Simo Saaranen, Mikko Jänkälä

Palvelinvalvonnan automatisointi

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

30.11.2012

Metropolia

Tekijät Otsikko Sivumäärä Aika	Simo Saaranen, Mikko Jänkälä Palvelinvalvonnan automatisointi 51 sivua + 2 liitettä 30.11.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Janne Salonen, Yliopettaja Timo Juselius, Palvelupäällikkö

Palvelinvalvonta on oleellinen ja tärkeä osa palvelimien ja palvelinympäristöjen ylläpidon kannalta. Sen avulla voidaan taata palvelimien jatkuva toimivuus. Lisäksi valvonta ennaltaehkäisee virhetilanteita sekä estää palvelimen mahdollisen vioittumisen. Valvonta on yleensä palvelu, ohjelma tai toimintatapa, jonka avulla palvelimia ja resursseja seurataan reaaliaikaisesti.

Tämän insinöörityön tarkoituksena oli toteuttaa osittain automatisoitu palvelinvalvontajärjestelmä sekä keskitetty päivitysten jakelu asiakaslaitteille. Insinöörityö suunniteltiin ja tehtiin projektina Academica Oy:n pyynnöstä. Valvontajärjestelmä rakennettiin yrityksessä olemassa olevalla Symantec Management Platform -alustalla.

Järjestelmän toteutus tapahtui kokonaisuudessaan Symantec Management Platform -alustan ominaisuuksia hyödyntäen. Toteutettu palvelinvalvontajärjestelmä on suunniteltu, toteutettu ja testattu huolellisesti insinöörityöntekijöiden toimesta. Saimme projektin aikana aktiivisesti tukea Academica Oy:n vakituiselta henkilöstöltä. Lisäksi järjestelmä testattiin ja hyväksyttiin yrityksen toimesta.

Työn alussa käydään läpi palvelinvalvonnan ja Symantec Management Platform -alustan teorian tärkeimmät ja keskeisimmät aiheet. Teorian jälkeen esitellään, miten palvelinvalvontajärjestelmä on käytännössä toteutettu. Käytännön toteutuksen jälkeen esitellään järjestelmän ominaisuuksien testaus- ja tuotantovaiheet.

Insinöörityön lopputuloksena oli kehitetty Academica Oy:lle entistä parempi palvelimien valvonta- ja ylläpitopalvelu. Järjestelmä otettiin tuotantokäyttöön ja sillä toteutetaan asiakaslaitteiden päivittäistä valvontaa, ylläpitoa sekä kriittisten tietoturvapäivitysten jakelua.

Avainsanat	Symantec, altiris, automatisointi, valvonta, palvelin

Authors Title Number of Pages Date	Simo Saaranen, Mikko Jänkälä Automation of Server Monitoring 51 pages + 2 appendices 30 November 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructors	Janne Salonen, Senior Lecturer Timo Juselius, Service Manager

Server monitoring is a critical part when maintaining servers and server environments. Monitoring can provide continuous operation to the servers. Furthermore it prevents errors from occurring and break downs. Usually monitoring is a service, a program or a procedure which provides real time monitoring for the servers.

The purpose of this thesis and project was to produce a semi-automatic server monitoring system which had to include a centralized system to distribute critical security updates to the client devices. The thesis was designed and produced for Academica Oy and the project was implemented with the Symantec Management Platform.

The whole system was built with the Symantec Management Platform features. The accomplished monitoring system was designed, implemented and tested carefully by the bachelor of engineering students. Academica Oy's staff actively supported the team during the project. The system was also tested and approved by the company.

At the beginning of this thesis the server monitoring and the Symantec Management Platform are explained in theory as to how the key features and components function. The system in practice is explained after the theory. Finally the testing and production procedures are exhibited.

As the result of this thesis the company received a better monitoring and maintaining service for their customers. The system was launched to the production environment. It is used on a daily basis to produce server monitoring, maintenance and for distributing system critical patches.

Keywords	Symantec, altiris, automation, monitoring, server

Sisällys

Lyhenteet ja määritelmät

ActiveX	Toinen nimi Microsoft Windows -ympäristössä käytetylle COM-tekniikalle.
AD	Active Directory. Microsoft Windows -toimialueen (Domain) käyttäjätietokanta ja hakemistopalvelu. Tämä sisältää tietoja käyttäjistä, tietokoneista ja verkon resursseista.
CMDB	Configuration Management Database. Tietopankki, joka sisältää tietoa IT-ympäristön komponenteista ja niiden yhteyksistä.
CPU	Central Processing Unit. Tietokoneen prosessori tai suoritin.
DNS	Domain Name System on Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
Domain	Toimialue on joukko Microsoft Windows -käyttöjärjestelmän sisältäviä tietokoneita, joita voidaan hallita keskitetysti yhdeltä tai useammalta palvelimelta.
EMS	Exchange Management Shell on rakennettu PowerShell-teknologialla.
Emulointi	Tarkoittaa toisen laitteen tai järjestelmän toiminnan jäljittelyä.
Exchange	Exchange Server on Microsoftin kehittämä postipalvelinjärjestelmä.
F-Secure	Tietoturvaratkaisuja tarjoava suomalainen yritys.
ICMP	Internet Control Message Protocol. Protokolla, jonka avulla voidaan lähettää yksinkertaisia viestejä toiselle laitteelle esimerkiksi virhetilanteesta.
Liitännäinen	Plug-in on tietokoneohjelma, joka toimii vuorovaikutuksessa isäntäsovelluksen kanssa.
Linux	Viittaa Linux-ydintä käyttävien Unixin kaltaisten käyttöjärjestelmien perheeseen.

Palvelin	Tietokone, jonka avulla tarjotaan palveluja muille ohjelmille ja laitteille verkon ylitse tai paikallisesti samassa koneessa.
Ping	Työkalu, jonka avulla voidaan kokeilla laitteiden tavoitettavuus.
Platform	Käytetään yleensä nimityksenä ohjelmistoalustasta ja siihen liittyvästä laitteistosta. Tässä tapauksessa kyseessä on Symantecin kehittämä hallinta-alusta, joka asennetaan palvelimelle.
PS	PowerShell on Microsoftin kehittämä seuraavan sukupolven komentotulkki Windows-käyttöjärjestelmiin.
RAM	Random Access Memory. Tietokoneen keskusmuisti tai työmuisti.
Site server	Toimipaikkapalvelin, joka tuo tarvittavan palvelun lähemmäksi käyttäjille. Esimerkiksi yrityksellä on kaksi toimipistettä ja päätoimipisteessä on palvelin, joka tuottaa jotain palvelua. Suuren käyttäjämäärän takia on kustannustehokkaampaa sijoittaa toinen palvelin toiseen toimipisteeseen, joka keskustelee pääpalvelimen kanssa.
SMC	Symantec Management Console. Hallintakonsoli Internet-selaimen kautta, jonka avulla voidaan hallita Symantec Management Platformia.
SMP	Symantec Management Platform. Hallinta-alusta, joka on suunniteltu tarjoamaan alustasta ja laitteistosta riippumattoman ratkaisun koko IT-ympäristön hallintaan.
SNMP	Simple Network Management Protocol. TCP/IP-verkkojen hallinnassa käytettävä protokolla jolla voidaan kysellä verkossa olevan laitteen tilaa ja laite voi myös itsenäisesti tehdä hälytyksiä.
SQL	Structured Query Language. Standardoitu kyselykieli, jonka avulla tietokantaan voidaan tehdä erilaisia hakuja, lisäyksiä tai muutoksia.
Symantec	Tietokoneohjelmistoja ja erityisesti tietoturvaohjelmistoja kehittävä kansainvälinen yritys.

Tietokanta	Kokoelma tietoa, joilla on yleensä yhteys toisiinsa. Esimerkiksi tietokanta voi olla yrityksen asiakasrekisteri.
Unix	Laitteistoriippumaton käyttöjärjestelmä.
Verkkoselain	Tietokoneohjelma, jonka avulla voidaan selata Internetiä. Esimerkiksi Internet Explorer, Mozilla Firefox ja Google Chrome.
Web part	Tunnetan myös nimellä Web Widget. Nämä ovat samankaltaisia kuin Portletit, jotka ovat erillisesti käsiteltäviä sisältöruutuja tai -ikkunoita.
Web Server	WWW-palvelin, joka jakaa dokumentteja http-protokollalla asiakasohjelmille ja koneille.
Windows	PC:lle tarkoitettu Microsoftin kehittämä graafisten käyttöliittymien ja käyttöjärjestelmien perhe.

1 Johdanto

Tämä insinöörityö on toteutettu kehitysprojektina Academica Oy:lle. Työ on kahden insinöörityöntekijän ja yrityksen työsuhteen aikana kehittynyt toimeksianto. Projekti toteutettiin Academican pyynnöstä sekä yhteistyönä yrityksen henkilöstön kanssa. Yrityksellä oli tarve kehittää tuotannossa olevaa palvelua liittyen asiakaslaitteiden valvontaan ja niiden ylläpitoon.

Projektin tavoitteena oli kehittää asiakkaille tarjottavaa palvelimien valvonta- ja ylläpitopalvelua. Ennen projektia käytössä ollut palvelu oli työläs ja raskas ylläpidettäväksi. Vanhasta järjestelmästä johtuen yritys halusi kehittää uudesta palvelusta mahdollisimman automaattisen ja helposti hallittavan kokonaisuuden. Lisäksi yritys halusi toteutetusta valvontajärjestelmästä mahdollisimman kattavan dokumentaation.

Koko projekti toteutettiin Symantec Management Platform -ohjelmistoalustan avulla, joka on Symantec-yrityksen kehittämä. Alustaa hyödyntämällä pystyttiin toteuttamaan kokonaisuus, jota voidaan hallita yksinkertaisesti verkkoselaimella. Palvelun avulla pystyttiin tuottamaan osittain automatisoitua valvontapalvelua. Lisäksi voitiin suorittaa palvelimien ylläpitoa helpottavia toimenpiteitä, kuten tietoturvapäivitysten ja ohjelmien jakelua keskitetysti. Projektin ohessa luotiin yritykselle kattava dokumenttikirjasto, josta löytyy palvelun toteutus-, toiminta- ja ylläpito-ohjeet.

Insinöörityön toteutuksessa ja lähteinä on käytetty muun muassa Symantec-yrityksen tuottamia virallisia dokumentteja ja käyttöohjeita. Lisäksi Academica Oy:lle tuotettu dokumenttikirjasto tukee tämän työn sisältöä ja asiatekstiä. Osa työn toteutuksesta perustuu testiympäristössä tehtyihin ja toimiviksi todettuihin kokeiluihin.

2 Palvelinvalvonta

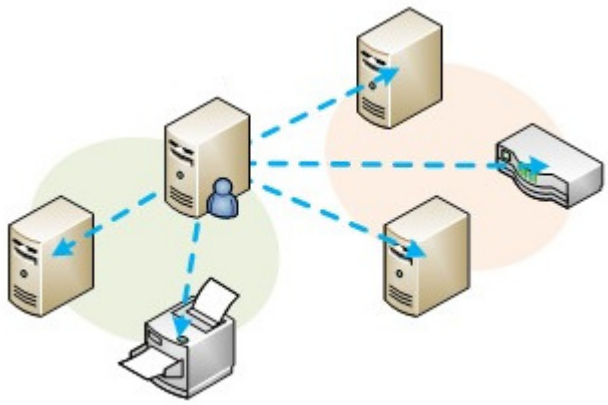
Valvonnalla tarkoitetaan yleensä laitteisto- tai sovelluspohjaista järjestelmää, jonka avulla valvotaan tietokoneen resursseja ja suorituskykyä. Yleensä valvontaan käytetään sovelluspohjaista järjestelmää. Käyttötarkoitus kohdistuu usein esimerkiksi fyysisiin laiteosiin, kuten prosessorin (CPU) käyttöasteeseen, sekä vapaan käyttömuistin (RAM) määrään. Valvontajärjestelmiä käytetään usein myös vapaan kiintolevytilan, järjestelmän yleisten tietojen ja verkkojen valvomiseen. [1.]

Palvelinvalvonnalla tarkoitetaan palvelua, ohjelmaa tai toimintatapaa, jonka avulla yritysten palvelimia ja resursseja seurataan pääasiassa reaaliaikaisesti. Sovelluksia ja toimintatapoja on monia erilaisia, ja Internet on pullollaan ratkaisuja ja ohjelmia. Tärkeintä on kuitenkin se, että valvonta on tehokasta ja se ehkäisee ongelmia riippumatta toteutustavasta.

Lähes kaikkien yritysten liiketoiminta on nykyään jatkuvasti riippuvaista informaatio- ja kommunikaatioteknologiasta. Jo pelkästään sähköpostin toimimattomuus voi lamauttaa joissakin yrityksissä toiminnan lähes kokonaan. Toinen hyvä esimerkki riippuvuudesta on sovellus, joka tekee asiakaslaitteelta SQL-kyselyitä tietokantapalvelimelle. Sillä voidaan tuoda pyydetty tieto käyttäjälle käytettäväksi. Ylipäätänsä isoissa tai keskisuurissa yrityksissä toiminta on riippuvaista suurilta osin sovelluksista tai palveluista, jotka toteutetaan yrityksen palvelimien toimesta. Siksi on erityisen tärkeää, että käyttöönotto ja toimivuuden takaaminen on toteutettu huolellisesti kaikissa yrityksissä, jotka ylläpitävät palvelimia itselleen tai muille.

Yrityksen liiketoiminnalle ei riitä, että palvelin tai palvelinympäristö on otettu käyttöön, ja se toimii. Jotenkin on myös varmistettava liiketoiminnan jatkuvuus. Tämä saatetaan välillä kokonaan unohtaa, kunnes ongelmatilanne kohdataan, ja silloin kaikki on jo myöhäistä. Näin ei saisi koskaan tapahtua teknologiakriittisessä yritysmaailmassa. Tässä kohtaa kuvaan astuu palvelinvalvonta. Palvelimen käyttöönoton, toimivuuden ja varmistuksen lisäksi, myös palvelinvalvonta on suunniteltava ja toteutettava. Tällöin voidaan jo puhua liiketoiminnan jatkuvuudesta teknologiakriittisessä yrityksessä.

Palvelinvalvonta on työtä, jonka tarkoituksena on ennaltaehkäistä ongelmia ja riskejä. Valvonnalla pyritään takaamaan palvelimen tai palvelinympäristön toiminta. Se ehkäisee myös tehokkaasti käyttökatkoksia ja ennen kaikkea laskee merkittävästi pitkällä aikavälillä ylläpitoon tarvittavaa aikaa ja kustannuksia. Hyvin suunniteltu ja toteutettu valvonta voi poistaa kokonaan tai lähes kokonaan mahdolliset ongelmatilanteet ja käyttökatkokset. Näistä syistä johtuen valvonnan suunnittelussa tärkeimpiä asioita on mahdollisten ongelmatilanteiden ja riskien kartoitus.



Kuva 1. Yksinkertainen valvontaympäristö [2.]

Kuvassa 1 on esitetty yksinkertainen valvontaympäristö. Tässä tapauksessa voidaan kuvitella esimerkiksi yhden yrityksen verkko- ja laiteympäristö. Kuvan valvontapalvelimesta lähtee nuolet yrityksen valvontaan kuuluviin asiakaslaitteisiin. Asiakaslaitteilla tarkoitetaan yleensä esimerkiksi yrityksen työasemia, tulostimia ja muita verkkolaitteita.

Valvontapalvelimen tarkoituksena on tehdä järjestelmänvalvojan asetusten mukaisesti tietyn väliajoin tarkistuskyselyitä ja -pyyntöjä asiakaslaitteille. Järjestelmänvalvojalla tarkoitetaan yrityksen toimihenkilöä, joka on vastuussa pääasiassa kaikista tai tietyistä tietoteknisistä toteutuksista yrityksessä. Kyselyiden ja pyyntöjen avulla valvontapalvelin pysyy ajan tasalla asiakaslaitteiden tilasta ja toiminnasta. Jos palvelin havaitsee jotain normaalista poikkeavaa, lähettää se pyynnön asiakaslaitteelle poikkeuksen korjaamiseksi, mikäli se on mahdollista. Tällä tavoin pyritään mahdollisimman paljon automatisoimaan laitteiden valvontaa ja poistamaan manuaalista työtä.

3 Symantec Management Platform

3.1 Yleistä

Symantec Management Platform on alun perin Altiris Inc. -nimisen yhtiön kehittämä palvelunhallintaohjelmisto. Altiris Inc. toimii nykyään Symantec-yrityksen tytäryhtiönä jatkaen tuoteperheen kehitystä [3]. Palvelunhallintaohjelmistot perustuvat ITIL-kirjastoon, joka on lyhenne sanoista Information Technology Infrastructure Library. ITIL on kokoelma käytäntöjä IT-palveluiden hallintaan ja johtamiseen [4].

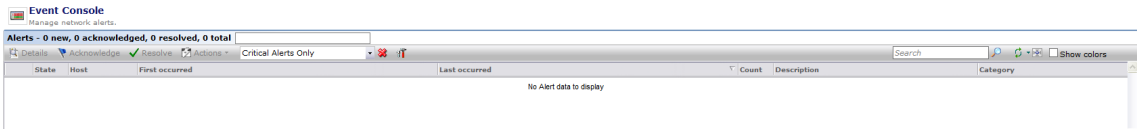
SMP (Symantec Management Platform) on hallinta-alusta, joka on suunniteltu tarjoamaan alustasta ja laitteistosta riippumattoman ratkaisun koko IT-ympäristön hallintaan. Hallinta-alustaan voidaan liittää erilaisia ratkaisuja. Ratkaisut hyödyntävät alustan palveluja, kuten tietoturvaa, raportointia, kommunikaatiota, paketinhallintaa ja Configuration Management Databasen (CMDB) tietoa. Koska ratkaisut jakavat saman alustan, ne voivat jakaa alustan palveluja ja tietoa. Alustan vahvuutena on ratkaisujen jakama tieto. Esimerkiksi yksi ratkaisu kerää tietoa yrityksen koneille asennetuista ohjelmista, toinen hyödyntää saatua tietoa lisenssien valvontaan ja kolmas ratkaisu voi hyödyntää molempia tietoja ohjelmistojen päivittämiseen. Tämä ratkaisujen ja alustan integraatio helpottaa erilaisten toteutusten käyttöä, koska kaikki toimii saman rajapinnan päällä. [5, s. 27.]

Alusta tarjoaa seuraavia ominaisuuksia

- roolipohjainen tietoturva
- viestintä ja hallinta
- ajastetut tai tapahtumasta seuraavat tehtävät ja säännöt
- paketinhallinta ja raportointi
- keskitetty hallinta yhtenäisen rajapinnan avulla
- configuration management database (CMDB).

Hallinta-alusta sisältää komponentteja, kuten esimerkiksi Notification Serverin. Se käsittelee tapahtumat, helpottaa yhteydenpitoa hallittujen koneiden välillä sekä koordinoi työtä ja tehtäviä muiden palvelujen kanssa. Symantec Management Console (SMC) on web-käyttöliittymä, jonka avulla valvotaan ja hallitaan valvontapalvelinta (Notification Server) sekä sen sisältämiä palveluja. Configuration Management Database (CMDB) on tietokanta, mihin säilötään kaikki tieto hallituista laitteista. Site servers -komponentin avulla hallinta-alustalla voidaan isännöidä useita erilaisia komponentteja, kuten paketinhallintaa ja tehtäväpalvelinta. Jos palvelinympäristössä jokin toinen palvelin itse pääalustan lisäksi isännöi jotain komponenttia, on se toimipaikkapalvelin. Symantec Management Agent on ohjelma, joka asennetaan asiakaslaitteelle, jota halutaan valvoa ja hallita valvontapalvelimella. Software Management Framework on rajapinta, jonka avulla hallitaan ohjelmistoja. Tällä sovelluksen hallintarajapinnalla voidaan hallita myös ohjelmia, jotka ovat ohjelmistokirjastossa (Software Library). Ohjelmistoluettelo (Software Catalog) tarjoaa keskitetyn paikan ohjelmistoihin liittyviin toimenpiteisiin. Raportit (Reports) tarjoaa työkalun ja tavan kerätä automatisoitua tietoa SMC:n välityksellä. Raporteista voidaan tarkastella kerättyä tietoa mistä tahansa hallitusta laitteesta. [5, s. 28.]

Valvontaratkaisu ja tapahtumakonsoli (Monitor Solution and Event Console) ovat yksi osa hallinta-alustan ratkaisua. Valvonnan tarkoituksena on vähentää IT-ympäristön hallintaan liittyviä kustannuksia. Valvontaratkaisulla voidaan tunnistaa ympäristön kunto keräämällä tietoa eri asiakaslaitteista, kuten palvelimista, ohjelmista ja verkkolaitteista. Valvonnalla voidaan analysoida kehitystä, eristää toistuvat ongelmat tutkimalla tietoa suorituskyvystä reaaliajassa sekä historiatiedoista. Valvontaratkaisun avulla voidaan paikantaa myös ongelmat, määritellä ongelmien syyt ja tehdä automatisointeja ongelmien ratkaisemiseksi. Tapahtumakonsoli (Event Console) vähentää tarvetta käyttää muita erillisiä työkaluja asiakaslaitteiden valvontaan. Konsoli kerää SNMP-viestejä, sekä muita tilaviestejä ja näyttää ne yhdessä paikassa. Kuvassa 2 on esitetty SMC:n kautta nähtävä tapahtumakonsoli. [6, s. 8.]



Kuva 2. Tapahtumakonsoli

3.2 Alusta ja hallinta

3.2.1 Symantec Management Platform

Symantec Management Platform ei itsessään tuota minkäänlaista hallintaa, vaan se koostuu erilaisista ratkaisuista ja kokoaa kaiken keskitetysti yhteen paikkaan. Ohjelma joka kytketään alustaan, on niin sanottu ratkaisu (Solution). Kun alustaan kytketään useita ratkaisuja, sanotaan niitä ryhmäksi (Suite). Kun ratkaisu tai ryhmä asennetaan, niin samalla asennetaan myös koko alusta, mikäli se ei ole jo asennettuna. [5, s. 27.]

Alustan asennuksen aikana kaikki palvelut (Services) asentuvat alustan mukana. Näihin palveluihin kuuluu myös Notification Server -palvelu. Kaikki palvelut asentuvat vastaavasti Notification Server -palvelimelle. Notification Server on palvelin, jota ohjataan SMC:n avulla, kun tuotetaan järjestelmänvalvontaa ja hallintaa. Osana alustan asennusta tulee myös CMDB, johon alustan ja ratkaisujen keräämä tieto tallennetaan. CMDB on Microsoft SQL Server -tietokanta. [5, s. 27.]

SMC on selainpohjainen konsoli, johon pääsee käsiksi valvontapalvelimelta. Konsoliin pääsee palvelimelta suoraan tai Internetin välityksellä [5, s. 28]. Konsoli on rakennettu osittain Microsoft ActiveX -komponenteilla, joten se vaatii toimiakseen Internet Explorer (IE) -pohjaisen verkkoselaimen. Internet Explorer -selaimen lisäksi on olemassa esimerkiksi Chrome-selaimeen asennettava liitännäinen nimeltä IE tab. Liitännäisellä voidaan emuloida IE:n eri versioita, joka antaa mahdollisuuden käyttää SMC:tä myös muilla selaimilla.

SMP ei käyttöönoton jälkeen aloita itsenäisesti keräämään tietoa hallittavista asiakaslaitteista. Asiakaslaitteista saadaan tarkempaa tietoa, kun niihin asennetaan agentti (Symantec Management Agent). Agentin avulla asiakaslaite on yhteydessä hallinta-alustaan ja siihen asennettuihin ratkaisuihin. Agentti vastaanottaa tehtäviä alustalta ja ratkaisuilta, asentaa asiakaslaitteeseen ohjelmia sekä lähettää asiakaslaitteesta kerättyä tietoa alustan tietokantaan. Tietokannan tietoa voidaan käyttää monella eri tapaa, kuten esimerkiksi generoida raportteja tai käynnistää automatisoituja tehtäviä. Agentti voidaan asentaa Unix-, Linux-, OS X- ja Windows-ympäristöihin. On olemassa kaksi erilaista agenttia. Ensimmäinen on Windows-ympäristöihin ja toinen Unix-sukuisiin käyttöjärjestelmiin. Tosin kaikkia Unix-käyttöjärjestelmiä ei tueta virallisesti, koska on mahdotonta testata agentin toimintaa tuhansissa eri jakeluissa. [5, s. 30.]

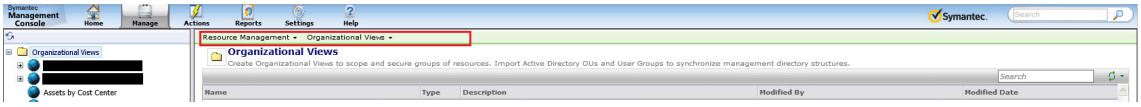
Kerättävä tieto ja suoritettavat tehtävät riippuvat siitä, mitä ratkaisuja alustaan on asennettuna. Alustaan voi olla asennettuna ratkaisu tai ryhmä ratkaisuja, mutta näitä kaikkia hallitaan yhden konsolin kautta. Eli jos myöhemmin päätetään ottaa käyttöön jokin muu ratkaisu, niin ei ole tarvetta opetella uuden liittymän käyttöä. [5, s. 30.]

3.2.2 Symantec Management Console

Symantec Management Console (SMC) on selainpohjainen käyttöliittymä, jota käytetään suoraan valvontapalvelimelta tai Internetin välityksellä. SMC on ensisijainen työkalu valvontapalvelimen ja sen komponenttien käyttöön. SMC:hen ei pääse käsiksi, mikäli käyttäjä ei ole jonkin palvelinvalvontaroolin jäsen. SMC:tä esiteltäessä se on jaettu kahteen osaan. Ensimmäinen osa on Header eli sivun yläosa. Yläosassa sijaitsee valikot, joista pääsee valvontapalvelimen hallintaan, sekä asennettujen ratkaisujen toimintoihin. Yläosassa on myös hakulaatikko, mistä voidaan suoraan hakea halutun resurssin, kuten esimerkiksi valvotun asiakaslaitteen tiedot. Kuvassa 3 on esitelty SMC:n yläosa. [5, s. 35–36.]

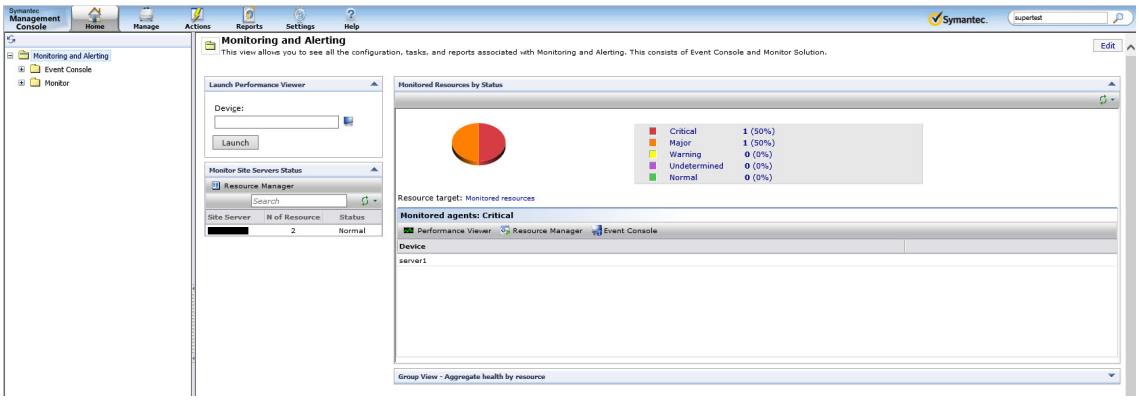
Kuva 3. Symantec Management Console Header (Yläosa)

Sivun yläosaan kuuluu myös niin sanottu Breadcrump-navigointi, joka avustaa käyttäjää valikoiden navigoinnissa. Se kertoo tarkan polun, missä käyttäjä sillä hetkellä sijaitsee. Navigointi on esitetty kuvassa 4. [5, s. 36.]



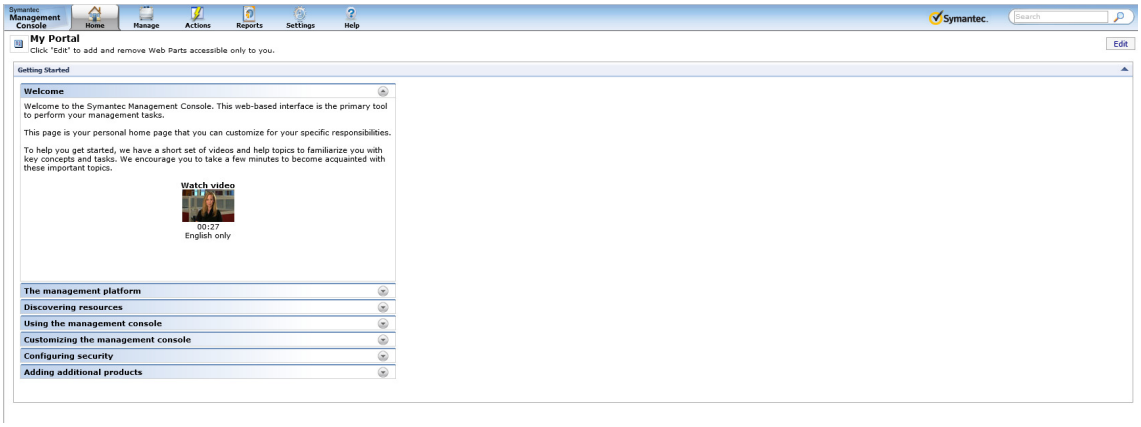
Kuva 4. Breadcrump-navigointi

Toista osaa SMC:stä sanotaan sisältöalueeksi (Content Area), jossa voi näkyä hakemistopuu ja sisältöalue. Hakemistopuu näkyy sivun vasemmassa ikkunaruudussa. Se näyttää hierarkkisessa järjestyksessä kohtia, joita käyttäjä voi valita, sekä työskennellä sivun oikeassa ikkunaruudussa. Sisältöalue on esitelty kuvassa 5. [5, s. 36.]



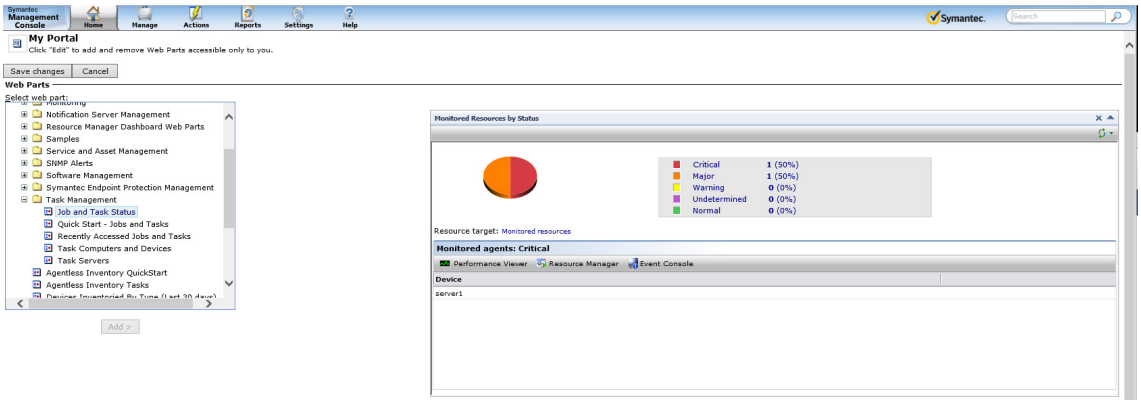
Kuva 5. Hakemistopuu ja työskentelysivu

Sisältöalueella voi olla myös portaalisivu, joka näyttää kokoelman erilaisista tiedoista, jotka esitetään web part -ikkunoissa. Portaalisivu on esimerkki kokosivun näkymästä (Full Page), jossa on yhden ikkunan näkymä ilman hakemistopuuta. Kuvassa 6 on esimerkki portaalisivusta. [5, s. 36.]



Kuva 6. Esimerkki portaalisivusta

Joitakin konsolin sivuja voidaan muokata käyttäjäkohtaisesti. Eli toisen käyttäjän muokkaama sivu näkyy toiselle käyttäjälle alkuperäisessä muodossa. Pääsääntöisesti muokkaus on mahdollista raportointi- ja suodatinsivuilla sekä hakemistopuun tilan muistissa pysymisellä. Myös minun portaali -sivun (My Portal) voi kukin käyttäjä muokata erilaisilla web part -ikkunoilla haluamansa näköiseksi. Kuvassa 7 on esitetty minun portaali -sivun muokkaamista erilaisilla web part -ikkunoilla. [5, s. 36.]



Kuva 7. Minun portaali -sivun muokkaus

3.3 Valvonta ja monitorointi

3.3.1 Notification Server

Notification Server (valvontapalvelin) on SMP:n ensisijainen komponentti. Notification Server ohjaa monia ratkaisuja. Se tuottaa SMC:n näkymän, sillä on sääntöpohjainen käyttäjähallinta ja se tuottaa raportteja ja ilmoituksia. Valvontapalvelin isännöi myös portaalin verkkosivuja ja on vastuussa ratkaisujen mukana tulleista ennalta määrätyistä säännöistä ja tehtävistä. [5, s. 42.]

Valvontapalvelimen ominaisuuksiin kuuluu verkossa olevien resurssien löytäminen, hallinta-agentin asentaminen ja konfigurointi asiakaslaitteisiin. Se kerää myös asiakaslaitteista tietoa ja tallentaa sen CMDB:hen. CMDB esitellään luvussa 3.3.2. Valvontapalvelin luo lisäksi verkkopohjaiset raportit, lähettää sääntöjen yksityiskohdat sekä toimittaa tarvittaessa erilaisia ohjelmia asiakaslaitteille. [5, s. 42.]

3.3.2 Configuration Management Database

Tietokantojen käsittely vaatii alustalta paljon resursseja. Mitä useampi ratkaisu on alustalle asennettuna ja se, miten niitä käytetään, vaikuttaa alustan tietokantojen järjestelmävaatimuksiin. Myös asiakaslaitteiden määrä, jotka kommunikoivat valvontapalvelimen kanssa, vaikuttaa suoraan siihen, miten paljon tietokanta vaatii alustalta resursseja. Jokainen valvontapalvelin voidaan konfiguroida käyttämään paikallisen tai etäpalvelimen CMDB-tietokantaa. Valvontapalvelin, jossa on paikallinen tietokanta, tarvitsee

enemmän resursseja kuin valvontapalvelin, joka käyttää etäpalvelimen tietokantaa. [5, s. 43.]

Paikallisesti asennettu CMDB asennetaan samalle palvelimelle kuin valvontapalvelin. Tällä konfiguraatiolla voidaan ylläpitää 1000 – 5000 asiakaslaitetta. Etäpalvelimelle asennettu CMDB on asennettuna erilliselle palvelimelle kuin valvontapalvelin. CMDB:n tekemä kuorma jakautuu kahden palvelimen kesken riippuen siitä, kumpi rooli on asennettuna kummalle palvelimelle. Tällaiselle konfiguraatiolle on suositeltavaa varata oma nopea verkkoyhteys palvelimien välille. Symantec suosittelee yhden gigatavun (1 GB) verkkoyhteyttä. [5, s. 43.]

3.3.3 Monitor Solution

Palvelimen valvonta auttaa takaamaan sen, että palvelin on aina saatavilla ja toiminnassa. Valvonnalla voidaan valvoa ympäristöjen kuntoa keräämällä haluttua tietoa asiakaslaitteista. Lisäksi voidaan analysoida tietoa ja sen perusteella eristää toistuvat ongelmat. Valvonnalla paikannetaan ongelmat ja määritellään niiden syyt sekä mahdollisuuksien mukaan automatisoidaan ongelmien korjaus. [7, s. 11.]

Valvontaratkaisu (Monitor Solution) tukee niin sanottua agenttipohjaista ja agentitonta valvontaa sekä on palvelinhallintapaketin (Server Management Suite) avainosa. Valvontaratkaisu tarjoaa monenlaista valvontaa palvelimille ja ohjelmille. Valvonta toteutetaan useamman keskenään toimivan valvontaratkaisun kautta, jotka käyttävät valvontaratkaisun yleisimpiä osia. Näitä osia kutsutaan myös ydinkomponenteiksi (Core Component). Jokainen valvontaratkaisu käyttää ydinkomponentteja valvontaratkaisun komponenttien lisäksi. Jokainen ratkaisu tarjoaa erilaisia raportteja, joiden avulla tietoa voidaan tarkastella. Ydinkomponenttien ja ratkaisukomponenttien erottaminen tarjoaa kokonaisvaltaista joustavuutta laitteiden valvontaan. [7, s. 11–12.]

Valvontaratkaisun ydinkomponentteihin kuuluva valvontaliitännäinen (Monitor Plug-in) suorittaa valvontatyön asiakaslaitteilla. Tämä on valvonta-agenttiin (Symantec Management Agent) asennettava liitännäinen. Agentti asennetaan asiakaslaitteille ja valvontaliitännäinen saa valvontapalvelimelta tiedon siitä, mitä asiakaslaitteella valvotaan. [7, s. 12.]

Agentiton valvonta on myös osa ydinkomponentteja. Siinä valvontapalvelu sijaitsee toimipaikkapalvelimella, joka toimii valvontaliitännäisen puolesta. Tämä sallii tietynlaisen valvonnan asiakaslaitteissa, joissa ei ole mahdollisuutta agentin asentamiseen [7, s. 12]. Näitä laitteita voidaan valvoa esimerkiksi SNMP-protokollan avulla.

Reaaliaikaan ja historiaan perustuva suorituskyvyn tutkiminen on yksi osa ydinkomponenteista. Ne sallivat asiakaslaitteen tietojen tutkimisen ja mahdollisten ongelmien tunnistamisen. Raportointi on myös ydinkomponentti, jonka avulla saadaan erilaisia tapoja analysoida tietoa, jota laitteista on kerätty. Raportteja voidaan luoda omien mieltymysten mukaan tiedosta, jota CMDB säilyttää. Lisäksi voidaan käyttää valmiita raporttipohjia tiedon tutkimiseen. [7, s. 12.]

Monitorointipaketin sisältämät välttämättömät ydinkomponentit, joita ovat

- käytännöt (Policy)
- metriikat (Metric)
- säännöt (Rule)
- tehtävät (Task).

Yllä olevia komponentteja tarvitaan käyttöjärjestelmän tai ohjelman monitorointiin. Monitorointipaketit ja komponentit sisältävät esikonfiguroituja käytäntöjä. Käytäntöihin on esiasetettu myös raja-arvoja tietyillä vakavuusasteilla (Severity). Näistä komponenteista kerrotaan lisää luvussa 3.3.4. [7, s. 13.]

Valvontaratkaisu siis kerää ja analysoi jatkuvasti tietoa, jota se saa verkossa olevilta valvottavilta asiakaslaitteilta. Kun valvontapalvelimelle tulee tietoa, joka täsmää johonkin kriteeriin, voidaan siitä nostaa hälytys vähintään tapahtumakonsoliin. Hälytyksen seurauksena voidaan myös suorittaa jokin toimenpide. [7, s. 14.]

3.3.4 Käytännöt, säännöt ja metriikat

Valvonta toteutetaan käytäntöjen, sääntöjen ja metriikoiden avulla. Myös hälytyksien nostaminen ja ongelmien mahdolliset ratkaisut automatisoidaan näiden komponenttien avulla. Valvonnan käytäntö on kokoelma erilaisia sääntöjä ja tehtäviä. Käytännöt kohdistetaan haluttuihin laitteisiin tai ryhmiin, joita halutaan valvoa. Ryhmät taasen sisältä-

vät useita valvottavia asiakaslaitteita, jotka ovat tässä tapauksessa palvelimia. Käytännöt ilmoittavat valvontaliitännäiselle tai etävalvontapalvelimelle (Remote Monitoring Server on sama palvelin, kuin valvontapalvelin), mitä tietoja asiakaslaitteesta halutaan valvoa. Nämä sisältävät tiedon myös siitä, kuinka tietoja pitäisi tarkastella. Säännöt joista käytännöt koostuvat, tutkivat tietoja niille annettujen raja-arvojen puitteissa. Asetettujen sääntöjen pohjalta liitännäinen voi suorittaa automatisoituja tehtäviä asiakaslaitteella. Valvontapalvelin käyttää käytäntöjen ja sääntöjen tietoja tehtäväpalvelimen (Task Server) tehtävien suorittamiseen, tosiaikaiseen suorituskyvyn valvontaan ja suorituskyvyn historiasta saataviin raportteihin. [7, s. 14.]

Säännöt siis kertovat, miten metriikasta tai tapahtumasta saatua tietoa pitää tulkita. Säännöt määrittävät myös, millaisella raja-arvolla automatisoidut tehtävät käynnistetään. Esimerkiksi säännössä voidaan määritellä, että seurataan Microsoft Windows -käyttöjärjestelmän tulostuspalvelua. Jos tulostuspalvelu kaatuu tai pysähtyy, agentti tunnistaa tämän tapahtuman. Tapahtumalle voidaan määrittää automaattinen tehtävä, mikä pyrkii käynnistämään palvelun uudelleen. [7, s. 14.]

Käytäntöön tai sääntöön voidaan määrittää toimenpide (Action) tai tehtävä (Task). Säännöt aktivoituvat, jos valvotun metriikan raja-arvo muuttuu yli sallitun arvon. Aktivoitunut sääntö lähettää hälytyksen (Alert) vähintään tapahtumakonsoliin. Lisäksi säännön aktivoituminen käynnistää tehtävän tai toimenpiteen suorittamisen, mikäli se on säännölle määritelty. Toimenpiteitä ja tehtäviä voidaan myös suorittaa ajastettuna. Niitä voidaan suorittaa myös vaadittaessa valvontapalvelimella tai asiakaslaitteella. Asiakaslaitteella suoritettava tehtävä tai toimenpide vaatii agentin, jotta se voidaan lähettää valvontapalvelimelta asiakaslaitteelle. [7, s. 14.]

Metriikat ovat koko valvonnan perusta. Ne määrittelevät, miten valvontaliitännäinen tai etävalvontapalvelin kerää tietoa asiakaslaitteen lähteistä. Metriikkana voidaan käyttää lähestulkoon mitä tahansa tietoa, mitä asiakaslaitteelta saadaan. Esimerkiksi Windows-palvelimelta voidaan kerätä metriikkaa kaikista kohteista, joita suorituskykyohjelma näyttää (Performance Monitor). Lisäksi voidaan valvoa tietyn palvelun (Service) toimivuutta tai seurata käyttöjärjestelmän lokeja. Tästä esimerkkinä levytilan prosentuaalinen käyttöaste: Microsoft Windows -alustasta saadaan metriikan avulla tietoon levyn vapaa tila, sekä levyn kokonaistila. Näitä kahta arvoa käyttämällä voidaan laskea vapaa prosentuaalinen levytila (a=vapaatila, b=levyn koko, ((a/b)*100) = vapaa levytila

prosentteina). Nämä yhdistelmämetriikat (Compound Metric), ovat yksinkertainen esimerkki siitä, miten CMDB:n tietoja voidaan yhdistellä.

3.4 Asiakaslaitteiden valvonta

Symantec Management Agent on sovellus, joka toteuttaa kommunikaation verkossa valvontapalvelimen ja asiakaslaitteiden välillä. Valvontapalvelin on vuorovaikutuksessa agentin kanssa, jotta jokaista asiakaslaitetta voidaan hallita ja valvoa SMC:n avulla. [5, s. 285.]

Palvelin ja agentti yhdessä tuottavat seuraavia toimintoja asiakaslaitteille

- kokoonpanon sekä ohjelmistojen valvonta
- ohjelmapäivitysten ja ohjelmien asennus
- kokoonpanon tietojen kerääminen
- käytäntöjen ja pakettien hallinta.

Kuten aikaisemmin on mainittu, agentti on saatavilla Windows-, Linux-, Unix- ja OS X -ympäristöille. Agentti sallii myös erilaisten ratkaisujen liitännäisten asentamisen itseensä. Esimerkiksi inventaarioratkaisun liitännäinen (Inventory Solution Agent Plug-in), sallii yksityiskohtaisen laitteiston ja ohjelmistojen tietojen keräämisen kaikista hallituista asiakaslaitteista. [5, s. 286.]

Agentti voidaan asentaa asiakaslaitteille joko työntämällä (Push) tai vetämällä (Pull). Agentin työntäminen voidaan myös ajastaa, mikäli se on tarpeellista. Agentin työntäminen tapahtuu SMC:n kautta. Vetäminen tapahtuu suoraan asiakaslaitteelta, menemällä asiakaslaitteen Internet-selaimella valvontapalvelimen tarjoamaan osoitteeseen, josta agentti asetuksineen asennetaan asiakaslaitteelle. Tämä vaatii myös IE-pohjaisen selainratkaisun, koska toteutuksessa on käytetty ActiveX-komponentteja. [5, s. 287.]

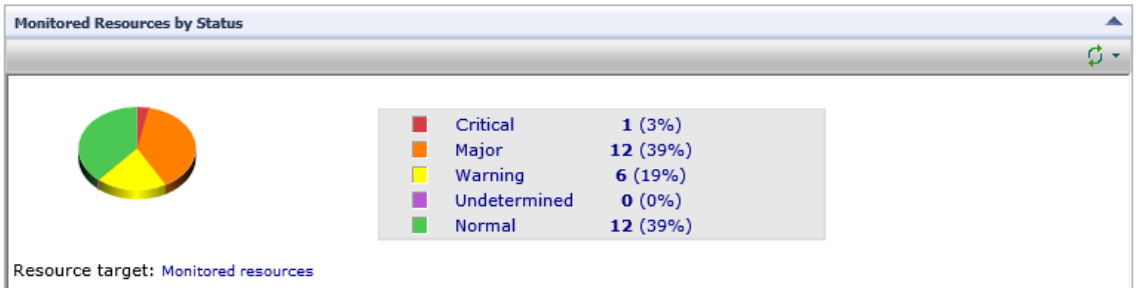
Valvontaliitännäinen asennetaan niihin asiakaslaitteisiin, joita halutaan valvoa. Liitännäinen vaatii agentin toimiakseen ja kommunikoidakseen valvontapalvelimen kanssa. Valvontaliitännäinen kerää seuraavanlaista tietoa asiakaslaitteista: Asiakaslaitteista kerätään ajoittain laitetietoja, jotka lähetetään valvontapalvelimelle (Inventory). Tätä

tietoa käytetään raportteihin. Raportit sisältävät tietoa ohjelmien havaitsemisesta sekä liitännäisen asetuksista asiakaslaitteella. Suorituskyvyn tiedot lähetetään valvontapalvelimelle ajoittain, mutta eri aikaan kuin edellä mainittu tieto. Suorituskyvyn tietoja käytetään historiaan perustuvassa suorituskykyä ilmaisevissa kaaviokuvissa. Näitä tietoja historiallinen suorituskyvyn näyttäjä (Historical Performance Viewer) sekä raportit näyttävät. Osaa asiakaslaitteelta saatavasta tiedosta voidaan näyttää myös reaaliaikaisella suorituskyvyn näyttäjällä (Real-time Performance Viewer). Säännöt (Rules) vastaavasti voivat käynnistää hälytyksiä (Alerts). Valvontaliitännäinen luo hälytyksen, kun säännön arviointi muuttaa säännön tilaa. Yksittäiset sääntöjen tilat määrittävät asiakaslaitteiden kokonaisvaltaisen tilan. [7, s. 25–26.]

Säännön antama tila asiakaslaitteelle voi olla

- normaali (Normal)
- informatiivinen (Informational)
- määrittelemätön (Undetermined)
- varoittava (Warning)
- vakava (Major)
- kriittinen (Critical).

Tilat näkyvät SMC:n valvonta ja hälytys -sivulla. Kuva 8 on esimerkki siitä, miten tilat voidaan näyttää.



Kuva 8. Piirakkadiagrammi asiakaslaitteiden tilojen jakaumasta

Asiakaslaitteita voidaan valvoa myös agentittomasti, eli ilman valvontaliitännäistä ja agenttia. Näitä laitteita valvotaan tällöin agentittomilla valvontamenetelmillä. Koska valvontaliitännäistä ei ole saatavilla, näitä asiakaslaitteita ei voida valvoa yhtä monipuo-

lisesti. Agentittoman valvonnan toteuttamiseen käytetään toimipaikkapalvelinta. Valvontapalvelintakin voidaan käyttää, jos verkon kokoonpano on suunniteltu oikein. Agentitonta valvontaa käytetään tapauksessa, jossa ei ole mahdollista asentaa agenttia asiakaslaitteelle. [7, s. 43–44.]

Esimerkkinä agentittomasta valvonnasta voidaan käyttää asiakaslaitteen tavoitettavuutta ping-komennolla. Komento lähettää ICMP Echo Request -paketteja asiakaslaitteelle. Mikäli asiakaslaite ei vastaa ICMP Echo Reply -paketilla, se ei ole tavoitettavissa. Tavoitettavuuden toimivuus on myös riippuvainen siitä, miten verkon kokoonpano on toteutettu. Tärkein asia on kuitenkin se, onko ICMP-liikenne sallittu verkossa.

3.5 Sovellus- ja tietoturvapäivitykset

Päivityksien tarkoitus on korjata ohjelman haavoittuvuuksia tai sen toimivuutta. Verkossa olevien palvelimien ja muiden asiakaslaitteiden haavoittuvuudet on tärkeää korjata. Korjaukset estävät esimerkiksi pääsyn käyttämään asiakaslaitteita luvatta.

Paikkaustenhallintaratkaisu (Patch Management Solution) auttaa toteuttamaan keskitetysti käyttöjärjestelmän ja ohjelmistojen päivityksen. Ratkaisu käyttää hyväkseen asiakaslaitteista kerättyä tietoa ja määrittää sen avulla, mitä päivityksiä asiakaslaitteille on saatavilla. Kun asiakaslaitteelle saatavat päivitykset on saatu selville, lataa ratkaisu tarvittavat päivitykset. Tämän jälkeen päivitykset levitetään avustajan (Wizard) avulla halutuille asiakaslaitteille. Ratkaisun avulla on myös mahdollista luoda toistuva ajastus, jotta hallitut asiakaslaitteet pysyvät päivitysten tasalla. [8, s. 11.]

Paikkaustenhallinnan keskeinen toiminta sisältää ohjelmistopankin (Repository). Tämä tarjoaa monipuolisesti tietoa ohjelmistotiedotteista (Software Bulletin), ohjelmistopäivityksistä, päivitysten vakavuusasteista ja ajotiedostojen (Executable) määrästä. [8, s. 11.]

Paikkaustenhallintaratkaisu on toteutettu ohjelmiston päivitysliitännäisellä (Software Update Plug-in). Liitännäinen analysoi automaattisesti hallittuja asiakaslaitteita. Se kerää myös päivityskohtaista tietoa tuetuista käyttöjärjestelmistä ja ohjelmista. Tämän tiedon avulla määritellään tarvitaanko asiakaslaitetta päivittää. Kun asiakaslaitteelle on päivityksiä saatavilla, voidaan ne jakaa sille ohjelmiston päivityssäännön avustajalla

(Software Update Policy Wizard). Tämä avustaja yksinkertaistaa päivitysten jakelua. Sen sijaan, että jokaiselle päivitykselle tehtäisiin oma sääntö, ne voidaan jakaa ohjelmistotiedotteina. [8, s. 12.]

Ohjelmistotiedote on Microsoftin näkökulmasta kerran kuukaudessa julkaistava jakelu, joka sisältää kaikki tärkeimmät ja kriittisimmät päivityksen Microsoftin käyttöjärjestelmille. Niitä käyttämällä voidaan jakaa useita päivityksiä yhdellä säännöllä. Ohjelmistotiedotteet eivät tule suoraan Microsoftilta paikkaustenhallintaan, vaan Symantec toimittaa ne itse myöhemmin omilta palvelimiltaan paikkaustenhallinnan jakeluun. Kun ohjelmistotiedotteet saapuvat on Symantec lisännyt niihin tietoa esimerkiksi päivityksen vakavuusasteesta ja tietoa sisälletyistä päivityksistä.

Ohjelmistotiedotteet tarvitsee vaiheistaa (Stage), jotta päivitykset saadaan ladattua ja jakelut luotua. Vaiheistamisen aikana jokainen päivitys joka ohjelmistotiedotteeseen kuuluu, ladataan päivityksen tuottajan (Microsoft, Adobe jne.) palvelimelta. Vaiheistetuista ohjelmistotiedotteista tarvitsee vielä tämän jälkeen luoda ohjelmiston päivityssääntö ja kohdistaa se haluttuihin asiakaslaitteisiin. [8, s. 12–13.]

Kun hallittu asiakaslaite saa siihen kohdistetun ohjelmiston päivityssäännön, se tarkistaa onko päivitys tarpeellinen. Tämän jälkeen, jos päivitystä ei ole jo asennettu, asiakaslaite lataa paketin valvontapalvelimelta. Tämän jälkeen riippuen liitännäisen oletus ohjelmiston päivityssäännöstä (Default Software Update Plug-in Policy), asiakaslaite asentaa päivityksen. [8, s. 13.]

Kaikkien edellä mainittujen toiminta on riippuvainen siitä, miten paikkaustenhallintaratkaisu on konfiguroitu. Ratkaisua asentaessa osa asetuksista määritetään ja osa jätetään oletusarvoille. Paikkaustenhallintaratkaisun taustalla on monia erilaisia automatisoituja toimenpiteitä, joiden asetuksia muuttamalla voidaan määritellä sen toimintaa. Voidaan muuttaa esimerkiksi sitä kuinka usein asiakaslaitteet saavat päivityksistä tietoa tai ne lähettävät tietoa valvontapalvelimelle jo asennetuista päivityksistä. Luvussa 4.3.3 kerrotaan yksi tapa toteuttaa päivitysten jakelu.

4 Palvelinvalvonnan automatisointi

4.1 Määrittely

Insinöörityö toteutettiin Academica Oy:lle projektiluontoisena suorituksena. Palvelinvalvonnan automatisointi oli projektina ja kokonaisuutena Academica Oy:n tilaama ja melkeinpä toivomuksena insinöörityömme aiheeksi. Yritys tarjosi ja hankki kaikki tarvitsemamme työkalut, ohjelmistot ja laitteet projektin suorittamista varten.

Projektin tarkoituksena oli

- suunnitella
- toteuttaa
- testata
- siirtää tuotantoon
- dokumentoida.

Academica Oy antoi selkeästi perusteet projektille ja insinöörityölle. Projektin pääpiirteittäin suoritettavaksi rungoksi yritys antoi yllä mainitun listauksen projektin tarkoituksesta. Yritys määritteli meille myös tarkemmin, mitä haluavat palvelinvalvontajärjestelmän toteutukselta sekä projektin dokumentoinnilta.

Insinöörityön palvelinvalvontajärjestelmä toteutettiin Symantec Management Platform 7.1 avulla. Symantecin valmistama ja suunnittelema hallinta-alusta oli jo osittain valmiiksi kokeilu- ja tuotantokäytössä. Alustaa käytettiin yrityksessä kuitenkin muihin kuin palvelinvalvontatarkoitukseen.

Valmis ja testattu palvelinvalvontajärjestelmä korvasi aikaisemman valvontajärjestelmän sekä toimitettavan palvelun tuotantokäytössä. Korvattava järjestelmä oli ollut jo hyvin kauan käytössä ja tuotannossa. Valvontaa ja palvelua haluttiin parantaa, koska se sisälsi runsaasti manuaalisia ja ihmistyövoimaa vaativia kohteita ja toimenpiteitä. Toimenpiteet olivat sen luontoisia, että niitä pystyttiin yksinkertaisesti automatisoimaan pienellä vaivannäöllä SMP:n avulla.

Palvelinvalvontajärjestelmämme myötä yrityksen ja asiakkaiden palvelimien valvonta, sekä toimitettava palvelu piti saada toteutettua mahdollisimman automaattiseksi. Projektilla pyrittiin myös minimoimaan manuaalinen ja ihmistyövoimaa vaativa työ. Tällä tavalla saatiin valvontaa ja palvelua tehostettua sekä manuaalisen valvonnan kuluttamaa aikaa siirrettyä muihin kriittisempiin töihin.

Toisin sanoen insinöörityössä oli tärkeää saada mahdollisimman paljon irti käytössä olevasta ohjelmistoalustasta ja sen tuomista automaattisista toiminnoista ja ominaisuuksista. Projektin lopputuloksena tuli siis olla mahdollisimman automaattinen, yksiselitteinen ja helposti ylläpidettävä palvelinvalvontajärjestelmä Academica Oy:lle.

4.2 Suunnittelu

Academica Oy:n uutta Symantec Management Platform 7 -palvelinvalvontajärjestelmää lähdettiin suunnittelemaan korvattavan järjestelmän ja ominaisuuksien pohjalta. Toisin sanoen ensiksi otettiin esiin vanhan valvontajärjestelmän dokumentaatiot ja tuotekortti. Dokumenttien ja järjestelmän pohjalta kartoitettiin valvontapalvelun ominaisuudet, toimintatavat ja ennen kaikkea valvonnan kohteet.

Uutta palvelinvalvontajärjestelmää suunniteltiin suurpiirteisesti vanhan järjestelmän, uusien ideoiden ja Academica Oy:n toivomuksien pohjalta. Tämä johtui siitä, että Symantec Management Platform oli entuudestaan täysin tuntematon molemmille insinöörityöntekijöille ja yrityksen ohjaajalle. Tästä syystä suunnittelua hankaloitti epätietoisuus, miten Symantecin alusta toimii ja mitkä ovat sen tärkeimmät ominaisuudet projektin kannalta. Toisin sanoen suunnittelun alkuvaiheessa ei vielä oltu varmoja, mitkä kaikki valvontakohteet vanhasta järjestelmästä pystytään toteuttamaan. Toisaalta tietämättömyys jätti myös paljon varaa ideoinnille ja palvelun kehittämiselle.

Suunnittelun lomassa etsimme ja keräsimme hyödyllistä materiaalia projektia ja insinöörityötä varten. Hyvänä esimerkkinä voidaan pitää Symantec Management Platform 7.1 -käyttöopasta, jota on käytetty myös paljon lähteenä tässä insinöörityössä. Aloitimme samalla lukemaan alustan käyttöopasta, jotta saisimme edes jotain informaatiota ennen projektin toteutuksen aloittamista.

Ennen varsinaisen toteutuksen aloittamista tutustuimme hieman oma-aloitteisesti SMP:n hallintatyökaluun eli SMC:hen. Ainoana apuna vielä tässä vaiheessa, sekä toteutuksen alussa, oli alustan käyttöopas ja ominaisuuksien kokeileminen. Valmiiksi asennettu SMP:n testialusta yrityksen palvelinympäristöön helpotti aloittamista ja tutustumista huomattavasti.

Erittäin positiivinen asia insinöörityömme ja projektin aloittamisen kannalta oli myös se, että saimme käyttöön yrityksen konsultoinnin tietotaidon. Eräs yrityksen vanhemmista konsulteista esitteli meille muutaman luennon aikana SMP:n tärkeimmät ja olennaisimmat ominaisuudet projektimme kannalta. Tärkeimpiin ominaisuuksiin ja niiden teoriaan on pureuduttu luvussa 3.

4.3 Toteutus

Palvelinvalvonnan toteutus aloitettiin määrittelyn, suunnittelun ja lyhyen ohjelmistoalustan esittelyn jälkeen. Pääasiassa toteutus alkoi alustaan tutustumisella, sekä ominaisuuksien kokeilemisella. Insinöörityön toteutus lähti siis täysin puhtaalta pöydältä. Edessä oli perehtyminen täysin uuteen ja vieraaseen ohjelmistoalustaan. Tavoitteena ohjelmistoalustan kannalta oli SMP:n ja SMC:n hallitseminen ainakin Academica Oy:n palvelinvalvonnan kannalta. Luvussa perehdytään tiiviisti, mutta mahdollisimman tarkasti toteutettuun palvelinvalvontajärjestelmään.

4.3.1 Säännöt, tehtävät ja hälytykset

Ohjelmistoalustan kokeilemisesta siirryttiin pian tutustumaan alustalle valmiiksi asennettuihin ja määriteltyihin valvontasääntöihin. Valmiiden sääntöjen avulla selvitettiin, mitkä palvelinvalvonnan määritellyt valvontakohteet pystytään toteuttamaan suoraan tai ainoastaan muokkaamalla sääntöjä. Toisin sanoen käytettiin mahdollisimman paljon hyväksi heti alussa valmiita valvontasääntöjä ja ominaisuuksia palvelinvalvonnassa. Tätä kautta pyrittiin minimoimaan uuden tiedon lisäämistä ja ennen kaikkea ohjelmistoalustan paisumista valvontapalvelimella. Valvontasääntöihin, tehtäviin ja hälytyksiin liittyvä teoria on esitelty luvussa 3.3.4.

Ennen varsinaisten valvontasääntöjen ja tehtävien toteuttamista, piti kuitenkin ymmärtää SMP:n perusasiat valvonnan toteuttamiseksi. Täytyi siis selvittää, mitkä kaikki komponentit ja ominaisuudet SMP:ssä vaikuttavat sääntöjen ja tehtävien valvontaan. Apuna selvityksissä toimivat Academica Oy:n konsultoinnin tietotaito, ohjelmistoalustan käyttöopas ja ominaisuuksien kokeileminen. Tärkeimmät ominaisuudet valvonnan kannalta olivat SMP:n valvontaratkaisu (Monitor Solution), asiakaslaitteen agentti (Agent), sekä agenttiin asennettava valvonnan liitännäinen (Monitor Plug-in). Valvontaratkaisuun liittyvä teoria on esitelty luvussa 3.3.3. Asiakaslaitteen agentin, sekä siihen liittyvien liitännäisten teoria on esitelty luvussa 3.4.

Säännöt elivät ja muuttuivat hieman projektin edetessä. Heti alussa oli kuitenkin päätettävä perusteet hälytyksille. Piti siis päättää, minkä nimisiä hälytystasoja käytettään ja ennen kaikkea mitkä olivat hälytystasojen seuraukset. Hälytyksiä päätettiin käyttää kolmessa eri tasossa. Jokainen hälytystaso ilmoittaa virheestä tapahtumakonsolissa, mutta suorittaa samalla tietyn toimenpiteen.

Hälytystasoiksi päätettiin

- varoitus (Warning)
- vakava (Major)
- kriittinen (Critical).

Varoituksen tarkoituksena oli ainoastaan tehdä ilmoitus tapahtumakonsoliin. Varoitus ilmoitti vähemmän kriittisestä tai mahdollisesti myöhemmin alkavasta ongelmasta, mikäli siihen ei aikanaan reagoida. Vakava hälytys lähetti tapahtumakonsolin ilmoituksen lisäksi sähköpostin. Sähköposti lähetettiin tiettyyn sähköpostiosoitteeseen, jonka seurauksena viesti generoitiin Altiriksen työnohjausjärjestelmään, joka oli Academica Oy:ssä käytössä. Tällä tavalla saatiin vakavat virhetilanteet melkeinpä heti työn alle, mikäli tapahtumakonsolia ei seurattu yhtä tiiviisti. Kriittisen tason hälytykset lähettivät tekstiviestin päivystäjän kännykkään. Kriittisen hälytyksen tekstiviestissä oli kuitenkin hieman vähemmän informaatiota kuin tapahtumakonsolin hälytyksessä tai sähköpostiviestissä. Kriittisellä hälytyksellä varmistettiin reagointi toimistoaikojen ulkopuolella. Tekstiviestin avulla päivystäjä pystyi katsomaan ja tarkistamaan tarkemmat virhetiedot tapahtumakonsolista tai työnohjausjärjestelmästä.

Yksi tärkeimmistä valvontakohteista palvelinvalvonnan kannalta on asiakaslaitteen tavoitettavuus. Toisin sanoen asiakaslaitteen tulee olla kytkettynä verkkoon, jotta se voidaan valvontapalvelimen toimesta tavoittaa. Asiakaslaitteen tulisi verkossa olon lisäksi vastata myös valvontapalvelimen tai muiden asiakaslaitteiden pyyntöihin. Palvelinvalvonnassa asiakaslaitteen tavoitettavuus toteutettiin kahdella tavalla.

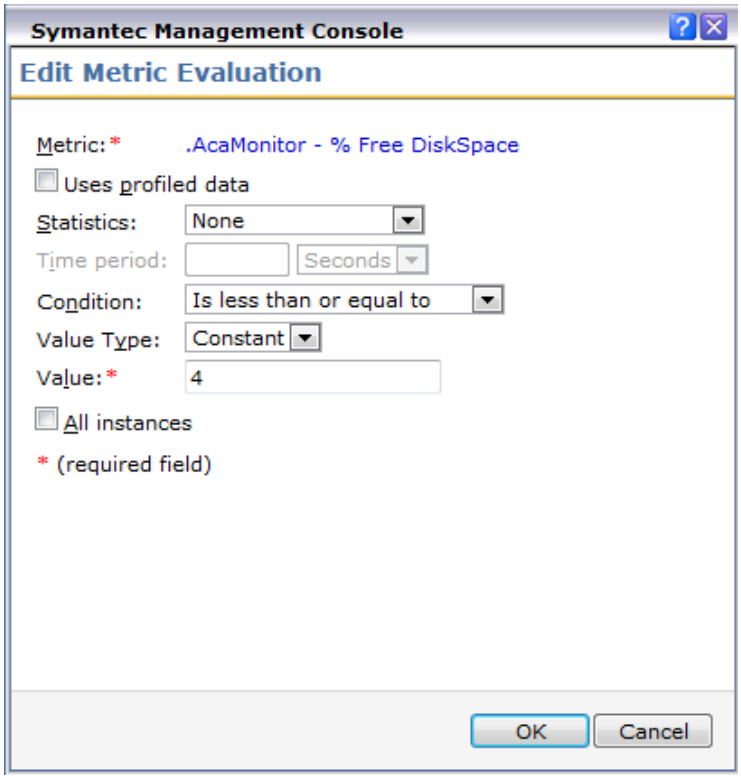
Ensimmäisenä toteutustapana asiakaslaitteen tavoitettavuudelle käytettiin SMP:n asennuksen mukana tulevaa sykäystä (Heartbeat). Valvonnan liitännäinen (Monitor Plug-in) voi lähettää valvontapalvelimelle (Notification Server) ajastettuja viestejä. Näitä ajastettuja viestejä kutsutaan sykäyksiksi. Sykäyksien avulla voidaan seurata vastaako asiakaslaitteen valvonnan liitännäinen valvontapalvelimelle. Tällä tavoin varmistetaan laitteiden välinen kommunikaatio. Samalla sykäykset lähettävät myös tiedon siitä, kuinka kauan asiakaslaite ja sen valvonnan liitännäinen on ollut päällä. Eli tällä tavoin voidaan olettaa, että asiakaslaite on päällä ja toiminnassa, mikäli liitännäinen vastaa. Vastaavasti jos liitännäinen ei vastaa, voidaan epäillä asiakaslaitteessa olevan jotain vikaa. Esimerkiksi vika voi olla liitännäisessä, joka ei yksinkertaisesti vastaa valvontapalvelimelle tai laitteiden välillä voi olla verkkovika. Mikäli sykäys epäonnistuu, tapahtumakonsoliin ilmestyy hälytys, jonka taso on kriittinen. [7, s. 22–23.]

Toisena toteutustapana käytettiin valvontasääntöä, joka tekee ICMP ping -testin asiakaslaitteelle. Ping on yksinkertainen verkkotyökalu, jonka avulla voidaan kokeilla laitteiden tavoitettavuutta verkossa. Ping mittaa samalla, kuinka kauan lähetetylle testiviestille kestää saada vastaus kohdelaitteelta. Yleensä normaaleissa vastausajoissa puhutaan muutamista millisekunneista. ICMP tulee sanoista Internet Control Message Protocol. Se on protokolla, jonka avulla on tarkoitus ilmoittaa yksinkertaisia viestejä toiselle laitteelle. ICMP:n avulla ei yleensä siirretä dataa laitteiden välillä, vaan ilmoitetaan esimerkiksi virhetilanteesta. Kyseinen valvontasääntö löytyy valmiiksi SMP:n asennuksen myötä. Valvontasäännön toiminta ei vaadi agentin asentamista asiakaslaitteelle, joten kyseessä on myös agentiton sääntö. Agentiton valvonta teoriassa käsitellään luvussa 3.4.

Kuten luvussa 2 mainitaan, oli asiakaslaitteiden fyysisten laiteosien valvonta myös erittäin tärkeää toteutuksen kannalta. Ensimmäiseksi halusimme valvoa jokaisen palvelimen kiintolevyjen käyttöä. Kiintolevy on tietokoneeseen asennettava fyysinen massamuisti, johon tallennetaan esimerkiksi ohjelmat ja muut tiedostot. Tieto säilyy kiintolevyllä, vaikka tietokone sammutettaisiin, toisin kuin käyttömuistin (RAM) sisältämä tieto.

Kiintolevyjen käyttöä ja toimintaa seurattiin usealla valvontasäännöllä. Pelkästään raportoinnin ja informaation kannalta seurattiin kiintolevyille kohdistuvia kirjoitus- ja lukupyyntöjen määrää tietyllä aikavälillä. Tässä tapauksessa puhutaan termistä Average Disk Queue Length. Lisäksi kiintolevyjen vapaata tilaa päätettiin seurata kolmiportaisesti. Ensimmäinen hälytys (varoitus) levyjen täyttymisestä aktivoituu, jos levyjen vapaa kapasiteetti on 6-10 prosenttia. Seuraava hälytys (vakava) aktivoituu, mikäli vapaa tila on 4-6 prosenttia. Vakavan hälytyksen aktivoitumisesta generoituu tehtäväkonsolin ilmoituksen lisäksi työpyyntö työnohjausjärjestelmään. Viimeinen hälytystaso (kriittinen) aktivoituu, mikäli vapaa tila kiintolevyllä laskee alle neljän prosentin. Kriittisestä hälytyksestä järjestelmä lähettää myös tekstiviestin päivystäjän kännykkään. Eli hälytystasojen tehtävät toimivat, kuten hälytystasot esiteltiin aikaisemmin tässä luvussa.

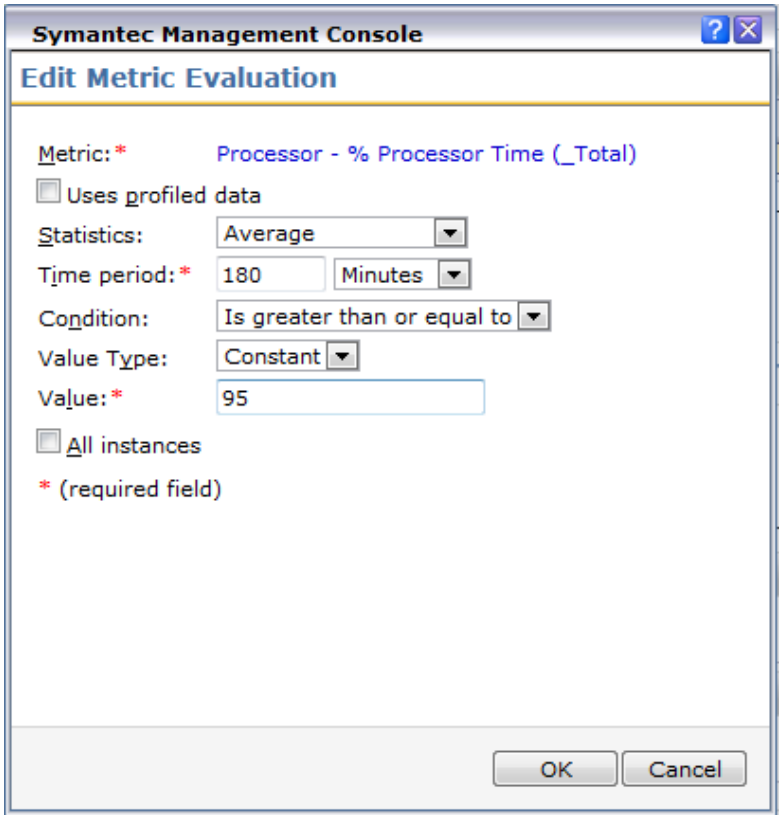
Lisäksi yrityksessä sovittiin, että tarvittaessa palvelimilla käytetään paikallisesti tiettyä kiintolevytunnusta varmistuksien käyttöön. Kiintolevytunnuksella tarkoitetaan kiintolevyn tunnuskirjainta eli esimerkiksi C-kirjain. Varmistuslevyn täyttymistä seurattiin tietyllä säännöllä. Vakava hälytys aktivoituu, mikäli varmistuslevyn vapaa tila on alle yksi prosentti 12 tunnin ajalta. Kuvassa 9 on esitetty esimerkkinä konfiguraatio kriittisestä levytilan täyttymisestä.



Kuva 9. Levytilan kriittinen hälytys

Toisena fyysisenä laiteosana seurattiin palvelimien prosessorien käyttöastetta. Käyttöasteen seuraamiselle halusimme kuitenkin järkevät rajat, koska yleensä tietokoneen prosessorin käyttöaste vaihtelee todella suurella skaalalla. Tämä osoittautuu varsinkin silloin jos prosessorilla on työtä pienillä aikaväleillä ja kohtuullisella kuormalla. Halusimme siis poistaa sellaiset yleiset tapaukset, joissa palvelimet tekee esimerkiksi varmistuksia, datan siivouksia tai muita raskaampia suorituksia isolla kuormalla. Nämä toimenpiteet ajoitetaan ja suoritetaan yleensä yöaikaan.

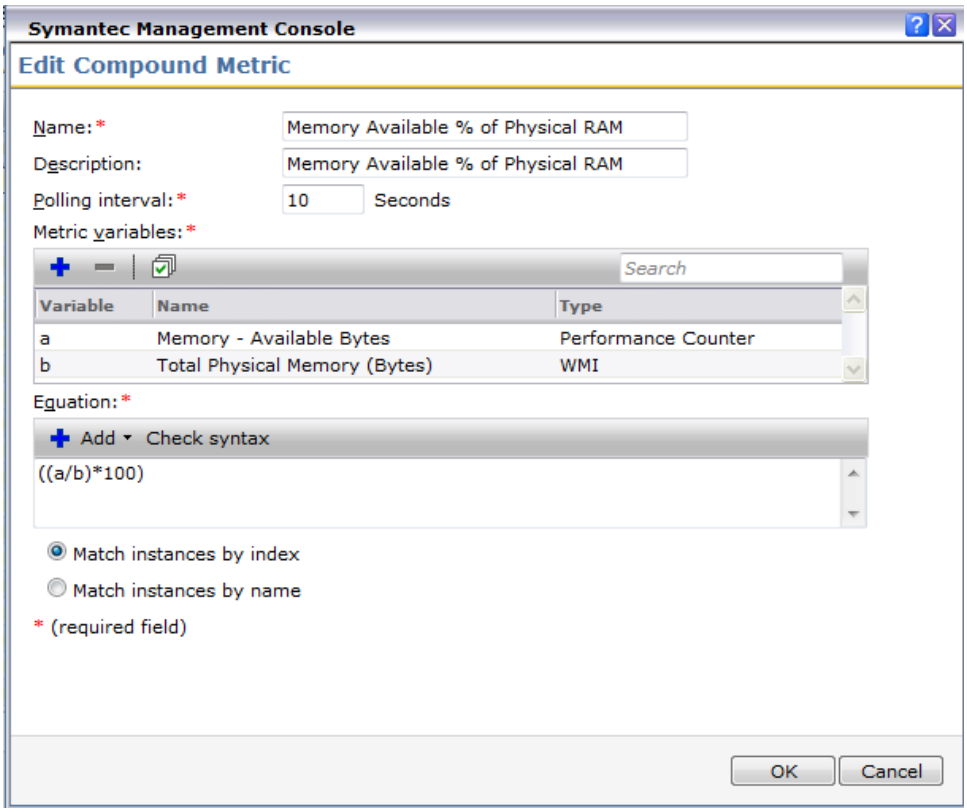
Prosessorin käyttöasteen valvonta ja hälytys päätettiin toteuttaa kahdessa tasossa. Lisäksi toteutuksessa käytettiin hyväksi SMP:n metriikoihin liittyvää statistiikkaominaisuutta. Prosessorin käyttöastetta valvova sääntö ja metriikka aktivoituvat, jos kerätyn statistiikan keskiarvo ylittää asetetun raja-arvon tietyllä aikavälillä. Tällä tavalla eliminoitiin hetkelliset kuormat ja piikit prosessorin käyttöasteessa. Ensimmäinen hälytys (varoitus) aktivoituu, jos palvelimen keskimääräinen prosessorin käyttöaste on yli 80 prosenttia yli kolme tuntia. Vakava hälytys aktivoituu vastaavasti, jos käyttöaste on yli 95 prosenttia yli kolmen tunnin ajan. Kuvassa 10 on esitetty esimerkkinä konfiguraatio vakavasta prosessorin käyttöasteesta.



Kuva 10. Prosessorin käyttöasteen vakava hälytys

Kolmantena fyysisenä laiteosana seurattiin palvelimien keskusmuistin (RAM) käyttöastetta. Sama käyttöasteen vaihtelun suuruus pätee myös keskusmuistille, kuten prosessorin käyttöasteelle. Keskusmuistin tapauksessa haluttiin käyttää ainoastaan varoitustason hälytystä, mikäli käyttöaste nousee liian korkeaksi. Koimme sen tässä tapauksessa riittäväksi, koska harvemmin keskusmuistin käyttöaste nousee korkealle, mikäli muistia on asennettu tarpeeksi laitteeseen. Yleensä prosessin jumiutuminen tai joku muu ohjelma kuitenkin saattaa nostaa käyttöasteen korkealle liian pitkäksi aikaa, jolloin palvelin saattaa kaatua.

Keskusmuistin käyttöasteen seuraamiseen käytettiin tässäkin tapauksessa metriikan statistiikan keskiarvoa. Lisäksi käyttöasteen laskemiseen käytettiin yhdistelmämetriikkaa, joka esitellään luvussa 3.3.4. Kuvassa 11 on esitetty käytetty yhdistelmämetriikka, jonka avulla käyttöaste lasketaan. Metriikka laskee vapaan muistin prosenttiosuuden vertaamalla vapaata keskusmuistia käytettyyn keskusmuistiin mittaushetkellä. Jos keskusmuistin vapaa tila on alle viisi prosenttia yli kolme tuntia, aktivoituu varoituksen tasoinen hälytys.



Kuva 11. Yhdistelmämetriikka vapaan keskusmuistin laskemiseksi

Olennainen tieto asiakaslaitteen verkossa olon lisäksi oli myös se, kuinka kauan asiakaslaite ja agentti ovat olleet päällä. Varsinkin palvelinmaailmassa koneilla on taipumus ajan myötä alkaa hidastumaan. Lisäksi palvelimet saattavat olla epävakaita, mikäli niitä ei välillä käynnistetä uudelleen. Palvelimen liian pitkä yhtäjaksoinen käyminen ei tässä projektissa pitäisi olla ongelma, koska valvonnan lisäksi suunniteltiin päivitysrutiinit valvottaville asiakaslaitteille. Päivitysrutiinien yhteydessä asiakaslaitteet käynnistetään aina uudelleen, jolloin palvelimen päällä olemisen aika nollautuu. Päivitysrutiinit ja siihen liittyvä teoria esitellään luvussa 3.5. Lisäksi projektissa tehty päivitysrutiini ja suoritus esitellään luvussa 4.3.3.

Halusimme kuitenkin varmistua siitä, että varoitus on myös olemassa, mikäli joku asiakaslaite on liian kauan päällä. Päätimme varoittaa kahdessa varoitusportaassa. Ensimmäinen hälytys aktivoituu, mikäli asiakaslaite on yli kaksi kuukautta, mutta alle kolme kuukautta yhtäjaksoisesti päällä. Järjestelmä tekee varoitustason hälytyksen, mikäli hälytys aktivoituu. Vakavan tason hälytys aktivoituu jos asiakaslaite on yli kolme kuukautta päällä. Tällä tavoin varmistetaan, että viimeistään kolmen kuukauden jälkeen luodaan työpyyntö asiasta, mikäli varoitukseen ei ole reagoitu.

Windows-palvelimet ilmoittavat lähes kaiken epänormaalin käytöksen ja virhetilanteet tapahtumienvalvonnassa (Event Viewer). Tapahtumienvalvonta on siis toisin sanoen palvelimen tapahtumien lokikokoelma. Palvelin merkitsee kuitenkin tapahtumia hyvin herkästi, varsinkin jos kysymyksessä varoituksen tasoinen lokimerkintä. Tässä tapauksessa meidän täytyi kartoittaa huolellisesti kaikki oleellisimmat lokitiedostot, joita seurataan valvonnassa.

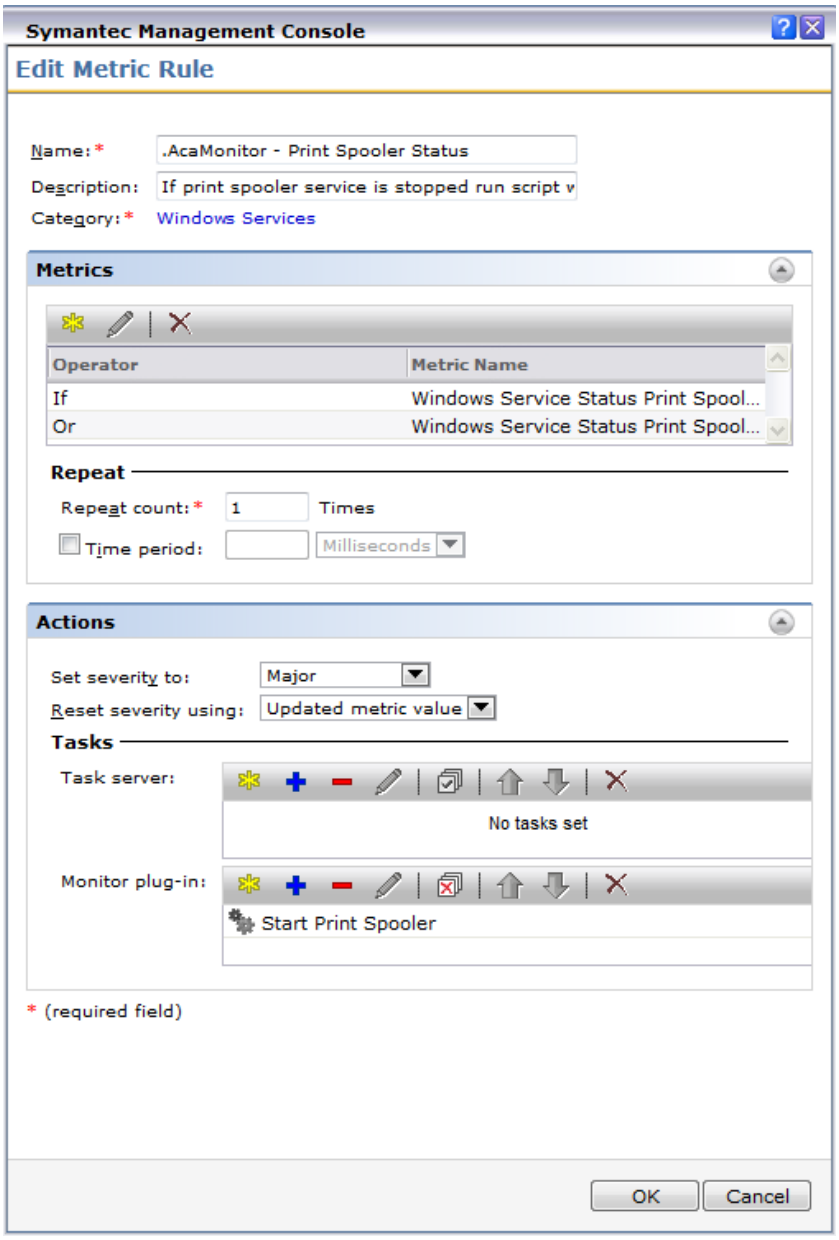
Palvelimen yleisen toimivuuden kannalta päätettiin, että seurataan ainoastaan kriittisiä lokimerkintöjä. Tapahtumienvalvonnassa löytyy kuitenkin useampi kategoria, joihin palvelimen virhetilanteet merkitään. Tässä tapauksessa valittiin ainoastaan kriittisen tason lokit, jotka ilmenevät järjestelmä- tai sovelluskategoriassa. Näihin kahteen kategoriaan tulee lähes poikkeuksetta kaikki tärkeimmät ja kriittisimmät virhemerkinnät. Järjestelmäkategoriaan tulee kaikki palvelinta itseään koskevat ilmoitukset, kuten esimerkiksi fyysisten osien virhetapahtumat. Sovelluskategoriaan merkitään yleensä kaikki ilmoitukset, jotka muodostuvat palvelimelle asennetuista sovelluksista ja ohjelmista.

Otimme myös valvonnassa seurantaan, mikäli Service Control Manager (SCM) merkitsee järjestelmäkategoriaan virhe- tai kriittisen lokin. Palveluiden hallintamanageri (Service Control Manager) on Windows-käyttöjärjestelmän prosessi, joka on yhteydessä käyttöjärjestelmän palveluprosessien kanssa (Service). SCM:n toiminta on kriittistä, koska se käynnistää viiveellä tai ilman, mutta tarvittaessa pysäyttää palvelun. [9.] Toisin sanoen palvelimen palveluita ei pystytä hallitsemaan, mikäli SCM ei toimi oikein. Sekä tästä että itse palveluiden valvonnallisista syistä, palveluiden hallintamanagerin seuranta oli erityisen tärkeää.

Palvelimien ylläpitämät ohjelmat ja resurssit toimivat pääasiassa tiettyjen prosessien (Process) ja palveluiden (Service) avulla. Palvelimen tärkeimpien omaisuuksien ja ohjelmien prosessit ja palvelut ovat sen elinehto. Siksi on tärkeätä kartoittaa etukäteen, minkälaisia asiakaslaitteita tullaan valvomaan. Asiakaslaitteiden kartoitus tehtiin pääasiassa sääntöjen suunnittelun ohessa, mutta jouduimme myös toteutuksen aikana muokkaamaan ja lisäämään valvottavia palveluita. Tämä johtui yleensä siitä, että tietyn ohjelman valvominen sisältää useita kriittisiä palveluita ja prosesseja.

Yksi tärkeä valvontakohde palveluiden osalta on palvelinympäristön peruspalvelut, joita palvelimet toteuttavat. Kaikki peruspalvelut eivät ole välttämättä asennettu kaikkiin palvelimiin. Näin palveluille jää enemmän resursseja käytettäväksi, mikäli ne ovat asennettu omille palvelimille. Useamman palvelimen konfiguraatio tekee palvelinympäristöstä myös vikasietoisemman. Kaikkia palveluita valvottiin siten, että jos tietty palvelu on pysähtynyt tai taukotilassa, niin hälytys aktivoituu. Lisäksi säännöille määriteltiin automaattinen tehtävä käynnistää palvelu uudelleen asiakaslaitteella, mikäli hälytys aktivoituu. Tehtävät ja niihin liittyvät ominaisuudet on teoriassa käsitelty luvussa 3.3.4.

Ensimmäinen tärkeä peruspalvelu on tulostuspalvelu. Jokaisesta Windows-tietokoneesta löytyy tulostuksen välitallennusohjelma (Print Spooler). Palvelun tehtävä on pitää huolta jonoon asetetuista tulostuspyynnöistä. Toisin sanoen kun käyttäjä haluaa tulostaa dokumentin, tulostusprosessi siirtyy palvelulle. Tämä tapahtuma vapauttaa myös prosessorin muihin tehtäviin, mikäli tulostin on varattuna. Kun tulostin vapautuu, välitallennusohjelma käskee tulostinta tulostamaan jonossa olevan dokumentin. Lisäksi palvelulla on muitakin tehtäviä. Se pitää huolta, mikä tulostustyö menee millekin tulostimelle, huolehtii jaetuista verkkotulostimista sekä pitää kirjaa, mikä laite on kytketty mihinkin porttiin. [10.]



Kuva 12. Tulostuspalvelun seuranta

Kuvassa 12 on esitetty esimerkkinä tulostuksen välitallennus -palvelun konfiguraatio. Yläreunasta löytyvät säännön nimi ja vapaavalintainen tarkennus. Metriikoista (Metrics) löytyy ehtolause tai -lauseet, joiden mukaisesti sääntö ja hälytys aktivoituvat. Kuten aikaisemmin mainittiin, peruspalveluiden hälytys aktivoituu, jos palvelu on pysähtynyt tai taukotilassa. Toimenpiteistä (Actions) löytyy, mikä on hälytyksen taso ja mitä arvoa käytetään kun valvontapalvelin kysyy tietyn ajan jälkeen palvelun tilaa uudelleen asiakaslaitteen agentilta. Tässä tapauksessa hälytystaso on vakava (Major) ja arvona käytetään päivitettyä arvoa (Updated Metric Value) eli mikä on saatu asiakaslaitteen agentilta uuden kyselyn yhteydessä.

Tehtävistä (Tasks) löytyvät automaattisesti suoritettava tehtävät, mikäli hälytys aktivoituu. Tässä tapauksessa valvontapalvelimelta saatu sääntö käskee valvonnan liitännäistä (Monitor Plug-in) käynnistämään palvelun uudelleen. Agentti lataa käytännöt ja säännöt valvontapalvelimelta tietyin väliajoin. Latauksen jälkeen säännöt ja tehtävät suoritetaan asiakaslaitteella, vaikka agentti ei olisi yhteydessä valvontapalvelimeen [7, s. 69]. Jos uudelleenkäynnistys onnistuu, käyttää valvontapalvelin seuraavaa säännölle päivitettyä arvoa. Tämä tarkoittaa sitä, että hälytys kuitataan ja se häviää itsestään SMC:n tapahtumakonsolista (Event Console).

Toinen tärkeä valvottava kohde peruspalveluissa on nimipalvelin ja siihen liittyvä palvelu. Nimipalvelimen olennaisin käsite ja palvelu on DNS (Domain Name System). DNS on nimipalvelujärjestelmä, jonka tarkoituksena on kääntää laitteiden, Internet-sivujen ja muiden resurssien nimiä IP-osoitteiksi (Internet Protocol). Laitteet ja resurssit voivat sijaita missä tahansa Internetissä tai yksityisessä verkossa. IP-osoite on jokaisen verkkolaitteen yksilöivä numerosarja, jonka avulla se kommunikoi muiden laitteiden kanssa verkossa. Toisin sanoen DNS voi olla esimerkiksi puhelinluettelo, joka kääntää osoitteen www.esimerkki.fi, IP-osoitteeksi 192.0.43.10. Ihmisen on huomattavasti helpompi muistaa kuvaava Internet-osoite, kuin sitä vastaava IP-osoite. [11.]

Kolmas palvelu on IP-osoitteisiin liittyvä protokolla, joka on DHCP (Dynamic Host Configuration Protocol). Se on protokolla ja samalla palvelun omaava laite, joka antaa asiakaslaitteelle käytettäväksi IP-osoitteen määritellystä IP-verkosta. IP-osoite voidaan antaa ennalta määritellyksi ajaksi tai pysyvästi. Lisäksi laite antaa protokollan avulla tiedon käytettävästä nimipalvelimesta sekä oletusyhdyskäytävän IP-osoitteen. Oletusyhdyskäytävän IP-osoite on verkkolaitteella, joka reitittää asiakaslaitteiden verkkoliikenteen tarvittaessa Internetiin. [12.]

Neljäs ja viimeinen tässä projektissa valvottu peruspalvelu on IIS (Internet Information Services). Se on Microsoft-yrityksen kehittämä web server -rooli, joka kuuluu osana Windows Server -käyttöjärjestelmiä. IIS kuuluu käyttöjärjestelmiin Windows Server 2000 -versiosta lähtien. Rooli tekee palvelimesta web serverin, jonka avulla esimerkiksi yritys voi jakaa informaatiota työntekijöiden ja muiden Internet-käyttäjien kanssa. Jaettu informaatio voi olla vaikkapa yrityksen julkiset ja sisäiset Internet-sivut. Web serveriin voi halutessaan lisätä erialisia lisäominaisuuksia perusasennuksen lisäksi. Ne parantavat web serverin tietoturvaa, koska kaikkia ominaisuuksia ei asenneta normaaliasen-

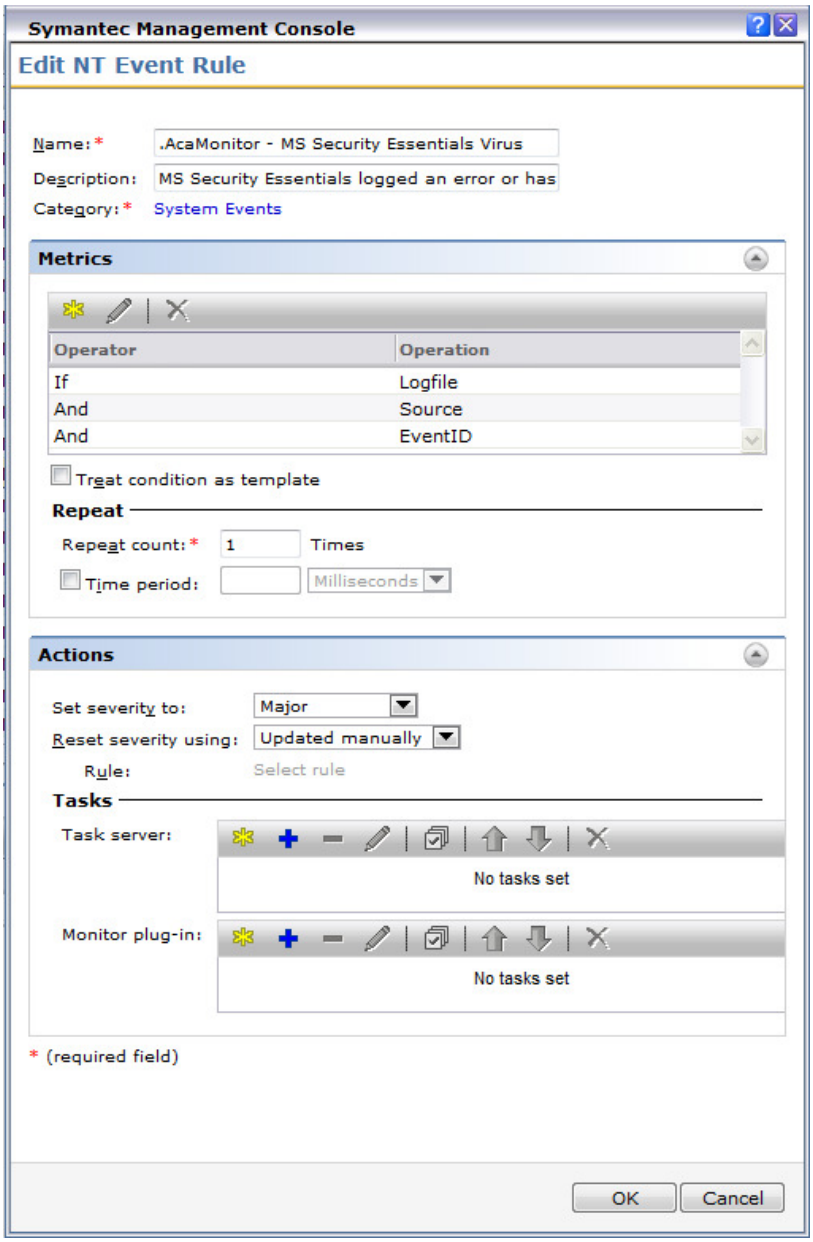
nuksen yhteydessä. Lisäominaisuuksien asennus tuo toisaalta joustavuutta web serverin ylläpitämiseen. [13.]

Peruspalveluiden lisäksi valvoimme Academica Oy:n asiakkaiden palvelimille asennettuja virustorjuntaohjelmia. Tämäkin suoritettiin valvomalla virustorjuntaohjelmien tärkeimpiä palveluja ja prosesseja. Valvottavat virustorjuntaohjelmat olivat Microsoft Security Essentials, Symantec Endpoint Protection ja F-Secure.

Virustorjuntaohjelmien palveluiden ja prosessien lisäksi valvoimme palvelimia, mikäli niihin iskee virus. Viruksella tarkoitetaan yleensä haittaohjelmaa tai koodia, joka yritetään saada kohdelaitteeseen tai sillä pyritään häiritsemään esimerkiksi verkkoliikennettä. Viruksen avulla levittäjä voi saada tärkeitä tallennettuja tietoja kohdelaitteesta tai ylipäätänsä seurata laitteen toimintaa, mikäli siellä tulee tapahtumaan jotain mielenkiintoista.

Jokainen virustorjuntaohjelma luo omalla tietyllä tapahtumatunnuksella (Event ID) tapahtumienvalvontaan (Event Viewer) lokin viruksesta. Valvonnassa seurataan ainoastaan lokeja, jotka muodostuvat tietyllä nimellä, tapahtumatunnuksella sekä kuuluvat tiettyyn kategoriaan. Symantec Endpoint Protection ja F-Secure luovat lokinsa sovelluskategoriaan. Microsoft Security Essentials luo lokinsa vastaavasti järjestelmäkategoriaan.

Virushälytys aktivoituu, jos tarkasti määritelty loki muodostuu asiakaslaitteessa. Virustorjuntaohjelmien prosessit on määritelty hälytystasolle varoitus. Vastaavasti palvelut ja virushälytys luodaan vakavana hälytyksenä. Palveluiden hälytys aktivoi jokaiselle palvelulle automaattisen uudelleenkäynnistyksen, jonka myötä prosessikin käynnistyy uudelleen asiakaslaitteella. Vastaavasti virushälytys on manuaalisesti ratkaistava tapahtumakonsolista, koska se myös todennäköisesti aiheuttaa vähintään tarkistustoimenpiteitä asiakaslaitteella. Eli palvelinvalvojan tulee tarkistaa asiakaslaitteen ja uhkan tilanne ennen kuin ratkaisee hälytyksen tapahtumakonsolista.



Kuva 13. Virus löytynyt Microsoft Security Essentials -virustorjuntaohjelmalla

Kuvassa 13 on esimerkkinä konfiguraatio, jos Microsoft Security Essentials -virustorjuntaohjelma löytää viruksen valvottavalta palvelimelta. Kuvan yläreunassa näkyvät säännön nimi ja vapaamuotoinen tarkennusteksti. Ehtolauseita löytyy kolme kappaletta. Ensimmäinen ehtolause vaatii, että loki pitää löytyä järjestelmäkategoriasta. Toinen sääntö vaatii ensimmäisen lisäksi, että lokin lähde on Microsoft Security Essentials -virustorjuntaohjelma. Kolmas sääntö vaatii kahden edellisen lisäksi, että lokin tapahtumatunnus (Event ID) tulee olla 1116. Nämä kolme ehtolausetta yhdessä aktivoivat säännön ja hälytyksen. Virushälytys täytyy manuaalisesti ratkaista tehtäväkonsolista, joten sille ei ole määritelty automaattista toimenpidettä.

Valvonta ja säännöt, jotka on kuvailtu tähän mennessä luvussa 4.3.1, ovat normaali valvontakäytäntö (Basic Monitor Policy). Se otetaan käyttöön kaikkiin palvelimiin, jotka liitetään Academica Oy:n palvelinvalvontajärjestelmään. Edellä mainittujen sääntöjen avulla valvotaan siis jokaisen palvelimen keskeisiä ja tärkeitä resursseja, jotka ovat välttämättömiä sen toiminnan kannalta.

Valvonnassa täytyi ottaa kuitenkin huomioon myös palvelinympäristössä olevien laitteiden eri roolit. Palvelimelle voidaan asentaa erilaisia rooleja, jona se toimii palvelinympäristössä. Roolit kuuluvat valmiiksi Windows Server -käyttöjärjestelmiin, mutta niitä ei asenneta käyttöjärjestelmän asennuksen yhteydessä. Projektin tapauksessa roolipalvelimena tarkoitetaan myös sellaisia laitteita, joihin on asennettu Microsoftin tai kolmannen osapuolen suurempia ohjelmistokokonaisuuksia. Palvelimen rooli voi olla esimerkiksi aikaisemmin mainitut DNS tai IIS. Roolipalvelimia valvottiin selkeyden ja palvelinvalvontajärjestelmän ylläpidon helpottamisen vuoksi omilla käytännöillä (Policy). Omat valvontakäytännöt mahdollistivat myös SMP:n ryhmien (Groups) käytön, joka käsitellään luvussa 4.3.2.

Roolipalvelimiksi valittiin laitteet, jotka ovat

- toimialueen hallintapalvelimet (Domain Controller Server)
- tietokantapalvelimet (Microsoft SQL Server)
- sähköpostipalvelimet (Microsoft Exchange Server)
- citrix-palvelimet.

Jokaiselle roolipalvelintyypille luotiin oma valvontakäytäntö paitsi toimialuepalvelimille. Omien käytäntöjen avulla pystytään normaalin valvontakäytännön lisäksi seuraamaan roolipalvelimien ominaisia ja tärkeitä resursseja. Tällä tavoin pystytään kohdistamaan säännöt juuri sellaisiin palvelimiin, joihin sääntöjen resurssit on varmasti asennettu. Käytäntöjen kohdistaminen myös poistaa mahdolliset turhat hälytykset juuri sellaisissa tapauksissa, joissa resursseja tai palveluja ei ole asennettu asiakaslaitteelle. Lisäksi pystytään tarvittaessa myöhemmin määrittelemään tarkemmin ja paremmin automatisoituja toimenpiteitä ja tehtäviä tietyn roolin omaaville palvelimille.

Toimialueen hallintapalvelin (Domain Controller) on palvelin, joka ylläpitää yrityksen toimialueen (Domain) käyttäjätilejä, tietokoneita sekä muita laitteita ja resursseja. Palvelimelle on asennettu aktiivihakemistopalvelut, jotka takaavat käyttäjätilien ja laitteiden keskitetyn hallinnan yhdestä paikasta. Hallintapalvelimella voidaan organisoida helposti resursseja. Organisoinnin avulla pystytään osoittamaan tiettyjä ryhmäsääntöjä (Group Policy) ja asetuksia halutuille organisaation osille (Object) tai spesifisti tietylle yksilölle. Toimialueen hallintapalvelin vastaa myös käyttäjätilien turvallisesta autentikoinnista. Jos yrityksen työntekijä kirjautuu työkoneelle toimialueen tunnuksella, se tarkistetaan oikeaksi hallintapalvelimen toimesta. Tarkistuksen jälkeen käyttäjä pääsee käyttämään yrityksen tietokonetta.

Toimialueiden hallintapalvelimien tärkeiden resurssien seuranta toteutettiin siten, että määriteltiin päivän välein ajastettu DCDiag-skripti. Skriptin suoritus kohdistettiin tehtyyn Domain Controllers -ryhmään, johon kuului kaikki palvelinvalvonnan toimialueen hallintapalvelimet. Skripti on yksinkertainen kirjoitettu komentokoodi. Sen avulla voidaan räätälöidä ja tehdä yksi tai useampi komento automaattisesti aina kun skripti suoritetaan. DCDiag (Domain Controller Diagnostic Tool) on Windows-käyttöjärjestelmän komentoriviltä käytettävä työkalu. Se analysoi yhden tai palvelinympäristön kaikki toimialueen hallintapalvelimet useilla erilaisilla testeillä. Työkalun tarkoitus on nimenomaan tarkistaa hallintapalvelimen kunto perustesteillä. [14.]

Skripti käskee testin lisäksi valvottavaa palvelinta kirjoittamaan virheestä tapahtumalokin (Event) tapahtumienvalvontaan (Event Viewer). Loki luodaan skriptin avulla sovelluskategoriaan tietyllä tapahtumatunnuksella (1337) ja nimellä (AcaADMonitor). Hälytys aktivoituu, jos spesifisti määritelty loki kirjoitetaan tapahtumienvalvontaan. Eli sääntö seuraa valvottavaa palvelinta, mikäli sinne luodaan tietty loki. Säännön hälytystaso on vakava. Se on osa normaalia valvontakäytäntöä (Basic Monitor Policy), mutta skriptin suoritus on kohdistettu vain tietylle palvelinryhmälle. Suoritettava skripti on esitetty kokonaisuudessaan liitteessä 1.

Tietokantapalvelimia valvottiin omalla käytännöllä (SQL Monitor Policy). Käytäntöön kuuluvat säännöt, jotka valvovat tietokantapalvelimen toiminnan kannalta tärkeitä palveluita sekä yhtä prosessia. Säännöissä noudatetaan samaa tapaa kuin normaalissa valvontakäytännössä. Hälytys aktivoituu, jos palvelun tila on pysähtynyt tai taukotilassa. Sääntö käskee myös automaattisen uudelleenkäynnistyksen määritellylle palvelulle, mikäli hälytys on aktiivinen. Olennaisin tietokantapalvelimen palvelu (SQL Server Ser-

vice) aktivoi ainoana kriittisen hälytyksen. Kriittinen hälytys lähettää tekstiviestin päivystäjän kännykkään, kuten aikaisemmin luvussa mainittiin. Näin varmistetaan, että päivystäjä reagoi tilanteeseen, mikäli palvelu ja itse SQL-palvelin lopettaa toimimasta esimerkiksi yöaikaan.

Sähköpostipalvelimia (Microsoft Exchange Server) valvottiin myös omalla käytännöllä (Exchange Monitor Policy). Yksi sääntö seuraa keskimääräistä sähköpostien toimitusaikaa (Average Delivery Time). Arvoa seurattiin raportoinnin ja statistiikan kannalta. Kyseessä on ainoastaan tietoa keräävä sääntö (Metric Collect), joka ei aktivoi hälytyksiä tai tehtäviä. Mikäli keskimääräinen lähetysaika alkaa kasvamaan huomattavasti voidaan olettaa, että palvelimella on jotain ongelmaa. Toinen sääntö seuraa varmuuden vuoksi onko palvelimen portti 25 auki. Sähköpostipalvelimet käyttävät oletuksena porttia 25 sähköpostien lähettämiseen.

Lisäksi valvontaan kuuluu samankaltainen skripti kuin toimialueen hallintapalvelimille. Skriptissä käytetään myös valmista työkalua sähköpostipalvelimen kunnon selvittämiseksi. Exchange-palvelimelta löytyy palveluiden kuntotarkastus -työkalu (Exchange Service Health Test). Työkalu testaa useilla perustesteillä palvelimen ja palveluiden kunnon. Tämäkin skripti käskee asiakaslaitetta luomaan lokin tapahtumavalvontaan, mikäli vikoja sähköpostipalvelimessa havaitaan.

Kolmas ja tärkein sääntö seuraa, jos palvelimella luodaan skriptin määrittelemä loki. Tapahtumatunnuksen pitää olla 1337, nimen AcaExchMonitor ja lokin täytyy löytyä sovelluskategoriasta. Hälytys aktivoituu tässäkin säännössä kriittisenä, joten tieto hälytyksestä lähtee myös päivystäjälle. Hälytyksen aktivoituminen vaatii lisäksi manuaalisen ratkaisun tapahtumakonsolista. Tällä tavalla varmistetaan, että hälytykseen reagoidaan ja se ratkaistaan tietoisesti. Suoritettava skripti on esitetty kokonaisuudessaan liitteessä 2.

Citrix-palvelimien oma käytäntö (Citrix Monitor Policy) toteutti pääasiassa samaa periaatetta kuin SQL-palvelimien käytäntö (SQL Monitor Policy). Citrix Systems Inc. on monikansallinen ohjelmistoyritys, joka tuottaa pääasiassa virtualisointipalveluja Windows-, Macintosh- ja Linux-ympäristöihin. Palvelujen avulla voidaan virtualisoida esimerkiksi palvelimia ja työasemia. Virtualisoinnilla tarkoitetaan tietoteknistä toteutustapaa. Se mahdollistaa ohjelmistoalustan avulla useamman itsenäisen tietokoneen toiminnan yhden fyysisen tietokoneen komponenteilla ja resursseilla.

Käytäntöön (Citrix Monitor Policy) kuuluvat säännöt, jotka valvovat Citrix-palvelimen tärkeitä palveluita, sekä tietyn järjestelmälokin muodostumista. Säännöissä noudatetaan samaa tyyliä kuin normaalissa valvontakäytännössä (Basic Monitor Policy). Hälytys (vakava) aktivoituu, jos palvelun tila on muu kuin käynnissä ja palvelu on asennettu palvelimelle. Sääntö käskee automaattisen uudelleenkäynnistyksen määrätylle palvelulle, mikäli hälytys on aktiivinen. Lisäksi seurataan asiakaslaitteen lokeja siltä varalta, että Citrix-palvelimen lisenssi on menossa vanhaksi. Lisenssillä tarkoitetaan palvelun käyttöön oikeuttavaa koodia. Citrix-ohjelmisto luo palvelimelle lokin järjestelmäkategoriaan, jonka tapahtumatunnuksena on 9015 ja hälytystasona on varoitus, jos lisenssi on vanhentumassa. Lisenssin vanhentuminen aktivoi myös vakavan hälytyksen. Tällä tavoin varmistetaan, että lokiin reagoidaan, koska Citrix-palvelin lopettaa toimintansa, mikäli lisenssi ehtii vanhentua.

Valvontakäytännöksi muodostuivat

- tavoitettavuuden valvontakäytäntö (Availability Monitor Policy)
- normaali valvontakäytöntö (Basic Monitor Policy)
- citrix-valvontakäytäntö (Citrix Monitor Policy)
- sähköpostin valvontakäytäntö (Exchange Monitor Policy)
- tietokantojen valvontakäytäntö (SQL Monitor Policy).

Kaikki valvottavat kohteet ja palvelut on pyritty läpikäymään toteutukseltaan ja toiminnaltaan luvussa mahdollisimman tarkasti. Sääntöjen yksittäisiä metriikoita ja niiden syvällistä toteutusta ei kuitenkaan tässä työssä käydä läpi. Tarkoituksena oli selventää toteutettu palvelinvalvonta ja sen toiminta konkreettisella tasolla. Kuvassa 14 on esitetty kaikki palvelinvalvontaan toteutetut kohteet ja palvelut mahdollisimman helposti ja yksiselitteisesti.

	SMC	Työpyyntö	Tekstiviesti		
	Varoitus	Vakava	Kriittinen	Lisätieto	Tilan muuttuminen
Hälytettävä asia					
Tavoitettavuus (verkossa olo)				Verkon konfiguraatio	Automaattisesti
Prosessorin käyttöaste (%)	80 %	95 %		Yli kolme tuntia, keskiarvo	Automaattisesti
Kiintolevyn vapaa tila (%)	10 %	6 %	4 %		Automaattisesti
Varmistuslevyn vapaa tila (%)		1 %		Yli 12 tuntia	Automaattisesti
Keskusmuistin käyttöaste (%)	5 %			Yli kolme tuntia, keskiarvo	Automaattisesti
Palvelimen päällä olo	2 kk	3 kk			Automaattisesti
Lokien seuranta (järjestelmä ja ohjelma)		Kriittiset lokit			Manuaalisesti
Lokien seuranta (järjestelmä)		Kriittiset lokit		Palveluiden hallintamanageri	Manuaalisesti
Asiakaslaitteen agentti (toiminta)			15 min	Sykäys (Heartbeat)	Automaattisesti
Virus löytynyt				Tietyt tapahtumatunnukset	Manuaalisesti
Järjestelmät ja palvelut	Palvelut yritetään käynnistää automaattisesti uudelleen.				
Exchange - palvelu			30min	Exchange palvelun tila -skripti	Manuaalisesti
SQL - palvelu		Selain, Agentti, Prosessi	Palvelin		Automaattisesti
Tulostus - palvelu		Palvelun tila		Pysähtynyt tai tauko	Automaattisesti
DHCP - palvelu		Palvelun tila		Pysähtynyt tai tauko	Automaattisesti
DNS - palvelu		Palvelun tila		Pysähtynyt tai tauko	Automaattisesti
IIS - palvelu		Palvelun tila		Pysähtynyt tai tauko	Automaattisesti
Virustorjunta - palvelu		Palvelun tila		Pysähtynyt tai tauko (MS Essentials, SEP, F-Secure)	Automaattisesti
Citrix - palvelu		Palvelun tila		Pysähtynyt tai tauko	Automaattisesti
AD - palvelu		Kerran päivässä		AD:n tila -skripti	Manuaalisesti

Kuva 14. Palvelinvalvonnan valvontakohteet yleisesti

4.3.2 Ryhmät ja kategorisointi

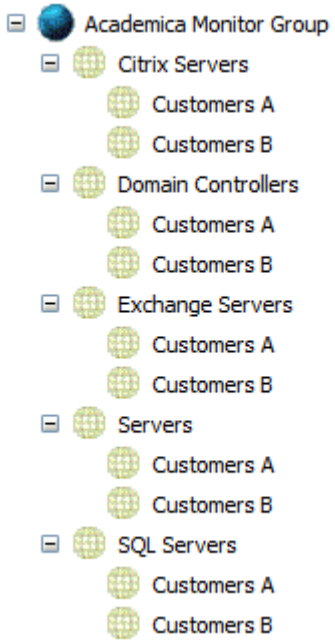
Organisaationäkymä (Organizational View) on SMP:n ominaisuus, jonka avulla voidaan hierarkkisesti ryhmitellä valvottavia resursseja. Sillä voidaan rakentaa todenmukainen rakenne valvottavista ja käytetyistä resursseista. Organisaationäkymät voidaan luoda esimerkiksi yrityksen toimipaikkojen, osastojen tai verkkorakenteen mukaan. Näkymät luodaan siis parhaaksi katsomalla tavalla. Jokainen resurssi voi esiintyä myös ainoastaan kerran organisaationäkymässä. [5, s. 358.]

Symantec Management Consolessa on oletuksena organisaationäkymä, johon kuuluvat kaikki tiedossa olevat asiakaslaitteet ja resurssit. Kun uusi asiakaslaite tai resurssi lisätään CMDB-kantaan, se lisätään myös oletuksena olevaan organisaationäkymään. Oletuksena uudet resurssit organisoidaan tyyppinsä mukaan. Tässä tapauksessa tyyppejä ovat esimerkiksi tietokoneet, käyttäjät ja paketit. Tyypit muodostavat oletuksena olevassa organisaationäkymässä myös organisaatioryhmät (Organizational Group). Organisaatioryhmät jakavat organisaationäkymän pienempiin hallittaviin osiin. Uusia resursseja voidaan kopioida haluttuun organisaationäkymään. [5, s. 358.]

Jokainen uusi resurssi lisätään automaattisesti oletuksena organisaationäkymään, eikä käyttäjä pysty tähän vaikuttamaan. On myös otettava huomioon, että resurssin lisäyksen jälkeen saattaa kestää hetken ennen kuin resurssi näkyy oikeassa organisaationäkymässä. Uudet resurssit lisätään oletuksena ylimmällä tasolla olevaan organisaatioryhmään ja pysyvät siellä niin kauan kun paikkaa ei vaihdeta käyttäjän toimesta. Resursseja voidaan myös poistaa mistä tahansa organisaationäkymästä paitsi oletuksena olevasta. Kun resurssi poistetaan CMDB-kannasta, se poistetaan myös automaattisesti kaikista organisaationäkymistä. [5, s. 358.]

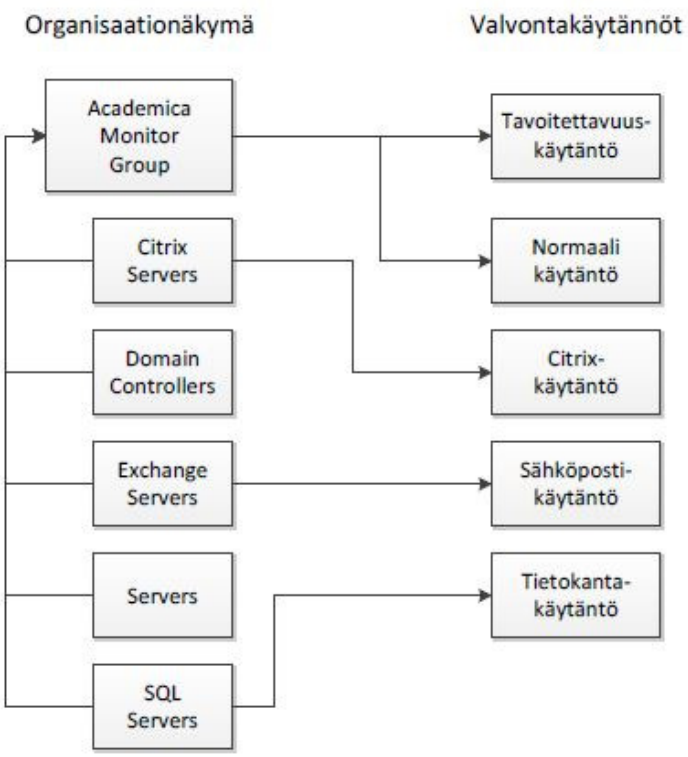
Palvelinvalvontaa ja tietoturvapäivityksiä ajatellen luotiin yksi organisaationäkymä (Academica Monitor Group). Tähän näkymään lisättiin kaikki palvelinvalvontaan liitettävät palvelimet. Organisaationäkymän alle luotiin lisäksi organisaatioryhmät valvontakäytäntöjen (Monitor Policy) mukaisesti. Jokaisen organisaatioryhmän alle luotiin vielä kaksi organisaatioryhmää, joihin jaettiin kahteen osaan asiakaspalvelimet riippuen palvelinroolista. Jakaminen tehtiin tietoturvapäivitysten asentamisen helpottamiseksi.

Valvontakäytännöt ja niiden toimintaperiaate on esitetty luvussa 4.3.1. Organisaationäkymän ja -ryhmien merkitys tietoturvapäivitysten kannalta on esitetty luvussa 4.3.3. Kuvassa 15 on esitetty edellisessä kappaleessa kuvattu organisaationäkymä ja -ryhmät.



Kuva 15. Organisaationäkymä ja -ryhmät

Organisaationäkymän ja -ryhmien luomisella on tarkoitus helpottaa palvelinvalvonnan ylläpitoa myös projektin jälkeen. Ryhmien avulla voidaan erittäin helposti kohdistaa haluttuja käytäntöjä ja sääntöjä. Kun ryhmä asetetaan käytännön tai säännön kohteeksi se kohdistuu kaikkiin ryhmässä oleviin asiakaslaitteisiin automaattisesti. Tämä helpottaa myös uusien asiakaslaitteiden lisäämistä. Kun uusi asiakaslaite liitetään johonkin ryhmään se saa automaattisesti ryhmälle kohdistetut valvontakäytännöt ja -säännöt. Täytyy kuitenkin muistaa, että agenttiin täytyy olla asennettuna valvonnan liitännäinen (Monitor Plug-in) ennen kuin käytännöt ja säännöt astuvat voimaan asiakaslaitteessa.



Kuva 16. Valvontakäytäntöjen kohdistuminen organisaatioryhmiin

Kuvassa 16 on esitetty, mitkä aikaisemmassa luvussa mainituista valvontakäytännöistä on kohdistettu millekin organisaatioryhmälle. Tavoitettavuuskäytäntö (Availability Monitor Policy) ja normaali käytäntö (Basic Monitor Policy) vaikuttavat organisaationäkymään (Academica Monitor Group). Toisin sanoen ne vaikuttavat kaikkiin valvottaviin palvelimiin, koska organisaationäkymään kuuluvat kaikki organisaatioryhmät. Lisäksi Citrix-palvelimille kohdistetaan Citrix-käytäntö ja Exchange-palvelimille sähköpostikäytäntö. Samoin tietokantapalvelimille kohdistetaan lisäksi tietokantakäytäntö. Eli organisaatioryhmille on kohdistettu valvontakäytännöt, kuten luvussa 4.3.1 on esitetty.

4.3.3 Windows-tietoturvapäivitykset

Palvelinvalvonnan lisäksi Academica Oy halusi rutiinipohjan Windows-tietoturvapäivityksille. Valmiin pohjan avulla yritys suorittaisi jatkossa kerran kuussa hallitun tietoturvapäivitysrutiinin palvelinvalvontaan kuuluville palvelimille. Päivitysten avulla pyritään poistamaan asiakaslaitteiden käyttöjärjestelmissä esiintyviä ongelmia sekä parantamaan tietoturvaa. Tarkoitus on pitää palvelimet jatkuvasti ajan tasalla ja toimintakuntoisina. Lisäksi tietoturvapäivitykset ja asennukset käynnistävät palvelimet automaattisesti uudelleen. Tällä toteutuksella palvelimet eivät ehdi olemaan liian pitkään yhtäjaksoisesti päällä sekä jumiutumaan ajan myötä. Yhtäjaksoista asiakaslaitteen käymistä seurattiin kuitenkin varmuuden vuoksi myös säännöllä, joka on esitetty luvussa 4.3.1. Tietoturvapäivityksiin ja niiden jakeluihin liittyvä teoria on esitetty luvussa 3.5.

Luvussa 4.3.2 esitetty organisaationäkymä luotiin valvonnan lisäksi tietoturvapäivityksiä silmällä pitäen. Academica Oy:n kanssa sovittiin, että palvelinvalvontaan lisättävät asiakaslaitteet jaetaan kahteen ryhmään (Customers A ja Customers B). Molemmille ryhmille jaetaan kuukausittain määritetyt kriittiset tietoturvapäivitykset kahden peräkkäisen yön aikana. Tällä tavoin pyrittiin vähentämään verkkokuormaa verrattuna tilanteeseen, jossa kaikille palvelinvalvontaan kuuluville palvelimille jaettaisiin tietoturvapäivitykset saman yön aikana. Kahden ryhmän käyttö toteutuksessa antaa paremman vikasietoisuuden. Asiakaslaitteiden jakaminen antaa myös mahdollisuuden reagoida tilanteeseen paremmin ja nopeammin, jos johonkin asiakaslaitteeseen päivitykset eivät asennu oikein tai jokin päivitys rikkoo palvelimen toiminnan.

Academica Oy halusi luonnollisesti lisätä myös oman palvelinympäristönsä valvonnan piiriin. Yrityksen palvelimien seuranta ei poikennut mitenkään asiakaspalvelimien valvonnasta. Valvonta suoritettiin täsmälleen samoilla käytännöillä ja säännöillä kuin asiakaslaitteiden palvelinvalvonta. Yrityksen omat palvelimet olivat kuitenkin tietoturvapäivitysten jakelemisen kannalta tärkeässä roolissa. Sovimme yrityksen kanssa, että kuukausittaiseen rutiiniin kuuluvat tietoturvapäivitykset asennetaan yrityksen palvelimille ennen kuin ne jaetaan keskitetysti asiakkaille. Toteutustavalla pystytään testaamaan jaettavat tietoturvapäivitykset ennen niiden jakelua asiakkaille. Testauksen avulla pystytään todentamaan jaettavien päivitysten toimivuus, sekä ehkäisemään ennalta virhetilanteet asiakkaiden palvelimilla.

Asiakaslaitteille tietoturvapäivitykset päätettiin jakaa kahden peräkkäisen yön aikana. Kahteen osaan jaetut asiakaslaitteet (Customers A ja Customers B) jaettiin vielä kahteen osaan. Toteutustapa parantaa vikasietoisuutta ja pienentää verkkokuormaa entisestään. Jakamisen avulla pystytään keskeyttämään jakelu muutamassa vaiheessa, mikäli vasta asiakaslaitteiden päivitysrutiinin yhteydessä havaitaan haitallinen päivitys.

Tietoturvapäivitysten jakelu suoritetaan neljällä agenttien päivitysliitännäisiä (Update Plug-in) käskevällä käytännöllä (Update Plug-in Policy). Käytäntöihin ajastetaan jokaisella rutiinikerralla ajankohdat, jolloin kohteeksi asetetuille asiakaslaitteille ladataan ja asennetaan tietoturvapäivitykset. Käytäntöjen kohdistamista ei tarvinnut ensimmäisen kerran jälkeen muuttaa, koska ne ovat toteutettu luvussa 4.3.2 esitettyjen organisaatioryhmien avulla. Kun uusi laite liitetään oikeaan organisaatioryhmään, se liitetään samalla automaattisesti oikeaan päivityskäytäntöön. Uusi asiakaslaite saa tietoturvapäivitykset kun siihen on asennettu myös agentin päivitysliitännäinen. Liitännäisen asentaminen asiakaslaitteille suoritetaan myös automaattisen käytännön avulla.

Ensimmäiseksi päivitetään ensimmäiseen asiakasryhmään (Customers A) ja ensimmäiseen puolikkaaseen (Set 1) kuuluvat asiakaslaitteet. Päivityspuolikas käsketään lataamaan ja päivittämään päivitykset käytännön määräämänä päivänä kello kahdeksan illalla. Lisäksi ajastukseen on määritetty, että lataus ja päivitys tulee suorittaa kello neljä aamuyöhön mennessä. Ensimmäiseen puolikkaaseen kuuluvat toimialueen hallintapalvelimet (Domain Controller Server), tulostus-, DHCP- ja tiedostopalvelimet. Toimialueen hallintapalvelimet päivitetään ensimmäiseksi, koska toimialueen (Domain) toiminnan kannalta se täytyy käynnistää uudelleen ensimmäisenä. Kuten luvussa 4.3.1 on esitetty, toimialueen hallintapalvelin autentikoi käyttäjiä ja resursseja määritetyssä toimialueessa, jonka vuoksi se on kriittinen palvelin.

Seuraavaksi päivitysvuorossa on ensimmäisen asiakasryhmän toinen puolikas (Set 2). Toinen puolikas aloittaa tietoturvapäivitysten lataamisen ja päivittämisen samana iltana ensimmäisen puolikkaan kanssa kello 12 yöllä. Lisäksi toisen puolikkaan käytännön ajastukseen on märitetty, että lataus ja päivitys tulee suorittaa myös kello neljä aamuyöhön mennessä. Molempien puolikkaiden päivityskäytäntöön on myös määritelty, että palvelin käynnistetään automaattisesti uudelleen, kun päivitykset on asennettu. Toiseen päivityspuolikkaaseen kuuluvat loput palvelimet, kuten esimerkiksi Citrix-, sähköposti- ja tietokantapalvelimet.

Toisen asiakasryhmän (Customers B) päivittäminen suoritetaan täsmälleen samalla tavalla, kuten kahdessa yllä olevassa kappaleessa on kuvattu. Ainoana erona on, että päivitykset toiselle ryhmälle suoritetaan seuraavana yönä ensimmäisestä asiakasryhmästä.

Molemmille asiakasryhmille (Customers A ja Customers B) on määritelty valmiiksi päivityskäytäntöjen lisäksi huoltoikkunat (Maintenance Window). Huoltoikkunat täytyy ajastaa asiakaslaitteille päivityskäytäntöjen yhteydessä. Ajastus tehdään molemmille asiakasryhmille oman päivitysyön ajaksi (20:00 – 04:00). Huoltoikkunat ovat käytäntöjä, joiden avulla pystyttäisiin ajastamaan esimerkiksi päivitysten lataaminen ja asentaminen. Tässä tapauksessa huoltoikkunoita käytetään valvonnan sääntöjen takia. Kun huoltoikkuna on käytössä asiakaslaitteella, se aktivoi kaikki valvontakäytännöt ja -säännöt pois päältä. Huoltoikkunan aktiivisuus päivitysajankohtana estää tilanteen, jossa valvontaliitännäinen hälyttäisi palvelimen tavoitettavuudesta (Availability Monitor Policy). Jokainen palvelin käynnistetään uudelleen päivityksen yhteydessä, joten jokainen palvelin hälyttäisi myös sen tavoitettavuudesta. Toteutuksella estetään turhat hälytykset ja tekstiviestit asiakaslaitteiden päivitysten aikana.

4.4 Testaus

Käytäntöjä, sääntöjä, metriikoita ja hälytyksiä luodessa oli oleellista saada varmistus niiden toiminnasta. Tämän takia oli todella tärkeää, että näiden kaikkien toimintaa testattiin käytännössä. Testaamista varten tarvittiin palvelin, jolla voitiin luoda mahdollisia vikatilanteita. Tärkeää oli myös se, että testipalvelin ei ollut minkäänlaisessa käytössä palvelujen tuottamiseksi. Testausta varten päätettiin ottaa käyttöön virtuaalipalvelin, jolle asennettiin testaukseen tarvittavat roolit ja palvelut.

Palvelimeen asennettiin seuraavat Microsoft Windows 2008 R2 -palvelimen roolit

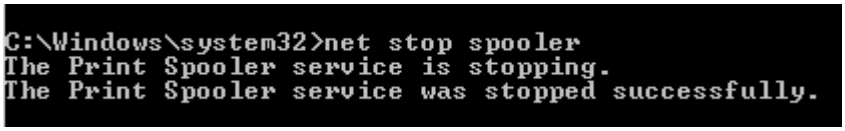
- active directory domain services
- DNS server
- web server (IIS).

Lisäksi palvelimelle asennettiin Microsoft Exchange 2010 -sähköpostijärjestelmä sekä F-Secure E-mail and Server Security -tietoturvaohjelmisto. F-Securen mukana palvelimelle asentui myös Microsoft SQL Server 2008 R2 Express -tietokantajärjestelmä. Rakennetulla kokoonpanolla pystyttiin testaamaan lähestulkoon kaikkia valvottavia ominaisuuksia. Seuraavat palvelut pystyttiin testaamaan Academica Oy:n demopalvelimella: Citrix-palvelut ja Microsoft SQL Server 2008 R2. Symantec Endpoint Protection -virusturvan valvonta testattiin tuotantopalvelimella, koska aikaisempien testauksien perusteella voitiin katsoa, että tästä ei ole tuotannolle haittaa.

4.4.1 Availability Monitor Policy ja Basic Monitor Policy

Asiakaslaitteiden tavoitettavuuden valvontaa testattiin pääasiassa sammuttamalla testipalvelinta ja tarkastamalla ilmeneekö hälytyksiä valvontakonsolissa. Automaattista ratkaisua testattiin käynnistämällä palvelin ja toteamalla, että hälytys katosi tietyn ajan kuluttua konsolista. Huomioitavaa käytännössä on sen helposti aiheuttamat virheelliset hälytykset. Verkon konfiguraation tulee sallia ICMP-liikenne, jotta tämä toimii oikein.

Perussääntöjä testattiin monilla erilaisilla toimenpiteillä. Esimerkiksi kaikki palvelut testattiin siten, että niitä sammutettiin tai keskeytettiin. Tämän jälkeen odotettiin, että valvontakonsoliin tulee tästä hälytys ja varmistettiin palvelun automaattinen uudelleenkäynnistys. Tämän onnistuminen tuli parhaiten ilmi siitä, että konsolissa oleva hälytys automaattisesti ratkaisi itsensä ja täten varoitus katosi konsolista. Kuvassa 17 on esitettynä tulostinpalvelun pysäyttäminen.



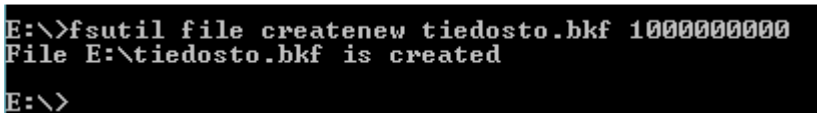
Kuva 17. Tulostinpalvelun sammuttaminen komentotulkilla

Windows järjestelmän lokien kriittisten ilmoitusten valvontaa testattiin siten, että PowerShell-komentotulkilla luotiin lokeihin tapahtumia. Valvontaliitännäinen tunnisti nämä virheet ja valvontakonsoliin tuli tästä hälytys näkyviin. Nämä hälytykset piti kuitata manuaalisesti, koska lokien status ei ole muuttuva. Kuvassa 18 on esitetty esimerkki lokin kirjoittamisesta. Tässä käytetään tasona virheellistä (Error), koska järjestelmän omiin

lokeihin ei voida kirjoittaa kriittisiä lokeja. Tämän tason toimivuuden perusteella voitiin olettaa, että myös kriittiset viestit tekevät hälytyksen.

Kuva 18. Lokin kirjoittaminen Windows-käyttöjärjestelmässä (PS-komentotulkki)

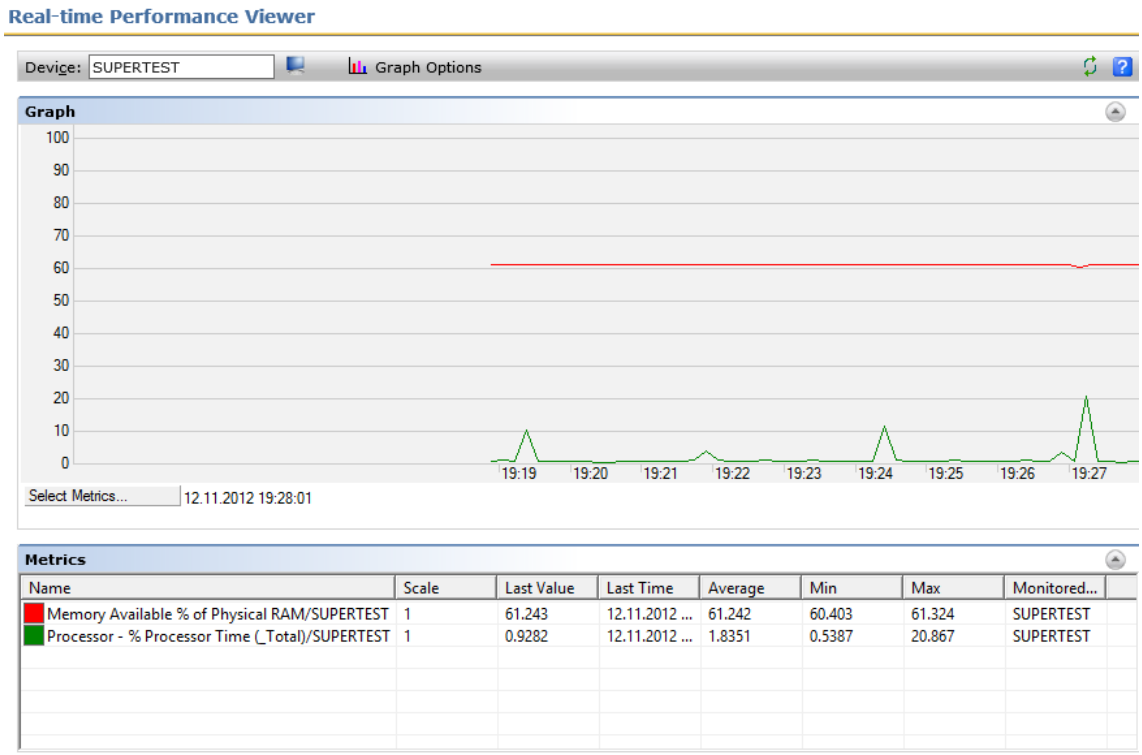
Kovalevyn käyttöastetta testattiin täyttämällä kovalevy tyhjällä tiedostolla. Komentotulkilla pystyttiin luomaan helposti isoja tiedostoja. Yhdellä komennolla saatiin levytila täyttymään haluttuun asteeseen. Kuvassa 19 on esitettynä esimerkki komentotulkin komennosta suuren tiedoston luomiselle. Kun levytilan käyttöasteen luoma hälytys tuli valvontakonsoliin, tiedosto poistettiin palvelimelta. Tämän jälkeen odotettiin, että valvontakonsoli automaattisesti ratkaisee hälytyksen ja hälytys katoaa konsolista.



Kuva 19. Gigabitin kokoisen ”tiedosto.bkf” -tiedoston luonti komentotulkilla

Viruskannereiden toimintaa testattiin palvelujen sammuttamisella, kuten sitä aikaisemmin tässä luvussa kuvattiin. Lisäksi Internetistä ladattiin kuhunkin ohjelmaan EICAR-nimisen organisaation kehittämä testivirus. European Institute for Computer Antivirus Research (EICAR) -organisaation julkaisema vaaraton haittaohjelman testirivi on maailman käytetyimpiä pikatestejä varmistamaan virustorjuntaohjelmiston toiminta [15]. Tämän viruksen avulla saatiin toteutettua tilanne, jossa palvelimella havaitaan virus ja tästä tapahtumasta nousee valvontakonsoliin hälytys. Nämä hälytykset pitää kuitata manuaalisesti, koska virushälytyksen seuranta tapahtuu Windowsin lokeja seuraamalla.

Muistin ja prosessorin käyttöastetta ei kyetty testaamaan. Luotimme siihen, että näistä valmiiksi löytyneistä metriikoista luodut säännöt toimivat kuten halusimme. Oletettavasti ne toimivat, koska hälytyksille annettiin kokemuksen perusteella raja-arvot. Myös metriikoiden antamien arvojen perusteella voitiin sanoa, että raja-arvot ovat oikeat. Tuotantoon siirtymisen yhteydessä säännöt todettiin lopulta toimiviksi. Kuvassa 20 on esitettynä metriikoiden antamia arvoja. Muistin ja prosessorin käyttöasteen säännöt on esiteltynä luvussa 4.3.1.



Kuva 20. Metriikoiden antamia arvoja

4.4.2 DCDiag-skripti

DCDiag-skriptin toimintaa testattiin aluksi luomalla hälytyksiä käyttöjärjestelmän tapahtumalokeihin. Tämä tapahtui esimerkiksi sammuttamalla jokin käyttöjärjestelmän oleellisimmasta komponenteista. Tällöin suorittamalla dcdiag-komento tietyillä tarkentavilla valinnoilla komentotulkissa (PowerShell) saatiin virheilmoitus kyseiseltä diagnostiikka työkalulta. Kuvassa 21 on esitettynä tämä komento ja virheen tulostuminen.

```
PS C:\Users\administrator2> dcdiag /q /skip:systemlog
          DFSR Service is stopped on [SUPERTEST]
        ..... SUPERTEST failed test Services
PS C:\Users\administrator2> _
```

Kuva 21. DFSR-palvelun sammuttamisesta aiheutunut virheilmoitus

Tämän jälkeen luotiin skripti, joka kirjoittaa tämän tulostuksen käyttöjärjestelmän tapahtumalokiin. Tämä skripti on esitetty kokonaisuudessaan liitteessä 1. Tätä tiettyä lokia seuraamalla pystyttiin ottamaan toimialuepalvelimen toimintaa tutkiva sääntö mukaan palvelinvalvontaan.

4.4.3 Exchange Monitor Policy

Kaikkien Microsoft Exchange -palveluiden toimivuutta oli helpointa valvoa Test-ServiceHealth cmdletillä ja tähän pohjautuvalla skriptillä. Tämä cmdlet tulee saataville Exchange-ohjelmiston asennuksen yhteydessä erillisen PSSnapinin mukana. Myös EMS (Exchange Management Shell) toimii tämän Snapinin avulla. Cmdlet on lyhyt komento, jonka avulla PowerShell suorittaa kulloinkin halutun skriptin. Kuvassa 21 on esitettynä PSSnapinin lisäys sekä Test-ServiceHealth cmdletin tuloste. Tämän cmdletin pohjalta tehtiin skripti. Se luo lokeihin tapahtuman, jos jokin tarvittavista palveluista on alhaalla. Valvontaliitännäinen tunnistaa tapahtumat lokin tunnisteen (ID) ja lähteen (Source) perusteella. Tätä testattiin paljon kaatamalla palveluita ja se todettiin toimivaksi ratkaisuksi näin monen palvelun valvontaan. Tätä menetelmää suunniteltaessa tultiin myös johtopäätökseen, että jos postipalvelimella on oikeasti jotain vikaa, niin sitä on parempi tutkia kunnolla. Tämän takia ei ole haitallista, että palvelut eivät lähde automaattisesti takaisin käyntiin. Tämä skripti on esitelty kappaleessa 4.3.1 ja se löytyy liitteestä 2.

```
PS C:\Users\administrator2> Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010
PS C:\Users\administrator2> Test-ServiceHealth


Role                        : Mailbox Server Role
RequiredServicesRunning     : True
ServicesRunning             : {IISAdmin, MSExchangeADTopology, MSExchangeIS, MSExchangeMailboxAssistants...}
ServicesNotRunning          : {}

Role                        : Client Access Server Role
RequiredServicesRunning     : True
ServicesRunning             : {IISAdmin, MSExchangeAB, MSExchangeADTopology, MSExchangeFBA...}
ServicesNotRunning          : {}

Role                        : Hub Transport Server Role
RequiredServicesRunning     : True
ServicesRunning             : {IISAdmin, MSExchangeADTopology, MSExchangeEdgeSync, MSExchangeServiceHost...}
ServicesNotRunning          : {}


PS C:\Users\administrator2> _
```

Kuva 22. PSSnapinin lisäys ja Test-ServiceHealth cmdletin tuloste

4.4.4 Citrix Monitor Policy ja SQL Monitor Policy

Citrix-käytännön testaamisessa käytettiin samoja toimenpiteitä, kuin muidenkin palveluiden toimivuuden testauksessa. Tässä käytännössä valvotaan myös yhtä tiettyä tapahtumaa. Tämän oli havaittu ilmoittavan lisensoinnin vanhentumisesta ja Academican pyynnöstä tämä yksi tietty loki lisättiin valvontaan ja sen toiminta testattiin luomalla tapahtuma lokeihin. Lokia seurataan lähteen (Source), tyypin (Type) ja tunnisteen (ID) avulla. Kuvassa 22 on havainnollistettu tapahtuma ja sen testaus.

```
PS C:\Windows\system32> New-EventLog System -Source MetaFrame
PS C:\Windows\system32> Write-EventLog System -Source MetaFrame -EntryType Warning -EventId 9015 -Message testi
```

Kuva 23. Seuratun tapahtuman luominen testauksessa

4.4.5 Hälytykset

Hälytyksiä ruvettiin testaamaan vasta, kun kaikki säännöt oli luotu käytäntöihin. Hälytykset sähköpostilla ja tekstiviestillä luotiin kappaleessa 4.3.1 esitetyn tavan mukaisesti. Käytäntöjen toiminta (Action) välilehdelle lisättiin vakavalle (Major) hälytykselle sähköpostin lähetys tehtävä (Task). Kriittiselle (Critical) hälytykselle lisättiin tekstiviestin lähetys tehtävä. Tämän jälkeen testipalvelimella luotiin vakavia ja kriittisiä tapahtumia ja tutkittiin olivatko hälytykset halutun mukaisia. Kuvassa 23 on esimerkki sähköpostiin tulleesta vakavasta hälytyksestä. Myöhemmin vastaanottajaksi sähköpostille annettiin Academican työnohjausjärjestelmä. Sinne viesti tuli samannäköisenä muodostaen samalla työtapahtuman.

```
Check SMC Events

Domain: SUPERTESTDOM
Server: SUPERTEST
IP:
Event time: 8.10.2012 15:25:00

Monitor Policy: .Academica Basic Monitor Policy
Monitor Rule: .AcaMonitor - Disk Free (%) - Major
Monitor Category: Disk
Rule State: Major
Metric: .AcaMonitor - % Free DiskSpace DeviceID="C:": 17,8147321068516, DeviceID="E:": 3,82516854272003
```

Kuva 24. Vakava hälytys testipalvelimelta

4.4.6 Windows-tietoturvapäivitykset

Tietoturvapäivitysten jakelun toteutus muuttui useasti projektin edetessä ja lopullista toteutusta ei testattu testialustalla. Tämä johtui siitä, että jakelun toimintaperiaate oli selvillä ja toteutustapa muuttui useasti. Päivityksiä ei aloitettu kuitenkaan missään vaiheessa jakamaan suoraan asiakaslaitteille. Academican kanssa sovittiin, että jatkossa yrityksen omaan toimialueeseen (Domain) kuuluvat palvelimet toimivat samalla testipalvelimina tietoturvapäivityksille. Toteutus on esitetty luvussa 4.3.3.

Testialustalla suoritettu tietoturvapäivitysten jakelun testaus eteni siten, että ohjelmistotiedotteesta luotiin sääntö. Sääntö osoitettiin suoraan tietylle testipalvelimelle määritetyllä ajastuksella. Ajastus luotiin päivitysliitännäisen käytännön (Update Plug-in Policy)

asetuksiin. Käytäntö kopioitiin oletuskäytännöstä (Default Update Plug-in Policy) ja kopioituun käytäntöön muokattiin haluttu ajastus. Päivitysten ajankohta oli yöllä, joten tulokset tarkistettiin vasta seuraavana päivänä. Tällä menetelmällä voitiin todeta tietoturvajakelun toimivuus.

4.5 Siirtäminen tuotantoon

Tuotantoon siirtymistä varten luotiin kirjallinen suunnitelma. Se sisälsi vaadittavat toimenpiteet siitä, miten asiakaspalvelin siirretään tuotantoon ja tarvittaessa pois tuotannosta. Suunnitelmaa luotaessa pohdittiin, mitä kaikkea tulee tehdä, jotta valvontakomponentit saadaan siirrettyä testipalvelimelta tuotantopalvelimelle. Tarkoituksena oli minimoida tuotantoon siirtymisessä aiheutuvat virhetilanteet. Kirjallinen suunnitelma nopeutti myös tuotantoon siirtymistä. Sen avulla pystyttiin tarkistamaan siirtymiseen tarvittavat askeleet.

Testipalvelimelta siirrettiin tuotantopalvelimelle käytännöt, ryhmät ja tehtävät. Käytäntöjen mukana siirtyivät myös toimenpiteet, säännöt ja metriikat. Ainoastaan ryhmien kohdistaminen käytäntöihin ja tehtäviin tuli tehdä uudestaan tuotantopalvelimella. Päivitysten jakelua ei siirretty tuotantoon, koska sen toiminnasta ja toteutuksesta piti sopia kolmannen osapuolen kanssa. Lisäksi päivitysten jakelu päätettiin ottaa käyttöön vasta, kun kaikki asiakaslaitteet on siirretty tuotantoon ja valvontapalvelu toimii suunnitelman mukaisesti.

Kun käytännöt, ryhmät ja tehtävät olivat siirretty tuotantoon, poistettiin agentti testipalvelimilta. Poistamisen jälkeen uuden palvelimen agentti asennettiin yhdelle testipalvelimista. Palvelimella oli tarkoitus testata onnistuiko siirto suunnitelman mukaisesti. Testausta varten varattiin riittävästi aikaa, jotta metriikoilla ehdittiin kerätä palvelimesta tarpeeksi tietoa.

Kun testipalvelimen valvonta oli todettu toimivaksi, otettiin Academica Oy:n oman toimialueympäristön palvelimet valvontaan. Academican omilla palvelimilla oli tarkoitus toteuttaa viimeinen valvonnan testaus. Palvelimia käytettiin lopulliseen testaukseen, jotta valvontapalvelua pystyttiin testaamaan tarpeeksi monipuolisesti.

Viimeisten testien ja toimivuuden toteamisen jälkeen aloitettiin asiakkaiden siirtäminen uuteen valvontajärjestelmään. Siirtäminen suunniteltiin ja toteutettiin pienissä erissä. Näin mahdollisten ongelmien korjaamiselle ja selvittämiselle jäi tarpeeksi aikaa. Lisäksi pienien erien lisääminen kuormittavat palvelinvalvonta-alustaa vähemmän, joten virhetilanteiden ja rasittumisen riski pienenee.

4.6 Dokumentointi

Academica Oy halusi uudesta palvelinvalvontajärjestelmästä luonnollisesti dokumentaation. Dokumentaation tulisi olla mahdollisimman kattava yrityksen omaan käyttöön. Sen piti olla lisäksi mahdollisimman yksinkertainen, selkeä ja helposti luettava.

Tavoite dokumentaatiolle oli, että jokainen yrityksen työntekijä tietää tutustumisen jälkeen perusasiat valvontakohteista ja itse palvelinvalvonnasta. Toisin sanoen ainakin osassa dokumentaatiota pyrittiin ohjekirjamaiseen ratkaisuun. Niiden avulla kuka tahansa pystyy tarvittaessa seuraamaan palvelinvalvontaa Symantec Management Consolen (SMC) avulla ja tietää hälytykset sekä niiden toimintatavat. Lisäksi jokainen tietää, miten reagoida tarvittaessa hälytykseen yrityksen omalla toimintatavalla.

Loimme lopulta dokumenttikirjaston, joka kattoi laidasta laitaan SMP:lle rakennetun palvelinvalvontajärjestelmän. Ensimmäisissä dokumenteissa esitellään lyhyesti pikaoppaan tavoin, mutta myös kattavasti palvelinvalvonnan käyttöönotto. Dokumenteissa esitellään kuvakaappauksien avulla askel kerrallaan, miten uusi asiakas tai asiakaslaite otetaan palvelinvalvonnan piiriin.

Yksi dokumentaatio sisältää jokaisen valvontakäytännön ja -säännön, joiden avulla valvontaa suoritetaan. Se sisältää kaikki konfiguraatiot säännöille kuvakaappauksia apuna käyttäen. Loimme myös yleisen palvelinvalvontaohjeen, jossa kerrotaan kaikki tarvittava normaaliin valvontarutiiniin. Dokumentti sisältää, miten SMC perusvalvonnassa toimii, hälytykset ja niiden toimintatapa sekä miten hälytyksiin tulee reagoida yrityksen toimintatapojen mukaisesti. Lisäksi selvitetään lyhyesti, mitä valvontakohteita on ja millä perusteella ne luovat hälytykset.

Tehtiin dokumentti myös siitä, miten tietoturvapäivityksiä jaetaan SMC:n avulla. Siihen on kerätty kaikki oleelliset ja vaikuttavat tekijät tietoturvapäivitysten jakelun kannalta. Loput dokumenteista ovat pääasiassa yrityksen sisäisiä asiakirjoja, joista yksi on esimerkiksi suunnitelma, miten palvelinvalvonta otetaan tuotantokäyttöön.

Dokumenttikirjastosta tuli siis erittäin laaja. Kirjaston toteuttamista helpotti kuitenkin se, että loimme dokumentteja samaan aikaan järjestelmän toteuttamisen kanssa. Oli huomattavasti helpompaa muutosten yhteydessä muokata olemassa olevia dokumentteja, kuin jälkeenpäin aloittaa koko dokumentointi. Tässä insinöörityössä on käytetty myös lähteenä luotua dokumenttikirjastoa. Ilman sitä insinöörityön raportin tekeminen olisi ollut erittäin paljon haasteellisempaa.

5 Loppupäätelmät

Insinöörityön ja palvelinvalvontajärjestelmän hahmottuminen kesti todella pitkään. Academica Oy ehdotti aihetta insinöörityöksi toukokuussa 2012, mutta toteutus alkoi vasta elokuussa 2012. Viivästyminen johtui pääasiassa yrityksen sisäisistä asioista sekä kesälomakaudesta. Suurin osa ajasta käytettiin suunnitteluun, koulutukseen, alustaan tutustumiseen ja testaukseen.

Projektin toteuttamista, suunnittelua ja testausta hidasti suurelta osin insinöörityöntekijöiden muut työtehtävät. Avokonttorimaisessa toimistossa tuli useasti erilaisia keskeytyksiä muiden työtehtävien takia. Lisäksi siirrettäessä päivitysten jakelua tuotantoon piti suunniteltu toteutus käyttää kolmannen osapuolen kautta. Järjestely hidasti oleellisesti päivitysten jakelun käyttöönottoa, mutta oli ymmärrettävää alustan ylläpitäjän näkökulmasta. Myös erilaiset asiakkaiden verkon konfiguraatiot aiheuttivat viivästystä, koska vikojen korjaamiseen piti paneutua tapauskohtaisesti.

Kokonaisuudessaan projekti toteutui suunnitelman mukaisesti ja alustan käyttöönotto pystyttiin aloittamaan aikataulussa. Suunniteltu käyttöönoton aikataulu muodostui kuitenkin vasta testauksen loppuvaiheessa. Insinöörityön yhteenvetoa kirjoittaessa järjestelmän käyttöönotto tuotantoon oli kesken osalle asiakkaista. Projekti eteni kirjoitushetkellä kuitenkin suunnitelman mukaisesti, koska suunniteltu valmistuminen oli ajoitettu vuoden loppuun.

Insinöörityön aikana opittiin käyttämään useita erilaisia Windows-ympäristön työkaluja, joiden avulla pystytään keräämään tietoa järjestelmästä. Palvelinvalvonnan oleellinen osa on tiedon kerääminen asiakaslaitteelta, josta voidaan päätellä laitteen tila. Työkaluja, tietoja sekä suunnitelmallisuutta käyttämällä kyettiin rakentamaan määritelty palvelinvalvontajärjestelmä Academica Oy:n käyttöön. Insinöörityö oli kokonaisuudessaan mielenkiintoinen ja monipuolinen. Projektin ansiosta tutustuttiin insinöörityöntekijöille täysin uuteen ohjelmistoalustaan. Ohjelmistoalustan hallitsemisesta tulee varmasti olemaan hyötyä myös tulevaisuudessa.

Lähteet

1. Wikipedia. Järjestelmän valvonta. 2012. Verkkodokumentti. <http://en.wikipedia.org/wiki/System_monitor>.

2. Symantec. Etävalvontapalvelimen konfigurointi. 2011. Verkkodokumentti. <http://www.symantec.com/business/support/index?page=content&id=HOWTO53252>.

3. Wikipedia. Altiris. 2012. Verkkodokumentti. <http://en.wikipedia.org/wiki/Altiris>.

4. Wikipedia. ITIL. 2012. Verkkodokumentti. <http://fi.wikipedia.org/wiki/ITIL>.

5. Symantec™ Management Platform 7.1 MP1 User Guide. 2011. Verkkodokumentti. <http://www.symantec.com/business/support/index?page=content&id=DOC3722>.

6. Monitor Solution 7.1 and Event Console 7.1 Release Notes. 2011. Verkkodokumentti. <http://www.symantec.com/business/support/index?page=content&id=DOC3664>.

7. Altiris™ Monitor Solution from Symantec 7.1 MR1 User Guide. 2011. Verkkodokumentti. <http://www.symantec.com/business/support/index?page=content&id=DOC3718>.

8. Altiris™ Patch Management Solution For Windows 7.1 from Symantec™ User Guide. 2011. Verkkodokumentti. <http://www.symantec.com/business/support/index?page=content&id=DOC3954>.

9. Wikipedia. Palveluiden hallintamanageri. 2012. Verkkodokumentti. <http://en.wikipedia.org/wiki/Service_Control_Manager>.

10. Network Printing. Tulostuspalvelu. Verkkodokumentti. <http://www.networkprinting.info/print-spooler.html>.

11. Wikipedia. DNS. 2012. Verkkodokumentti. <http://en.wikipedia.org/wiki/Domain_Name_System>.

12. Parker, Don. 2006. Understanding the DHCP Protocol. Verkkodokumentti. <http://www.windowsnetworking.com/articles_tutorials/Understanding-DHCP-Protocol-Part1.html>.

13. Schmidt, Peter. 2007. Introduction to Internet Information Services 7.0. Verkkodokumentti. <http://www.windowsnetworking.com/articles_tutorials/Introduction-Internet-Information-Services.html>.

14. Microsoft Technet. DCDiag. 2010. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/cc776854(v=ws.10).aspx>.

15. Wikipedia. EICAR. 2012. Verkkodokumentti. <http://en.wikipedia.org/wiki/EICAR_test_file>.

Toimialueen hallintapalvelimen DCDiag-skripti

```
$source=0

$source=get-wmiobject win32_nteventlogfile -filter "filename='application'" | select -expand sources | select-string -pattern AcaADMonitor

if ($source) {} else {new-eventlog -logname application -source AcaADMonitor}

$test=0

$test=dcdiag /skip:Systemlog /q

if ($test) {Write-EventLog Application -source AcaADMonitor -eventid 1337 -entrytype Error -message "Following tests failed: $test"} else {exit}
```

Sähköpostipalvelimen kunnon tarkistus -skripti

```
$source=0

$source=get-wmiobject win32_nteventlogfile -filter "filename='application'" | select -expand sources | select-string -pattern AcaExchMonitor

if ($source) {} else {new-eventlog -logname application -source AcaExchMonitor}

Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010

$services=0

$services=test-servicehealth | Select-Object RequiredServicesRunning, ServicesNotRunning | Where-Object {!$_.psiscontainer} | foreach {$_.ServicesNotRunning} | select -uniq

if ($services) {Write-EventLog Application -source AcaExchMonitor -eventid 1337 -entrytype Error -message "Following services failed: $services"} else {exit}
```