkoympäristössä. Työssä ei käsitellä hajautettuja sovelluksia yleisellä tasolla kovin laajasti, vaan keskitytään työn produktina syntyvään Extranet-sovellukseen ja sen suunnitteluun Operations Managerilla (kappale 5).

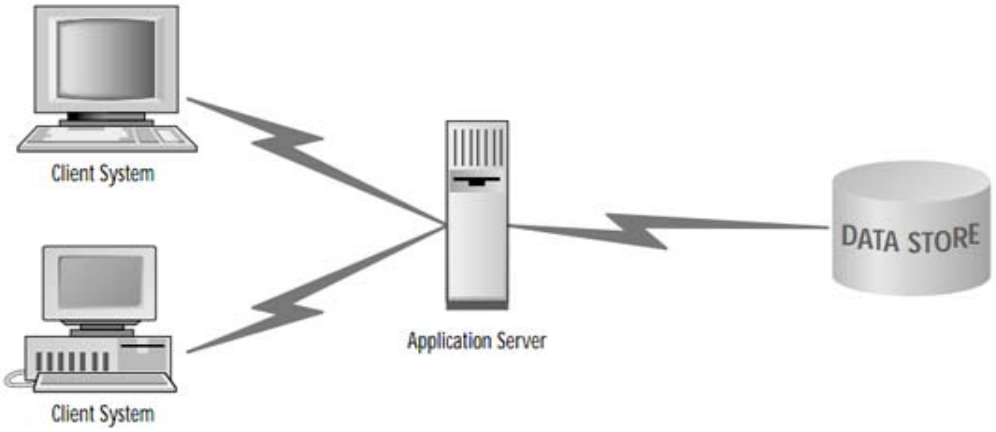
4.1 Määritelmä ja arkkitehtuuri

Hajautetun sovelluksen määritelmä täyttyy, kun verkossa operoiva ohjelma tai palvelu käyttää kahta tai useampaa fyysistä porrasta toimintaansa. ”Työasema-palvelin” -yhdistelmässä se jakautuu kahteen osaan, niin kutsuttuihin ’front end’ (ensisijainen käyttö) ja ’back end’ (taustakäyttö) puoliin. Front end on yleensä työasemapuoli, joka vaatii vain minimiresurssit. Back end-puoli koskee palvelinta ja/tai tietokantaa, jonka vaatimukset ovat yleensä korkeammat sen käsitellessä suuria määriä tietoa. Näistä syntyy aiemmin työssä käsitelty end-to-end -käsite. Laajemmassa hajautetussa sovelluksessa voi olla useita front- ja back end -pisteitä.

Hajautetun sovelluksen idea pohjautuu pidemmän ajan takaa ohjelmistosuunnittelun maailmasta, kun työasema ja palvelin saatiin kommunikoimaan keskenään. Se on esimerkkinä yksinkertaisin ja sitä kutsutaan arkkitehtuurisesti kaksiportaiseksi (Two-tier) hajautetuksi sovellukseksi. Näitä ratkaisuja on edelleen laajalti käytössä monissa eri sovelluksissa. Tällainen on esimerkiksi web-selaimesta palvelimelle lähtevä lomaketieto, josta saadaan vahvistusviesti vastaanotetusta tiedosta. Tällaisen ympäristön vianhallinta on melko yksinkertaista, eikä tarvitse välttämättä OpsMgr:n tasoista ohjelmistoa rinnalle.

Hieman edistyksellisempi kolmiportainen (Three-tier) sovellus on nykyisin yleinen arkkitehtuuri monessa yrityskäytössä olevassa sovelluksessa. Kuvio 5 kuvaa kyseistä tilannetta, jossa välissä oleva palvelin (Application Server) hallinnoi tiedon jakamista ja käsittelyä tietokannan (Data Store) ja käyttäjän (Client System) liittymän välillä. Käytännössä tällainen ratkaisu voisi olla esimerkiksi yksittäinen intranet (organisaation oma lähiverkko) tai extranet (myös asiakkaille ja kumppaneille) sovellus.

Näistä esimerkeistä saadaan sovellettua vieläkin laajempia ja monimutkaisempia sovelluksia. Arkkitehtuurisesti ne ovat kolmiportaisia sovelluksia, joissa portaita on jaettu useampiin kerroksiin (layer) ja kaikilla kerroksilla voi olla useita komponentteja, jotka muodostavat loogisen kokonaisuuden. (Meyler ym., 2007, 950-953)



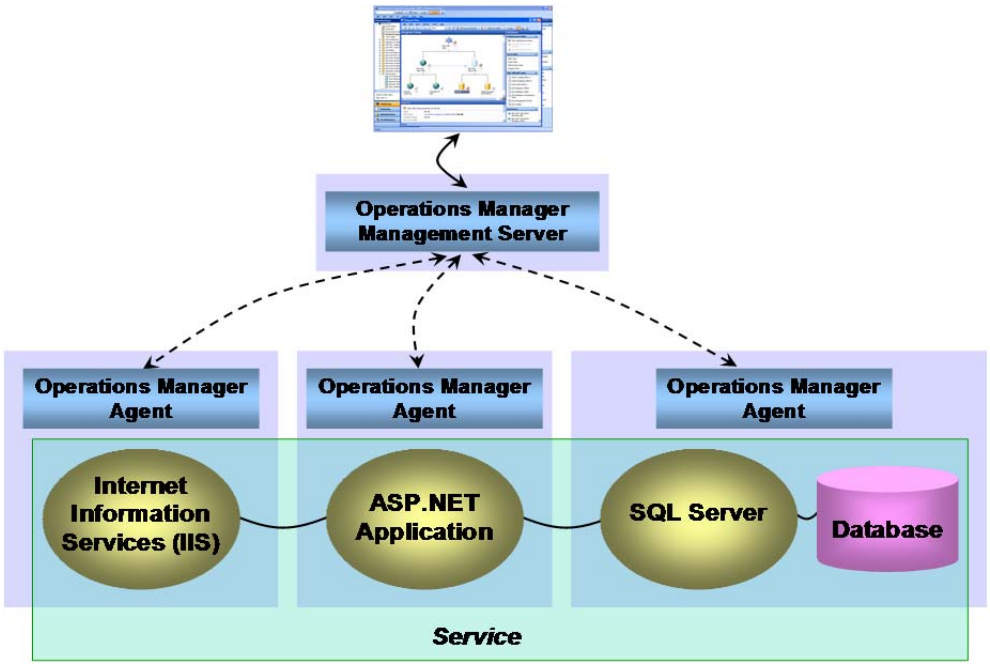
Kuvio 5. Kolmiportainen arkkitehtuuri

4.2 Hajautetun sovelluksen hallinta OpsMgr:lla

Jokaisen IT-osaston tavoitteena on tarjota yritykselle vakaita ja toimivia palveluita. IT-infrastruktuurin eri osien hallinta ja järjestelmällinen valvonta on huomioon otettava asia. Liiketoimintaa tekevät ja pyörittävät ihmiset eivät ole kiinnostuneita yksittäisistä teknisistä seikoista, vaan siitä, toimiiko jokin palvelu kokonaisuutena, kuten sähköposti. Ylläpitäjä joutuu ottamaan huomioon useita eri seikkoja. Jokainen palvelu pitää sisällään ison joukon perustana olevia palveluita ja komponentteja, joista se on riippuvainen, sekä ohjelmisto- että laitetasolla. Pelkän ohjelmiston osasten yksittäinen tarkastelu ei riitä. Operaattorin (ylläpitäjä) on tärkeää ymmärtää, että jokainen pieni pala kokonaisuutta on yhtä tärkeä liiketoiminnalle ja jokaiseen tulisi panostaa sekä kiinnittää huomiota samalla painoarvolla. Perinteisestä teknologiakeskeisestä näkökulmasta on siis aiheellista siirtyä asiakaslähtöisempään palvelunäkökulmaan ja hahmottaa kokonaisuuden tärkeys. Tämä seikka tulisi huomioida jo määrittelyssä ja mietittäessä mukaan otettavia komponentteja.

Kuten aiemmissa kappaleissa on käynyt ilmi, OpsMgr pystyy valvomaan lähes kaikkea, mikä liittyy hajautettuun sovellukseen valittuihin objekteihin. Niihin pystytään myös vaikuttamaan hyvinkin laajasti pääkäyttäjätason (administrator) oikeuksia käyttämällä. Distributed Applications -hallintaominaisuudet ovat OpsMgr:ssa ehkä parhaita vahvuuksia, jotka tuovat esille end-to-end palvelunhallinnan periaatteita. Tämä pätee niin yksinkertaisiin kuin monimutkaisempiinkin kokonaisuuksiin. Ominaisuudet pääsevät oikeuksiinsa tosin vasta sitten, kun niiden pohjalta on tehty suunnittelua ja niitä käytetään tehokkaasti hyödyksi. Tämä vaatii paitsi perehtymistä ohjelmiston mahdollisuuksiin, niin myös pidempiaikaista testaustyötä omassa ympäristössä. Oleellisinta on löytää eri komponenttien vaikutus kokonaisuuteen eri tilanteissa, kuten vian sattuessa.

Kuviossa 6 on mallinnettu yksinkertainen esimerkki siitä, miten useamman komponentin omaava sovellus mallintuu OpsMgr:iin. Keskimmäinen ASP.NET –sovellus kuvaa pääkomponenttia, jota tukevat IIS-, (Internet Information Services) ja SQL (Structured Query Language) -tietokantapalvelimet. Lisäksi mukaan kuuluu verkko, joka yhdistää ja toimii tiedonvälittäjänä sekä joitain verkkolaitteita, kuten kytkin tai palomuuri, jotka ohjaavat tietoliikennettä oikein. Pääkomponenteissa olevat agentit (Operations Manager Agent) valvovat niiden tilaa ja raportoivat suoraan hallintapalvelimelle (Management Server), josta nähdään sovelluksen kokonaiskuva ja tilatietoja kaikista yksittäisistä palasista. (Chappell, D. Introducing SCOM 2007, 8-9)



Kuvio 6. Esimerkki hajautetun sovelluksen toimintaperiaatteesta

Operations Managerissa itsessään on sisäänrakennettuna useampi valmiiksi määritelty hajautettu sovellus. Seuraavassa mainitaan kolme merkittävintä pohjaa. Näistä ensimmäinen on ***Operations Manager Management Group***, joka käsittää valmiin paketin hallintaryhmän luomiselle omassa ympäristössä. Tällä saadaan siis valmis pohja (template) lähtökohdaksi omalle toiminnalle, jota lähdetään edelleen kehittämään omien tarpeiden mukaiseksi. Tähän hajautettuun sovellukseen on laitettu valmiiksi työkaluja, joita tarvitaan jokaisen hallintaryhmän monitoroinnissa.

Toinen valmis hajautettu sovellus (Distributed Application) on ***Active Directory Topology Root***, joka on asennettu Active Directoryn omasta hallintapaketista (Management Pack). Tästä on hyötyä sitä enemmän, mitä laajempi AD-ympäristö on ja mitä laajemmalle se on levittäytynyt. Tähän hajautettuun sovellukseen on määritelty valmiiksi kaikki tärkeimmät ja oleellisimmat valvontakohteet AD:lle, joten oman työn osuus helpottuu selvästi.

Kolmas valmiiksi määritelty hajautettu sovellus on Exchange Service, joka tulee Exchange -hallintapaketista. Exchange Server on yksi maailman eniten käytetyimmistä palveluista yrityksissä tarjoamaan sähköposti-, kalenteri- ja yhteisöviestintäpalvelut. Se on myös toiminnaltaan erittäin palvelukriittinen, eikä sallisi yhtään käyttökatkosten aiheuttamia viivästyksiä. Se on monimutkainen ja haastava valvottava, sillä siinä on paljon itsenäisiä komponentteja, joista yhdenkin ongelmallinen toiminta voi estää esimerkiksi sähköpostin kulun. (Meyler ym., 2007, 958-966)

4.2.1 Distributed Application designer

Hajautettua sovellusta voidaan lähteä suunnittelemaan perinteisin keinoin, kynällä paperille, kuten aiemmin on tehty ohjelmistosuunnittelussa. Toinen vaihtoehto on käyttää jotain erillistä suunnitteluohjelmistoa. OpsMgr:n konsolissa itsessään on valmiina työkalu, jonka avulla mallintaminen on hieman helpompaa. Sen käyttöliittymä on graafinen ja se mahdollistaa objektien hakemisen ja yhdistelemisen verkkoympäristöstä. Hajautetun sovelluksen luontiin voidaan käyttää valmista mallipohjaa tai luoda oma pohja. Uutta sivupohjaa (template) voidaan käyttää myöhemmin kokonaisuutena esimerkiksi isomman hajautetun ympäristön osana, mikäli sen komponenteista joku tai kaikki liitty-

vät ympäristöön. Tällöin siitä tulee hallittu osa suurempaa ketjua, joka kuuluu automaattisesti valvonnan piiriin olemassa olevilla määrityksillä ja säännöillä. Tarpeen mukaan sääntöjä voidaan muokata uuteen kokonaisuuteen sopiviksi.

Valmiista esimääritellyistä pohjista voidaan valita esimerkiksi ”Line of business Web Application”, jota on käytetty myös tämän työn produktissa. Se on perusta web-pohjaiselle palvelulle, joka sisältää valmiiksi komponentit verkkosivulle ja tietokannalle ja jonka valvonnan alaisuuteen voidaan lisätä suoraan uusia komponentteja. Jos valmiista pohjista ei löydy sopivaa, voidaan suunnittelu aloittaa täysin tyhjältä pöydältä.

Distributed Application Designer tallentaa automaattisesti komponentit, objektit ja mallin hallintapakettiin (Management Pack). Samalla kun se tekee mallin, tekee se myös oletusnäkymät kuten diagramminäkymän, joka kertoo visuaalisesti komponenttien relaatiot. Myös hälytysnäkymä on erikseen. (End-to-end Whitepaper, 2007, 6-7)

5 Case: Extranet-sovelluksen suunnittelu

Opinnäytetyön raportointiosuuteen haluttiin ottaa mukaan käytännön produkti, koska sen toteutukselle oli tarvetta kohdeyrityksessä. Samalla saatiin aikaan dokumentointi määrittelystä mallinnukseen. Kyseessä ei ole testiympäristö, vaan hajautettu sovellus suunnitellaan suoraan käyttöönotettavaksi olemassa olevaan todelliseen ympäristöön. Käyttötapaukseksi valittiin Extranet-sovellus, johon sisältyy erilaisia palvelimia ja palveluita sekä verkon aktiivilaitteita. Näistä syntyy dynaaminen kokonaisuus, jossa komponentit ovat relaatiossa keskenään ja välittävät tietovirtoja toisilleen. Kokonaisuudesta saatiin mallinnettua OpsMgr:n avulla hajautettu sovellus (Distributed Application) ja topologiakuvaus (liite 3), josta nähdään mukana olevat objektit ja niiden riippuvuussuhteet.

Produktin tarkoituksena on luoda mallinnus ja määrittelyitä käyttöönotettavalle sovellukselle, joka on tarkoitus lisätä seuraavassa vaiheessa monitoroinnin piiriin. Tällä haetaan tehokkuutta ja toimintavarmuutta, jotta saadaan pidettyä palvelutaso mahdollisimman korkeana. Tämä auttaa myös jatkossa hallitsemaan ympäristöä paremmin, kun sovellukset ovat jaettu loogisiin kokonaisuuksiin, joita on helpompi käsitellä. Mallinnettuun kokonaisuuteen on jälkeenpäin mahdollista lisätä uusia tai poistaa olemassa olevia komponentteja.

Extranetin käyttöliittymä on internet-selainpohjainen ja sisäänpääsy vaatii käyttäjätunnuksen ja salasanan. Sovelluspalvelin on sijoitettu yrityksen verkkoympäristössä niin sanotulle suojavyöhykkeelle (Demilitarized Zone, liite 1), joka on erillään yrityksen sisäverkosta. Tämä takaa huomattavan tietoturvan, kun ulkoverkosta tulevat yhteydet eivät tule yrityksen sisäverkkoon, vaan palomuurin läpi suojavyöhykkeelle. Myös sisäverkosta Extranet:iin lähtevä yhteys kulkee oman palomuurin läpi.

5.1 Määrittely ja mallinnus

Hajautettu sovellus on luonteeltaan dynaaminen ja tällöin riippuvainen useammasta tekijästä. Uuden sovelluksen käyttöönotossa selkein ja johdonmukaisin lähtökohta on selvittää ensin, mitä kaikkia objekteja tarvitaan mukaan, ja sen jälkeen mallintaa topologinen kaavio, mistä nähdään objektien sijoittuminen verkossa. Tämä helpottaa huomattavasti sovelluksen toteuttamista esimerkiksi OpsMgr:lla. Lähtökohtaisesti ohjelmistoteknisiä haasteita voisivat olla esimerkiksi laajennettavuus, vikasietoisuus ja skaalautuvuus (joustavuus, mukautuvuus), mutta OpsMgr:n toimintojen ja mahdollisuuksien puitteissa näitä ongelmia ei käytännössä tarvitse huomioida mallinnuksessa.

Koska kohdeyrityksen Extranet-ympäristö oli jo olemassa ja toiminnassa, ei sitä tarvinnut suunnitella ja määritellä uudelleen. Tämän johdosta tiedettiin valmiiksi kaikki siihen liittyvät olennaiset komponentit, joten päätettäväksi jäi se, mitkä kaikki niistä otetaan monitoroitavaan sovellukseen mukaan. Minimissään valvottavana olisi vain sovelluspalvelin ja SQL-tietokanta, mutta saatu hyöty olisi olematon, koska ongelma voisi olla monessa muussakin verkon risteyskohdassa, eikä sitä tällöin helposti havaittaisi. Opinnäytetyön puitteissa ei määritelty Extranet-sovellusympäristöä hajautetuksi sovellukseksi aivan täydellisenä, mutta siitä mallinnettiin pohja, jossa on mukana käytännössä kaikki siihen tässä vaiheessa liittyvät komponentit. Operations Manager sallii hajautetun sovelluksen vapaan muokkaamisen, joten niistä ei tarvitse tehdä kerralla lopullisia versioita. Produktiin kuuluvia komponentteja käsitellään kappaleessa 5.2 ja MS Visiolla luotu mallinnus Case:n sovelluksen verkkokaaviosta on liitteessä 3.

5.2 Kokoonpanon komponentit

Opinnäytetyön osalta varsinaiseen hajautettuun sovellukseen ei otettu mukaan aivan kaikkia mahdollisia komponentteja, sillä niiden määrittely osoittautui aikaa vieväksi ja työlääksi. Toisaalta jokaisen mahdollisen palvelun valvominen ei välttämättä olisi johdonmukaista, joten tarvekartoituksessa tulee seuloa, mikä palvelut vaikuttavat sovelluksen toimintaan oleellisesti. Kokoonpanon osalta päädyttiin käsittelemään ensimmäisen vaiheen perusversiota, jonka mallinnus on jo aloitettu MS Vision lisäksi myös suoraan Operations Managerin Distributed Application Designeriin. Nykyistä verkkomallinnus-

ta tullaan täydentämään ja kehittämään tämän työn jälkeen. Seuraavassa on käyty läpi peruskomponentit, jotka tulevat valvonnan alaiseksi toisessa vaiheessa.

Sovelluspalvelin on hajautetun sovelluksen tärkein komponentti ja se hallinnoi lähes kaikkia Extranetin toimintoja. Palvelin käsittää käytännössä suurimman osan kyseisen hajautetun sovelluksen palveluista. Sovelluspalvelimelle on asennettu itse Extranet-sovellus, joka tarvitsee tuekseen joukon erilaisia Windows-palveluita. Näitä ovat esimerkiksi tietokantapalvelut (IIS, SQL), etäkäyttöpalvelut (Terminal Services, Remote Desktop) ja tulostuspalvelun (Print Services). Sovelluspalvelin toimii samalla Extranetin projektiarkistona. Se on varustettu Windows Server-käyttöjärjestelmällä, joten sitä valvoo oma agentti.

Web-palvelin on niin sanottu julkinen palvelin ja sovelluksessa keskeisin komponentti, joka toimii alustana palveluun sisäänkirjautumiselle ja selainpohjaiselle käyttöliittymälle. Palvelin on sijoitettu fyysisesti suojavyöhykkeelle (DMZ, kappale 6.3). Tällä minimoidaan hyökkäyksen vaikutuksia, sillä web-palvelimelle päästyään mahdollisella verkkohyökkääjällä on edessään toinen palomuuri, joka tekee sisäverkkoon pääsyn hyvin vaikeaksi. Web-palvelin on myös oman agentin valvonnassa.

MS SQL Server -tietokantapalvelin on asennettuna sovelluspalvelimelle ja hallinnoi extranetin tiedonhakua ja tietokantoja. Se tarjoaa tekniikan tehdä hakuja arkistosta ja etsiä materiaalia. Se on myös helposti laajennettavissa tietomäärän kasvaessa. SQL-server on osa sovelluspalvelinta, joten sille ei ole omaa agenttia, vaan palvelimen agentin tehtäviin kuuluu valvoa myös sitä. Se on kuitenkin yksi tärkeimmistä palveluista, joten sen erillinen seuranta on aiheellista. Ei riitä, että tiedetään, jos koko palvelin ei ole toiminnassa, vaan tarvitaan välitön informaatio myös tietokantapalvelun vikatilanteista.

Internet Information Services (IIS) on keskeinen komponentti web-palvelimella, jonka tulee olla toiminnassa katkotta. Siihen liittyen toiminnassa on erilaisia MS Access -tietokantoja ja se tarjoaa extranetin kirjautumispalvelun ja käyttäjän tunnistautumisen. IIS palvelu on myös sovelluspalvelimen sisäinen palvelu, ja sen avulla voidaan käyttää selainpohjaista webaccess-liityntää tässä kappaleessa alempana esiteltävän Remote Desktopin sijasta. Myös IIS on palvelimen agentin valvonnassa erillisenä palveluna.

Oracle Client on Oraclen tietokantayhteyteen tarkoitettu erillinen sovellus. Se on toiminnassa sovelluspalvelimella. Sen avulla saadaan toiselta tietokantapalvelimelta siirrettyä ja välitettyä tietoa muualla toimivalle Oracle-palvelimelle, eikä tällöin tarvitse ottaa erillistä yhteyttä. Sovelluksen edut kasvavat, jos ympäristössä on useampia tietolähteitä, joiden tarvitsee välittää tietoa Oracle-palvelimelle. Tämä komponentti kuuluu muiden tietokantaobjektien tavoin palvelinagentin alaisuuteen.

Terminal Services-palvelu on myös yksi tärkeistä yhteystoimintoja tarjoavista palveluista, jota tulee monitoroida. Sen avulla saadaan etäyhteydellä käyttöön sovelluspalvelimen työpöytä ja sovellukset, ikään kuin ne olisivat paikallisella laitteella. Tätä voidaan hyödyntää paitsi ylläpitäjien toimesta ylläpidollisissa tehtävissä, niin myös käyttäjien toimesta tavallisten toimenpiteiden hoitamiseen. Jos tähän palveluun tulee katkos, ei sovelluspalvelimelle käytännössä pysty ottamaan etäyhteyttä.

Remote desktop (RDP)-palvelun avulla mahdollistetaan etäkäyttö joko ohjelmistopohjaisesti erillisellä Windows-sovelluksella tai web-sivustoa hyödyntämällä. Se on kriittinen palvelu ja on prioriteetiltään korkealla, jolle ei sallita katkoksia kovin pitkäksi aikaa. Nämä tulee huomioida määriteltäessä hälytysrajoja ja niiden luonnetta Operations Managerin puolella. Remote Desktop-palvelu on ikään kuin työkalu, jolla hyödynnetään Terminal Services -palvelua ja sillä saadaan kohdeaseman työpöytänäkymä graafisena omalle näytölle.

Internet Service Provider Router (ISP-reititin) on internetyhteyden palveluntarjoajan reititin, joka jakaa liikennettä ja ohjaa halutut osoitekyselyt oikeaan paikkaan, kuten tässä tapauksessa ensin DMZ:lle ja edelleen extranet-palvelimelle. Reitittimet eivät sisällä käyttöjärjestelmää, joten niiden valvontaan tullaan käyttämään SNMPv2 (kappale 3.3) valvontatekniikkaa, johon riittää käytännössä verkkoyhteys. Diagnosoitavaksi saatavan tiedon sisältö voi olla kovin suppeaa, mutta usein verkkolaitteista riittää tieto siitä, ovatko ne toiminnassa ja kulkeeko verkkoliikenne oikein.

Intrusion Prevention System (IPS-laite) sijoittuu reitittimestä seuraavaksi, jonka läpi liikenne kulkee. Sen tehtävänä on valvoa liikennettä ja havaita siinä mahdollinen haitallinen aktiviteetti. Tämä pienentää riskiä sille, että suojavyöhykkeelle asti pääsisi haitallis-

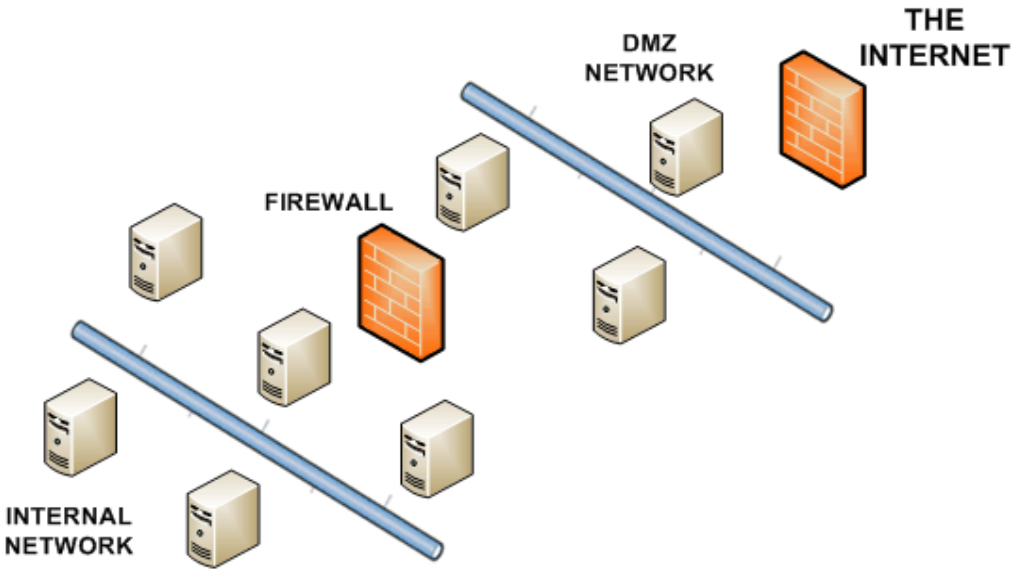
ta liikennettä tai verkkohyökkäyksiä. Analysoinnin ohella se lähettää tilannetietoja palvelimelle liikenteen tilasta. IPS-laite ei ole välttämätön, mutta se tuo vakautta ja turvaa verkkopalveluille. Sen monitorointiin sovelletaan myös SNMP-käytäntöä.

Palomuurit ovat liikenteen suodattajia. Ne valvovat paitsi hyökkäyksiä niin myös eitervetullutta muuta haittaliikennettä. Yrityksen verkossa voi olla useita palomuureja suorittamassa eri tehtäviä, jos verkko on jaettu moneen osaan. Nykyään monet palomuurit kykenevät hallitsemaan useamman verkon yhtäaikaista suodatusta, mutta on turvallisempaa edelleen käyttää useampaa laitetta, kuten esimerkiksi DMZ:n molemmilla puolilla, sisä- ja ulkoverkon liikenteelle. Palomuurit ovat myös agentittomia, joten ne saadaan valvontaan kuten reititin ja IPS-laitekin.

5.3 Demilitarized Zone

Demilitarized Zone on yrityksen omasta sisäverkosta eristetty verkkoalue, niin kutsuttu suojavyöhyke. Fyysisesti se sijoittuu internetin ja sisäverkon väliin ja sen tarkoituksena on lisätä tietoturvaa internetistä tulevien yhteyksien ja uhkien varalta. Suojavyöhykkeelle voidaan sijoittaa esimerkiksi julkisia palvelimia, joilla on tarve olla yhteydessä internettiin. Tällöin niitä ei tarvitse sijoittaa yrityksen omaan sisäverkkoon. Lisäksi DMZ:n molemmin puolin on yleensä asetettu palomuurit valvomaan liikennettä. Ne tulisi määritellä sallimaan vain välttämättömät yhteydet niin internetistä DMZ:lle kuin myös DMZ:lta yrityksen sisäverkkoon. (Techrepublic, DMZ, 2005)

Kohdeyrityksessä oli jo valmiina oma suojavyöhykealiverkko, joten sitä ei tarvinnut pystyttää erikseen. Extranetin sovelluspalvelin oli sijoitettu sinne, ja näin myös asiakkaat pääsevät kirjautumaan palvelimelle suoraan internetistä. Tietoliikenteen reititys on hoidettu niin, että sisäverkosta yhdistettäessä käytetään sisäverkon osoitetta ja ulkoverkosta tultaessa palomuuri ja kytkin (yhdistää verkon osia toisiinsa) osaavat ohjata liikenteen suojavyöhykkeelle, kun Extranetin kirjautumissivua ladataan internet-selaimessa. Web-palvelimesta poiketen pääpalvelin ei ole DMZ:lla, vaan sisäverkossa.
Kuviossa 7 on havainnollistettu suojavyöhykkeen sijoittuminen verkkoympäristöön. Se on käytännössä aina kahden palomuurin (Firewall) välissä, eikä sieltä ole suoraa uhkaa yrityksen sisäverkolle.



Kuvio 7. DMZ-alueen sijoittuminen verkossa

5.4 Casen yhteenveto

Case-osuuden tavoitteena oli suunnitella ja määritellä kokoonpano hajautetulle sovellukselle (Extranet-ympäristö) sekä mallintaa se verkkokaavioksi. Tämä on ensimmäinen vaihe projektille, jonka seuraavassa vaiheessa sovellus otetaan OpsMgr:lla tapahtuvan palvelunvalvonnan piiriin. Diagrammikaavion (liite 4) mallin mukaisesti hajautetun sovelluksen suunnittelu on aloitettu myös Operations Manager designerilla, mutta se on tässä vaiheessa kesken, eikä esimerkiksi mitään hälytysrajoja tai sijaisagenttimäärityksiä ole vielä tehty. Ne tullaan toteuttamaan tämän opinnäytetyön jälkeen. Tässä vaiheessa ei nähty tarpeelliseksi suorittaa hälytyksiin liittyviä määrittelyjä erikseen, koska ne olisivat vaatineet aiheeseen liittyvää käsittelyä laajemmin ja työssä käsiteltävä sisältö olisi paisunut turhan laajaksi. Liite 4 näyttää kuitenkin esimerkkinä, millaisen kaavionäkymän Operations Managerin hajautetun sovelluksen suunnittelutyökalu antaa. Näkymiä on erilaisia, kuten ”terveydentilakaavio”, josta ilmenee sen hetkiset ongelmakomponentit tai mahdollisesti tulevat ongelmat, jotka kannattaa tarkastaa ajoissa.
Case-osuuden tavoitteet saavutettiin suunnitellulla tavalla. Määrittely ja mallinnus saatiin siihen vaiheeseen, että Operatios Manageriin voi lisätä loputkin objektit, jonka jälkeen tapahtuu erilaiset hälytysmääritykset. Mallille tuli dynaamisuutta ja muokkausva-

raa, sillä myöhemmin siitä voidaan poistaa tai siihen voidaan lisätä halutessa objekteja. Tällöin vain uusien objektien omat määrittelyt tulee huomioida, muuten ne ovat tervetulleita sovellukseen. Extranet-sovelluksen ottaminen monitoroinnin alaisuuteen kokonaisuudessaan jo tässä vaiheessa olisi ollut liian laaja paitsi ajallisesti, niin myös työmäärällisesti. Nyt projekti on jaoteltu muutamaan eri osaan, mikä selkeyttää koko suunnitteluprosessia. Lopputuloksena voidaan todeta, että palvelutason ja valmiuden nostossa on edetty jälleen askel eteenpäin ja käyttöönottoprojekti voi jatkua.

6 Yhteenveto ja pohdinta

Tässä opinnäytetyössä perehdyttiin hajautetun sovelluksen määrittelyyn ja mallinnukseen Microsoftin järjestelmänhallintaohjelmisto System Center Operations Manager 2007 R2:n avulla. Mallinnus toteutettiin olemassa olevan verkkoympäristön Extranet-sovellukselle. Opinnäytetyössä käsiteltiin myös palvelunhallintaa yleisesti liiketoiminnassa ja sitä, miten siihen tarkoitetun ohjelmiston käyttöönotto ja hyödyntäminen vaikuttaa IT-yksikön toimintaan ja työskentelymalleihin.

6.1 Päätelmät

Kohdeyrityksessä on jo jonkin aikaa ollut käytössä kyseinen Operations Manager hallintaohjelmisto ja sen on todettu olevan hyödyllinen hankinta. Se on tuonut lisäarvoa jo yksinkertaisessa peruskäytössä, esimerkiksi ilmoittaessaan sähköpostilla, jos jokin palvelin ei ole jostain syystä käytettävissä. Tällainen käytäntö sopii pienelle yritykselle muutamien palvelinten hallintaan, mutta kun kyseessä on selvästi suurempi ympäristö ja paljon komponentteja, tarvitaan hieman pidemmälle vietyjä menetelmiä.

Ilman minkäänlaista hallintaohjelmistoa verkkoympäristön valvonta ja sitä kautta palveluiden toimintavarmuuden takaaminen ovat heikolla pohjalla. Toiminta on reaktiivista, mikä tarkoittaa käytännössä sitä, että odotetaan jonkin vian tapahtuvan ja ilmenevän jotain kautta ja vasta sitten aletaan toimenpiteisiin. Kun yrityksen toiminta ja koko kasvavat, myös IT-ympäristön infrastruktuuri kasvaa, mikä tarkoittaa kasvavaa riskiä IT-palveluille, kun laitekapasiteetti ja valvonnan määrä lisääntyvät. Jos vikatapausten ja palvelukatkosten määrä alkaa lisääntyä, liiketoiminta kärsii vääjäämättä.

Hallintaohjelmiston käyttöönotto on jo sinänsä askel kohti proaktiivista toimintaa, mutta hajautettujen sovellusten kokonaisvaltainen kartoittaminen ja lisääminen monitoroinnin piiriin tuovat vieläkin enemmän etuja pitkällä tähtäimellä. Se auttaa ennakoimaan ja sitä kautta välttämään suurempia palvelukatkoksia tai laiterikkoja. Lisäksi se selkeyttää hallintaa IT-ylläpidon näkökulmasta, koska isompia kokonaisuuksia saadaan nivottua yhteen eikä kymmeniä, tai jopa satoja yksittäisiä komponentteja, tarvitse valvoa erikseen.

Prosessi ei ole kuitenkaan aivan yksinkertainen, vaan se vaatii suunnitelmallista etenemistä. Kokonaisuudet tulee mallintaa huolellisesti ja miettiä, mitkä objektit kannattaa sisällyttää mihinkin hajautettuun sovellukseen. Päällekkäisyyksiä tulisi pyrkiä välttämään ja saada aikaan loogisia kokonaisuuksia, sillä ympäristön kasvaessa on tärkeää, että valvonta on systemaattista eikä ”pirstaloitumista” pääse syntymään. Lisäksi jos valvottavia objekteja otetaan holtittomasti keräämään tietoa eri paikoista, saattaa sen hallinta ja olennaisen asian seulonta vaikeutua. Tietomäärän kasvaessa ja fyysisten laitteiden lisääntyessä kannattaa laajempia valvottavia kokonaisuuksia jakaa useampien eri ylläpitohenkilöiden alaisuuteen niin, että tietty henkilö vastaa tietystä kokonaisuudesta.

6.2 Opinnäytetyöprosessi

Kuten työn alussa todettiin, idea yhdistää opinnäytetyö käytännön työelämän projektin kanssa syntyi yrityksen tarpeesta tehostaa palvelunhallintaa ja palvelinympäristön valvontaa. Mahdollisuuksia valita sopiva sovelluskohde oli lukuisia ja prosessin alussa punnittiinkin, mikä olisi työn laajuuteen ja yrityksen tarpeisiin nähden sopiva kohde. Lopulta päädyttiin valitsemaan Extranet-ympäristö ja siihen liittyvät komponentit.

Produktin prosessi lähti liikkeelle tarvekartoituksesta, jota ei kuitenkaan dokumentoitu erikseen mainittavasti, vaan kirjattiin ylös pääpiirteittäin, mitä tarvittaisiin ja mitä lähdetään hakemaan projektilta. Samalla, kun suunniteltiin hajautetun sovelluksen mallintamista ja toimintaa, päätettiin opinnäytetyön viitekehyksen sisällöstä ja rakenteesta. Koska Operations Manager on toteutettu ITIL-, ja MOF-kehysten pohjalta, päädyttiin käsittelemään niitä palvelunhallinnan näkökulmasta. Tästä saatiin myös hieman uusia vinkkejä ja mahdollisia toimintatapojen kehittämisideoita yrityksen koko tietotekniikkaympäristön hallintaa silmällä pitäen.

Kun tarvittavat komponentit ja palaset oli mallinnettu verkkotopologiaksi Microsoft Visio-ohjelmalla sekä teoriapohja selvennetty, alettiin sovellusta suunnitella suoraan OpsMgr:iin sen omalla Distributed Application Designer:lla. Tämä osoittautui aluksi hieman hankalaksi ja vaatikin jonkin aikaa selvittää, miten objektien lisääminen tapahtuu oikeaoppisesti ja miten niiden riippuvuussuhteet toisiinsa saadaan määriteltyä oikein. Operations Manager on kuitenkin melko pitkälle automatisoitu ohjelmisto, eikä

käsin tehtävää määrittelyä tarvita kovinkaan paljon. Tämä prosessi jatkuu myös opinnäytetyön valmistumisen jälkeen.

Opinnäytetyöprosessi kokonaisuudessaan onnistui pitkälti suunnitelmien mukaisesti ja teoriaosuuden viitekehys saatiin halutunlaiseksi. Käytännön suunnittelussa ongelmia tuotti eniten kokemuksen puute Operations Managerin käytössä ja sen hallinnan käytännön tietämyksestä. Alun perin suunnitelmana oli toteuttaa tämän työn puitteissa myös koko hajautetun sovelluksen hallinnan ja monitoroinnin määrittely ja käyttöönotto, mutta se osoittautui liian suureksi kokonaisuudeksi. Näin ollen päädyttiin käsittelemään määrittelyn ja mallinnuksen lisäksi palvelunhallintaa sekä itse Operations Managerin toimintaa suurpiirteisesti. Nämä toimivat luonnollisesti tukena projektin edetessä seuraavaan vaiheeseen.

Teoriaosuudessa suurin haaste oli löytää lähdemateriaalia ja saada siihen perustuvaa rakentavaa lähdekritiikkiä, koska vertailtavia ohjelmistoja ei ollut soveliasta ottaa työhön mukaan. Vaihtoehtoisia toteutustapoja ei myöskään käytännössä ole tai sellaisten soveltaminen Operation Managerin kanssa samaan aikaan yrityksen ympäristöön olisi ollut lähes mahdotonta. Sitä varten olisi pitänyt perustaa erillinen testiympäristö, mutta tähän ratkaisuun ei nähty tarvetta lähteä.

Prosessin aikana projektiin osallistuneet henkilöt kokoontuivat 3-4 kertaa. Tällöin käytiin läpi vaatimuksia ja tavoitteita produktin osalta. Mitään varsinaista aikataulua Extranet-sovelluksen määrittelylle ja mallinnukselle valvonnan osalta ei asetettu, vaan se eteni opinnäytetyön raportoinnin kanssa käsi kädessä. Varsinaista ajallista takarajaa ei ollut, vaan päätettiin, että opinnäytetyön osuus päättyy siihen, kun hajautettu sovellus on pääpiirteittäin mallinnettu ja seuraavaan vaiheeseen voidaan siirtyä luontevasti.

Prosessi oli kokonaisuutenaan opettava kokemus paitsi työelämän erillisenä projektina, niin myös dokumentointiprojektina raportointiosuuden puolesta. Projekti auttoi hahmottamaan verkkoympäristöä ja sen toimintaa sekä Operations Managerin toimintaa ja käyttöä. Nämä auttavat huomattavasti seuraavissa vaiheissa siirtyä valvomaan Extranet-sovellusta keskitetysti. Käytännön osuudessa tuli esiin muutamia seikkoja, joita on hyvä huomioida jatkossa vastaavia projekteja tehdessä. Aikataulut tulee asettaa realistisiksi,

mieluummin hieman väljemmiksi, jos kyse on omasta ympäristöstä, eikä asiakkaan vaatimasta aikataulusta. Tarvekartoitus kannattaa suunnitella huolellisesti ja miettiä, mitkä kaikki ovat välttämättömiä, mitkä kenties hyödyllisiä ja mitkä mahdollisesti lisäksi tulevia, ei-kriittisiä objekteja. Suositeltavaa on myös jaotella prosessi osiin niin, että määritetään, mitä tehdään missäkin osassa ja kuinka kauan ne voisivat viedä aikaa. Tästä voidaan tehdä johtopäätös, että Scrum-viitekehykseen (liite 1) perustuva työskentelymalli olisi voinut olla sopiva myös tälle opinnäytetyölle. Osittain sitä käytettiinkin, mutta vain soveltaen ja lähinnä raportointiosuutta tehtäessä, koska varsinaisia työtehtäviä ei voinut laiminlyödä.

6.3 Tavoitteiden saavuttaminen ja tulevaisuus

Kohdeyrityksen IT-infrastruktuuri on elävä ja muuttuva. Ohjelmistollisesti muutoksia tulee kohtalaisen usein ja palveluja pyritään kehittämään kysynnän ja tarpeiden mukaisesti. Myös laitteisto päivittyy säännöllisesti ja verkon rakenne muuttuu muun muassa yritysfuusioiden ja uusien toimipisteiden avaamisen myötä. Nämä kasvattavat IT-osaston työmäärää ja samalla valvottavan ympäristön koko suurenee, mikä lisää myös tarvetta tehostaa verkkoympäristön valvontaa.

Opinnäytetyölle asetetut tavoitteet saavutettiin pääosin kokonaan projektin aikana. Alkuperäisestä tavoitteesta ottaa hajautettu sovellus täysin monitoroinnin piiriin jouduttiin tinkimään, sillä valvonnan toteuttaminen samaan opinnäytetyöhön olisi paisuttanut työn liian suureksi ja vienyt aikaa kohtuuttomasti. Produktilla saatiin kuitenkin aikaan pohja hajautetulle sovellukselle halutusta kokonaisuudesta ja sitä tullaan kehittämään sekä tarkentamaan myös opinnäytetyön jälkeen. Hajautetun sovelluksen etuna on sen täysi muokattavuus, joten jatkossa siitä voidaan poistaa tai siihen voidaan lisätä uusia objekteja ilman, että se sotkee olemassa olevaa kokonaisuutta. Tulevaisuudessa Operations Manageria tullaan käyttämään tehokkaammin hyödyksi muidenkin laajempien sovellusten osalta ja joitain uusia ideoita valvontakokonaisuuksista saatiin syntymään tämän projektin aikana.

Aikataulullisia tavoitteita ei koettu tarpeelliseksi asettaa, vaan kehitys eteni sen mukaan kun aikaa ja resursseja riitti, sillä ohessa oli hoidettavana lukuisia muita työtehtäviä. Teknisiä haasteita työn aikana tuli lähinnä hallintaohjelmiston käytön osalta. Siihen voisi olla ratkaisuna ulkopuolinen koulutus tai konsultointi, mutta niiden soveltuvuus tulisi harkita aina tapauskohtaisesti.

Tulevaisuudessa hajautettujen sovellusten hallinnan ja valvonnan merkitys yrityksissä tulee varmasti kasvamaan. Mitä pidemmälle projekti etenee, sitä ilmeisempää on, että sen merkitys ja tärkeys tulee esiin. Omat kokemukseni osoittautuivat positiivisiksi ja valitulla ohjelmistolla työskentely joustavaksi. Palvelunhallinnan kehittäminen ja hajautettujen sovellusten hallinta ovat luonteeltaan proaktiivista toimintaa. Kun niitä kerran lähdetään viemään yrityksessä eteenpäin ja huolellisesti oikeaan suuntaan, tulevat niiden tuomat edut ja hyödyt väistämättä esiin. Mitä suuremmaksi yrityksen IT infrastruktuuri kasvaa, sitä suurempi merkitys sen kokonaisvaltaisella hallinnalla ja valvonnalla tulee olemaan; ei pelkästään liiketoiminnan kannalta, vaan myös IT-osaston työskentelyn kannalta.

Lähteet

Price, B., Mueller, J., P., Fenstermacher, S. 2007. Mastering System Center Operations Manager 2007. United States.

Meyler, K., Fuller, C., Joyner, J. & Dominey, A., P. 2008. System Center Operations Manager 2007 Unleashed. United States.

Antila J., Ylöstalo P. 2002. Proaktiivinen toimintatapa. Edita Prima Oy. Helsinki

Chappell, D., Chappell & Associates, 2007. Introducing Microsoft System Center Operations Manager 2007. Luettavissa : http://download.microsoft.com/download/0/a/3/0a3913c6-63a9-4442-b616-767789982605/introducing_system_center_operations_manager_2007_v1.5.doc Luettu 18.4.2011

Microsoft, Dell 1/2009. Simplify and Transform Your IT Infrastructure into a Strategic Business Asset. Whitepaper. Luettavissa : http://whitepaper.talentum.com/whitepaper/view.do?id=25051. Luettu 18.2.2011

OGC Official Sites: ITIL. 2010. OGC, TSO, APMG. Luettavissa : http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx Luettu 22.2.2011

Arraj, V. ITIL : The Basics. May 2010. Whitepaper. Luettavissa : http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf Luettu 20.2.2011

Kneller, M. 2010. Executive Briefing: The Benefits of ITIL. Whitepaper. Luettavissa : http://www.best-management-practice.com/gempdf/OGC_Executive_Briefing_Benefits_of_ITIL.pdf. Luettu 23.2.2011

Strengthen network defenses by using a DMZ, Techrepublic, 2005. Luettavissa : http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/5756029 Luettu 24.4.2011

International Organization for Standardization, Information technology, Service management, Part 1: Specification, 2011. Luettavissa : http://www.iso.org/iso/catalogue_detail?csnumber=41332 Luettu 13.4.2011

Microsoft System Center, Operations Manager Overview, 2010. Luettavissa : http://download.microsoft.com/download/a/0/a/a0a7e90b-d20d-4052-8930-53edac404fe0/Whitepaper-System_Center_Operations_Manager_2007_Overview.pdf Luettu 8.3.2011

Microsoft System Center Operations Manager 2007 Documentation, Design Guide, 2008. Luettavissa : http://www.microsoft.com/downloads/en/details.aspx?FamilyID=d826b836-59e5-4628-939e-2b852ed79859&DisplayLang=en Luettu 14.4.2011

Fox, C., Downing, J., Microsoft System Center Operations Manager 2007 Documentation, Operations Guide, 2009. Luettavissa : http://www.microsoft.com/downloads/en/details.aspx?FamilyID=d826b836-59e5-4628-939e-2b852ed79859&DisplayLang=en Luettu 18.4.2011

Microsoft Webcast: Optimizing Application Platform Infrastructure to Advanced Business, Event ID: 1032321928. Katsottavissa/ladattavissa: https://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032321928&EventCategory=5&culture=en-US&CountryCode=US Luettu 23.4.2011

End-to-end Service Monitoring Whitepaper, Microsoft Corporation, 12/2007: Luettavissa : http://go.microsoft.com/fwlink/?LinkId=82945 Luettu 8.3.2011

Kempf, J. & Austein, R. March 2004. Internet Requests For Comments. 3724 - The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture. Luettavissa : http://www.faqs.org/rfcs/rfc3724.html Luettu 20.4.2011

Microsoft TechNet, Simple Network Management Protocol, 2011. Luettavissa : http://technet.microsoft.com/en-us/library/cc731328.aspx Luettu 29.04.2011

Liitteet

Liite 1. Keskeiset käsitteet ja määritelmät

Active Directory	Käyttäjätietokanta ja hakemistopalvelu, joka tarjoaa tavan nimetä, kuvata, hallita ja suojata verkon resursseja
ActiveX	Selaimen liitännäinen, lisäosa, joka mahdollistaa jonkin halutun verkkopohjaisen sovelluksen toiminnan
Distributed Application	Useammassa järjestelmän koneessa olevien ohjelmakomponenttien yhteistoiminnallinen sovellus
DMZ	Demilitarized Zone, yrityksen aliverkko, kutsutaan myös nimellä eteisverkko, joka sijoittuu sisäverkon ja internetin väliin suojattuna erillisenä verkkona
End-to-end käsite	Moniportaisen sovelluksen objektien päätepisteiden välisen tietoliikenteen kommunikointi (ja sen valvonta)
IT	Information technology, Informaatioteknologia, globaali termi tietotekniikalle
ISO/IEC 20000	IT-palvelunhallinnan virallinen standardi, käsittäen ITIL:n ja muita ITSM-kehyksiä (IT Service Management)
ITIL	IT Infrastructure Library, epävirallisesti standardoitu ”tietokirjasto” IT-palveluiden hallintaan
Klusteri	Useamman tietokoneen verkotettu malli, jossa muut koneet toimivat klooneina tarvittaessa, esimerkiksi vikatilanteissa

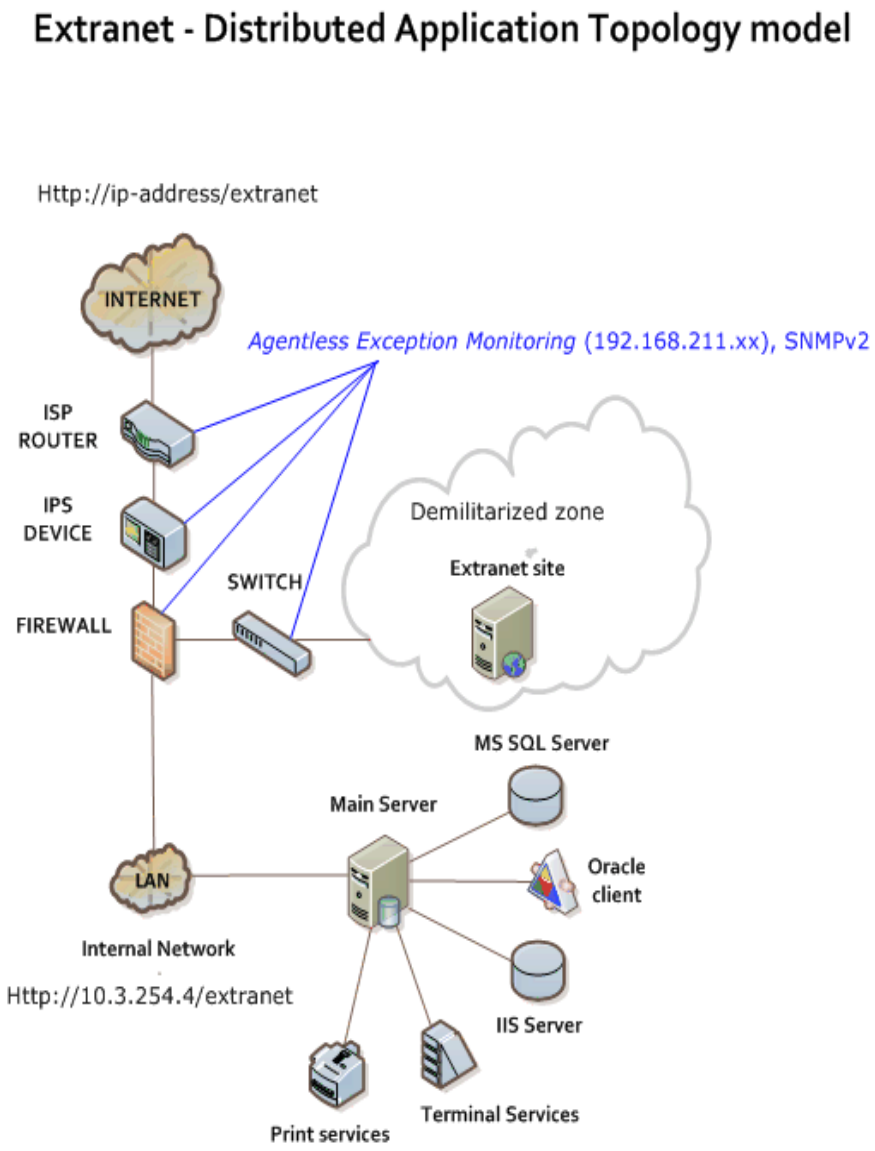
Konfigurointi	Palveluiden ja toimintojen asetusten määritys
Kytkin	Yhdistää lähiverkon tai muiden pakettikytkentäisten verkkojen osia toisiinsa
Management Pack (MP)	XML-dokumentti, joka sisältää rakenteen ja määrittelyt valvoa tiettyä laitetta tai palvelua
Microsoft Management Console (MMC)	Työkalu ja rajapinta ylläpidolle Windows-ympäristön hallintaan
MOF	Microsoft Operations Framework, laajennettu ITIL joka tarjoaa kokonaisvaltaisen näkemyksen ja konseptin palveluiden hallintaan. (Microsoftin kehittämä)
Monitorointi	Palveluiden ja toimintojen tilan valvonta
Operations Console	Erillinen sovellus hallintapalvelimella, jolla valvotaan ja hallitaan verkkoympäristöä ja sen komponentteja
OpsMgr / SCOM	Palvelinhallintaohjelmisto (kappale 3). Työssä käytetään yleisesti lyhennettä OpsMgr
OpsMgr agentti	Pieni sovellus, joka välittää tietoa monitoroitavalta laitteelta hallintapalvelimelle
OpsMgr client	Palvelin tai työasema, jota valvotaan agentin avulla
Palomuuri	Järjestelmä tai laite, joka suodattaa suojattavan verkon ja vaarallisemman verkon välisiä yhteyksiä muun verkko-hyökkäyksiä vastaan

Policy	Käytäntö, sääntö tai toimintaperiaate
Powershell	Windowsin komentotulkki, jonka avulla voidaan suorittaa ylläpidollisia toimenpiteitä tekstimuotoisilla käskyillä
Proseduuri	Sarja toimintoja tai tehtäviä, jotka samalla tavalla suoritettuina tuottavat aina saman lopputuloksen
Reititin	Tietoverkkoja yhdistävä laite. Välittää tietoa tietoverkon eri osien välillä
RSS-syöte	Uutissyöte, jonka avulla voi seurata usean eri sivuston päivityksiä yhdestä paikasta, tarvitsematta käydä jokaisessa paikassa erikseen
Scripti	Komentosarja. Voidaan kirjoittaa useita peräkkäisiä, loogisia kokonaisuuksia tehtävien automatisointiin
Scrum-viitekehys	Tarkoin vaiheistettu projektinhallintamenetelmä, tiivis ryhmätyömetodi, tavoitteet täydentyvät toteutuskierroksilla
Semanttisuus	Mahdollistaa asioiden painottamisen ja merkityksellisyyden, oikeiden asioiden parempi ja nopeampi tunnistaminen (XML-kieli ja dokumentit tuovat näitä mahdollisuuksia)
Web Console	Mahdollisuus valvoa/seurata verkon keskeisiä toimintoja selaimen kautta ilman erikseen asennettavaa ohjelmistoa
XML	eXtensible Markup Language; rakenteellinen kuvauskieli, joka auttaa jäsentämään laajoja tietomassoja selkeämmin

Liite 2. Etuja ja ominaisuuksia ITIL:n elinkaaren tasoilta

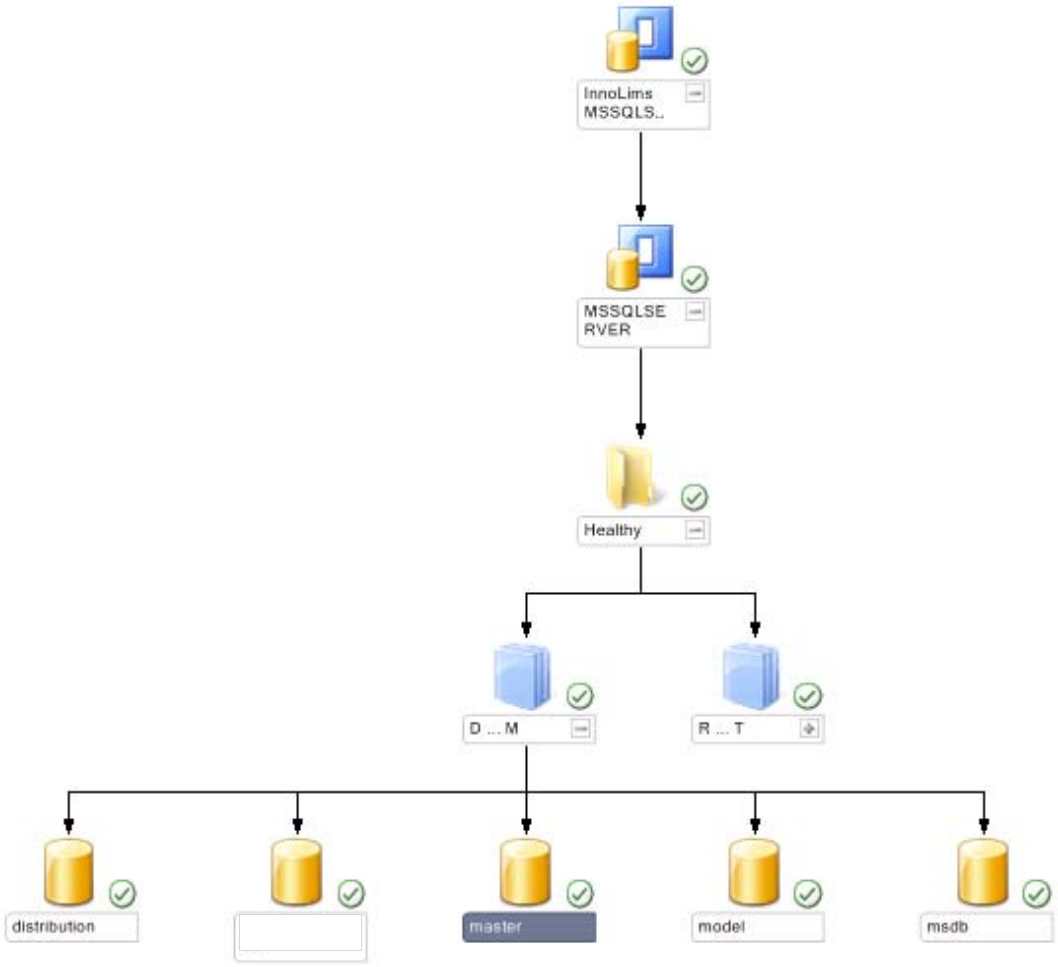
Kuten kappaleessa 2.1 todetaan, ITIL on joukko hyviksi havaittuja käytäntöjä palveluiden hallintaan. Liitteen kuviossa on mallinnettu sen periaate, jossa IT-osasto ensin rakentaa palvelustrategiansa. Sitä sovelletaan palveluiden mallinnuksessa, muutoksissa sekä toimintaperiaatteissa. Jokaisessa vaiheessa kerätään kokemuksia hyvistä ja huonoista puolista ja pyritään kehittämään niiden avulla jokaista palvelun vaihetta ja muokkaamaan sitä kautta myös strategiaa toimivammaksi.

Liite 3. Hajautetun sovelluksen (Case Extranet) visio-mallinnus



Kuvassa on mallinnettu hajautettu sovellus verkkokaaviona, josta näkyy siihen kuuluvat objektit sekä niiden sijoittuminen. (Internet ja LAN eivät varsinaisesti kuulu extranet-sovellukseen, mutta ne helpottavat hahmottamista). Main Server on pääpalvelin, joka hallinnoi päätoimintoja. Sinisellä viitatut objektit ovat verkkolaitteita, joita valvotaan Simple Network Management Protocol v2:lla. Laitteet tukevat kyseistä protokollaa. Niille voidaan myös määrittää sijaisagentit, esimerkiksi web-palvelimen agentti, joka hoitaa agentin tehtäviä ikään kuin etäyhteydellä.

Liite 4. Distributed Application Designer, Diagram View



Liitteessä esimerkki Operations Managerin suunnittelutyökalun Diagram-näkymästä. Sillä saadaan selkeä näkymä kaikista objekteista ja niihin liittyvistä palveluista puukaaviomaisena, hierarkisena rakenteena. Esimerkissä on avattu MS SQL Serverin rakennetta. Kaavioista nähdään myös, jos jonkin objektin kohdalla on ongelmia. Tällöin vihreän merkinnän tilalle tulee punainen ruksi ja asia kannattaa tarkastaa.