Sami Lindfors

SCOM:N TEHOKAS HYÖDYNTÄMINEN YRITYKSEN PALVELINYMPÄRISTÖN VALVONNASSA

Liiketalouden koulutusohjelma
Tietojenkäsittelyn suuntautumisvaihtoehto
2012

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

SCOM:N TEHOKAS HYÖDYNTÄMINEN YRITYKSEN PALVELINYMPÄRISTÖN VALVONNASSA

Lindfors, Sami
Satakunnan ammattikorkeakoulu
Liiketalouden koulutusohjelma
Huhtikuu 2012
Ohjaaja: Grönholm, Jukka
Sivumäärä: 48
Liitteitä: -

Asiasanat: System Center Operations Manager, palvelin, valvonta, kehittäminen

---

Tämän opinnäytetyön toimeksiantajana toimi Sachtleben Pigments Oy:n tietohallinto. Tietohallinnon toimenkuvaan kuuluu esimerkiksi työasemien käyttöönotto ja asennus, palvelimien ylläpito, kehittäminen ja käyttäjätuen antaminen.

Opinnäytetyön tarkoituksena oli tutustua ja tutkia SCOM-järjestelmää sekä tehostaa sen käytön hyödyntämistä yrityksen palvelinympäristön valvonnassa. Päätehtävänä oli tutustua talon ympäristöön ja määritellä sen valvonnan tarvetta, ja käytännössä tämä tarkoitti mm. aiheettomien hälytyksien poistamista jo olemassa olevasta järjestelmästä.

Opinnäytetyön teoriaosassa tutkitaan ja esitellään SCOM:n sisältämät toiminnot ja ominaisuudet sekä kerrotaan mihin niitä käytetään. Kaikkia SCOM:n ominaisuuksia ei ole otettu käyttöön Sachtleben Pigments Oy:n IT-ympäristössä, mutta kaikki ominaisuudet ovat kuitenkin työssä käyty läpi jos tulevaisuudessa joitain ominaisuuksia otetaan käyttöön.

Tietohallinnon toimenkuva ja valvonnan tarpeet käydään läpi opinnäytetyön kappaleessa 6. Valvonnan toteutus ja onnistuminen sekä sen tulevaisuuden kehittämiskohteet käydään läpi kappaleessa 7. Samalla todettiin kuinka SCOM:n eri ominaisuudet tehostavat yrityksen palvelinympäristön valvontaa.

Työ aiheen parissa jatkuu vielä opinnäytetyön jälkeenkin parantamalla SCOM:n käyttöä ja hyödyntämistä entuudestaan.

EFFICIENT USE OF SCOM TO MONITOR COMPANY SERVER ENVIRONMENT

Lindfors, Sami
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information Technologies
April 2012
Supervisor: Grönholm, Jukka
Number of pages: 48
Appendices: -

Keywords: System Center Operations Manager, server, monitoring, development

---

The employer of this thesis was Sachtleben Pigments Oy IT-department. The job description of the IT-department includes installing and commissioning new workstations, server maintenance, development and user helpdesk.

The purpose of this thesis was to introduce, and to examine SCOM-system, and also to improve the use of it in company server environment. The main purpose was to get to know the company environment, and to define the need of monitoring, and in practice this meant among other things the removal of unnecessary alerts from already existing system.

In the theory part of the thesis the SCOM-system functions and features are examined and introduced, and also explained how they are used. All of the features of SCOM have not been taken into use in Sachtleben Pigments Oy IT-environment, but all features have been studied in this thesis if in the future some of these features would be commissioned.

The job description and monitoring needs of IT-department are reviewed in chapter 6 of the thesis. The implementation and success of monitoring, and the future development targets are reviewed in chapter 7. At the same time it was stated how different features of SCOM improve the monitoring of company server environment.

Work with this subject will continue even after the thesis to improve the use and utilization of SCOM even more.

SISÄLLYS

1 JOHDANTO

Yrityksen palvelinympäristön ollessa suuri tai pieni on palvelimia valvottava ja seurattava aika ajoin jotta yrityksen palvelut toimisivat. Niinpä palvelimia varten on luotu keskitettyjä valvontatyökaluja. Palvelimien ylläpidon kannalta keskitetty valvontajärjestelmä helpottaa valvottavia asioita. Normaaliin tapaan valvottavat asiat käydään läpi palvelin kerrallaan. Yrityksen palvelimien laajuus riippuu tietopalveluista joita yrityksessä käytetään. Keskitetty hallintaohjelma tarjoaa helpotusta palvelimien toiminnan valvomiseen. Valvonnan tavoitteena on palveluiden paremman saatavuuden takaaminen ja ongelmatilanteiden ennaltaehkäisy.

Tässä opinnäytetyössä tutkitaan Microsoftin valmistamaa valvontatyökalua nimeltä System Center Operations Manager 2007 R2. Tämä kyseinen ohjelma löytyy jo valmiiksi asiakasyrityksen (Sachtleben Pigments Oy) käytöstä. Opinnäytetyön tarkoituksena on kyseisen ohjelman ja sen toimintojen esittely sekä sen käytön tehostaminen asiakasyrityksen näkökulmasta.

Havaintomateriaalina käytän itse ohjelmaa ja siihen liittyvää kirjallisuutta, sekä pohjatietoja saamastani kolmen päivän peruskurssista kyseisen ohjelman käyttöön ja hallintaan liittyen. Tarkoituksena on saada ohjelma palvelemaan mahdollisimman hyvin yrityksen tarpeita.

Opinnäytetyössä esitellään aluksi asiakasyritys ja sen jälkeen käsitellään yleisesti asiaa palvelimien hyvinvoinnin seuraamisesta ja tarkkailusta. Seuraavaksi esitellään Microsoftin valvontatyökalun esittely ja sen toiminnot ja ominaisuudet, sekä käydään läpi asiakasyrityksen palvelinympäristön rakenne ja valvottavien asioiden tarpeet ja niiden toteutus. Lopuksi käydään läpi työn onnistuminen ja tulevaisuuden kehittämiskohteet ohjelman käyttöön liittyen.

2 YRITYSESITTELY

Sachtleben Pigments Oy on titaanidioksidia valmistama teollisuuden yritys. Yritys sijaitsee Kaanaan teollisuuspuistossa, joka on Meri-Porissa. Porin tehdas kuuluu saksalaiseen Sachtleben Chemie konserniin. Puhekielessä puhuttaessa Sachtelebenista tarkoitetaan kahta tehdasta ja yhtä tiimiä. Porin tehdas toimii yhteistyössä Saksan tehtaan kanssa, joka sijaitsee Duisburgissa. Tuotantoa suoritetaan näillä kahdella toimipaikalla. Molemmat, sekä suomalainen että saksalainen tehdas, ovat amerikkalaisen Rockwood-konsernin ja Kemiran omistuksessa. Rockwood-konserni omistaa yhteisyrityksestä 61 % ja Kemira 39 %. (Sachtlebenin yritysesite)

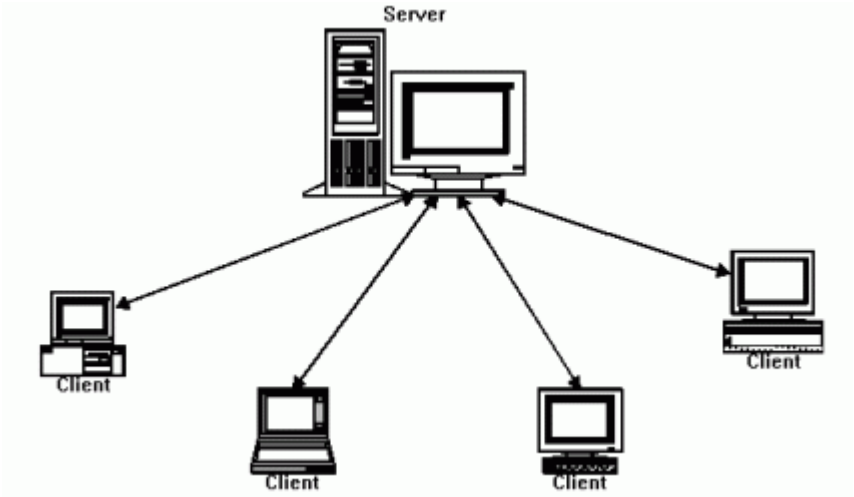
Sachtleben tunnetaan maailmanlaajuisesti 130 vuoden kokemuksesta ja korkealuokkaisista tuotteistaan. Pitkäaikaiset asiakkaat tietävät: Sachtlebenin luotettavuuteen ja toimintakykyyn voi luottaa. Tämä perinne luo vankan perustan menestykkäälle tulevaisuudelle. Koko Sachtlebenin liikevaihto on noin 570 miljoonaa euroa ja henkilöstöä on noin 1700. Saksan tehtaalla Duisburgissa työskentelee 1150 henkilöä, ja Porin tehtaalla Kaanaassa työskentelee 550 henkilöä. Myynti on globaalia ja jakautunut seuraavasti: 55% Eurooppa, 20% Aasia/Tyynimeri, 20% Amerikat, 5% Lähi-ita/Afrikka. (Sachtlebenin yritysesite)

Sachtleben Pigments Oy:n juuret Porissa ulottuvat vuoteen 1961. Yritys on silloin aloittanut toimintansa nimellä Vuorikemia. Tämän jälkeen yritys on toiminut Kemira Pigments Oy nimellä. Vuonna 2008 yrityksen nimi muuttui Sachtleben Pigments Oy:ksi yrityskauppojen myötä. Kemira Pigments yhdistyi tällöin saksalaisen Sachtleben Chemie:n kanssa. (Sachtlebenin yritysesite)

Sachteleben valmistaa titaanidioksidia. Titaanidioksidi on keinotekoinen kemiallinen yhdiste, jonka raaka-aineena on ilmeniitti. Sachtlebenin Porin tehdas käyttää titaanidioksidin valmistukseen 300 000 tonnia ilmeniittiä vuodessa. Tärkeimmät käyttökohteet titaanidioksidille ovat: maalit, painovärit, elintarvikkeet ja kosmetiikka. Näiden jokapäiväisten tuotteiden valmistamisessa titaanidioksidin tarve on tasaisen varmaa. (Sachtlebenin yritysesite)

3 YLEISTÄ PALVELIMIEN HYVINVOINNISTA

Palvelimen tehtävänä on tarjota palveluita käyttäjille. Kuvassa 1 on hahmoteltu palvelin, jonka kanssa asiakaskoneet keskustelevat. Suurin osa palveluista yritysympäristössä on toimittava lähes kellon ympäri. Palveluiden toiminnan turvaamiseksi palvelimen ylläpitoa ja hyvinvointia on tarkkailtava. Palvelimien elinkaari on lyhyempi kuin tavallisten työasemien, koska ne käyvät kovemmalla rasituksella. Palvelimia ei juuri koskaan sammuteta kuten työasemia. Ainoastaan huoltotöiden aikana palvelin voidaan joutua hetkeksi sammuttamaan. Esimerkiksi muistin lisääminen tai jonkun uuden ohjelman käyttöönotto saattaa vaatia uudelleenkäynnistämisen. Koska palvelimet pitävät elintärkeitä palveluita yllä, kuten sähköpostia ja käyttäjien omia tiedostoja, tulee palvelimen huolto suorittaa nopeasti ja tarkkaan harkittuna ajankohtana, ja ennen kaikkea hyvissä ajoin ilmoittaa siitä yrityksen sisällä. Huolellinen palvelimen huoltotyön esivalmistelu säästää aikaa ja vaivaa ja palvelee parhaalla mahdollisella tavalla yrityksen tarpeita.



Kuva 1. Palvelimen (Server) ja Asiakaskoneiden (Client) toimintamalli (http://blogs.gameshastra.in/wp-content/uploads/2011/01/jw-1019-jxta1.gif, haettu 7.11.2011)

3.1 Fyysiset olosuhteet

Palvelimien fyysiseen hyvinvointiin vaikuttaa palvelinhuoneen (Kuva 2) olosuhteet. Palvelinhuone koostuu tietoverkon operatiivisessa käytössä olevista laitteista. Viralllisemmin palvelinhuonetta kutsutaan IT-laitetilaksi. Palvelinhuoneen laitteet vaativat toimiakseen tietyt muuttumattomat olosuhteet. Palvelimien fyysisen hyvinvoinnin kannalta palvelinhuoneen vaatimukset on oltava kunnossa. Fyysisen turvallisuuden kannalta tärkeä peruslähtökohta on kulunvalvontajärjestelmä. Palvelinhuone tulee olla lukittu. Kulunvalvontajärjestelmän avulla saadaan rajoitettua, kenellä on pääsy palvelimien luokse ja näin ollen voidaan pienentää asiattoman käytön vaaraa. Kulunvalvontajärjestelmän avulla on myös mahdollista seurata palvelinhuoneessa tapahtuvaa liikennöintiä. Kulunvalvontaraportista voidaan tarkkaan nähdä päivämäärineen ja kellonaikoineen kuka on liikkunut palvelinhuoneessa. (Perkola Timo, Tietoviikko 2007)

Palvelinhuoneen koko on mitoitettava palvelimien vaativan tilan mukaisesti. Liian ahtaassa palvelinhuoneessa saattaa ilmetä lämpötilaongelmia. Palvelinhuoneessa on oltava riittävästi ilmatilaa jokaiselle palvelimelle. Palvelinhuone on oltava myös riittävän laaja mahdollisia laitelisäyksiä ajatellen. Nykyään palvelinten virtualisointi vähentää palvelimien kasvua IT-laitetiloissa. Virtualisoinnin avulla voidaan yhden fyysisen palvelimen sisällä ajaa virtuaalisia palvelimia jotka toimivat samalla tavoin kuin fyysisetkin palvelimet. Virtuaalisointialusta eli fyysinen palvelinrauta on oltava riittävän tehokas ja siinä on oltava asennettuna virtualisointiin mahdollistavat ohjelmat. Virtuaalisten palvelimen fyysisen hyvinvoinnin seuraaminen on tehokkaampaa, kun palvelimet ovat samassa fyysisessä raudassa. (Tapiola.fi Palvelintilan suunnitteluohje 2011)

Tyypillisesti fyysiset palvelimet asennetaan räkkiin (rack) eli niille erikseen tarkoitettuun laitekehikkoon. Laitekehikkoon kuuluun yleensä myös lukittava etuovi, joka suojaa palvelimia. Laitekehikkoja on myös saatavilla jäähdytyksellä varustettuna. Ilman jäähdytettyä räkkiä tulee palvelinhuoneen ilmastointi toteuttaa erillisenä. Ilmastoinnin avulla saadaan pidettyä palvelinhuoneen lämpötila ja kosteus tasaisena. Palvelinten käyttöikä lyhenee, jos ne käyvät jatkuvasti liian kuumina. Palvelimen sisäinen lämpötila on useita asteita kuumempi, kuin palvelinhuoneen lämpötila. Lii-

allinen kuumuus palvelimen sisällä voi aiheuttaa levy-aseman rikkoutumisen tavallista useammin. Suositeltu palvelinhuoneen lämpötila on noin 16 – 24 °C. Lämpötilaa on hyvä tarkkailla samalla kun asioi palvelinhuoneessa. Lämpötilan seurannan ohella on myös kiinnitettävä huomioita tilojen suhteelliseen kosteuteen. Suhteellisella kosteudella tarkoitetaan yksinkertaisesti vesihöyryn määrää ilmassa. Liiallinen kosteus saattaa aiheuttaa oikosulkuja ja palvelimen komponentit saattavat muuttua hauraiksi. Suositusilmankosteus palvelinhuoneelle on 40 – 55 %. Palvelimet kestävät kyllä kosteuden vaihtelua 10 – 90 % välillä, mutta olisi suositeltavaa pysyä suositelluissa raja-arvoissa. (Tapiola.fi Palvelintilan suunnitteluohje 2011)

Palvelinhuoneessa tulee olla myös asianmukaiset sammutusjärjestelmät sekä palvelinhuoneen on täytettävä tietyt paloturvallisuusluokitukset. Palvelinhuoneessa ei saa olla ylimääräistä palokuormaa. Palvelinhuone on siivottava säännöllisesti, jotta pölystä ja roskista aiheutuvat paloriskit ja laiterikot saadaan minimoitua. Siistijöiden tulee olla koulutettu siivoamaan keskustiloja. Palvelinhuoneessa ei saa säilyttää esineitä tai tavaroita, joita siellä ei tarvita. Myös ylimääräiset verkko- ja virtakaapelit tulee siirtää pois palokuormaa keräämästä. Palvelinhuoneen välittömässä läheisyydessä olevissa huoneissa ei saa olla merkittävää määrää palokuormaa, kuten palavia nesteitä ja suuria paperiarkistoja. Palvelimien sähkönsaanti on varmistettava sähkökatkojen vuoksi UPS – laitteilla, joiden tehtävä on taata palvelimille tasainen virransaanti lyhyissä sähkökatkoksissa ja syöttöjännitteen epätasaisuuksissa.

Kuva 2. Mallikuva nykyaikaisesta palvelinhuoneesta. Kuvassa on vierekkäin seitsemän laitekehikkoa ja hallintakonsoli. (http://us.123rf.com/400wm/400/400/ vla-

dru/vladru1105/vladru110500017/9572316- modern-server-room-done-in-3d-black.jpg, haettu 8.11.2011)

3.2 Ohjelmalliset olosuhteet ja palvelinroolit

Palvelimien toiminnan edellytyksenä on fyysisten olosuhteiden lisäksi ylläpidettävä palvelimilla toimivia käyttöjärjestelmiä ja ohjelmia. Palvelimen rooli määrittelee tietyt puitteet, jotka on täytettävä, jotta palvelin palvelisi tuotantoympäristössä parhaalla mahdollisella tavalla. Ennen uuden palvelimen käyttöönottoa palvelinta voidaan testata erillisessä testiympäristössä. Testiympäristössä havaitaan mahdolliset virheet joita voidaan korjata ennen palvelimen käyttöönottoa tuotantoympäristöön. Jokaisessa palvelimessa on oltava perusasiat kunnossa: käyttöjärjestelmän tietoturvapäivitykset ja virustentorjunta sekä varmuuskopiointi. Käyttöjärjestelmän elinkaari on myös syytä ottaa huomioon. Elinkaari määrittelee, kuinka kauan käyttöjärjestelmää tuetaan. Virustentorjuntaohjelmiston toiminta ja sen uudet virustunnistetietopäivitykset ovat yksi osa tietoturvaa. Säännöllisellä varmuuskopioinnilla varaudutaan tilanteisiin, jossa palvelin vikaantuu niin, että se joudutaan palauttamaan varmuuskopiolta, tai muilta tiedon palautustarpeen aiheuttavilta syiltä, esimerkiksi inhimillisiltä virheiltä.

Yleisimpiä palvelinrooleja:

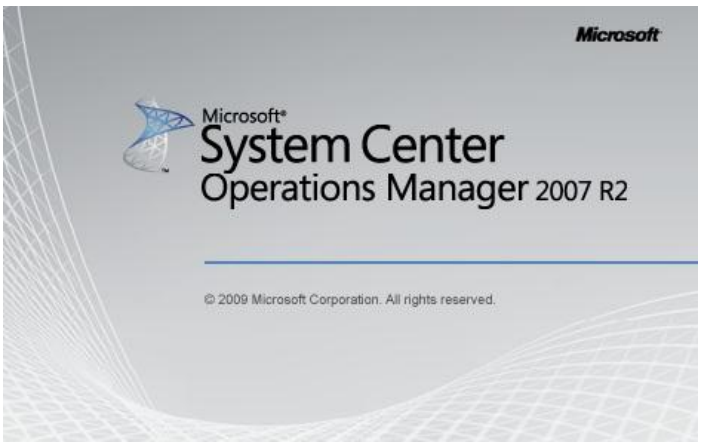
- Tiedostopalvelin (file server), säilyttää ja jakaa tiedostoja. Tiedostopalvelimella säilytetään yhteisiä sekä yksityisiä tiedostoja. Tiedostot ovat turvassa tiedostopalvelimella koska sieltä otetaan säännöllisesti varmuuskopio.
- Tietokantapalvelin (database server) voi sisältää yhden tai useamman tietokannan. Tietokanta on kokoelma tietoja, joilla on yhteys toisiinsa. Yritystasolla tietokantapalvelimella voi olla useita erilaisia tietokantoja, kuten: asiakastietokanta, osto- ja laskutus tietokanta.
- Tulostinpalvelin (print server) hallinnoi yrityksen tulostimia. Tulostimet on jaettu käyttäjille tulostinpalvelimen kautta. Tulostimien ylläpidot suoritetaan keskitetysti tulostuspalvelimelta.
- Sähköpostipalvelin (mail server) pitää sisällään käyttäjien sähköpostilaatikot ja postikannat. Sähköpostipalvelin huolehtii yrityksen sähköisestä viestinnästä.

- Sovelluspalvelin (application server) pitää sisällään ohjelmia, joita käyttäjät voivat käyttää asentamatta niitä omalle työasemalleen.

4 SYSTEM CENTER OPERATIONS MANAGER 2007 R2

4.1 Historia

Vuonna 2000 Microsoft esitteli ensimmäisen valvontaohjelmistonsa: Microsoft Operations Managerin (MOM), joka tarjosi yrityksille työkalun verkon monitorointiin. Sen avulla saatiin valvottua yrityksen palvelimia ja niillä toimivia palveluita. Tämä työkalu helpotti huomattavasti yrityksien IT-infrastruktuurin valvontaa. Seuraavaksi Microsoft esitteli tuotteen Microsoft Operations Manager 2005:n (MOM 2005), joka perustui edelliseen versioonsa sisältäen muutamia uudistuksia. Näiden kahden ensimmäisen ohjelmistotuotteen jälkeen IT-infrastruktuuri kehittyi hurjaa vauhtia eteenpäin ja niinpä System Center Operations Manager 2007 (SCOM) valmistettiin täysin uuteen lähdekoodin perustuen uusilla ominaisuuksilla ja uusilla ratkaisuilla. SCOM:in uusin versio on 2007 R2 (Kuva 3), jota esitellään seuraavassa luvussa. Uusin versio Microsoftin valvontatuote perheestä on Microsoft System Center Operations 2012 RC, joka on vielä kokeiluversio. Sen julkaisuajankohtaa ei ole vielä päätetty.
(Wikipedia; Meyler ym 2010, 14)



Kuva 3. Kuvaruutukaappaus SCOM tuotteesta

4.2 Esittely

Microsoft System Center Operations Manager 2007 R2 (kuva 3) on kolmannen sukupolven tuote ja se julkistettiin maaliskuussa 2009. SCOM tarjoaa hyvän valvontatyökalun kaikenkokoisille yrityksille. SCOM asennus on jokaisessa ympäristössä omanlaisensa ja näin ollen se tulee säätää valvottavan ympäristön mukaisesti. Yleispätevää asennusta ei siis ole. Ohjelma mukautuu pikkuhiljaa käytössä ylläpitäjän toimesta tarpeitaan vastaavaksi. Palvelinympäristön valvonta SCOM:ia hyödyntäen lisää tietohallinnon liiketoiminnan resursseja tehokkaasti. Mikäli yrityksessä on kymmeniä, satoja tai tuhansia valvottavia palvelimia ja palveluita, niin näiden yksittäinen läpikäyminen olisi melko työlästä ja aikaa vievää. SCOM tarjoaa valvonnan ja hallinnan haasteisiin automatisoidun ja keskitetyn hallintaympäristön. Loppukäyttäjän palvelut ja sovellukset ovat korkealla prioriteetilla yritysmaailmassa. SCOM:in avulla palveluiden ja sovellusten toimivuus saadaan varmistettua, ja joissain tilanteissa ohjelma pystyy suoraan korjaamaan vian. (Wikipedia)

Microsoft on erityisesti panostanut SCOM:in tehokkuuteen hallita Microsoft tuotteista koostuvaa ympäristöä. SCOM:in avulla pystytään myös valvoa UNIX ja Linux ympäristöjä. SCOM:in valvontamahdollisuudet eivät ulotu pelkästään palvelimiin ja työasemiin. Myös verkon aktiivilaitteita ja hajautettuja sovelluksia on mahdollisuus valvoa SCOM:in avulla. SCOM on ohjelmana hyvin joustava ja säädettävä, joten se pystyy hyvin elämään muuttuvassa ympäristössä. Helppokäyttöisen käyttöliittymän avulla SCOM:in toiminnan seuraaminen on helppoa. Valvottavien asioiden määrittely ja asetusten säätäminen tarvitsee hieman syvällisempää tuntemusta. Valvontaan liittyviä sääntöjä on mahdollista muokata ylläpitäjän haluamalla tavalla. Esimerkiksi: jos jokin säännöllinen toiminto aiheuttaa virheen, on mahdollista luoda poikkeus kyseiselle asialle, jotta vältyttäisiin turhalta hälytykseltä.
(Microsoft a)

4.3 Toiminta ja rakenne

SCOM-ympäristö vaatii toimiakseen vähintään yhden palvelimen. Käyttöjärjestelmän minivaatimus on vähintään Windows Server 2003 SP1. Palvelimella tulee olla käyttöjärjestelmän lisäksi SQL Server 2005 tai 2008 tietokanta. SCO- ympäristö koostuu useista palvelinrooleista, jotka on mahdollista asentaa yhteen palvelimeen. Kuitenkin Microsoft suosittelee roolien hajauttamista useammalle palvelimelle paremman käytettävyyden ja toiminnan takaamiseksi. Etenkin jos yrityksen valvontatarpeiden määrä on riittävän suuri. Yksinkertaisuudessaan SCOM toimii valvonta agenttien avulla, jotka asennetaan kohdekoneisiin. Nämä agentit välittävät tiedot SCOM hallintapalvelimelle. (Price ym 2007, 46-53)

SCOM-järjestelmän ylläpitäjän, joka vastaa SCOM:in hallinnasta ja toiminnasta, tulee olla tietoinen mistä SCOM järjestelmä muodostuu. SCOM-järjestelmän asennus koostuu hallintaryhmästä (Management Group). Hallintaryhmä on perusosa SCOM:in toiminnallisuutta. Minimissään SCOM ympäristö koostuu RMS-palvelimesta (Root Management Server) ja Operational Database tietokannasta. RMS palvelin on SCOM järjestelmänhallinnan ydinosa. Kun SCOM hallintakonsolin aukaisee se ottaa yhteyttä RMS palvelimeen. Hallintakonsoli on tyypillisesti asennettu RMS palvelimeen. Kaikki hallintaryhmän jäsenet keskustelevat RMS palvelimen kanssa. RMS palvelin pyörittää Operational Database tietokantaa. Tietokanta on SQL-muotoinen ja se sisältää kaikki oleelliset asiat, kuten asennusympäristön konfiguraatiot ja tiedon kaikesta valvotusta datasta. (Price ym 2007, 46-53)

RMS-palvelin huolehtii mm. siitä mitä valvotaan ja miten valvotaan. Valvonta agentit voivat kerätä informaatiota ilman RMS palvelimen käskytystä. Kaikki SCOM-palvelinroolit ovat RMS alisteisia, eli ne keskustelevat sen kanssa toimiakseen. RMS-palvelin on asennuksen yhteydessä luonut operatiiviseen tietokantaan kryptausavaimen. Eli tietokanta on asennuksen yhteydessä suojattu kryptausavaimella. Katastrofintilanteen sattuessa, jos RMS-palvelin kaatuu, ja se joudutaan uudelleen rakentamaan, olemassa olevaa operatiivista kantaa ei voi käyttää uudessa ympäristössä jollei ole tallessa tallennettua kryptausavainta. Uutta asennusta pystyttäessä SCOM-asennusvelho sisältää System Center Capacity Planner liitännäisen, joka te-

kee laskennalisen ja arvioivan mallin SCOM:in vaatimasta laiteympäristöstä. (Meyler ym 2010, 1-10)

4.4 SCOM palvelinroolit

SCOM-ympäristön asennus sisältää kaiken kaikkiaan 11 eri palvelinroolia. Edellisessä luvussa käytiin lyhyesti läpi perusrakenne eli RMS palvelin, Operational Database ja Management Group. Seuraavassa luettelossa käydään niiden toimintaa tarkemmin läpi. Edellä mainittujen roolien jälkeiset palvelinroolit ovat tukirooleja. Juurijärjestelmä koostui ainoastaan RMS palvelimesta ja sen Operational Database tietokannasta sekä mahdollisista hallintapalvelimista.

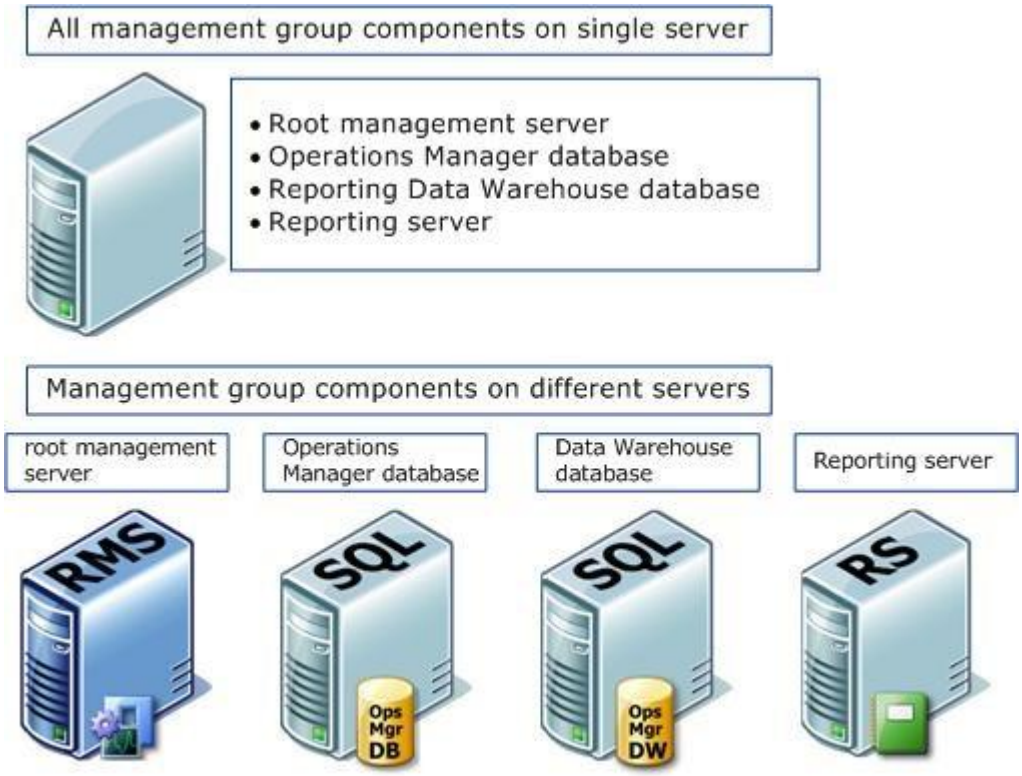
Palvelinroolit:

Root Management Server ensimmäiseksi SCOM-ympäristöä perustettaessa puhutaan hallintaryhmästä, joka vähintään koostuu RMS-palvelimesta, joka pitää sisällään operatiivisen tietokannan ja on koko järjestelmän ydinosa. RMS toimii koordinaattorina valvottavien laitteiden terveydentilojen tarkkailuun. RMS-palvelin vastaanottaa valvonta agenttien tietoja. Jotta RMS-palvelin ei kuormittuisi liikaa, voidaan SCOM-järjestelmä hajauttaa hallintaryhmiin. Hajauttaminen ei ole pakollista, mutta suositeltavaa isoissa ympäristöissä. Idea järjestelmän hajauttamisessa on se että valvonta agenttien informaatio ei mene suoraan RMS-palvelimelle, vaan se kiertää hallintaryhmään kuuluvien palvelimien kautta, jotka välittävät tiedon RMS-palvelimelle. Tämä vähentää huomattavasti RMS-palvelimen kuormitusta. Useiden hallintapalvelimien avulla saadaan kerättyä kaikki data valvotuista järjestelmistä ja silti ylläpitää loppukäyttäjän palveluita. RMS-palvelin on vastuussa tiettyjen kriteerien täyttymisestä hajautettujen sovelluksien ja palveluiden terveydentilan ylläpitämiseksi.

RMS-palvelin sisältää kaksi palvelua, jotka eivät ole käytössä muilla hallintapalvelimilla (Management Servers). **The System Center Management Configuration** palvelun vastuu on ilmoittaa hallintaryhmän palvelimille ja agenteille uudet konfiguraatiot, jos uusia määrityksiä on tehty. **System Center Data Access** käsittelee kaikkia hallinta ja web-konsolissa olevaa liikennettä. Hallintaryhmässä voi olla vain yksi

RMS-palvelin. Isojen ympäristön SCOM käyttöönotossa on mahdollista klusteroida eli kahdentaa RMS-palvelin, jotta valvonta-agenttien tiedonkulku olisi hajautetumpaa.

Management Servers hallintapalvelimet pitävät yhteyttä valvonta-agentteihin, jotka ovat asennettu valvottaviin kohteisiin. Hallintapalvelimet välittävät valvonta-asioihin liittyvää informaatiota valvonta-agenteille. Kun valvonta-asetuksia muutetaan, hallintapalvelin välittää muuttuneet asetukset valvonta-agenteille. Hallintapalvelimet ikään kuin ohjailevat valvonta agenttien toimintaa. Valvonta-agentit keräävät hallintapalvelimilta saatujen määräyksien mukaan datatietoja. Datatiedot pitävät sisällään erilaisia lokitietoja mm. hälytyksien määrästä ja valvottavien asioiden terveydentilan raportoinnista. Vähintään yhdestä hallintapalvelimesta muodostuu **Management Group** eli hallintajoukko (Kuva 4). Hallintajoukko sisältää erilaisia palvelinrooleja, joita käsitellään tässä luvussa.



Kuva 4. Kuvassa on hahmoteltu malli kahdella eri tapaa toteutetusta **Management Group** hallintajoukosta palvelinrooleineen. Kuvan alaosassa näkyvät neljä eri palve-

lin roolia on hajautettu neljään eri palvelimeen. Kuvan yläpuolella oleva yksittäinen palvelin sisältää itsessään kaikki samat palvelut kuin neljän palvelimen hajautettu hallintajoukko.

4.5 SCOM tukiroolit

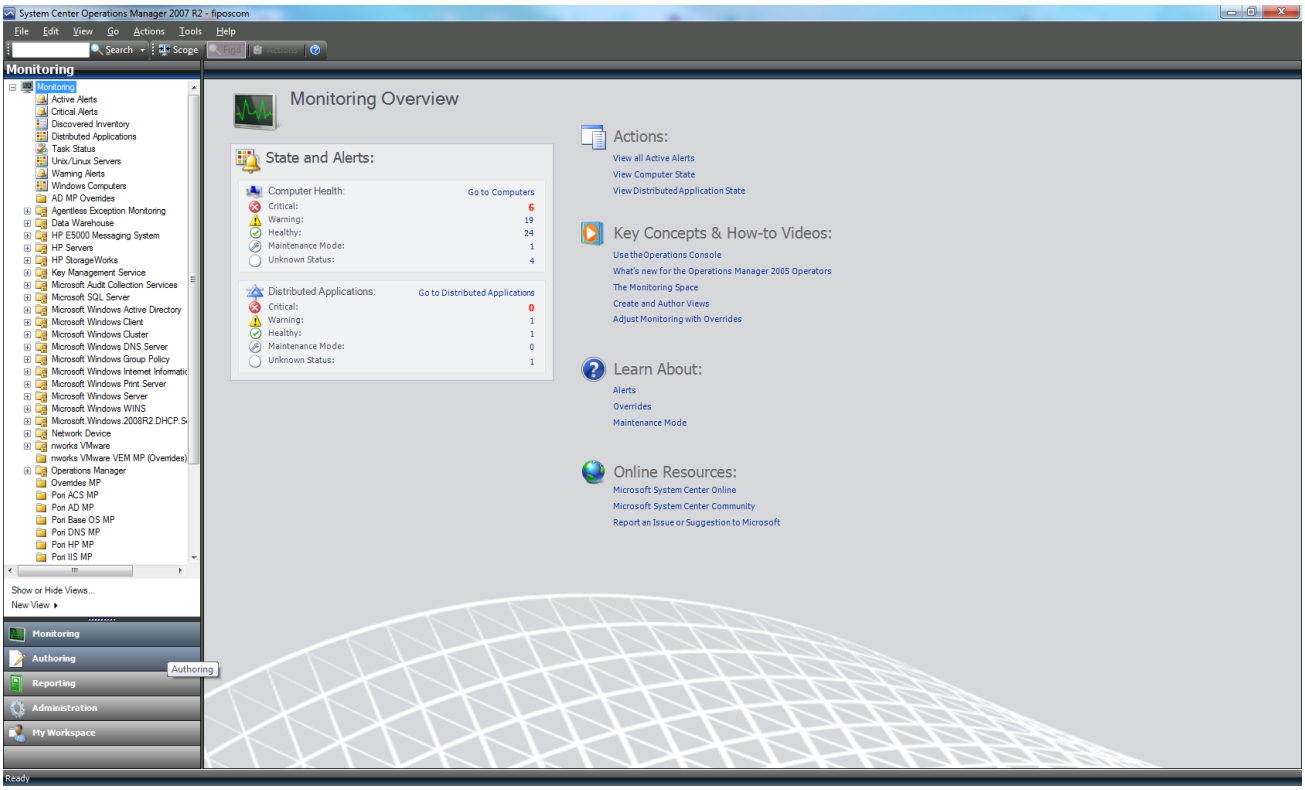
Supporting roles (tukiroolit) ovat erilaisia päälleliimattuja hallintaryhmän osia. Osa näistä tukirooleista on tietokantaperusteisia ja tukirooleihin kuuluvat myös hallintakonsoli, web-konsoli ja asiakasperustaiset palvelut. Osa näistä tukirooleista on välttämättömiä SCOM ympäristön toiminnallisuudessa.

Gateway Server on operations manager 2007:n uusi palvelu. Gateway palvelu mahdollistaa sellaisten tietokoneiden valvonnan, jotka sijaitsevat ei luotetussa AD-metsässä. Ei luotetussa AD-metsässä oleviin koneisiin on asennettu normaalisti valvonta agentti. Gateway serverin asetukset mahdollistavat agentin välittää tietoja ei luotetusta AD-metsästä luotettuun AD-metsään. Tällä tavalla pystytään toteuttamaan valvonta koskien omia järjestelmiä, jotka voivat olla yhteistyökumppanin käytössä tai DMZ verkossa tai kokonaan erillisessä toimialueessa. Tämä tukirooli ei ole pakollinen palvelinrooli SCOM-ympäristössä. Ei luotetussa AD-metsässä olevan tietokoneen agentti välittää tiedon (kuva 5) kerberos pohjaisella autentikointi menetelmällä Gateway Server palveluun. Gateway server palvelu taas välittää agentin tuoman tiedon sertifikaatti pohjaisella autentikoinnilla hallintapalvelimelle joko suoraan RMS-palvelimelle tai hallintapalvelimella.

Kuva 5. Vasemman puoleinen vihreällä pohjalla oleva ympäristö kuvaa omaa AD-metsää, sinisellä pohjalla oleva ympäristö on yhteistyökumppanin ei-luotettu AD-

metsä. Kuvasta on luettavissa miten tiedonkulku tapahtuu agentilta omalle hallintapalvelimelle.

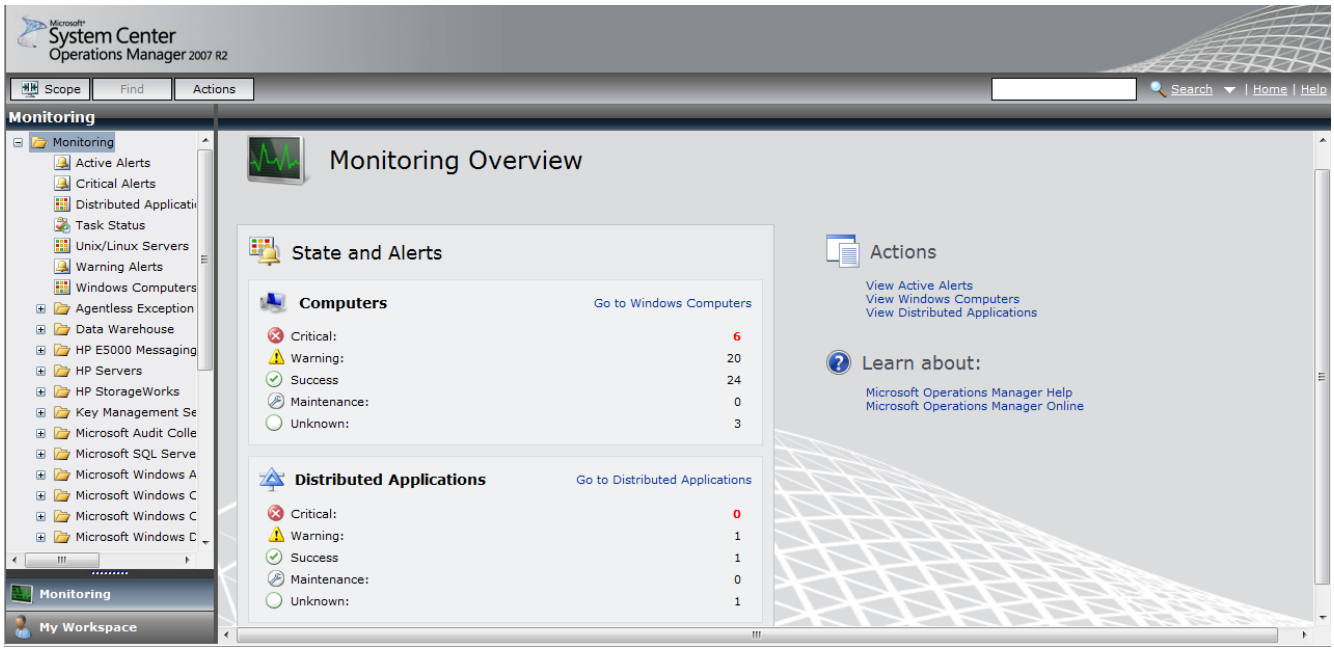
Operations Console eli hallintakonsoli. SCOM-ympäristöä asennettaessa oletusasetuksilla hallintakonsoli asentuu hallintapalvelimiin, tai pelkästään RMS-palvelimelle, jos hallintaympäristöä ei ole hajautettu. Hallintakonsoli (kuva 6) on myös mahdollista asentaa järjestelmänylläpitäjän toimesta myös työasemalle. Hallintakonsolin käyttö omalta työasemalta säästää SCOM-ympäristön kuormitusta. Vähintään yksi asennus hallintakonsolista pitää tehdä, jotta SCOM-ympäristöä pystytään hallinnoimaan. Hallintakonsoli on myös mahdollista asentaa muiden järjestelmien ylläpitäjien työasemille.



Kuva 6. Kuvaruutukaappaus Operations Console hallintakonsoli ohjelmiston päänäkymästä.

Web Console eli webbikonsoli on ulkoasultaan samannäköinen kuin ohjelmallinen hallintakonsoli ohjelmisto. Webbikonsoli ei ole pakollinen SCOM ympäristön toiminnallisuudessa, mutta se on suositeltavaa asentaa. Webbikonsoli on kätevä valvon-

ta-asioita seuratessa. Webbikonsoli (kuva 7) on helppo ottaa auki mistä tahansa yrityksen lähiverkossa olevalta työasemalta. Esimerkiksi jos huomataan, että jotain tiettyä hälytystä tulee aika ajoin joltain valvottavalta kohde koneelta. Tällöin tilannetta voidaan seurata epäillyltä työasemalta käsin, ja tehdä eri kokeilua ja seurata koko aika hälytysten tilaa nettiselaimen päällä toimivasta webbikonsolista. Webbikonsoli on tarkoitettu vain hälytyksien katselua varten. Varsinaisten muutosten tekeminen webbikonsolissa on hyvin rajattua. Käytännössä se toimii vain katselua varten. Webbikonsoli tarvitsee IIS palvelun toimiakseen.



Kuva 7. Kuvaruutukaappaus Webbikonsolin päänäkymästä suoraan nettiselaimelta.

Reporting Server perustuu SQL-pohjaisiin raportointipalveluihin. Raportointipalvelimen tehtävänä on lähettää kyselyitä tietokantaan ja esittää halutut raportit HTML-muodossa. Raportointipalvelua hyödyntämällä pystytään tuomaan hallintakonsolista haluttuja erilaisia raportteja, kuten esimerkiksi raportteja kaikista aktiivisista hälytyksistä. Reporting server palvelu on asennettava, jos halutaan tuottaa raportteja hallintakonsolista. Raportointipalvelun avulla on helppo tuoda raportteja halutulta aikaväliltä.

Reporting Data Warehouse Database on SQL-tietokanta jota käytetään hallintaryhmän historiatietojen tallentamiseen. Tämä tietokanta pitää sisällään dataa pitkältä

aikaväliltä. Reportin Data Warehouse tietokantaan pumpataan operatiivisesta tietokannasta tietoa määritellyin aikavälein. Tämä palvelu mahdollistaa kattavat historiatieto raportit ja tehostaa historiatietojen etsimistä. Tämä palvelinrooli on vaadittu vain, jos luodaan raportinomaisesti tietoja pitkältä aikaväliltä

Audit Collection Services Collector (ACS) on eräänlainen tietoturvalokeja keräävä lisäpalvelu. Tietoturvalokit sisältävät valvottavista koneista erilaisia informaatioita, kuten esimerkiksi käyttäjän epäonnistuneet kirjautumiset ja onnistuneet kirjautumiset. Windows palvelinkäyttöjärjestelmät tallentavat paikallisesti jatkuvasti erilaisia audit policy lokeja, jotka sisältävät mm. kirjautumistietoja. ACS-palvelu osaa hakea yksilöllisesti valvontapolitiikkaan liittyviä lokitietoja valvottavailta palvelimilta. Palvelu mahdollistaa myös näkemään tiedostojen tapahtumahistoriat. Esimerkiksi jos halutaan tietää, kuka on muokannut jotain yksittäistä tiedostoa tai vaikka hävittänyt sen. Tietoja pystytään keräämään reaaliajassa tämän palvelun avulla.

ACS tulee asentaa hallinnoivalle palvelimelle (management server), joka on konfiguroitu vastaanottamaan tietoturvalokeja. ACS ei ole SCOM-ympäristön oletusasetuksissa mukana, vaan se on lisäpalvelu. ACS:n asennuksen yhteydessä asennetaan tietoja keräävä palvelu hallintapalvelimelle.

ACS Forwarder ACS:n toiminnan mahdollistamiseksi on agenteille mahdollistettava forwarder ominaisuus, jotta agentti osaa välittää juuri oikeanlaista valvontapolitiikkaan liittyvää tietoa ACS palveluun. Tämä ominaisuus tulee olla päällä, jotta ACS-palvelu voi toimia.

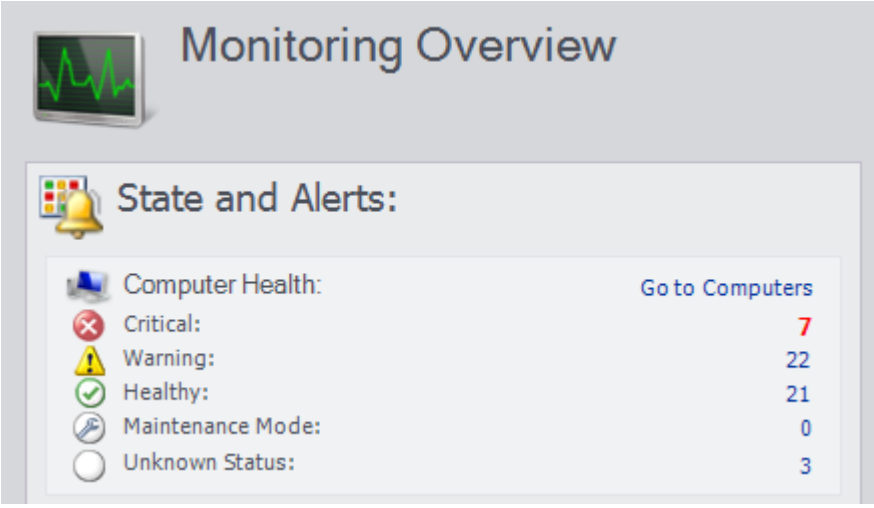
ACS Database on ASC-palvelun tietokanta, jossa säilytetään agenttien keräämät tietoturvalokit. Tietokanta on pakollinen ACS-palvelun toiminnassa. Tietokanta on SQL-pohjainen ja palvelimella tulee olla asennettuna SQL Server 2005 tai 2008. Tietokanta voi olla samalla hallintapalvelimella kuin ACS-palvelu, mutta on hyvinkin suositeltavaa pitää tietokanta erillisellä palvelimella ja määritellä siihen käyttöoikeudet vain SCOM-ympäristön ylläpitäjälle. ACS-palvelu koostuu näistä kaikista kolmesta ominaisuudesta. (Microsoft b)

5 HALLINTAKONSOLIN KÄYTTÖ JA SEN OSAT

Operations Console eli hallintakonsolin kautta nähdään kaikki SCOM-ympäristöön liittyvät tilanteet, asetukset ja konfiguraatiot. Hallintakonsoli sisältää erilaisia työtiloja (workspace). Näiden työtilojen takaa hoidellaan SCOM-ympäristöön liittyviä asioita. Hallintakonsolille on mahdollista asettaa käyttäjäoikeuksia. Käyttäjäoikeuksien rajauksella hallintakonsolin puolesta pystytään rajaamaan työtilojen käyttöä. Käyttäjätunnuksille annetut oikeudet määrittelevät sen mitkä työtilat näytetään. Esimerkiksi jos SCOM-ylläpitäjän roolia on hajautettu muutamalle henkilölle, on ehkä tarpeen asettaa joitain rajoituksia SCOM:n hallinnan suhteen. Hallintakonsolin käyttöliittymä on tuttua tyyliä Microsoftilta, perustuen samaan rajapintaan kuin Outlook 2007. Seuraavaksi käydään läpi mitä työtilat pitävät sisällään ja mitä niiden kautta on mahdollista tehdä.

5.1 Monitoring

Monitoring-työtila aukeaa oletusnäkymänä kun hallintakonsoli on avattu. Kaikilla SCOM-ympäristön käyttäjillä on pääsy monitoring-työtilaan. Monitoring-työtilan kautta on nähtävissä laajat ja yksityiskohtaiset tiedot kaikista valvontaan liittyvistä asioista. Päänäkymä monitoring-työtilassa näyttää suoraan pikayhteenvetona valvottavien tietokoneiden terveydentilan (kuva 8.). Vakaa terveydentila on ilmaistu (healthy) nimisenä pääikkunassa. Yksittäisen palvelimen terveydentila voi olla myös (warning) tyyppinen eli tarkoittaa sitä, että palvelin toimii, mutta siellä on jotain korjattavaa. Toinen mittari terveydentilalle on (Critical) joka on jo hieman ”vaarallisempi”. Critical terveydentilassa olevalle palvelimelle on mahdollisesti tapahtunut jotain toimintaa haittaavaa. Voidaan esimerkiksi ajatella tulostinpalvelinta jossa ”Print Spooler” palvelu lakkaa toimimista. Tämän palvelun toiminnan katkeaminen aiheuttaa tulostuskatkoksen käyttäjille. SCOM-ylläpitäjän on helppo huomata tällainen virhe tarkkaillessaan valvottavien kohteiden terveydentilailmaisimia.



Kuva 8. Monitoring-työtilassa oleva valvonnan pikanäkymä näyttää yhteenvedon, montako palvelinta on ja missä terveydentilassa ne ovat. Yhteenveto näyttää myös huoltotilassa olevat palvelimet ja tuntemattomassa tilassa olevat palvelimet.

5.1.1 Hälytysnäkymät

Monitoring-näkymä jakaa hälytykset kahteen luokkaan, jotka ovat Active Alerts ja Critical Alerts, eli aktiiviset ja kriittiset hälytykset. Näihin kahteen hälytysnäkymään hälytykset tulevat reaaliajassa, jos joku tietty hälytys toistuu useasti. Hälytyksien edelleen lähettäminen yleensä määritellään SCOM-järjestelmän ylläpitäjän sähköpostiin sekä myös mahdollisesti tekstiviestillä matkapuhelimeen. On helppo tehdä erilaisia kokeiluja valvottavaan palvelimeen liittyen ja samalla seurata hälytysten mahdollista ilmentymistä hallintakonsolin kautta. Hälytykset ovat tarkasti SCOM-järjestelmässä ylhäällä. Hälytysnäkymästä näkee kellon ja päivämäärän tarkkuudella hälytysten tiedot, sekä tietenkin itse hälytyksen lähteen ja aiheen. SCOM-järjestelmä oletusasetuksien mukaan lajittelee hälytysten tarkkuustilan. Uudet hälytykset näkyvät ”New” nimisenä. Korjatut ja itsestään ratkenneet ongelmat siirtyvät ”Closed” nimisiksi. SCOM:in oletusasetukset sulkevat hälytykset erikseen määritellyllä aikavälillä, jos hälytyksiä ei ratkaista.

Hälytysnäkymässä olevia hälytyksiä voi tarkastella hyvin yksityiskohtaisesti. Jokaisten hälytyksien yksityiskohtainen näkymä kertoo tarkat tiedot hälytyksen sisällöstä. Jos hälytys on todettu vahingossa aiheutetuksi tai aiheettomaksi, on se mahdollista sulkea hälytysnäkymässä. Valvottavien kohteiden terveydentilan objektit näkyvät

Healt Explorer-näkymässä. Health Explorer näyttää kohtaan valvottavien objektien tilan puumaisella rakenteella, jos jokin objekti saa hälytykset silloin. Health Explorer perii hälytyksen ylätasolle ja näyttää jonkin olevan vialla valvottavassa kohteessa.

5.1.2 Korjaavat toiminnot

Hälytyksiä tarkasteltaessa on mahdollista suorittaa erilaisia korjaavia toimintoja (Recovery Tasks). Hälytystä tarkastettaessa ohjelma ehdottaa ongelman korjaamiseksi korjaavaa toimintoa, joka on mahdollista suorittaa valvottavaan kohteeseen suoraan hallintakonsolin kautta. Tämän mahdollistamiseksi tulee olla määritelty Action Account toiminto, jolle annetaan oikeudet tehdä tarvittavia korjaustoimenpiteitä kohdekoneisiin. Valmiit korjausehdotukset eivät aina välttämättä ratkaise ongelmaa, mutta useimmiten niillä ongelma on korjattavissa.

Vika voi olla joskus syvemmällä ja silloin asiaa pitää lähteä ratkaisemaan jollain muulla tavalla. Korjaavia toimintoja ei ole tarjolla kaikille hälytyksille. Tietyille perustason hälytyksen korjaavia toimintoja löytyy valmiiksi SCOM ympäristöstä, mutta kaikenkattava se ei ole. Korjaavat toiminnot on myös mahdollista suorittaa automaattisesti. Valvonta-agentin action account on mahdollista konfiguroida halutessa reagoimaan hälytyksiin ennalta määritellyin korjaustoimenpitein. Kun vika on korjattu automatisoidusti tai manuaalisesti, hälytystila kytkeytyy tietyn ajanhetken jälkeen pois päältä. Hälytyksen terveydentila on mahdollista myös tarkastuttaa uudelleen käsiajolla heti korjaavan toimenpiteen suoritettua.

5.1.3 Palvelimien ja agenttien terveydentila

Monitoring-työtilassa on windows computers kansio, jonka sisältä löytyy näkymä valvottavien palvelimien ja niissä olevien agenttien terveydentilasta. Tämä näkymä on hyödyllinen tarkasteltaessa terveydentilaa palvelimien näkökulmasta. Näkymässä olevien palvelimien terveydentilat näkyvät samalla tavalla kuin yksittäiset hälytykset health, warning tai critical merkintänä. Tässä näkymässä on helppo tutkia yksilöllisesti mitä hälytyksiä valvonnan piirissä olevissa palvelimissa on päällä. Myös agentin terveydentila näkyy tässä ikkunassa. Agentin terveydentila on toimiessaan healt-

hy. Agentin terveydentilan indikaattori healhty muuttuu harmaalla merkityksi jos agentin toiminnassa on jotain vikaa.

Yleisin syy agentin toiminnan vikaantumiseen on palvelimen uudelleenkäynnistys ilman, että Maintenance Mode olisi laitettu päälle ennen uudelleenkäynnistystä. Tai sitten agenttia ei ole muistettu poistaa valvonnan piiristä palvelimen poistamisen yhteydessä. Valvonnan kannalta on erittäin tärkeää huomioida huoltotilan (Maintenance Mode) käyttäminen. Huoltotilaa käytetään jos tiedetään, että palvelin käynnistetään uudelleen, esimerkiksi jonkun asennuksien loppuun saattamiseksi tai vaikkapa jonkun vian korjaamiseksi. Jos hallintakonsolin kautta ei ole merkitty huoltotilaa päälle uudelleen käynnistettävälle palvelimelle, antaa agentti automaattisesti hälytyksen SCOM-järjestelmään kun palvelin sammutetaan. Tämä johtuu siitä että agentti vastaanottaa tietyin väliajoin sydämensykettä (hearbeat) kertoakseen, että palvelin on toiminnassa. Käyttämällä huoltotilaa vältytään turhilta hälytyksiltä. Huoltotilan minimi päälläoloaika on viisi minuuttia, mutta erikseen on määriteltävissä pidempikin aika huoltotilalle ja tämän jälkeen huoltotila kytkeytyy automaattisesti pois päältä.

5.2 Authoring

Authoring työtilassa on työkalu valvonnan hallintaan. Lyhykäisyydessään tässä työtilassa voidaan määritellä mitä valvotaan ja miten valvotaan. Kuka tahansa SCOM-operaattori näkee authoring työtilan omassa hallintakonsolissaan. Kaikki operaattorit pystyvät tässä työtilassa muokkaamaan ja luomaan valvontaan liittyviä hallintaobjekteja.

5.2.1 Management Pack Templates

Management Pack Templates valikko mahdollistaa luomaan erikseen kustomoituja valvontaan liittyviä objekteja. Asennusvelhon kautta luodaan malli näiden kustomoitujen objektien valvonnasta ja valvontasäännöistä. SCOM:in ensiasennus sisältää vakiojoukon tiettyjä valmiiksi kustomoituja valvontaobjekteja. Näitä valmiita objekteja voidaan käyttää perustana itse luoduille hallintaobjekteille.

Esiasennetut valvontaobjektit:

OLE DB Data Source sisältää tietokantaan valvottavan objektin. Tämän avulla on mahdollista valvoa yksittäisen tietokannan toimivuutta. Valvottaviin tietokantoihin on mahdollista asettaa erilaisia tietokantakyselyjä, joiden kautta voidaan valvoa tietokannassa tapahtuvia muutoksia.

Process Monitoring valvontaobjektin avulla voidaan tarkkailla jotain tiettyä prosessia ja sen toimintaa. Se voi olla vaikkapa jokin palvelimella toimiva sovellus. Tämän hallintaobjektin voidaan myös ehkäistä ei toivottujen prosessien käynnistymistä valvottavassa kohdekoneessa.

TCP Port ominaisuus mahdollistaa sovelluksen kuunnella jotain erikseen määriteltyä TCP-porttia. Tällä valvontaobjektilla voidaan valvoa TCP-portteja käyttäviä sovelluksia, kuten DNS, DHCP tai Web-sivua, jonka portti on tunnettu. Internetissä on saatavilla lista rekisteröidyistä ja tunnetuista TCP-porteista.

Unix/Linux Log työkalun avulla on mahdollista tuoda erilaisia haluttuja lokitietoja erikseen määritellystä Unix/Linux koneesta tai kokonaista ryhmästä Unix/Linux koneita.

Unix/Linux Service sovelluksen avulla voidaan valvoa Unix/Linux koneissa toimivia prosesseja ja toimintoja, sekä myös paikallisia prosesseja.

Windows Service avulla on mahdollista valvoa erilaisia Windows-pohjaisia instansseja. Erilaisia Windows-pohjaisia valvottavia palveluita voivat olla esimerkiksi CPU:n käyttöaste ja muistinkäyttö.

5.2.2 Distributed Applications

Hajautetut sovellukset ovat järjestelmiä, jotka vaativat toimiakseen vähintään kahden tai useamman koneen. Hajautetut sovellukset toimivat client-server tyyppisesti. Hajautetut sovellukset eivät toimi yksittäisellä palvelimella, vaan ne koostuvat kom-

ponenteista, joita pyöritetään useissa eri palvelimissa. Hajautettujen sovelluksien valvontapaketilla on mahdollista valvoa yksittäisen hajautetun sovelluksen eri komponenttien toimivuuden tasoja. Hajautettu sovellus voi olla vaikka jokin toiminnanohjausjärjestelmä, joka toimii hajautetusti kahdessa eri toimipisteessä, mutta on silti molempien toimipisteiden käyttäjille samanlainen. Kytkin ja reitittimet välittävät tietoa käyttäjille ja käyttäjät välittävät tiedon web-palvelimella ajettavaan ohjelmaan ja ohjelma puolestaan taas välittää tiedot eri palvelimessa sijaitsevaan tietokantaan. Tämä on yksi esimerkki hajautetusta sovelluksesta.

5.2.3 Groups

Groups valikosta voidaan luoda kokoelma valvottavista kohteista ja kohdistaa johonkin olemassa olevaan valvontaryhmään tai itse luotuun valvontaryhmään. Näiden valvontaryhmien avulla helppo on saada valvontaan liittyviä tietoja erikseen määritellyistä valvontakohteista. Esimerkkejä muutamista valmiista valvontaryhmistä: All Windows Computer, eli tämän valvontaryhmän kautta on nopeasti nähtävillä kaikkien windows tietokoneiden valvonnan tila. SQL Computers on ryhmä, jonka sisältä löytyy kaikki tietokoneet, jotka sisältävät SQL tietokantoja. nWorks VMware Datastores: tämän valvontaryhmän avulla saadaan nähtyä kaikki virtuaalialustan massamuistin valvontaan liittyvät tilanteet.

5.2.4 Management Pack Objects

Management Pack (MP) on SCOM:in hallintapaketti. Se on ikään kuin tietoämpäri, joka pitää sisällään valvontaan liittyviä objekteja. MP:t ohjailevat agenttien toimintaa. Jokainen MP pitää sisällään tietyt peruselementit. Nämä peruselementit ovat osa MP:n toimivuutta. Peruselementtien pohjalta on mahdollista luoda itse muutoksia hallintapaketteihin. MP:n peruselementit ovat:

Attributes ovat MP:ssä olevia ominaisuuksia, joiden avulla määritellään mitä tietoja valvottavista kohteista halutaan saada ulos. Attribuutteja voivat olla esimerkiksi laitteen sarjanumero ja levytila. Omia attribuutteja on myös mahdollista tehdä, jos halutaan valvonnan näyttävän tietoja jostain tietystä objektista.

Monitors ovat monitoreja jotka huolehtivat agentin tiedonkulusta. Monitorit määrittelevät valvottavien objektien terveydentilan. Jokainen monitori pitää sisällään tietolähteitä. Tietolähteitä ovat: event logs, performance data, scripts. Event logit pitävät sisällään tapahtumatietoja, esimerkiksi windows palvelimen kirjautumistapahtumat. Performance data on suorituskykyä mittaava monitori. Scriptit ovat eräänlaisia koodinpätkiä, joiden avulla monitorit keräävät haluttua tietoa.

Object Discoveries näkymä näyttää kakki objektit joita löytyy valvontaan asetetuista palvelimista. Eli tässä näkymässä näkyy kaikki MP:n määrittelemät objektit, jotka agentti on löytänyt kohdekoneista. Object Discoveries näkymästä on helppo tarkastaa kaikki omasta ympäristöstä löytyvät valvottavat objektit.

Overrides ovat valvontasääntöjen poikkeuksia. Poikkeuksia voidaan tehdä attribuutteihin ja valvonnasta löytyneihin objekteihin. Esimerkiksi jos jokin valvottavan palvelimen muistin tiedetään käyvän korkealla aina silloin tällöin, on siitä mahdollista tehdä erikseen määritelty poikkeus, ettei joka kerta tulisi hälytystä kun muistin käyttö ylittää tietyn vakio raja-arvon.

Rules ovat eräänlaisia sääntöjä, joiden avulla agentti nostaa hälytyksiä tai kerää tietoja analysoidakseen erilaisia raportteja. Jokainen sääntö pitää sisällään samalla tavalla tietolähteitä kuin monitoritkin.

Service Level Tracking on palvelutason tarkkailuun liittyvä ominaisuus. Sen avulla voidaan seurata esimerkiksi tärkeiden palvelujen käyttöastetta. Sähköposti on tyypillinen tärkeä palvelu jokaisessa yrityksessä. Sähköpostin palvelutasoa on mahdollista tarkkailla luomalla sen sovelluksesta oma service level-objekti, joka seuraa sähköpostipalvelin toimivuutta ja siitä on mahdollista ajaa toimivuus raportteja esimerkiksi päivä, kuukausi tai vuositasolla. Tällä ominaisuudella voi myös haluttaessa vertailla kaikkien valvonnassa olevien palvelimien käyttöastetta halutuin raportein.

Task ovat tehtäviä, joita agentti voi suorittaa valvottavissa kohteissa. Kun agentti saa hälytyksen, esimerkiksi jonkun tärkeän Windows-palvelun pysähtymisestä, on mahdollista suorittaa korjaustoimenpide suoraan agentin päästä. MP:t pitää sisällään tiet-

tyjä valmiita ehdotettuja tehtäviä, joita on mahdollista käynnistellä hallintakonsolista käsin.

Views ovat erilaisia näkymiä jonka avulla hallintakonsoli näyttää valvottavat objektit ja kerätyn datatiedon valvonnasta. Valvottavista kohteista on saatavilla näkymiä eri kategorioiden mukaisesti. Oletusnäkymiä ovat: hälytysnäkymä, konekohtainen näkymä, ja esimerkiksi suoritettavien tehtävien näkymä. Erilaisia näkymiä on myös mahdollista rakentaa itse.

5.3 Reporting

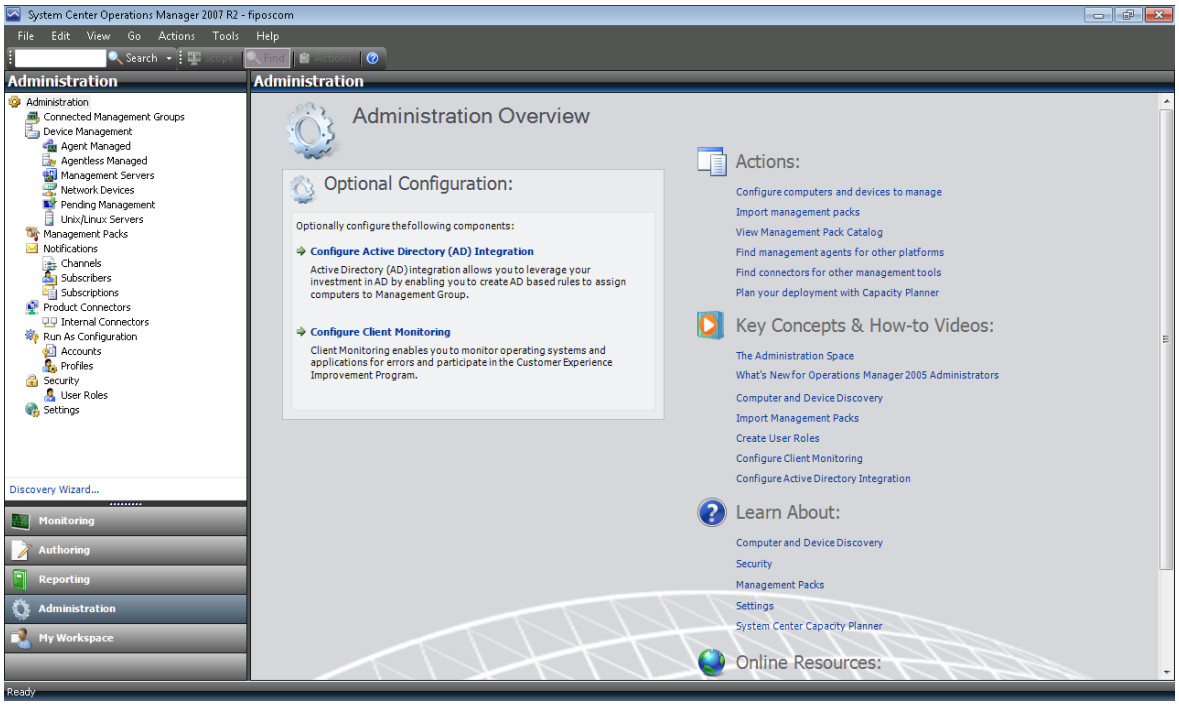
Reporting työtilassa voidaan tuottaa valvontaan liittyviä raportteja. Reporting työtila ei näy hallintakonsolissa ennen kuin kaikki raportointipalveluun liittyvät komponentit ovat asennettuna. Kun reporting työtila on näkyvissä, voidaan sen kautta suorittaa raportteja esimerkiksi jonkin tietyn valvontaryhmän osalta. Esimerkkinä kaikkien Windows Xp-tietokoneiden levytila resurssien tiedot yhtenä raporttina. Reporting palvelu sisältää oletuksena valmiita raporttipohjia, joita voi hyödyntää yrityksen valvontaraporttien tulostamiseksi.

Reporting palvelulla voidaan myös rakentaa yritykselle räätälöityjä valmiita raporttipohjia, jotta haluttuja raportteja olisi helppo tuottaa. Esimerkki räätälöidystä raportista on virtuaalisointi alustan datastoren levynkäyttöaste raportti. Kyseinen raportti tuo tiedot virtuaalialustan levyntilan käyttöasteesta. Koska raportointi palvelu perustuu SQL:ään, on raporttipohjia mahdollista tehdä myös Microsoftin Visual Studio ohjelmalla. Reporting työtila sisältää myös työkalun, jonka avulla voi tehdä räätälöityjä raportteja. Raportteja on mahdollista suorittaa myös ajastettuna. Esimerkiksi Tietoturvalokeista voidaan halutessa tehdä ajastettu raportti kerran kuukaudessa ja osoittaa raportti haluttuun hakemistoon. Raportteja voidaan ajaa myös halutessa SQL:n päällä toimivalla webbisovelluksella. Etuja webin päällä toimivaan raporttipalveluun on käytettävyys mistä tahansa työasemasta ilman, että siihen olisi asennettu hallintakonsoli.

5.4 Administration

Administration työtilan (kuva 9) kautta hallitaan koko SCOM-ympäristöön liittyviä konfiguraatioita. SCOM-ympäristön asennuksen yhteydessä luodaan ylläpitotunnukset Operations Manager administrators-ryhmään. Tähän ryhmään kuuluvat käyttäjät näkevät administration työtilan hallintakonsolissa. SCOM-ympäristön ylläpitäjällä on täydet oikeudet hallita administration työtilan kautta koko ympäristön asetuksia. Administration-työtilassa hoidetaan kaikki valvontapalvelimiin liittyvät konfiguraatiot, sekä agenttien asennukset ja niiden toiminnan ylläpito. Myös management packetit (MP) asennetaan ja konfiguroidaan tässä työtilassa. MP:t ovat yksinkertaisuudessaan ikään kuin säilytysämpäreitä, jotka ohjaavat agenttien toimintaa, mitä valvotaan miten valvotaan.

Administration-tietoruutu pitää sisällään yleisnäkymän hallintaryhmien yksityiskohtaisista asetuksista. Sen kautta nähdään myös toiminnot, joita voidaan suorittaa hallintaryhmissä ja myös aputoiminnot, joita voidaan suorittaa hallintaryhmissä. Uutta SCOM-ympäristöä käyttöönotettaessa administration-paneelissa on asennusvelho, jonka avulla pystytään tehdä valvonta-agenttien asennukset.



Kuva 9. Kuvaruutukaappaus hallintakonsolin Administration työtilan päänäkymästä.

5.4.1 Connected Management Groups

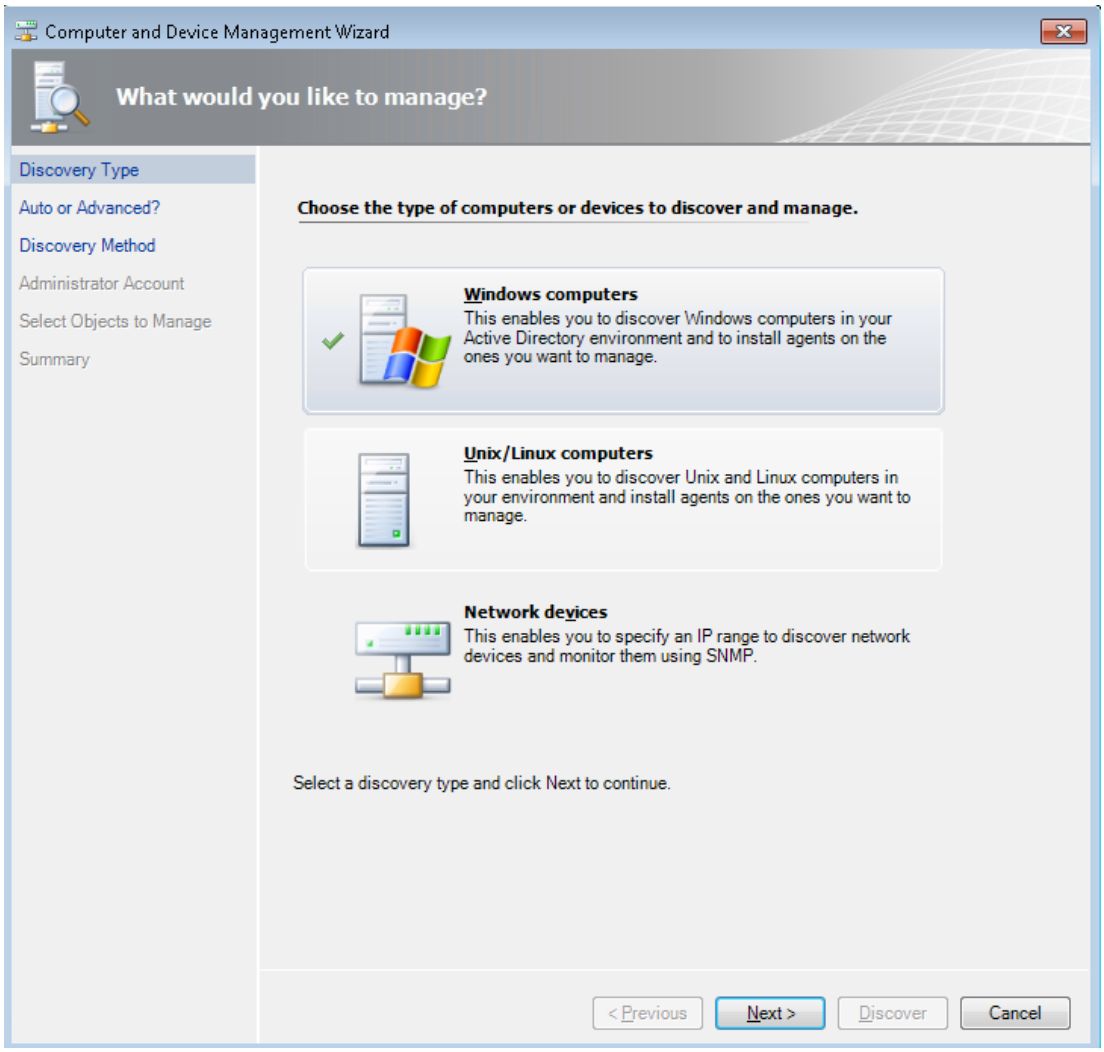
Hallintaryhmät ovat oleellinen osa hallintaryhmä hierarkiassa. Tässä näkymässä näkyvät määritellyt hallintaryhmät, mikäli SCOM-ympäristön asennus on niin laaja, että sitä on hajautettu. Hallintaryhmät voidaan konfiguroida toimimaan yhteistyössä hierarkisella tasolla. Hallintaryhmien yhteistyö mahdollistaa SCOM-ylläpitäjien ja operaattoreiden tutkia ja hallita hälytyksiä mistä tahansa valvontaryhmästä. Hallintaryhmiä ei yleensä luoda jos SCOM-ympäristön vastuu on vain yhdellä henkilöllä.

5.4.2 Device Management osat

Device Management valikko koostuu erilaisista tietoruuduista, jotka näyttävät agenttien olemassaolon ja niiden toimivuuden. Device Management valikon alta kohdassa **Agent Managed** nähdään agenttien terveydentila ja mm. valvottavien kohteiden IP-osoitteet. Agentittomat valvontatapaukset näkyvät **Agentless Managed** valikossa. Agentittomia valvontakohteita voivat esimerkiksi olla verkon aktiivilaitteet kuten kytkimet ja reitittimet. Tietovalikko **Unix/Linux Servers** lajittelee erikseen niiden päällä olevat valvontakohteet mikäli niitä on. Tärkein tietoruutu agentin asennuksen kannalta on **Pending Management** tietoruutu, joka näyttää parhaillaan käynnissäolevat tehtävä, esimerkiksi agenttia asentaessa.

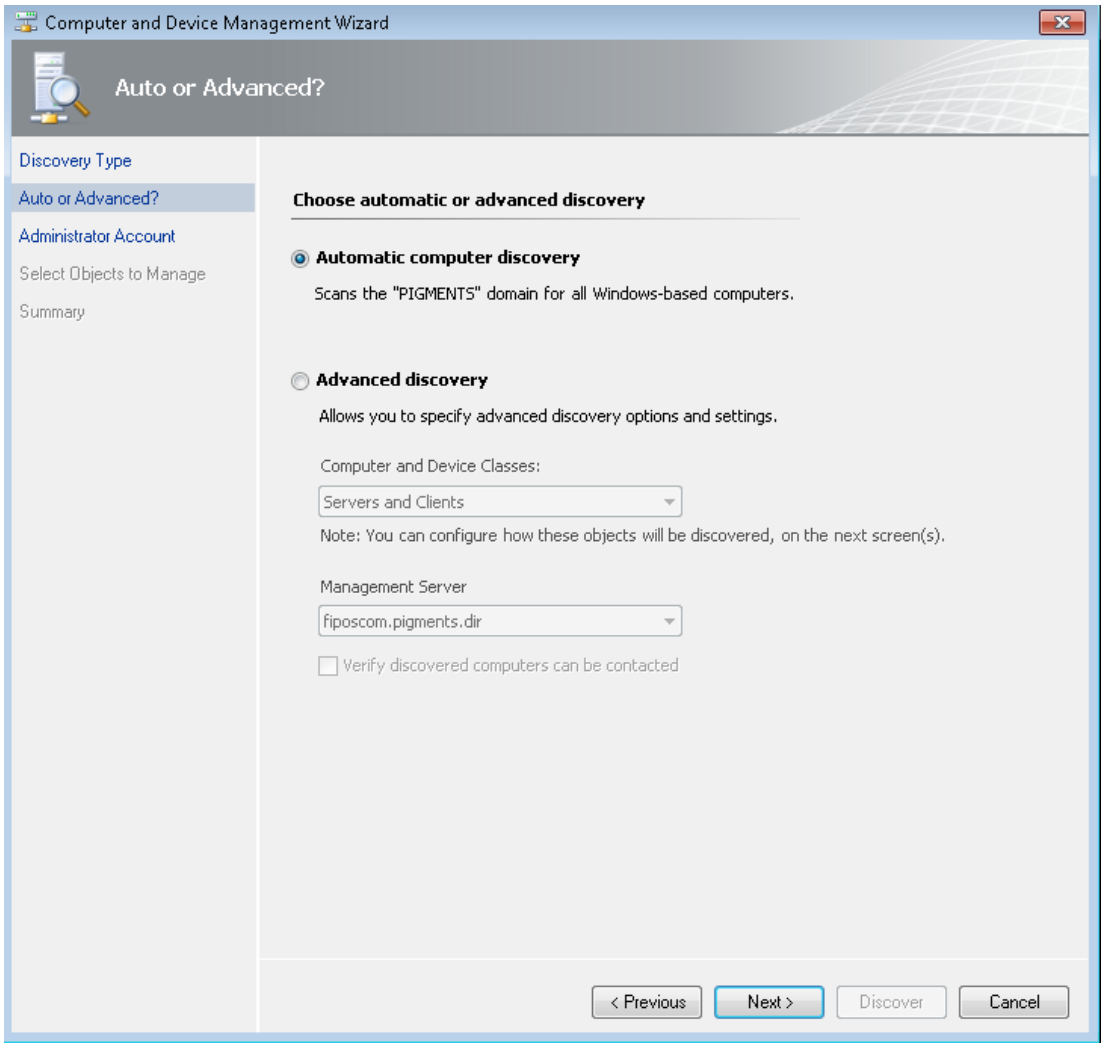
5.4.3 Agentin asennus

Valvonta-agentti voidaan asentaa joko ohjatulla Discovery Wizard (kuva10) toiminnolla tai vaihtoehtoisesti manuaalisella asennuksella itse valvottavasta kohteesta käsin. Discovery Wizard toiminnon avulla agentti voidaan asentaa suoraan hallintakonsolista käsin. Discovery Wizard velho tekee käynnistyessään kyselyn Active Directory palvelimelle, ja saa tätä kautta tietoonsa kaikki AD:ssa olevat työasemat ja palvelimet. Ennen kuin voidaan varmistua siitä, että Discovery Wizard löytää kaikki AD:ssa olevat koneet, on varmistettava, että palomuuri ei ole estänyt kyselyyn tarvittavia portteja. Agentti voidaan myös asentaa samalla asennuskerralla useaan eri kohteeseen Discovery Wizard toimintoa käyttäen.



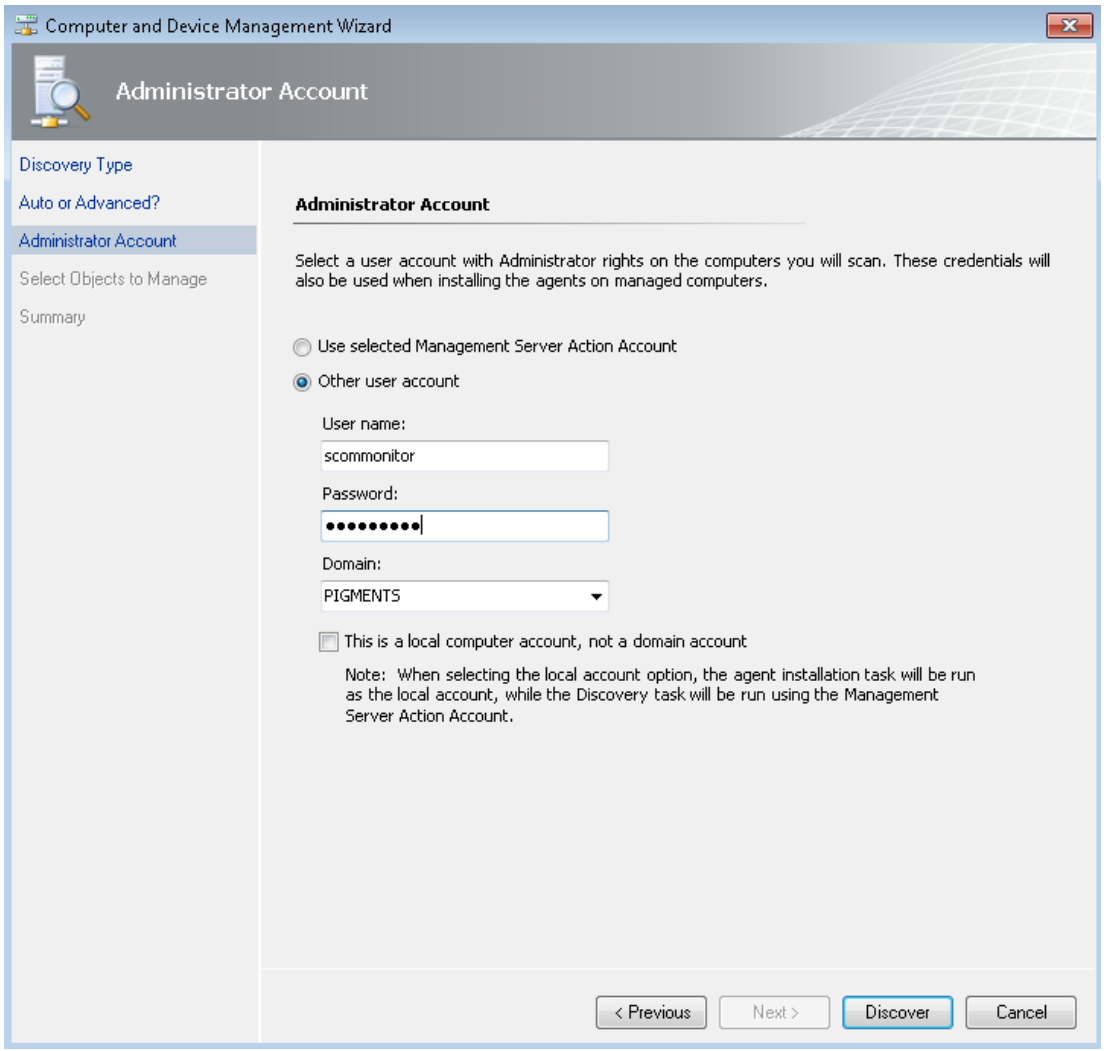
Kuva 10. Kuvaruutukaappaus agentin asennusvaiheesta 1/6

Aluksi valitaan mitä laitteita halutaan etsiä ja laittaa valvonnan piirin. Oletuksena asennustoiminto hakee AD:n Windows-tietokoneet ja näyttää niistä listan. Tämän asennustoiminnon avulla voidaan myös etsiä Unix/Linux tietokoneita tai verkkolaitteita. Jokaiseen näistä kohteesta voidaan asentaa valvonta tämän toiminnon avulla. Agentin asentaminen tällä ohjatulla toiminnolla on nopeaa ja tehokasta. Tässä kohtaa asennetaan agentti win7 testikoneeseen. Valitaan kohta Windows Computers ja siirrytään next-komennolla eteenpäin.



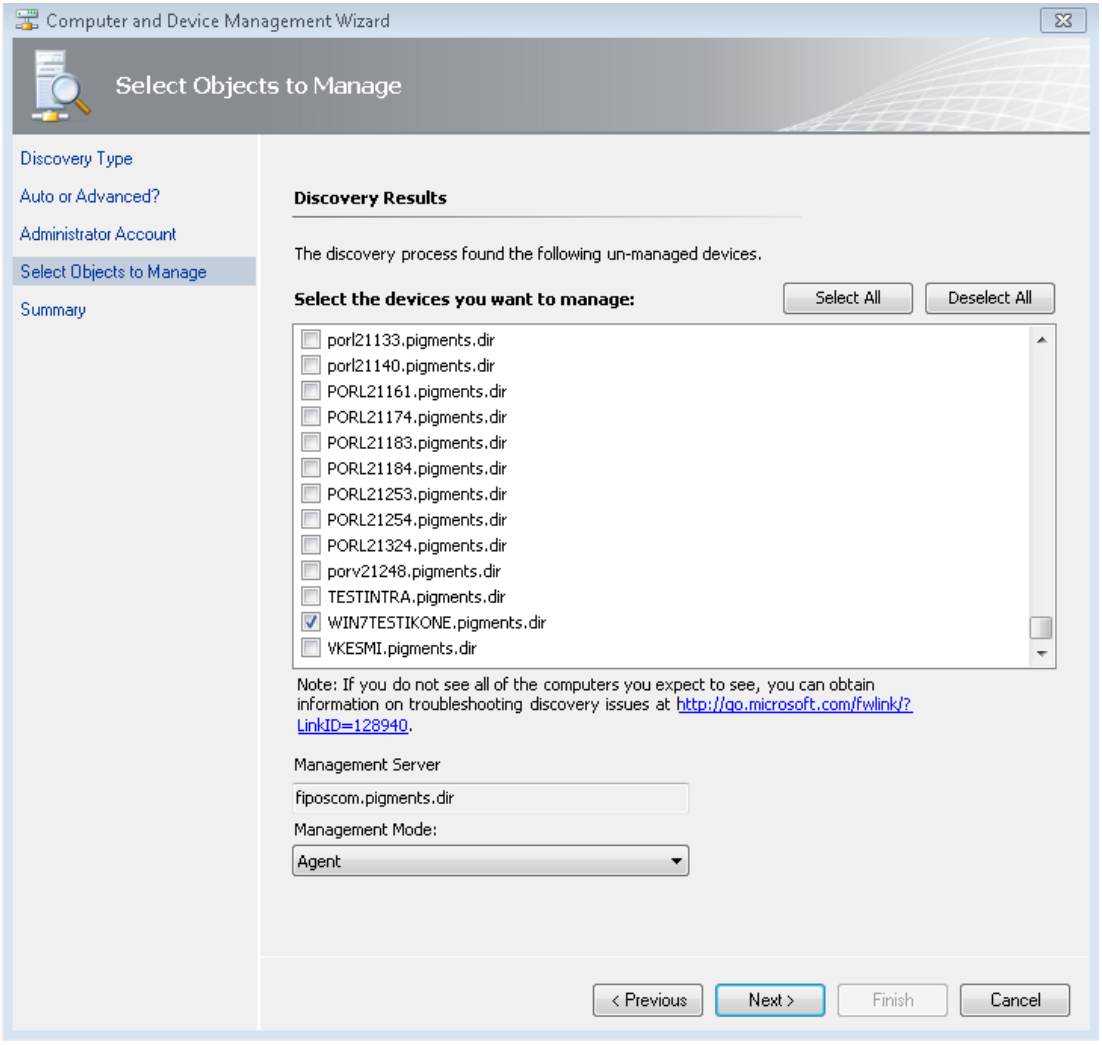
Kuva 11. Agentin asennusvaihe 2/6

Seuraavassa ruudussa on mahdollista valita Automatic computer discovery tai Advanced discovery. Ensimmäinen valinta (Kuva 11) tutkii automaattisesti kaikki yrityksen toimialueessa (Active Directory) olevat windows tietokoneet ja näyttää niistä listauksen niistä koneista, joista ei valvonta-agenttia vielä löydy. Toista vaihtoehtoa käytetään silloin, kun halutaan asentaa agentti jonnekin toiselle toimialueelle tai johonkin jo valmiiksi tiedettävissä olevaan kohteeseen. Kumpikin asennustapa on yhtä nopea. Molemmilla asennustavoilla on mahdollista asentaa useita agentti asennuksia samalla kertaa. Tässä esimerkissä käytetään tapaa Automatic computer discovery ja valitaan next painikkeellä eteenpäin.



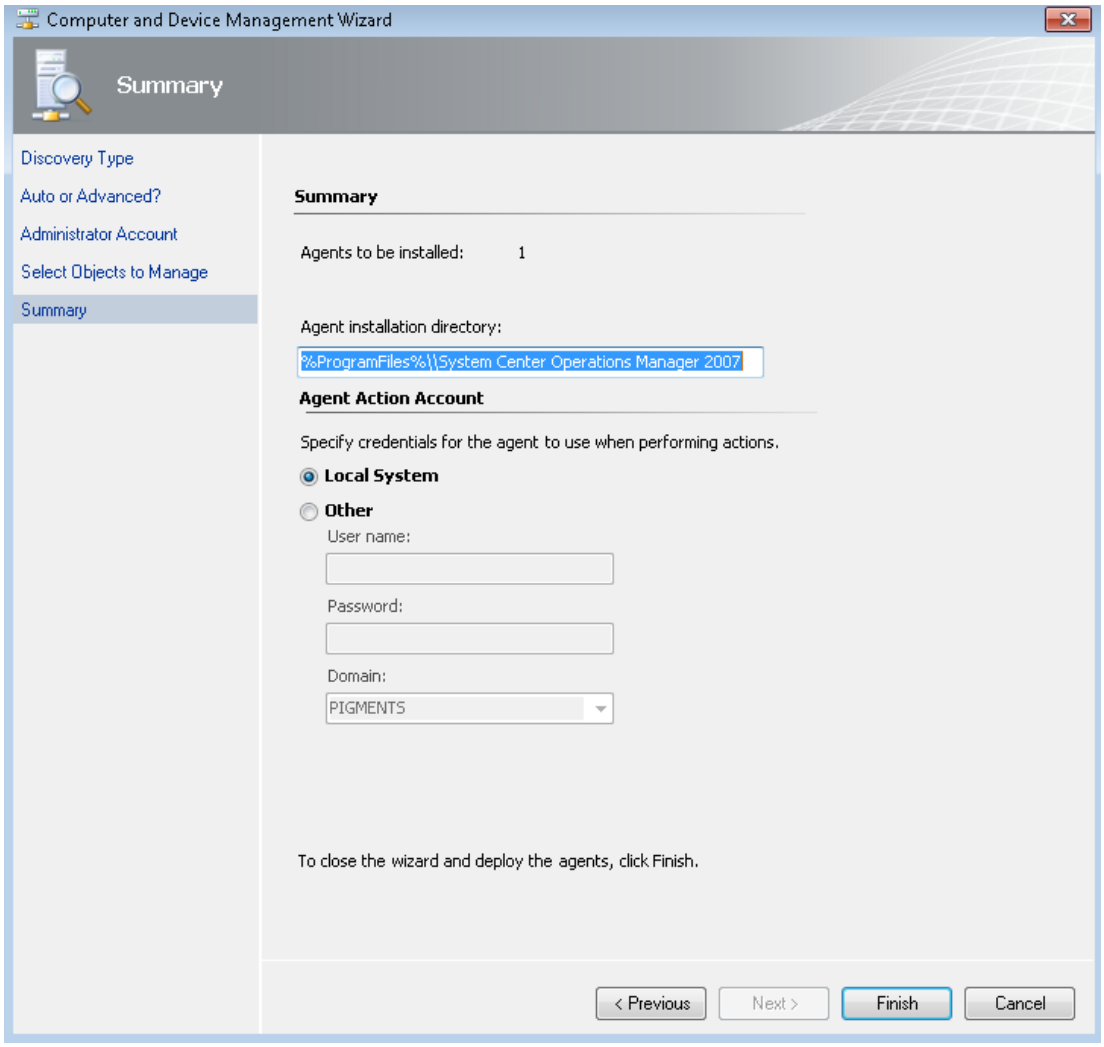
Kuva 12. Agentin asennusvaihe 3/6

Ennen kuin ohjattu toiminto alkaa (Kuva 12) hakea tietokoneista toimialueesta, on tietokoneiden etsimistä varten annettava ohjelmalle tunnus, jossa on järjestelmänvalvojan oikeudet. Tässä esimerkissä asennukseen käytetään erikseen luotua scommonitor nimistä toimialueen tunnusta, jolla on järjestelmänvalvojan oikeudet. Tämä tunnus sisältää riittävät oikeudet etsimään toimialueesta löytyvät valvomattomat tietokoneet ja mahdollistaa siten agentin asennuksen. Tässä kohtaa on myös mahdollista käyttää ns. Action Account tunnusta, joka on teknisesti sama kuin esimerkissä käytetty asennustunnus, mutta eroaa siinä määrin, että sen avulla agentilla olisi oikeuksia tehdä korjaavia toimenpiteitä valvonkohteessa. Tässä kohtaa käytetään pelkkää asennustunnusta ja valitaan other user account, syötetään tunnus ja valitaan discover-painikkeella haku käyntiin.



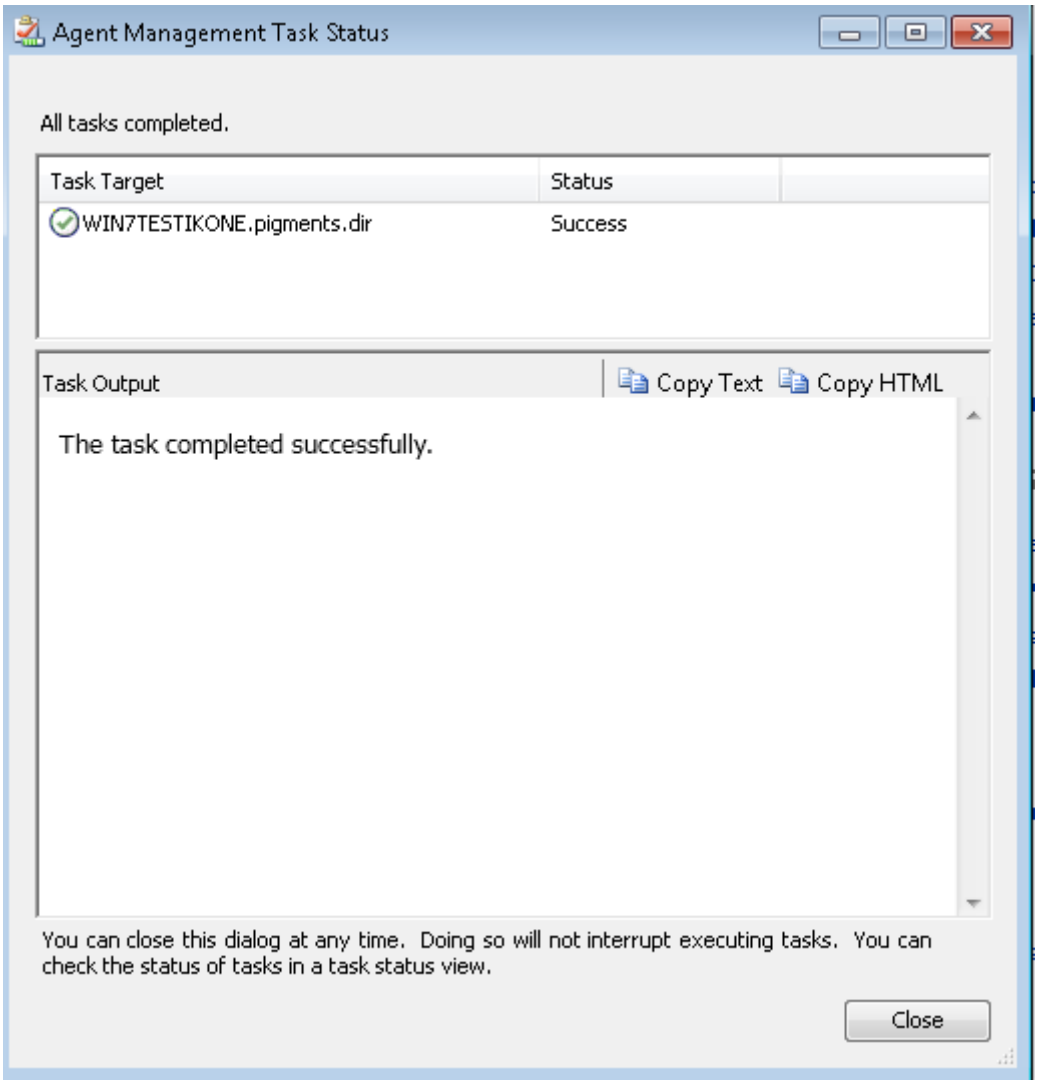
Kuva 13. Agentin asennusvaihe 4/6

Haku kestää hetken aikaa noin kahdesta viiteen minuuttiin. Tämän jälkeen haku (Kuva 13) antaa kuvassa näkyvän listauksen vapaista tietokoneista, joihin ei vielä ole valvontaa asetettu. Valitaan haluttu kohde, tässä esimerkissä WIN7Testikone, ja siirrytään next painikkeella eteenpäin. Mikäli valvottava kohde on vanha laite, jota ei haluta kuormittaa syystä tai toisesta agentin asennuksella, voidaan valitan kohdasta management mode vaihtoehto agentless mode. Agentitonta valvontaa voidaan käyttää myös pienissä yrityksissä. Agentiton valvonta vähentää verkkoliikennettä ja eikä se vaadi ohjelmallista asennusta valvottavaan kohteeseen. Tässä esimerkissä asennetaan agentti normaaliin tapaan valvottavaan kohteeseen ja valitaan next-painikkeella eteenpäin.



Kuva 14. Agentin asennusvaihe 5/6

Ohjattu asennustoiminto (Kuva 14) kysyy vielä valvottavan kohteen valitsemisen jälkeen tunnuksia, joilla agentti voi tehdä korjaavia toimenpiteitä valvontakohteessa. Jos aikaisemmassa vaiheessa olisi käytetty asennustunnuksen sijasta Action Account tunnusta, tätä ikkunaa ei tässä kohtaa asennuksessa tulisi esiin. Nyt kun agentin asennus on tehty asennustunnuksilla, on agentille vähintään annettava paikallisen järjestelmänvalvojan oikeudet korjaavia toimintoja varten. Valitaan kohta Local System ja valitaan finish. Tämän jälkeen asennuksen viimeinen vaihe tulee esiin, josta voidaan seurata asennuksen etenemistä. Asennusvaiheen viimeisessä ikkunassa lukee kunkin valvottavan kohteen perässä Started kun asennus on vielä kesken. Agentin asennusten tultua valmiiksi jokaisen kohteen perässä lukee Success. Asennusta ilmaisevan ikkunan voi sulkea halutessaan, sillä asennus jatkuu siitä huolimatta taustalla. Asennuksessa voi tulla virhe, jos asennusvaiheen lopussa on kirjoitettu Action Account tunnuksen salasana on väärin.



Kuva 15. Agentin asennusvaihe 6/6

Kuva agentin asennuksen viimeisestä vaiheesta (Kuva 15), kuvasta nähdään, että agentin asennus kohteeseen WIN7Testikone on onnistuneesti suoritettu. Tämän jälkeen kyseessä oleva valvottava kohde näkyy Agent Managed välilehdellä Healthy merkinnällä varustettuna. Agentti on mahdollista poistaa kahdella eri tapaa. Agent Managed välilehdellä valitaan valvonnasta poistettavaksi haluttu kohde. Klikattaessa poistettavaa kohdetta hiiren oikealla näppäimellä avautuu pieni valikko, josta löytää kaksi termiä, Uninstall ja Delete. Ensimmäinen poistaa agentin valvottavasta kohteesta ja jälkimmäinen taas tuhoaa tiedon valvonnan piiristä. Haluttaessa poistaa agentti on suoritettava molemmat poisto-toimenpiteet edellä mainitussa järjestyksessä. Jos agentin automaattiasennus ei suostu menemään lävitse, silloin on mahdollista asentaa agentti käsiajona. Manuaalinen asennus suoritetaan OpsMgr mukana tulleelta

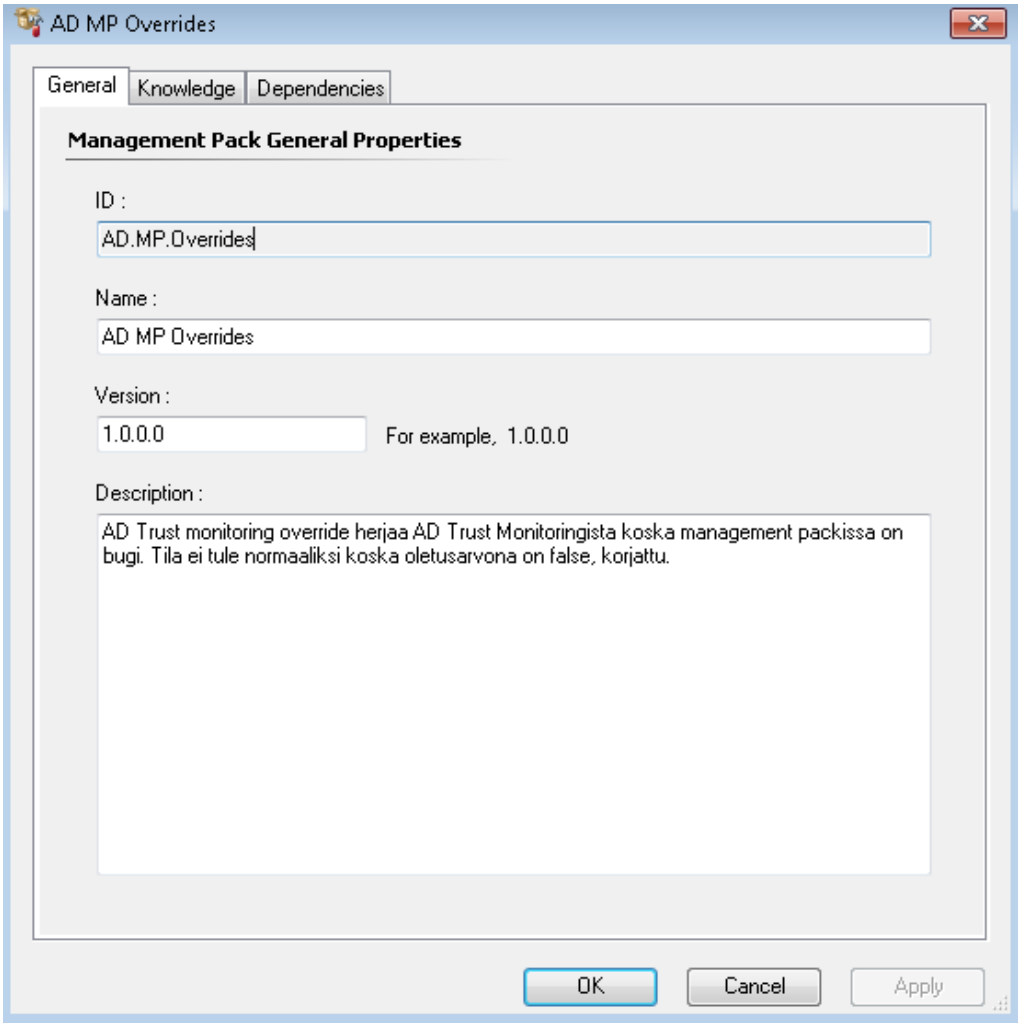
medialta valvottavasssa kohteessa. Asennustapa on samankaltainen kuin ohjelman asennus.

5.4.4 Management Pakettien asennus ja hyödyntäminen

Hallintakonsolin osassa Management Packs voidaan luoda omia MP:itä ja tarkastella mitä MP:itä on asennettuina. SCOM-vakioasennus pitää sisällään suuren määrän Microsoftin tarjoamia MP:itä. Jokaisen MP:n kohdalla listassa näkyy tarkka kuvaus siitä, mikä MP on kyseessä ja mikä on sen versio. MP:n nimestä pystyy päättelemään mitä se voisi sisältää. Esimerkiksi Microsoft Audit Collection Services MP sisältää joukon erilaisia määrityksiä auditointitietojen valvonta-asioihin liittyen. MP voi olla myös sinetöity (sealed), joka tarkoittaa, että MP on digitaalisesti allekirjoitettu ja suojattu. Sinetöityyn MP:hen ei voida tallentaa muutoksia päälle. Koska kaikki MP:t ovat tuotesidonnaisia, eli liittyvät johonkin tuotteeseen, esimerkiksi HP Proliant Servers MP on HP:n palvelimien valvontaan liittyvä hallintapaketti. Koska jokaisesta MP:sta on oma versionumero, niitä on helppo ylläpitää. MP:itä kannattaa väliajoin päivittää, koska uudemmissa versioissa on aina jotain parannuksia. Microsoftilta löytyy MP:itä lähes jokaista ohjelmaa varten. Voidaksemme valvoa jotain tiettyä systeemiä tarvitaan aina agentti ja MP, joka määrittelee mitä agentti valvoo ja kuinka se tapahtuu.

Itse asennetut ja tehdyt MP:t tallentuvat SCOM:in operatiiviseen tietokantaan. MP:itä voi hakea netistä hakusanoilla Management Pack ja tuotenimi. Esimerkiksi nworks VMware MP, joka on virtuaalialustoihin liittyvä kolmannen osapuolen hallintapaketti. Lähes jokainen käyttöympäristö pääsee liikkeelle valmiiksi olevilla MP:illä, mutta haluttaessa laajentaa valvontaa kaikkiin laitteisiin tarvitaan kolmannen osapuolen MP:itä ja itse tehtyjä ja muokattuja MP:itä. MP:t ovat msi-tiedostotunnisteella olevia tiedostoja. Niitä ei voi suoraan latauksen jälkeen asentaa vaan ne pitää ensin purkaa ja hallintakonsolin kautta lisätä järjestelmään komennolla Import Management Packs. Tällä komennolla voidaan tuoda jo valmiiksi tietokoneelle ladattu MP tai avata suoraan hallintakonsolin kautta web-katalogi, joka ohjaa itsensä Microsoftin sivuille ja tarjoaa sitä kautta erilaisia MP:itä ladattaviksi. Kolmansien osapuolien valmistamia MP:itä ei välttämättä löydy valmiista web-katalogista.

Asennettaessa uusia MP:itä on luettava tarkasi MP:ihin liittyvät dokumentit. Osa MP:istä ovat riippuvaisia toisista MP:istä. Tämä voi aiheuttaa ongelmia uutta MP:tä käyttöönotettaessa, jos dokumenttia ei ole luettu ja MP tarvitsee jonkun MP:n toimiakseen. Olemassa olevista MP:itä voi tarkastella yksityiskohtaisesti. Yksityiskohtaisemmassa tarkastelussa näkyy onko MP riippuvainen jostain toisesta MP:stä. MP:itä voi myös halutessaan poistaa SCOM järjestelmässä, mutta siinä kohtaan kannattaa olla äärimmäisen tarkka. Jokaisen valvonnan piirissä on mukana juuri tietty MP. Jos valvonnan piirissä olevan MP:n poistaa ilman, että valvottavaa systeemiä ei ole poistettu ensin, valvonnan piiristä voi saada sekaannuksen aikaan SCOM-järjestelmässä. MP:itä kannattaa olla mieluummin liikaa kuin liian vähän. MP:den tarkoitus on helpottaa valvontaa ja hallintaa. Itse luodut ja muokatut MP:t (Kuva 16) on myös mahdollista sinetöidä. Kun omaa MP:tä luo, sille pitää antaa oma ID numero, nimi ja versionumero sekä tarkempi kuvaus.



Kuva 16. Itse luotu AD MP Overrides hallintapaketti.

AD MP Overrides on Active Directory hallintapaketille itseluotu MP, joka sisältää poikkeussäännön. Alkuperäisenä ongelmana oli Active Directory hallintapaketissa oleva bugi, eli virhe, joka toistui aina ongelmallisesti. Vika ilmeni terveydentilailmaisimessa Health Explorer näkymässä. Kun valvottavan koneen terveys oli kunnossa, jäi järjestelmä silti ilmoittamaan sen olevan epäkunnossa. AD Trust monitoring valvoo AD-metsien välistä luottamusta. Jos metsien välinen luottamus ei ole kunnossa, se antaa hälytyksen ja jättää valvottaman kohteen tilan virheelliseksi. Kun AD-metsien välinen luottamus on todennettu onnistuneesti, valvottava kone on takaisin healthy-tilassa terveenä.

AD Trust Monitoring sisälsi oletuksena negatiivisen arvon kohdassa LogSuccessEvent joka tarkoittaa onnistunutta kirjautumista toimialueiden välillä. Pienellä poikkeussäännöllä oma MP saatiin korjattua tämä vaivaa vika. MP:ita luodessa SCOM ohjelma tarjoaa aina oletustallennuspaikkana kohdan Default Management Pack, joka on MP:iden oletustallennuspaikka. Kyseiseen paikkaan ei kuitenkaan ole järkevää luoda ja tallentaa MP:itä, koska sieltä olisi silloin vaikea erotella niitä. Suositellumpi tapa on tehdä jokaisesta MP:stä oma itsensä ja antaa siitä tarkat tiedot.

5.4.5 Notifications

Notifications-tietoruudun kautta määritellään hälytyksien ilmoituksien jakelu. Hälytykset voidaan ajastetusti ohjata esimerkiksi tietohallinnon yhteiseen sähköpostilaatikkoon, jossa ne ovat kaikkien tukihenkilöiden luettavissa. On myös mahdollista määritellä hälytykset lähetettyinä sähköpostilla erikseen määritellyille henkilöille vaikka SCOM-järjestelmän ylläpitäjälle. Ilmoituksien lähettämiseksi sähköpostitse on ohjelmalle annettava sähköpostipalvelimen nimi ja osoite, johon ilmoitukset lähtevät sekä niiden lähetysaika. Sähköpostissa olevan hälytysilmoituksen aihe on mahdollista rakentaa näkymään haluavansa tavalla. Notifications-asetuksista voidaan määritellä erilaisia määrityksiä hälytysilmoituksiin. Tyypillinen ryhmittely on kriittiset hälytykset ja tavalliset hälytykset. Näiden kahden väliltä on myös täysin itse konfiguroitavissa tietyt asia,t jotka haluaa hälytysilmoituksissa nähdä.

5.4.6 Product Connectors

Product Connectors tietoruutu näyttää SCOM-järjestelmän sisäiset yhteydet (Internal Connections). Tällä tarkoitetaan sitä, että jos valvonnan piirissä on laite, joka ei ole Windows-pohjainen tai se ei pysty suoraan keskustelemaan SCOM-järjestelmän kanssa on sen välille mahdollista luoda sisäinen tiedonkerääjä, joka synkronoi valvontakohteesta tiedot SCOM:iin. HP Custom Data Manager Connector on esimerkiksi yksi sellainen. Se kerää Hewlett Packard palvelimilta valvontaan liittyvää tietoa oman hallintapakettinsa avulla. Tämän jälkeen HP Custom Data Manager Connector tuo valvontatiedot SCOM järjestelmään nähtäväksi.

5.4.7 Run As Configuration and Profiles

Tämän tietoruudun kautta hallinnoidaan SCOM järjestelmään liittyviä käyttäjätilejä, joita käytetään agentin asennuksissa ja MP:n komponenteissa. Käyttäjätilejä hyödynnetään nostamaan oikeuksia tietyillä toimintatasoilla. Nämä jaetaan kahteen ryhmään Run As Accounts ja Run As Profiles. Ensimmäinen sisältää käyttäjätilit, joita käytetään hallintaryhmässä, jotta päästään tiettyihin hallintaryhmän komponentteihin. Näitä käyttäjätilejä käytetään erilaisten tehtävien suorittamiseksi, kun agentin oma action account tai käyttäjätili ei omaa riittävästi oikeuksia suorittamaan tiettyjä tehtäviä. Jälkimmäinen Run as Profiles-ryhmän kautta voidaan määritellä tarkemmin näitä erilaisia käyttäjätilejä ja niiden sisältämiä oikeuksia.

5.4.8 Security and Settings

Security-tietoruutu jaottelee SCOM-järjestelmän käyttäjäroolit. SCOM-ympäristön ollessa hajautettu on järkevää ajatella käyttäjäroolien hajauttamista. User Roles asetuksien kautta voidaan hallinnoida käyttäjärooleja. Käyttäjäroolit ovat ryhmitelty eri toimintojen mukaan. Päätason käyttäjärooli on administrator tyyppinen, jolla on kaikki oikeudet SCOM-ympäristöön hallintaan. Muita rooleja ovat operator ja read-

only operator. Ensimmäisellä käyttäjäroolilla on oikeudet tehdä pieniä muutoksia SCOM-ympäristössä kuten agentin asennuksen. Read-only operatorilla on ainoastaan vain lukuoikeudet SCOM-hallintakonsoliin. Read-only tasoinen käyttäjä ei pysty tekemään mitään konfigurointeja tai muutoksia järjestelmään. Settings-valikko sisältää valvontaan liittyviä määrittelyjä agentin ja palvelimen näkökulmasta. Settings-valikko sisältää myös yleis-asetuksia. Agentin sydämensykettä (heartbeat) pystytään säätämään tämän valikon kautta. Normaali sydämensyke on 60 sekuntia, mutta sitä voidaan tarvittaessa säätä pienemmäksi tai suuremmaksi. Ajatellaan esimerkkinä tilannetta, jossa valvottava kohde antaisi satunnaisia hälytyksiä sydämensykkeen menettämisestä. Tässä tilanteessa voisi olla paikallaan säätää sydämensykkeen asetusta joko agentin tai palvelimen päästä. Palvelimeen liittyen voidaan säätää sellaista asetusta, joka määrittelee, montako sydämenlyöntiä agentti voi menettää, jonka jälkeen se käynnistää hälytyksen. Normaaliasetuksissa sydämenlyönnin menetys on viisi kertaa. Näiden ominaisuuksien säätö voi olla tarpeen, jos valvottava kohde on hidas.

Yleisasetuksien kautta voidaan säätää hälytyksien toimintaan vaikuttavia asetuksia. Uusi hälytys on järjestelmän mukaan aina New-niminen ja ratkaisematon tai ratkaistu hälytys on Closed niminen. Normaali oletusasetuksena SCOM-hallintakonsoli kuittaa aktiiviset hälytykset 60 päivän kuluessa automaattisesti ratkaistuksi, mikäli niille ei tehdä mitään toimenpiteitä. Jos jokin hälytys on ratkaisematta ja vaivaa pitkään, voidaan tällöin tätä auto-resolve aikaa muuttaa. Kun hälytys on korjattu, saattaa olla, että valvottavan kohteen tila muuttuu vakaaksi, mutta tieto siitä asiasta ei ole vielä mennyt operatiivisen tietokantaan. Vakioasetuksena tähän asiaan on seitsemän päivän auto-resolve asetus, joka kertoo tietokannalle valvottavan kohteen olevan jälleen vakaa.

5.5 My Workspace

My workspace on hallintakonsolin viimeinen valikkoruutu. Sen avulla voidaan rakentaa käyttäjäkohtainen kojelauta. Kojelaudalla tarkoitetaan itse rakennettua näkymää, joka voi koostua mistä tahansa hallintakonsoliin liittyvistä osista. Rakentamalla itse omanlaisensa kojelaudan ylläpitäjän on mahdollisesti helpompi tarkkailla juuri haluttuja asioita yhden ikkunan kautta. Kaikilla käyttäjärooleilla on oikeudet My

workspace näkymään. Omanlaisia kojelauta näkymiä voidaan luoda myös useita ja ne voidaan tallentaa, jotta ne ovat helposti saatavilla. Omat kojelaudat ovat käytännöllisiä esimerkiksi jos ylläpitäjällä on monta kuvaruutua työasemallaan. Näin yksi kuvaruutu voidaan pyhittää juuri haluttujen asioiden seurantaa varten.

6 SACHTLEBEN PIGMENTS OY:N PALVELINYMPÄRISTÖ

Sachtleben Pigments Oy:n tietohallinto-osastolla työskentelee kolme SAP-asiantuntijaa ja viisi teknistä asiantuntijaa. Tietohallinnon ylläpidolla (Taulukko 1.) on noin 500 työasemaa ja 55 palvelinta sekä 120 kirjoitinta, 60 verkkolaitetta ja kulunvalvontalaitteisto. Talon omalla tietohallinnolla riittää ylläpidettävää, sillä myös osa tietohallinnon työtä on myös uusien laitteiden käyttöönotto ja käyttäjäopastus. Tietohallinnon palvelinympäristö on hajautettu fyysisesti kahteen eri paikkaan. Suurin osa palvelimista on virtualisoitu. Kaiken kaikkiaan tietohallinnon 55 palvelimesta on 40 virtuaalipalvelinta.

Palvelimien määrää voidaan helposti lisätä yrityksen tarpeiden kasvaessa. Tietohallinnon käytössä olevassa virtuaali-alustassa on riittävä kapasiteetti mahdollisia uusia palvelimia varten. Uuden palvelin luominen virtuaalialustaan on nopeaa ja tehokasta, koska luonnin yhteydessä voidaan käyttää kloonina ja vanhaa olemassa olevaa toimivaa palvelinta. Uuden virtuaalipalvelimen käyttöönotto on myös nopeampaa kuin fyysisen palvelimen, koska laitetta ei tarvitse kasata eikä asentaa räkkiin. Tietohallinnon kannalta virtualisointi vähentää konesalin fyysisten laitteiden määrää ja pienentää sähkönkulutusta ja sen myötä myös jäähdytystarvetta. Tietohallinnon vastuulla on järjestelmien ylläpito ja IT-infrastruktuurin kehittäminen.

Tiedostopalvelin	3
Sähköpostipalvelin	2
Tulostuspalvelin	3
Tietokantapalvelin	5
Sovelluspalvelin	17
Tietokanta/Sovelluspalvelin	25

Taulukko 1. Sachtlebenin Tietohallinnon Palvelinroolit eriteltyinä.

6.1 Monitoroinnin tarpeet

Monitoroinnin tarpeet määrittelee palvelukriittisyys. Palvelimien toiminnan käyttöaste tulisi pitää mahdollisimman korkeana. Palvelukriittisyys mitataan siltä pohjalta, miten pitkä palvelukatko aiheuttaa ongelmia tuotannolle tai muulle yrityksen ydintoiminnalle. Lisäksi tavoitteena on, että monitoroinnin avulla päästään sellaiseen tilaan, jossa kaikki järjestelmien käyttökatkot ovat suunniteltuja ja niistä on tiedotettu etukäteen jo hyvissä ajoin yrityksen henkilöstölle. Koska Sachteben Pigments Oy on teollisuuden tuotantolaitos, on selvää, että osa palveluista tulisi olla tarjolla vuorokauden ympäri. Tuotantokriittiset palvelut tulisi olla katkon ilmaantuessa jälleen toiminnassa neljän tunnin vasteajalla. Kriittisimpiä palveluita toiminnan kannalta ovat: tuotannon raportointi, tiedosto- ja sähköpostipalvelin sekä laboratorio ja lopputuotteen pakkaukseen liittyvät palvelut. Toimistotyöaikana toimivat palvelut, kuten matkalaskuohjelma, CAD-järjestelmät eivät ole niin kriittisiä toiminnan kannalta kuin tuotantoon sidoksissa olevat palvelut. Nämä kaikki palvelutarpeet määrittelevät monitoroinnin tarpeen haasteet. SCOM-työkaluna tarjoaa hyvät mahdollisuudet tarkkailla palveluita ja palvelinten käyttöastetta.

6.2 Monitoroinnin toteutus

Tekniseltä näkökulmalta tarkasteltuna monitorointi on asennettu SCOM-agentin avulla kaikkiin tietohallinnon ylläpidossa oleviin palvelimiin. Myös kaikki verkon aktiivilaitteet ovat valvonnan piirissä. Esimerkiksi kytkimet ovat valvonnan piirissä SNMP-protokollan avulla. Kaikki hälytykset tulevat suoraan SCOM-

hallintakonsoliin reaaliajassa, sekä myös tietohallinnon yhteiseen sähköpostiosoitteeseen, josta hälytykset ovat kaikkien tukihenkilöiden nähtävissä. Tietohallinnon SCOM-ympäristöä ei ole hajautettu. SCOM-ympäristöllä on pääsääntöisesti yksi ylläpitäjä ja kaikki SCOM-järjestelmään liittyvät palvelinroolit ovat samalle palvelimelle asennettu. Tietohallinnon käytössä olevat SCOM-palvelinroolit:

- Operations Console
- Web Console
- Audit Collection Services Collector (ACS)
- ACS Forwarder
- ACS Database
- Reporting Server, Reporting Server Database

Hälytysten vaivaton seuranta onnistuu myös käytössä olevan webbipalvelimen avulla mistä tahansa tehtaalla olevasta työasemasta selaimen kautta. Tietoturvalokeista ja hälytyksistä lähetään kuukausitasolla automatisoituja raportteja ylläpidolle. Monitoroinnin toteutuksessa on myös käytetty kolmannen osapuolen MP:itä koska tietohallinnon IT-infrastruktuuri sisältää mm. HP Proliant palvelimia ja HP kytkimiä ja virtuaali-alustana on VMware ESXi 5. Kaikkien monitoroitavien kohteiden valvontaa hyödyntävät MP:t ovat asennettu SCOM-ympäristöön ja myös muutamaa räätälöityä MP:tä käytetään järjestelmässä, jotka ovat juuri tarkoitettu määrittelemään tiettyjä valvonnan piirissä olevia kriittisiä asioita. Tietohallinnon toiminnalliselta näkökannalta SCOM-ylläpitäjän tehtävänä on tarkastaa hälytykset vähintään kerran päivässä ja tehdä niistä käytössä olevaan SAP-toiminnanohjaus järjestelmään oma palveluilmoitus. Jos hälytys on sen luontoinen, että se vaatii toimenpiteitä, on jokaisesta toimenpiteestä tehtävä oma palveluilmoitus SAP-järjestelmään.

7 KEHITTÄMISKOHTEET

7.1 Monitoroinnin onnistuminen ja ongelmien ratkaisu

Osa työsuoritustani on ollut SCOM-järjestelmän kehittäminen ja hälytyksien seuranta. SCOM-työkaluna menettää merkityksensä, jos hälytyksiä tulee päivittäin suurissa määrin. Kun hälytyksiä tulee paljon, ylläpitäjältä saattaa jäädä huomioimatta tärkeät hälytykset. Ajatellaan seuraavaa tilannetta. Ylläpitäjän sähköpostiin ilmestyy päivittäin 500 hälytystä. Mitä todennäköisimmin suurin osa hälytyksistä on ns. turhia hälytyksiä. On toki mahdollista, että kaikki olisivat oleellisia mutta harvemmin käy niin. Iso osa työtäni oli karsia turhia hälytyksiä, joita ilmestyi valmiiksi asennettuun ympäristöön lähes satelemalla päivittäin. Yksi hyvä turhan hälytyksen esimerkki on varmuuskopiointi. SCOM-järjestelmä antoi muutaman palvelimen varmuuskopioinnin aikana aina hälytyksen tietokannan pysäyttämisestä. Tämä on aivan normaali tapa, että kanta pysäytetään varmuuskopioinnin ajaksi. Karsimalla tämän hälytyksen saatiin yksi turha hälytys pois muiden joukosta.

Tärkeän hälytyksen esimerkki voisi olla hälytys levytilan vähyydestä, tai jonkun tärkeän palvelun toiminnan lakkaamisesta. Palvelimilla muut tärkeät hälytyksen aiheet ovat: levypakan levyjen toimintakunto, virtuaalipalvelimien terveydentilat, sekä muut kriittiset tekijät, jotka voivat aiheuttaa palvelukatkoksen tai uhata tietoturvaa. Hälytykset tulee tarkastaa huolellisesti, vaikka ne eivät aiheeltaan olisikaan aina kriittisiä. Toinen hyvä esimerkki hälytyksiä karsiessa oli hälytys liian suuresta prosessorin käyttöasteesta muutamalla virtuaalipalvelimella, joka ilmestyi joka päivä. Ongelma saatiin korjattua lisäämällä jokaiseen virtuaalipalvelimeen vähintään kaksi prosessoria. Nyt hälytysten määrä on vähentynyt huomattavasti.

7.2 Tulevaisuuden kehittämiskohteet

SCOM-järjestelmän hälytykset ovat mahdollista karsia suoraan tekemällä poikkeuksia valvontasääntöihin. Liiallinen poikkeuksien luominen valvontasääntöihin ei ole välttämättä paras ratkaisu. Hälytyksiä karsiessa kannatta aina tarkistaa hälytyksen

tarkat tiedot ja miettiä ensin, onko hälytys ratkaistavissa jollain muulla tapaa kuin poikkeussäännön tekemisellä. Esimerkiksi jollain levytilan siivoamisella tai koneen resursseja kasvattamalla voidaan hälytys saada ratkaistuksi. Toki on tilanteita, joihin lopullinen ratkaisu löytyy poikkeussäännön luomalla.

Kun SCOM-järjestelmä toimii siten kuin sen pitäisi eli hälyttäisi vain oleellisesti asioista, voisi olla paikallaan määritellä äärettömän kriittisistä hälytyksistä hälytysilmoitus suoraan ylläpitäjän matkapuhelimeen. Agenttien korjaavat toimenpiteet ovat yksi hyvä kehityskohde. Luotaessa agenteille erilaisia korjaavia toimenpiteitä, voivat agentit silloin korjata jotain pikkuhälytyksiä automaattisesti, kuten jonkin Windows-palvelun uudelleen käynnistäminen. SCOM ei oma-aloitteisesti korjaa tai hoida ongelmia vaan toimii työkaluna joka antaa hälytykset halutuista asioista ja niiden korjaaminen jää ylläpitäjän hoidettavaksi. Sen avulla pystytään määrittelemään prosessit hälytyksien tullessa. Esimerkiksi jos hälytys koskee jonkun toisen tukihenkilön vastuualuetta. SCOM-apuvälineenä ilmoittaa mahdollisista tulevaisuuden ongelmista etukäteen järjestelmän ylläpitäjälle.

8 LOPUKSI

Tutustuminen SCOM-ympäristöön oli haastavaa ja mielenkiintoista. Ensi näkemältä SCOM-ympäristö vaikutti melko laajalta ja sekavalta. SCOM:in tehokas hyödyntäminen osana toimenkuvaani antoi valmiudet lähteä tutkimaan sitä, mitä SCOM pitää sisällään ja kuinka sitä voisi kehittää parhaalla mahdollisella tavalla ja tehdä siitä opinnäytetyö. Päästessäni SCOM koulutukseen sain paljon uutta tietoa ja koko järjestelmä alkoi aueta paremmin. Koulutuksessa käytiin myös läpi SCOM-ympäristön asennus ja käyttöönotto, joten voisin kuvitella osaavani jotenkuten pystyttää asentamattomaan ympäristöön.

SCOM-ympäristöön tutustuminen on vienyt ison osan aikaa. SCOM on järjestelmänä niin suuri, että sen syvällisempi omaksuminen vaatii rauhallista otetta. Olen työskennellyt paljon SCOM:in parissa, mutta en voi pitää itseäni vielä asiantuntijana.

SCOM:in käyttöön liittyen on tarjolla muutama kirja, joita olen lukenut ahkerasti ja sitä kautta tutustunut SCOM toimintoihin. Myös Microsoftin Tech-Net sivustoilla olevia Virtual-Lab harjoitusohjelmia olen käyttänyt hyödykseni opiskellessani SCOM ympäristön tehokasta hyödyntämistä.

Sachtleben Pigments Oy:n tietohallinto hyötyy varmasti SCOM:in toiminnan kehittämisestä ja parantamisesta. SCOM:in avulla pystytään tarjoamaan helpotusta säännöllisiin asioihin, joita palvelimilta on määrä tarkastaa. Tietohallinto pystyy ennaltaehkäisemään virheet saadessaan tiedon oleellisista hälytyksistä reaaliajassa. Kokonaisuudessaan suurin osa tarpeettomista ja turhista hälytyksistä on saatu pois tekemällä muutoksia valvontasääntöihin ja valvottaviin laitteisiin.

SCOM-ympäristön kehittäminen on ollut melko työlästä ja aikaa vievää. Parhainta SCOM:in kehittämisessä on ollut onnistumisen tunne, kun on löytänyt ratkaisun jonkun hälytyksen karsimiseksi tai mahdollisen vikatilanteen korjaamiseksi. Myös hälytyksien aiheuttajien tutkiminen on ollut mielekästä ja haastavaa. Lopuksi haluan kiittää työpaikan opinnäytetyön ohjaajaa Jarkko Tuomisaloa opinnäytetyön ohjauksesta ja yhteistyöstä

LÄHTEET

Fenstermacher Scott, Mueller John Paul, Price Brad 2007: Mastering System Center Operations Manager 2007. Wiley Publishing, Inc. Canada

Microsoft a, Microsoft System Center Operations Manager. [Viitattu 15.11.2011] Saatavissa http://www.microsoft.com/en-us-/server-cloud/system-center/operations-manager.aspx

Microsoft b, Introducing Microsoft System Center Operations Manager 2007 R2. [Viitattu 03.12.2011] Saatavissa http://download.microsoft.com/download/B/1/D/B1D2450B-FF55-46BF-9E54-49FF984C89BD/SC_OpsMgr2007_R2-IntoductionWP.pdf

Dominey Andy, Fuller Cameron, Joyner John, Meyler Kerrie 2010: System Center Operations Manager 2007 R2 Unleashed. Sams. Usa

Perkola Timo, Yritysturvallisuus lähtee palvelinhuoneesta Tietoviikko 2007. [Viitattu 25.10.2011] Saatavissa http://www.tekniikkatalous.fi/tyo/yritysturvallisuus+lahtee+palvelinhuoneesta/a43049

Tapiola, Palvelintilan suunnitteluohje 2011. [Viitattu 28.10.2011] Saatavissa http://www.tapiola.fi/NR/rdonlyres/631EEED3-E45E-4085-AB2B-43EA53CC958D/0/C10c1palvelintilansuunnitteluohje.pdf

Wikipedia, vapaa tietosanakirja [Viitattu 31.10.2011] Saatavissa http://en.wikipedia.org/wiki/System_Center_Operations_Manager