Mikko Nieminen

System Center Operations Manager 2012 R2 -monitorointijärjestelmän toteutus MSP-yritysverkossa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

18.11.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Mikko Nieminen System Center Operations Manager 2012 R2 -monitorointijärjestelmän toteutus MSP-yritysverkossa 39 sivua 18.11.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Account Manager Toni Samuelsson Yliopettaja Janne Salonen

Tämän insinöörityön tarkoituksena oli suunnitella ja toteuttaa erityyppisten palvelinjärjestelmien monitorointi käyttäen System Center Operations Manager 2012 R2 -ohjelmistoa. Työn toimeksiantajana oli yritys A, joka tarjoaa asiakkailleen erilaisia hallittuja IT-ratkaisuja pilvi- ja virtuaalipalveluina.

SCOM-palvelinympäristö oli työtä aloitettaessa valmiiksi esiasennettu ja käyttövalmis, joten työssä keskityttiin sovelluksen tyypillisen perusasennuksen yksityiskohtaisen läpikäynnin sijasta lähinnä valvonnan laajuuden määritykseen, valvontatoimintojen testaukseen eri palvelin- ja verkkolaitealustoilla sekä monitoroinnin varsinaiseen toteutukseen ja tuotantokäyttöönottoon. Työn puitteissa uusi valvontajärjestelmä myös dokumentoitiin sisäistä käyttöä varten kiinnittäen huomiota monitoroinnin ylläpitoon tulevaisuudessa ja palautumiseen mahdollisista vikatilanteista.

Lopputuloksena yrityksellä oli käytössään täysin toimiva monitorointijärjestelmä, jonka piiriin voi joustavasti lisätä uusia hallittavia palveluita sekä valvonnan kohteita ladattavissa olevien hallintapakettien avulla.

Avainsanat	Palvelinten valvonta, SCOM, palveluntarjoaja

Author(s) Title Number of Pages Date	Mikko Nieminen Implementing System Monitoring for a MSP Using System Center Operations Manager 2012 R2 39 pages 18 November 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Toni Samuelsson, Account Manager Janne Salonen, Principal Lecturer

The purpose of this thesis was to design and implement infrastructure and service monitoring for several distinct types of server platforms using System Center Operations Manager 2012 R2. The thesis was carried out as a project for company A, a managed services provider offering hosted IT environments as cloud and virtualized services.

As the needed SCOM 2012 R2 server infrastructure was effectively pre-installed and in place prior to beginning work on this project, the main emphasis of this thesis, instead of describing typical server installation procedures in detail, was on defining the appropriate monitoring scope, carrying out necessary testing for various platforms and components and finally implementing the new monitoring tool into production. The monitoring environment was also documented for internal use, with an eye on future maintenance and disaster recovery.

The outcome of this thesis is a fully functional monitoring solution that is easily extendable and scalable. New monitoring objects can easily be introduced to the environment in the form of downloadable Management Packs.

Keywords	Server monitoring, SCOM, service provider

Sisällys

Lyhenteet

SCOM	System Center Operations Manager. Microsoftin kehittämä järjestelmäriippumaton palvelinten ja palveluiden valvontaohjelmisto.
SLA	Service Level Agreement. Asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot.
MP	Management Pack, eli ”hallintapaketti”. Laite- tai sovellustoimittajan tuotteelleen laatima sarja sääntöjä ja monitoreja SCOM:n kanssa käyttöönotettavaksi.
SQL	Structured Query Language. Standardoitu kyselykieli relaatiotietokantojen luomiseen ja niiden muokkaamiseen.
AD	Active Directory. Microsoftin kehittämämä hakemistopalvelu Windows-toimialueverkkoihin.
WAP	Windows Azure Pack. Microsoftin luoma kokoelma teknologioita, joiden avulla IT-palveluntarjoajien on mahdollista tarjota Windows Azure -palveluita omasta konesalistaan.
OOB	Out-of-band. Varsinaisesta datansiirtokanavasta erillinen siirtokanava, jota hyödyntäen esimerkiksi fyysisiä palvelimia voi hallita etänä käyttöjärjestelmän ulkopuolella.
SNMP	Simple Network Management Protocol. TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla.
SSH	Secure Shell. Salattuun tietoliikenteeseen käytetty viestintäprotokolla.
ICMP	Internet Control Message Protocol. TCP/IP-protokollapinoon kuuluva viestintäprotokolla.

1 Johdanto

Puhuttaessa laajoista ja monimutkaisista moderneista verkkoympäristöistä, erityisesti IaaS (Infrastructure as a Service) -palveluntarjoajien ns. ”multitenant”-verkkoinfrastruktuurista, ei toimivan ja täsmällisen palveluiden monitoroinnin merkitystä ja tarpeellisuutta voi kylliksi korostaa. On voitava aina olla riittävissä määrin varma tarjottujen palveluiden saatavuudesta, useimmissa tapauksissa ympäri vuorokauden ja vuoden jokaisena päivänä. Mahdolliset häiriöt ja vikatilanteet on niiden sattuessa paikannettava ripeästi ja niitä on reaktiivisten toimien lisäksi pyrittävä myös ehkäisemään proaktiivisilla menetelmillä. Tehokkaan valvonnan tuominen kulloinkin kyseessä olevaan ympäristöön auttaa pääsemään näihin tavoitteisiin ja täten helpottaa järjestelmien ylläpitämistä merkittävästi.

Konesaliverkkojen monitorointiin ja palveluiden hallintaan on nykypäivänä saatavilla useita erityyppisiä ja eri alustoille suunnattuja valvontasovelluksia, joilla kullakin saattaa olla yksi tietty käyttökohde tai mahdollisesti useitakin eri sovellutuksia ympäristön hallinnassa. Microsoftin kehittämä System Center Operations Manager (SCOM) on eräs yritys yksinkertaistaa konesalin palveluiden hallintaa tuomalla yhden sovelluksen alle mahdollisuus sekä verkkolaitteiden, fyysisten ja virtuaalisten palvelimien, levyjärjestelmien että sovellusten saatavuuden ja tehokkuuden monitorointiin. SCOM soveltuu erityisesti Microsoftin teknologioihin pohjautuvien ympäristöjen hallintaan ja on yksi nykypäivän käytetyimmistä monitorointiratkaisuista.

Tämän opinnäytetyön tarkoituksena on kuvailla yritys A:n palvelin- ja verkkoympäristössä syksyn 2015 aikana käyttöönotetun System Center Operations Manager 2012 R2 -valvontatyökalun toteutusprojektin vaiheet, aina huolellisen monitorointitarpeiden ja kohteiden kartoituksen sekä valvontatoimintojen testauksen kautta varsinaiseen tuotantoon siirtymiseen asti. Uuden monitorointityökalun käyttöönoton on odotettu helpottavan yrityksen IT-infrastruktuurin ylläpitäjien päivittäisiä työtehtäviä ja avaavan uudenlaisia näkökulmia palveluiden saatavuudesta myös muualla yrityksen organisaatiossa toimiville, esimerkiksi asiakkaiden kanssa solmittujen SLA-sopimusten vaatimustasoja tarkkaileville johtotason henkilöille.

2 Projektin taustaa

2.1 Yritys

Yritys A on pääkaupunkiseudulla toimiva yritys, joka tarjoaa hallittuja IT-ratkaisuja pilvi- ja virtuaalipalveluina sekä kotimaisille että ulkomaisille asiakkaille. Yrityksen laaja verkkoinfrastruktuuri pitää sisällään jaettujen palvelujen ja palvelimien lisäksi myös erilaisia asiakkaille kokonaan tai osittain dedikoituja ympäristöjä. Hallinnan piirissä on kaiken kaikkiaan useita satoja työasemia sekä eri käyttötarkoituksilla varustettuja palvelimia.

Yritys panostaa jatkuvasti palveluidensa ja toimintansa kehittämiseen eri osa-alueilla, yhden merkittävimmistä ponnistuksista ollen tämä projekti uuden monitorointijärjestelmän käyttöönottamiseksi tuotantoympäristössä. Työasemien hallintaa varten yrityksellä on jo olemassa joukko hyviksi havaittuja ja ajan tasalla olevia työkaluja, ja uusi SCOM-järjestelmä onkin tarkoitettu käyttöönotettavaksi nimenomaan tehostamaan ja virtaviivaistamaan palvelinjärjestelmien sekä verkkolaitteiden monitorointia tällä hetkellä käytössä olevien työkalujen tilalle ja rinnalle.

2.2 System Center Operations Manager 2012 R2

2.2.1 System Center 2012 R2 lyhyesti

System Center Operations Manager 2012 R2 -sovellus kuuluu Microsoftin System Center 2012 R2 -tuoteperheeseen. System Center -tuotteet tähtäävät niitä käyttävien organisaatioiden päivittäisten konesalin hallintatoimintojen virtaviivaistamiseen, yksinkertaistamiseen, ja automatisointiin. System Center koostuu useasta eri komponentista, joilla kullakin on oma erikoistunut tehtävänsä IT-infrastruktuurin luonnissa ja ylläpidossa. Eri tuotteet tukevat toisiaan yhdessä käytettyinä, mutta ovat erittäin tehokkaita työkaluja yksittäisinäkin komponentteina kun tähdätään jonkin tietyn toiminnon tai palvelun toteutukseen. [1, s. 5.]

System Center 2012 R2 pitää sisällään seuraavat ohjelmistot ja komponentit:

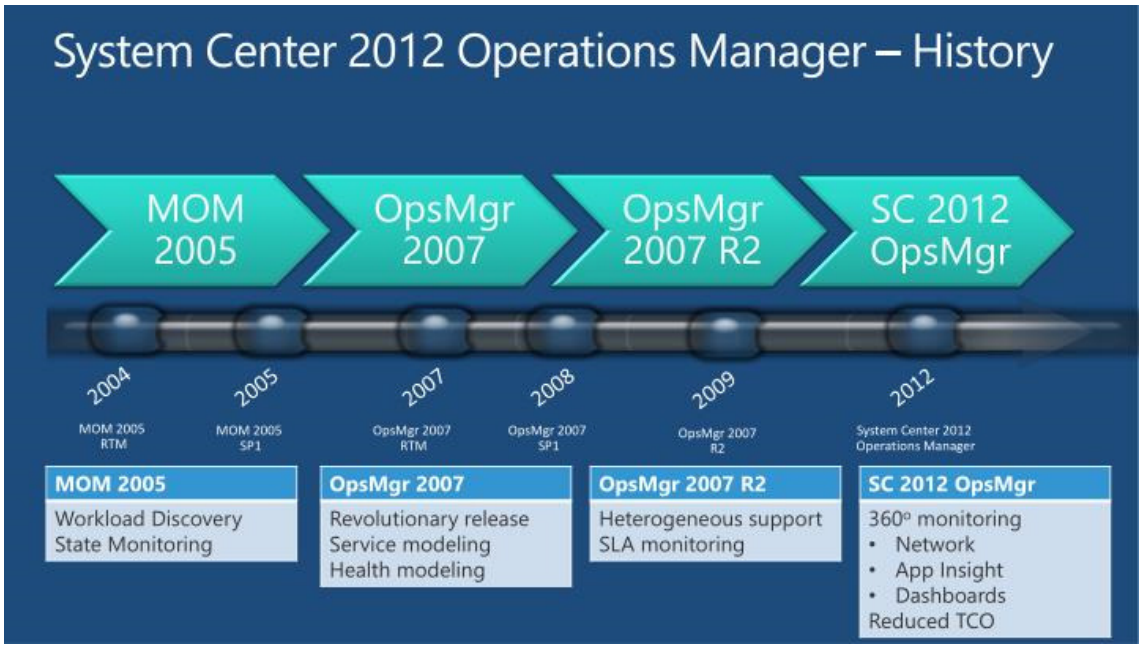
- System Center Configuration Manager
- System Center Operations Manager

- System Center Data Protection Manager
- System Center Service Manager
- System Center Virtual Machine Manager
- System Center Orchestrator
- System Center Endpoint Protection
- System Center App Controller.

System Centerin eri osa-alueiden toiminnan ja käyttötarkoituksen ymmärtäminen on oleellista modernin Microsoftin teknologioihin pohjautuvan IT-arkkitehtuurin hallinnan kanssa tekemisissä oleville ylläpitäjille. Tämän insinöörityön puitteissa System Centerin muihin ominaisuuksiin ja sovelluksiin ei kuitenkaan tarkemmin syvennytä Operations Manageria lukuun ottamatta.

2.2.2 Operations Managerin historiaa

Microsoftin luoman System Center Operations Manager (SCOM)-valvontaohjelmiston juuret ovat englantilaisen Serverware Groupin 1990-luvun lopulla kehittämässä ”SeNTry ELM” -nimisessä hallintasovelluksessa, jonka ominaisuuksiin lukeutui muun muassa mahdollisuus selata usean Windows NT -alustaisen palvelimen tai työaseman tapahtumalokeja yhdestä sijainnista. Oikeudet sovellukseen osti kuitenkin Mission Critical Software -niminen yritys, joka nimesi tuotteen uudelleen ”Enterprise Event Manageriksi”. Mission Critical Software päätyi lopulta kirjoittamaan tuotteen lähdekoodin kokonaan uudelleen, ja tässä yhteydessä sovelluksen nimi vaihtui jälleen. Uudeksi nimeksi tuotteelle tuli OnePoint Operations Manager (OOM). Mission Critical Software yhdistyi alkuvuodesta 2000 NetIQ:n kanssa, joka puolestaan myi tuotteen oikeudet Microsoftille. Tästä eteenpäin tuote tunnettiin nimellä Microsoft Operations Manager (MOM). Ohjelmistolle julkaistiin tällä nimellä vielä uusi versio, Microsoft Operations Manager 2005, josta eteenpäin sovelluksesta on käytetty nimeä System Center Operations Manager. Ensijulkaisunsa System Center Operations Manager sai versiolla 2007, johon julkaistiin myöhemmin täydennyksinä Service Pack 1- sekä R2-versiot. Viimeisin markkinoilla oleva SCOM-versio on System Center Operations Manager 2012 R2, joka sisältää aiempiin verrattuna lukuisia uusia ominaisuuksia jo aiemmissa versioissa tutuksi tulleiden toimintojen lisäksi (ks. kuva 1). [2, s. 17.]



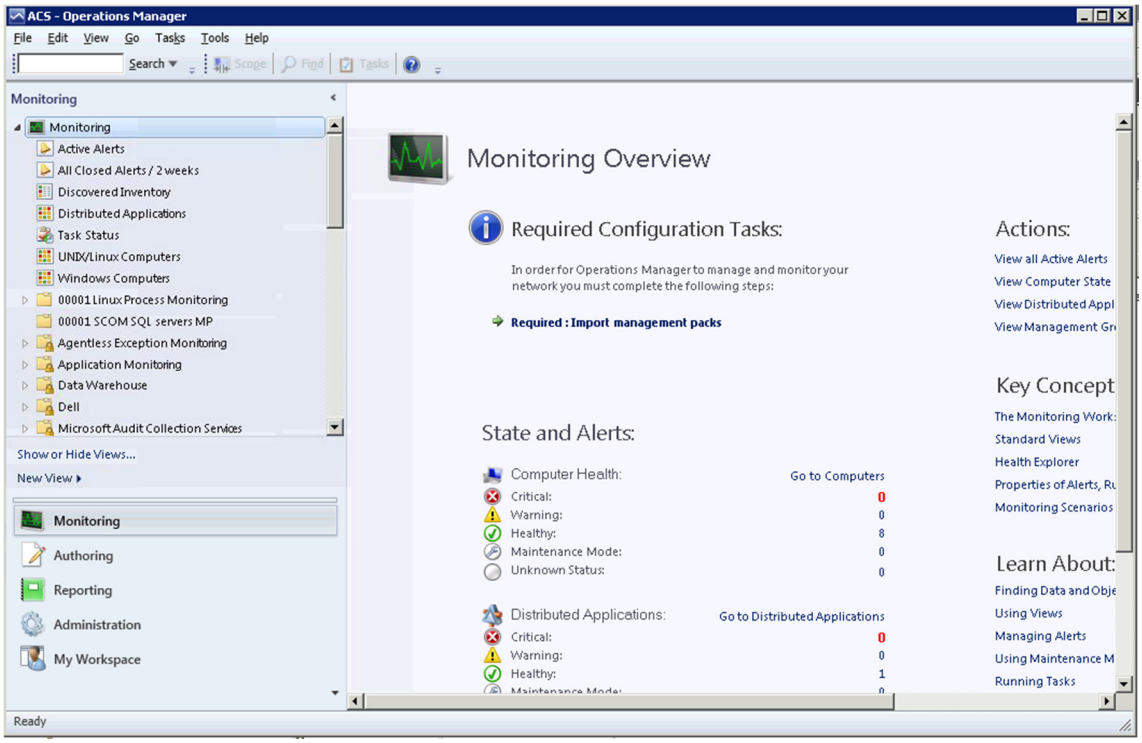
Kuva 1. System Center Operations Managerin ominaisuuksien kehitys vv. 2004 – 2012 [3].

2.2.3 Ominaisuudet ja käyttökohteet

Operations Manager -ohjelmiston avulla IT-infrastruktuurin ylläpitäjien on mahdollista valvoa yhden näkymän kautta useiden laitealustojen, palvelujen, sovellusten ja verkkolaitteiden suorituskykyä, saatavuutta ja yleistä terveyttä. Operations Manager -konsolista (ks. kuva 2) voi nopeasti paikantaa mahdolliset ongelmatekijät verkkoympäristön valvottujen kohteiden joukosta. SCOM-ympäristö on myös hallittavissa ja automatisoitavissa PowerShell-komentojen avulla. Se käyttää tarkoitukseen räätälöityä PowerShell-konsolia nimeltään ”Operations Manager Shell”. SCOM:in avulla voidaan valvoa Microsoft Windows -käyttöjärjestelmällä varustettuja työasemia ja palvelimia ja niillä ajettavia palveluja, sovelluksia ja toimintoja, kattavaa määrää erilaisia Unix/Linux-järjestelmiä palveluineen sekä erilaisia verkkolaitteita, esimerkiksi kytkimiä ja reitittimiä.

Operations Managerin pääasiallisena tehtävänä on kertoa käyttäjälle, mitkä valvonnan piirissä olevista kohteista eivät toimi ennalta määritettyjen sääntöjen ja monitorien mukaisella tasolla, lähettää hälytyksiä, kun se havaitsee ympäristössä potentiaalisia ongelmia sekä antaa myös neuvoja, suoria toimintaohjeita ja jopa mahdollisia ratkaisuja havaittujen ongelmien korjaamiseksi. Monitoroinnin laajuus on täysin ylläpitäjän itsensä määritettävissä valitsemalla monitoroinnin piiriin tulevat laitteet ja kohteet sekä tuomalla

oman valintansa mukaan sovellukseen ns. Management Packeja eli hallintapaketteja, jotka sisältävät käyttövalmiita sääntöjä sekä monitoreja eri toimintojen valvomiseen.



Kuva 2. Operations Manager -konsoli yritys A:n ympäristössä projektin alussa

Valvottavia kohteita voidaan tarkkailla erilaisten monitorien ja sääntöjen avulla, tai niillä voidaan ajaa Operations Manager -konsolin kautta erilaisia komentoja jonkin tietyn toiminnon tai diagnostiikan suorittamiseksi. Monitorit eroavat säännöistä toiminnallisella tasolla suuresti, vaikka päällisin puolin molemmilla voidaankin saavuttaa hyvin samankaltaisia tuloksia valvonnan kannalta. Monitorit tarkkailevat valvotun kohteen terveyden tilaa (engl. ”health state”) lähestulkoon reaaliajassa. Ne antavat hälytyksiä, kun tilassa havaitaan muutoksia huonompaan suuntaan ja vastavuoroisesti ilmoittavat käyttäjälle, kun terveystilan on jälleen havaittu palautuneen normaalille tasolle, jonka jälkeen ne sulkevat itsenäisesti luomansa hälytykset. Monitoreista ei kerätä dataa Data Warehouse -tietokantaan kirjoitettavaksi, vaan tietoa terveystilan muutoksista ja hälytyksistä käsitellään pelkästään Operations -tietokannassa. Kohteiden terveystilasta ei ole käytettävissä pidempiaikaista dataa raportointitarkoituksia varten. Sääntöjen avulla sen sijaan on mahdollista toteuttaa tiedonkeruu esimerkiksi kohteen suorituskyvystä ja tapahtumahistoriasta, sillä sääntöjen keräämä data kirjoitetaan myös Data Warehouse -tietokantaan. Säännöillä on monitorien tapaan myös mahdollisuus erilaisten hälytysten luomiseen. Säännöt eivät kuitenkaan tarkkaile edellä mainittua kohteen terveystilaa, vaan hälytysten

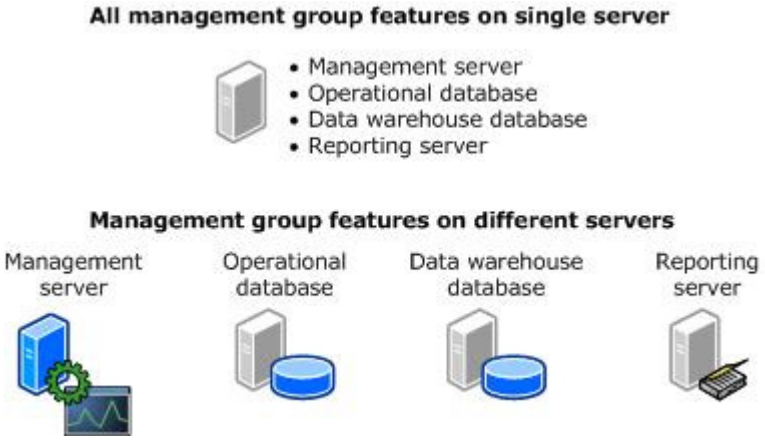
luonti perustuu esimerkiksi tietyn järjestelmän tapahtuman (engl. ”event”) havaitsemiseen, tai kun kohteen suorituskyky tippuu määritellylle tasolle, esimerkiksi CPU:n käyttö ylittää 80 %. [4, s. 4-5.]

2.2.4 Toimintaperiaate

Operations Manager -ympäristö koostuu asennuksen yhteydessä luotavasta perusyksiköstä, Management Groupista eli hallintaryhmästä, sekä valvonnan kohteena oleville laitteille asennettavista agenteista, jotka keräävät monitoroitavista kohteista dataa ja vertaavat sitä ennalta määritettyihin arvoihin. Agenteilta kerätyn datan perusteella Operations Manager voi luoda hälytyksiä tai käyttää datan pelkkiin arkistointi- ja raportointitarkoituksiin.

Hallintaryhmä pitää sisällään vähintään yhden Management Serverin, hallintapalvelimen, joka välittää agenteilta kerätyn datan eteenpäin SCOM:in tietokantoihin ja toimii myös yhteyspisteenä Operations-konsolille, jonka kautta ympäristöä hallinnoidaan ja valvotaan. Hallintapalvelimen lisäksi SCOM-ympäristö tarvitsee käyttöönsä kaksi erillistä MS SQL -tietokantaa, eli Operational-tietokannan sekä Data Warehouse -tietokannan. Operational-tietokanta sisältää hallintaryhmän konfiguraation ja asetukset sekä kaiken hallintaryhmän keräämän monitorointidatan, jota säilytetään Operational-tietokannassa oletusarvoisesti seitsemän päivän ajan. Data Warehouse -tietokanta puolestaan säilöö valvonta- sekä hälytysdataa pidempijaksoisesti raportointitarkoituksiin. Kaikki sääntöjen avulla kerätty, Operational-tietokantaan kirjoitettu data kirjoitetaan myös Data Warehouse-tietokantaan, joten ajettavista raporteista saatava tieto on aina täysin ajanmukaista. [4, s. 6.]

Edellä kuvatut hallintaryhmän perustoiminnot voivat sijaita erillisillä, kullekin tehtävälle omistetuilla palvelimilla, tai vähimmillään yhdellä ja samalla palvelimella (ks. kuva 3).



Kuva 3. Hallintaryhmän rakenne [4, s. 6].

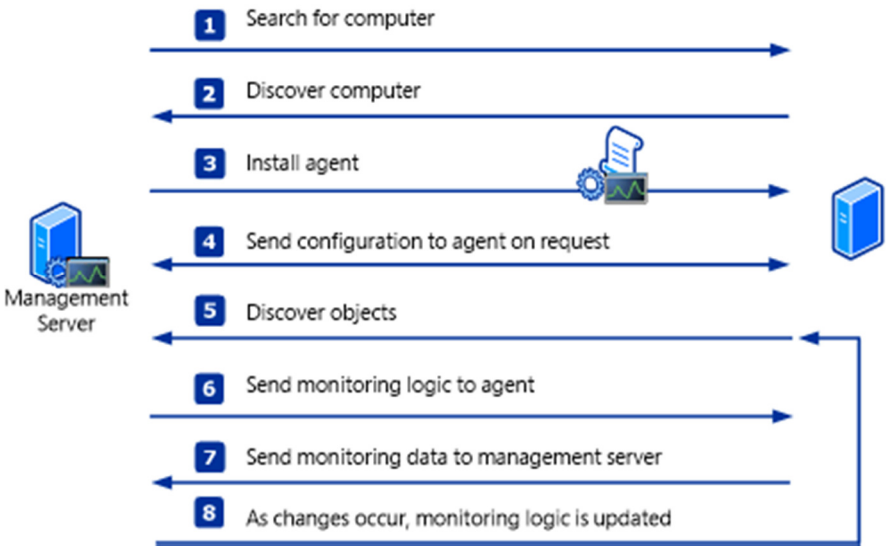
Kuten jo aiemmin on todettu, hallintapalvelimen tehtävänä SCOM-ympäristössä on olla yhteyspisteenä valvonnan alaisuudessa oleville agenteille ja monitorointiympäristöä hallinnoivalle ylläpitäjälle, sekä välittää agenteilta kerätty data edelleen tietokantoihin kirjoitettavaksi. Yhteen hallintaryhmään voi sisältyä joko pelkästään yksi tai mahdollisesti useita hallintapalvelimia. Kun näiden palvelinten lukumäärä ylittää kahden, niistä muodostuu ns. ”resource pool” eli resurssivaranto, ja valvontatyö jaetaan tasaisesti kaikkien sen jäsenten kesken. Mikäli jokin hallintapalvelimista kaatuu tai häviää verkosta, muut resurssivarannon jäsenpalvelimet ottavat hävinneen palvelimen tehtävät hoitaakseen. Lisättäessä uusia jäseniä resurssivarantoon ottavat niin ikään uudet palvelimet käynnissä olevia monitorointitehtäviä vastuulleen täysin automaattisesti. Tavallisen hallintapalvelimen lisäksi on olemassa ns. ”gateway” eli yhdyskäytäväpalvelin, jonka avulla on mahdollista valvoa myös kohteita, jotka ovat luotettujen AD-toimialueiden ulkopuolella.

Operations Manager -ympäristössä termi ”agentti” tarkoittaa käytännössä valvottavalle laitteelle asennettavaa palvelua, jonka vastuulla on kommunikointi hallintaryhmän suuntaan aiemmin kuvaillulla tavalla. Agentit siis keräävät tietoa ja tarkkailevat valvomaansa laitetta hallintapalvelimelta saamansa konfiguraation mukaisesti. Kullakin hallintapalvelimella on omat valvottavat kohteensa, eli yksittäinen agentti on jokaisena hetkenä yhteydessä vain yhteen hallintapalvelimeen kerrallaan. Yksi tärkeimpiä suorituskyvyn mittareita SCOM-ympäristössä on agentin laitteelleen laskema terveystila, jonka avulla ylläpitäjät voivat havaita mahdolliset suorituskyvyn putoamiset tai vikatilanteet agenteilla. Agentti voi toimia myös ns. ”proxy”-tilassa, jolloin se voi välittää monitorointitietoa hallintaryhmälle jonkin toisen laitteen puolesta, jolle ei esimerkiksi syystä tai toisesta voi asentaa omaa agenttia.

Agentin toiminta valvottavalla laitteella on havaittavissa yhtenä Windowsin järjestelmäpalveluna (engl. ”service”), joka on nimeltään ”System Center Management Health Service”. Palvelu ajaa hallintapalvelimelta saamansa konfiguraation mukaisesti asiakaslaitteella tarvittaessa erilaisia käskyjä ja suorittaa datan keräyksen. Silloinkin, kun palvelu ei syystä tai toisesta saa yhteyttä määritettyyn hallintapalvelimeensa, se jatkaa datan keräämistä konfiguraationsa mukaisesti ja siirtää sen jonoon hallittavan laitteen levyasemalle. Kun yhteys hallintapalvelimeen jälleen palautuu, lähetetään tämä jonoon siirretty data normaalisti eteenpäin tietokantoihin tallennettavaksi.

Aiemmin mainitut SCOM-agenttien konfiguraatiot, joiden perusteella dataa kerätään valvonnan kohteilta, määritellään hallintapalvelimelle ladattavia hallintapaketteja (Management Pack) hyödyntäen. Hallintapaketit sisältävät erilaisille sovelluksille ja palveluille räätälöityjä monitorointisääntöjä ja tiedot, joiden avulla hallintapalvelin osaa paikallistaa valvotuilta laitteelta kunkin MP:n kohteena olevat toiminnot. Merkittävä osa saatavilla olevista valmiista hallintapaketeista on ns. sinetöityjä, mikä tarkoittaa sitä, että niiden sisältöön ei suoraan voi tehdä muutoksia tai muokkauksia. Mahdollisille ylläpitäjän itse tekemille muutoksille on tällöin luotava uusi hallintapaketti ja kohdistettava se halutulla tavalla. [4, s. 5-10.]

Kuvassa 4 esitellään pääpiirteittäin Operations Managerin resurssien etsintään ja uusien laitteiden monitoroinnin aloittamiseen käyttämä menetelmä. SCOM etsii verkosta koneobjektia ylläpitäjän asettaman konfiguraation mukaisesti ja löytäessään etsityn laitteen asentaa sille monitorointiagentin. Hallintapalvelin lähettää agentille pyynnöstä konfiguraatiotiedot palvelimella asennettuna olevien hallintapakettien sisällön mukaisesti. Agentti vertaa saamaansa konfiguraatiota hallittavan laitteen tietoihin ja kokoonpanoon, ja välittää hallintapalvelimelle tiedon löytämistään komponenteista. Tämän jälkeen hallintapalvelin lähettää saamiensa tietojen perusteella agentille monitorointilogiikan, ja agentti ryhtyy valvomaan määriteltyjä kohteita. Mahdollisten muutoksien tapahtuessa monitorointilogiikkaa päivitetään ja valvottavien komponenttien resurssienetsintä aloitetaan uudelleen.



Kuva 4. Valvottavan laitteen lisääminen monitoroinnin piiriin [4, s. 9.]

2.2.5 Tyypillinen SCOM-palvelinasennus pääpiirteittäin

SCOM-järjestelmää käyttöönotettaessa on parhaimman lopputuloksen saamiseksi suotavinta lähteä liikkeelle huolellisesta ympäristön suunnittelusta, joka sisältää kokonaiskuvan monitoroitavien laitteiden ja kohteiden määrästä ja tyypistä, ympäristön tarvitsemien palvelin- ja verkkoresurssien sekä käyttäjäroolien määrityksen, tietokantojen ja mahdollisen raportoinnin suunnittelun ja ympäristön tietoturvan sekä ilmoitusten toteutuksen. Microsoft on luonut erilaisten palvelinympäristöjen suunnittelun tueksi sarjan tuotekohtaisia IPD ”Infrastructure Planning and Design)-oppaita, jotka sisältävät ohjeita ja parhaita käytäntöjä ympäristön mitoitukseen sekä käyttöönottoon liittyen. Oppaat ovat ladattavissa veloituksetta Microsoftin verkkosivuilta. Käyttöönotto-ohjeistuksen lisäksi dokumentti sisältää myös Operations Managerin järjestelmävaatimukset kaikkien palvelinroolien osalta. Tämän opinnäytetyön puitteissa järjestelmävaatimuksia ei tarkemmin käydä läpi. [1, s. 26-27.]

Olennaisimpia osuuksia suunnittelussa on SCOM-palvelinroolien jakamisen ja hallintapalvelimien kokonaislukumäärän mitoittaminen. Kuten aiemmin on todettu, Operations Managerin käyttöönsä vaatimat palvelinroolit voivat kaikki sijaita samalla palvelimella, tai ne voidaan jakaa usean järjestelmän kesken. Mikäli kyseessä on vain pieni monitorointiympäristö, on ensimmäinen vaihtoehto täysin validi suorituskyvyn kannalta. Tyypillisintä on kuitenkin eriyttää Operational- ja Data Warehouse-tietokannat omille SQL-palvelimilleen tai palvelinklustereille, ja asentaa hallintapalvelinrooli erilliselle palvelimelle. Vielä

tähän mennessä käsittelemättömiä palvelinrooleja ovat Web Console (Web-pohjainen käyttöliittymä jolla pääsee käsiksi SCOM:in dataan ja raportteihin HTTP-tai HTTPS-yhteyden yli) sekä Reporting Services- eli raportointipalvelurooli. Web Consolen voi asentaa olemassaolevalle hallintapalvelimelle, tai sen voi sijoittaa omalle palvelimelleen. Raportointipalvelun tulisi sijaita samalla palvelimella SCOM:in tietokantojen kanssa, sillä raportit muodostetaan Data Warehouse -tietokannan sisällön pohjalta.

Tietokantojen ja hallintapalvelimen lisäksi SCOM tarvitsee käyttöönsä tietyn määrän käyttäjätilejä, joita käytetään järjestelmän sisäisiin toimintoihin ja esimerkiksi tietokantoihin yhdistämiseen. Tarvittavien tunnusten joukossa ovat seuraavat:

- ”Management Server Action Account”, jonka olisi suositeltavaa olla domain-käyttäjätunnus. Tunnuksella tulee myös olla paikalliset järjestelmänvalvojan oikeudet hallintapalvelimella.

- Käyttäjätunnus “System Center Configuration Service” ja “System Center Data Access Service”-palveluja varten, joita käytetään Operational-tietokantaan yhdistämiseen sekä sen muokkaukseen. Tämä käyttäjätili voi olla joko paikallinen järjestelmätili tai domain-käyttäjätunnus.

- “Data Reader Account”, domain-käyttäjätunnus. SQL Reporting Services yhdistää tämän tunnuksen avulla Data Warehouse -tietokantaan raporttien luomiseksi.

- “Data Writer”, domain-käyttäjätunnus. Hallintapalvelin käyttää tätä tunnusta datan kirjoittamiseksi Data Warehouse -tietokantaan, ja tiedon lukemiseen Operational-tietokannasta.

Lisäksi agenttien asennusta ja hallinnointia varten tarvitaan kaksi käyttäjätunnusta, jotka ovat:

- ”Local Administrator Account”. Tätä tunnusta käytetään SCOM-agentin asennukseen push-menetelmällä ja sillä täytyy olla paikalliset pääkäyttäjän oikeudet ko. laitteella.

- ”Agent Action Account”. Kaikki datankeruu ja toimintojen suorittaminen agenteilla tapahtuu tällä tunnuksella. Yleisimmin käytössä on paikallinen järjestelmätili.

SCOM vaatii myös verkkoympäristön osalta eri hallinta- ja tietokantapalvelimien sekä agenttien välillä tapahtuvaan liikennöintiin tietyn määrän avoimia TCP- ja UDP-portteja. Tärkeimpinä mainittakoon TCP-portti 5723, jonka kautta Windows-agentit kommunikoivat hallintapalvelimen kanssa, TCP-portti 1433 tietokantayhteyksiä varten hallintapalvelimelta Operational- ja Data Warehouse-tietokantoihin, TCP-portti 5724 Operations Manager-konsolin ja hallintapalvelimen välillä (mikäli konsoli ei ole asennettu hallintapalvelimelle vaan sitä käytetään muusta sijainnista), TCP-portit 22 sekä 1270 Unix- ja Linux-agenttien hallinnointiin hallintapalvelimelta sekä UDP-portit 161 ja 162 verkkolaitteiden hallinnointiin. Tarkempia palomuurikonfiguraatioon liittyviä vaatimuksia ei tämän insinöörityön puitteissa käydä läpi. Yksityiskohtaiset tiedot verkkoympäristöön kohdistuvista vaatimuksista ovat saatavilla esimerkiksi aiemmin mainitusta IPD-oppaasta. [5, s. 55-59.]

Kun huolellinen suunnittelu on saatu päätökseen, voidaan siirtyä asennusvaiheeseen. Asennus käynnistetään palvelimella, josta on tarkoitus luoda uuden hallintaryhmän ensimmäinen hallintapalvelin. Korkealla tasolla läpikäytynä SCOM-asennus sisältää seuraavat vaiheet:

- Asennettavat ominaisuudet. Valitaan SCOM-järjestelmän toiminnot, jotka palvelimelle halutaan asentaa.

- Asennushakemiston valinta. SCOM-asennuksen voi sijoittaa järjestelmälevyn ohella mihin tahansa muuhun haluamaansa sijaintiin.

- Edellytystarkistus. Asennusohjelma tarkistaa, että palvelimella on olemassa kaikki SCOM-asennuksen edellyttämät komponentit ja että verkkoympäristö täyttää Operations Managerin sille asettamat vaatimukset.

- Asennustyypin valinta. Määritetään, liitetäänkö palvelin johonkin olemassa olevaan hallintaryhmään vai luodaanko uusi.

- Operational-tietokannan määritys. Annetaan sen palvelimen verkkonimi ja tiedot, jolle asennusohjelma luo Operational-tietokannan.

- Data Warehouse-tietokannan määritys. Annetaan sen palvelimen verkkonimi ja tiedot, jolle asennusohjelma luo Data Warehouse-tietokannan.

- Operations Managerin käyttäjätilien määritys. Annetaan asennusohjelmalle järjestelmän tarvitsemien edellä kuvailtujen eri käyttäjätilien tiedot.

Tämän jälkeen asennus käynnistyy ja sen edistymistä voi tarkkailla asennusohjelmasta. Onnistuneen asennuksen jälkeen on vielä tarpeellista asentaa Operations Manager -konsoli ympäristön hallinnointia varten, mikäli sitä ei varsinaisen ympäristön asennuksessa tehty. Konsoli voi sijaita hallintapalvelimella tai sen voi asentaa mille tahansa muulle palvelimelle tai työasemalle, josta on mahdollista muodostaa vaadittu verkkoyhteys hallintapalvelimelle. [1, s. 40-63.]

3 Käytettävät palvelinympäristöt

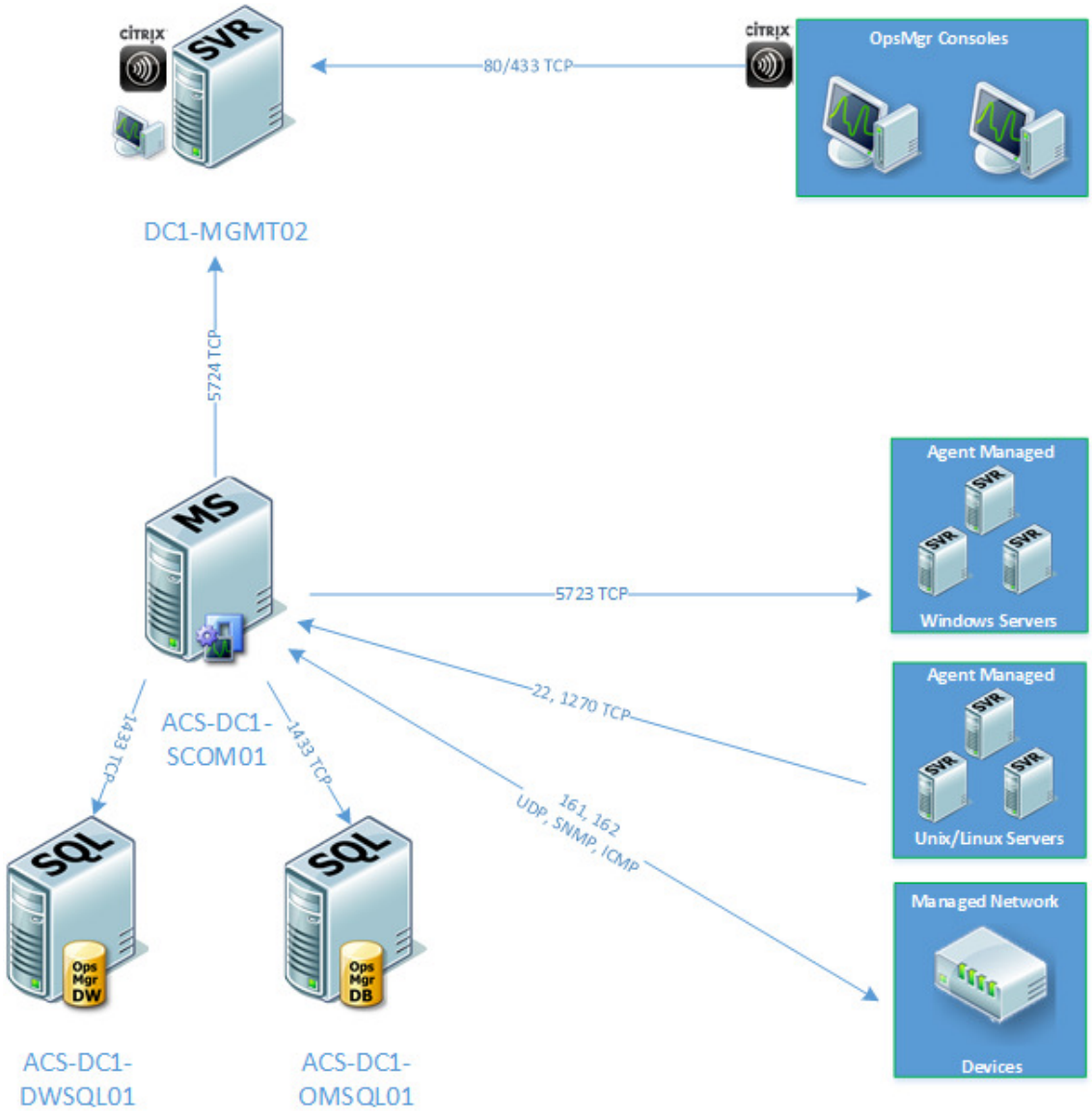
3.1 Yleiset lähtökohdat

Aloitettaessa tämän insinöörityön käytännönläheisempää osuutta, oltiin yritys A:n tulevan SCOM 2012 R2 -järjestelmän käyttöönoton osalta tilanteessa jossa vaadittu palvelinympäristö oli jo esiasennettu eli tarvittavat palvelimet, SQL-tietokannat, käyttäjätunnukset, verkkokonfiguraatiot ym. edellytykset olivat valmiiksi luotuina ja määriteltyinä. Projekti oli jo aiemmin alkanut huolellisella perehtymisellä Operations Managerin toimintaan ja ominaisuuksiin, sillä SCOM oli tekijälle entuudestaan tuttu vain pintapuolisella tasolla ja perusperiaatteidensa osalta. Pohjatietojen hankkiminen tapahtui itsenäisesti hyödyntäen erilaisia Microsoftin sekä erilaisten kolmansien osapuolten tarjoamia kirjallisia ja sähköisiä oppimateriaaleja.

Seuraavaksi toteutettavina vaiheina olivat monitoroitavien järjestelmien ja palveluiden määritys yrityksen sisäisenä prosessina, testiympäristön pystytys, monitorointitoimintojen testaus eri alustoilla ja lopulta saatujen tuloksien ja havaintojen pohjalta monitorointiagenttien asennus tuotantojärjestelmiin ja ympäristön lopullinen konfigurointi sekä hienosäätö. Tulevissa luvuissa keskitytään näiden vaiheiden läpikäyntiin ja hyödynnettävien järjestelmien tekniseen kuvaukseen.

3.2 SCOM-palvelinympäristön kuvaus

Yritys A:n käyttöön tulevan SCOM-palvelinkokoonpanon (ks. kuva 5) osalta päädyttiin ratkaisuun, jossa hallintaryhmän käyttöön asennettiin yksi hallintapalvelin (”ACS-DC1-SCOM01”), ja Operational- sekä Data Warehouse-tietokannat sijoitettiin omille palvelimilleen (”ACS-DC1-OMSQL01” sekä ”ACS-DC1-DWSQL01”). Palvelinroolien eriyttäminen lisää suorituskyvyn kasvamisen lisäksi omalta osaltaan järjestelmän vikasietoisuutta ja mahdollistaa joustavamman tavan palautua mahdollisista vikatilanteista.



Kuva 5. Yritys A:n SCOM-palvelinympäristö

Varsinaisten palvelinroolien jakamisen lisäksi Operations Manager -konsoli on asennettuna erilliselle palvelimelleen (”DC1-MGMT02”), josta se on ylläpitäjien käytettävissä Citrixin XenApp-sovellusvirtualisointiratkaisun kautta jaettuna virtuaalisovelluksena. Näin vältytään konsolin manuaaliselta asennukselta kunkin ylläpitäjän työasemalle ja myös suorilta RDP-yhteyksiltä hallintapalvelimelle pelkissä konsolin käyttötarkoituksissa.

Käytettävä SCOM-palvelininfrastruktuuri on täysin virtualisoitu ja sijaitsee yrityksen käytössä olevassa Windows Azure Pack -ympäristössä, jonka saatavuus ja toimintavarmuus on korkea. Koska koko ympäristö on virtualisoitu, on Operations Managerin käyttöön saatavilla tarvittaessa erittäin nopealla aikataululla lisää fyysisiä resursseja (CPU, RAM, levytila) sekä myös kokonaan uusia palvelimia, jos esimerkiksi hallintaryhmän sisältämien hallintapalvelimien määrää nähtäisiin tarpeelliseksi kasvattaa, vaikkapa lisääntyneen monitorointitarpeen johdosta. Alla olevasta taulukosta 1 on tarkasteltavissa SCOM-ympäristön palvelimien käytössä olevat resurssit ja käyttöjärjestelmien sekä ohjelmistojen versiotiedot projektin alussa.

Taulukko 1. SCOM-palvelinten kokoonpano

Palvelin	CPU	RAM	HD	Käyttöjärjestelmä	SQL Server-versio
ACS-DC1-OMSQL01	4 ydintä	8GB	180GB	Windows Server 2012 R2	SQL Server 2012
ACS-DC1-DWSQL01	4 ydintä	8GB	300GB	Windows Server 2012 R2	SQL Server 2012
ACS-DC1-SCOM01	2 ydintä	4GB	80GB	Windows Server 2012 R2	n/a

3.3 Monitoroitavat järjestelmät ja palvelut

Monitoroinnin piiriin oli tarkoitus ottaa kirjava joukko yrityksen verkkoinfrastruktuuriin kuuluvia sekä sisäisessä että asiakkaiden käytössä olevia jaettuja palveluja ja laitteita. Näiden kartoittamiseksi järjestettiin tapaaminen, jossa käytiin läpi olemassa olevat palvelut ja niiden senhetkinen monitorointiväylä sekä pyrittiin palvelukohtaisesti määrittämään parhain lähestymistapa uuteen monitorointiin siirtymiselle. Kaikkia järjestelmiä ei tultaisi siirtämään uuden SCOM-järjestelmän piiriin yhdellä kertaa, vaan siirtyminen toteutettaisiin porrastettuna, palvelu kerrallaan.

Tapaamisessa esille tulleiden avainpalveluiden ja -järjestelmien joukossa olivat esimerkiksi nämä käytössä olevat eri teknologiat:

- AD DS (Active Directory Domain Services) ja AD-ympäristön toimialueen ohjauskoneet
- DFS (Distributed File System) eli hajautetun tiedostojärjestelmän avulla toteutetut tiedostojaot
- Citrix XenDesktop
- System Center Configuration Manager 2012 (SCCM)
- System Center Data Protection Manager 2012 (DPM)
- NPS-palvelin (Network Policy Server)
- RRAS VPN -palvelin (Routing and Remote Access -palvelinroolin avulla toteutettu VPN-yhteys)
- DirectAccess-palvelin
- Tulostuspalvelin
- MS SQL -tietokannat.

Palvelinjärjestelmien ohella valvonnan alaisuuteen päätettiin ottaa myös erikseen määritelty joukko verkkolaitteita, mikä pitää sisällään esimerkiksi asiakkaiden tiloissa sijaitsevia erilaisia kytkimiä, reitittimiä ja WLAN-tukiasemia. Useimmin esiintyneiden laitevalmistajien joukossa olivat Cisco, HP sekä Juniper.

SCOM-monitoroinnin konfiguroiminen asiakkaille kokonaan dedikoituihin virtuaaliympäristöihin päätettiin jättää vielä myöhemmin perinpohjaisesti selvitettäväksi, ja tullaan todennäköisesti toteuttamaan erillisenä projektinaan.

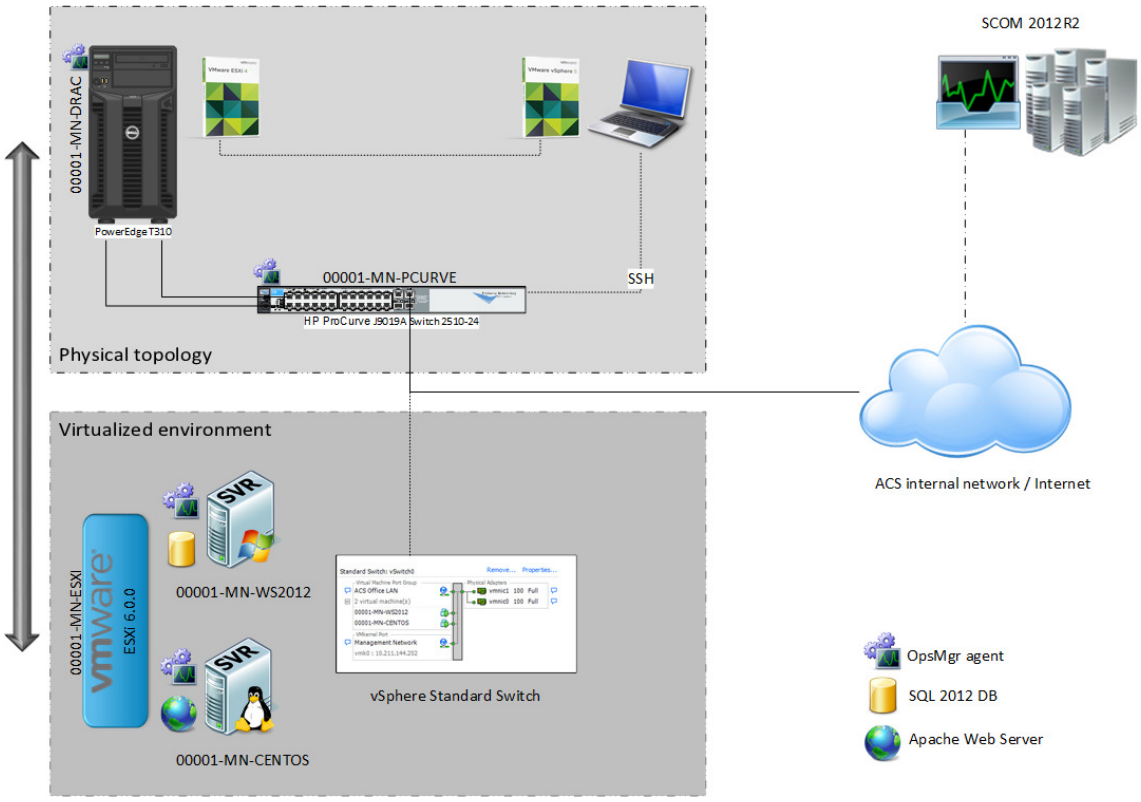
3.4 Testiympäristön kuvaus

Työn tekijällä oli vapaat kädet toteuttaa monitorointitoimintojen testaus eri alustoilla ja laitteilla. Alusta pitäen oli selvää, että Operations Managerin toimintaa tultaisiin tutkimaan Windows-järjestelmien ja erilaisten verkkolaitteiden lisäksi myös Linux-pohjaisella kokoonpanolla, jotta mahdollinen tuotantokäyttöönotto sujuisi jouhevammin näiden osalta. Samalla karttuisi kokemusta huomioonotettavista seikoista monitorointia aloitettaessa ja sen hienosäätämiseksi agentin jo ollessa asennettuna.

Kokeilualustoiksi ja -laitteiksi valikoituivat näillä lähtökohdilla:

- Windows-palvelin (ja SQL-tietokanta)
- Linux-palvelin (ja Apache web-palvelin)
- verkon aktiivilaite (kytkin)
- OOB-hallintalaite (Dell DRAC -järjestelmä).

Testausta varten pystytettiin työn tekijän toimesta yrityksen muusta verkkoinfrastruktuurista erillinen VMware-pohjainen virtualisointiympäristö ”00001-MN-ESXI” (ks. kuva 6), johon sijoitettiin testaukseen käytettävät kaksi virtuaalikonetta (Windows- ja Linux-palvelimet, ”00001-MN-WS2012” ja ”00001-MN-CENTOS”). VMware ESXi 6.0.0-pohjainen hypervisor asennettiin ja konfiguroitiin Dell PowerEdge T310 -rautapalvelimelle (verkkonimi ”00001-MN-DRAC”), joka yhdistettiin testausta varten konfiguroituun HP ProCurve 2510 -malliseen kytkimeen (”00001-MN-PCURVE”). Kytkimeltä oli yhteys yritys A:n sisäverkkoon ja sen palveluihin sekä tarvittaessa myös internetiin.



Kuva 6. Testiympäristö

Fyysinen palvelin otettiin monitoroinnin piiriin sillä sijaitsevan OOB-hallintatoiminnon ”iDRAC6 Express” avulla. DRAC eli ”Dell Remote Access Controller” on laitevalmistaja Dellin kehittämä järjestelmä rautapalvelimien etähallitsemiseen ja monitorointiin käyttöjärjestelmän ulkopuolisena itsenäisenä väylänä. DRAC on monitoroitavissa SNMP:n (Simple Network Management Protocol) välityksellä. Toiminnolle määritettiin kiinteä IP-osoite ja sille annettiin oma verkkonimi ”00001-MN-DRAC” tunnistamisen ja monitoroinnin helpottamiseksi.

VMware ESXi on ns. “bare metal”-tyypin hypervisor, eli virtualisointiympäristöä ajetaan suoraan fyysisen palvelinraudan päällä. ESXi-ympäristölle annettiin oma verkkonimi ”00001-MN-ESXI”, jonka avulla siihen voitiin muodostaa yhteys muilta verkon työasemilta vSphere-konsolilla ja päästä näin hallinnoimaan ympäristössä sijaitsevia virtuaalikoneita. Virtualisointiympäristössä otettiin käyttöön ns. ”NIC teaming” -ominaisuus eli verkkokorttien yhteiskäyttö, jolla kahdennettiin ympäristön verkkoyhteys hyödyntämällä fyysisen palvelimen kumpaakin olemassa olevaa verkkokorttia ja Ethernet-porttia.

Testiympäristöön oli myös olennaista saada käyttöön täysin hallittavissa oleva, muusta verkosta erillinen verkkolaite, jotta voitaisiin tehokkaasti jäljentää erilaisia tilanteita, joissa

kytkimeen tai johonkin sen valvotuista porteista ei saada yhteyttä häiritsemättä muun verkon toimintaa testitoimenpiteiden seurauksena. Kytkimelle ”00001-MN-PCURVE” annettiin riittävä peruskonfiguraatio, jossa muun muassa määritettiin tarpeelliset VLAN-asetukset, asetettiin oletusyhdyskäytävä ja sallittiin SSH-yhteydet kytkimelle. Määritettävänä oli myös käytettävä SNMP-yhteisönimi, jonka avulla verkkolaitetta tultaisiin lopulta monitoroimaan.

Linux-palvelimen ”00001-MN-CENTOS” osalta päädyttiin konfiguraatioon, jossa käyttöjärjestelmänä oli CentOS 6.7 Final, jonka itsensä lisäksi valvottavana kohteena ns. ”LAMP-stack” eli Linuxiin pohjautuva Apachen, PHP:n ja MySQL-tietokannan avulla toteutettu web-palvelin. LAMP:n avulla rakennettiin erittäin yksinkertainen web-sivu monitorointitarkoituksia varten. Palvelimella oli käytettävinä resursseina yksi virtuaalinen CPU, kaksi gigatavua keskusmuistia sekä 40 gigatavua levytilaa.

Windows-palvelimella ”00001-MN-WS2012” oli tiettyjen Windowsin perustoimintojen lisäksi tarkoitus monitoroida MS SQL -palvelinta ja siihen luotua yksinkertaista tietokantaa. Käyttöjärjestelmänä palvelimella olikin Windows Server 2012 R2 Standard -kokeiluversio, ja tietokannan luomiseksi asennettiin ja konfiguroitiin myös kokeiluversio SQL Server 2012 -ohjelmistosta. Palvelimella oli käytettävissä kaksi virtuaalista CPU:ta, neljä gigatavua keskusmuistia sekä 40 gigatavua levytilaa käyttöjärjestelmäasennukselle ja 50 gigatavua tietokannan datalevyksi.

4 Monitorointitoimintojen testaus

4.1 Windows-palvelin

4.1.1 Monitoroinnin aloittaminen

Käyttöjärjestelmän asennuksen, toimialueeseen liittymisen, päivitysten asennuksen ynnä muiden tyypillisten perustoimenpiteiden jälkeen, joita tämän työn puitteissa ei ole tarkoituksenmukaista käydä yksityiskohtaisesti läpi, testipalvelimen 00001-MN-WS2012 käyttöönotto monitorointikokeilua varten jatkui SCOM-agentin asennuksella. Agentin asennukseen Windows-, Unix- ja Linux-järjestelmille on käytettävissä yhteensä kolme eri metodia:

- ns. ”push”-menetelmällä Operations Manager-konsolin kautta Discovery Wizardin avulla

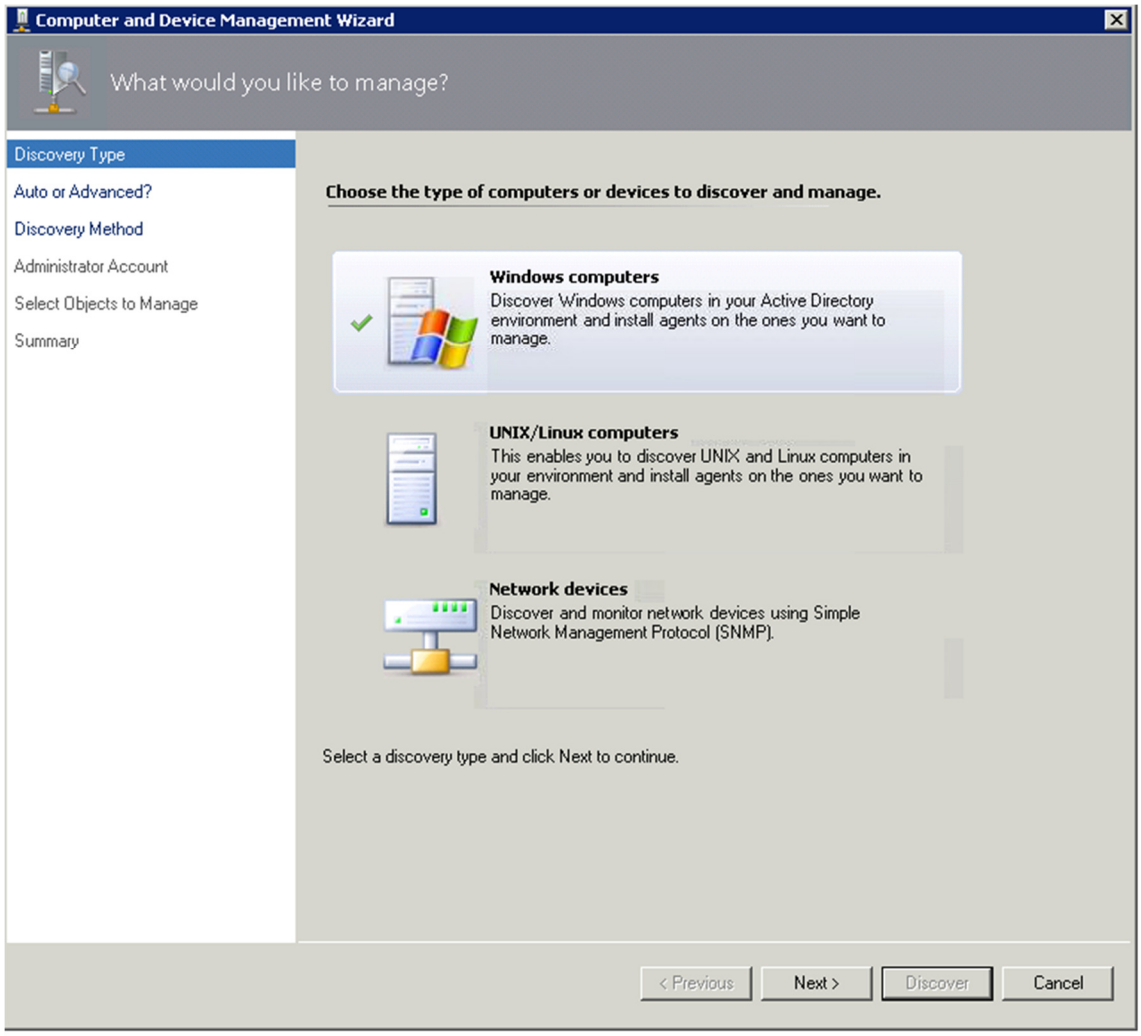
- asennuksen käynnistäminen SCOM 2012 R2-asennusmedialta suoraan kohdekoneella

- asennuksen käynnistäminen komentorivin avulla suoraan kohdekoneella

SCOM-agentti on myös mahdollista ns. paketoida ja sen asennus automatisoida System Center Configuration Manager -ohjelmiston avulla.

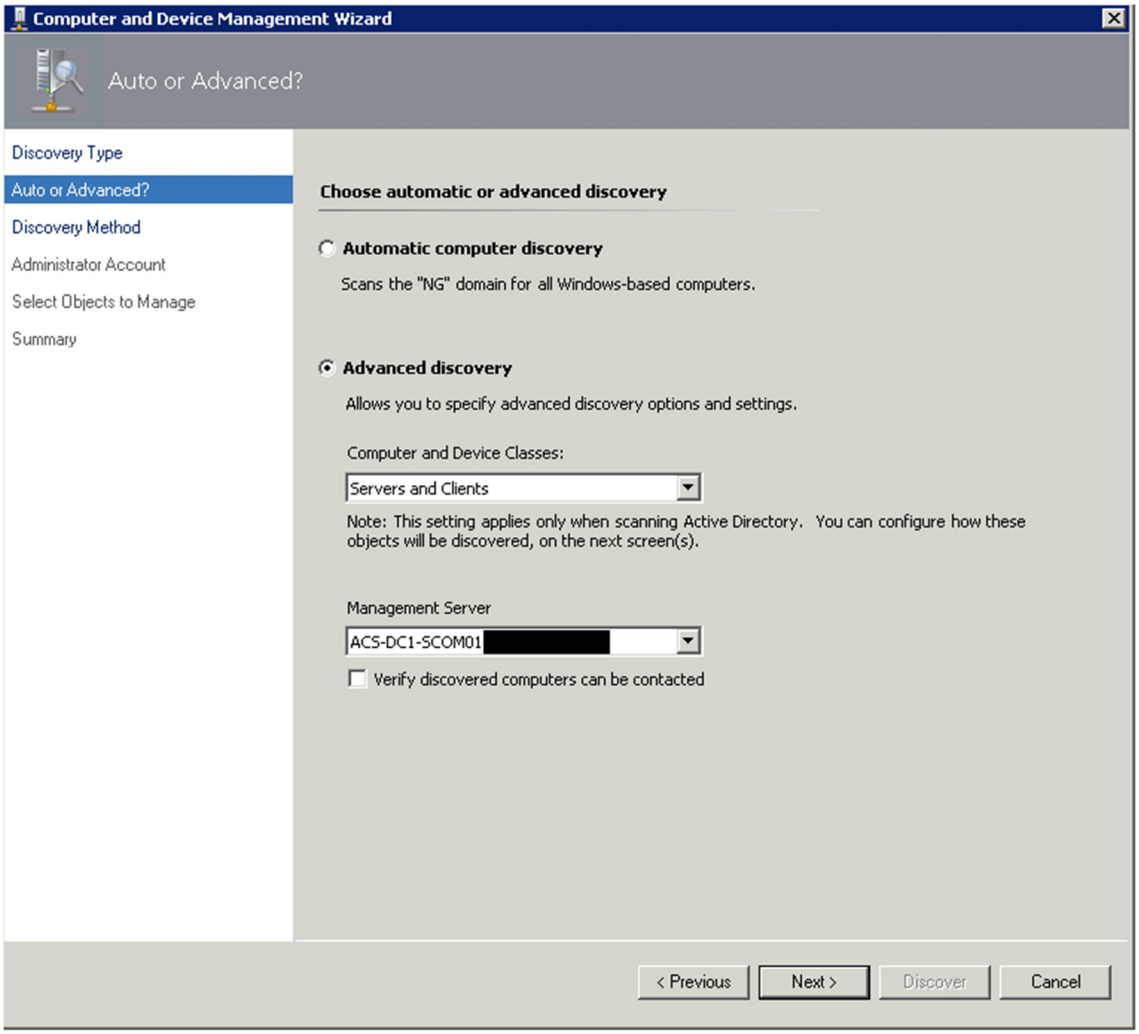
Suositeltavin tapa agenttien asennukseen on sallia tarvittavat tietoliikenneyhteydet asianmukaisiin TCP/UDP-portteihin ja asennus Discovery Wizardin avulla, sillä muilla tavoin käyttöön otettujen SCOM-agenttien versioita ei voi esimerkiksi päivittää suoraan Operations Manager -konsolista käsin, vaan toimenpiteet täytyy näissä tapauksissa suorittaa manuaalisesti suoraan kohdekoneelle kirjautuen.

Agentin asennus aloitetaan käynnistämällä ”Discovery Wizard” (ks. kuva 7) Operations Manager -konsolin ”Administration”-välilehdeltä.



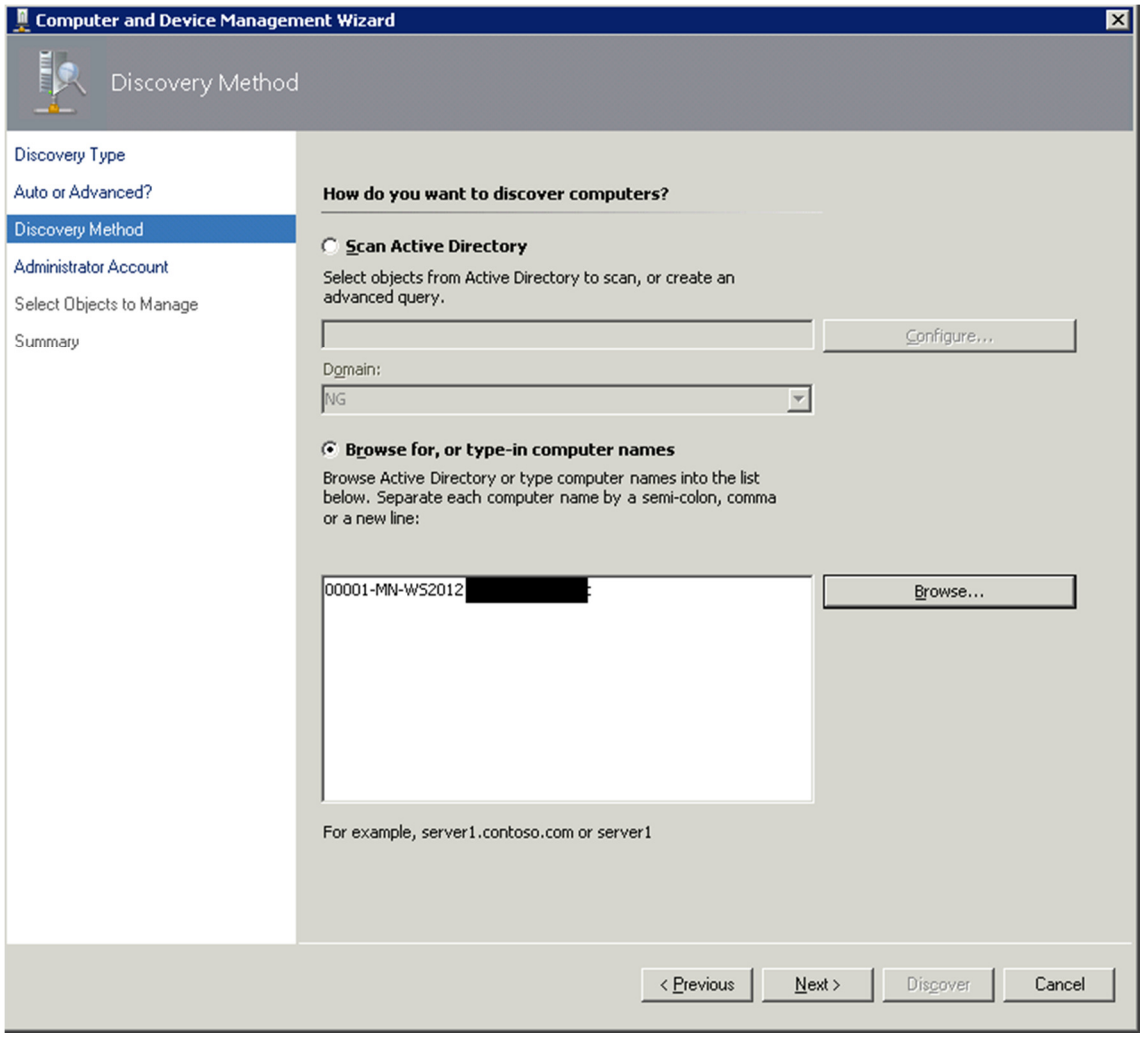
Kuva 7. Valitaan asennusvelhon alussa etsittävän resurssin tyyppi Windows-laitteeksi

Kun asennusvelholle on annettu tieto etsittävän resurssin tyypistä, valitaan resurssin etsimiseen käytettävä menetelmä kuvassa 8 esiintyvistä vaihtoehdoista. Tyypillisimmin valitaan ”advanced”, jolloin kohdejärjestelmät voi määrittää haluamallaan tavalla käsin. Laajassa verkkoympäristössä järjestelmien haku pelkkää domain-nimeä käyttäen palauttaisi hyvin todennäköisesti suuren määrän tarpeettomia hakutuloksia, joten haun tarkentaminen spesifioimalla hakutermit tapauskohtaisesti on suositeltavaa.



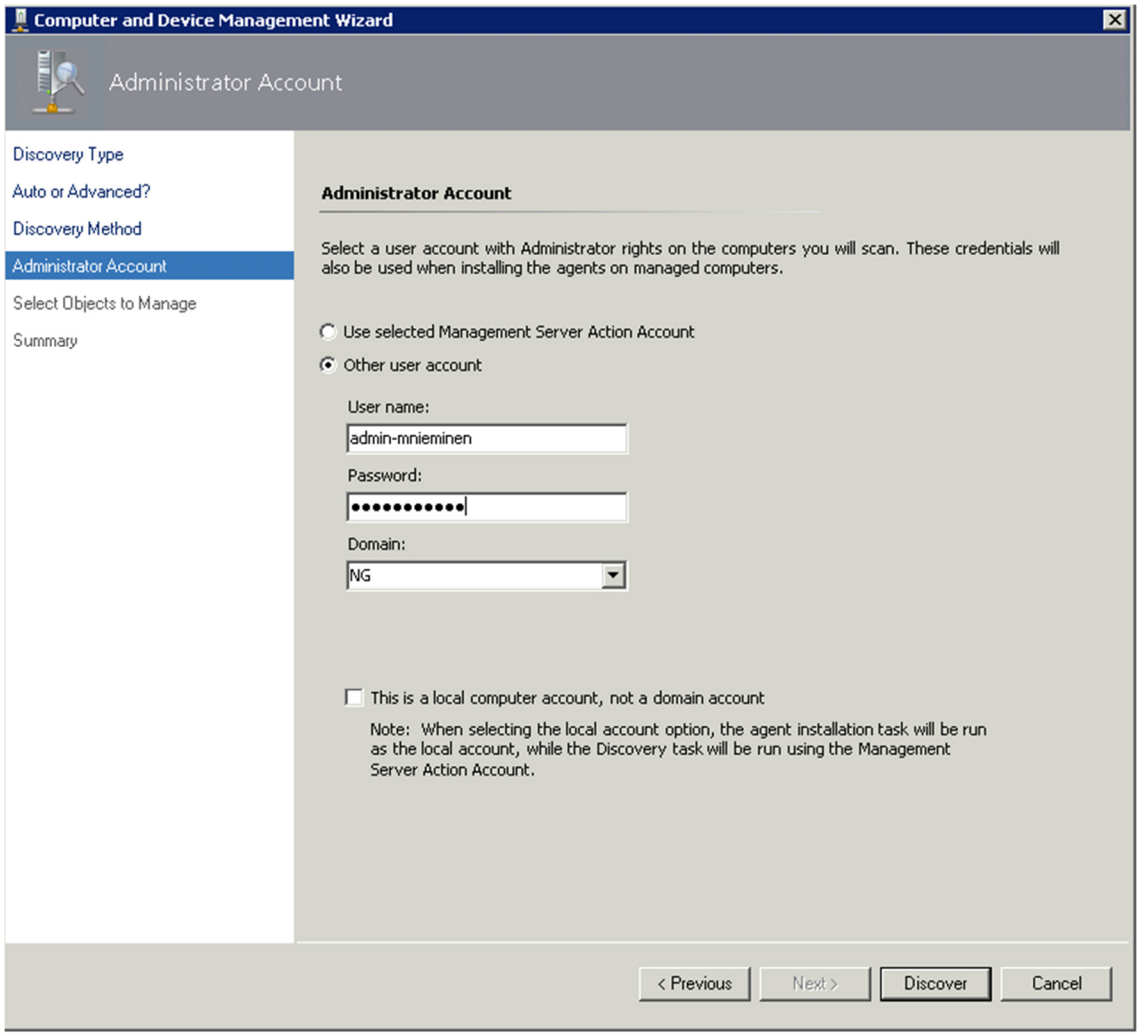
Kuva 8. Resurssienetsintämenetelmän valinta

Seuraavassa vaiheessa (ks. kuva 9) on mahdollista joko määrittää kysely, jonka perusteella asennusvelho hakee AD:sta kaikki käyttäjän antamat ehdot täyttävät koneobjektit agentin asennusta varten, tai vaihtoehtoisesti antaa asennusvelholle yksitellen ne tietokoneiden nimet, joille agentti halutaan asentaa. Mikäli agentteja on asennettavana kerralla vain hillitty määrä kuten tässä tapauksessa, lienee jälkimmäinen vaihtoehto tehokkaampi. Velholle annettiin siis testipalvelimen nimi, ja näin asennusta päästiin jatkamaan.



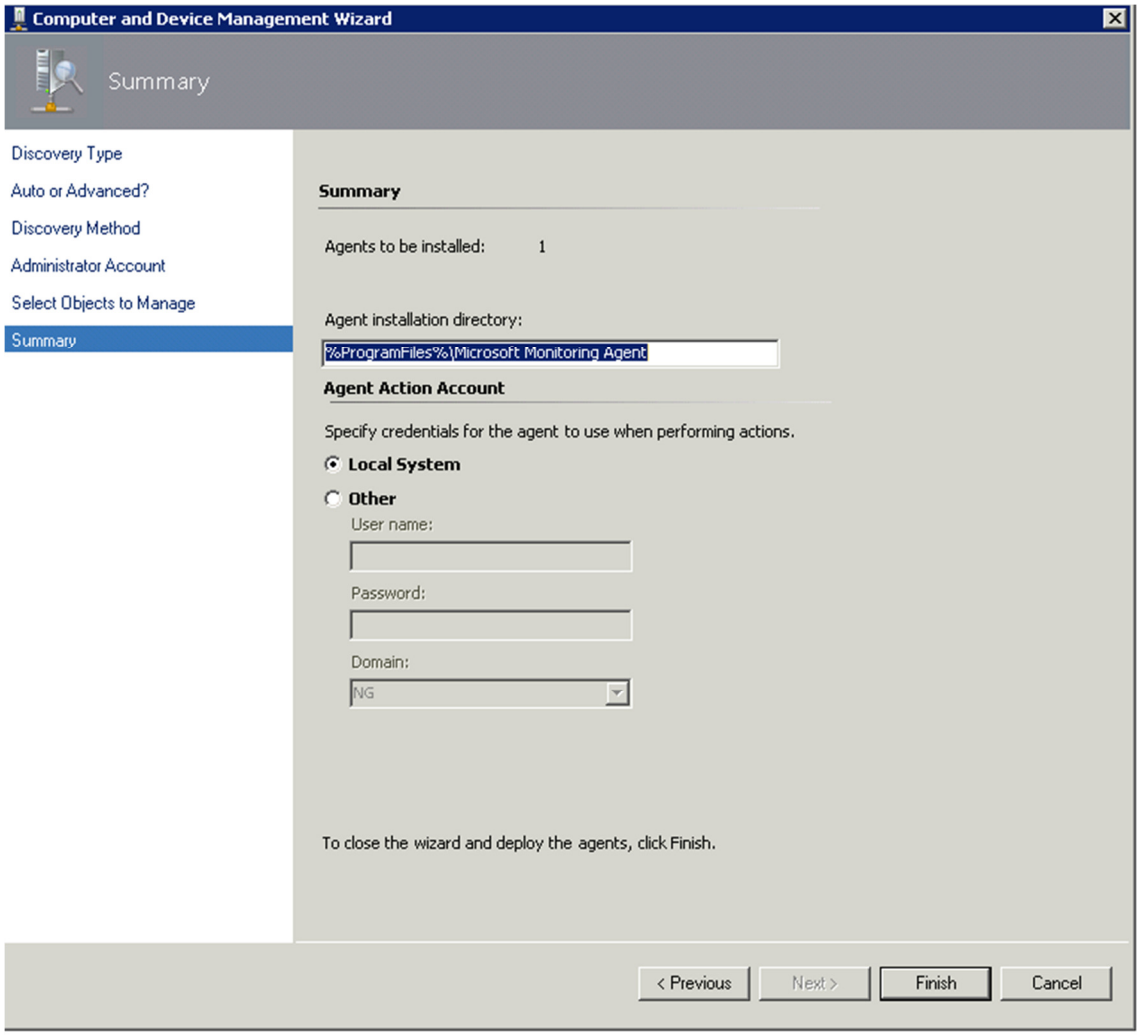
Kuva 9. Asennuskohteen määrittely

Seuraavassa vaiheessa asennusprosessia (ks. kuva 10) asennusvelholle annetaan käyttäjätunnukset, joilla varsinainen agentin asennus loppujen lopuksi suoritetaan. Käytettävillä tunnuksilla tulee olla paikalliset järjestelmänvalvojan oikeudet kohdekoneella, ja toimenpiteeseen voi käyttää SCOM-järjestelmään määritettyä ”Management Server Action Account” -käyttäjätiliä, jos se täyttää nämä vaatimukset, tai vaihtoehtoisesti mitä tahansa muita käyttäjätunnuksia, joilla on vaaditut oikeudet. Tässä esimerkissä syötettiin tekijän omat ylläpidon käyttäjätunnukset.



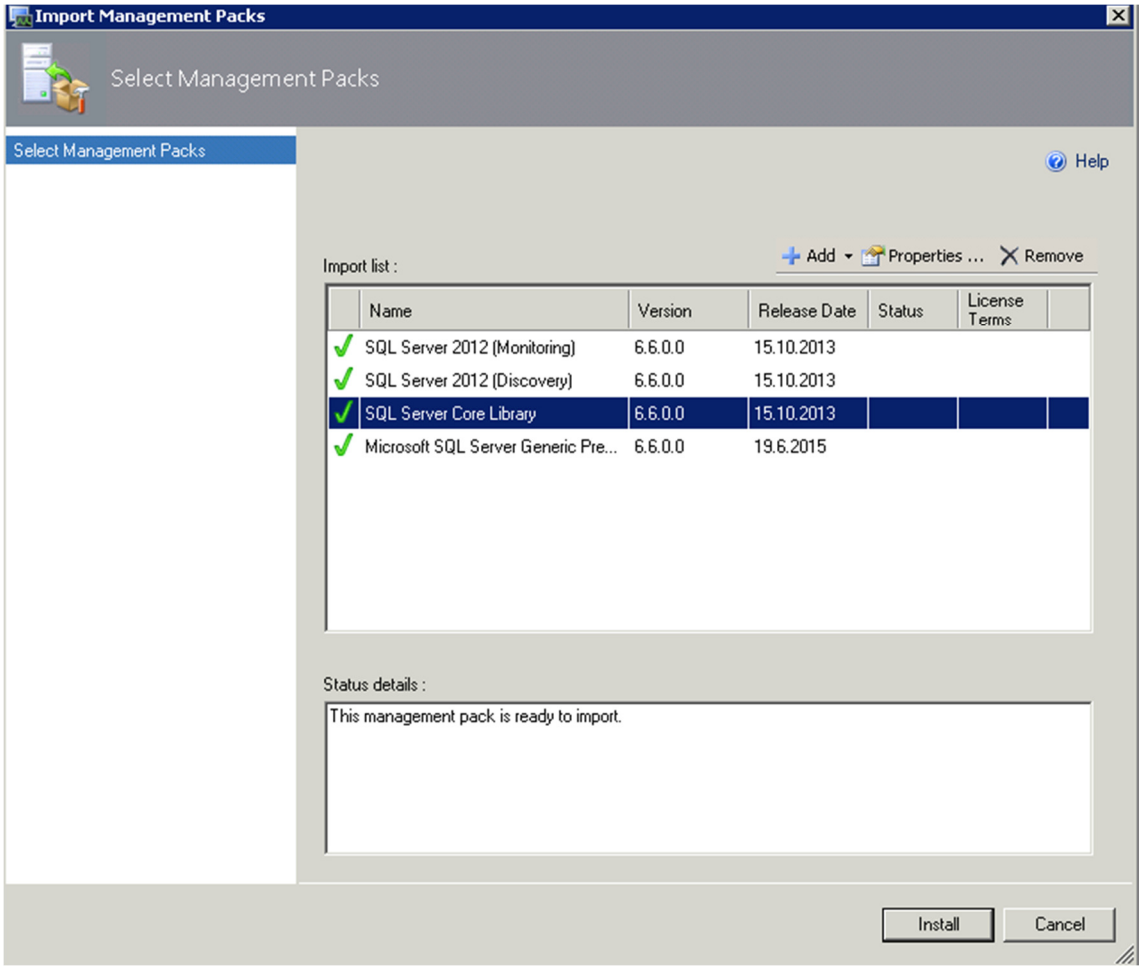
Kuva 10. Asennukseen käytettävän käyttäjätunnuksen määrittely

Painikkeella ”Discover” käynnistetään resurssienetsintä asennusvelholle annettujen tietojen perusteella. ”Select Objects to Manage”-välilehdellä vielä vahvistetaan agentin asennus etsintätoiminnon löytämille järjestelmille, ja ”Summary”-välilehdellä (ks. kuva 11) agentin asennus käynnistetään. Valittavana tässä vaiheessa on vielä agentin asennushakemisto, mikäli siihen on tarpeellista vaikuttaa, ja kohdekoneella käytettävä ”Agent Action Account”. Kuten aiemmin todettua, Windows-järjestelmillä on tyypillistä käyttää tähän tarkoitukseen paikallista järjestelmätiliä (”Local System”), mutta tarpeen mukaan tätä varten voi määrittää jonkin muunkin käyttäjätilin, esimerkiksi tilanteessa jossa järjestelmätilin käyttö on estetty erinäisistä syistä.



Kuva 11. Agentin asennuksen viimeistely

Agentti saatiin asennettua testipalvelimelle onnistuneesti, ja pienen viiveen jälkeen palvelin ilmestyikin näkyviin Operations Manager -konsoliin. Koska tarkoitus oli itse käyttöjärjestelmän lisäksi mahdollistaa myös kohdekoneelle asennetun SQL-palvelimen valvonta, oli tarpeellista tuoda SCOM-ympäristöön SQL Server 2012 -toiminnolle kohdistettu hallintapaketti (ks. kuva 12), joka sisältää SQL-palvelimen monitorointiin räätälöityjä monitoreja, sääntöjä ja komentoja. Hallintapaketin onnistuneen lisäämisen jälkeen SCOM-järjestelmä päivitti luvussa 2.2.4 kuvaillun periaatteen mukaisesti kohteen monitorointilogiikkaa, tunnisti palvelimella asennettuna olevan SQL-palvelimen komponentit ja lisäsi ne monitoroinnin piiriin.

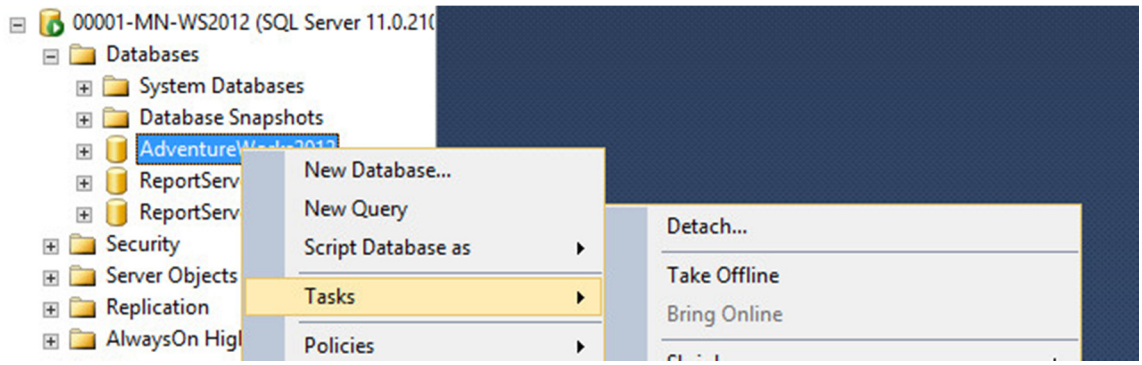


Kuva 12. SQL Server 2012 -hallintapakettien tuominen SCOM-ympäristöön

4.1.2 Testausmenetelmät

Testausprosessi aloitettiin eräällä valvontatoiminnoista eittämättä kriittisimmällä, eli jäljellä olevan vapaan levytilan määrää seuraavan monitorin kokeilulla. Levytilan määrän valvontaan Windows Server 2012- sekä 2012 R2 -käyttöjärjestelmille on käytössä monitori nimeltä ”Windows 2012 Logical Disk Free Space Monitor”, jolla on mahdollista valvoa jäljellä olevaa levytilaa joko säädettävissä olevalla prosentti- tai megatavurajalla. Kohdekoneen järjestelmälevylle luotiin fsutil-sovellusta hyödyntäen ns. ”dummy”-tiedosto, joka pudotti jäljellä olevan levytilan määrän kriittiselle tasolle. Kun havaittiin, että tilanteesta syntyi odotusten mukaisesti hälytys Operations Manager -konsoliin, poistettiin dummy-tiedosto palvelimelta. Hetken päästä järjestelmä sulki aiemmin luomansa hälytyksen havaitessaan, että levytilaa oli palvelimella jälleen riittävästi. Monitorin voitiin todeta toimivan odotetunlaisesti.

SQL-palvelimen valvonnan osalta oli tarkoitus luoda testitarkoituksiin kaksi erilaista vikatilannetta, joista ensimmäisessä valvonnan alainen SQL-testitietokanta siirtyy offline-tilaan, ja toisessa kohdepalvelimen koko ”SQL Server” -palvelu lakkaa vastaamasta. Hyödynnettävinä monitoreina tässä yhteydessä ovat järjestyksessä ”SQL Server 2012 DB” sekä ”SQL Server 2012 DB Engine”. Koe aloitettiin avaamalla kohdepalvelimen SQL-instanssi SQL Server Management Studiolla ja viemällä testitietokanta offline-tilaan kuvan 13 mukaisesti.



Kuva 13. Tietokannan vieminen offline-tilaan

Hetken päästä monitori loi havaitsemastaan häiriöstä hälytyksen, jonka jälkeen tietokanta tuotiin takaisin online-tilaan ja monitorin annettiin sulkea hälytys. Ladattaessa SQL-palvelimien hallintapaketti Operations Manageriin, tulee sen mukana joukko erilaisia ”taskeja” eli agenteilla suoritettavia toimintoja. Tämä mahdollistaa tietokantojen käsittelyn suoraan konsolista käsin, ja tässä tapauksessa tietokanta voitiin palauttaa online-tilaan Operations Manager -konsolin avulla, ilman kohdepalvelimelle tai sen SQL-instanssiin erikseen kirjautumista.

Seuraavaksi luotiin koko SQL-palvelimen kaatumista jäljittelevä tilanne pysäyttämällä koepalvelimen SQL Server -järjestelmäpalvelu. Operations Manager havaitsi tämän ja synnytti aiheesta hälytyksen. Asiaan reagoitiin käynnistämällä kyseinen palvelu uudelleen, ja monitori sulki jälleen luodun hälytyksen.

SQL-palvelimen monitorointitoimintojen voitiin näiden kokeilujen perusteella todeta toimivan odotusten mukaisesti.

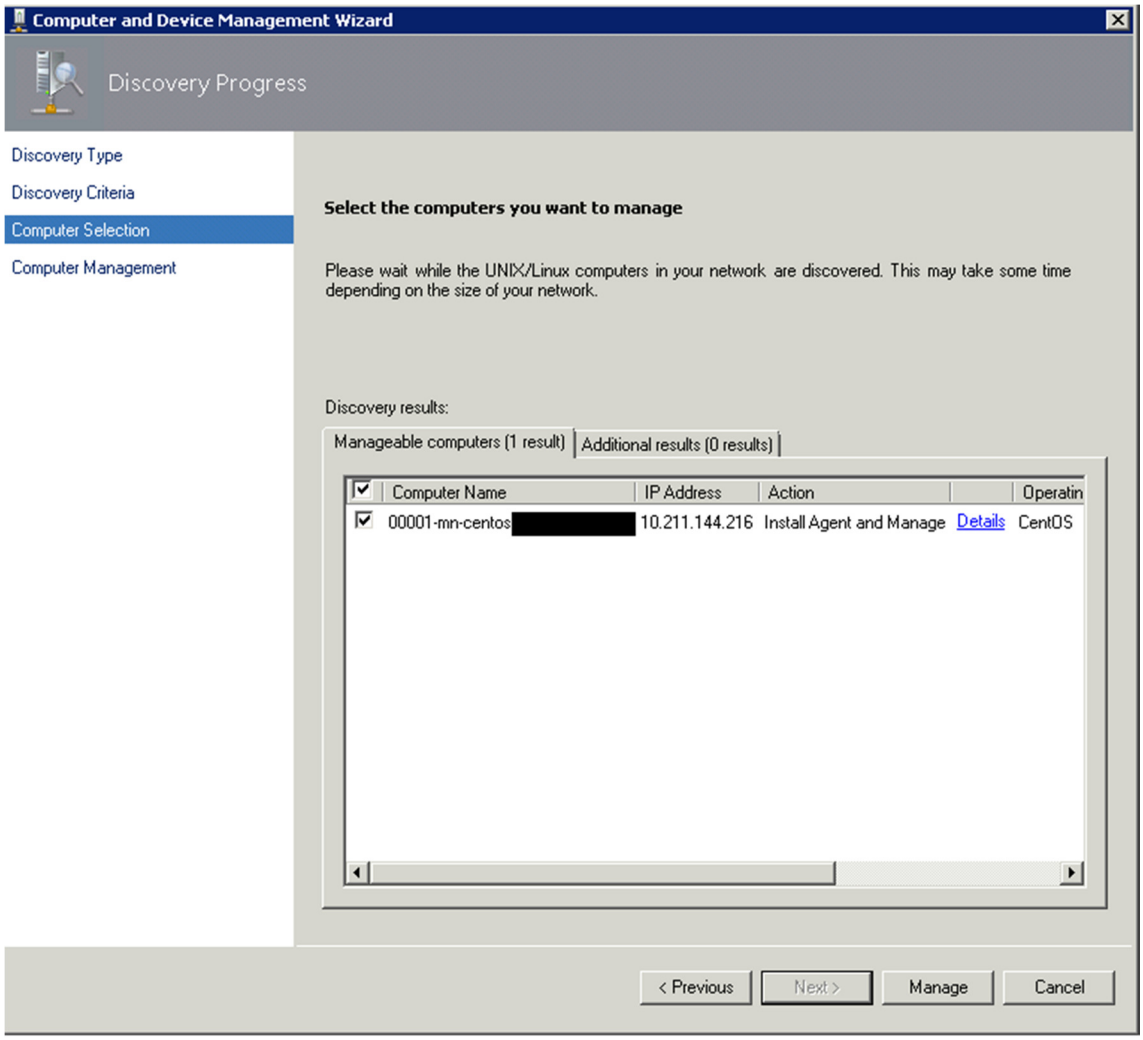
4.2 Linux-palvelin

4.2.1 Monitoroinnin aloittaminen

Kuten Windows-testipalvelimenkin tapauksessa, Linux-järjestelmä oli ennen Operations Manager-agentin asennusta valmiiksi konfiguroitu käyttöjärjestelmän ohella valvottaviksi tarkoitettuine web-palvelimineen. Linuxille SCOM-agentin voi asentaa Windows-järjestelmien tapaan joko resurssienetsintävelhon avulla Operations Manager -konsolista, tai käsiasennuksena komentorivillä. Linux-agenttien asentamiseksi on myös määritettävä tarpeelliset ”Run As” -tilitiedot eli tunnukset, joita käytetään järjestelmien monitorointiin.

Jotta testaukseen käytetty CentOS-versio 6.7 olisi ollut mahdollista tuoda monitoroinnin piiriin, oli myös tarpeellista päivittää Unix- ja Linux-järjestelmien valvontaan käytetyt hallintapaketit, sillä järjestelmän ensiasennuksen mukanaan tuomat MP-versiot eivät riittäneet käyttöjärjestelmän tunnistamiseksi. Tämä onnistui Operations Manager -konsolista samaan tapaan kuin aiemmin läpikäydyssä Windows-esimerkissä SQL-hallintapaketin osalta.

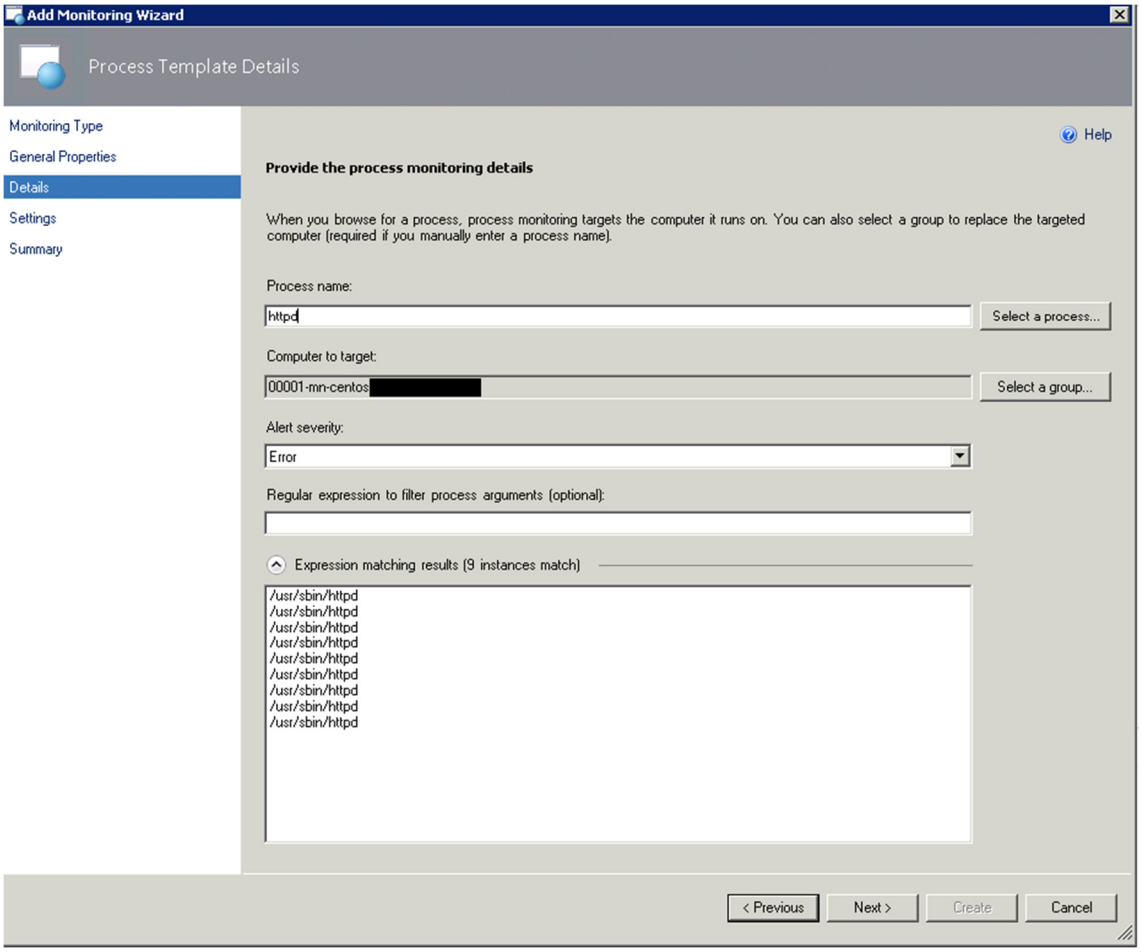
Asennus käynnistetään resurssienetsintävelhon avulla Operations Manager -konsolista samaan tapaan kuin Windows-järjestelmilläkin, valiten velhon alussa etsittävän resurssin tyypiksi Unix- ja Linux-järjestelmät. Etsintävelholle annetaan etsittävän laitteen tai laitteiden verkkonimi. Vaihtoehtoisesti etsintään voi käyttää myös järjestelmän IP-osoitetta. Tarpeellista on myös määrittää käyttäjätunnus, jolla on riittävät oikeudet asentaa agentti kohdejärjestelmälle. Etsintävelholle annetut tiedot laitteiden löytämiseksi pyydetään vielä vahvistamaan, jonka jälkeen ollaan kuvan 14 mukaisessa tilanteessa, ja agentin asennus voidaan käynnistää. Asennus suoritetaan SSH-yhteyden yli eli hyödyntäen TCP-porttia 22. Yhteyksien varmentaminen valvottaville laitteille on toteutettu sertifikaatein. [6, s. 29-30.]



Kuva 14. Linux-agentin asennus

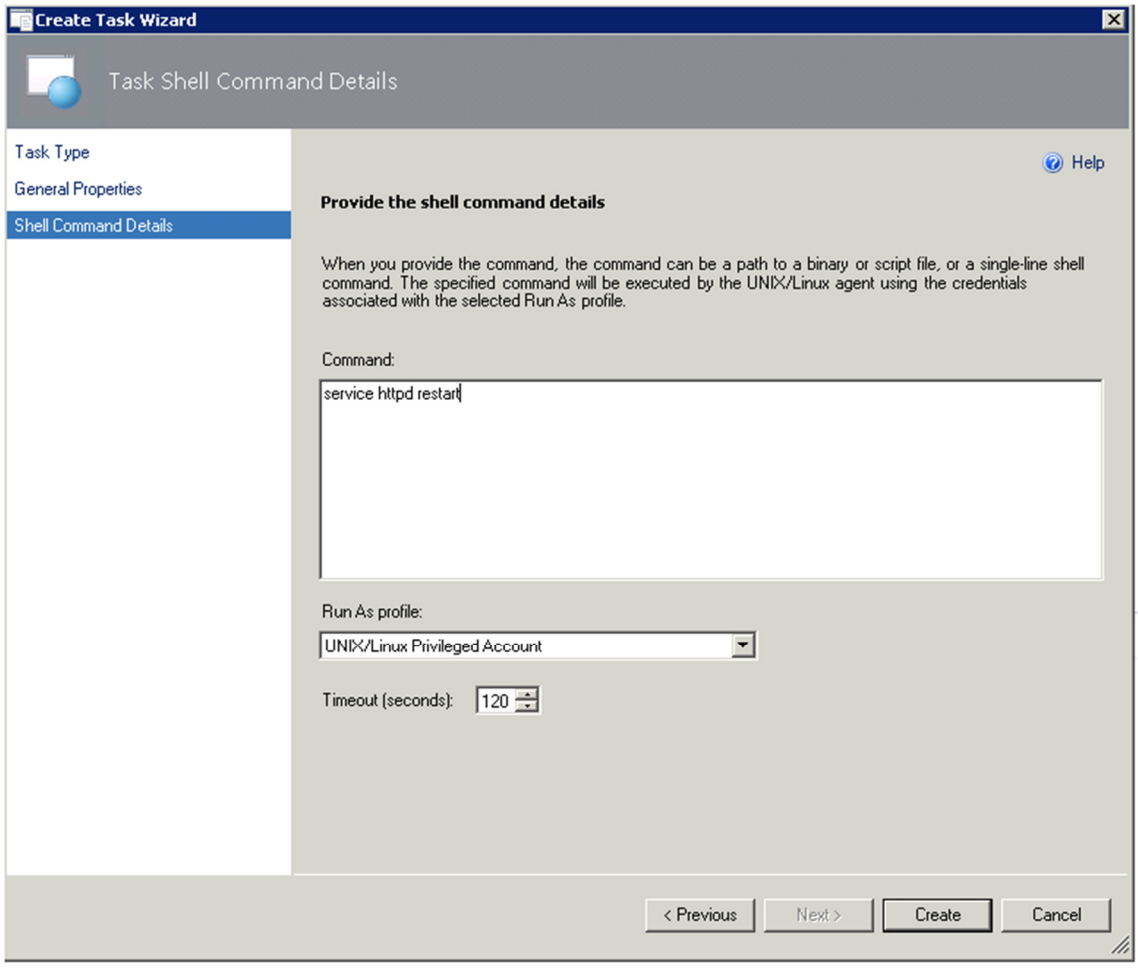
4.2.2 Testausmenetelmät

Web-palvelimen valvontaa varten luotiin Operations Manager -konsoliin tarkoitukselle omistettu, yksinkertainen monitori (ks. kuva 15), joka määritettiin tarkkailemaan CentOS-palvelimella käynnissä olevien ”httpd”-prosessien lukumäärää. Rajaksi asetettiin yksi esiintymä, ja kun tämä alitettaisiin, voitaisiin Apache-palvelimen olettaa olevan jonkinlaisessa häiriötilassa tai kokonaan pysähtynyt.



Kuva 15. Monitorin luominen“httpd”-prosessille

Kun monitori oli luotu, voitiin siirtyä suunnittelemaan testaustoimenpiteitä. Oman monitorin luonnin lisäksi Operations Manager -konsolin ominaisuuksia päätettiin hyödyntää myös luomalla oma “task”, jonka avulla kohdekoneen httpd-daemonin voi käynnistää esimerkiksi mahdollisessa vikatilanteessa uudelleen pelkällä napin painalluksella. Taskin luonti alkoi lisättävän toiminnon nimeämisellä ja kohdehallintapaketin valinnalla. Seuraavaksi valittiin monitori, johon uusi task oli tarkoitus liittää. Tähän käytettiin juuri luotua httpd-monitoria. Lopuksi määritettiin ajettava komento ja annettiin käyttäjätunnukset, joilla kyseinen komento halutaan ajaa kohdekoneella (ks. kuva 16).



Kuva 16. Taskin luonti Linux-agentille

Testitoimenpiteenä Linux-palvelimelle kirjauduttiin root-tunnuksilla, ja lopetettiin “pkill”-komentoa hyödyntäen yhdellä komentorivillä kaikki käynnissä olleet httpd-prosessit. Tästä syntyi hetken päästä hälytys Operations Manager -konsoliin, johon reagoitiin suorittamalla aiemmin konfiguroitu task. Httpd-daemonin käynnistyessä uudelleen taskin suorittamisen yhteydessä tilanne palautui palvelimella normaaliksi, ja asiasta aiemmin syntynyt hälytys sulkeutui monitorin toimesta automaattisesti.

Web-palvelimen testauksen lisäksi Linux-palvelimella päätettiin jäljentää myös tilanne, jossa kohdekoneen CPU-käyttö ylittää normaaliksi määritellyn ylärajan. Tämä toteutettiin käynnistämällä kohdepalvelimella asianmukaisin argumentein “stress”-niminen prosessi, joka nostaa suorittimen tai suorittimien kuormituksen 100 prosenttiin ennalta määritellyksi ajaksi. Havaittuaan tämän normaalista poikkeavan tilanteen loi Operations Manager asiasta hälytyksen monitorin ”Operating System Total Percent Processor Time”

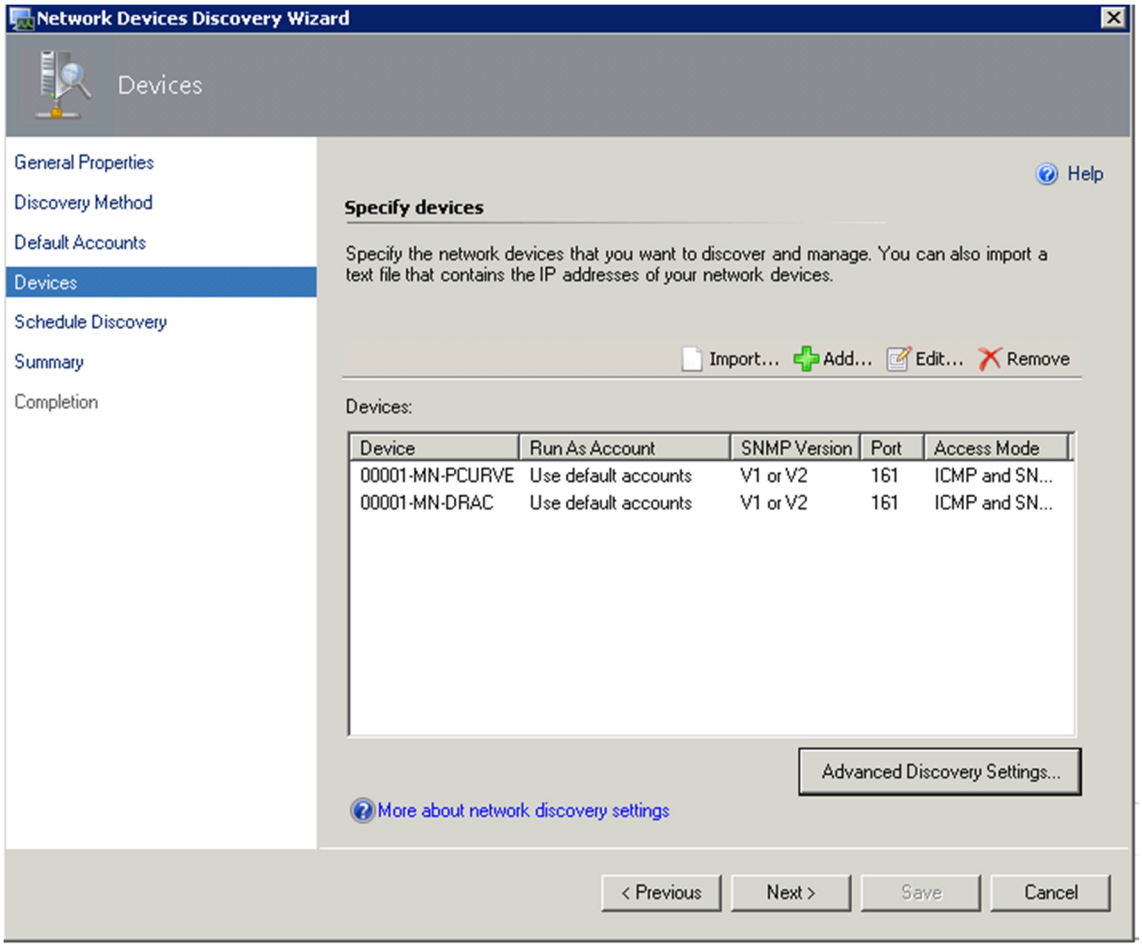
avulla. Kun tämä keinotekoinen kuormitus poistettiin lopettamalla stress-prosessi palvelimella, monitori sulki hälytyksen.

4.3 Verkkolaitteet

4.3.1 Monitoroinnin aloittaminen

Verkkolaitteiden lisäämiseksi monitoroinnin piiriin Operations Managerissa on tarpeellista luoda konsoliin ns. ”discovery rule” eli sääntö, jolla määritetään etsittävät resurssit, niiden hakuväli sekä muut asianmukaiset parametrit. Etsintää varten on käytössä velho, joka käynnistetään konsolin ”Administration”-välilehdeltä ”Network Management” -alaosiosta. Aluksi velholle annetaan luotavan säännön nimi, etsintään käytettävä hallintapalvelin ja resurssivaranto. Seuraavana vaiheena määritetään haun tyyppi, joka voi olla joko eksplisiittinen (säännön avulla etsitään vain erikseen nimettyjä laitteita) tai rekursiivinen, jolloin etsintäsääntö pyrkii löytämään verkosta erikseen määritettyjen lisäksi myös näihin suoraan kytkettynä olevat, varsinaisen haun ulkopuolella olevat verkkolaitteet. Kuten palvelinjärjestelmien haussakin, myös verkkolaitteiden löytämiseksi tarvitaan erityiset ”run as”-tilitiedot, mikä verkkolaitteiden tapauksessa tarkoittaa tiedonhakuun käytettävän SNMP-yhteisönimen tai -nimien antamista (engl. ”community string”). Jotta laitteita voitaisiin valvoa SNMP-protokollan avulla, tulee SNMP-liikenteen olla sallittuna ja SNMP-palvelun käynnistettynä valvottavilla laitteilla. Valvontaan voidaan käyttää myös yksinkertaisia ICMP (ping)-kutsuja, mikäli kohdelaite ei tue SNMP-protokollaa tai sitä ei haluta hyödyntää. Vaihtoehtona on myös näiden kahden valvontatavan yhdistelmä. Testiympäristössä yhteisönimenä oli SNMP:n käyttämä vakio eli ”public” ja sen avulla laitteisiin oli vähintään lukuoikeudet.

Velholle annetaan valvottavien laitteiden DNS-nimet (tai IP-osoitteet), SNMP-versio, valvontatapa ja käytettävä UDP-portti (ks. kuva 17). Tietojen antamisen jälkeen määritetään etsintäsäännön käynnistysväli, joka oletusarvoisesti on asetettu tapahtuvaksi kerran viikossa. Automaattisen haun voi myös kytkeä pois päältä, jolloin etsinnän voi ajaa manuaalisesti haluaminaan ajankohtina tarpeen mukaan. Säännön luonnin jälkeen etsintä suoritetaan ensimmäisen kerran, ja löydettävissä olevat verkkolaitteet tulevat pikapuoliin näkyviin Operations Manager -konsoliin.



Kuva 17. Verkkolaitteiden etsintävelho

4.3.2 Testausmenetelmät

Tarkoituksena oli tutkia monitoroinnin toimintaa tilanteessa, jossa valvonnan alaiselta kytkimeltä ”00001-MN-PCURVE” poistuu käytöstä monitoroitu kytkinportti ja tämän myötä kyseisen portin takana sijaitseva, niin ikään monitoroinnin piirissä oleva laite (testiympäristön fyysinen palvelin ”00001-MN-DRAC”). Kuten jo testiympäristön kuvauksessa mainittiin palvelimen kaksi 1000Base-T -luokan verkkokorttia oli asetettu yhteiskäyttöisiksi, jolloin verkkoyhteydet virtualisointiympäristön testipalvelimiin eivät häiriintyneet yksittäisen verkkoportin toimimattomuudesta. Testitoimenpiteiden aikana yhteyskatkoista kärsi siis vain DRAC-järjestelmä, joka oli määritetty vastaamaan kutsuihin vain tämän kyseisen verkkokortin saamaa IP-osoitetta käyttäen. Häiriö jäljennettiin kahdella eri tavalla, joista ensimmäinen toteutettiin kirjautumalla kytkimelle sisään SSH-yhteyden yli, siirtymällä konfiguraatiotilaan ja yksinkertaisesti poistamalla käytöstä (komennolla ”disable”) ethernet-portti numero 1. Toisessa testitilanteessa jäljiteltiin kytkinportin ja/tai

verkkokaapelin fyysistä rikkoutumista irrottamalla toimenpiteen kohteena olleeseen ethernet-porttiin kytkettynä ollut verkkokaapeli.

Testitoimenpiteistä aiheutui Operations Manageriin ennakko-odotusten mukaisesti hälytykset, yksi kytkinportin verkosta poistumisen yhteydessä monitorin ”Interface Status” toimesta ja toinen DRAC-järjestelmän tavoittamattomuuden johdosta, tässä tapauksessa synnyttäjänä monitori nimeltä ”Network Device Responsiveness”. Palauttamalla valvottu kytkinportti käyttöön, joko kytkimen konfiguraatiotilasta käsin (”enable”-komennolla) tai kytkemällä jälkimmäisessä testitilanteessa irrotettu verkkokaapeli takaisin porttiin, hälytykset sulkeutuivat asianmukaisten monitorien havaitessa tilanteen normalisoituneen.

5 Tuotantokäyttöönotto

Kun erilaiset monitorointitoiminnot oli saatu testatuiksi edellisessä luvussa kuvailtujen toimenpiteiden mukaisesti, oli aika ryhtyä näistä saatuja havaintoja hyödyntäen toteuttamaan monitorointia tuotantoympäristössä. Tähän kuului SCOM-agenttien asentaminen valvottaville palvelinjärjestelmille ja monitoroinnin piiriin otettavien verkkolaitteiden sisällyttäminen asianmukaiseen etsintäsääntöön, tarvittavien hallintapakettien tuonti Operations Manageriin sekä niiden sisältämien sääntöjen ja monitorien muokkaus tarpeiden mukaan, hälytysten konfiguroiminen, Operations Manager -konsolin räätälöiminen eri tavoin ja lopuksi monitorointijärjestelmän dokumentoiminen ylläpitotoimien ja vikatilanteista palautumisen helpottamiseksi tulevaisuudessa.

5.1 Agenttien asennus palvelimille ja verkkolaitteiden haku

Monitorointiagentit valvottaville Windows-järjestelmille asennettiin suurimmilta osin push-menetelmällä, eli suoraan Operations Manager-konsolista asennusvelholla. Kaikissa tapauksissa kohdejärjestelmällä vallinnut palomuurikonfiguraatio ei tätä sallinut erinäisistä syistä. Tällöin vaihtoehtona oli aiemmin todetun mukaisesti agentin asennus manuaalisesti kohdepalvelimelta käsin Operation Manager-asennusmedian avulla, jolloin palomuuriin tarvittiin avaus vain TCP-portille 5723, jonka kautta agentit kommunikoivat hallintapalvelimensa kanssa.

Valvonnan piiriin otettavilla verkkolaitteilla varmistettiin käytössä oleva SNMP-yhteisönimi ja muut tarpeelliset tiedot, jonka jälkeen laitteet voitiin lisätä käytettävään resurssienetsintäsääntöön. Etsintäsäännön ajointervalli jätettiin vakioarvoonsa, eli verkkolaitteiden etsintä tapahtuu automaattisesti kerran viikossa, muina aikoina tarpeen mukaan (esimerkiksi uusia laitteita sääntöön lisättäessä tai tarpeettomia siitä poistettaessa) käynnistämällä toimenpide manuaalisesti Operations Manager -konsolista käsin.

5.2 Hallintapaketit

5.2.1 Valinta ja tuominen Operations Manageriin

Käytettävät hallintapaketit valittiin aiemmin esiteltyjen valvonnan piiriin otettavien kohteiden ominaisuuksien mukaisesti. Microsoft tarjoaa hallintapaketteja suurimmalle osalle itse kehittämistään tuotteista ja toiminnoista, ja nämä ovat lisättävissä Operations Manageriin suoraan verkkokatalogin kautta hakemalla ja asentamalla. Käytössä oleville kolmannen osapuolen palvelinjärjestelmille ja sovelluksille voi itse kehittäjän tai käyttäjäyhteisön toimesta olla saatavilla joko veloituksettomia tai maksullisia hallintapaketteja. Nämä täytyy tuoda SCOM-ympäristöön manuaalisesti. Kullekin valvottavalle toiminnolle pohdittiin tapauskohtaisesti parhaat lähestymistavat, ja tarvittavat hallintapaketit tuotiin ympäristöön.

5.2.2 Luonti ja muokkaus

Ladatut hallintapaketit ovat käytännössä täysin käyttövalmiita sellaisinaan, ja Operations Manager päivittää itsenäisesti monitorointilogiikkaansa aina uuden hallintapaketin läsnäolon havaitessaan. Järjestelmä ryhtyy täysin automaattisesti valvomaan kohdekoneilta paikantamiaan hallintapakettien sisältöön täsmääviä kohteita. Hallintapakettien sisältämien monitorien ja sääntöjen oletusmäärittelyissä voi kuitenkin useimmissa sovellutuksissa ilmetä parantamisen varaa, kunkin valvottavan ympäristön tarpeiden mukaisesti. Tiettyjen hallintapakettien kohdalla niiden tuloksellinen käyttö voi edellyttää jo lähtökohtaisesti muutoksien tekemistä pakettien sisältöön, sillä jossain tapauksissa osa hallintapaketin sisältämistä monitoreista tai säännöistä ei välttämättä ole hallintapaketin tuonnin jälkeen automaattisesti käytössä.

Hyvänä käytännön esimerkkinä voidaan mainita Windows Server 2012 R2 -käyttöjärjestelmän monitorointiin omistettuun hallintapakettiin sisältyvät, vapaan levytilan valvontaan käytettävät monitorit ”Windows Server 2012 Logical Disk Free Space (MB) Low”, ”Logical Disk Free Space” sekä ”Windows Server 2012 Logical Disk Free Space (%) Low”, jotka eivät oletusarvoisesti ole aktiivisina, vaan ne täytyy ottaa käyttöön luomalla kullekin monitorille ns. ”override” eli ohitus, jolla monitorin valmiit oletusarvot korvataan uusilla. Kyseisten monitorien käyttämät prosentti- ja megatavurajat kriittisen levytilan määrittämiseen ovat myös todennäköisesti liian alhaiset useimpiin sovellutuksiin, ja näihinkin voi mahdollisesti olla tarvetta puuttua samassa yhteydessä. Mainitut monitorit otettiin käyttöön tässäkin verkkoympäristössä näitä ohituksia hyödyntäen.

Parhaana käytäntönä ohitusten parissa toimiessa on aina luoda ohituksia varten tarkoitukselle omistettu, erillinen hallintapaketti, joka sisältää nämä manuaalisesti muutetut arvot. Kuten jo aiemmin luvussa 2.2.4 todettiin, suurin osa laitevalmistajien tarjoamista hallintapaketeista on ns. sinetöityjä, joihin käyttäjä ei edes voi itse laatimiaan muutoksia tallentaa. Ohitusten kohteen voi rajata yksittäisen objektin tasolle, objektiluokaksi (jolloin kaikki monitoroinnin piirissä olevat, kuvaukseen täsmäävät objektit ovat ohituksen alaisuudessa) tai halutut objektit sisältäväksi ryhmäksi. [2, s. 207.]

5.3 Hälytysten konfigurointi

Erilaisten sääntöjen ja monitorien luomien hälytysten lähettämiseen ulos Operations Manager -järjestelmästä on saatavilla useita eri tapoja. Käytettävissä on SMTP-kanava ilmoitusten välittämiseen sähköpostitse, IM (Instant Message)-kanava, SMS- eli tekstiviestikanava ja komentokanava, jolla mahdollistetaan jonkin tietyn komennon suorittaminen automaattisesti aina hälytysten aktivoituessa. Sähköposti-ilmoitusten konfiguroiminen vaatii käytettävissä olevan sähköpostipalvelimen, joka sallii viestien välittämisen joko anonyyminä tai autentikoituna. Tekstiviesti-ilmoitusten mahdollistaminen vaatii hallintapalvelimen käyttöön modeemin, joka tukee SMS PDU (Packet Data Unit) -muotoisten viestien lähettämistä, ja pikaviesti-ilmoituksia käyttöönotettaessa vaaditaan jokin käytettävissä oleva pikaviestipalvelu, esimerkiksi Microsoft Lync. Määritettävänä on myös ilmoitusten saaja tai saajat, ne hälytystyypit joista ilmoituksia halutaan vastaanottaa sekä kellonajat, jolloin ilmoituskanavan on oltava aktiivinen. [5, s. 773-783.]

Lähtökohtaisesti ilmoitusten toimitustavaksi valittiin ainoastaan SMTP-kanava. Sähköpostiviestien välittäjänä toimii yrityksen käyttämä Microsoft Exchange 2013 -sähköpostipalvelu. Järjestelmästä lähtevien sähköpostien vastaanottajaksi määritettiin yrityksen Service Desk, joka reagoi viesteihin asianmukaisella tavalla, hälytysten sisällöstä riippuen joko tarttuen vikatilanteisiin itse tai tarvittaessa ohjaten pyynnöt eteenpäin, kulloinkin kyseessä olevalle asianmukaiselle taholle.

5.4 Konsolinäkymien luonti

Valmiiksi olemassa olevien erityyppisten ja -sisältöisten konsolinäkymien lisäksi Operations Managerin käyttäjillä on mahdollisuus luoda omien tarpeidensa mukaan räätälöityjä näkymiä, esimerkiksi juuri tietyntyyppisten hälytysten sisältöön tai vaikkapa halutulla tavalla rajattuun laiteinventaarioon. Näkymien luonti tapahtuu konsolin ”My Workspace” -välilehdellä, ja käytettävissä on lukuisia eri näkymätyyppejä, joita voi esittää ruudulla yhdenaikaisesti useita. My Workspace -työtila on käyttäjäkohtainen, eli kullakin konsolin käyttäjällä on mahdollisuus omien, personoitujen näkymiensä luontiin. [5, s. 719.]

Hyödyllisten lisänäkymien tarve yritys A:n ympäristössä tulee epäilemättä tarkentumaan lopullisesti vasta, kun uuden konsolin käyttöönotosta on ehtinyt kulua aikaa, ja sen käyttö sekä tarjoamat mahdollisuudet ovat tulleet sen operaattoreille syvemmin tutuiksi. Operations Manager-konsoliin luotiin harjoittelumielessä ”General status dashboard” -niminen koontinäyttö, joka sisältää kullakin hetkellä avoinna olevat sekä suljetut hälytykset, ja palvelinten sekä verkkolaitteiden senhetkisen terveystilan. Tämän näkymän avulla konsolin käyttäjä saa nopeasti hyvän yleiskatsauksen verkkoympäristön tilanteeseen ja voi mahdollisen ongelmatekijän havaitessaan ryhtyä tarvittaviin korjaustoimenpiteisiin.

5.5 Dokumentointi

Uudesta SCOM-järjestelmästä laadittiin yrityksen sisäiseen wikipalveluun tarkoitukselle omistettu tukisivu, joka sisältää palvelun ja ympäristön kuvauksen sekä myös ohjeita muille ylläpitäjille ja tukihenkilöille tyypillisimpien päivittäistoimintojen suorittamiseen, kuten esimerkiksi järjestelmän synnyttämiin hälytyksiin reagoimiseen, uusien agenttien asennukseen ym. Wiki pyritään pitämään aina ajan tasalla mahdollisista ympäristöön

tehtävistä muutoksista ja muista havainnoista. Järjestelmän ydinkomponentit ja tärkeimmät yhteydet eri aliverkkoihin ja VLAN:hin havainnollistettiin myös laatimalla Microsoft Visio -sovellusta hyödyntäen ympäristöstä graafinen dokumentti, jota niin ikään tullaan päivittämään mahdollisten muutosten tai päivitysten tapahtuessa.

5.6 Ylläpito ja vikatilanteista palautuminen

Päivitysten asentaminen SCOM-järjestelmään tullaan hoitamaan palvelinjärjestelmille käytössä olevien parhaiden käytäntöjen mukaisesti. Samalla pyritään järjestelmän käyttämättömyysajan minimoimiseen ja yleisesti välttämään sen toiminnan häiriintymistä. Toimenpiteet tulee suunnitella huolellisesti, sillä tyypilliset UR (Update Rollup) -kokonaisuudet edellyttävät varsinaisten päivitysten asentamisen lisäksi useimmiten myös tiettyjen SQL-skriptien ajamista Operations Managerin tietokantoja vasten. Palvelimelle asennettavien päivitysten yhteydessä tulee huolehtia myös varsinaisten agenttien versiopäivityksistä. Mikäli agentti on asennettu Operations Manager-konsolista push-menetelmällä, ja vallitseva palomuurikonfiguraatio edelleen sallii tämän, voi agentin päivittää samalla toimintamallilla konsolista käsin päivitysvelhon avulla. Agentin ollessa manuaalisesti asennettuna kohdekoneelle Operations Manager -asennusmedian avulla, tai push-menetelmän vaatimien asianmukaisten TCP-porttien ollessa suljettuna, tulee myös agentin päivitykset asentaa käsin kohdekoneelle.

Järjestelmän sisältämien palvelinkoneiden ja tietokantojen varmuuskopioinnista tullaan huolehtimaan käytössä olevaa System Center Data Protection Manager 2012 -sovellusta hyödyntäen. DPM-järjestelmä hyödyntää VSS (Volume Shadow Copy) -teknologiaa ja sen avulla mahdollistetaan lähes jatkuvalla tasolla tapahtuva datan suojelu sekä palautus. DPM:n toimintalogiikka muistuttaa hieman SCOM:n vastaavaa, eli varmuuskopioitaville laitteille asennetaan toiminnoista huolehtiva agentti, joka kommunikoi keskitetyn hallintapalvelimen kanssa ja huolehtii varmuuskopioinnin toteutumisesta määritettyinä aikoina. Varmuuskopioinnin tyyppi ja sen kohteet konfiguroidaan DPM-järjestelmän hallintakonsolista käsin. [1, s. 55.]

6 Yhteenveto

Työn tavoitteena oli toimivan, modernin ja hyvin dokumentoidun monitorointiratkaisun konfiguroiminen yritys A:n käyttämään verkkoympäristöön. Tavoitteen voidaan työn tuloksien perusteella todeta täyttyneen erinomaisesti. Uusi monitorointijärjestelmä on jo osoittanut tehokkuutensa ja monikäyttöisyytensä useissa yhteyksissä ja on helpottanut vikatilanteiden ehkäisyä ja niihin reagoimista häiriöiden sattuessa. Järjestelmän avulla valvottavista kohteista on saatavissa runsaasti erityyppistä tietoa useita eri käyttötarkoituksia varten. Monitoroinnin skaalan laajentamiselle jatkossa on saavutettu hyvä pohja, ja varsinaiseen SCOM-palvelinarkkitehtuuriin on helposti lisättävissä kapasiteettia, jos tarve niin vaatii. Työssä kuvaillusta testausprosessista saatiin runsaasti erittäin käyttökelpoisia havaintoja, jotka olivat hyvin sovellettavissa todellisiin palvelinjärjestelmiin varsinaisen tuotantoympäristön valvontaa suunniteltaessa ja sitä toteutettaessa. Uusi SCOM 2012 R2 -järjestelmä tulee epäilemättä tuottamaan projektin toimeksiantajalle runsaasti lisäarvoa palveluiden saatavuuden valvontaan tulevaisuudessa.

Työtä aloitettaessa Microsoftin System Center -tuoteperhe oli tekijälle jo entuudestaan hyvinkin tuttu tietyiltä osin, palvelinjärjestelmien ylläpidosta saadun aiemman työkokemuksen sekä aihepiiriin liittyvien opintojen pohjalta. Sen sijaan tässä työssä hyödynnetty SCOM-järjestelmä ja siihen liittyvät käsitteet olivat tulleet tutuiksi vain kohtuullisen pintapuolisella tasolla. Projektin edetessä tieto ja ymmärrys kyseisen monitorointiratkaisun parissa työskentelemisestä karttui kuitenkin huomattavasti. Insinöörityön aiheena uuden monitorointijärjestelmän käyttöönotto oli erittäin antoisa, ja se avasi kokonaan uusia näkökulmia erilaisten verkkoympäristöjen valvontaan. Tekijän perehtyminen aihepiiriin jatkuu edelleen päivittäin työtehtävien ohella sekä niiden puitteissa.

Lähteet

1 Tulloch et al. Introducing System Center 2012 R2, Technical Overview. 2013. E-kirja. Microsoft.

2 Cornelissen et al. 2013. Mastering System Center 2012 Operations Manager. John Wiley & Sons.

3 Savage, Daniel. Microsoft System Center 2012 Operations Manager – An Overview of What's New. Verkkodokumentti. <https://channel9.msdn.com/Events/TechEd/Europe/2012/MGT301>. 27.6.2012. Luettu 16.10.2015.

4 Ricks et al. Key Concepts for System Center 2012 – Operations Manager. 2013. E-kirja. Microsoft.

5 Ricks, Byron. System Center 2012 R2 Operations Manager Documentation. 2013. E-kirja. Microsoft.

6 Ricks, Byron. Operations Guide for System Center 2012 – Operations Manager. 2013. E-kirja. Microsoft.