TAMPEREEN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

MOM-palvelun tuottaminen

Heikki Laukkanen

Tietojenkäsittelyn koulutusohjelma
Toukokuu 2007
Työn ohjaaja: Maritta Hoffrén

TAMPERE 2007

TAMPEREEN
AMMATTIKORKEAKOULU

Tekijä(t) Heikki Laukkanen

Koulutusohjelma(t) Tietojenkäsittely

Opinnäytetyön nimi MOM-palvelun tuottaminen

Työn valmistumis-kuukausi ja -vuosi toukokuu 2007

Työn ohjaaja Maritta Hoffrén **Sivumäärä:** 31

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli tutkia ITIL-viitekehyksen (IT Infrastructure Library) valossa järjestelmävalvonnan tehokasta toteutusta Microsoft Operations Manager 2005 (MOM) -ohjelmistolla monen palvelutoimittajan ympäristössä. Tutkintotyö tehtiin toimeksiantona MediWare Oy:lle, jossa toimin palveluasiantuntijana. Työssäni kehitän järjestelmävalvontaa suurissa organisaatioissa, joissa on useita eri palvelutoimittajia.

Yritysten sähköiset palvelut ovat yleistyneet kovaa vauhtia ja työntekijät ovat niistä entistäkin riippuvaisempia. Järjestelmien ylläpidon merkitys kasvaa yhä suuremmaksi, mitä enemmän ihmiset käyttävät tietokoneita paperin ja kynän sijaan. Useat yritykset ovat jo täysin tai ainakin osittain riippuvaisia sähköisten palveluiden saatavuudesta. Tästä syystä järjestelmien toiminnan valvonta on välttämätöntä ja se on pyrittävä automatisoimaan mahdollisimman kattavaksi.

Valvontapalvelun tuottaminen suurissa organisaatioissa on haastava tehtävä jo pelkästään useiden eri toimittajien vuoksi, jotka ylläpitävät eri järjestelmiä ja valvovat niitä kukin omalla tavallaan. Tästä syystä syntyy hyvin helposti eriäviä näkemyksiä asiakkaan ja toimittajan välillä palvelutason täyttymisestä.

Tutkintotyössä kerrotaan ensin ITIL-viitekehyksen taustaa, jonka jälkeen keskitytään selvittämään palvelukeskeisen järjestelmänvalvonnan toteuttamista edellä mainitun kaltaisessa monen toimittajan ympäristössä MOM 2005:n avulla. Työssä käydään läpi MOM-järjestelmän toiminta ja tutkitaan sen soveltuvuutta asiakasympäristöön.

Selvitys osoitti, että MOM 2005 soveltuu skaalautuvuutensa ansiosta hyvin monen toimittajan ympäristöihin ja sillä pystytään tuottamaan luotettavaa tietoa valvottavien järjestelmien tilasta.

Avainsanat MOM ITIL palvelunhallinta valvonta ylläpito

TAMPEREEN
AMMATTIKORKEAKOULU

Author(s) Heikki Laukkanen

Degree Programme(s) Business Information Systems

Title Production of MOM service

Month and year May 2007

Supervisor Maritta Hoffrén **Pages:** 31

ABSTRACT

The purpose of this final thesis was to research production of service management in multivendor environment with Microsoft Operations Manager 2005-software by reflecting ITIL (IT Infrastructure Library). This thesis has been commissioned to MediWare Oy where I work as a service specialist. In my job I develop systems monitoring for large organizations that have multiple service vendors.

Electric services have become rapidly common and workers are even more dependent on them. Importance of systems administration grows even greater, when people use computers instead of pencils. Many companies are already fully or at least partially dependent on availability of electric services. This is why monitoring of systems operation is necessary and must be automated as much as possible.

Production of monitoring services is challenging task in large organizations because of multiple vendors who administrates different systems and is monitoring them by their own means. This is why it creates easily differing views between the client and vendor how the service level agreement is being met.

Firstly in my thesis I tell about the background of ITIL, after that I concentrate on investigating implementation of service centered systems monitoring in the multi vendor environment mentioned before by using MOM 2005. In the thesis I go through MOM system and how it adapts to client environment.

As a conclusion I can say, that MOM 2005 fits well to multivendor environment for its scalability and it can be used to produce reliable information about the monitored systems state.

Keywords MOM ITIL service management monitoring maintenance

SISÄLLYSLUETTELO

Lyhenteet ja selitykset

Palvelutasosopimus (SLA) on palveluntarjoajan ja tilaajan välille tehtävä sopimus, jossa määritellään sopiva palvelutaso. Sopimuksen tuloksena tehdään muodollinen asiakirja, jossa määritellään mm. osapuolten velvollisuudet, laatuun ja suoritetasoon liittyvät tavoitteet, hinnat ja vaaditut resurssit.

TCP (Transmission Control Protocol), tietoliikenneprotokolla, jolla luodaan internet-tietokoneiden välille yhteyksiä. Protokolla pitää huolta, siitä, että tavujonot pilkotaan ip-paketeiksi ja että paketit saapuvat perille oikeassa järjestyksessä.

Tietämyskanta on tietokanta, jonne yrityksessä talletetaan kaikki hyödylliset ohjeet, joiden avulla jonkin tietyn asian suorittaminen on mahdollista. Tietämyskannan avulla pyritään vähentämään ns. hiljaisentiedon määrää yrityksessä.

UDP (User Datagram Protocol), TCP/IP-yhteyskäytäntö, jolla sovellus voi lähettää tietoja toiselle tietokoneelle. Eroaa TCP:stä siten, että paketin perillepääsyä ei vahvisteta ja siten saadaan suurempi nopeus.

1. Johdanto

Sähköiset palvelut ovat yleistyneet kovaa vauhtia ja ihmiset ovat niistä entistäkin riippuvaisempia. Järjestelmien ylläpidon merkitys kasvaa yhä suuremmaksi, mitä enemmän ihmiset käyttävät tietokoneita paperin ja kynän sijaan. Useat yritykset ovat joko täysin tai osittain riippuvaisia sähköisten palveluiden saatavuudesta, jolloin palveluiden käyttökatkot ja huono suorituskyky voivat tuottaa niille huomattavia tappioita. Terveydenhuoltoala ei ole poikkeus tässä suhteessa, päinvastoin sähköisten palveluiden saatavuuden merkitys on entistäkin kriittisempi käsitellessä potilastietoja ja hoidonohjauksen muuttuessa täysin sähköiseksi.

Suurin osa tietojärjestelmien käyttökatkoksista ja huonosta suorituskyvystä tunnistetaan liian myöhään. Tämä tarkoittaa yleensä sitä, että käyttäjä itse ilmoittaa asiakastukeen, ettei pääse palveluun käsiksi tai palvelu toimii hitaasti. Jotta tämän kaltaiset yrityksen tuottavuuteen suoraan tai epäsuorasti vaikuttavat vikatilanteet pystyttäisiin ennakoimaan, on tietojärjestelmiä valvottava aktiivisesti. Useimmiten yrityksissä järjestelmätuki ja ylläpito koetaan kuitenkin voittoa tuottamattomaksi toiminnoksi ja tämän vuoksi siihen ei haluta sijoittaa suuria summia rahaa, vaikka juuri ennakoivalla ylläpidolla yrityksissä voidaan tehdä huomattavia säästöjä.

Terveydenhuoltoalan yritykset ostavat sähköisiä palveluita useilta eri toimittajilta. Sen vuoksi käyttäjälle näkyvä palvelu saattaa olla riippuvainen hyvin monesta eri toimittajien tuottamasta palvelusta. Tällaiset ympäristöt asettavat omat haasteensa järjestelmänvalvonnalle. Opinnäytetyössäni pohdin, kuinka tämän tyyppisessä monen toimittajan ympäristössä voidaan tehokkaasti tuottaa ennakoivaa järjestelmänvalvontaa MOM 2005 (Microsoft Operations Manager)-ohjelmistolla.

Opinnäytetyö on tehty toimeksiantona MediWare Oy:lle, jossa toimin teknisenä palveluasiantuntijana. Työskentelen osana PASSI (ProActive Services for System Infrastucture)- ylläpitopalvelua, jossa tuotamme ennakoivaa ylläpitoa terveydenhuoltoalan organisaatioille.

Aluksi kerron palvelun tuottamisesta ITIL- viitekehyksen valossa ja kuinka MOM 2005 tukee ITIL- viitekehyksen antamia ohjeita. Lopuksi mietin millaisia eri rooleja palvelun tuottamisessa tarvitaan sekä miten MOM 2005 otetaan teoriassa käyttöön monen toimittajan ympäristössä.

2. ITIL- viitekehys

ITIL- viitekehys on joukko hyväksi havaittuja tapoja auttaa tuottamaan korkeatasoisia IT-palveluita. ITIL rajaa laajan kirjon erilaisia hallintakäytäntöjä, jotka ovat tarkoitettu tukemaan yrityksiä hyvän taloudellisen sekä laadullisen arvon tavoittelussa IT-palveluissa. Sen alkuperäinen kehittäjä on Iso-Britannian hallituksen ylläpitämä tietotekniikan ja telekommunikaation virasto CCTA (UK Government's Central Computer and Telecommunications Agency). ITIL- standardin kehitys alkoi jo 1980-luvulla CCTA:n toimesta, josta myöhemmin muodostui OGC (the UK Government's Office of Government Commerce). Sittemmin ITIL on levinnyt Euroopan kautta Yhdysvaltoihin ja vuosien kuluessa siitä on kehittynyt *de facto*- malli IT-palveluiden hallintaan.

Alun perin CCTA keräsi tietoa siitä, kuinka eri organisaatiot toteuttivat palvelunhallintaa. He analysoivat ja hyödynsivät sellaiset tavat, jotka soveltuivat parhaiten asiakkaidensa käyttöön, joihin kuului Ison-Britannian hallituksen eri yksiköitä. Pian muutkin havaitsivat, että ohjeet sopivat hyvin myös hallituksen ulkopuolisille organisaatioille.

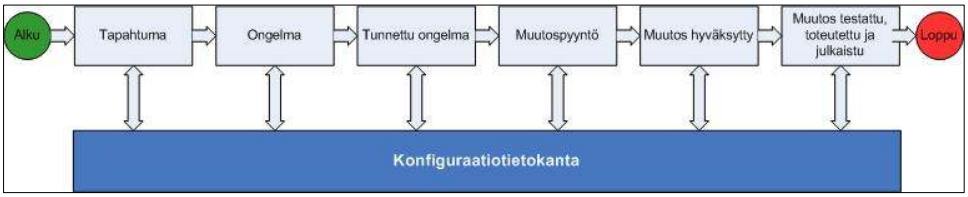
ITIL käsittelee palvelunhallintaa toimintaprosesseina. Nämä määrittelevät tavoitteet, toiminnot ja vaatimukset, jotka voidaan liittää kokonaisuudeksi IT-organisaatioissa. ITIL ei aseta tarkkoja sääntöjä, miten prosesseja pitää noudattaa vaan antaa suosituksia, joita voidaan hyödyntää tarpeiden mukaan eri organisaatioissa. Se tarjoaa erilaisen ajattelumallin toimia ja käsitellä palvelunhallintaa. Yritykset siis voivat käyttää ITIL- viitekehystä tukena kehittäessään omaa palvelunhallintaprosessia.

Aiemmin yritykset ovat ainoastaan keskittyneet tekniseen näkemykseen, mutta tänä päivänä korostetaan enemmän palvelun laatua liiketoiminnan näkökulmasta. IT-organisaatioiden pyrkiessä täyttää nämä odotukset, heidän on keskityttävä palvelunlaatuun ja enemmän asiakaslähtöiseen ajattelumalliin. Samalla kustannukset nousevat korkeiksi, mikä asettaa paineita kehittää enemmän liiketoimintalähtöistä ajattelumallia palvelunhallintaan. ITIL keskittyy korkealaatuisen palvelun tarjontaan asiakaslähtöisestä näkökulmasta. Tämä tarkoittaa sitä, että IT-organisaatioiden pitäisi tarjota asiakkaille juuri sitä palvelua, mistä he ovat asiakkaan kanssa sopineet (Best Practise For Service Support: 1-2.).

2.1. Palvelunhallinta (Service Management)

Kaikki ITIL:in määrittelemät prosessit liittyvät toisiinsa. Jotta paremmin voisi ymmärtää kuinka nämä liittyvät toisiinsa, alla olevassa luettelossa on selvitetty tapahtumanhallintaketjua eri prosessien kautta (Best Practise For Service Delivery: 7.):

1. Käyttäjä soittaa palvelupisteeseen ilmoittaakseen ongelmasta.
2. Tapahtumanhallintaprosessi käsittelee ilmoituksen ja kirjaa sen konfiguraatiotietokantaan.
3. Ongelmanhallintaprosessi tutkii syytä tapahtumaan ja ottaa yhteyttä kapasiteetinhallintaan saadakseen apua prosessiin. Palveluntasonhallinta hälyttää, että palvelutasosopimus on ylitetty. Muutospyyntö tehdään jos ongelman korjaus edellyttää muutosta järjestelmiin.
4. Muutoksenhallinta koordinoi muutospyynnön.
5. Taloudenhallintoprosessi auttaa käsittelemään mahdollisen päivityksen vaatimat kustannukset.
6. Palvelunjatkuvuudenhallinta ottaa osaa muutoksenhallintaprosessiin varmistaakseen, että järjestelmän palauttaminen nykyiseen tilaan on mahdollista.
7. Versionhallintaprosessi valvoo, että muutos tehdään oikein ja että konfiguraationhallinta saa päivitetyt tiedot muutoksesta.
8. Saatavuudenhallintaprosessi varmistaa tarvitseeko laitteistoa päivittää, jotta se vastaa annettuja saatavuuden ja luotettavuuden vaatimuksia.
9. Konfiguraationhallintaprosessi valvoo, että konfiguraatiotietokantaan päivitetään tarvittavat tiedot koko prosessin ajan. Kuvassa (Kuva1) näkyy kuinka konfiguraatiotietokanta toimii olennaisena osana koko tapahtumanhallintaketjua.



Kuva 1. Konfiguraatiotietokanta osana tapahtumanhallintaketjua.

2.2. Tapahtumanhallinta (Incident Management)

Tapahtumanhallinnan ensisijainen tehtävä on palauttaa järjestelmä normaaliin toimintatilaan. Tällä pyritään minimoimaan liiketoiminnalle aiheutuvia menetyksiä ja samalla on tarkoitus varmistaa, että paras palvelun laatu ja saatavuus säilytetään. Järjestelmän normaalin toiminnan raja-arvot määritellään palvelutasosopimuksessa. (Best Practise For Service Support: 71.)

ITIL määrittelee termin tapahtuma (Incident):

- mikä tahansa muutos, joka ei ole osa normaalia toimintaa
- mikä aiheuttaa tai voi aiheuttaa poikkeaman palvelussa tai sen laadussa.

Seuraavassa muutaman käytännön esimerkki tapahtumista (Best Practise For Service Support: 71):

- Ohjelma
  - Palvelu ei ole käytettävissä
  - Ohjelmavirhe, joka estää asiakasta työskentelemästä
  - Levynkäytön raja-arvo ylitetty

- Laitteisto
  - Järjestelmä alhaalla
  - Automaattinen hälytys
  - Tulostin ei toimi
  - Järjestelmän asetuksiin ei päästä käsiksi

- Palvelupyyntö
  - Asiakas pyytää tietoa/neuvoa/ohjeita
  - Salasana unohtunut

ITIL:n mukainen keskitetty palvelupiste (Service Desk) vastaa tapahtumien vastaanottamisesta sekä valvoo niiden koko ratkaisuprosessia. Käytännössä palvelupiste toimii ns. omistajana jokaiselle tapahtumalle. Jotta tapahtuman ratkaisu toimisi mahdollisimman tehokkaasti, on tapahtumanratkaisuprosessi suunniteltava ja toteutettava säännönmukaisesti. Käytännössä tapahtumanhallintaprosessi käynnistyy siitä, kun käyttäjä ilmoittaa ongelmasta palvelupisteeseen tai järjestelmänvalvonnassa huomataan poikkeama. Palvelupisteessä päivystäjä kirjaa tapahtuman tapahtumanhallintasovellukseen ja pyrkii ratkaisemaan tapahtuman mahdollisimman nopeasti, jotta palvelu saadaan palautettua normaaliin tilaan. Jos päivystäjä ei kykene ratkaisemaan varsinaista tapahtumaa, hän koettaa keksiä kiertotien, jonka avulla käyttäjä voi jatkaa työskentelyä tapahtumasta huolimatta. Päivystäjä voi myös siirtää tapahtuman asiantuntijaryhmälle, joka pyrkii ratkaisemaan tapahtuman varsi-

naisen aiheuttajan. Tärkeintä tässä prosessissa on tehokkuus, jotta käyttäjälle aiheutuisi mahdollisimman lyhyt keskeytys palvelun käytössä.

Hyvin hoidetun tapahtumanhallintaprosessin etuina organisaatiolle on palveluiden käyttökatkojen lyhentyminen. Ratkaisut tapahtumiin saadaan nopeasti ja asiakkaiden kokemukset palveluita kohtaan paranevat. Yritykset voivat tapahtumanhallinnan avulla seurata palveluntasosopimusten toteutumista ja kehittää tarpeen mukaan ratkaisuja havaittuihin heikkouksiin.

2.3. Kokoonpanonhallinta (Configuration Management)

Kokoonpanonhallinta tarjoaa yritykselle loogisen mallin sen infrastruktuurista ja palveluista tunnistamalla, kontrolloimalla, ylläpitämällä ja varmistamalla, että jokaisesta kokoonpanon osasta (esim. laitteet ja ohjelmistot) on ajan tasalla oleva tieto järjestelmässä. Kokoonpanonhallinta mallintaa myös palveluiden ja järjestelmän osien välisiä riippuvuuksia. Tämä on erittäin tärkeä tieto esimerkiksi kapasiteetinhallinnalle sekä saatavuudenhallinnalle. Kokoonpanonhallinnan tehtävät ovat (Best Practise For Service Support: 121.):

- Kirjata kaikki IT-järjestelmien ja -palveluiden rakenne ja konfiguraatiot organisaation sisällä.
- Tarjota ajan tasalla oleva tieto ja dokumentaatio muille palvelunhallintaprosesseille.
- Verrata dokumentaatiota infrastruktuuriin ja korjata kaikki eroavaisuudet.

2.4. Kapasiteetinhallinta (Capacity Management)

Kapasiteetinhallinta ei ole pelkästään suorituskyvynhallintaa, vaan se pyrkii varmistamaan myös, että organisaatio pystyy tuottamaan palveluita nykyisiin ja tuleviin kapasiteetin ja suorituskyvyn asettamiin vaatimuksiin kustannustehokkaasti. Esimerkiksi organisaatiot eivät voi yksiselitteisesti päättää vaihtaa kaikkia työasemia vain vastatakseen tulevaisuuden suorituskykyvaatimuksia, joita palvelut asettavat. Kapasiteetinhallinnan on ymmärrettävä liiketoiminnan vaatimukset, jotka asetetaan palvelun tuottamisella ja verrattava niiden tuottamiin kustannuksiin. (Best Practise For Service Delivery: 120.)

Suorituskyvynhallintaa tehdään useissa yrityksissä jälkiviisaina. Käytännössä tämä tarkoittaa, että suorituskykyongelmiin reagoidaan vasta ongelmien ilmettyä järjestelmässä. Tämä tarkoittaa sitä, että käyttäjät kokevat ongelmia palveluiden toiminnassa tai kokonaista palvelua ei voida käyttää.

Tietojärjestelmä on yhtä hyvä kuin sen heikoin lenkki. Suurissa organisaatioissa tämä tarkoittaa usein sitä, että palveluiden saatavuus riskeerataan jonkin hyvin yksinkertaisen mutta järjestelmän kannalta kriittisen komponentin

alimitoittamisella. Tätä tehdään yleensä vain, jotta saavutettaisiin kustannussäästöjä. Harvat yrityksen tietohallinnosta vastaavat päälliköt ovat niin tietoisia tulevaisuuden vaatimuksista, että he osaisivat tehdä realistisia ennusteita järjestelmän käyttöasteesta ja siitä millaista laite- yms. kapasiteettia palvelun tuottamiseen tullaan tarvitsemaan tulevaisuudessa.

Järjestelmänhallintaohjelmat sisältävät usein mahdollisuuden asettaa erilaisia hälytyksiä tiettyjen suorituskyvyn raja-arvojen ylittyessä. Suorituskyvystä voidaan myös tällaisten työkalujen avulla kerätä tilastoa, mikä helpottaa usein arvioimaan tulevaisuuden vaatimuksia, mitä eri palvelut asettavat järjestelmälle ja sen eri komponenteille (Kuva2). Lisäksi tällaisen tilaston avulla voidaan myös määrittää milloin järjestelmässä on turvallisinta suorittaa huoltotoimia (esimerkiksi varmistukset).

Kuva 2. Prosessorin kuormakuvaaja.

2.5. Palvelutasonhallinta (Service Level Management)

Palveluntasonhallinta on nimitys prosessille, jossa suunnitellaan, koordinoidaan, sovitaan, valvotaan ja raportoidaan palvelutasosopimusten mukaisesti saavutetuista tavoitteista, jotta vaadittu palvelutaso voidaan saavuttaa järkevin kustannuksin tinkimättä palvelun laadusta. Oikeaoppisella palveluntasonhallinnalla voidaan saavuttaa selvä parannus nykyisten palveluiden laatuun ja palvelukatkojen määrän väheneminen. Tehokas palveluntasonhallinta johtaa huomattaviin säästöihin kun järjestelmän ylläpitäjiltä kuluu vähemmän aikaa yhä harvemmin ilmenevien ongelmien selvittämiseen. (Best Practise For Service Delivery: 27.)

Palvelutasonhallinnan tarkoituksena on ylläpitää ja parantaa IT-palveluiden laatua jatkuvan sopimisen, valvonnan ja raportoinnin kautta. Käytännössä tämä tarkoittaa hyvien palvelumallien kehittämistä ja huonojen pois kitkemistä. Näin voidaan saavuttaa parempi IT-palveluiden toimintavarmuus.

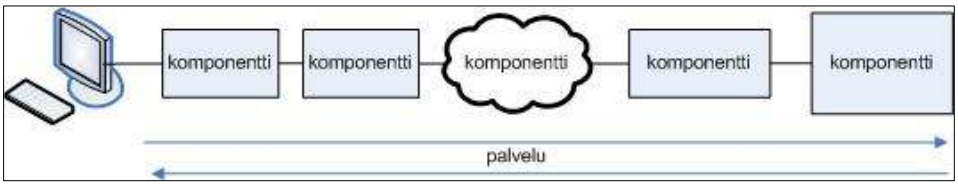
Palvelutasonhallinta on oleellinen jokaisessa organisaatiossa, jotta voidaan määrittää organisaation toimintojen tukemiseen tarvittavien IT-palveluiden kapasiteetti. Ilman palvelutasohallintaa ei voida valvoa, täyttyvätkö organisaation liiketoiminnan asettamien palvelutasojen vaatimukset (ja jos eivät täyty, niin mikä on syy tähän). Palvelutasosopimuksia hallitaan palveluntasohallinnan kautta. Palvelutasosopimukset määrittävät tarkat raja-arvot, joita vastaan organisaation palveluiden saatavuutta verrataan.

2.6. Saatavuudenhallinta (Availability Management)

Yrityksen liiketoiminnan riippuvuus palveluiden saatavuudesta on yhä ilmeisempi. Käytännössä kehitys on saavuttanut sen pisteen, missä palvelukatkos tarkoittaa koko yrityksen toimintojen pysähtymistä. Tämän päivän trendi on tarjota yrityksen asiakkaille palveluita vuorokauden ympäri sähköisessä muodossa. Tämä nostaa palveluiden saatavuudenhallinnan merkitystä yrityksissä, koska asiakkaat muodostavat mielikuvansa yrityksestä yhä enemmän palveluiden laadun perusteella. Tämä saattaa tarkoittaa sitä, että lyhyt käyttökatko saa asiakkaan harkitsemaan toisen yrityksen palveluja. (Best Practise For Service Delivery: 211.)

Saatavuudenhallinnan lähtökohta on, ettei palvelun toiminta ole kiinni vain yhden järjestelmän komponentin toimivuudesta, vaan pikemmin jokaisen järjestelmän komponentin summa. Palvelua on osattava ajatella käyttäjän näkökulmasta, joten jokainen järjestelmän osa voi olla elintärkeä liiketoiminnan eri palvelujen kannalta. Saatavuudenhallintaprosessissa pyritään varmistamaan tämän palveluketjun toimivuus.

Käyttäjän näkemä palvelu saattaa parhaassa tapauksessa hyödyntää useita eri järjestelmän komponentteja. Jos kuvan (Kuva3) esittämistä komponenteista ei toimi, palvelua ei voida toimittaa.



Kuva 3: Palvelunsaatavuuden riippuminen järjestelmän eri komponenteista (Best Practise For Service Delivery: 216.)

2.7. Turvallisuudenhallinta (Security Management)

Saatavuudenhallinta on hyvin läheisessä suhteessa turvallisuudenhallinnan kanssa. Saatavuudenhallinta saa turvallisuudenhallinnalta ohjeita ja asetuksia miten eri palveluita ja tietoja voidaan käyttää. Turvallisuudenhallinnalla pyritään valvomaan järjestelmän käyttöoikeuksia. Tärkeimmät seikat joihin organisaation turvallisuutta suunnitellessa pitää muistaa, ovat (Best Practise For Service Delivery: 243.):

- Tuotteet ja palvelut ovat ainoastaan erikseen sallittujen käyttäjien saatavilla.
- Tuotteiden ja palveluiden on oltava palautettavissa virhetilanteista siten, että niiden turvallisuus ja salassapito ei kärsi.
- Laitteiden ja järjestelmien fyysinen käyttö täytyy olla estetty muilta kuin erikseen sallituilta käyttäjiltä.
- Ohjelmien looginen käyttö täytyy olla estetty muilta kuin erikseen sallituilta käyttäjiltä.
- Järjestelmänhallintaoikeudet saa olla vain valituilla henkilöillä ja ryhmillä.
- Tiedon täytyy olla saatavilla palvelutasosopimuksessa sovittuina aikoina erikseen sallituille käyttäjille.

Terveydenhuoltoalan yrityksissä palveluiden käyttöoikeudet ovat hyvin merkittävässä asemassa, koska tietosuojalaki asettaa kovat vaatimukset potilastietojärjestelmien tietosuojalle. Ylläpidon tehtävänä on varmistaa, etteivät käyttäjät pääse käsiksi arkaluontoisiin potilastietoihin ilman heille erikseen myönnettävää käyttöoikeutta. Lisäksi joka kerta kun käyttäjä tutkii potilaan tietoja, täytyy järjestelmän tallentaa tapahtumasta tieto, jotta voidaan jälkeenpäin nähdä ketkä kaikki käyttäjät ovat potilaan tietoja lukeneet tai muuttaneet.

Järjestelmänylläpitäjän pitää myös valvoa, ettei kukaan vahingossa tai tarkoituksella lisää jollekulle käyttäjälle liikaa oikeuksia. Järjestelmän valvontaohjelmistoissa voidaan asettaa esimerkiksi hälytys siitä, kun joku käyttäjä lisätään järjestelmänvalvojaryhmään. Tällä tavalla voidaan valvoa, ettei kukaan pääse lisäämään huomaamatta erittäin korkeita käyttöoikeuksia esimerkiksi tietomurtoaikeissa.

3. Microsoft Operations Manager 2005

3.1. Yleistä

Microsoft Operations Manager 2005 (MOM) on suunniteltu apuvälineeksi organisaatioiden elintärkeiden järjestelmien ylläpitoa ja valvontaa varten. Tuote sisältää nimestään huolimatta mahdollisuuden liittää muidenkin laite- ja ohjelmistovalmistajien tuotteita valvontaan. MOM 2005 mahdollistaa järjestelmäylläpitäjien suorittaa keskitettyä valvontaa hajautetuista järjestelmistä. Esimerkiksi suurissa organisaatioissa, joissa useat konttorit saattavat sijaita eri mantereilla, keskitetyn valvontakonsolin avulla voidaan pitää huolta yritystoiminnan kannalta elintärkeiden palveluiden saatavuudesta.

MOM-konsolissa voidaan valita valvontatasoja sen mukaan millä tarkkuudella eri hälytyksiä halutaan kerätä valvottavista järjestelmistä. Esimerkiksi suurissa organisaatioissa tietojärjestelmistä voidaan saada satoja tuhansia tapahtumia päivässä ja tästä syystä MOM-konsoliin on syytä asettaa rajoituksia tiedon keruulle. Näin vältetään tietoliikenneyhteyksien ruuhkautuminen tapahtumatietojen paljouden vuoksi.

Järjestelmäylläpitäjä voi asettaa MOM-konsoliin erilaisia hälytysrajoja, joiden avulla voidaan valvoa esimerkiksi palveluiden saatavuutta tai järjestelmän suorituskykyä. Jokaisesta järjestelmän aiheuttamasta hälytyksestä jää tapahtumahistoriaan tieto. Tietojen avulla ylläpitäjän on helpompi selvittää, mikä aiheutti hälytyksen ja korjata mahdollinen ongelma.

MOM 2005:n avulla voidaan asettaa myös automaattisia toimintoja tiettyjen ehtojen täyttyessä. Nämä voivat olla hälytysluonteisia tai suorittaa korjaavia toimenpiteitä. Esimerkiksi levytilan uhatessa loppua kesken järjestelmä voidaan määrittää automaattisesti poistamaan väliaikaistiedostoja levyltä.

MOM 2005 sisältää myös laajan tietämyskannan Microsoftin tuotteista. Tietämyskanta nopeuttaa järjestelmäylläpitäjän työtä hänen selvittäessään uutta ongelmatilannetta. MOM-konsolista tapahtuman tietojen kautta ylläpitäjä voi suoraan siirtyä tietämyskantaan ja yrittää löytää jo olemassa olevaan ratkaisun ongelmaan. Lisäksi ylläpitäjät voivat itse lisätä tietämyskantaan ongelman ratkaisussa helpottavia tietoja tulevaisuuden varalle.

MOM mahdollistaa myös palvelutasosopimusten valvomisen automaattisesti. Uuden hälytyksen syntyessä tapahtumalle kirjataan alkamishetken aikaleima. Jos järjestelmänylläpitäjä ei kuittaa hälytystä eri tilaan riittävän ajoissa, MOM kirjaa tapahtumasta palvelutasosopimuksen seurantaan poikkeaman. Järjestelmä voidaan myös asettaa suorittamaan uusi hälytys, jos palvelutasosopimuksen asettamat aikarajat uhkaavat umpeutua.

Hallintapaketit, joiden avulla MOM 2005 kerää järjestelmistä ja palveluista tietoa sisältävät paljon valmiiksi asetettuja sääntöjä, jotka helpottavat valvonnan käyttöönottoa. Säännöt voidaan jakaa kolmeen ryhmään: tapahtumat, hälytykset ja suorituskykytieto. Lisäksi MOM 2005 sisältää valmiita raportteja, joita voidaan tehdä järjestelmästä kerätyistä tiedoista. Nämä raportit voidaan jakaa kuuteen eri ryhmään:

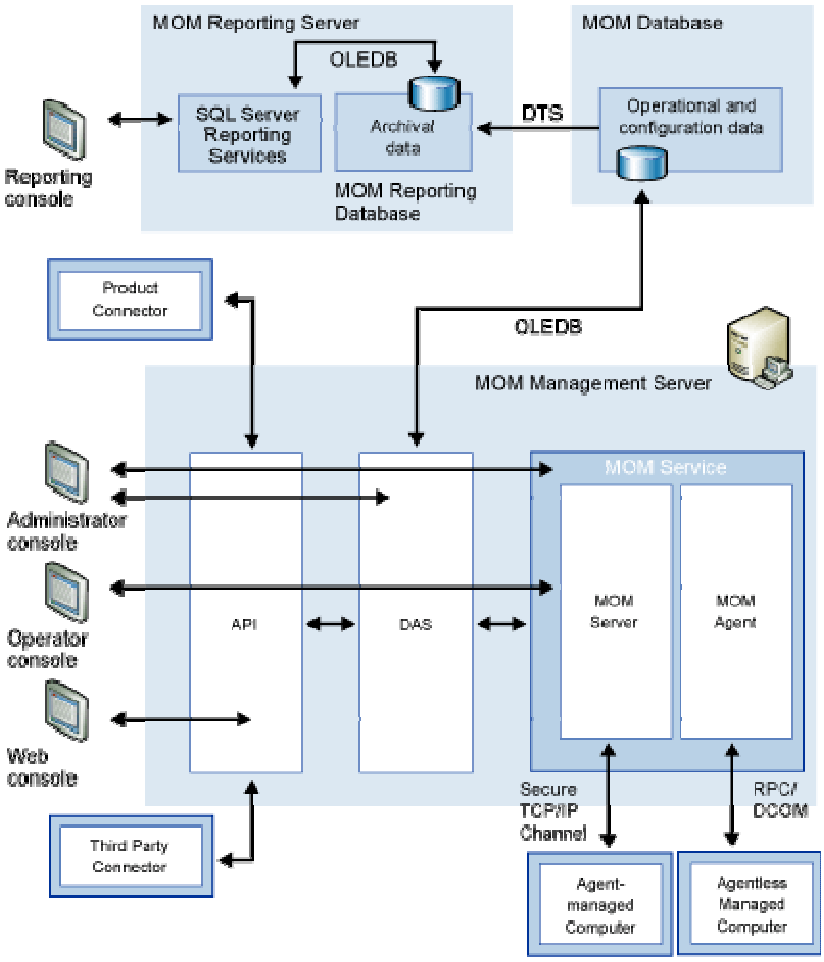
- operaatiot
- kapasiteetti ja käyttö
- luotettavuus ja saatavuus
- konfiguraatio ja inventaario
- turvallisuus

3.2. MOM 2005 rakenne

Microsoft Operations Manager 2005 koostuu vähintään yhdestä hallintaryhmästä, johon liitetään ylläpidettävät laitteet ja niiden tarjoamat palvelut. Hallintaryhmään kuuluvia laitteita voidaan lisäksi jakaa omiin ryhmiin esimerkiksi niiden tarjoamien palveluiden tai käyttäjien perusteella.

Hallintaryhmässä pitää olla yksi hallintapalvelin, jossa käytännössä itse MOM-palvelua ajetaan ja hallitaan. MOM-hallintapalvelimella tarvitaan lisäksi ns. operatiivinen tietokanta, joka pitää sisällään valvottavilta koneilta kerätyn tiedon, niiden valvontaan tarvittavat asetustiedot sekä koko MOM 2005:n käyttöön vaadittavat asetukset. Tämän hallintapalvelimen kautta järjestelmän ylläpitäjät pääsevät käsiksi hallinta- sekä valvontakonsoleihin. Hallintapalvelin on MOM-palvelun kannalta keskeisessä asemassa, sillä kaikki valvottavat koneet ja palvelut lähettävät tietoa suoraan tälle palvelimelle.

MOM-palvelun tuottamiseen vaaditaan myös operatiivisen tietokannan lisäksi raportointitietokanta. Tähän raportointitietokantaan siirretään aika ajoin valvottavilta laitteilta ja koneilta kerättyä tietoa. Raportointitietokannan ja raportointikomponentin avulla MOM palvelusta voidaan tuottaa erilaisia tilastoja ja raportteja pitkältä aikaväliltä. Raporttikomponenttia käytetään raportointikonsolin kautta. Kuvassa (Kuva4) näkyy MOM 2005-järjestelmän eri komponenttien väliset suhteet.



Kuva 4: Microsoft Operations Manager 2005 rakenne. (Microsoft)

3.3. Hallintaryhmä (Management Group)

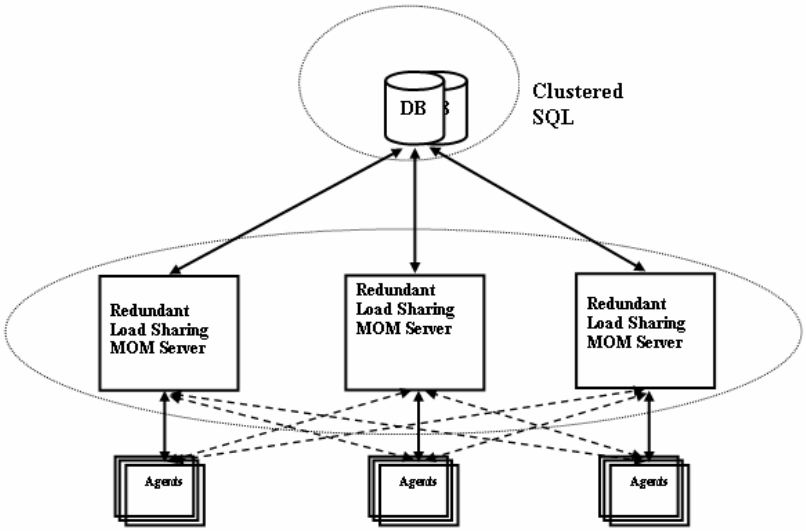
Jotta monimutkaista tietojärjestelmää voitaisiin hallita tehokkaasti, on se jaettava osiin. MOM 2005 käyttää omassa arkkitehtuurissaan ns. hallintaryhmiä, joihin valvottavat tietokoneet voidaan jakaa. Valvottavat koneet voidaan käytännössä jakaa hallintaryhmiin niiden maantieteellisen sijainnin tai eri osastojen perusteella. Muutama pääsääntö kuitenkin pätee jokaiseen hallintaryhmään:

- Hallintaryhmään kuuluu yksi tai useampi hallintapalvelin
- Hallintaryhmään on liitettävä valvottavat koneet
- Hallintaryhmään kuuluu MOM-tietokanta
- Jokaisella hallintaryhmällä on hallinta- ja valvontakonsoli

Lisäksi hallintaryhmään voi kuulua seuraavia asioita:

- MOM:n web-konsoli
- MOM-raportointipalvelin ja MOM-raportointikonsoli

Suurissa organisaatioissa hallittavia laitteita saattaa olla tuhansia yhtä hallintaryhmää kohden, jolloin hallintapalvelimelle kohdistuva kuorma saattaa nousta liian suureksi. Tätä varten MOM-hallintaryhmät sallivat asentaa useamman hallintapalvelimen ryhmää kohden. Etäagentit (valvottaville palvelimille asennettavat ohjelmistot) ottavat yhteyttä aina ensisijaiseen palvelimeen, mutta osaavat vaihtaa hallintapalvelinta jos eivät saa vastausta riittävän nopeasti. Hallintaryhmän kaikki hallintapalvelimet ottavat yhteyttä samaan MOM-tietokantapalvelimeen. Kuvan (Kuva5) tapauksessa MOM-tietokantapalvelin on klusteroitu palvelun saatavuuden varmistamiseksi.



Kuva 5. MOM 2005 kuorman jakaminen usealle hallintapalvelimelle. (Microsoft Operations Manager)

Jokaisen MOM-asennuksen yhteydessä asennusohjelma luo oletuksena yhden hallintaryhmän. Hallintaryhmän asetuksia voi myöhemmin muuttaa hallintakonsolin avulla. Tärkeätä on kuitenkin muistaa, että asennuksen aikana asetettua hallintaryhmän nimeä ei voida vaihtaa myöhemmin.

3.4. Hallinta-agentit (Management Agents)

MOM-hallintapalvelin käyttää pääasiassa etäagentteja laitteistojen valvontaan. Tietokoneita, joita valvotaan näiden etäagenttien avulla, kutsutaan agenteilla hallituiksi koneiksi. MOM 2005-arkkitehtuuri mahdollistaa myös koneiden valvomisen ilman varsinaisia etäagentteja. Tällöin hallintapalvelin valvoo suoraan laitetta WMI (Windows Management Interface)-rajapinnan avulla.

Etäagentti suorittaa seuraavia toimintoja:

- Kerää tietoa hallittavasta tietokoneesta.
- Valvoo tiettyjä palveluita ja ohjelmistoja erinäisten loki-tiedostojen ja suorituskykymittareiden avulla.
- Prosessoi hallintatietoja ja toimii annettujen ohjeiden pohjalta. Esimerkiksi etäagentit eivät lähetä kaikkea kerättyä tietoa hallintapalvelimelle saman tien vaan siirtävät sitä osissa tietyin aikavälein.

Etäagentti lähettää määräajoin ns. sykeviestin, joka kertoo hallintapalvelimelle, että agentti on kunnossa ja siihen saadaan yhteys tietoverkon ylitse. Etäagentti on mahdollista myös asettaa vaihtamaan hallintapalvelinta, johon se on ensisijaisesti yhteydessä (jos esimerkiksi yhteyttä ensisijaiseen hallintapalvelimeen tietoverkkokatkoksen takia ei voida muodostaa, lähettää etäagentti tietonsa toiselle hallintapalvelimelle). Tämän mahdollistamiseksi MOM-ympäristössä pitää olla vähintään kaksi hallintapalvelinta.

Etäagentti voi toimia myös tiedonvälittäjänä toiselle agentille eli ns. proxy:na: jos toinen etäagentti ei saa suoraan lähetettyä tietoa hallintapalvelimelle, voi tämä yrittää kommunikoida käyttämällä toista etäagenttia hyväksi. (Managing Your Infrastructure Using Microsoft Operations Manager 2005: 3-5.)

Hallintapalvelin ja etäagentit käyttävät tiedonvälitykseen TCP/IP-protokollaa. Oletuksena kommunikointiin käytetään TCP-porttia 1270. Jos agentilla hallittu tietokone on palomuurin takana, täytyy tällöin avata palomuurista kyseinen portti, jotta agentti pystyy lähettämään tietoa hallintapalvelimelle. Etäagentti käyttää ns. sykeviestin välittämiseen UDP-protokollaa ja porttia 1270. Paikalliset agentit käyttävät tiedonvälitykseen TCP-porttia 135 ja DCOM-portteja. Käytännössä paikallinen agentti ei voi toimia, jos hallittavan koneen ja hallintapalvelimen välissä on palomuuri.

Microsoft Operations Manager 2005 tarjoaa myös mahdollisuuden asettaa etäagenttien ja hallintapalvelinten välille todennuksen. Tällöin etäagentti todentaa itsensä hallintapalvelimelle käyttäen Kerberos 5-protokollaa ennen asetus- ja hallintotietojen siirtoa. Tällöin vältytään riskiltä että järjestelmään

kuulumaton agentti voisi syöttää virheellistä tietoa hallintapalvelimelle aiheuttaen siten käyttökatkoja tai vääriä hälytyksiä.

3.5. Hallintapaketit (Management Packs)

MOM 2005:n hallintapaketit sisältävät ennalta määritettyjä asetuksia ohjelmistojen valvontaan (esimerkiksi Exchange-hallintapaketin avulla on mahdollista valvoa Exchange-sähköpostipalvelun toimintaa). Nämä asetukset sisältävät mm. sääntöryhmät palveluun liittyviin toimintoihin. Lisäksi jokainen hallintapaketti sisältää sääntöihin liittyvän tietämyskannan, joka määrittää kuinka tietyt ongelmat ohjelman tai palvelun suhteen pitäisi selvittää. Hallintapaketit pitävät myös sisällään valmiit raportit, joita kunkin paketin avulla voidaan luoda valvottavasta ohjelmasta tai palvelusta. Hallintapaketit ovat hallintaryhmäkohtaisia.

Microsoft tuottaa kaikkiin omiin tuotteisiinsa valmiita hallintapaketteja. Suurin osa näistä toimitetaan MOM 2005:n asennusmedian mukana. Uusimmat versiot hallintapaketeista löytyvät Microsoftin omilta verkkosivuilta. MOM 2005:een löytyy myös muiden valmistajien tekemiä hallintapaketteja, joiden avulla nämä haluavat tukeva omia tuotteidensa valvontaa (esimerkiksi HP:lla on hallintapaketit heidän Proliant-palvelimiensa laitetason valvontaan).

Käyttäjät voivat myös rakentaa omia hallintapaketteja tallentamalla tehdyt muutokset omaan pakettiinsa. Tällä tavalla sääntöryhmät ja asetukset voidaan kopioida toiseen hallintaryhmään ja varmistaa.

3.6. MOM-tietokanta

MOM-tietokanta on keskitetty säilytyspaikka tapahtumille, hälytyksille, suorituskykytiedolle ja säännöille. MOM tallentaa kaiken tiedon ja asetukset Microsoftin SQL Server 2000 (Onepoint)-tietokantaan. Tietokannan koko kasvaa sitä mukaa, kun järjestelmä kerää tietoa hallittavilta laitteilta.

Oletuksena MOM-tietokannasta siirretään neljän päivän aikajaksoissa vanhat valvontatiedot raportointitietokantaan. MOM-hallintajärjestelmä ei kuitenkaan oletuksena valvo, että tiedot saadaan välitettyä raportointitietokantaan säännöllisesti. Tästä syystä ongelmatilanteissa saattaa käydä niin, että MOM-tietokanta, jonka koko maksimissaan on vain 30G, tulee täyteen. Tämän vuoksi järjestelmän ylläpitäjä voi asettaa hälytyksen tietokantaan, jos valvontatietoja ei saada siirrettyä raportointitietokantaan. Ylläpitäjän on syytä myös varmistaa säännöllisesti, ettei MOM-tietokanta pääse kasvamaan liian suureksi. MOM-tietokannan sulava toiminta on koko hallintajärjestelmän toiminnan kannalta elintärkeää.

MOM-tietokantaan tallennetaan kriittistä tietoa, jonka pitää olla saatavilla jatkuvasti. Jos tietokantapalvelin hajoaa tai on muuten tavoittamattomissa, tämä saattaa aiheuttaa liiketoiminnalle suuria menetyksiä. Tällaisten tilanteiden ehkäisemiseksi MOM-tietokanta kannattaa varmistaa monistamalla palvelua useammalle palvelimelle (klusteroimalla). Lisäksi MOM-tietokannasta on otettava säännöllisiä varmuuskopioita. Käytännössä tämä tarkoittaa sitä, että tietokantaa kopioidaan aktiivisesti (replikoidaan) varalla olevalle tietokantapalvelimelle. Tällöin ensimmäisen MOM-tietokantapalvelimen rikkoutuessa toinen tietokantapalvelin ottaa ensimmäisen roolin ja palvelun toiminta pystytään säilyttämään lähes tai täysin katkottomana.

Tietokantapalvelimien klusterointi helpottaa myös huoltotoimia. Jos esimerkiksi ensimmäiselle tietokantapalvelimelle pitää tehdä korjauksia, voidaan palvelut siirtää toiselle palvelimelle. Ilman tätä toista tietokantapalvelinta suuremmat huoltotoimenpiteet aiheuttaisivat käyttökatkon koko hallintajärjestelmälle.

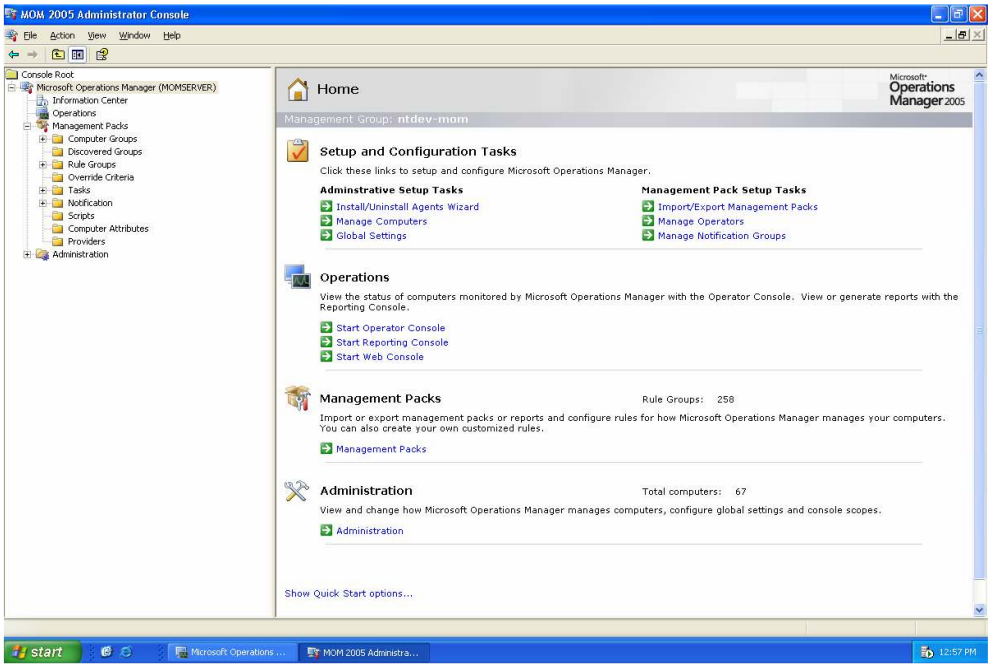
3.7. MOM-raportointitietokanta

MOM-raportointitietokannan tehtävänä on säilyttää valvontatietoja pitkältä aikaväliltä. Koska MOM-tietokanta on suunniteltu vain lyhytaikaiseen tiedonsäilytyseen, täytyy tiedot siirtää ennen pitkää raportointitietokantaan (oletuksena MOM-tietokanta säilyttää tiedot vain neljän päivän ajan). Lisäksi MOM-tietokannan pieni fyysinen koko (30G) tulee hyvin nopeasti täyteen suurissa organisaatioissa.

MOM-raportointitietokanta säilyttää tapahtuma-, hälytys- ja suorituskykytietoja yli vuoden ajan, joten sieltä voidaan ajaa raportteja tarvittaessa erimittaisilta aikajaksoilta. Vaikka Microsoft ei itse suosittele raportointitietokannan varmistamista, olisi tämä syytä tehdä säännöllisesti. Raportointikannan avulla organisaatio voi nähdä järjestelmän käyttöasteen sekä mahdolliset ongelmakohdat pitkältä aikaväliltä. Ilman raportointikannan sisältämää tietoa kapasiteetinhallintaa on siis lähes mahdotonta tehdä.

3.8. MOM-hallintakonsoli

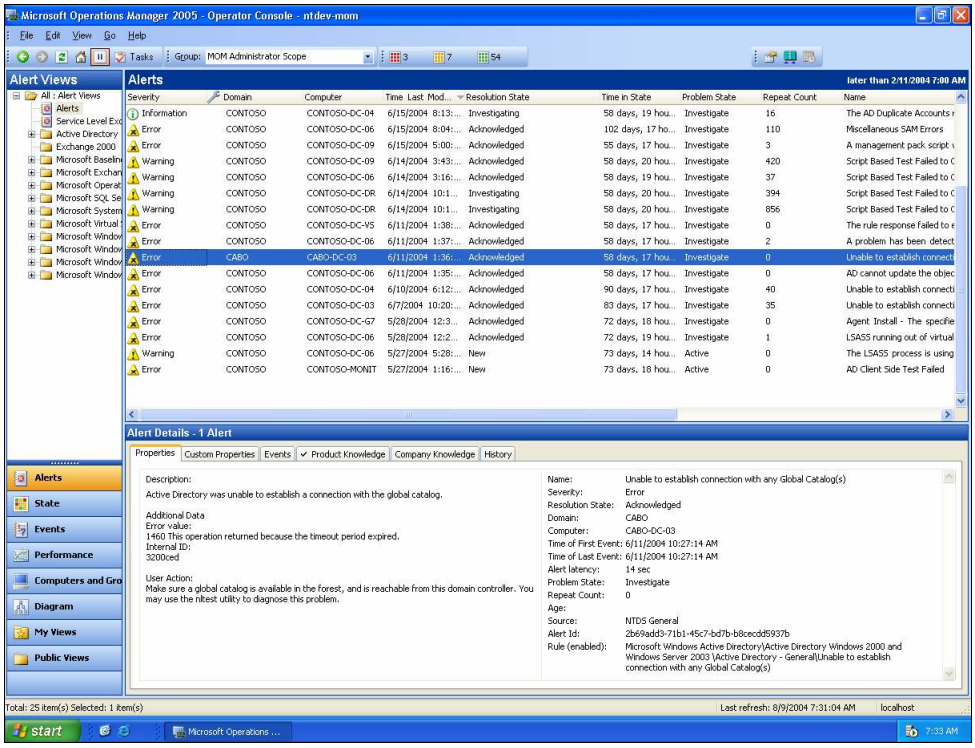
MOM-hallintakonsoli käyttää Microsoft Management Console (MMC)-tekniikkaa. Konsolin avulla ylläpitäjä voi muuttaa MOM-komponenttien asetuksia koko hallintaryhmässä. MOM-etäagenttien asentaminen ja poistaminen hallittavilta laitteilta tapahtuu myös tämän konsolin avulla. MOM-hallintakonsoli helpottaa myös valvottavien laitteiden ylläpitoa ja siltä voidaan suorittaa huoltotoimenpiteitä hallintaan kuuluville koneille. Hallintakonsolin perusnäkymä kuvassa (Kuva6).



Kuva 6. MOM 2005-hallintakonsoli

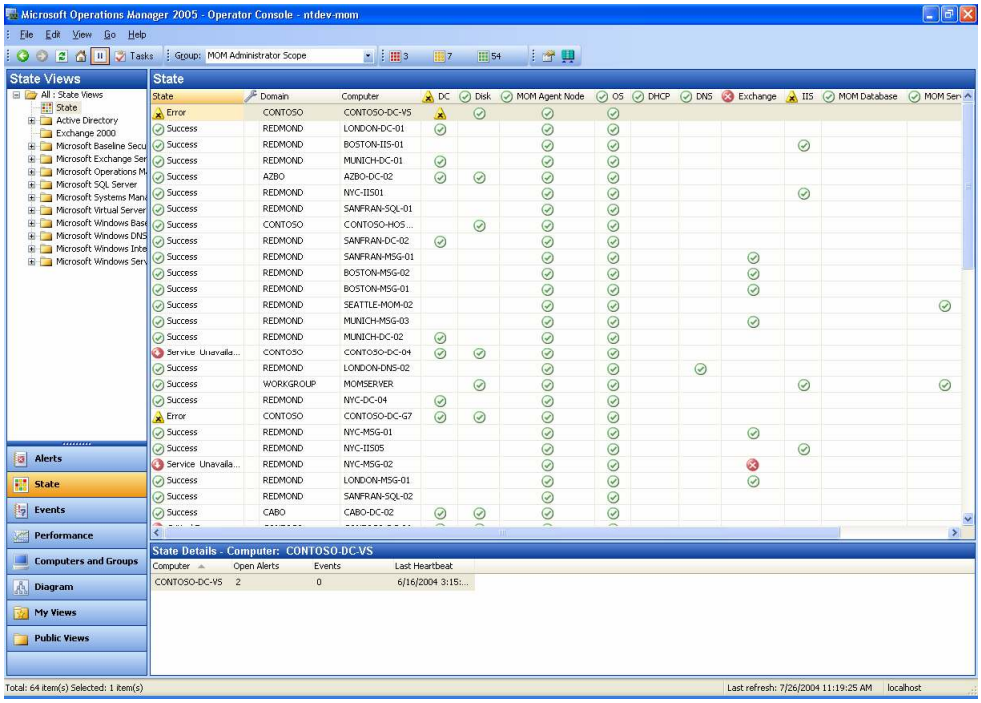
3.9. MOM-valvontakonsoli

MOM-valvontakonsolin avulla järjestelmän ylläpitäjät ja valvojat voivat helposti silmäillä järjestelmästä saatuja hälytyksiä ja tapahtumia. Suurin ongelma isoissa organisaatioissa on valtavan tietomäärän hallinta. Valvontakonsolin näkymä ei saa sisältää yhdellä kertaa liikaa tietoa, muuten olennaisen tiedon havaitseminen on liian vaikeaa. Tästä syystä MOM:n valvontakonsolissa koneet ovat jaettu valmiiksi valvottavien tuotteiden tai palveluiden mukaisesti valmiiksi omiin ryhmiinsä. Ylläpitäjät voivat myös luoda henkilökohtaisia näkymiä valvontakonsoliin, kuten alla olevassa kuvassa (Kuva7).



Kuva 7. MOM 2005-valvontakonsoli.

Valvontakonsolin ehkä käyttökelpoisimpia näkymiä on ns. tilanäkymä. Tässä näkymässä kaikkien valvottavien laitteiden tarjoamat palvelut näkyvät yhdellä silmäyksellä. Vaakarivillä näkyy aina yksi laite ja pystyrivillä kyseisen laitteen tarjoamat palvelut ja sen tämänhetkinen tila. Rivin viimeisessä solussa näkyy tärkeysjärjestyksessä vakavin hälytys. Jos yhtään hälytystä ei ole auki tällä laitteella, niin solussa on vihreä ikoni, kuten kuvassa (Kuva8).

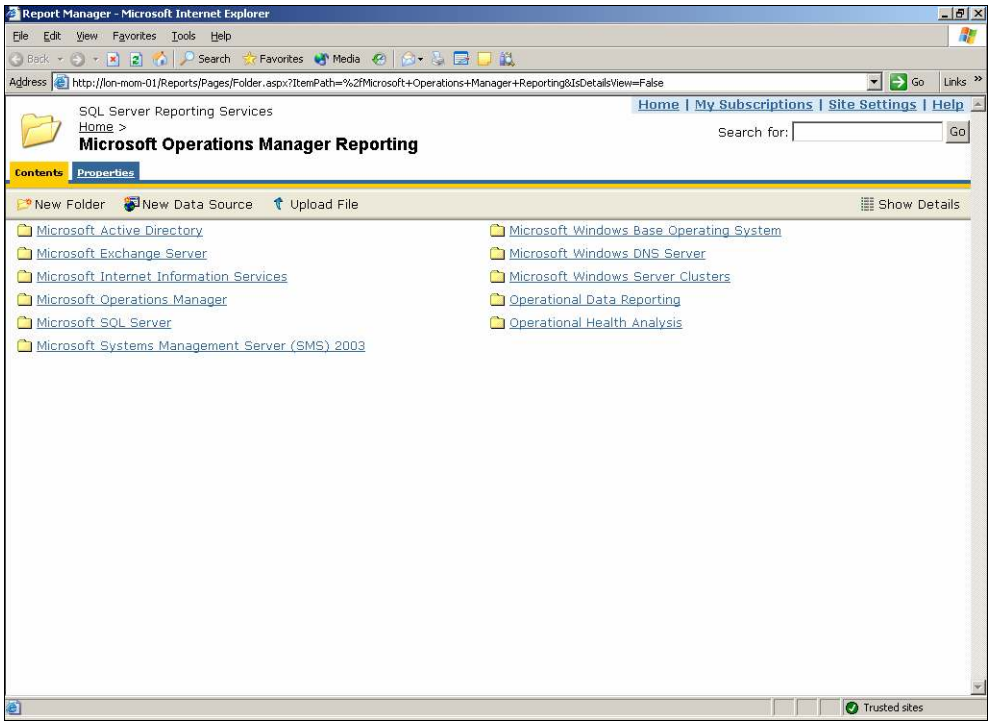


Kuva 8. Valvontakonsolin tilanäkymä.

MOM 2005:ssa on myös selainpohjainen konsoli, joka sisältää suppeamman kirjon valvontakonsolin toiminnoista. Web-konsoli on tarkoitettu järjestelmän valvontaan vain poikkeustilanteissa.

3.10. MOM-raportointikonsoli

MOM-raportointikonsoli on täysin selainpohjainen ja se sisältää valmiiksi valtavan kirjon erilaisia raporttipohjia. Käytännössä kaikkien hallintapaketti-en mukana tulevat raporttipohjat ovat tämän konsolin avulla saatavilla. Raporttikonsolilla tuotettavat raportit voidaan tallentaa myöhempää käyttöä varten useissa eri muodoissa. Kuvassa (Kuva9) on MOM-raportointikonsolin perusnäkymä.



Kuva 9. MOM 2005-raportointikonsoli.

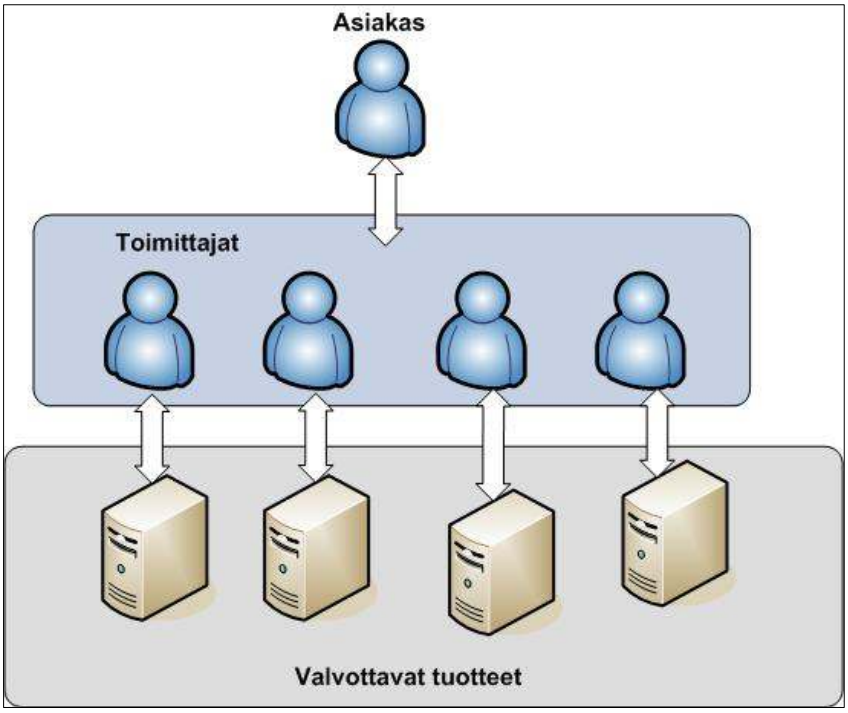
4. Monen toimittajan ympäristöt

Terveydenhuoltoalan organisaatiot (esimerkiksi sairaanhoitopiirit) ovat usein suuria kooltaan ja pitävät sisällään useita eri järjestelmä- ja palvelutoimittajia. Tämä osaltaan johtuu julkishallinnon organisaatioita koskevista kilpailutussäännöistä, jotka pakottavat kilpailuttamaan kaikki julkiset hankinnat tietyin ehdoin.

4.1. Monen toimittajan ympäristön haasteet

Suurin haaste monen toimittajan ympäristöissä on palveluiden valvonta. Jokainen toimittaja pyrkii valvomaan toimittamiaan laitteita tai palveluita omalla valvontajärjestelmällä. Vaikka kaikki toimittajat saataisiinkin käyttämään samaa valvontajärjestelmää tuotteisiinsa, tulee haasteeksi tällöin tietosuoja-asetukset. Jokainen toimittaja saa hallita vain niitä laitteita, jotka on toimittanut organisaatiolle ja sama pätee myös laitteiden tai palveluiden tilan näkemiseen. Esimerkiksi kuvassa (Kuva10) laitevalmistaja A voisi käyttää hyväkseen tietoa, jos hän näkisi laitevalmistaja B:n toimittamien järjestelmien olevan jatkuvasti epäkunnossa. Sama pätee myös raportointiin: usein suurissa organisaatioissa toimittajat valvovat omia tuotteitaan ja raportoivat asiakkaalle järjestelmässä havaituista ongelmista. Asiakas ei valvo itse tuotetta vaan saa kaiken tiedon palvelujen toiminnasta suoraan toimittajilta, jolloin palvelutason puolueeton seuraaminen on hyvin vaikeaa.

Valvonnan haasteet ilmenevät etenkin ongelmatilanteissa, joissa pitäisi nopeasti määrittää, mistä järjestelmän komponentista käyttökatkos johtuu. Jokainen toimittaja normaalisti toteaa, ettei vika johdu heistä vaan jonkun toisen toimittamista laitteista tai palvelusta. Valvonnan avulla pitäisi siis kyetä hallitsemaan koko järjestelmää ja auttaa paikantamaan vika mahdollisimman nopeasti.



Kuva 10. Asiakkaan ja toimittajan suhde normaalisti.

Ongelma on ratkaistavissa sillä, että jokainen toimittaja sitoutuu käyttämään asiakkaan määrittelemää valvontatuotetta ja asiakas itse valvoo palveluiden saatavuutta. Keskitetyllä valvonnalla voidaan näin varmistaa, että kukin toimittaja hoitaa sovitun palvelutason tuottamisen. Asiakas toimii itse valvojana tai vaihtoehtoisesti ulkoistaa edunvalvonnan kolmannelle osapuolelle.

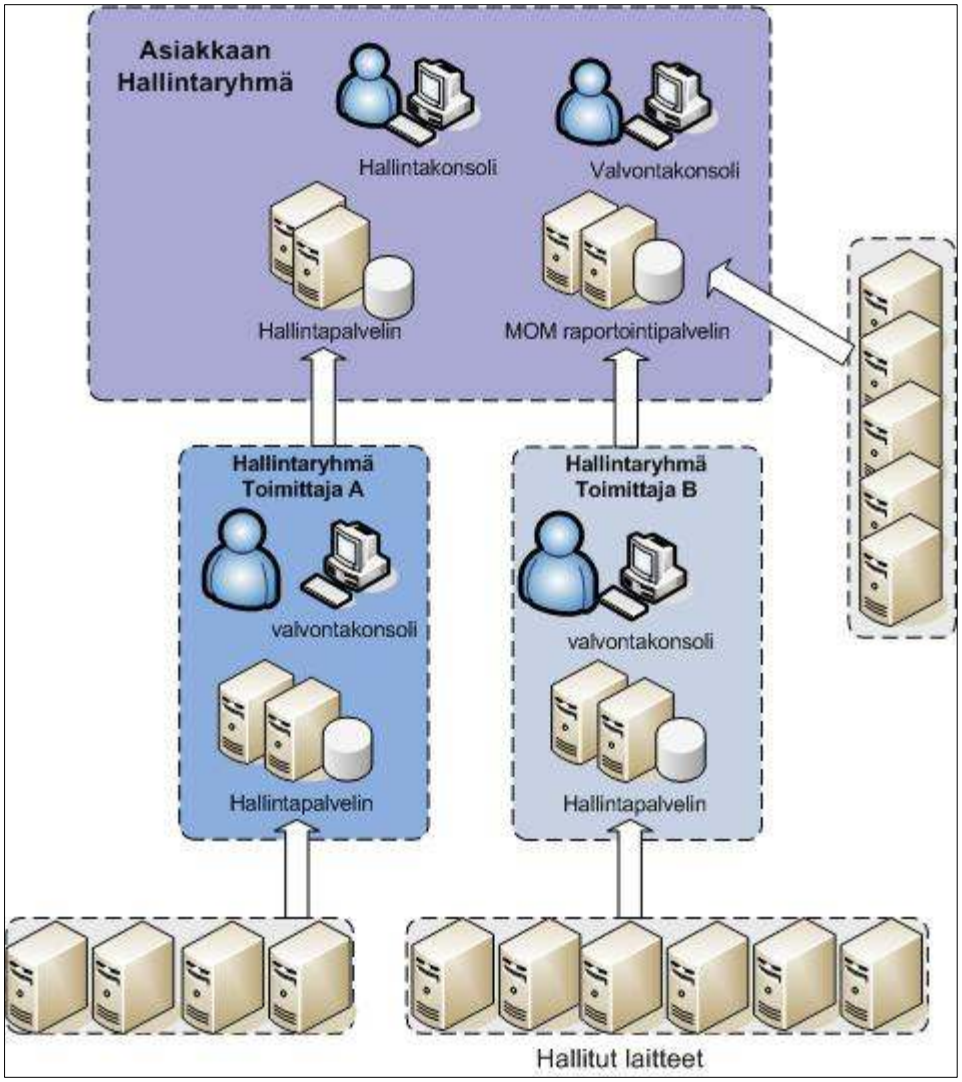
4.2. Hallintaryhmien yhdistäminen (Multitiering)

MOM 2005:n etuna on sen skaalautuvuus. MOM:n hallintaryhmät tarjoavat loogisen tavan jakaa eri toimittajien tarjoamat laitteet ja palvelut omiin ryhmiinsä. Microsoft Connector Framework (MCF) on rajapinta, jolla voidaan yhdistää joko hallintaryhmiä tai vaihtoehtoisesti eri valvontatuotteita toisiinsa. MCF mahdollistaa hälytystiedon siirtämisen kahden eri järjestelmän välillä. Kun kaksi MOM-hallintaryhmää yhdistetään, kutsutaan niiden välistä yhteyttä MOM-to-MOM Connector-integraatioksi.

Integraation avulla voidaan siis luoda kuvan yksitoista kaltaisia skenaarioita. Kuvassa toimittajilla A ja B on omat hallintaryhmänsä, johon heidän ylläpitämänsä palvelut/palvelimet kuuluvat. Molemmissa hallintaryhmissä on omat MOM-hallintapalvelimet, MOM-tietokanta sekä MOM-raportointikanta. Toimittaja A ja toimittaja B eivät voi nähdä toistensa palveluiden tilaa saati hallita niitä. MOM hallintapalvelimelta välitetään hälytystiedot asiakkaan tai kolmannen ”puolueettoman” osapuolen hallintapalvelimelle, joka valvoo molempia toimittajia. Kolmas osapuoli voi sekä valvoa että hallita molempien toimittajien laitteita palvelutason ja asiakkaan edun-

valvonnan näkökulmasta. Lisäksi kolmannen osapuolen hallintaryhmään voi kuulua myös omia laitteita, joita valvotaan suoraan MOM-etäagenttien avulla.

Asiakkaan itse valvoessa toimittajien tuottamia palveluita hän saa parhaan edun MOM 2005-tuotteesta. Ylläpidossa olevilta palvelimilta lähetetään valvontatietoja toimittajan hallintapalvelimelle, josta tieto edelleen välitetään asiakkaan omalle hallintapalvelimelle. Alla olevassa kuvassa (Kuva11) jokainen toimittaja näkee vain omassa hallintaryhmässä olevat palvelimet ja asiakas näkee kaikki ylläpidettävät palvelut.



Kuva 11. Asiakas itse toimii edunvalvojana.

5. MOM valvonnan eri roolit

Järjestelmänvalvonnan toteuttaminen suurissa organisaatioissa vaatii selkeätä työjärjestystä ja suunnitelmallisuutta toteutukselta. MOM-valvonta kannattaa toteuttaa ITIL:in virtuaalisen palvelupistemallin mukaisesti, jossa tehtävät on jaettu eri loogisten roolien vastuulle.

5.1. Koordinaattori

Koko MOM-valvonnan kannalta tärkeintä roolia esittää koordinaattori. Koordinaattorin tehtävänä on hallita koko valvonnan suunnittelua ja toteutusta. MOM-koordinaattori toimii yhteyshenkilönä kaikkien osapuolien välillä ja vastaa asioiden etenemisjärjestyksestä. Koordinaattori seuraa valvonnan tapahtumien elinkaarta ja puuttuu sellaisiin tapahtumiin, joiden ratkaisuvastuu on epäselvä tai joiden palvelusopimuksen mukainen ratkaisuaika uhkaa ylittyä.

5.2. Konfiguraatioryhmä

Konfiguraatioryhmän tehtävänä on vastata konfiguraatiotietokannan sisällöstä yhteistyössä palveluiden konfiguraatiotietokannan ylläpitäjien kanssa. Konfiguraatioryhmän vastuulla on:

- Konfiguraatiotietokannan rakenteen kehittäminen ja ylläpito
- Konfiguraatiotietojen ja niiden välisten riippuvuuksien ylläpito konfiguraatiotietokannassa.
- Konfiguraatiotietojen välitys toiminnanohjausjärjestelmään osana tapahtumanhallintaprosessia.
- Alla kuvatun MOM-ryhmän informointi valvontaan tarvittavista muutoksista.

5.3. MOM-ryhmä

MOM-ryhmän tehtävänä on vastata itse asiakkaan keskitetyn valvonnan käytettävyydestä ja konfiguroinnista. MOM-ryhmän tehtäviin kuuluu lisäksi kaikki raportointiin liittyvät toiminnot kuten:

- MOM-valvottavien palvelimien suorituskyky
- MOM-valvottavien palvelimien kapasiteetinhallinta

MOM-ryhmä vastaa myös uusien palvelinten liittämisestä valvontaan ja integraatioiden toteuttamisesta muiden toimittajien hallintaryhmiin.

6. Johtopäätökset

Päällimmäiseksi huomioksi tutkintotyön tekemisestä jäi se, että ITIL-viitekehys sopii hyvin tukemaan yrityksen jo olemassa olevia palveluprosesseja. ITIL määrittää selkeästi, mitä eri prosessien tuloksena pitäisi syntyä ja antaa vapauden yrityksille toteuttaa prosessin vaiheet eri tavoin.

ITIL-viitekehys kehittyy myös päivä päivältä eri muotoon. Tämän tutkintotyön kirjoitushetkellä ITIL on julkaissut juuri uuden version viitekehyksestä. Tulevaisuudessa toivottavasti useat eri suomalaiset yritykset huomaavat hyödyntää tätä suunnitellessaan ylläpitopalveluiden tuottamista.

Tutkintotyötä kirjoittaessa olen havainnut, että palvelunhallintaprosessien tuottaminen on hyvin aikaa vievää työtä ja vaatii jatkuvaa kehittämistä. MOM 2005 sopii hyvin suurten organisaatioiden järjestelmien valvontaan ja ylläpitoon. Ohjelmiston käyttöönotto vaatii paljon suunnittelua, mutta palkitsee pitkällä aikajuoksulla.

Tutkintotyössä käsittelemäni malli MOM-valvonnan toteuttamisesta hallintaryhmien yhdistämisellä toisiinsa, on otettu käyttöön asiakasympäristöissä ja olemme havainneet ratkaisun toimivaksi. Hallintaryhmien yhdistämisessä on kuitenkin otettava huomioon kuinka valvontatietoa ja hälytysten kuittauksia siirretään eri ryhmien välillä. Kyseessä on monen eri järjestelmän ketju, joissa automaattinen tiedonvälitys saattaa aiheuttaa helposti myös ei toivottuja tilanteita. Tilanteen tekee vielä monimutkaisemmaksi jos hälytystietoja välitetään automaattisesti toimittajien omiin valvontatuotteisiin.

Eri toimittajien omien valvontajärjestelmien liittäminen MOM-valvontaan on haastava tehtävä. Kun MOM-hallintaryhmien yhdistäminen toimii yksinkertaisesti, on taas toisten valmistajien valvontatuotteiden yhdistäminen MOM-valvontaan monimutkainen prosessi. Monen toimittajan ympäristöissä keskitetyn valvonnan tuottaminen vaatii selkeitä rooleja, jotta palvelun tuottaminen saatetaan tehdä tehokkaasti. Ilman tehokasta koordinointia palvelun tuottaminen on varmasti hyvin vaikeaa.

Lähteet

Kirjallisuus

Best Practise For Service Delivery. Office of Government Commerce (OGC) 2005.

Best Practise For Service Support. Office of Government Commerce (OGC) 2005.

Managing Your Infrastructure Using Microsoft Operations Manager 2005. Microsoft Official Cource (2287A) 2005.

Internet

ITIL Open Guide. [online] [viitattu 25.4.2007].
http://www.itlibrary.org/

Microsoft Operations Manager. [online] [viitattu 11.03.2007].
www.microsoft.com/mom