WWW.JAMK.FI

LABRANET-VERKON MONITOROINTI

Jussi Sunnari

Opinnäytetyö
Marraskuu 2010

Tietoverkkotekniikka
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) SUNNARI, Jussi	Julkaisun laji Opinnäytetyö	Päivämäärä 9.11.2010
	Sivumäärä 64+3	Julkaisun kieli SUOMI
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty ( )
Työn nimi LABRANET-VERKON MONITOROINTI		
Koulutusohjelma Tietoverkkotekniikka		
Työn ohjaaja(t) RANTONEN, MIKA		
Toimeksiantaja(t) Jyväskylän ammattikorkeakoulu Oy		

Tiivistelmä

Opinnäytetyön tarkoituksena oli etsiä ja ottaa käyttöön Jyväskylän ammattikorkeakoulun Teknologia-yksikön LabraNet-verkkoon uusi valvontaohjelmisto. LabraNet-verkko oli alunperin vain yksikön omassa tuotantokäytössä, mutta nykyään se kasvaa ja monipuolistuu nopeasti tarjoten palveluitaan muille yksiköille. Tästä johtuen vanha valvontaohjelmisto koettiin rajoittuneeksi, eikä se vastannut nykyajan vaatimuksia.

Verkonvalvonnan tarkoitus on parantaa verkon luotettavuutta, käytettävyyttä ja suorituskykyä. Valvonta toteutettiin pääosin SNMP:tä käyttämällä. SNMP on yleisin verkonvalvontaan liittyvä prokolla, jota useimmat tietoverkkoihin liittyvät laitteet tukevat. Valvontakohteita ovat mm. reitittimet, kytkimet, palvelimet, tulostimet, tietokoneet ja palvelut. Lisäksi toteutettiin LabraNet-verkkoon toimiva raportointijärjestelmä. Raportoinnin tarkoituksena on pitää henkilökunta ajantasalla tuotantoverkon tilasta.

Projekti aloitettiin määrittelemällä valvontaohjelmiston vaatimukset. Ohjelmistoja verrattiin vaatimuksiin ja parhaat tuotteet testattiin. Testattujen sovellusten joukossa oli avoimeen- ja suljettuun lähdekoodiin perustuvia tuotteita. Testattujen ohjelmistojen väliset erot olivat merkittäviä ja lopulta valituksi tuli Manage Enginen tuottama OpManager-verkonvalvontaohjelmisto.

OpManager:in käyttöönottoon kuului LabraNet-verkon aktiivilaitteiden, palvelimien ja palveluiden valvonnan toteutus. Halutut laitteet lisättiin valvontaan ja niille määriteltiin valvonta- ja hälytyskohteet, lisäksi kofiguroitiin ohjelmiston muut ominaisuudet LabraNet-verkolle soveltuviksi. Lopuksi pidettiin koulutustilaisuus, jossa henkilökunta koulutettiin ohjelmiston käyttöön.

Työn tuloksena saatiin LabraNet-verkkoon testattu ja toimiva verkonvalvontaohjelmisto.

Avainsanat (asiasanat)
Verkonvalvonta, raportointi, SNMP, MIB, OpManager, LabraNet

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
SUNNARI, Jussi	Bachelor´s Thesis	9.11.2010
	Pages 64+3	Language FINNISH
	Confidential ( ) Until	Permission for web publication ( )

Title
LABRANET NETWORK MONITORING

Degree Programme
Data Network Technology

Tutor(s)
RANTONEN, Mika

Assigned by
JAMK University of Applied Sciences

Abstract

The focus of this thesis was to implement a new monitoring program to the LabraNet network at the JAMK University of Applied Sciences. The LabraNet network was originally designed and used for the needs of the technology unit's production, however, it is rapidly expanding and becoming more and more versatile. Thus, a new more sophisticated monitoring system was needed to replace the old limited network monitoring program unsuitable for today's needs.

The main purpose of network monitoring is to improve the network's reliability, usability and performance. The new monitoring system was mainly implemented using the SNMP protocol, which is the most commonly used protocol in network monitoring because of its capability to support the vast majority of network equipment. The monitored network equipment consists of routers, switches, servers, printers and computer services. In addition to the network monitoring, a reliable reporting system was created and implemented within the LabraNet. The sole purpose of the reporting system is to keep the network managers updated of the LabraNet's status.

The project was initiated by defining the needs of the network monitoring program. Different programs were compared to the requirements of the new system and the most suitable ones were tested. Among the new tested programs were OpenSource-based commercial products. The differences between the programs were beyond huge and finally OpManager network monitoring program, produced by Manage Engine, was chosen.

Implementing the OpManager for production use also included executing the monitoring of LabraNet's devices. The selected devices were added into monitoring and the alert triggers were configured. Other features of the OpManager were also configured to suit the needs of LabraNet. After the monitoring system was fully implemented in the LabraNet network, a training session was held for the personnel.

As a result of this thesis a tested and highly functional monitoring system was implemented in the LabraNet network.

Keywords
Network monitoring, reporting, SNMP, MIB, OpManager, LabraNet

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

AD	Active Directory
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CPU	Central Processing Unit
DNS	Domain Name System
ELPA	Elektroninen ICT-palvelutoiminta LabraNet-ympäristössä
ICT	Information and Communication Technologies
IP	Internet Protocol
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JAMK	Jyväskylän Ammattikorkeakoulu Oy
MIB	Management Information Base
MDT	Mean Down Time
MTBR	Mean Time Between Failures
MTTR	Mean Time To Repair
LASSO	Langattomien sovellusten kehitysympäristö
OID	Object IDentifier

RAM	Random-Access Memory
RMON	Remote Network-Monitoring
SGMP	Simple Gateway Monitoring Protocol
SSH	Secure Shell
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TKI	Tutkimus-, Kehittämis- ja Innovaatiotoiminta
UDP	User Datagram Protocol
VPN	Virtual Private Network
WMI	Windows Management Instrumentation

1 TYÖN KUVAUS

1.1 Tehtävä ja tavoite

Opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa LabraNet-verkkoon uudistettu palveluiden monitorointi- ja raportointijärjestelmä. Lähtökohtaisesti LabraNetistä löytyi jo jonkinlainen monitorointijärjestelmä, mutta monitoroinnin kehittäminen oli ollut viime aikoina esillä. Tämän projektin yksi tavoite oli yhtenäistää järjestelmä yhden sovelluksen pohjalle. Tällä pyrittiin helpottamaan, selkeyttämään ja parantamaan verkon monitorointia.

Työn tavoitteena oli toteuttaa LabraNet-verkkoon testattu, käyttöönotettu ja toimiva verkon monitorointiohjelmisto. Tavoitteen saavuttamiseksi oli selvitettävä ja dokumentoitava ITIL-suositusten (Information Technology Infrastructure Library) mukaiset vaatimukset monitoroinnille ja raportoinnille sekä otettava huomioon ylläpitäjien toiveet. Oli myös vertailtava monitorointityökalujen ominaisuuksia suhteessa vaatimuksiin ja valittava käyttötarkoitukseen sopivin ohjelmisto. Parhaat ohjelmistot asennettiin ja testattiin, ja saatujen tulosten perusteella LabraNetin henkilöstö valitsi parhaan ohjelmiston. Lopuksi valittu ohjelmisto implementointiin, testattiin syvemmin, otettiin käyttöön ja todettiin toimivaksi. LabraNetin henkilöstö koulutettiin ohjelmiston käyttöön.

1.2 Toimeksiantaja

JAMK (Jyväskylän Ammattikorkeakoulu Oy) on perustettu vuonna 1994, ja sen omistaa viisi osapuolta: Jyväskylän kaupunki, Jyväskylän koulutuskuntayhtymä, Saarijärven kaupunki, Äänekosken kaupunki ja Jämsän kaupunki. JAMK:ssa opiskelee noin 8000 opiskelijaa seitsemällä eri koulutusalalla. (Jyväskylän ammattikorkeakoulu 2010.)

JAMK koostuu neljästä koulutusta tuottavasta yksiköstä ja hallintoyksiköstä. Ammatillinen opettajakorkeakoulu tarjoaa mahdollisuuden kokeneiden opettajien kouluttautumisen useamman osa-alueen hallitseviksi opettajiksi. Hyvinvointiyksikkö on terveys- ja hyvinvointialan kouluttaja sekä alan yritysten ja yhteisöjen kehittämiskumppani. Liiketoiminta ja palvelut -yksikkö kouluttaa tradenomeja, restonomeja, ves-

tonomeja ja medianomeja sekä vastaa JAMK:n kieli- ja viestintäopinnoista. Teknologiayksikkö on jaettu neljään tulosalueeseen: ICT (Information and Communication Technologies), konetekniikka, logistiikka ja luonnonvarat sekä rakentaminen. (Jyväskylän ammattikorkeakoulu 2010.)

Teknologiayksikön ICT-tulosalue on jaettu myös neljään koulutusohjelmaan, automaatioon, mediatekniikkaan, ohjelmistotekniikkaan ja tietotekniikkaan. Tämä opinnäytetyö edustaa tietotekniikan koulutusohjelman mahdollisuuksia. Tarkemmin määriteltynä toimeksiantajana toimi ICT:ltä löytyvän LabraNet-verkon ylläpito.

1.3 LabraNet

1.3.1 Verkko yleisesti

Aikoinaan verkon rakentamiseen päädyttiin, koska IT-instituuttiin (Information Technology) haluttiin JAMK:n tuotantoverkosta erillään oleva opetusympäristö. Verkon asemaa puolsi myös se, että siitä saatiin rakennettua juuri halutunlainen ja jatkossa sen muokkaaminen olisi nopeaa ja helppoa. Erityisesti opetuskäytössä LabraNet on näyttänyt monipuolisuutensa, ja se näkyy myös opetuksen laadussa. (Huuskonen 2010.)

LabraNetin johtajana toimii Jarmo Siltanen, ja sen henkilökuntaan eli ylläpitäjiin kuuluvat kirjoitushetkellä Antti Järvinen, Juha-Pekka Koho ja Marko Vatanen. Järvinen vastaa verkon palvelimien ylläpidosta, Koho ja Vatanen puolestaan verkon toimivuudesta. Lisäksi heillä on tilanteen mukaan apuna opiskelijoista valittuja assistentteja.

Verkon rakenne (Huuskonen 2010):

- 20 verkon aktiivilaitetta
- 12 fyysistä palvelinta
- virtuaalityöasemia n. 350
- virtuaalipalvelimia n. 50
- 300 fyysistä työasemaa
- 700 opiskelijaa

Kuten listauksesta huomataan, LabraNetin laajuus on varsin huomattava ja virtualisoinnin myötä sen tarjoamat mahdollisuudet ovat lähes rajattomat.

1.3.2 Verkon palvelut

LabraNetin tarjoamat palvelut opiskelijoille ja opettajille ovat välttämättömiä opetuksen ja oppimisen kannalta. Tällä hetkellä verkon palvelut ovat vain ICT-yksikön käytössä ja talon sisällä hyvin rajalliset suhteessa tietokoneiden kokonaismäärään. Tulevaisuudessa verkon palveluita tullaan varmasti laajentamaan myös enemmän talon ulkopuolelle, jolloin palveluiden käytettävyydestä tulee entistä tärkeämpää. (Huuskonen 2010.)

JAMK:n sisällä on käynnissä projekti nimeltä ELPA (Elektroninen ICT-palvelutoiminta LabraNet-ympäristössä). Sen ensisijaisena tavoitteena on tuotteistaa ja tarjota LabraNetin palveluita myös muiden JAMK:n yksiköiden käyttöön. Projektilla pyritään tukemaan TKI-toimintaa (Tutkimus-, kehittämis- ja innovaatiotoiminta) ja sen tavoitteena on JAMK:n näkyvyyden parantaminen sekä ICT-koulutuksen ja TKI-toiminnan integrointi. (Huuskonen 2010.)

Verkon palvelut voidaan jakaa yleisesti kahteen osaan. Ensimmäiseen kuuluvat tietoverkkopalvelut: verkkolevytila, etäkäyttö, LabraNetin verkkosivut, kotisivutila, virtualisointi ja tietoturva. Toiseen osaan kuuluvat infrastruktuuripalvelut: työasemat, tulostus, spidernet, cisco-akatemia, langaton verkko ja muut laboratoriot. Lopuksi vielä helpdesk ja asiantuntijapalvelut omina kokonaisuuksinaan. (Vuorenmaa 2009, 40-41.)

2 ITIL VAATIMUKSET

2.1 ITIL yleisesti

ITIL on yli 20 vuotta kehitetty ja käytetty IT-palveluihin ja hallintaan kohdistuva kokoelma käytännön ohjeista. ITIL ei ole standardi vaan ohjeistus, jota noudattamalla verkon hallinnan pitäisi olla laadukasta.

ITIL on kehityksensä aikana päässyt jo kolmanteen versioon, joka jakautuu viiteen eri kokonaisuuteen. Uusin versio painottaa erityisesti palvelun elinkaarta. Ensimmäisessä osassa ohjeistetaan palvelustrategiaan liittyvissä asioissa. Seuraavassa osassa vinkkejä annetaan palvelun suunnitteluun. Kolmas osa käsittelee suunnitellun palvelun transitiota, eli vanhasta palvelusta siirtymistä uudempaan, palvelun muokkausta

tai mahdollisesti myös kokonaan uuteen palveluun siirtymistä. Neljäs osa puolestaan opastaa palvelutuotannossa, joka sisältää ylläpidollisia asioita. Viides ja viimeinen osa muodostaa kokonaisuuden muiden osien kanssa opastamalla jatkuvaan palvelun kehittämiseen. (IT Service Management Forum Finland 2010.)

Tässä opinnäytetyössä keskitytään erityisesti neljännen osan palvelutuotannon asioihin. Luvussa 2.2 käydään läpi monitorointiin ja kontrollointiin liittyvät tärkeimmät asiat.

2.2 Monitorointi ja kontrollointi

2.2.1 Yleistä

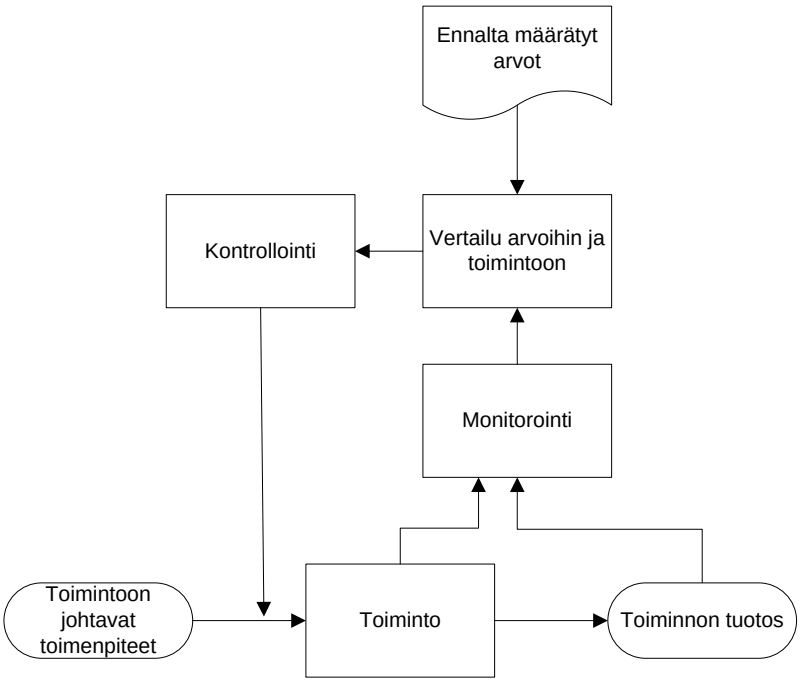
Monitorointi tarkoittaa toimintaa, jolla pyritään huomaamaan tilanteita, joita verkossa tapahtuu jatkuvasti. Palvelutuotannossa tämä tarkoittaa seuraavanlaisia toimenpiteitä (Service Operation 2007, 149-150):

- Käytetään monitorointiin työkaluja, joilla voidaan valvoa verkon tilaa.
- Varmistetaan, että ennalta määritellyt verkolle asetetut vaatimukset täyttyvät. Mikäli eivät täyty, hälytysraja ylittyy ja valvontaohjelmisto lähettää hälytyksen ylläpitäjille.
- Havainnoidaan, että suorituskyky ja käyttöaste ovat ennalta määriteltyjen arvojen sisällä.
- Huomataan, mikäli verkossa tapahtuu epänormaalia toimintaa esim. tietoturvassa.
- Havaitaan luvattomat muutokset esim. ohjelmiston käyttöönotossa.
- Varmistetaan, että verkon sääntöjä noudatetaan.
- Pystytään jäljittämään tuotoksia ja varmistetaan, että ne noudattavat ennalta määrättyjä laatuvaatimuksia.
- Kaikki suorituskykyyn liittyvä data tulee ottaa huomioon.

2.2.2 Yksivaiheinen monitoroinnin kontrollisilmukka

Yleisin malli monitoroinnin suorittamiseen on monitoroinnin kontrollisilmukka (Monitor Control Loop). Vaikka se vaikuttaa yksinkertaiselta, on siinä kuitenkin monia ominaisuuksia, jotka liittyvät palveluiden hallintaan. Seuraavaksi esitellään silmukan perusrakenne ja sen tuomat lisäominaisuudet monitorointiin. (Service Operation 2007, 150-151.)

Kuviossa 1 nähdään silmukan perusperiaate. Yksittäistä toimintaa ja sen tuotosta mitataan käyttäen ennalta määrättyjä normia tai standardia, joka määrittelee, onko se suorituskyvyn tai laadun hyväksyttävän alueen sisällä. Muutoin toimenpiteisiin on ryhdyttävä kontrolloimalla toimintoa ja palauttamalla toiminnon tuotos halutunlaiseksi. (Service Operation 2007, 151.)



KUVIO 1. Yksivaiheinen monitoroinnin kontrollisilmukka (Service Operation 2007, 151.)

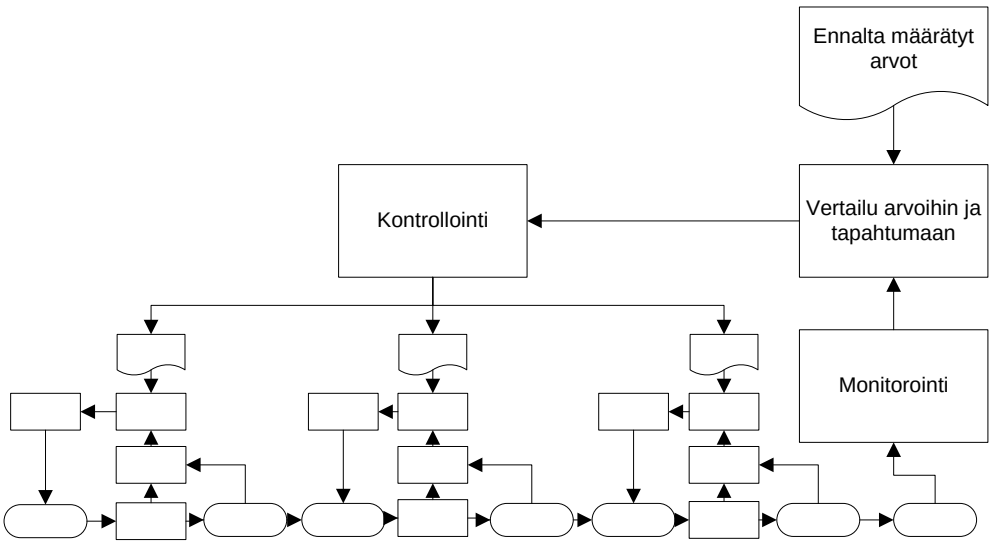
Silmukasta on olemassa kahdenlaista tyyppiä (Service Operation 2007, 151.):

- Avoimessa silmukassa toiminto on suunniteltu suorittamaan tiettyä asiaa ympäristöolosuhteista riippumatta, esim. varmuuskopiointi voidaan aloittaa sovitussa ajassa ja sen suorittamisessa ei oteta huomioon muun ympäristön tapahtumia.
- Suljetussa silmukassa verkon ympäristö otetaan huomioon ja toiminnon kulkuun puututaan kontrollointivaiheessa. Esimerkiksi verkon reitittimen ylikuormittuessa muuttuu reititys niin, että pakettivirta kiertää verkon alueen kautta, jossa ruuhkaa ei ole niin paljon.

2.2.3 Monivaiheinen monitoroinnin kontrollisilmukka

Kuvio 1 on hyvä lähtökohta määrittelemiselle, miten yksinkertainen kontrollisilmukka työskentelee, mutta kehittyneemmässä kontrolloinnissa tilanne on paljon monimutkaisempi.

Kuvioon 2 on yhdistetty neljä kappaletta kuvion 1 kaaviota, ja se valaisee kolmesta merkittävästä toiminnasta koostuvaa prosessia, joista jokaisella on syöte ja tuloste. Tuloste tulee syötteeksi seuraavaa toimintoa varten. Kuviossa on kaksinkertaista takaisinkytkentää. Ensimmäiset silmukat arvioivat vain määritellyn toiminnon kulkua ja viimeinen silmukka arvioi kokonaisuutta ja toimintojen suorituskykyä. (Service Operation 2007, 152.)



KUVIO 2. Monivaiheinen monitoroinnin kontrollisilmukka (Service Operation 2007, 152.)

Esimerkkinä voisi kuvitella liukuhihnan, jossa työstetään jotakin esinettä. Esineeseen tehtäisiin muutoksia toiminto kerrallaan ja toiminnon onnistuminen arvioitaisiin joka kerralla erikseen. Viimeinen silmukka toimisi kokonaisuuden laadunvarmistajana, joka voisi sitten säätää kutakin toimintoa tarpeen mukaan saavuttaakseen täydellisen lopputuotteen. (Service Operation 2007, 152-153.)

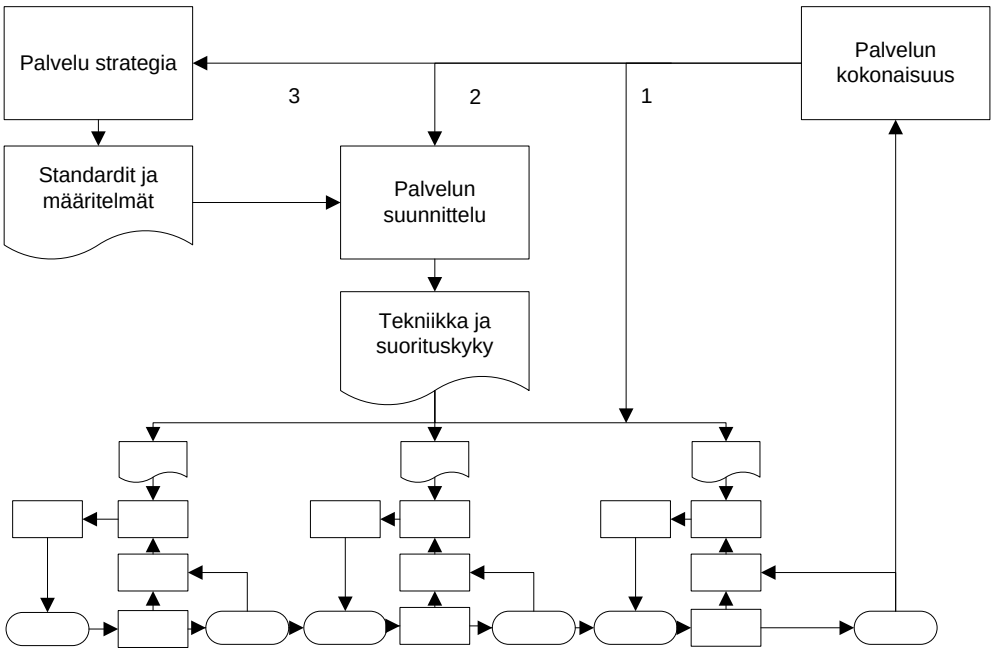
Käytännössä voidaan todeta muutamia tapoja, kuinka ja missä silmukoita voidaan hyödyntää IT-palveluissa (Service Operation 2007, 153):

- Suorituskykytoiminnoissa: kutakin toimintoa ja sen siihen liittyvää tuotosta voidaan mitata, jotta ongelmat prosessissa tunnistetaan, ennen kuin se on kokonaisuudessaan on valmis.
- Tehokkuusprosessissa: toiminto-ruutu esittää koko prosessin yksittäisenä kohteena. Esimerkiksi muutoksenhallinta mittaa prosessin onnistumista tarkastamalla, toteutettiinko muutos ajallaan, määrityksen ja talousarvion arvoissa.
- Suorituskyky laitteessa: toiminto-ruutu voisi edustaa palvelimen vasteaikaa sovitun työmäärän alla.
- Laitteiden sarjan suorituskyky, esim. vasteaika yli verkon, kun käytetään sovellusta etäpalvelimelta.

2.2.4 Palveluiden hallinnan monitoroinnin kontrollisilmukka

Kuviossa 3 käsitellään IT-palveluiden hallinnan monitoroinnin kontrollisilmukka (IT Service Management Monitor Control Loop).

Kuvio 3 koostuu kahden edellisen kuvion summasta ja yläosaan lisätyistä toiminteista. Kuviosta tulee esille, kuinka prosessien tai komponenttien valvonta voidaan yhdistää jatkuvaan palvelun kehittämiseen. (Service Operation 2007, 154.)



KUVIO 3. Palveluiden hallinnan monitoroinnin kontrollisilmukka (Service Operation 2007, 154)

- Palvelunhallinnassa jokaista toimintoa valvotaan tietyllä palvelutuotannon prosessilla. Tämä varmistaa, että jokainen toiminto on varmasti vaatimusten mukainen.
- Määritykset palvelulle on tehty palvelua suunniteltaessa, ja ne perustuvat standardeihin sekä normeihin, jotka puolestaan on määritelty palvelustrategiassa.
- Kaikki muutokset organisaation palvelustrategiassa, arkkitehtuurissa, palvelusalkuissa tai palvelutasovaatimuksissa määrittelevät nopeasti uudelleen valvottavat kohteet ja niiden kontrolloinnin.
- Palvelun rakenne toimii siltana useiden ryhmien välillä, joten kokonaisuuden hallinta voidaan toteuttaa tehokkaasti ja määrätietoisesti.

Kuviosta 3 tulee myös ilmi erilaisia tilanteita ja sitä kautta etenemismahdollisuuksia. Numerot viittaavat kuviossa esiintyviin etenemismahdollisuuksiin (Service Operation 2007, 155):

1. Tässä tapauksessa palvelulle on huomattu tarve kehittyä ja siitä seuraa muutoksia toiminnoissa.

2. Tässä tapauksessa palvelutasovaatimuksia täytyy muokata, esim. palvelu voi olla liian kallis tai ylläpito on mahdotonta. Palvelu suunnitellaan ja toteutetaan uudelleen.
3. Tässä tapauksessa määrityksiä, jotka on määritelty palvelun suunnitteluvaiheessa, ei noudateta. Toiminnot täytyy tutkia ja ne pitää yhdenmukaistaa määritysten kanssa, eli ainakin toista on muokattava.

Palveluiden muutoksissa järjestelmä takaa seuraavaa (Service Operation 2007, 156):

- Uusille palveluille ympäristön, jossa tekninen arkkitehtuuri ja palvelulle määritellyt vaatimukset ovat kunnossa. Kaikki ryhmät siis ovat uudesta palvelusta tietoisia ja voivat vastata palvelutasovaatimuksiin.
- Olemassa oleville palveluille muutoksen hallinta voi määritellä kaikki ne toiminnot, jotka palvelu vaatii toimiakseen vaaditulla tavalla.

Kokonaisuutena voidaan todeta, että se, mitä monitoroidaan ja kontrolloidaan, tulee olla tulevaisuuteen tähtäävää. Pitää keskittyä palveluun ja sen vaikutukseen organisaatiossa eikä vain yksittäisiin komponentteihin. Aina pitää muistaa, mitä oikein on tarkoitus saada aikaan?

2.2.5 Sisäinen ja ulkoinen monitorointi sekä kontrollointi

Sisäisellä monitoroinnilla ja kontrolloinnilla tarkoitetaan, että useimmat organisaation ryhmät ovat keskittyneet hoitamaan vain heille itselleen määriteltyjä tehtäviä. Näin ollen he keskittyvät vain palveluihin, joita he aktiivisesti käyttävät. Tällainen monitorointi tapahtuu lähes itsestään ja on hyvin suotavaa palveluiden kannalta. Esimerkiksi service deskin johtaja keskittyy organisoimaan työvoimansa niin, että puhelimiin on tarpeeksi työntekijöitä vastaamassa. (Service Operation 2007, 157.)

Ulkoisella monitoroinnilla ja kontrolloinilla tarkoitetaan, että vaikka kukin ryhmä on vastuussa omasta alueesta, he eivät silti toimi täysin itsenäisesti. Jokaisella tehtävällä, jonka he suorittavat, tai laitteella, jota he käyttävät, on vaikutus koko organisaatioon. Ryhmä voi jakaa usean muun ryhmän kanssa resursseja esim. palvelimelta. Tästä johtuen esim. palvelimien hallintaan erikoistuneen ryhmän on kyettävä monitoroimaan tapahtumia ja pystyttävä reagoimaan niihin tarvittavalla tavalla. Jos vaikkapa palvelimella on ruuhkaa, palvelimen on silti pystyttävä suorittamaan tärkeimpien

sovellusten ajaminen, jotta perustoiminnot organisaatiossa eivät kaadu. (Service Operation 2007, 157.)

Ero sisäisen ja ulkoisen tarkkailun välillä on tärkeä. Jos palvelutuotanto keskittyy vain sisäiseen tarkkailuun, sillä on hyvin hallittu infrastruktuuri, mutta ei mitään mahdollisuutta ymmärtää palvelujen laatua. Jos palvelutuotanto keskittyy vain ulkoiseen tarkkailuun, se ymmärtää, miten kehno palvelun laatu on, mutta sillä ei ole mitään käsitystä siitä, mikä sen aiheuttaa ja millä sen voi korjata.Todellisuudessa jokaisessa organisaatiossa on kuitenkin sekoitus molempia menetelmiä, eikä tilanne ole näin musta-valkoinen. (Service Operation 2007, 157.)

2.2.6 Kohteiden määrittely

Monitorointi- ja kontrollointikohteiden määrittely tulee aloittaa palvelutasojen edellytyksistä. Niistä selviää, kuinka organisaation ryhmät arvioivat palvelunsa suorituskykyä ja tehokkuutta. Palvelun suunnittelun aikana tulee ottaa huomioon myös, kuinka palvelu saadaan aloitettua ja kuinka sitä hallitaan. Pitää muistaa kapasiteetin hallinnan määritykset edulliselle palvelun ylösajolle ja jatkuvalle saatavuudelle. (Service Operation 2007, 157-158.)

Palvelun suunnitteluprosessi auttaa löytämään oikeat kohteet, joita monitoroidaan ja kontrolloidaan (Service Operation 2007, 158-159):

- Kohteiden tulee tuottaa dataa organisaation ryhmien toiminnoista. On sovittava, miten, kuinka usein ja millä lailla monitorointia suoritetaan.
- Tärkeimmät kohteet pitää tunnistaa, ja niiden suorituskyky ja saatavuus tulee ilmoittaa palvelutasoihin liittyvissä dokumenteissa.
- Laitteen suorituskyvyn tulee vastata vaatimuksia, joita palvelu vaatii.
- Kaikkien tukiryhmien tulee tietää roolinsa, jotta he pystyvät suoriutumaan tehtävistään mahdollisimman hyvin.

Tärkeimpänä tulee jälleen muistaa, että kohteiden löytämisessä tulee ajatella kokonaisuutta. Kohteet pitää valita niin, että niiden monitorointi hyödyttää mahdollisimman suurta joukkoa. Valintatilaisuudessa on hyvä olla eri osastojen henkilöitä, jotta valvonnasta tulee mahdollisimman kattava. (Service Operation 2007, 158-159.)

2.2.7 Monitorointitavat

On olemassa useita erilaisia tapoja monitoroida ja myös erilaisia paikkoja, jossa oikean tyylinen monitorointi on tärkeää. Tämä luku 2.2.7 keskittyy tapojen selvittämiseen ja niiden kohdistamiseen oikeaan paikkaan.

Aktiivinen ja passiivinen monitorointi (Service Operation 2007, 159-160):

- Aktiivinen monitorointi viittaa laitteen tai järjestelmän jatkuvaan monitorointiin sen tilan määrittämiseksi. Tekniikkana käytetään pollausta (polling), joka tarkoittaa valvontaohjelmiston jatkuvaa kyselyä laitteen tilasta. Tämän tyyppinen tarkkailu on hyvin intensiivistä, joten sen kuluttaa myös paljon resursseja. Aktiivista tapaa käytetään kriittisten laitteiden tai järjestelmien käytettävyyttä monitoroitaessa. Myös vian diagnosoinnissa aktiivinen monitorointi on yleinen.
- Passiivinen monitorointi on tavallisempaa ja käytännössä ”kuuntelulaitteeseen” välitetään tapahtumia tarkkailuagentilta. Passiivisen monitoroinnin onnistumisen edellytys ovat hyvin määritellyt valvontakohteet ja hälytysten rajaarvot (triggers), joiden ylittyessä hälytys lähtee valvontaohjelmistoon.

Reaktiivinen ja proaktiivinen monitorointi (Service Operation 2007, 159-160):

- Reaktiivinen monitorointi on suunniteltu käynnistämään toiminnon tietyn tyyppisen tapahtuman tai virheen jälkeen. Esim. palvelimen suoritustehon huononeminen saattaa käynnistää uudelleenkäynnistyksen. Pääosin reaktiivista monitorointia käytetään virheiden varalla, mutta sitä voidaan hyödyntää myös sarjassa tapahtuvien toiminteiden kanssa. Valvontapa ei ole ennakoiva, mutta korjaustoimenpiteet ovat sitäkin nopeampia tai ainakin nopeampia, kuin ns. Adidas-verkonvalvonnassa.
- Proaktiivista monitorointia käytetään havaitsemaan tapahtumien kuviot, jotka osoittavat, että järjestelmä tai palvelu saattaa pian olla epäkunnossa. Ennakoivaa tarkkailua käytetään yleensä kehittyneissä ympäristöissä, jossa nämä kuviot on havaittu aikaisemmin useita kertoja ja niistä on pystytty muodostaan selkeitä trendejä vertailua varten. Useimmiten proaktiiviseen moni-

torointiin yhdistetään jokin korjaava toiminto, jolloin automatisointi hoitaa työn ylläpitäjän sijasta.

On myös huomattava, että reaktiivinen ja proaktiivinen monitorointi voivat esiintyä aktiivisena ja passiivisena, kuten taulukossa 1 kuvataan.

TAULUKKO 1. Reaktiivinen ja proaktiivinen monitorointi (Service Operation 2007, 160)

	Aktiivinen	Passiivinen
Reaktiivinen	Käytetään määrittämään mikä laite aiheuttaa vian ja mikä siinä on vikana. Perustuu tietämykseen topologiasta.	Havaitsee tapahtuneita asioita tietyllä aikavälillä ja päättää tapahtumista, sekä miten toimitaan. Esim. salasana kolmesti väärin aiheuttaa lukituksen ja käyttäjän on itse pyydettävä uusi salasana.
Proaktiivinen	Käytetään määrittelemään reaaliaikainen tilatieto laitteesta. Usein käytössä kriittisissä komponenteissa, esim. runkoreitittimissä.	Havaitsee tapahtumia tietyllä aikavälillä ja päättää tapahtumista niin pitkälle, että asia on korjattu. Esim. käyttäjätunnuksen mennessä lukkoon järjestelmä lähettää automaattisesti uudet tunnukset sähköpostiin tai matkapuhelimeen.

Jatkuva ja poikkeustilanteessa mittaaminen (Service Operation 2007, 160-161):

- Jatkuva mittaus keskittyy monitoroimaan järjestelmää reaaliaikaisesti taatakseen, että se noudattaa suorituskykynormeja. Esimerkiksi sovelluspalvelin on käytettävissä 99.9 prosenttia sovitusta ajasta. Ero jatkuvan mittauksen ja aktiivisen monitoroinnin välillä on, että monitoroinnin ei tarvitse olla jatkuvaa. Useimmiten hyvää kapasiteettia ja tehokkuutta arvostetaan enemmän kuin jatkuvan mittauksen tuomia etuja, sillä mittaaminen kuluttaa paljon palvelimen resursseja.
- Poikkeustilanteessa mitatessa ei saada reaaliaikaista suorituskykyä selville, mutta sitä käytettäessä saadaan poikkeukset tehokkaasti selville kuten jatkuvassakin mittauksessa. Esimerkiksi, jos tapahtuma ei suoriudu kokonaan loppuun, otetaan mittaaminen käyttöön vian selvittämiseksi. Tämä on halvempaa ja helpommin mitattavissa, mutta voi johtaa pidempiin palvelun katkok-

siin. Yleisesti ottaen tällaista tapaa mitata voidaan käyttää vähemmän kriittisissä järjestelmissä.

Suorituskyky ja laatu (Service Operation 2007, 160-161):

- Suorituskyky tarkoittaa esim. kuinka moneen puheluun service deskin henkilökunta pystyy tunnissa vastaamaan.
- Laatu tarkoittaa esim. kuinka usein service deskin henkilökunta selvittää ongelmatilanteet.

Yleisin virhe, mikä näiden välillä tapahtuu, on niiden sekoittaminen keskenään. Raportissa saatetaan esim. kirjoittaa, että ”palvelun laatu on kohdallaan, koska puhelimeen vastattiin 99-prosenttisesti 30 sekunnin aikana”. Tässä tapauksessa laadulla tarkoitetaan suorituskykyä ja palvelun laatu unohdetaan täysin. Puhelimessahan on voitu sanoa, että ”en tiedä, kiitos ja kuulemiin”. Nämä kaksi asiaa tulisi raportissa esittää toistensa yhteydessä, mutta erikseen. (Service Operation 2007, 160-161.)

2.2.8 Mittaaminen ja mittarit

Tämä luku 2.2.8 keskittyy etupäässä tarkkailuun ja kontrollointiin lähtökohtana palvelutuotannolle. Pitää huomioida, että ei voi keskittyä kovin tarkasti mittaamiseen tai metriikkaan, koska ne ovat jokaisessa organisaatiossa yksilölliset. Tärkeää kuitenkin on, että jokaisella organisaatiolla on jonkinlaiset suuntaviivat, joita ne noudattavat ja jotka tukevat tavoitteita. (Service Operation 2007, 163-164.)

2.2.8.1 Mittaaminen

Mittaus viittaa mihin tahansa tekniikkaan, jota käytetään arvioimaan kohteen laajuutta (extent), mittavuutta (dimension) tai kapasiteettia (capacity) suhteessa määriteltyihin ja vaadittuihin arvoihin (Service Operation 2007, 163-164).

- Laajuus viittaa yhteensopivuuden tai valmistumisen asteeseen, esim. kaikki muutokset, jotka verkkoon tehtiin.
- Mittavuus viittaa nimikkeen kokoon, esim. tapauksien määrä, jotka service desk ratkaisi.
- Kapasiteetti viittaa nimikkeen kykyyn, esim. tapahtumien maksimilukumäärä, joita palvelin voi käsitellä minuutissa.

Mittauksen tekee mielenkiintoiseksi se, että on mahdollista esim. verrata palvelimen tapahtumien määrää, merkitystä ja prosessia standardiin tai haluttuun ennalta määriteltyyn tasoon. (Service Operation 2007, 163-164.)

2.2.8.2 Mittarit

Mittareiden määrittelyssä on tärkeätä, että tiedetään mitä ja miten mitataan. Mittarin on selkeästi pystyttävä esittämään tuloksensa ja sen perusteella tehdään myös tarvittavat toimenpiteet. Ennalta hyväksi todettu mittari ei välttämättä toimi hyvin jokaisessa organisaatiossa, vaan sitä täytyy muokata, ennen kuin se voi olla tehokas. (Service Operation 2007, 164.)

Esim. suorituskykymittari viittaa tiettyyn, sovittuun suoritustasoon, jota käytetään mittaamaan organisaation tai prosessin tehokkuutta. Suorituskykymittarit ovat uniikkeja jokaisessa organisaatiossa ja ovat pakotettuja yhdistymään tiettyihin syötteisiin, tulosteisiin ja toimintoihin. (Service Operation 2007, 164.)

On huomioitava, että samanlaisia mittareita voidaan käyttää saavuttamaan hyvin erilaisia tuloksia. Esim. eräs organisaatio käytti mittaria: ”prosenttiosuus ongelmista, jonka service desk on ratkaissut”, jolla se arvioi sen suorituskykyä. Tämä toimi tehokkaasti noin kahden vuoden ajan, minkä jälkeen tietotekniikkajohtaja alkoi tajuta, että tätä mittaria käytettiin ehkäisemään tehokasta ongelman hallintaa. Eli jos kahden vuoden jälkeen, 80 prosenttia kaikista tapauksista on riittävän helppoja tullakseen ratkaistuksi 10 minuutissa, miksei niille ole saatu automaattista ratkaisua? Itse asiassa vanhasta mittarista tuli uusi mittari sitä varten, miten tehottomasti ongelmien hallinta toimi. (Service Operation 2007, 164.)

2.3 Raportointi

2.3.1 Yleistä

Raportti yksin luo tietoisuutta, mutta raportti toimintasuunnitelmalla saavuttaa tuloksia. (Service Operation 2007, 162.)

Monitorointi ilman kontrollointia on merkityksetöntä ja tehotonta. Monitorointi pitäisi aina suunnitella takaamaan, että palvelu ja sen toiminnalliset tavoitteet kohtaa-

vat. Tämä tarkoittaa, että jos ei ole selkeää tarkoitusta järjestelmän tai palvelun valvomista varten, sitä ei pitäisi valvoa. Lisäksi valvontaan on aina liitettävä myös vaadittavat toimenpiteet erilaisten tapahtumien varalle. (Service Operation 2007, 162.)

Lisäksi pitäisi myös muistaa, että toimenpiteet saattavat vaikuttaa useisiin henkilöihin. Esim. yksittäinen tapahtuma, kuten sovellusvirhe, saattaa käynnistää toiminnon sovellusten hallinnassa palvelun korjaamiselle. Käyttäjät aloittavat omatoimisen tutkimisen ja hallinta aloittaa määrittelemään, kuinka tämä tapahtuma voidaan estää tulevaisuudessa. (Service Operation 2007, 162.)

2.3.2 Raporttien tyypit

Raporttien tyypit voidaan jakaa kolmeen ryhmään sen mukaan milloin ja mitä raportissa julkaistaan (Cattaneo 2009):

- Tuotannolliset raportit julkaistaan esim. viikoittain ja niissä tulee ilmi palveluiden tila ja erityiset tapahtumat, joita on sattunut.
- Poikkeusraportit julkaistaan, kuten nimikin kertoo poikkeustilanteissa, kun jotakin hyvin merkittävää on sattunut, esim. palvelutasojen pudotus.
- Kausiraportit julkaistaan pitkältä aikaväliltä ja niissä esitetään laajakatseisesti tapahtuneita asioita. Raportti voi sisältää tietoa suorituskyvystä suhteessa palvelutasomäärityksiin, yleisiä trendejä ja lopuksi vaikkapa toimenpiteitä, jolla laatu saadaan pidettyä kunnossa.

2.3.3 Toimimaton raportointi

Kokemus on osoittanut, että toimintahäiriöisessä organisaatiossa on enemmän raportteja, kuin tehokkaassa organisaatiossa. Tämä johtuu siitä, että raportteja ei käytetä aloittamaan ennalta määriteltyjä toimintasuunnitelmia, vaan pikemminkin (Service Operation 2007, 162):

- Yritetään unohtaa oikea syy keksimällä poikkeuksellinen tapahtuma.
- Yritetään selvittää enemmän syyllistä, kuin vian aiheuttavaa tekijää.
- Luodaan suunnitelmia suunnitelmien päälle, jolloin mitään ei koskaan tapahdu.

Toimimattomissa organisaatioissa tuotetaan useita raportteja, joita kenelläkään ei ole aikaa, halua tai kiinnostusta tutkia.

2.3.4 Palveluiden raportointi

Tässä osiossa tutustutaan palveluiden raportoinnin eri näkökulmiin ja määritellään niiden tarkoitusta. Pohditaan, kuinka lukijakunta määritellään, sekä tarkastellaan, mihin kaikkeen raportteja voi käyttää. (Continual Service Improvement 2007, 105.)

Huomattava määrä dataa kerätään päivittäisessä monitoroinnissa liiketoiminnan keskellä esim. palvelunlaadun mittauksissa, mutta vain pieni osa siitä on tärkeää ja hyödyllistä. Enemmistö datasta jää organisaation sisäisen monitoroinnin hetkelliseen tarpeeseen. Liiketoiminnassa on tärkeätä nähdä edellisen jakson tulokset, jotta tiedetään, millä tasolla ollaan menossa ja kuinka tulevaisuudessa panostetaan eri osa-alueisiin. (Continual Service Improvement 2007, 105.)

Ristiin viittaavat tulokset ovat tärkeitä, koska ne määrittelevät tarkasti, mistä mikäkin asia on johtunut. Näin ollen on mahdollista korjata oikeata paikkaa, oikealla tavalla. (Continual Service Improvement 2007, 105.)

Ei ole hyväksyttävää kuvata raportteihin esim. palvelutasojen noudattamista suureilla, jotka ovat tilastollisesti epäselviä. Raportin pitää olla todenmukainen, eikä sen sisällössä saa olla mitään epätarkkuutta. Pitää olla selkeä kuva siitä, mitä on tapahtunut, mitä on tehty ja kuinka toistuminen estetään. (Continual Service Improvement 2007, 105.)

Raportin pitää keskittyä vahvasti tulevaisuuteen, mutta on myös hyvä kertoa selkeästi, onko mennyt toiminta vaikuttanut positiivisesti vai negatiivisesti organisaation liiketoimintaan. (Continual Service Improvement 2007, 105.)

Raportoinnissa tulisi noudattaa selkeitä sääntöjä ja menettelytapoja. Ideaali lähestymistapa raportin rungon rakentamiselle olisi määritellä liiketoimintaan keskittynyt kokonaisuus palveluiden suunnittelun yhteydessä. Samalla määritellään, kuinka raportointi otetaan käyttöön ja kuinka sitä hallitaan. Sisältö voisi olla seuraavanlainen (Continual Service Improvement 2007, 105):

- Määritellään lukijakunta ja heidän vaikutuksensa liiketoimintaan.
- Päätetään, mitä mitataan ja raportoidaan.
- Hyväksytään termien ja rajojen määritelmät.
- Määritellään laskukaavojen perusteet (MTTR, MTBF, MDT ym.).
- Päätetään raportoinnin aikavälit.
- Päätetään, kenellä on oikeus lukea raportteja.
- Määritellään raporttien analysoinnin ajankohdat.

Määrittelemällä raportin runko kehitysvaiheessa laadukkaaksi on raporttien luominen yksinkertaista, lukeminen helppoa ja sen pääkohdat liiketoiminnan vaikutukselle on helppo tunnistaa. (Continual Service Improvement 2007, 106.)

Raportit voidaan julkaista esim. paperilla, sisäverkossa, www-sivuilla, sähköpostilla tai vaikkapa organisaation keskustelupalstalla. (Continual Service Improvement 2007, 106.)

Yksinkertainen, tehokas, muokattavissa oleva ja automatisoitu raportointi on edellytys menestykselliselle ja kehittyvälle raportoinnille, sekä myös etu organisation toiminnalle ja kehitykselle. (Continual Service Improvement 2007, 106.)

3 SNMP

SNMP (Simple Network Management Protocol) on yleisin verkonhallinnassa käytetty protokolla ja se kuuluu TCP/IP-protokollaperheeseen (Transmission Control Protocol/Internet Protocol). Rakenteeltaan protokolla on hyvin yksinkertainen ja se lienee syy sen tehokkaaseen kehitykseen ja suosioon. Protokolla on myös tarvittaessa hyvin kevyt verkolle ja kuljetuskerrokselle. Tiedonsiirrossa käytössä on yhteydetön UDP (User Datagram Protocol). (Reponen 2006, 16.)

3.1 Rakenne

Verkonhallinnalle voidaan määrittää kolme tärkeintä peruselementtiä (Lummevaara 2008, 10):

- verkonhallinta-asema
- verkonhallinta-agentti
- agentin tietokanta, MIB

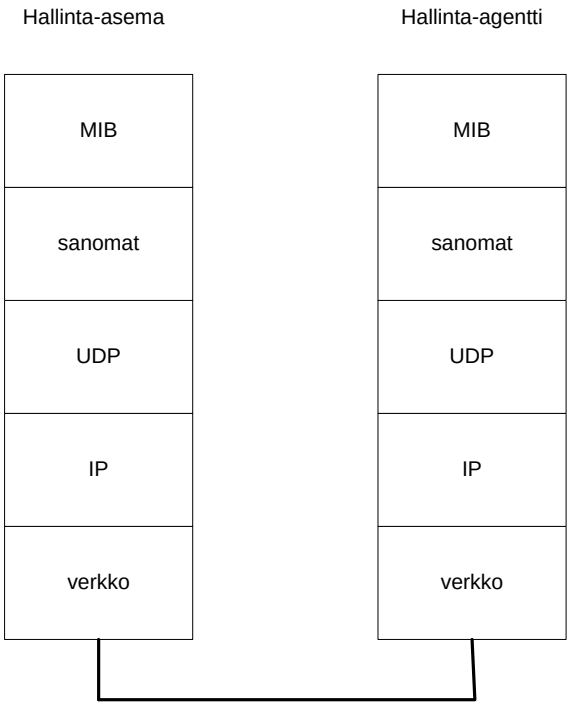
Verkonhallinta-asema on ylläpidon tärkein työväline, sillä siinä käytetään hallintaohjelmistoa. Ohjelmisto- ja alustavaihtoehtoja on olemassa lukematon määrä. (Lummevaara 2008, 11.)

Verkonhallinta-agentti on valvottavassa laitteessa oleva ominaisuus. Agentilta voidaan kysellä laitteen tietoja, sille voidaan myös lähettää käskyjä ja se osaa myös lähettää hälytyksiä laitteen toiminnassa tapahtuvista muutoksista. (Lummevaara 2008, 12.)

Agentin tietokanta, eli MIB (Management Information Base) on valvottavassa laitteessa oleva kokonaisuus, jonka eri osat kuvaavat laitteen eri ominaisuuksia ja niiden tiloja. Samantyyppisissä laitteissa on samanlaiset tietokannat, mutta jokaisella valmistajalla on myös omat erityisominaisuudet esim. palvelunlaadun monitorointia varten. (Lummevaara 2008, 13.)

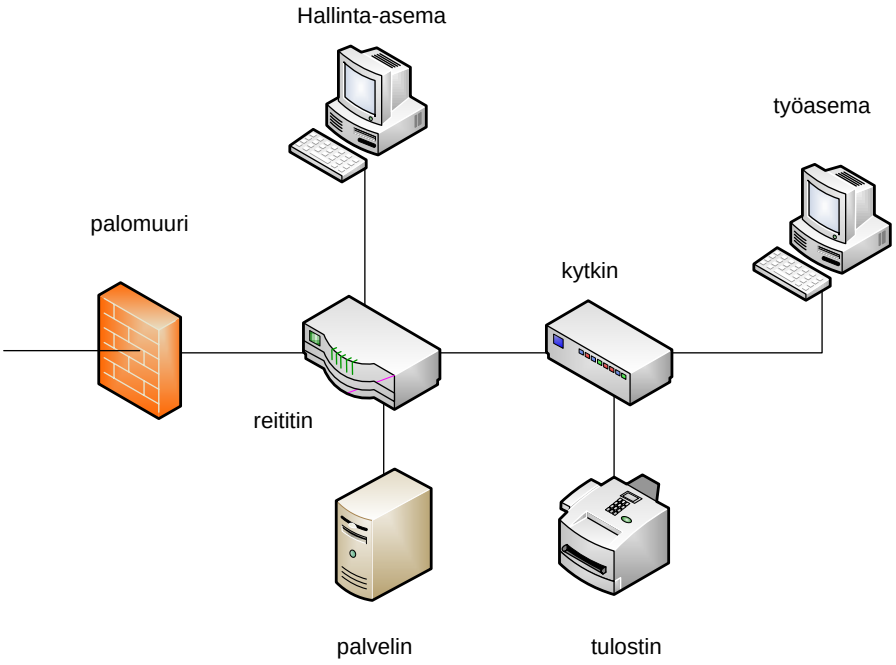
3.2 Toiminta

Hallinta-asema ja hallinta-agentti kommunikoivat keskenään lähettämällä yksittäisiä UDP-paketteja toisilleen, kuvio 4. Kyselyä kutsutaan pollaukseksi (polling) ja se tapahtuu halutuin väliajoin. Verkon kuormituksen kannalta ei ole järkevää tavoitella jatkuvaa reaaliaikaisuutta. (Reponen 2006, 19.)



KUVIO 4. Hallinta-aseman ja hallinta-agentin välinen yhteys (Reponen 2006, 19.)

Protokollalla on mahdollista valvoa kaikenlaisia laitteita, jotka tukevat SNMP:tä. Yleisimmät laitteet näkyvät kuviossa 5 ja ne ovat reitittimet, kytkimet, palomuurit, palvelimet, työasemat ja tulostimet. (Reponen 2006, 17.)



KUVIO 5. Valvottavat kohteet

Agentit käyttävät UDP-porttia 161 sanoman vastaanottoon ja Trap-sanoma vastaanotetaan hallinta-aseman UDP-portista 162. (Lummevaara 2008, 15.)

3.3 SNMP-sanomat

GetRequest-sanomalla hallinta-asema pyytää hallinta-agentilta tietyn objektin arvoa MIB-tietokannasta. Agentti palauttaa GetResponse-sanomalla arvon hallinta-asemalle. GetNextRequest-sanoma poikkeaa edellisestä vain sen suhteen, että pyyntö kohdistuu seuraavaan objektiin. GetBulkRequest-sanoma puolestaan kysyy kerralla halutun joukon arvoja. Get-sanomia käytetään usein ajastimen kanssa, jolloin verkon tilannetta voidaan seurata halutun väliajoin. On kuitenkin muistettava, että liian tiheä kysely voi kuormittaa verkkoa turhaan verrattuna kyselyiden tuomaan hyötyyn. (Kaario 2002, 277.)

SetRequest-sanomalla voi hallinta-asema asettaa hallinta-agentin MIB-tietokantaan halutun arvon haluttuun objektiin. Vanhoja SNMP versioita käytettäessä tämä sanoma on hieman vaarallinen, sillä aikaisten SNMP versioiden tietoturva on olematonta. Sanomalla voidaan myös nollata objektin arvo. (Kaario 2002, 278.)

Trap-sanomia käytetään yleisimmin hälytysten lähettämiseen hallinta-agentilta hallinta-asemalle. Agentille on ennalta asetettu raja-arvot, joiden ylittyessä sanoma lähetetään. Yleisimmin hälytyksiä lähtee esim. uudelleen käynnistyksistä, linkkien kaatumisista tai kovalevyjen täyttymisestä. Tapauksesta riippuen hallintaohjelmista lähettää hälytyksen vielä ylläpitäjälle. (Kaario 2002, 278.)

InformRequest-sanoma kuljettaa informaatiota hallinta-asemien välillä ja se luokitellaan samantyyppiseksi kuin trap-sanoma. Vastaanottava hallinta-asema myös kuittaa vastaanottamansa informaation. (Kaario 2002, 279.)

3.4 Kehitys

SNMP:n kehitys on aloitettu SGMP:n (Simple Gateway Monitoring Protocol) päälle 1980-luvun lopussa. SGMP oli sen aikainen reitittimien hallintaan tarkoitettu protokolla. Ennen 1990-lukua SNMP v1 oli jo saatu spesifioitua, mutta sillä oli useita heikkouksia, kuten tietoturva. Tästä johtuen 1990-luvun alussa aloitettiin SNMP v2:n ke-

hitys. Kahdella ensimmäisellä on useita samanlaisia piirteitä, mutta toisessa versiossa protokollan tarjoamat operaatiot ovat tehokkaampia ja tietoturvaankin oli saatu parannusta. 1990-luvun lopussa kehitystä kaivattiin edelleen tietoturvaan ja SNMP v3:ta aloitettiin kehittämään. 2000-luvun alussa SNMP v3 oli valmis ja se on edelleen uusin versio. (Lummevaara 2008, 14.)

3.4.1 SNMP v1

SNMP v1 tukee yksinkertaisimpia sanomia: Get, Set ja Trap. Suurimmat ongelmat ovat tietoturvassa, sillä viestejä ei salata, eikä käyttäjiä tunnisteta. Ainut turva, minkä protokolla tarjoaa on salasana (community string) , mutta sekin lähetetään selkokielisenä, joten kuka tahansa voi saada sen selville tarkkailemalla verkon liikennettä. Salasanoja oli kuitenkin kahdenlaisia, luku-oikeuksiin (public) ja luku+kirjoitus-oikeuksiin (private). (Lummevaara 2008, 14-17.)

Paketin perusrakenne on jaoteltu kolmeen: version numero, salasana ja loppuosa halutulle sanomalle. (Lummevaara 2008, 17-18.)

3.4.2 SNMP v2

SNMP v2 toi tullessaan kaksi uutta käskyä GetBulkRequest:in ja InformRequest:in. Lisäksi julkaistiin MIB-II tietokanta. Versioita on kuitenkin kaksi, ensimmäisenä SNMP v2c, jonka tietoturvaa ei parannettu, mutta sen sijaan suorituskykyä, luotettavuutta ja hallinta-asemien välistä kommunikointia. Tämä versio on jäänyt yleiseen käyttöön. Toinen versio on SNMP v2u, jossa tietoturvan merkitystä korostettiin. Viestit saadaan nyt salattua ja eheys varmistettua, sekä niiden lähettäjä tunnistettua. Tämä versio toimii pohjana SNMP v3:lle. (Hautaniemi 1994, kohta 4.6.1.)

Versiot 1 ja 2 eivät kuitenkaan ole yhteensopivia, joten niille kehitettiin ratkaisuksi välittävät agentit ja kaksikieliset hallinta-asemat. Välittävä agentti toimii hallinta-aseman ja hallinta-agentin välissä. Käytännössä sen kääntää SNMP v2:n mahdollistamat kaksi uutta sanomaa SNMP v1:n ymmärtämiksi. Kaksikielinen hallinta-asema tallentaa hallinta-agenttien versiot muistiinsa ja osaa täten lähestyä agenttia oikeanlaisilla sanomilla. Rakenne vastaa SNMP v1:stä. (Lummevaara 2008, 20-21.)

3.4.3 SNMP v3

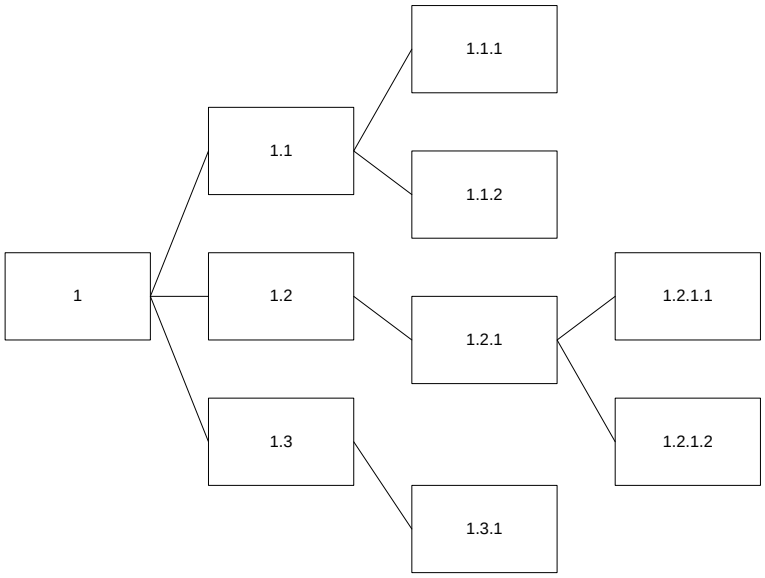
SNMP v3 on uusin versio SNMP-verkonhallintaprotokollasta ja se pohjautuu SNMP v2u:n päälle. Paketin eheys pystytään takaamaan, käyttäjä on mahdollista tunnistaa ja tieto voidaan lähettää salattuna. Samalla aiempien versioiden yksittäinen salasana korvataan ryhmänimellä sekä käyttäjänimellä. Lisäksi tietoturvalle on mahdollista määrittää kolmesta eri tasosta mieluisin yhdistelemällä seuraavia kohtia. (Lummevaara 2008, 20-23.)

- noAuth(noPriv): autentikointi selkokielisellä käyttäjänimellä, kuten SNMP v1 ja SNMP v2c.
- auth(noPriv): autentikointi suojatulla käyttäjänimen salasanalla.
- (auth)Priv: autentikointi suojatulla käyttäjänimen salasanalla ja lisäksi koko paketti salataan.

Paketin rakenne muuttuu siten, että versio-osa pysyy ennallaan, mutta salasana -kohta muutetaan tietoturvaparametreille ja sanomalle varattu osa voidaan salata. (Lummevaara 2008, 23-25.)

3.5 MIB-tietokannat

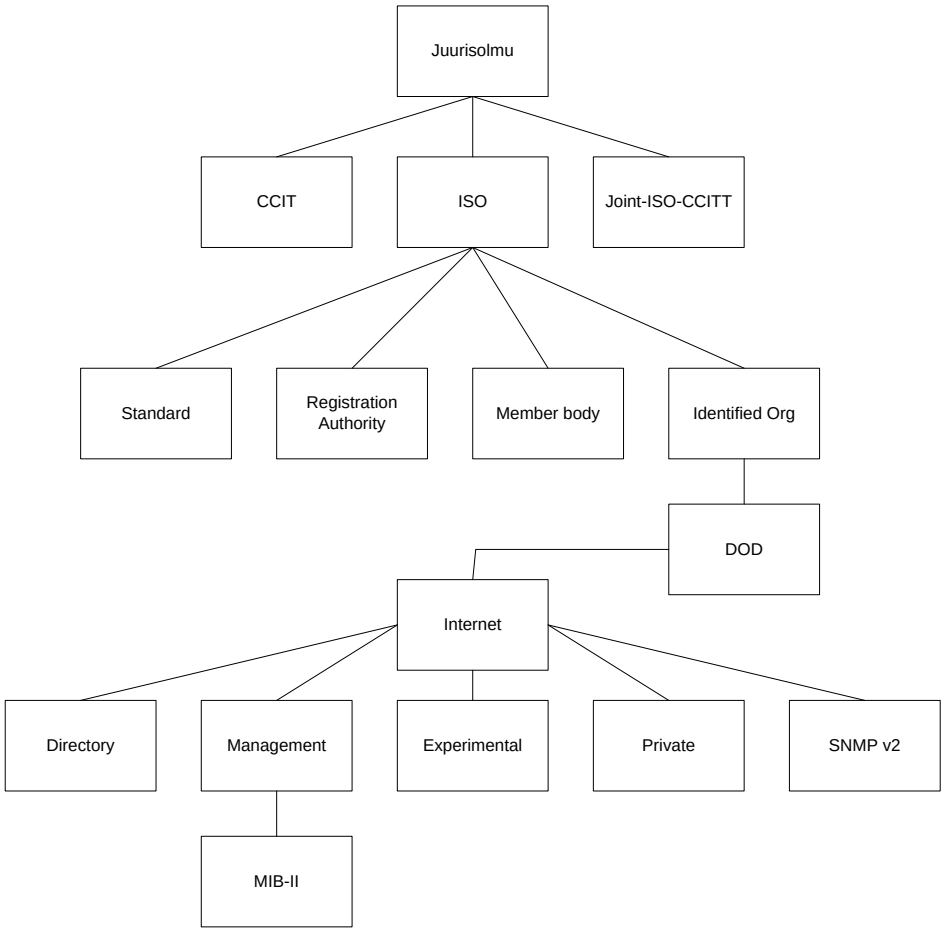
Hallintatietokannat ovat yksi tärkeimmistä elementeistä SNMP:tä käytettäessä. Niissä säilötään hallinta-agentin kaikki tieto, mitä se on valvottavalta laitteelta kerännyt. Tietokantojen rakenne esitetään usein puumaisena muotona, kuten kuviossa 6, ja sen oikean objektin tunnistuksessa OID (Object Identifier) käytetään leksikografista järjestystä. Käytännössä tämä tarkoittaa puhelinluettelon mukaista järjestystä, mutta kirjaimet korvataan numeroilla. Esim. a=1, b=2, c=3 jne. (Kaario 2002, 273-274.)



KUVIO 6. Leksikograafinen järjestely

Kaikki tietokannat ovat kuvattu samalla kielellä, ASN.1:llä (Abstract Syntax Notation One). Tämä mahdollistaa valmistajien toteuttaa uusia objekteja tietokantoihin mielensä mukaan, kunhan ne noudattavat yleistä kehystä, SMI:tä (Structure of Management Information). Lisäksi laitteistolla ja alustalla ei ole niin suurta merkitystä, kunhan ne vain ymmärtävät ASN.1-kieltä. Tietojen lähetyksessä käytetään yleistä BER-koodaussääntöä (Basic Encoding Rules), joka mahdollistaa vastaanottajan purkaa tiedot haluamaansa ja ymmärtämäänsä muotoon. (Kaario 2002, 273.)

Myös tietokannoissa on ajan saatossa tapahtunut kehitystä. Ensimmäisessä MIB:ssä objekteja pyrittiin rajoittamaan sataan, mutta lopulta niitä kertyi 114 kappaletta. Myöhemmässä MIB-II:ssa objektien määrä nousi jo 171:een. MIB-II on edelleen käytössä oleva tietokanta, kuviossa 7. (Hautaniemi 1994, kohta 4.3.2.)



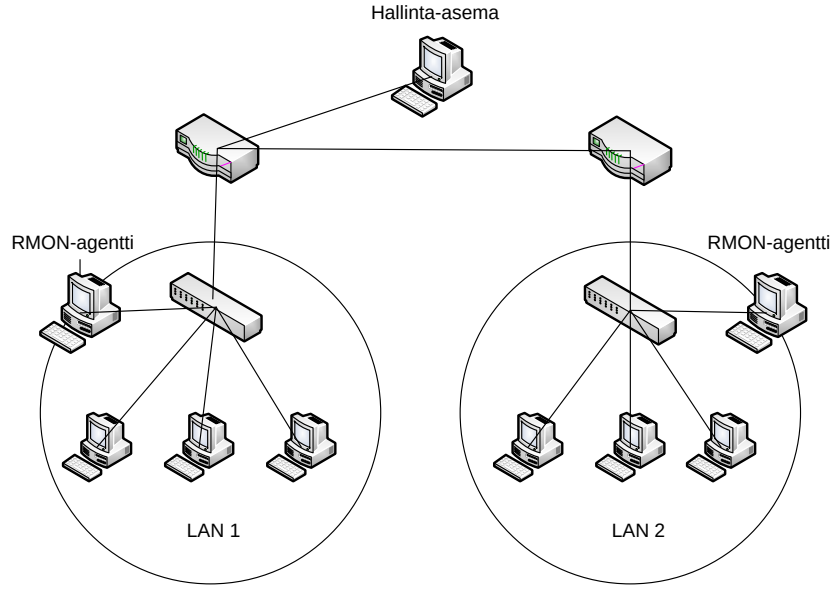
KUVIO 7. MIB-II tietokanta (Kaario 2002, 275.)

3.6 RMON

RMON (Remote Network-Monitoring) on SNMP:hen tarkoitettu lisäominaisuus ison verkon vaativampaan monitorointiin. Sen ideana on hyödyntää verkon eri alueita valvontakohteina ja asettaa erillinen RMON-agentti vastuuseen tietystä alueesta verkossa. Tällä tavalla pystytään vähentämään hallinta-aseman kuormitusta. RMON-agentti kerää ja analysoi oman lähiverkkonsa liikennettä, sekä lähettää sen valmiina koosteena hallinta-agentille. (Lummevaara 2008, 25.)

Kuviossa 8 näemme, kuinka RMON-agentit ja hallinta-asema voidaan sijoittaa verkkoon. Hajauttamalla järjestelmää sen aiheuttama verkon rasitus kevenee huomattavasti ja vikasietoisuus paranee. Mikäli linkki katkeaa RMON-agentin ja hallinta-aseman välillä, niin tieto säilyy agentilla ja se lähetetään hallinta-asemalle linkin korjauduttua. On myös mahdollista käyttää useampaa hallinta-asemaa ympäri verkkoa,

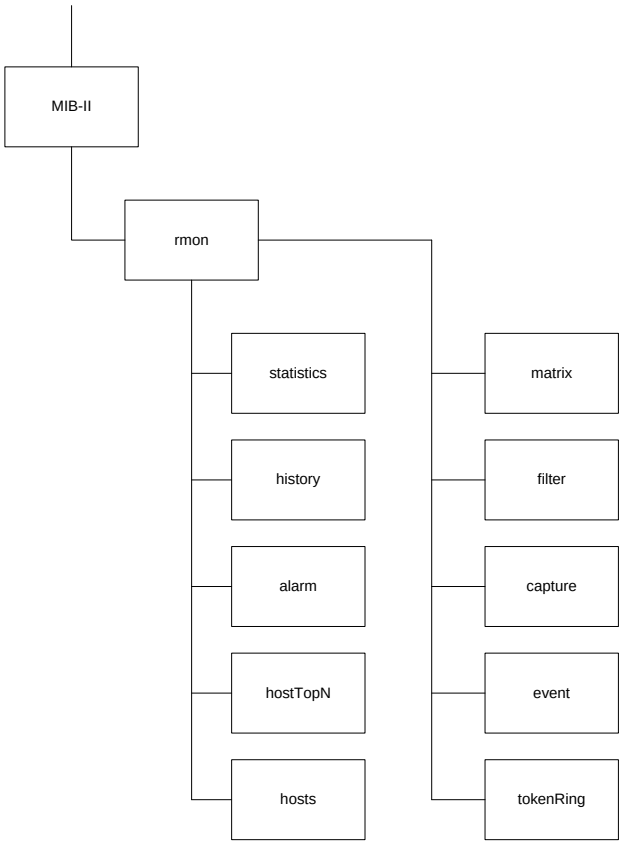
jolloin pikainen siirtyminen toiselle asemalle tuo ylläpidolle jälleen tietoa agentilta. Lisäksi verkon valvonta muuttuu jatkuvaksi, jolloin monitorointi kehittyy ja reaaliaikaiset hälytykset ovat mahdollisia. (Lummevaara 2008, 26.)



KUVIO 8. RMON-agentin käyttö

RMON:lle on myös määritelty tietokantoja kaksin kappalein RMON1-MIB ja RMON2-MIB, molemmat ovat laajennuksia MIB-II kantaan. Ensimmäinen versio monitoroi OSI-mallin kerroksia yksi ja kaksi. (Lummevaara 2008, 27.)

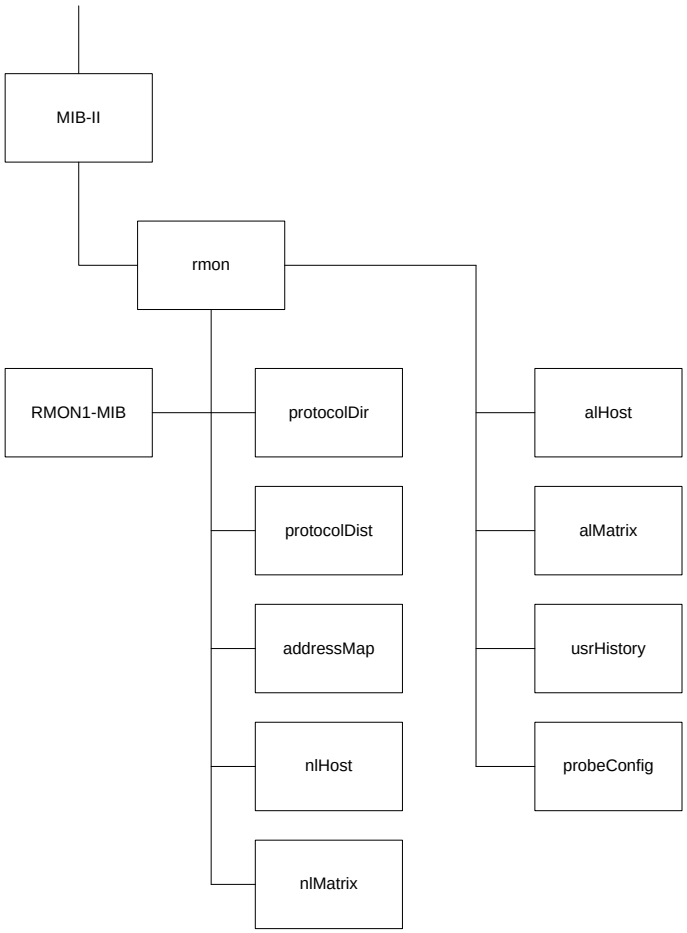
Kuviossa 9 näemme kohteet, joita RMON-agentin tulisi monitoroida. Tärkeimpänä voisi mainita alarm-kohdan, joka vertailee event-kohdan sisältämiä raja-arvoja ja lähettää mahdolliset hälytykset hallinta-asemalle. (Lummevaara 2008, 28.)



KUVIO 9. RMON1-MIB (Lummevaara 2008, 29.)

RMON2-MIB on laajennus RMON1-MIB:n. Sen tarkoituksena on valvoa OSI-mallin kerroksia 3-7. Näin ollen tietokantojen yhdistyessä on mahdollisuus monitoroida kaikkea liikennettä lähes kaikella tavalla. (Lummevaara 2008, 29.)

Kuviossa 10 esiintyy RMON2-MIB:n osat RMON1-MIB:n lisäksi. Mainittakoon vaikka-pa nlHost-toiminto, joka tilastoi yhden tietokoneen kaiken liikenteen IP-osoitteiden perusteella. (Lummevaara 2008, 30.)



KUVIO 10: RMON2-MIB (Lummevaara 2008, 30.)

4 TYÖKALUT

4.1 Vaatimukset

4.1.1 LabraNetin palvelut, mittarit ja mittaaminen

Projektissa tullaan luomaan kokonaisuus LabraNetin monitorointiin, joten mittarit ovat olennainen osa työtä. Mittarit ja mittaamistavat ovat ennalta määritelty Antti Vuorenmaan opinnäytetyössä vuonna 2009. Seuraavaksi suppea katsaus palveluihin, mittareihin ja mittaamistapoihin. Jokainen mittari on yksittäinen vaatimus monitorointisovellukselle, joten niistä jokainen tulee ottaa huomioon (taulukko 2).

TAULUKKO 2. Valvontakohteet ja mittarit

Palvelu	Mittari	Mittaaminen
Verkkolevy	saatavuus	ping
	kapasiteetti	kokonaislevytilan määrää suhteessa käytettyyn
Etäkäyttö	saatavuus	ping
	käyttöaste	Windows Server 2008 Routing and Remote Access
www	saatavuus	ping port 80
	käyttöaste	proserssorin käyttöaste
Kotisivutila	saatavuus	ping port 80
	käyttöaste	proserssorin käyttöaste
	kapasiteetti	kokonaislevytilan määrää suhteessa käytettyyn
Virtualisointi	saatavuus	ping
	käyttöaste	VMware VirtualCenter Server
Palomuuri	saatavuus	ping
	käyttöaste	proserssorin käyttöaste
Työasemat	muutokset	ohjelmistopakettien muutostikettien määrä
Tulostus	saavutettavuus	ping
Spidernet	saavutettavuus	ping
Cisco-akatemia	saavutettavuus	ping
LASSO	ei	ei
Helpdesk	kapasiteetti	tikettien määrä suhteessä ylläpitäjien määrään tietyllä ajanjaksolla
Muut	kapasiteetti	tikettien määrä tietyllä ajanjaksolla

Verkkolevytila mahdollistaa käyttäjien tallentaa omia tiedostoja LabraNetin tarjoamalle verkkoasemalle. Ensimmäisenä mittarina käytetään palvelun saatavuutta ja sitä voidaan mitata pingaamalla. Toisena mittarina käytetään kokonaislevytilan määrää suhteessa käytettyyn. Käyttäjien kuluttamaa levytilaa voidaan myös mitata keskiarvona.

Etäkäyttö mahdollistaa käyttäjien liittymisen LabraNettiin suojatun VPN-yhteyden (Virtual Private Network) ylitse. Tällöin esimerkiksi verkkolevyjen käyttö mahdollistuu kotikoneelta. Mittarina käytetään etäkäyttöpalvelimen saatavuutta ja sitä mitataan pingaamalla. Toisena mittarina käytetään VPN-yhteyksien määrää suhteessa maksimiarvoon, joka on 240 kappaletta. Mittaaminen onnistuu tällä hetkellä Windows Server 2008 Routing and Remote Access-työkalun avulla.

LabraNetin verkkosivut pitävät käyttäjät ajan tasalla verkon tapahtumista. Sivuilta löytyy myös ohjeita, yhteystietoja ja muuta verkon informaatiota. Ensimmäinen mittari mittaa palvelun saatavuutta pingaamalla www-palvelimen porttia 80, jota http-protokolla käyttää. Toisena mittarina mitataan palvelimen kapasiteettiä prosessorin käyttöasteena.

Kotisivutila on tarkoitettu käyttäjien julkaisuille Internetissä. Mittareina toimivat samat kuin verkkolevytilalla ja LabraNetin verkkosivuilla, niitä myös mitataan samalla tavalla.

Virtualisointi mahdollistaa opetuksessa käytettävät virtuaaliset työasemat ja palvelimet. Mittarina toimii VMware ESX-palvelimen saatavuus ja kapasiteetin mittauksessa hyödynnetään palvelimen prosessorin ja muistien käyttöastetta. Saatavuutta mitataan pingaamalla ja käyttöastetta VMware VirtualCenter Server -ohjelmistolla.

Tietoturvan merkitys on nykypäivänä kasvamassa ja siksi sen toteutumistakin on tärkeä valvoa. Tärkeimpänä edellytyksenä turvalliselle verkolle on sen palomuuri, jonka toimintaa myös valvotaan. Mittareina käytetään verkkorajapinnan saatavuutta ja palomuurin prosessorin rasitusprosenttia.

Työasemat ja niiden sisältämät ohjelmistot ovat käyttäjiä ajatellen näkyvin ja tärkein osa verkkoa. Koska koneet harvemmin täysin hajoavat, niin mittariksi on määritelty ohjelmistopakettien muutostikettien määrä. Tiketit ovat helposti laskettavissa järjestelmän käyttämästä sovelluksesta.

Tulostus on jo arkipäivää pienessäkin verkossa, jotta tämä palvelu saadaan pysymään verkossa jatkossa, niin on sen saatavuutta monitoroitava. Mittaus suoritetaan yksinkertaisesti pingaamalla.

SpiderNet on LabraNetin testiympäristö erityisesti tietotekniikan koulutushaaralle. SpiderNet sisältää useita kymmeniä eri valmistajien laitteita toisiinsa kytkettynä ja niistä on mahdollisuus muodostaa mitä erikoisimpia verkkoympäristöjä. SpiderNettiin pääsy on hoidettu erillisellä reitittimellä, joka kontrolloi pääsyä verkon laiteympäristöön. Mittarina käytetään pelkästään saatavuutta, eli mittaamisessa käytetään pingausta.

Cisco-akatemia on SpiderNetin rinnalla toimiva verkkoympäristö Cisco CCNA- ja CCNP-opintojaksoille (Cisco Certified Network Associate, *Cisco Certified Network Professional*). Toiminnaltaan ne ovat samanlaiset, joten mittarit ja mittaaminen ovat identtiset.

Langaton verkko eli LASSO on langattomien sovellusten kehitysympäristö. Mittareita ei tälle palvelulle ole määritelty, koska laitteistoa ei käytetä aktiivisesti.

Helpdesk on LabraNetin ylläpitäjien palvelu, josta käyttäjät saavat apua tarvittaessa. Mittarina toimii tikettien määrä suhteessa ylläpitäjien määrään tietyllä ajanjaksolla.

Asiantuntijapalvelut ovat kaikki muut palvelut mitä edellä ei mainittu. Palvelussa käytetään vain kapasiteettimittaria, eli tikettien määrä tietyllä ajanjaksolla.

4.1.2 Henkilökunnan vaatimukset

Pelkkä kyky mitata oikeita asioita ei pelkästään riitä sovelluksen valintaperusteeksi, vaan on olemassa myös muita vaatimuksia esim. käyttöönoton ja käytettävyyden suhteen. Seuraavaksi LabraNetin henkilökunnan asettamat vaatimukset.

- mahdollisesti OpenSource
- Linux yhteensopiva
- autodiscovery
- SNMP v3
- agentit
- tukee yli 50:tä palvelinta
- tukee yli 300:taa isäntäkonetta
- hyvä dokumentointi
- hälytykset ryhmille/käyttäjille
- automaattinen verkon topologia
- graafinen kuvaus statistiikalle
- plug-initön

Sovelluksen täytyy olla Linuxia tukeva (CentOS). Käyttöönoton helpottamiseksi täytyy olla hyvä dokumentointi ja autodiscovery, joka tarkoittaa, että sovellus osaa etsiä kaikki laitteet tietyltä IP-alueelta. Jotta laitteiden välinen kommunikointi olisi parasta mahdollista, niin SNMP v3 ja isäntäkoneille (host) asetettavat agentit tulee olla tuettuina. Määrällisesti sovelluksen tulee hallita yli 300 isäntäkonetta ja yli 50 palvelinta. Toiminnoiltaan sovelluksen tulee olla mahdollisimman laaja, kattaen vähintään hälý-

tykset ja kuviot, mutta sen täytyy myös olla mahdollisimman yksinkertainen hallittava ja mielellään ilman plug-inejä.

4.2 Kartoitus

Alkuperäisen suunnitelman mukaan tarkoitus oli etsiä OpenSource-tuote, joka tarkoittaa sitä, että sen käytöstä ei peritä mitään maksua. Projektin edetessä kuitenkin huomattiin ilmaisten sovellusten toteutuksen olevan jotain aivan muuta mitä dokumenteissa oli kerrottu. Jouduimme turvautumaan varavaihtoehtoihin ja maksullisiin sovelluksiin. Kartoituksen eteneminen on jaettu kahteen vaiheeseen, jotka käsitellään kappaleissa 4.2.1 ja 4.2.2.

4.2.1 Avoimen lähdekoodin tuotteet

Monitorointisovellusten etsiminen tuotti jonkin verran alussa vaikeuksia, mutta erilaisten listojen ja arvosteluiden mukana ehdokkaita kertyi yhteensä 34 kappaletta. Liitteessä 2 on lista sovelluksista ja karsintaan johtaneista syistä.

Kartoitus aloitettiin listaamalla seitsemän tärkeintä ominaisuutta, joita sovellukselta vaadittiin. OpenSource, agentit, autodiscovery, SNMP v3, käyttöjärjestelmä, maksuttomuus ja dokumentointi. Vuorenmaan määrittelemät mittarit ja mittaamistavat olivat hyvinkin yksinkertaisia, eikä niitä otettu taulukkoon mukaan. Jokaiseen sovellukseen tutustuttiin, niin pitkälle, kunnes mahdollinen puute löytyi. Puolet ehdokkaista karsiutui maksullisuuteen ja maksuttomista vastaavasti puolet epälaadukkaaseen toteutukseen.

Ensimmäisen karsinnan jälkeen kahdeksan sovellusta olivat muita parempia: Hyperic HQ, Nagios Core, OpenNMS, Opsview, Pandora FMS, Shinken, Zabbix ja Zenoss. Joukosta erottui edukseen erityisesti Pandora FMS ja Zabbix. OpenNMS tuli kuitenkin hyvin lähellä kärkikaksikkoa. Pandora ja Zabbix ovat täysin OpenSource tuotteita, mutta yritykset saavat tuottoa myymällä esim. tukipalveluita ilmaisen sovelluksen rinnalla. Näin ollen sovellusten on mahdollista kehittyä yhä paremmiksi ammattilaisten käsissä.

4.2.2 Parhaimmisto

Molemmat sovellukset läpäisivät selkeästi kaikki vaatimukset, joita edellä asetettiin. Sovellusten välinen paremmuus ei kuitenkaan vielä selvinnyt, joten päädyimme testaamaan molemmat sovellukset, jotta mahdolliset erot saataisiin selville. Molemmat sovellukset erottuivat selkeästi edukseen ominaisuuksien ja Internetistä luettujen satunnaisten kehujen perusteella, mutta itse käyttö onkin sitten asia erikseen.

4.2.2.1 Pandora FMS

Pandoran asennuksen kanssa ei selvitty helpolla, sillä sovellus vaatii paljon enemmän erillisiä paketteja asentuakseen, kuin Zabbix. Pakettien puuttuminen ja niiden etsiminen, sekä yhteensopimattomuusongelmien jälkeen Pandora saatiin kuitenkin asennettua.

Tutustumisen alkaessa sovelluksessa havaittiin jo vakavia puutteita. Esimerkiksi autodiscovery jumittui ensimmäisen muokkauksen jälkeen. Lisäksi sovellus ei kyennyt piirtämään yksinkertaisinta kuvaajaa laitteen saatavuudesta. Asiaa vielä pahensi se, että Pandoran kotisivuilla olevassa demossa 1000:sta laitteesta hajatestillä ei saatu yhdestäkään kuvaajaa ulos.

Pandora hylättiin lopullisesti SNMP-testien antaman tuloksen perusteella. Valvottavan kohteen lisääminen sovellukseen on tehty äärimmäisen vaikeaksi. Esimerkiksi prosessorin käyttöasteen valvomiseksi sovellukseen oli tehtävä viisi erillistä asetusta, jotta yhteys saataisiin muodostettua. Lisäksi sovellukseen olisi käsin lisättävä jokaisen laitteen oma MIB. Useista yrityksistä huolimatta SNMP:tä ei saatu edes toimimaan.

Lisäksi pahoista puutteista kertoo esim. ohjeen kielen vaihtuminen englannin ja espanjan välillä. Eikä ohjeen poikkeavuus itse sovelluksen käytöstä auttanut sen toimintaan saattamisessa. Kaikkien näiden puutteiden summana todettiin, että Pandora FMS on soveltumaton LabraNetin tarpeisiin ja se päätettiin hylätä.

Sovelluksesta löytyi kuitenkin muutamia hyviäkin ominaisuuksia, kuten ulkoasun selkeys, valvontakartan (map) yksinkertainen automaattinen piirto, logien näyttö webkäyttöliittymässä ja käyttäjien hallinta.

4.2.2.2 Zabbix

Zabbixin asennus oli alussa hieman helpompaa, kunnes sovelluksen automaattinen alkukonfiguroinnin tarkastus pysäytti asennuksen täysin. Lopulta löytyi aktiivisen kehittäjän tekemä scripti, joka asensi Zabbixin käyttökuntoon itsestään, joten asennus oli helppoa.

Sovelluksen ulkoasu herätti heti luottamusta ja siitä huomasi, että huomattavasti laadukkaammasta tuotteesta oli kysymys kuin Pandora. Konfigurointi tapahtui ohjeiden mukaan hetkessä ja sovellus löysi laitteet nopeasti. Ensimmäinen paha virhe sattui kuitenkin heti käyttäjien hallinnassa. Yhden uuden käyttäjän luominen aiheutti sen, että sovellukseen ei pystynyt kirjautumaan edes adminin tunnuksilla. Edes tietokantojen muokkaaminen ei korjannut asiaa, vaan koko sovellus piti asentaa uudestaan.

Puhtaalta pöydältä aloitettaessa siirryttiin laitteiden hälytysten konfigurointiin, jossa kuitenkin huomattiin pahoja virheitä, valvottavien kohteiden listaus ei nimittäin toiminut, joten ne täytyi muistaa ulkoa tai kirjoittaa ylös. Laajemmassa käytössä tämä tuskin tulisi toimimaan hetkeäkään. Saman tyylinen ongelma ilmeni myös, kun valvontakarttaa alettiin piirtämään, sillä laiteryhmän lisääminen ei toiminut, vaan jokainen laite piti lisätä mappiin yksitellen. Topologian piirtämisen mahdollisuudet olivat kuitenkin yleisesti korkealla tasolla, sillä jokainen linkkiväli aina porttia myöten pystyttiin määrittämään valvontaan ja integroimaan mappiin. Muina hyvinä puolina mainittakoon autentikointi ja IPv6 tuki, näitä ei kuitenkaan koskaan testattu.

Yleisesti Zabbixin käyttö kuitenkin ontui niin pahasti. Sen monimutkaisuus ja käsittämättömät virheet aiheuttivat sen, ettei sillä nähty olevan tulevaisuutta LabraNetin valvonnassa.

4.2.3 Suljetun lähdekoodin tuotteet

Kahden OpenSouce-sovelluksen poisjättämisen jälkeen projektisuunnitelmaa oli muutettava ja myös maksullisia sovelluksia otettiin testattavaksi. Tästä johtuen projektin aikataulua jouduttiin myös venyttämään reilusti, sillä asiat päätettiin tehdä kerralla hyvin.

Päätimme, että testeihin otettiin mukaan myös maksullisia sovelluksia sekä kolmannella sijalla ollut OpenSource-sovellus OpenNMS. Maksullisten sovellusten kartoitus aloitettiin aiemmin luodun listauksen perusteella, josta mukaan valittiin parhaimmilta vaikuttaneet tuotteet.

4.2.3.1 Opennms

LabraNetissä oli ennalta ollut käytössä OpenNMS, joten siitä oli myös ennalta suuntaa antavia kokemuksia. Tuote on yksi vanhimmista olemassa olevista avoimeen lähdekoodiin perustuvista monitorointiohjelmistoista ja voi olla varma, että se jatkaa kehittymistä vielä vuosia eteenpäin. Asennus sujui ensimmäistä kertaa helposti ja sovellusta päästiin heti testaamaan. Ulkoasultaan OpennNMS on hyvinkin pelkistetty, eikä esim. värien tuomaa informaatiota ollut juurikaan hyödynnetty.

Ensimmäinen ja merkittävin poikkeavuus verrattuna Zabbixiin ja Pandoraan oli se, että konfigurointi tehdään tekstitiedostoihin, eikä suoraan web-käyttöliittymään. Yksinkertaisissa asioissa helppo ja hyvä, mutta monimutkaisempiin asioihin mentäessä käyttömukavuus kärsi erittäin paljon. Lisäksi tiedostojen muokkaaminen vaatii hyvin usein palvelun uudelleen käynnistäminen ja jatkuvilla muutoksilla aikaa kuluu paljon hukkaan.

SNMP:n käyttöönotto sovelluksessa oli tehty helpoksi, mikä varmaankin on ollut yksi tavoite ohjelman luonteen kannalta, sillä siinä ei ollut agentteja käytettävissä ollenkaan. Joitakin viitteitä tosin yhteistyöstä Nagioksen ja Hypericin kanssa löytyi, jotka viittasivat, että agentteja olisi mahdollista ottaa käyttöön.

Suuria puutteita ei OpenNMS:stä testeissä löytynyt, joten sen voisi luokitella parhaimmaksi OpenSource sovellukseksi testijoukosta. Kuten aikaisemmin mainittiin, niin konfigurointi tekstitiedostoihin on hankalaa ja työlästä, mutta hyvänä puolena siitä voidaan mainita vaikka helppo varmuuskopiointi. Mappien piirtäminen oli helppoa ja niihin määriteltävää informaatiota oli tarpeeksi. Harmittavasti valvontakartat eivät tällä hetkellä toimineet, kuin Internet Explorer -selaimella.

4.2.3.2 Maksulliset sovellukset

Kartoituksen jälkeen mukaan valittiin seitsemän vaihtoehtoa: Hyperic HQ, NetQos, Nimsoft, SevOne, Zenoss, Zyrion Traverse ja OpManager. Seuraavaksi tiivistelmä eri tuotteiden vertailusta.

Hyperic HQ:n yhteydenottolomake ei ilmeisesti toiminut kahdesta yrityksestä huolimatta, lisäinformaation puutteesta johtuen se karsiutui pois. NetQos ja Nimsoft osoittautuivat saman yrityksen tuotteiksi, mutta samalta yritykselläoli tarjota vielä parempi sovellus nimeltään Spectrum. Valitettavasti hinta nousi useisiin kymmeniin tuhansiin euroihin, joten mahdollisuudet sen hankkimiseen katosivat. SevOne oli myyjän puheiden mukaan maailman paras ja mukana olisi toimitettu jopa valmiiksi konfiguroitu fyysinen palvelin. Vaikka palvelin olisi pudotettu tilauksesta pois, niin hinta oli kuitenkin viisinumeroinen. Ainoana yrityksenä SevOne vaati kolmen sopimuksen allekirjoitusta ennen kuin se olisi edes luovuttanut tuotteensa testattavaksi. Näihin emme suostuneet, joten pudotimme sen pois. Hyvänä puolena mainittakoon kuitenkin erinomainen yhteydenpito ja ystävällisyys. Zenossille otettiin yhteyttä kahdesti ja toinen tuotti tulosta, valitettavasti hinta-arvion laskeminen on edelleen kesken, eikä ole valmistunut muistutuksista huolimatta. Zyrionin hinta oli yksinkertaisesti liikaa, eikä testaamista edes harkittu. Joukon paras tuote OpManager löytyi Manage Engineltä, joka oli laadukas ja hinnaltaan maltillisin. Testiversio oli heti saatavilla ja ainoana maksullisena sovelluksena se haastoi OpenNMS:n.

Päätimme asentaa OpManagerin Windows alustalle, koska sillä ei testauksen kannalta ollut juurikaan väliä. Asennus sujui ongelmitta ja ulkoasu kertoi heti, että olimme maksullisen sovelluksen kanssa tekemisissä. Perusominaisuuden kuten autodiscovery ja dashboard saatiin hetkessä konfiguroitua, eikä mitään ongelmia koko testin aikana havaittu.

Tuotteesta on pelkkää hyvää sanottavaa, sillä käyttöliittymä, hallinnointi, grafiikat, ominaisuudet, valvontakartat ja yleisesti kokonaisuus oli parasta mitä eteen oli tullut. Mikäli haluttavaa ominaisuutta ei heti löytynyt, niin manuaali kertoi selkeästi mistä mikäkin löytyi ja miten sitä käytettiin. Muutamana erikoisuutena mainittakoon mm. IP-kameroiden ja Active Directoryn valvonta.

4.3 Valinta

Aikataulun venyessä oli selvää, että valinta tehtiin Opennms:n ja OpManagerin välillä. Sovellusten ominaisuuksia vertailtiin tarkasti ja pidemmän korren veti selkeästi OpManager. Opennms:stä ei ole pahaa sanottavaa, se on oikeanlaiseen ympäristöön varmasti hyvä valinta. Taulukko liitteessä 3.

OpManagerista oli kuitenkin saatavilla useita eri versioita ja niihin add-on ominaisuuksia. Lisäksi piti varmistua valvottavien kohteiden määrästä, sillä hinta nousi valvottavien laitteiden lukumäärän mukaan. Tarjolla oli kolme eri versiota: Professional, Essential ja Deluxe. Näistä ensimmäinen tarjosi kaikki tarvittavat perusominaisuudet. Essential toi mukanaan MS Exchangen, VMware ESX:n, MS SQL:n ja Active Directoryn (AD) monitoroinnin. Lisäksi NetFlow-analysaattori ja tekstiviestihälytykset oli lisätty. Deluxen ominaisuuksina mainittakoon mm. palvelutasojen hallintaa ja VoIP valvontaa. Näille ei kuitenkaan nähty mitään tarvetta ja hintakin nousi ominaisuuksien lisääntyessä melko korkealle. Vertailu liitteessä 4.

Vertasimme Professionalia johon oli lisätty VMware ESX:n ja AD:n valvonta Essentialversioon. Hintojen ollessa kuitenkin hyvin lähellä toisiaan päädyimme suoraan parempaa Essentialiin, joka tarjosi lähes samalla rahalla kaiken sen mitä Professional, mutta lisäksi vielä enemmän tarpeellisia ominaisuuksia.

5 KÄYTTÖÖNOTTO

OpManager Essentialin toimitti Espoolainen yritys nimeltä Ironnet Oy. Asiakaspalvelu oli koko prosessin ajan aktiivista, nopeaa ja asiantuntevaa. Tilauksen teon jälkeen sovellus saatiin heti ladattua ja aktivointitiedosto tuli hetkeä myöhemmin perässä.

Alkuperäisestä suunnitelmasta poiketen sovellus asennettiin sittenkin Windows:in päälle, koska WMI:n (Windows Management Instrumentation) ja Active Directoryn valvonta vaativat sen. Käyttöjärjestelmäksi valittiin Microsoft Server 2008 R2. Asennus sujui ongelmitta ja tuote oli heti käyttövalmis.

5.1 Konfigurointi

5.1.1 Laitteiden lisääminen ja poistaminen

Käyttöönotto aloitettiin suorittamalla automaattisen haun (autodiscovery) mahdollistavat asetukset. Ensimmäisenä valittiin pääkäyttäjän valikosta (admin) laitteiden etsimiseen liittyvät tunnistusmekanismit (credential settings) ja sinne määriteltiin halutunlaiset etsintätavat. Käytimme kolmea erilaista tapaa tunnistaa laite: SNMP v1, SSH (Secure Shell) ja WMI. Käytimme SNMP v1:stä aktiivilaitteille, mutta palvelimille SNMP v1:stä, ja SSH:ta tai WMI:tä alustasta (template) riippuen.

1. SNMP v1:n luominen oli hyvin yksinkertaista, sillä asetuksiin tarvitsi määrittää vain lukuoikeuksien ja kirjoitusoikeuksien salasanat, jotka vastaavat laitteeseen asetettuja.
2. SSH:ta käytettiin Linux-palvelimiin kirjautumiseen. Root-pääkäyttäjä ei kelpaa käyttäjäksi tietoturvasyistä, vaan kirjautuminen piti suorittaa jollain muulla käyttäjällä.
3. WMI:tä käytettiin Windows-palvelimille kirjautumiseen. Tärkeimpänä piti tietää, että localhost-laitteeseen ei voinut OpManagerin kautta kirjautua.

SNMP:n asentaminen Linux-laitteeseen (CentOS) oli hyvin yksinkertaista. Komennoilla "yum net-snmp" ja "yum net-snmp-utils" saatiin asennettua tarvittavat paketit laitteeseen. Tiedostoa /etc/snmp/snmpd.conf muokkaamalla asetettiin vakiosalasana "public" uuteen salaiseen salasanaan. Komennolla "chkconfig snmpd on" määriteltiin automaattinen palvelun käynnistyminen ja lopuksi komennolla "service snmpd restart" käynnistettiin palvelu uudelleen, jolloin asetukset tulivat voimaan. Palomuuriin voi joutua tekemään aukon portille, mikäli sen asetukset niin vaativat.

SNMP:n asennus Microsoft Server-palvelimelle oli myös melko yksinkertaista. Palvelimen pääkäyttäjän työkaluista (administrator tools) löytyi kohta, josta voi lisätä haluttuja ominaisuuksia (add feature) palvelimelle. Työkalulla saatiin asennettua SNMP-palvelu (SNMP service) käyttöön. Tässä vaiheessa oli tärkeätä muistaa kirjautua ulos ja sisään palvelimelta, jotta kaikki SNMP-palvelun valikot tulivat esiin. Yleisistä asetuksista (general) saatiin määriteltyä, että palvelu käynnistyy automaattisesti. Trap-viestien lähettämiseksi, sille tarkoitetulle välilehdelle, tuli määrittää OpManager-

palvelimen IP-osoite, jonne paketit lähetettiin. Turvallisuus-välilehdelle (security) tarvittiin kaksi määritystä. Ensimmäiseen kohtaan kirjoitettiin ryhmänimi (community name), johon määriteltiin salasana ja salasanalla saatavat oikeudet palvelimella. Toiseen kohtaa asetettiin IP-osoite, jolla määriteltiin, mikä IP-osoite sai vastaanottaa paketteja (SNMP packets to IP), eli käytännössä IP-osoite, jolla voitiin kirjautua palvelimen SNMP-palveluun.

Yleisesti WMI on vakiona päällä Windows:issa ja SSH Linuxissa, eikä niitä tarvitse erikseen konfiguroida.

Kun laitteita haluttiin poistaa valvonnasta, tuli suorittaa seuraavat toimenpiteet. Pääkäyttäjän valikosta otettiin käyttöön konfiguroinnin avustaja (quick configuration wizard), josta valittiin laitteen poisto (delete device). Listasta sai valita halutun laitteen tai laitteet poistettaviksi. Laitteen pystyi poistamaan myös laitteen omalta sivulta toiminto-valikosta (action), josta valittiin poisto (delete).

Seuraavaksi suoritettiin automaattinen haku, joka osasi etsiä laitteita halutulta IP-osoitealueelta. Pääkäyttäjän valikosta valittiin laitteiden etsintä (discover devices). IP-osoitteen ja aliverkon peitteen pystyi syöttämään kenttiin ja valita aikaisemmin luodut tunnistusmekanismit käyttöön. Laitteita pystyi etsimään myös yksi kerrallaan pääkäyttäjän valikon lisää laite -toiminnolla (add device).

OpManagerin löytäessä laitteita, voitiin heti valita, mitkä laitteet haluttiin lisätä ja mitkä poistaa, lisäämällä tai poistamalla ruksi laitteen nimen edestä.

5.1.2 Ryhmittely

Laitteiden löydyttyä oli aika karsia ylimääräiset laitteet pois, sillä kohteiden määrä oli lisenssissä rajoitettu sataan kappaleeseen. Tämän jälkeen laitteet määriteltiin ryhmiin, elleivät ne siellä jo olleet. Sovellus osasi hyvin määritellä aktiivilaitteet omiin ryhmiinsä, mutta useammat palvelimet jäivät kuitenkin tuntematon -ryhmään (unknown). Määrittelimme yhteensä seitsemän ryhmää: switches (kytkimet), routers (reitittimet), firewalls (palomuurit), servers (palvelimet), ELPA, projects (projektit) ja printers (tulostimet). Tämän jälkeen OpManager rekisteröitiin hankitulla lisenssillä ja laitteiden määrä pysyi hyvin sen rajoissa, joka oli 100 kappaletta.

5.1.3 Laitteiden tunnistus

Jotta ohjelmisto toimisi oikein, oli jokainen laite tunnistettava oikein. Tämä tarkoittaa käytännössä sitä, että laitteen merkki, malli ja ohjelmisto tiedettiin, sekä konfiguroitiin sovellukseen, ellei se sitä jo tiennyt.

Ongelmia aiheutti erityisesti Juniperin palomuuri, jota OpManager ei tunnistanut. Laitteen tunnistamisessa oli kolme kohtaa, jotka piti suorittaa. Ensimmäiseksi piti saada haltuun MIB-tiedosto, joka sopi ko. laitteelle ja jossa sijaitsi haluttu tieto. MIB-tiedostot löytyivät valmistajan sivuilta, jonne MIB:lle on tehty useimmiten oma hakukone, näin ainakin Juniperin ja Ciscon tapauksissa. Myös ohjelmiston versio tuli ottaa huomioon tiedostoja valittaessa, sillä ne saattavat muuttua päivitysten mukaan. Toisena kohtana laitteelle tehtiin oma alusta (template). Viimeisenä piti tietää oikea OID, jossa haluttu tieto sijaitsi. Juniperin palomuuriin OID:t löytyivät valmistajan nettisivuilta MIB-selaimella (MIB browser).

Valmistajalta MIB-tiedostot vietiin OpManagerin tiedostoon "./opmanager/mibs". Pääkäyttäjän valikosta valittiin laitteiden alustaan keskittynyt työkalu (device templates), jonne tehtiin uusi alusta (new template). Alustalle määriteltiin ensimmäisenä sen nimi (template name), tässä tapauksessa Juniper-palomuuri. Koska laite ei ollut tuettuna sovelluksessa, ei myöskään automaattinen laitteen tunnistaminen toiminut (query device). Lisää laite -kohdasta (add monitors) pystyttiin lisäämään uusia valvontakohteita ja niitä piti käyttää, koska ennalta määritellyt kohteet eivät toimineet. Tässä vaiheessa ennalta selvitetyt OID:t lisättiin (add bulk), määriteltiin valvontakohteen nimi, OID, valvonnan aikaväli, yksikkö ja mahdollisesti hälytykseen johtanut arvo. Tämän jälkeen valmis alusta liitettiin haluttuun laitteeseen ja päivityksen jälkeen valvonta alkoi. Yhdistämällä laitteen tiedot, MIB:t ja OID:t voitiin siis luoda tuntemattomalle laitteelle oikeanlainen alusta ja valvoa sen toimintaa. Lopuksi ilmoitettiin Juniperin toimivaan valvontaan tarvittavat tiedot myös OpManagerin foorumille, jossa oltiin hyvin tyytyväisiä.

Valitettavasti jokaiselta laitteelta ei saatu haluttuja kohteita valvottaviksi. Suurimmat haasteet tarjosivat hieman harvinaisemmat kytkimet: Nortel Ethernet Switch ja SAN Fiber Switch. Laitteissa saatiin SNMP-yhteydet toimimaan, mutta haluttuja arvoja eivät laitteet suostuneet luovuttamaan millään testatulla menetelmällä.

5.1.4 Hälytykset

Sovelluksessa oli muutamia hälytyskohteita valmiiksi konfiguroituna, kuten porttien sulkeutuminen ja palvelimen saavuttamattomuus. Uuden hälytyksen luominen tapahtui seuraavalla tavalla. Aluksi määriteltiin halutun tyyppinen hälytystapa. Mikäli käyttöön haluttiin sähköposti, niin ensimmäisenä tuli määrittää pääkäyttäjän valikosta löytyvät sähköpostipalvelimen asetukset (mail server settings), johon kuului palvelimen DNS-osoite (Domain Name Sysytem) tai IP-osoite, portti ja sähköpostiosoitteet. Sähköpostiosoitteisiin kuului lähettäjän ja vastaanottajan osoitteet. Tämän jälkeen määriteltiin hälytyksen profiili (notification profiles). Profiiliin asetettiin vastaanottajan sähköpostiosoite ja viestityyppi, joka lähetetään hälytyksen tapahtuessa. Viestin tyyppejä ja niiden tuomaa informaatiota voitiin muokata hyvinkin paljon, vakioviesti lienee useimmissa tapauksissa riittävä.

Nyt oltiin valmiina määrittämään laitteen valvontakohteeseen hälytys. Laitteen hallintasivulta valittiin valvontakohteiden (monitors) alta suorituskykykohteet (performance monitors), jonne lisättiin haluttu valvontakohde. Hälytyksen lisääminen tapahtui yksinkertaisesti lisää laite -kohdasta (add monitors) ja valitsemalla listasta haluttu kohde. Muokkaa -kohdasta (edit) voitiin määrittää hälytyksen raja-arvo, sekä rearm-arvo (poistoarvo), jolla hälytys kuittautui pois listalta. Huomioitavaa oli, että poistoarvon oli oltava pienempi, kuin hälytysarvon. Testauksessa käytettiin CPU-arvoa (Central Processing Unit), joka kuvaa prosessorin käyttöastetta. Määrittelimme sille prosentuaalisesti hälytykseen johtavaksi arvoksi 90 ja poistoarvoksi 70. Tämän jälkeen aikaisemmin tehtyyn ilmoitusprofiiliin (notification profile) valitaan edellä tehty hälytystapa, joka haluttiin suorittaa hälytyksen tapahtuessa. Samalla voitiin määrittää ko. profiiliin millaisen hälytyksen yhteydessä sitä käytettiin. Lopuksi valittiin raja-arvon ylittyminen (threshold rule is violated) käyttöön ja sieltä kyseinen CPU-arvo kohteeksi. Nyt CPU-arvon ylitettyä 90% raja-arvon järjestelmä lähetti hälytyksen haluttuun sähköpostiin.

Samalla testattiin myös palvelimilta tulevat syslogit ja ne toimivat oikein hyvin. Syslogit ovat tietoja siitä, mitä järjestelmässä tapahtuu ja niissä voidaan esim. kertoa käyttäjän kirjautuneen ulos laitteelta. Valvontapöydälle (dashboard) määriteltiin sysloglisäosa (widget), johon kaikki syslogit ilmestyivät. Lisäosilla tarkoitetaan pieniä yksi-

köitä valvontapöydällä, joihin voitiin määritellä haluttuja toimintoja. Halutunlaiset toimenpiteet tietyn tyyppisille syslogeille voitiin määritellä syslogien sääntöihin (syslog rules). Esimerkiksi palvelimen lähettäessä tiedon, että DNS-palvelin on sammunut, voidaan lähettää automaattinen käsky, jolla palvelu käynnistyy uudelleen.

Hälytykset toimivat testeissä kuten pitikin, mutta suurempia kokonaisuuksia tai muutoksia ei ryhdytty tekemään. LabraNetin henkilökunta tekee ne myöhemmin tarpeidensa mukaan.

5.1.5 Valvontakartta

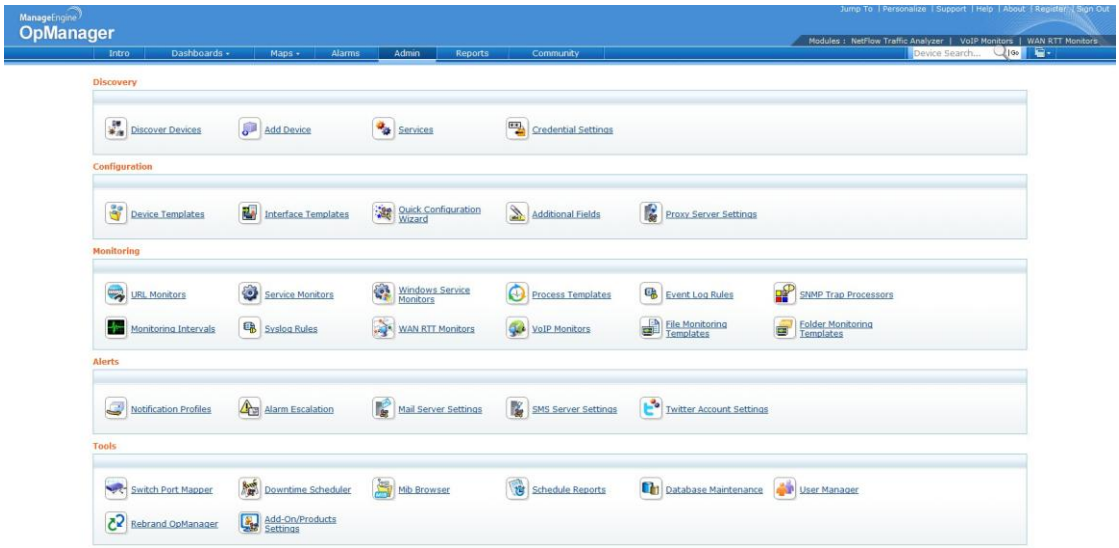
Valvonnan helpottamiseksi on kehitelty valvontakartat (maps), joista ilmenee mm. verkon topologia. Valvoja pystyy tekemään valvontakartan, joka täyttää sen hetkiset tarpeet mahdollisimman hyvin. LabraNetistä päädyttiin tekemään looginen topologiakartta. Valvontakartan tekeminen oli helppoa ja sen tuoma hyöty on korvaamaton. Halutut laitteet ja niiden linkkivälit määriteltiin valvontakarttaan, joten pelkkää kuvaa katsomalla selviää verkon sen hetkinen tilanne. LabraNetistä tehtiin kaksi valvontakarttaa, joista ensimmäinen seurasi aktiivilaitteita sekä verkkoa ja toinen vain palvelimia.

Valvontakartan piirtäminen on tehty helpoksi. Ensimmäiseksi luotiin uusi valvontakartta (create new business view). Sivulle avautui valkoinen pohja, jonka täyttö oli helppo aloittaa taustakuva lisäämällä. Laitteiden lisääminen tapahtui lisää laite -painikkeesta (add device) ja listasta pystyi valitsemaan halutut laitteet, jotka valvontakartassa esitetään. Lisää yhteys -kohdasta (add link) voitiin muodostaa yhteys haluttujen laitteiden välille. Kun yhteys oli tehty, niin sovellus kysyi vielä laitteiden portit, joita käytettiin. Ennen valvontakartan piirtoa oli tärkeää, että SNMP toimii, jotta rajapinnat (interfaces) ovat laitteen tiedoissa näkyvillä. Lopuksi valvontakartta tallennettiin ja lisättiin lisäosana valvontapöydälle (dashboard).

5.2 Toiminta

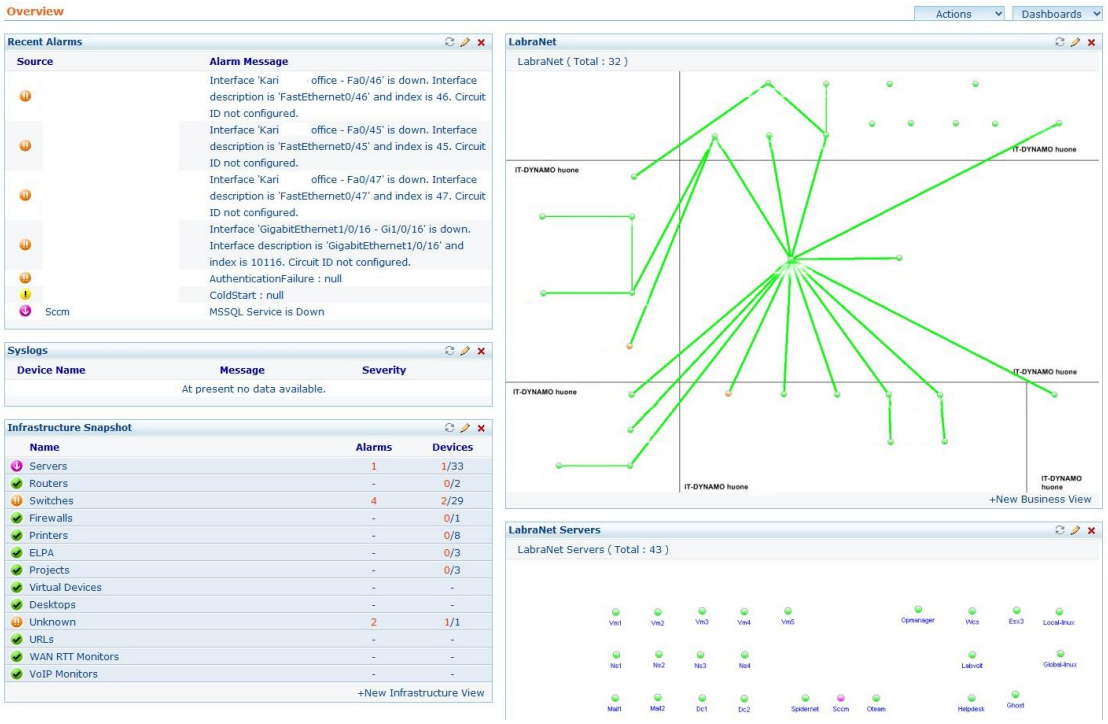
OpManagerin hallinta tapahtui pääosin sovelluksen pääkäyttäjän valikosta, joka näkyy kuviossa 11. Valikko oli jaettu viiteen osaan, jossa ensimmäisessä on laitteiden etsintään tarvittavia toimintoja. Tärkeimpinä mainittakoon automaattinen haku (au-

todiscovery) ja laitteiden tunnistusmekanismit (credential settings). Toisessa osassa oli laitteiden konfiguraatioihin vaikuttavia valikoita esim. laitteiden ja linkkivälien alusta (device templates, interface templates). Kolmannessa osassa keskityttiin laitteiden monitorointiin. Tärkeimpänä palveluiden valvonta (service monitors), jonne määriteltiin eri palveluiden käyttämät portit, jotka mahdollistivat palveluiden valvonnan. Neljännestä osasta hallittiin hälytyksiä, tärkeimpinä ominaisuuksina hälytyksien profiilit (notification profiles) ja hälytyksiin käytettävät asetukset esim. sähköpostipalvelimien osoitteet ja porttien määrittäminen (mail server settings). Viimeisessä osassa oli kokoelma työkaluja, kuten käyttäjien hallinta (user manager) ja MIB-taulukoiden selain (MIB browser).



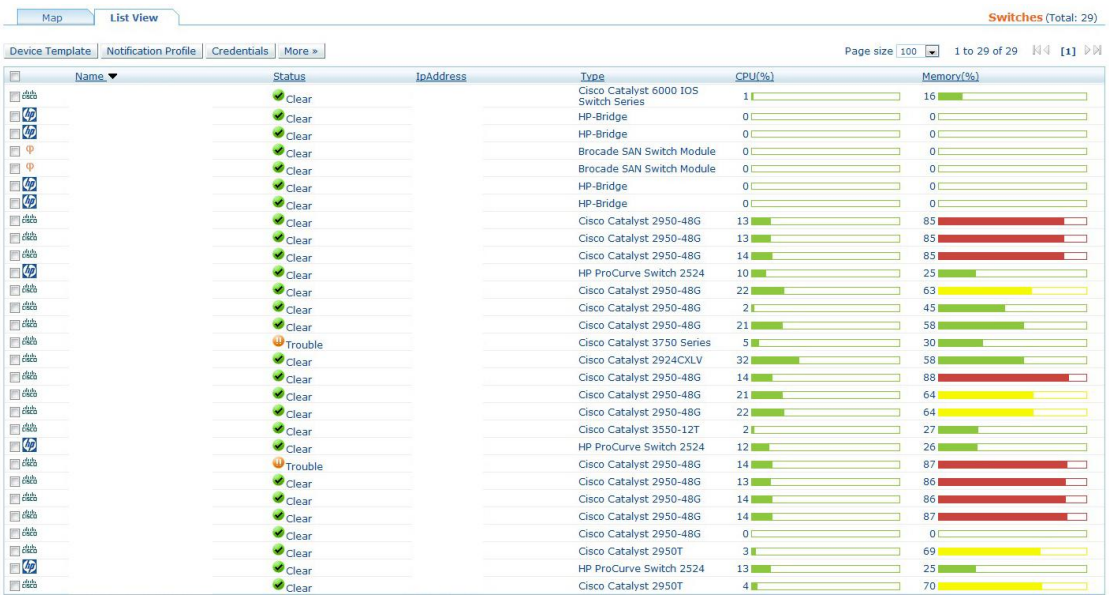
KUVIO 11. Pääkäyttäjän valikko

Valvontapöytä (dashboard) oli luultavasti eniten käytössä oleva sivu, joka näkyy kuviossa 12. Sivulle oli mahdollista lisätä tarpeen mukaan mitä tahansa lisäosia (widget). Lisäosan sisältö koostuu esim. valvontakohteista, joita yksi laite tai ryhmä sisältää. Kuviossa on vasemmalle ylös määritelty hälytykset, sen alle syslog-hälytykset ja niiden alle puolestaan tiivistelmä kaikkien laiteryhmien tilasta. Oikealla puolella on LabraNetin valvontakartta, jossa verkon topologia näkyy linkkitiloineen. Sen alla näkyy puolet LabraNetin palvelimista. Erilaisia valvontapöytiä oli mahdollisuus tehdä lisää tarpeen mukaan ja ne pystyttiin erottelemaan käyttäjäkohtaisesti.



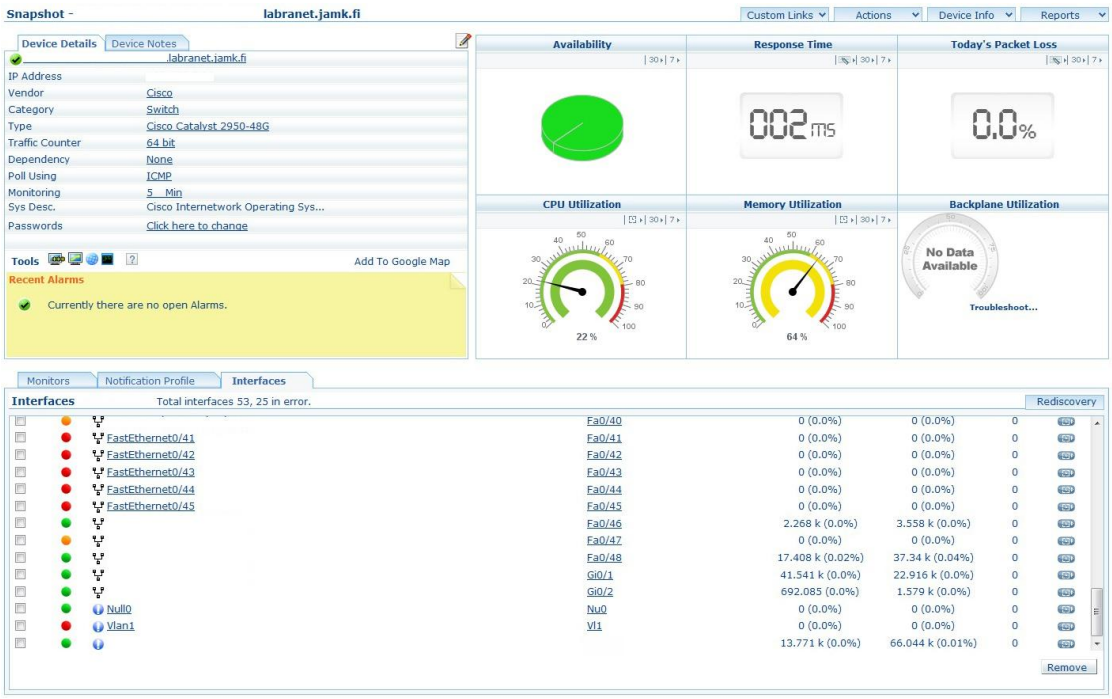
KUVIO 12. Valvontapöytä

Konfiguroinnin alussa laitteet määriteltiin ryhmiin ja kuviossa 13 havainnollistetaan kuinka kytkimien ryhmä listautuu. Sarakkeet vasemmalta oikealle: valmistajan merkki, laitteen nimi, laitteen tila, IP-osoite, laitteen malli, CPU-käyttöaste ja RAM-käyttöaste (Random-Access Memory).



KUVIO 13. Kytkimien listaus

Mentäessä yhä syvemmälle sovellukseen saadaan laitteen hallintasivu esille (kuvio 14). Vasempaan yläkulmaan on asetettu osio, jossa on laitteen perustiedot. Sen alta löytyy toinen välilehti, johon voi vapaasti kirjoittaa lisätietoja. Kaikki perustiedot ovat vapaasti muokattavissa hiiren painalluksella kohteen päällä. Oikeassa yläkulmassa on kokonaisuus, jossa on laitteen valvontaan liittyviä perustietoja. Arvot ovat selkeästi havainnollistettu graafisten mittareiden avulla, joten niiden lukeminen on todella nopeaa ja helppoa. Valitettavasti näitä graafisia mittareita ei saanut muutettua, esim. väylien käyttöaste (backplane utilization) olisi haluttu korvata laitteen lämpötilalla. Alimmaisessa osassa on kolme välilehteä, joista esillä on laitteen liitäntärajapinnat (interfaces). Kuviosta näkee hetkessä porttien tilan ja liikennemäärän. Muilla välilehdillä on mahdollisuus määrittää valvontakohteet (monitors) ja laitekohtaisesti käytettävät hälytysprofiilit (notification profiles).



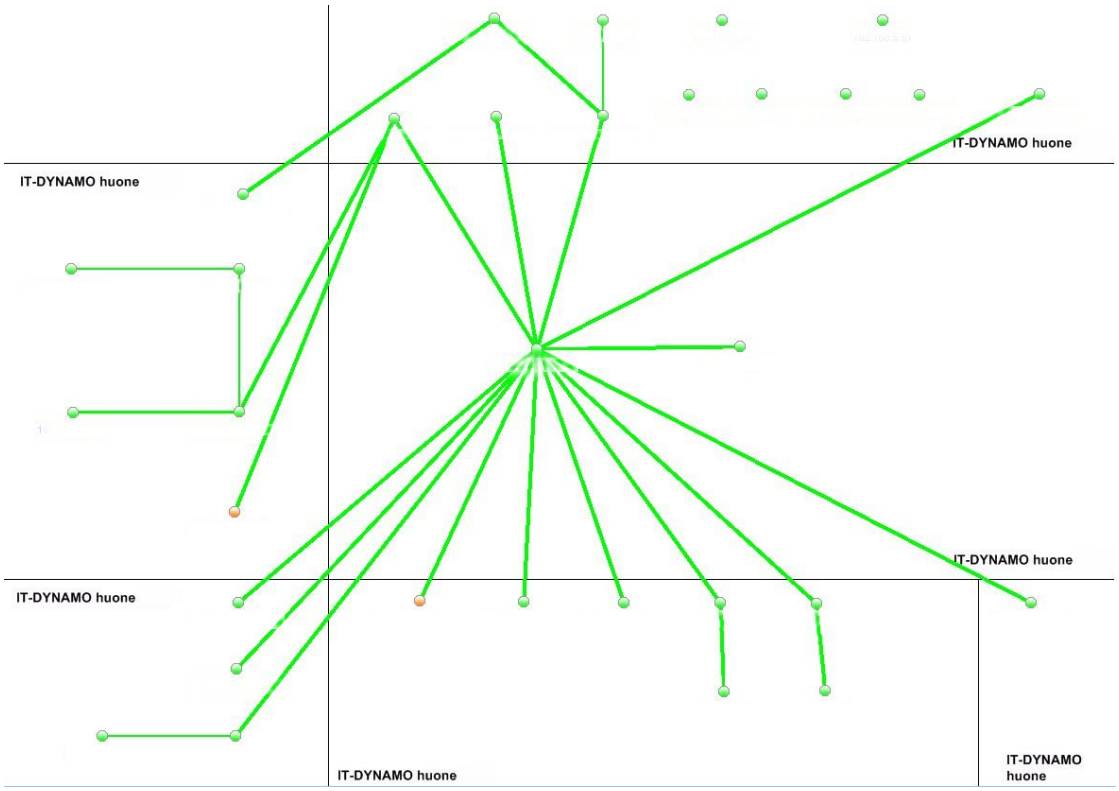
KUVIO 14. Laitteen hallintasivu

Kuviossa 14 käytiin lävitse rajapintojen listaus. Listasta valitsemalla oli mahdollisuus siirtyä sivulle, jossa informaatiota tuli vain yhdestä rajapinnasta (kuvio 15). Vasemmassa laidassa on tärkeimpänä rajapinnan käyttöaste ja sen muut perustiedot. Liikenteen profiili on määritelty myös erittäin tarkasti mm. pakettien koon ja määrän mukaan. Oikeassa laidassa on graafisia kuvaajia samoista asioista, mitä vasemmassa

laidassa numeerisesti esitetään. Kuvaajat on mahdollista määrittää halutuista arvoista lisäosien (widget) avulla.

KUVIO 15. Laitteen rajapinta

Mielestäni suurimman hyödyn valvonnassa antoi valvontakartta, joka on piirretty kuvioon 16. Kuviosta selviää heti, missä mahdollinen ongelmakohta on ja mihin kaikkiin laitteisiin se saattaa vaikuttaa. Kuviossa punaisena olevat pallot kuvaavat laitteita, joista hälytys on tullut. Hiirellä pystyy suoraan klikkaamaan laitetta ja siirtymään sen tietoihin (kuvio 14). Myös porttien välinen liikenne tulee esille viemällä hiiri vihreällä esitetyn linkin päälle ja siitä painamalla pääsee rajapintoihin käsiksi (kuvio 15).



KUVIO 16. Valvontakartta

Valvontakarttaan on käyttöönoton jälkeen tullut päivitys, jossa laitteita kuvaavien "pallojen" paikalle on mahdollisuus sijoittaa ikoneita kuvaamaan laitetta. Lisäksi liikennemäärä tulee näkyville viemällä hiiri linkin päälle.

5.3 Raportointi

Raportointi koettiin tärkeäksi ominaisuudeksi jo projektin alkumetreillä erityisesti johtoryhmän osalta. Järkevää ratkaisua mietittäessä raporttien jaottelusta päädyttiin kolmeen raporttiin. Ensimmäisestä raportista esitettäisiin aktiivilaitteiden, eli kytkimien, reitittimien ja palomuurien saatavuus ja CPU-käyttöasteet. Toisessa raportissa tulisi olla vastaavat mittarit palvelinlaitteiden osalta. Kolmannessa raportissa puolestaan keskitytään vain palveluiden saatavuuteen porttikohtaisella valvonnalla.

Käytännössä tämä ei kuitenkaan onnistunut, kuten oli kaavailtu, sillä raporttien tekemisessä tuli vastaan rajoituksia. Samalle raportille ei saatu liitettyä eri ryhmiä, kuten kytkimiä, reitittimiä ja palomuureja. Lisäksi samaan raporttiin ei pystytty lisää-

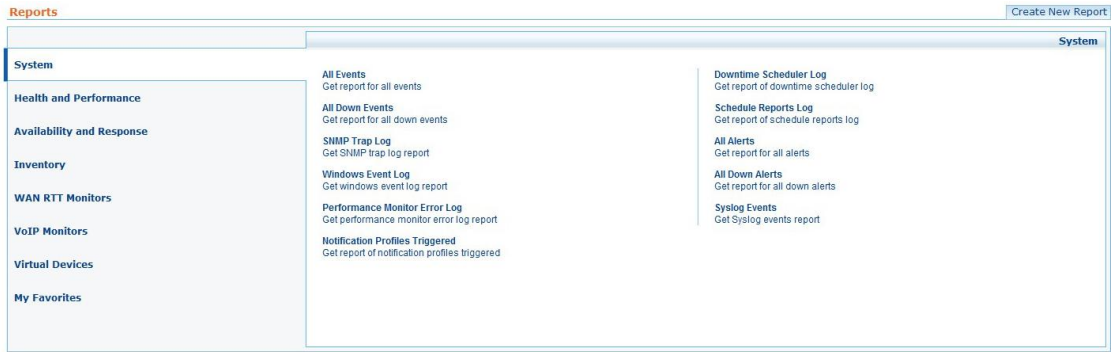
mään kahta kohdetta samanaikaisesti, kuten saatavuutta ja CPU-käyttöastetta. Mikäli kaikista ryhmistä ja kohteista olisi tehty raportit erikseen, olisi niitä kertynyt yhteensä ainakin yhdeksän kappaletta. Tällainen ratkaisu ei kuitenkaan palvele tiheään tehtävää raportointia kovin hyvin.

Sovellus tarjosi onneksi valmiin pohjan kaikkien laitteiden saatavuudelle, samanlainen raporttipohja löytyi myös CPU-käyttöasteelle. Aivan halutunlaiseen lopputulokseen ei siis päästy, mutta hyvin lähelle sitä. Palvelinten palveluporttien saatavuuden seuraamiselle löytyi myös valmis pohja, jollaista alun perin haluttiinkin. Liitteessä 3 esimerkki valmiista PDF-raportista, jossa kuvataan laitteiden saatavuutta.

Kuviossa 17 näkyy terveys ja suorituskyky -kohdasta (Health and Peformance) valittu yleiskuvan antava terveysraportti (Healt Raport), joka kertoo laitteiden yleisen kunnon. Ylärivissä vasemmalta oikealle on saatavuus, vastausaika pingiin ja pakettihävikki. Alarivissä vasemmalta oikealle on prosessorin käyttöaste, muistin käyttöaste ja kovalevyn käyttöaste, jota tosin valvottiin kuvankaappauksen yhteydessä vain yhdestä laitteesta.

KUVIO 17. Yleisraportti laitteiden tilasta

Sovelluksessa oli selkeästi panostettu raportointiin. Kuten kuviosta 18 selviää, niin raporttipohjia ja käyttötarkoituksia oli useita kymmeniä. Lisäksi käyttäjällä oli mahdollisuus luoda lisää raportteja.



KUVIO 18. Raportti-valikko

Hyvänä lisäominaisuutena oli raporttien automaattinen luominen tietyn ajanjakson välillä ja niiden välittäminen haluttuihin sähköposteihin. Näin ollen LabraNetin henkilökunnan ei tarvinut muistaa raporttien lähettämistä johdolle, vaan se toimi automaattisesti.

5.4 Koulutus

Käyttöönoton helpottamiseksi päätettiin järjestää koulutustilaisuus LabraNetin johtohenkilökunnalle. Koulutuksessa käytiin lävitse OpManagerin peruskäyttö, jota tarvitaan pienimuotoiseen verkonvalvontaan.

Koulutuksen aluksi käytiin läpi OpManageriin kirjautuminen ja kaikki perusvalikot mitä sovellus tarjoaa. Tämän jälkeen poistettiin yksi palvelimen valvottavien listalta automaattisen velhon (wizard) avulla. Jotta palvelin saatiin lisättyä takaisin, tehtiin SNMP ja SSH tunnistusmekanismit. Myös SNMP-palvelun lisääminen Linux-alustalle demottiin. Laite lisättiin takaisin valvottavien listalle ja se määriteltiin oikean tyyppiseksi Linux-laitteeksi.

Hälytykseen vaadittavien asetusten teko aloitettiin sähköpostipalvelimen konfiguroimisella. Seuraavaksi tehtiin hälytys-profiili, jota sovellus käyttää, kun mahdollinen hälytys tapahtuu. Viimeiseksi tehtiin tärkein eli lisättiin valvottavan kohteen laitteeseen raja-arvo ja yhdistettiin hälytys-profiili siihen.

Koska OpManager ei vielä tukenut, eikä luultavasti tule tukemaankaan, kaikkia mahdollisia laitteita mitä LabraNetistä löytyi, niin käytiin lävitse uuden alustan (template) luominen tuntemattomalle laitteelle. Laitteelle määriteltiin myös valvontakohteet ja niille hälytykset.

Valvontakartan (map) tekeminen ja siitä saatua hyötyä havainnollistettiin tekemällä sovellukseen uusi valvontakartta.

Lopuksi keskityttiin johtoryhmälle ehkäpä tärkeimpään ominaisuuteen, eli raporttien tuottamiseen. Käytiin lävitse raporttipohjat, jotka vastasivat aiemmin määriteltyjä vaatimuksia. Raporttien tyypit ovat edellisessä kappaleessa 5.3.

6 YHTEENVETO

6.1 Työn aloitus

Opinnäytetyön tarkoituksena oli toteuttaa Jyväskylän ammattikorkeakoulun Teknologia-yksikön LabraNet-verkkoon uusi valvontaohjelmisto. Projekti päätettiin aloittaa, koska vanha valvontaohjelmisto koettiin käytössä rajoittuneeksi, eikä se vastannut nykyajan vaatimuksia. Uuden ohjelmiston oli tarkoitus parantaa verkon luotettavuutta, käytettävyyttä ja suorituskykyä.

LabraNet tarjoaa palveluitaan pääosin opetuskäyttöön oppilaille ja opettajille. Palvelut voidaan jakaa kahteen osaan. Ensimmäiseen kuuluvat tietoverkkopalvelut: verkkolevytila, etäkäyttö, LabraNetin verkkosivut, kotisivutila, virtualisointi ja tietoturva. Toiseen osaan kuuluvat infrastruktuuripalvelut: työasemat, tulostus, SpiderNet, Cisco-akatemia, langaton verkko ja muut laboratoriot. Lopuksi vielä helpdesk ja asiantuntijapalvelut omina kokonaisuuksinaan.

Työ aloitettiin määrittelemällä sen vaatimukset LabraNetin henkilökunnan kanssa. Niihin kuuluivat valvontaohjelmistolle ja työn sisällölle asetetut vaatimukset. Tärkeimpinä mainittakoon ohjelmiston soveltuvuus ITIL:in määrittämiin suosituksiin ja Antti Vuorenmaan opinnäytetyössä suunnittelemien valvontakohteiden ja tapojen toteuttaminen.

6.2 Työn vastaavuus ITIL:n vaatimuksiin

ITIL on yli 20 vuotta kehitetty ja käytetty IT-palveluihin ja hallintaan kohdistuva kokoelma käytännön ohjeita. ITIL ei ole standardi vaan ohjeistus, jota noudattamalla verkon hallinnan laadukkuus on lähes taattu. Projekti toteutettiin ohjeistuksen perusteella ja seuraavissa kappaleissa on pohdintaa siitä, kuinka hyvin valvontaohjelmisto saatiin ITIL:n suosituksia vastaavaksi.

6.2.1 Kontrollointisilmukat

Kappaleessa 2.2.2 esiteltiin ITIL:in perustuva yksivaiheinen monitoroinnin kontrollointisilmukka. Sen pääperiaatteena on, että toimintoa on mahdollista muokata, mikäli se ei tuota haluttua lopputulosta. OpManagerin osalta periaate toteutuu osittain, koska se valvoo verkon toimintoja ja niiden lopputulosta. Koska ohjelmisto on keskittynyt pääosin vain valvontaan, eikä niinkään hallintaan, täytyy mahdolliset muutokset tehdä muilla työkaluilla, jotta haluttu lopputulos saavutetaan.

Kappaleessa 2.2.3 esiteltiin monivaiheinen monitoroinnin kontrollointisilmukka. Sen pääperiaatteena on, että valvontaa laajennetaan ja lopputuloksen tarkastelussa otetaan huomioon usean muuttujan aiheuttama lopputulos.

Kontrollointisilmukoiden yhteisenä esimerkkinä voidaan ottaa tiedostonsiirto ulkoverkosta sisäverkkoon, jonka seurauksena palomuuri kaatuu. Valvontakohteita ovat liikennemäärä ulkoverkosta palomuuriin, palomuurin prosessorin ja muistin käyttöasteet, palomuurin lämpötila ja liikennemäärä palomuurista sisäverkkoon. Näitä viittä kohtaa voidaan pitää erillisinä yksivaiheisina kontrolliosioina ja niitä tarkastelemalla pitäisi myös palomuurin kaatumiseen johtanut syy selvitä.

Liikennemäärät ovat suoraan yhteydessä palomuurin prosessorin ja muistin käyttöasteeseen, mikäli kapasiteettiä liikenteen käsittelyyn on liian vähän, aiheuttaa se ylikuormitusta ja mahdollisen kaatumisen. Jos palomuuri kuitenkin kykenee käsittelemään liikenteen, eikä kaatuminen johdu siitä, voidaan katsoa palomuurin lämpötilaa. Lämpötilan nouseminen johtuu useimmiten suuresta laitteen käyttöasteesta ja huonosta ilmanvaihdosta. Mikäli ei oteta huomioon mahdollisia ohjelmallisia häiriöitä, voidaan esimerkin ratkaisuna pitää ylikuumentumista ja siitä seurannutta laitteen kaatumista.

OpManager ei pysty ratkaisemaan ylikuumenemisen ongelmaa tehostamalla jäähdytystä, mutta sen avulla saatiin helposti selville mikä palomuurin kaatumiseen johti. Näin ollen voimme todeta, että kontrollointisilmukoiden periaate toimii nykyisellä valvontaohjelmistolla oikein hyvin.

6.2.2 Valvontakohteiden valinta

ITIL:n suositusten mukaan valvontakohteet tulee valita mahdollisimman laajasti kokonaisuutta ajatellen. Valvontakohteet oli ennalta määritelty Antti Vuorenmaan opinnäytetyössä (taulukko 2), mutta ne tarkastettiin vielä kertaalleen LabraNetin henkilökunnan kanssa. Muutoksia tehtiin yleisellä tasolla, niin että jokainen verkkoon kuuluva linkkiväli laitettiin valvontaan, pois lukien yksittäisille tietokoneille menevät yhteydet. Lisäksi verkkolaitteiden kohdalla tämä tarkoitti, että niistä valvottiin vähintään prosessorin ja muistin käyttöastetta, sekä lämpötilaa. Palveluiden valvonta toteutettiin Vuorenmaan määrittelemillä tavoilla, eli porttikohtaisella saatavuudella ja erillisien ohjelmien tarjoamilla mittareilla.

Mielestäni muutokset olivat hyviä, sillä ne laajensivat erityisesti aktiivilaitteiden tietoja. Lisäksi OpManagerissa oli valmiiksi tehty widgettejä, jotka kertoivat graafisesti esim. prosessorin käyttöasteen, joten niiden poisjättäminen olisi ollut ominaisuuksien hukkaan heittämistä.

Valitettavasti kaikista aktiivilaitteista ei saatu laajennettuja tietoja ulos (Nortel Ethernet Switch ja SAN Fiber Switch), joten niiden valvontakohteina toimi ainoastaan saatavuus. Mielestäni valvontakohteiden valinta kuitenkin onnistui ITIL:n suositusten mukaan, sillä valvottavana oli kaikki verkon aktiivilaitteet ja palvelut.

6.2.3 Monitorointitavat

Kappaleessa 2.2.7 esiteltiin aktiivista, passiivista, reaktiivista ja proaktiivista monitorointia, sekä niiden yhdistelmiä. LabraNetissä ei ole jatkuvaa aktiivista monitorointia, jolla tarkoitetaan reaaliaikaista valvontaa ihmisten toimesta. Vikatilanteissa tämä kuitenkin otetaan välittömästi käyttöön, jotta vika ja sen vaikutukset tulevat heti tietoon. Näin korjaustoimenpiteet ja palautuminen saadaan mahdollisimman nopeasti toteutettua.

LabraNetin yleisin valvontatapa on passiivinen, jolla tarkoitetaan ohjelmistojen tekemää valvontaa. Kun mahdollinen vikatilanne syntyy järjestelmä lähettää ilmoituksen henkilökunnalle, jolloin siirrytään aktiiviseen valvontaan. Passiivisen valvonnan edellytys on hyvin toteutetut valvontakohteiden valinnat sekä hälytysarvojen ja hälytystapojen järkevä määrittely. Valvontakohteet käsiteltiin edellisessä kappaleessa 6.2.2. LabraNetin aktiivilaitteille tehty valvontaväli vaihteli laitteesta riippuen viiden ja viidentoista minuutin välillä. Hälytysarvot määriteltiin laitteen valvontakohteiden ja niiden tarkoituksen mukaan. Yleisesti määriteltiin sähköpostihälytys käyttöön, koska henkilökunnalla on matkapuhelimet mukana, johon sähköpostit myös saapuvat. Kovin tarkkoja raja-arvoja ja hälytysprofiileita ei ehditty tekemään aikarajan puitteissa, joten LabraNetin henkilökunta tekee ne myöhemmin tarpeidensa mukaan.

Reaktiivista monitorointitapaa käytetään LabraNetissä, mutta ei vielä tässä järjestelmässä. Proaktiivista monitorointitapaa ei voitu vielä hyödyntää, koska OpMangerin käyttö on vasta alkuvaiheessa, eikä vaadittavia trendejä ole olemassa. Sovelluksesta löytyy kuitenkin mahdollisuudet näiden tapojen käyttöönottoon ja hyödyntämiseen.

Valitettavasti passiivista monitorointia ei ehditty kehittämään yksityiskohtaisesti jokaiselle laitteelle ja palvelulle erikseen, mutta tärkeintä on, että valvontakohteet ovat määritelty ja mahdollisesta viasta saadaan tieto järjestelmän kautta. Tulevaisuudessa kokemuksen kautta saadun tiedon perusteella monitorointitapoja on kuitenkin mahdollisuus kehittää sovelluksen ominaisuuksien ansiosta. Uskon, että valvonta tulee kehittymään pitkälti passiivisen ja reaktiivisen valvonnan sekoituksena.

6.2.4 Raportointi

Raportti on kooste verkossa tapahtuneista asioista. Se kertoo verkon tapahtumista ja laitteiden tilasta tietyllä aikavälillä. ITIL:n mukaan raportointi on turhaa, mikäli siihen ei liitetä toimintasuunnitelmaa. Tässä työssä emme kuitenkaan käsitelleet toimintasuunnitelmia erikseen, mutta hyvänä esimerkkinä voidaan pitää kuviossa 17 näkyvää prosessoreiden käyttöastetta kuvaavaa pylväsdiagrammia. Kuviosta selkeästi näkee, että yksi laite on erittäin rasittunut ja asialle tulisi tehdä jotain. Toimintasuunnitelmaksi voisi kehittää esim. laitteen vaihdon tehokkaampaan, liikenteen kierrättämisen muuta kautta tai laitteiden vähentämisen kytkimestä.

LabraNettiin määriteltiin kolme raporttia, joihin kuuluivat kaikkien laitteiden saatavuus, prosessorin käyttöaste ja palveluiden saatavuus. Nämä raportit edustavat tuotannollista raporttimallia, joka toimitetaan LabraNetin johdolle halutulla aikavälillä. Aikaväliä ei päätetty, mutta se sijoittuu viikon ja yhden kuukauden välille.

OpManager tarjosi hyvät raportointiin liittyvät mahdollisuudet ja mielestäni niitä hyödynnettiin myös erinomaisesti. ITIL ei varsinaisesti määrittely millaisia ja millä aikavälillä raportteja pitäisi tuottaa. Valitsimme raporttien sisällön loogisesti tärkeimpien valvontakohteiden mukaan ja aikavälin riittävän tiheäksi, jottei mahdollisia epämiellyttäviä yllätyksiä tule yhdellä kertaa ainakaan liian montaa. Näin ollen poikkeamiin pystytään puuttumaan nopeasti ja tehokkaasti.

6.3 Työn tekeminen

Työn aloittaminen ja suunnittelu tuntui aluksi hyvin helpolta, mutta sen edetessä alkoi todellisuus valjeta. Suurin haaste oli ehdottomasti Linux-laitteille tehtävät asennukset ja konfiguroinnit, jotka eivät varmasti olisi onnistuneet ilman apuvoimia. OpenSource-tuotteista luopuminen oli suorastaa helpotus ja lopputuloksen kannalta myös erittäin merkittävä päätös.

OpManagerin kanssa työskennellessä vaaditut asiat saatiin hyvin tehtyä ilman suurempia ongelmia. Graafisen käuttöliittymän ansiosta konfiguroiminen oli helppoa ja nopeaa, virheitä oli lähes mahdoton tehdä verrattuna tekstitiedostoihin kirjoittamiseen. OpMangerin tekninen tuki auttoi minua ongelmissa kiitettävällä arvosanalla.

Lopputulos on mielestäni erinomainen, LabraNetissä on nyt nykypäivän vaatimuksia vastaa verkonhallintasovellus. Sitä on mahdollista kehittää monipuolisemmaksi ja laajemmaksi verkon kasvun mukana.

Kiitos Antti Järviselle Linux-laitteiden konfiguroinnin avustuksesta. Kiitos Marko Vataselle LabraNetin muokkaamisesta tarpeisiini. Kiitos LabraNetin johdolle luottamuksesta ja mahdollisuudesta toteuttaa tämä opinnäytetyö.

6.4 Tulevaa

Kuten aikaisemmin mainittiin, niin Essential-versio toi mukanaan MS Exchangen, VMware ESX:n, MS SQL:n ja Active Directoryn valvontamahdollisuudet. Projektin aikataulu oli kuitenkin tuplaantunut, joten päädyimme ratkaisuun, että LabraNetin henkilökunta suorittaa lisäominaisuuksien käyttöönoton myöhemmin. Näin ollen varmistuimme siitä, että sovellus saatiin ajallaan käyttöön testattuna ja käyttövalmiina, eikä aikaa kulunut uusien ominaisuuksien testaamiseen.

Alkuperäisen suunnitelman mukaan LabraNetissä oli myös tarkoitus ottaa SNMP v3 käyttöön, mutta kiireisen aikataulun johdosta se päätettiin jättää myöhemmin tehtäväksi.

LÄHTEET

Bibbs, E. & Matt, B. 2006. Comparison of SNMP versions 1, 2 and 3. Tutkimus. Xin Tang. Viitattu 23.2.2010. Http://www.infosecwriters.com/text_resources/pdf/SNMP_BMatt.pdf.

Cattaneo, M. 2009. ITIL v3 Service Level Agreement Monitoring (SLAM) Charts, Video. Charles Sturt University. Viitattu 23.2.2010. Http://www.youtube.com/watch?v=FsY7lZtfdiI.

Continual Service Improvement. 2007. Office of Goverment Commerce. Iso-Britania: The Stationery Office.

Hautaniemi, M. 1994. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. Diplomityö. Aalto-yliopiston teknillinen korkeakoulu, Tietotekniikan osasto. Viitattu 23.2.2010. Http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/diplomityo.book.html.

Huuskonen, J. 2010. ELPA. Sähköpostiviesti 9.3.2010. Vastaanottaja J. Sunnari. Yleistietoa ELPA-projektin sisällöstä.

IT Service Management Forum Finland. 2010. itSMF:n kotisivut. Viitattu 24.2.2010. Http://www.itsmf.fi.

Jyväskylän ammattikorkeakoulu. 2010. Jyväskylän ammattikorkeakoulun kotisivut. Viitattu 23.2.2010. Http://www.jamk.fi.

Kaario, K. 2002. TCP/IP-verkot. Porvoo: WS Bookwell.

Lummevaara, V. 2008. SNMP v3 verkonhallinta & Ciscoworks. Opinnäytetyö. Satakunnan ammattikorkeakoulu, Tekniikan Porin yksikkö, Tietoktekniikan koulutusohjelma. Viitattu 23.2.2010. Https://publications.theseus.fi/handle/10024/740.

Reponen, E. 2006. Verkonvalvonta tutkimusverkossa. Tutkintotyöraportti. Tampereen ammattikorkeakoulu, Tietojenkäsittelyn koulutusohjelma. Viitattu 23.2.2010. Https://oa.doria.fi/handle/10024/5077?show=full.

Service Operation. 2007. Office of Goverment Commerce. Iso-Britania: The Stationery Office.

Vuorenmaa, A. 2009. LabraNetin IT-palveluiden hallinta. Opinnäytetyö. Jyväskylän ammattikorkeakoulu, Teknologiayksikkö, Tietotekniikan koulutusohjelma.

LIITTEET

Liite 1. Sovellusten vertailutaulukko

sovellus	agentit	etsintä	SNMP	SNMP v3	käyttis	maksullinen	dokumentointi	hylkysyy	muuta	sijoitus
AdRem NetCrunch	ei	ok?	ok	ok?	?	on	ei			
Argus							huono		kehitys lopetettu	
Cacti	ei								plugineja	
CiscoWorks						on			paljon komponetteja	
Colletd									pelkkiä plugineja	
FreeNATS				ei					olematon foorumi	
Ganglia	ok				ok		huono		paljon plugineja, sekava	
Groundwork		on				on			kallis	
Hyperic HQ	ok?	ok	ok	ok	ok	on?	ok		hinta?	3
Intellipool NM					win	on			Windows 2003 tai Windows 2008	
IPHost NM		ok		ok	win	on				
Manage Engine		ok	ok	ok	ok	on	ok			
Munin		ei			ok				paljon plugineja	
Nagios Core		plugin	plugin			ei		plugineja		4
NetMRI						on			25:n laitteen lisenssi $4,495	
NetQoS	ok					on				
Nimsoft			ok			on				
Opennms	ok	ok	ok	ok	ok	ei	ok		huonot kokemukset?	2
OPNET ace live					win	on				
Opsview	ok	ok	ok	ok				plugineja	toimii Nagioksen päällä	4
Orion	ok	ok	ok	ok	win	on			solarwinds	
Packet Trap	ok	ok	ok	ok	win	on				
Pandora FMS	ok	ok	ok	ok	ok	ei	ok			1
Performance Co-Pilot							ok		liian yksinkertainen	
Recinnoiter									epäselvä	
Scrutinizer									ilmaisversio nollaa ohjelmiston	
Server Check	ok	ok	ok		win					
SevOne			ok		win?	on				
Shinken	ok	plugin	plugin					plugineja	toimii Nagioksen päällä	4
Spice Works	ok	ok	ok		win					
Tclmon	ok	ok	ok				ei			
Zabbix	ok	ok	ok	ok	ok		ok			1
Zenoss	ei?	ok	ok	ok	ok	on	ok			3
Zyrion Traverse	ok	ok				on				

Liite 2. OpManager ja Opennms

OPMANAGER	OPENNMS
Pikavalinnat laitteen hallinnassa: info, ping, trace route, browser, telnet, RDC, interfaces, notifications, alerts, ym.	Info, status, events, alarms, graphs, interfaces
Muokattavat dashboard: Widgetit ja erilaiset näkymät, kaikki täysin muokattavissa eri tilanteisiin sopiviksi.	Valvonta ryhmät, hälytykset, huomautukset, status ja grafiikka.
Muokattavat valvontakohteet: response time, packet loss, cpu, memoru, disk, active processes ym.	Pääosin sama, suppeampi.
Yli 600 valmista device templatea + lisäys mahdollisuus. Valmiit MIB:t ja niiden lisäysmahdollisyys. Lisäksi MIB-selain	Tunnisti testikytkimen ja antoi sille oikean OID:n. Lisäysmahdollisuus?
Mapit, voi yhdistää Google Mappiin.	Sama, mutta map toimii vain IE:llä. Ei voi yhdistää Google Mappiin.
Käyttäjien hallinta. Käyttäjäkohtaiset asetukset.	Pääosin sama, laajemmat infot. Ei käyttäjäkohtaisia asetuksia.
WMI valvonta Windows- ympäristölle (pitää olla Windows asennuspohjana)	Onnistuu plugineilla.
Live viewing: lämpotila ja portin liikenne	Ei ole tarkoitettu live-seurantaan.
Palveluiden valvonta: Web, HTTPS, FTP, IMAP, LDAP, Telnet, MySQL, MS-Exchange, SMTP, POP3, WebLogic, Finger, Echo, DNS, NTTP ym.	Pääosin sama. Lisäysmahdollisuus?
Active Directoryn monitorointi (Essential edition).	Ei ole.
Nettisivujen valvonta: vastausaika ja saatavuus.	Sama ominaisuus.
Valvontakameroiden lisäys: CCTV View.	Ei ole.
Hälytystavat: EMail, SMS, WebAlerts, Run a progmram, Run a system command, Log a ticket (lisäosa), twitter.	E-mail, WebAlerts, sms plugin.
Intergroituu kaikkiin ManageEnginen tuotteisiin. Mahdollistaa erittäin suuren ja kattavan verkonhallinnan.	Yhteistyössä mm. Hypericin kanssa (agentit). Lisäosilla toimivia.
Auditointi.	Ei ole.
Raportointi, kattavampi.	On, mutta melko vaatimaton.
Konfigurointi graafisesta käyttöliittymästä.	Konfigurointitiedostot tekstinä, hankalia.
Loistava ohjekirja.	Ohjekirja ok.

Liite 3. Raportti

ManageEngine
OpManager

Devices Availability

Category	**All Devices**	Business View	**All Devices**
Period	**Last 30 days**	Time Window	**Full 24 hours**
Showing	**All**	Generated At	**Sun, 29 Aug 2010 12:11:59 EEST**

Name	Up	On Hold	Maintenance	Dependent Unavailable	Down	Availability(%)
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	0 Sec	100
	23 Days 12 Hours	0 Sec	0 Sec	0 Sec	0 Sec	100
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	12 Mins 54 Secs	99.96
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	19 Mins 58 Secs	99.94
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	19 Mins 58 Secs	99.94
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	19 Mins 58 Secs	99.94
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	14 Mins 45 Secs	99.96
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	9 Mins 58 Secs	99.97
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	0 Sec	100
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	0 Sec	100
	15 Days 1 Hour	0 Sec	0 Sec	0 Sec	0 Sec	100
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	17 Mins 56 Secs	99.95
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	17 Mins 59 Secs	99.95
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	14 Mins 57 Secs	99.96
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	19 Mins 12 Secs	99.94
	23 Days 13 Hours	0 Sec	0 Sec	0 Sec	14 Mins 56 Secs	99.96