Opinnäytetyö (AMK / YAMK)

Liiketalouden koulutusohjelma

Yrityksen tietoliikenne ja tietoturva

2016

Vesa Heirola

VERKONVALVONTA YRITYKSESSÄ: CASE VAKKA-SUOMEN VOIMA OY

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK / YAMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalouden koulutusohjelma

2016 | 37

Vesa Heirola

VERKONVALVONTA YRITYKSESSÄ: CASE VAKKA-SUOMEN VOIMA OY

Teknologian kehittyessä myös yritysten tietoverkot kasvavat, mikä edellyttää niiden valvontaa toimivuuden varmistamiseksi. Verkonvalvontaohjelman avulla yrityksen työntekijät pystyvät reagoimaan vikatilanteisiin nopeasti tai estämään niiden syntymisen kokonaan. Verkonvalvontaohjelman avulla saadaan lisäksi tärkeää informaatiota verkosta, jota voidaan käyttää hyväksi tulevissa laitehankinnoissa.

Opinnäytetyön tavoitteena oli luoda toimiva verkonvalvontaratkaisu yritykselle. Verkonvalvontaohjelman tuli kattaa satojen laitteiden kokoinen verkko, ja sen työkalut tuli olla monipuoliset ja tehokkaat. Toimeksiantaja oli valinnut sopivan ratkaisun, joka tuli käyttöönottaa.

Opinnäytetyön teoriaosuudessa perehdyttiin verkonvalvonnan perusteisiin ja selitetään yleisimpiä verkonvalvontaprotokollia, joista suurimmaksi osaksi keskitytään SNMP-protokollaan. Lisäksi käydään tarkemmin läpi varsinaista verkonvalvontaohjelmaa ja sen käyttöönottoon liittyviä asioita.

Kilpailutuksen jälkeen uudeksi verkonvalvontaohjelmaksi yritys on valinnut Qentinel Oy:n tuotteen nimeltä NetEye. Ohjelma oli kattava, monipuolinen ja edullinen vaihtoehto yritykselle.

Tavoitteet täyttyivät ja valvontakohteiden hälytysrajat konfiguroitiin sopiviksi. Lisäksi laitteista saatiin käyttäjälle paljon aikaisempaa enemmän informaatiota. Verkkolaitteiden tilannetta pystyy tarkkailemaan helposti NetEyen WWW-käyttöliittymästä.

ASIASANAT:

Verkonvalvonta, TCP/IP, SNMP, verkonhallinta

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Business Administration | Telecommunications and Information Security

2016 | 37

Vesa Heirola

NETWORK MONITORING IN COMPANY: CASE VAKKA-SUOMEN VOIMA OY

As technology advances, company networks grow as well, which consequently requires their supervision in order to ensure functionality. With network monitoring software, employees can react to error situations quickly or prevent them from occurring at all. Network monitoring software also gives important information about a network, which can be used for the benefit of future equipment purchases.

The objective of this thesis was to implement a functional network monitoring solution for the commissioning company. The network monitoring software should cover hundreds of network devices and its tools should be versatile and efficient. The commissioning company had already chosen a suitable solution, which had to be implemented.

The theoretical part of the thesis introduces the basic concepts of the network monitoring and explains the most common network monitoring protocols, with particular emphasis on the SNMP protocol. In addition, the thesis presents the actual network monitoring software and issues related to its implementation.

After competitive bidding, the commissioning company chose for its new network monitoring software a product called NetEye produced by a company called Qentinel Ltd. NetEye was a comprehensive, versatile, and affordable solution to the commissioning company.

The objective of this thesis was achieved and the alert limits of the network devices were configured to be suitable. In addition, the devices provided much more information to the user than before. The situation of the network can now be easily observed from the NetEye Web interface.

KEYWORDS:

Network monitoring, TCP/IP, SNMP, network management

SISÄLTÖ

KUVIOT

TAULUKOT

KÄYTETYT LYHENTEET TAI SANASTO

CPU	Suoritin tai prosessori, joka suorittaa tietokoneen käskyjä (engl. Central Processing Unit)
FCAPS	Verkonhallinta-standardi, jonka lyhenne määrittyy siihen sisältyneiden osa-alueiden nimien etukirjaimista
HOST	Verkon solmukohta, esimerkiksi palvelin, kytkin tai reititin
ICMP	TCP/IP-pinon kontrolliprotokolla (engl. Internet Control Message Protocol)
IP	IP-pakettien kuljetuksesta verkossa vastaava protokolla (engl. Internet Protocol)
ITU	International Telecommunication Union
KPI	Mittaa laitteen suoritusta (engl. Key Performance Indicator)
MIB	Laitteen yksittäinen objekti (engl. Management Information Base)
OID	Yhden kohteen yksilöivä numerosarja (engl. Object Identifier)
Ping	TCP/IP-protokollan työkalu, jolla selvitetään laitteen saatavuutta (engl. Packet InterNet Groper)
SNMP	Tietoliikenneprotokolla TCP/IP-verkkojen hallintaan (engl. Simple Network Monitoring Protocol)
TCP	Tietoliikenneprotokolla, jolla luodaan yhteys tietokoneiden välille (engl. Transmission Control Protocol)
TTL	Paketin toiminnassa olo aika (engl. Time To Live)
VSV	Vakka-Suomen Voima
VSV-E	VSV- Energia Oy

1 JOHDANTO

1.1 Perustietoa ja taustaa

Tämän työn toimeksiantajana toimi Vakka-Suomen Voima Oy, jonka tarvitsi päivittää konserninsa verkonvalvontaa. VSV-konserni tekee tiivistä yhteistyötä Rauman Energia Oy:n kanssa, jonka verkko myös tulisi lisätä uuteen verkonvalvontajärjestelmään.

VSV-konsernin emoyhtiö on Vakka-Suomen Voima Oy, joka hoitaa sähköjakelua noin 24 000 asiakkaalle. Yhtiön toiminta alkoi Uudessakaupungissa noin 100 vuotta sitten. VSV-konserniin kuuluvat myös VSV-Energia Oy, Suunnittelutoimisto Enertel Oy ja VER-TEK OY. Rauman Energia Oy on Rauman kaupungin kokonaan omistama energiayhtiö, joka tuottaa energiapalveluita. Tuotteita ovat muun muassa kaukolämpö ja sähkönsiirto sekä niihin liittyvät palvelut. Lisäksi Rauman Energia Oy ja Vakka-Suomen Voima Oy omistavat puoliksi sähkön hankinta- ja myyntiyhtiön nimeltä Lännen Omavoima Oy. (Vakka-Suomen Voima Oy 2016.)

Yhtiöt olivat yhdessä valinneet tulevaksi verkonvalvonta ratkaisuksi Qentinel Oy:n NetEye-verkonvalvontajärjestelmän sen edullisen hinnan ja laajojen työkalujen ansiosta. Yritykset tarvitsivat työntekijän, joka käyttöönottaisi kyseisen järjestelmän ja hallinnoisi sitä vuoden 2015 kesän ajan. Minut valittiin järjestelmän käyttöönottajaksi.

1.2 Tavoitteet

Opinnäytetyön tavoitteena oli luoda toimiva verkonvalvonta ratkaisu VSV-konsernin ja Rauman Energia Oy:n verkkolaitteille ja palveluille. Verkonvalvonta toteutettiin Qentinel Oy:n NetEye-verkonvalvontajärjestelmällä. Järjestelmällä oli tarkoitus myös kerätä hyödyllistä tietoa eri verkkolaitteista ja niiden toiminnoista.

Käytännön työni oli asentaa NetEye-palvelin ja lisätä sen WWW-käyttöliittymään yritysten valvontaan halutut verkkolaitteet ja palvelut. Verkkolaitteille tuli asettaa sopivat hälytysrajat, joiden ylittyessä järjestelmä lähettää hälytyksen verkonhallitsijoille. NetEyen pääsivun puunäkymä tuli konfiguroida sopivanlaiseksi, jotta molempien yritysten omat valvontakohteet olisivat erikseen.

Käyttäjä- ja hälytysryhmät tuli määrittää erikseen molemmille yrityksille, jotta vältyttäisiin turhilta hälytyksiltä esimerkiksi VSV-konsernin pääkytkimen hälytykset eivät menisi Rauman Energia Oy:n verkonhallitsijalle.

NetEyen laajoista ominaisuuksista tässä työssä tärkeimmät olivat ICMP- ja SNMP-pohjaiset työkalut. Näillä työkaluilla kerättiin tietoa muun muassa verkkoliikenteen laadusta, palvelimien levytilasta, muistin ja suorittimen käytöstä sekä tiettyjen porttien toiminnasta.

2 VSV-KONSERNI JA RAUMAN ENERGIA OY

Vakka-Suomen Voima Oy, VSV-Energia Oy, VERTEK Oy ja Suunnittelutoimisto Enertel Oy muodostavat VSV-konsernin. Tämän lisäksi VSV ja Rauman Energia Oy omistavat puoliksi Lännen Omavoima Oy:n.

VSV-konsernin emoyhtiö on Vakka-Suomen Voima Oy, joka hoitaa konsernissa sähkönjakelun asiakkaille. VSV vastaa sähkönsiirrosta noin 24 000 asiakkaalle sekä myös muista sähköverkkoon liittyvistä palveluista. Toiminta alkoi yli 100 vuotta sitten Uudessakaupungissa. (Vakka-Suomen Voima Oy 2016.)

VSV omistaa VSV-Energia Oy:n, joka syntyi kun kaukolämpöyhtiö VS Lämpö Oy ja sähkötuotantoyhtiö VSV-Energiapalvelu Oy fuusioituivat yhdeksi yhtiöksi 1.1.2015. VSV-E tuottaa kaukolämpöä Uudellekaupungille, sekä vastaa konsernin sähköntuotanto-osuuksista ja sähkötuotantoon liittyvästä kehittämisestä. (Vakka-Suomen Voima Oy 2016.)

VERTEK Oy rakentaa sähkö- ja televerkkoja koko Suomen alueella. Yhtiö hoitaa voimajohtojen, sähköjakeluverkkojen ja teollisuuden sähköverkkojen rakentamisen lisäksi valokaapeliverkkojen, ATK-sisäverkkojen ja mastoasennusten toteuttamista. VERTEK Oy omistaa kokonaan tytäryhtiönsä Rauman Sähköpalvelu Oy:n. (Vakka-Suomen Voima Oy 2016.)

Suunnittelutoimisto Enertel Oy on perustettu vuonna 1992. Sen päätoimisena työnä on tuottaa sähköenergian jakelu- ja käyttöjärjestelmiä, sähköteknisiä tieto- ja turvajärjestelmiä sekä näihin liittyviä palveluita. (Enertel 2016.)

Rauman kaupunki omistaa kokonaan Rauman Energia Oy:n, joka on energiapalveluiden tuottaja. Rauman Energia perustettiin vuonna 1997, jonka palveluksessa on keväällä 2016 35 työntekijää. (Rauman Energia Oy 2016.)

3 VERKONHALLINTA JA -VALVONTA

Teknologian kehittyessä yritysten tietoliikenneverkot kasvavat, mikä tarkoittaa niiden tarkkaa valvomista virhetilanteiden minimoimiseksi. Pienikin tietoliikenne-yhteyskatkos voi merkitä yritykselle suuria taloudellisia menetyksiä. Hyvällä verkonvalvonnalla voidaan virhetilanteiden minimoimisen lisäksi muun muassa vähentää laitekustannuksia ja tehostaa työntekijöiden toimintaa. Verkonvalvontaohjelman työkalut auttavat tunnistamaan potentiaaliset ongelmat, jotka voivat aiheuttaa verkon kaatumisen. (Nash & Behr 2007.)

Verkonhallinta ja verkonvalvonta-termejä käytetään tarkoittamaan samaa asiaa. ISO (International Organization for Standardization) on luonut näistä kahdesta verkonhallintastandardin X.700, jossa on yhdistetty verkonvalvonta sekä verkonhallinta samaan kokonaisuuteen. (Miller 2009.)

3.1 Verkonhallinnan määritelmä

Verkonhallinta tarkoittaa eri asioita eri ihmisille. Joissakin tapauksissa siihen kuuluu yksinäinen verkonvalvontajärjestelmä ja protokolla-analysaattori. Muissa tapauksissa verkonhallinta sisältää jaetun tietokannan, automaattisesti toimivat verkkolaitteet ja työasemat, jotka tuottavat reaaliaikaisesti graafista kuvaa tietoliikenteestä ja verkon muutoksista. Yleensä termi verkonhallinta on palvelu, joka tarjoaa erilaisia työkaluja, sovelluksia ja laitteita verkonhallitsijan käyttöön, jotta voidaan valvoa ja hallita verkkoa. (Jaakohuhta 2005, 306.)

Verkonhallinta on yksi iso kokonaisuus, johon on yleensä liitetty myös verkonvalvonta. FCAPS on standardi, joka on luotu yhdistämään verkonhallinta ja verkonvalvonta-termit. FCAPS-standardissa on viisi pienempää osa-aluetta, jotka ovat seuraavat:

- vikojenhallinta
- käytön hallinta
- kokoonpanon hallinta
- suorituskyvyn hallinta
- turvallisuuden hallinta (Wikipedia 2016a.)

Vikojenhallinta on yksi tärkeimmistä osa-alueista yrityksen verkon toimivuuden takaamiseksi. Vikatilanne tarkoittaa poikkeamaa normaalista toiminnasta verkon sisällä, minkä vuoksi jokin palvelu toimii heikosti tai ei toimi lainkaan. Vikatilanteiden hallintaan kuuluvat verkossa olevien laitteiden vikojen -havaitseminen, erottaminen ja korjaaminen. Vian korjaamisen jälkeen tulee seurata laitetta, jossa vika on ilmennyt toiminnan varmistamiseksi. Vian aiheuttajan syyt tulee dokumentoida tulevaisuuden vikatilanteita varten. (Jaakohuhta 2005, 309.)

Verkonhallitsijalla täytyy olla oikeus hallita laitteiden välisiä yhteyksiä ja tarvittaessa muokata reititystä käyttäjien tarpeiden mukaiseksi. Kokoonpanon hallinnan tehtäviin kuuluu laitteiden ylläpito, käynnistys tai pysäytys sekä tunnistus ja verkossa olevien laitteiden välisten yhteyksien määrittäminen. Kaikki tehtävät pystytään suorittamaan etänä verkonhallintaohjelmiston avulla. (Wikipedia 2016a.)

Käytön hallinnassa voidaan seurata eri käyttäjien verkon käyttöä. Tietoa käyttäjien verkon käytöstä hyödynnetään muun muassa tulevaisuuden laitehankinnoissa. Joissakin tapauksissa joudutaan myös rajaamaan verkon käyttöä eri käyttäjien tai käyttäjäryhmien osalta. Käytön hallinnasta on hyötyä myös laskutuksessa, kun tiedetään tarkkaan eri henkilöiden verkon palveluiden käyttö. (Jaakohuhta 2005, 310; Puska 2000, 307.)

Suorituskyvyn hallinnan pääasia on pitää verkon toiminta hyväksyttävällä tasolla. Sen työnä on kerätä tietoa verkossa olevien laitteiden tai palveluiden suorituskyvystä. Verkon suorituskyky koostuu valvonnasta ja hallinnasta. (Jaakohuhta 2005, 310.)

Turvallisuuden hallinta on tärkeä verkonhallinnan osa-alue, jolla voidaan hallita käyttäjäoikeuksia ja mahdollisia oikeusrikkomuksia. Turvallisuuden hallinnalla tarkoitetaan verkon laitteisiin pääsyä ja tarkastustoimia sekä pääsyä tietoon, jota verkkolaitteilta on kerätty. (Jaakohuhta 2005, 310.)

3.2 Verkonvalvonnan perusteet

Verkon ylläpitäjän vastuualueisiin kuuluu huolehtia verkon suorituskyvyn riittoisuudesta, jotta verkko toimisi moitteettomasti. Uusien laitteiden tai asiakkaiden liittäminen verkkoon saattaa luoda pullonkaulaefektin. Verkon ylläpitäjän tehtäviin kuuluu estää pullonkaulaefektin syntyminen, tai muun vastaavan, joka hidastaa verkkoliikennettä tai aiheuttaa verkon ylikuormittumisen. (Koegh 2001, 276.)

Verkonvalvonta termiin sisältyvät ITU-T:n verkonhallintastandardi X.700:n mukaan seuraavat osa-alueet: suorituskyvyn hallinta, vikojen hallinta ja käytönhallinta. Verkonvalvonnalla tarkoitetaan yleisesti verkossa olevien fyysisten laitteiden sekä tietokoneohjelmien valvontaa. Verkonvalvonta koostuu normaalisti verkonvalvontaohjelmasta, valvottavista laitteista ja SNMP-protokollasta. Verkonvalvonnan suoranainen tavoite ei ole lisätä tietoturvaa verkolle, vaan parantaa sen toimintakykyä sekä nopeuttaa vikatilanteiden huomaamista ja korjaamista.

Verkonvalvontaohjelman avulla yritys voi välttyä isoilta taloudellisilta menetyksiltä, sen reaaliaikaisen hälytysjärjestelmän ansiosta. Se valvoo verkkoa jatkuvasti, kun se huomaa verkossa poikkeaman esimerkiksi viiveen vastauksessa, se ilmoittaa käyttäjälle hälytyksen muodossa mahdollisesta vikatilanteesta. Hälytyksen ilmoitustapoja on monia, mutta yleisimpiä ovat tekstiviesti ja sähköposti. Joissakin ohjelmissa on mahdollista ladata älypuhelimeen oma valvontasovellus, minne ilmoitus lähetetään.

Verkonvalvontaohjelmia on tuhansia. Ne ovat ulkonäöllisesti ja työkalullisesti erilaisia, mutta niillä on kuitenkin yksi tärkeä yhteinen tekijä: SNMP-protokolla. Muitakin verkonvalvontaprotokollia on, mutta näistä yleisin on SNMP (Simple Network Monitoring Protocol). Se on kehitetty juurikin verkonvalvontaan. Sen avulla pystytään valvomaan lähes mitä vain verkkolaitetta tai verkon palvelua.

4 PROTOKOLLAT

4.1 ICMP

ICMP (Internet Control Message Protocol) on kontrolliprotokolla, joka on kehitetty viestimään laitteiden välillä erilaisista ongelmista ja virheistä. Kyseistä protokollaa käyttävät avukseen monet verkkolaitteet, kuten kytkimet, reitittimet ja isäntäkoneet. ICMP sisältää muitakin toimintoja kuin virheen raportoinnin, se muun muassa selvittää yksittäisen laitteen saatavuutta ja uudelleenohjaa reitityksen tarpeen vaatiessa. (Wikipedia 2016b.)

ICMP-protokolla on sijoitettu arkkitehtuurissa verkkokerroksessa sijaitsevan IP:n alle. Kaikki sanomat, jotka ICMP-protokollalla lähetetään, sisällytetään IP-pakettiin ja lähetetään vastaanottajalle IP-osoitetta hyväksi käyttäen. (Wikipedia 2016b.)

ICMP on tärkeä valvontaprotokolla, joka kuuluu jokaisen verkonvalvontaohjelman työkaluvalikoimiin sen generoimien hyödyllisten sanomien vuoksi. Sanomia on yhteensä olemassa 27 erilaista, joista tämän opinnäytetyön kannalta tärkeimmät ovat seuraavat:

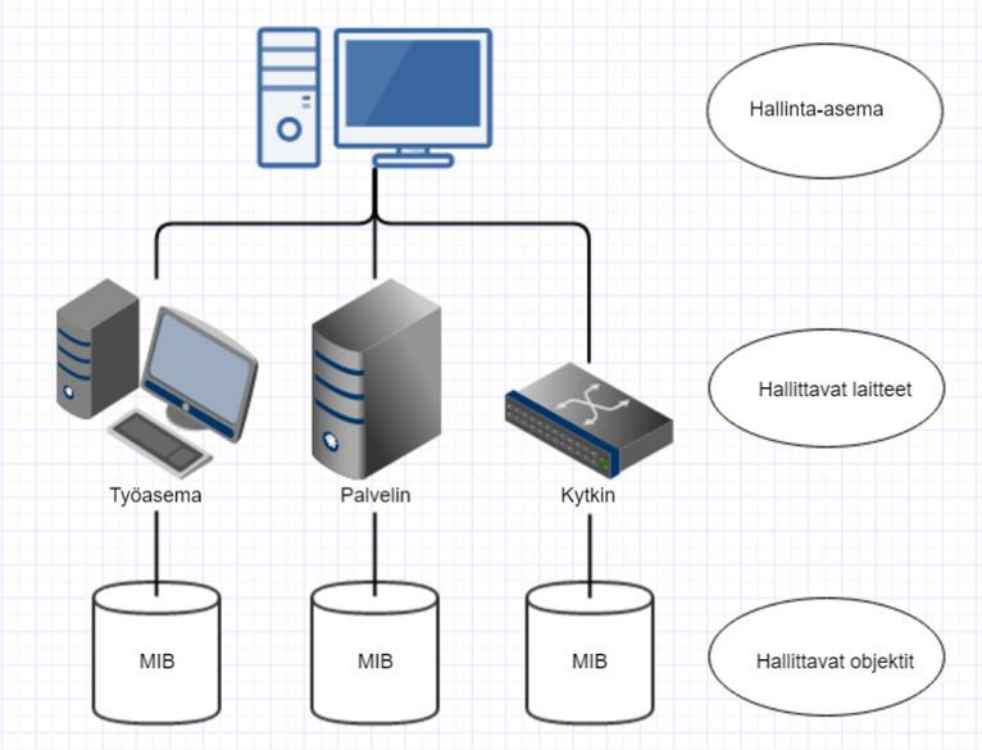
- Echo- ja Echo reply- viesti saadaan syöttämällä PING komento laitteelta toiselle. Echo reply sanoma palautuu, jos kohdekone löytyy.
- Destination Unreachable- viesti lähetetään kyselyn suorittaneelle laitteelle, kun viesti ei pystynyt välittämään määränpäähän.
- Redirect- viesti lähetetään kyselyn suorittaneelle laitteelle reitittimen osalta silloin, kun reititin löytää uuden paremman reitin sanomalle.
- Time exceeded- viesti palautuu reitittimestä kyselyä suorittaneelle laitteelle, kun TTL:n (Time to Live) arvo nollaantuu. Kun arvo nollaantuu, on reitittimen tehtävänä tuhota paketti. (Microsoft 2016.)

4.2 SNMPv1

SNMP on keskeisin verkonhallintaan kehitetty protokolla, jolla valvotaan TCP/IP-verkkojen toimintaa. Protokollan tehtävänä on kysellä verkossa olevien laitteiden tilaa ja raportoida mahdollisista virhetilanteista. SNMP on valmistajariippumaton verkonhallintarat-

kaisu, jonka vuoksi sillä voidaan valvoa useimpia verkkolaitteita. SNMPv1:n käyttö nykyaikana on melko harvinaista sen huonon tietoturvan vuoksi. Kuviossa 1 on havainnollistettu SNMPv1:n hallintaympäristön rakenne, joka koostuu seuraavista komponenteista:

- Hallinta-agenteista (Management Agent), kuten reitittimistä, kytkimistä, työasemista, palvelimista ja tulostimista
- Hallinta-asemasta (Management Station), joka kerää laitteilta saadun tiedon
- Hallintatietokannasta (Management Information Base), joka koostuu eri objekteista. Objektit ovat muuttujia, jotka kuvaavat hallinta-agenttien jotain pienempää osaa (Jaakohuhta 2005, 313.)

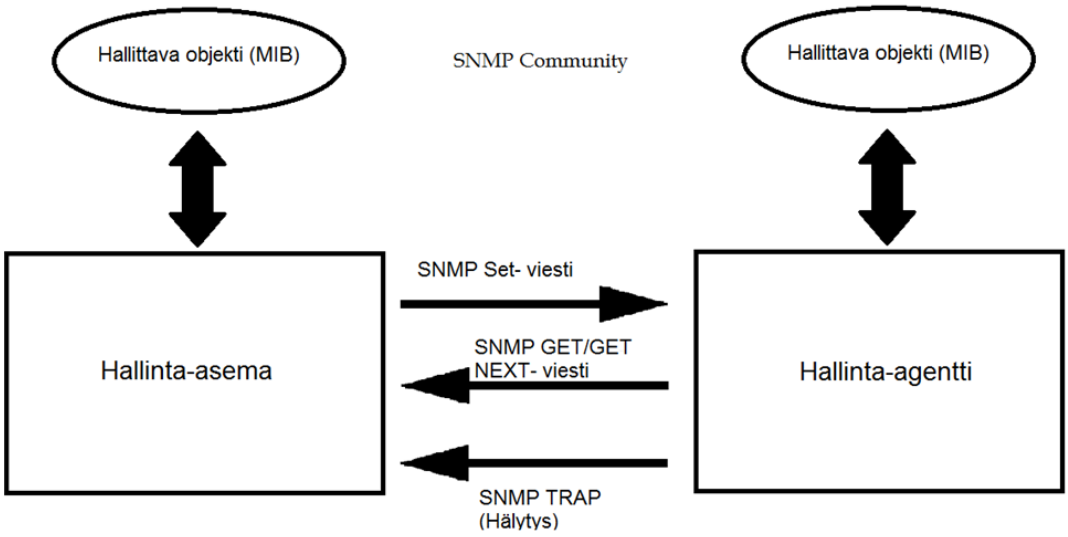


Kuvio 1. SNMP-hallintaympäristön rakenne (Jaakohuhta 2005, 313.)

SNMPv1:n kommunikointi agenttien välillä on tehty erittäin yksinkertaiseksi. Kuviossa 2 on selvennetty protokollan kommunikointitapaa. Protokollassa on neljä erilaista viestiä, jotka ovat seuraavat:

- GET, jota hallinta-asema käyttää saadakseen yhden tiedon agentilta
- GETNEXT, jota käytetään useamman tiedon eli tietosarjan hakuun. Tällainen on esimerkiksi taulukko
- SET, jolla hallinta-asema voi muokata hallinta-agenttien objektien arvoja

- TRAP, joka informoi hallinta-asemaa verkon merkittävistä tapahtumista. (Cisco 2016a.)



Kuvio 2. SNMP:n kommunikointi (Haikonen, Hlinovsky & Paju 2000.)

4.2.1 SNMPv2

Ensimmäisen SNMP-version oltua käytössä useita vuosia havaittiin siinä oleellisia ongelmia ja parannuskohteita. Tämä johti kehitystä alkuperäisestä protokollasta toiseen versioon, jonka tarkoituksena oli parantaa SNMP:n ensimmäistä versiota monelta osin. SNMPv2:n päätavoitteet olivat parantaa tietoturvaa, joustavuutta, tehokkuutta sekä laajentaa protokollan toimintaa. (TCP/IP Guide 2016.)

SNMPv2 lisättiin myös kaksi uutta operaatioita: GETBULK ja INFORM. GETBULK operaatio on verrattavissa GETNEXT operaatioon. Operaatiota käytetään suuren datamäärän hakemisessa. INFORM operaatio on samankaltainen kuin TRAP, mutta se saa kuittaussanoman tiedon välityksestä. (Net-SNMP 2016 & Cisco 2016a.)

Tietoturvaa on parannettu toisessa versiossa mahdollisella yhteisöavaimella, joka luotiin käyttäjän tunnistusta varten. SNMPv2 on edelleen varsin laajassa käytössä, vaikka uudempi versiokin SNMP:sta on luotu. (Cisco 2016b.)

4.2.2 SNMPv3

SNMPv3 on protokollan uusin käytössä oleva versio, joka otettiin käyttöön vuonna 2002. SNMPv3 on täyttänyt IETF:n (Internet Engineering Task Force) mukaan täyden Internet-standardin mitat, joka on korkein mahdollinen RFC-standardi. Versio luotiin osittain samasta syystä kuin toinen versiokin, nimittäin lisäämään tietoturvaa. Suojauksen lisäksi parannettiin myös etäkonfigurointia. (Cisco 2016c.)

SNMPv3:n suurimpana tietoturvallisuuden erona aiempaan versioon on sen turvajärjestelmä. Turvajärjestelmän tehtävät ja niiden tarkoitukset ovat seuraavat:

- Eheyden tarkistus: Varmistaa ettei paketteja ole muutettu siirron aikana
- Autentikointi: Varmistaa oikea lähde
- Salaus: Varmistaa ettei tieto välity ulkopuolisille. (Cisco 2016c.)

Tuoreimmassa versiossa on myös uusi käytäntö yhteisöavaimelle. Uudessa menetelmässä on käytössä ryhmä- ja käyttäjänimet. Jokaiselle ryhmälle ja käyttäjälle voidaan määritellä omat tietoturvatasot. Tietoturvatasoja on kolme, jotka määrittyvät joko autentikointisalasanalla, salaussalasanalla tai molemmilla. (Lummevaara 2008, 22.)

5 QENTINEL NETEYE VERKONVALVONTAJÄRJESTELMÄ

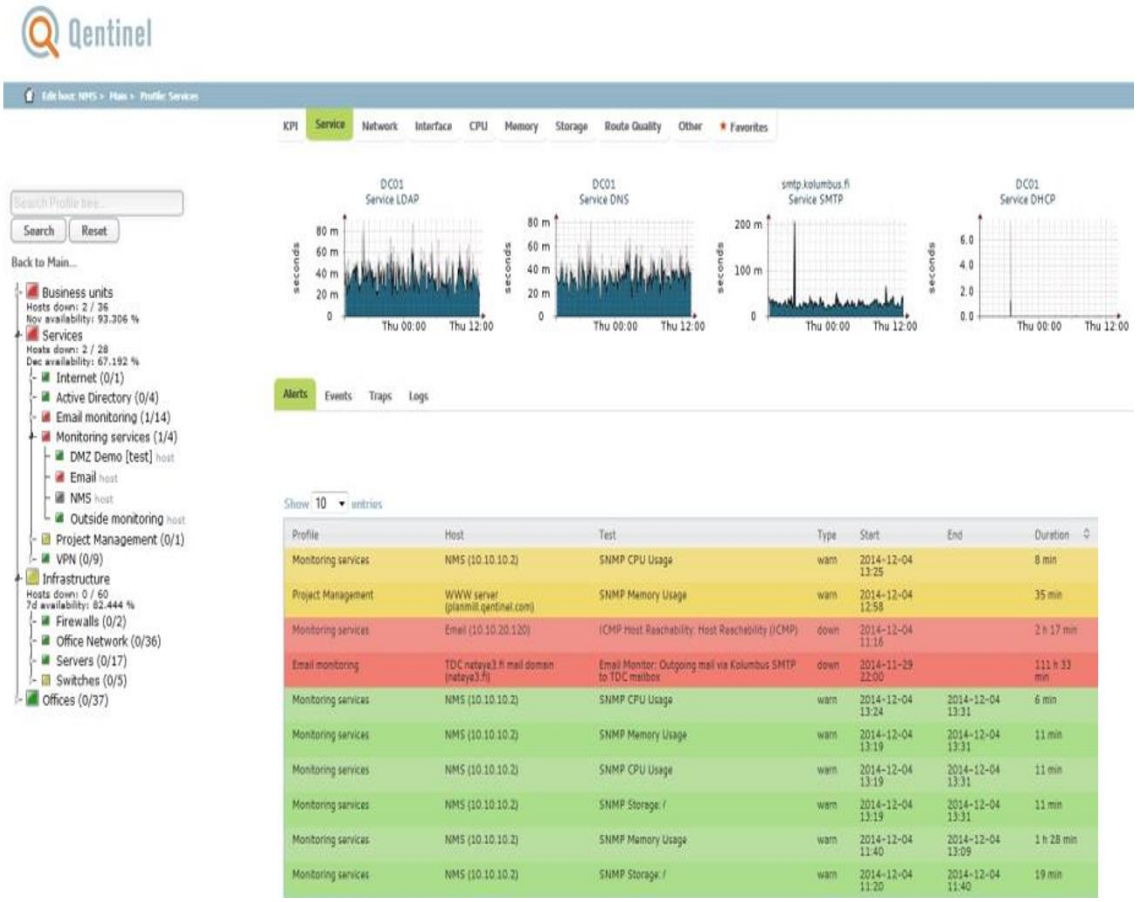
Qentinel NetEye valvoo ICT-palveluja, verkkoa sekä antaa arvokasta informaatiota palvelujen tuottamiseen liittyvistä resursseista. Perusvalvonnan lisäksi NetEyen työkalut mahdollistavat suorituskyvyn- ja käytettävyyden valvonnan ulottumisen komponenteista aina liiketoimintaprosessien suorituskyvyn mittaamiseen saakka. Selainpohjaisesta WWW-käyttöliittymästä hallitaan koko järjestelmää. (Qentinel Oy 2016, Cinia Group Oy 2016.)

Qentinel Oy:n mukaan NetEyen tärkeimmät ominaisuudet ovat:

- Reaaliaikainen valvonta
- Skaalautuvuus erilaisiin ympäristöihin
- ICT-palvelujen visualisointi palvelukartoilla
- Käyttäjäryhmäkohtaiset näkymät
- Monipuoliset raportointimahdollisuudet
- Käyttäjäsimulaatio
- Integroitavuus (Qentinel Oy 2016.)

Qentinel NetEyessa on selainpohjainen WWW-käyttöliittymä, josta koko järjestelmää hallitaan. Käyttöliittymä on jaettu kahteen loogiseen ryhmään: valvontaan ja hallintaan. Hallinta on käyttäjille, jotka voivat konfiguroida järjestelmää. Valvonta on käyttäjille, jotka voivat vain valvoa laitteiden toimimista muokkaamatta järjestelmää.

Käyttöliittymän pääsivu päivittyy automaattisesti tietyin väliajoin antaakseen valvojalle mahdollisimman helpon tulkinnan valvottavien kohteiden nykytilasta. Pääsivu on mahdollista myös päivittää itse painamalla F5-nappia useimmissa selaimissa. NetEyen pääsivu on esitetty kuviossa 3.

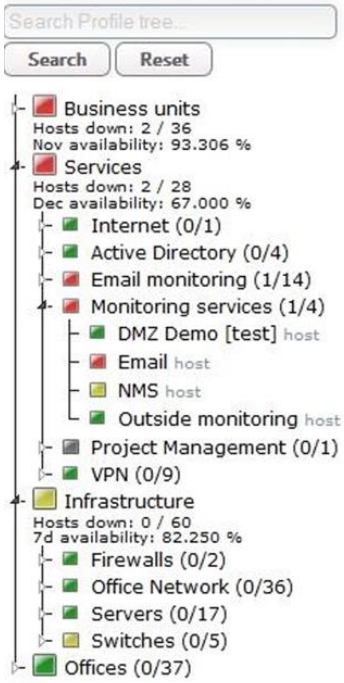


Kuvio 3. NetEyen pääsivu (Qentinel NetEye 4.1.0 Administrator manual 2013.)

5.1 Puunäkymä

Käyttöliittymän pääsivun vasemmassa reunassa on Qentinel NetEyen puunäkymä, jossa on listattu kaikki valvottavat laitteet. Puunäkymä koostuu eri ryhmistä, joita kutsutaan profiileiksi. Omana profiilinaan voivat olla esimerkiksi kytkimet ja palvelimet. Hallintaoikeudet omaava käyttäjä pystyy itse luomaan puunäkymästä omanlaisensa kokonaisuuden ja muokkaamaan sitä tarpeen vaatiessa.

Jokaisen profiilin nimen perässä on kaksi lukua sulkujen sisällä. Ensimmäinen kertoo hälytystilassa olevien isäntien määrän kyseisessä profiilissa. Toinen luku kertoo isäntien kokonaismäärän profiilin ja sen aliprofiilien alla. Kuviossa 4 on esitetty Qentinel NetEyen puunäkymä. (Qentinel NetEye Administrator manual 2013, 7-8.)



Kuvio 4. Pääsivun puunäkymä (Qentinel NetEye 4.1.0 Administrator manual 2013.)

Kuviosta 4 nähdään profiilien neljä eri tilaa, jotka ovat kuvattuna erivärisillä neliöillä:

- Vihreä neliö: kaikki testit ovat menneet hyväksytysti läpi
- Keltainen neliö: varoitus tila, esimerkiksi jokin isäntä ei vastaa SNMP-kyselyyn
- Punainen neliö: yhden tai useamman kyselyn suorittaminen epäonnistuu, tai testi on ylittänyt määritetyn hälytysrajan, joka tarkoittaa laitteen olevan hälytystilassa
- Harmaa neliö: profiili ei ole valvottavana tai yhtään isäntää profiilissa ei ole aktiivisessa valvonnassa.

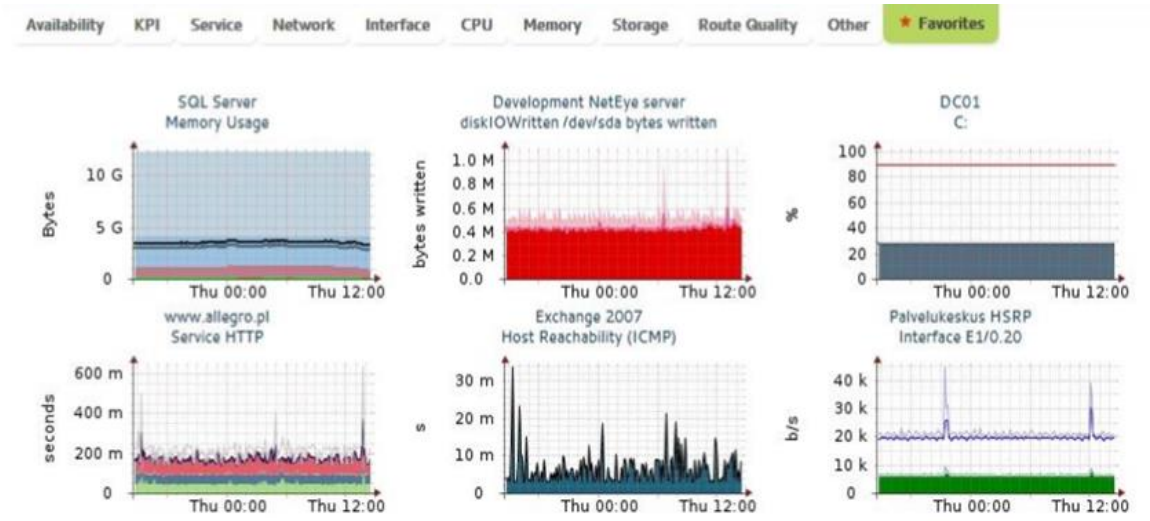
5.2 Valvonnan ylänäkymä

NetEyen pääsivun yläreunassa on valvonnan ylänäkymä. Ylänäkymää käytetään näyttämään aikaan perustuvia kaavioita eri kategorioista, jotka perustuvat käyttäjän määrittämiin arvoihin profiileissa. Kaikki objektit NetEyessa voidaan merkitä KPI (Key Performance Indicator) merkinnällä, jolla saadaan kerättyä kokoon kaikki yrityksen kannalta kriittisimmät kaaviot. (Qentinel NetEye 4.1.0 Administrator manual 2013, 9-10)

Ylänäkymässä voi olla enintään 10 eri välilehteä. Saatavilla olevien välilehtien lukumäärä riippuu eri testeistä, joita on konfiguroitu järjestelmään. Kuviossa 5 on esitetty valvonnan

ylänäkymä. Mahdolliset testit, joita käyttäjä voi ylänäkymään konfiguroida ovat seuraavat:

- Availability
- KPI
- Service Latency
- Network Latency
- Interface
- CPU
- Memory
- Storage
- Route Quality
- Other
- Favorites (käyttäjä saa itse määrittää, mitä kaavioita haluaa lisätä) (Qentinel NetEye 4.1.0 Administrator manual 2013, 9-10.)



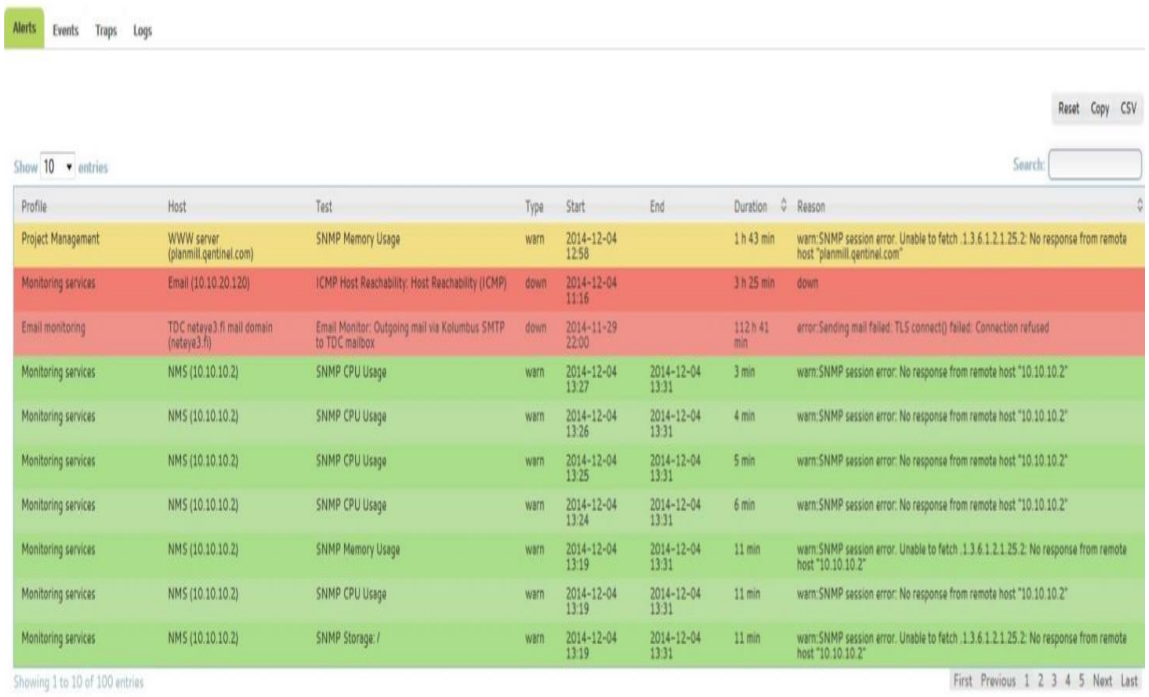
Kuvio 5. Valvonnan ylänäkymä (Qentinel NetEye 4.1.0 Administrator manual 2013.)

5.3 Ilmoitusnäkymä

NetEyen sivun alaosassa on ilmoitusnäkymä, josta näkee valvottavien kohteiden tapahtumat ja hälytykset. Ilmoitusnäkymässä on neljä eri välilehteä, jotka ovat: Hälytykset, Tapahtumat, Lokit ja Trapit.

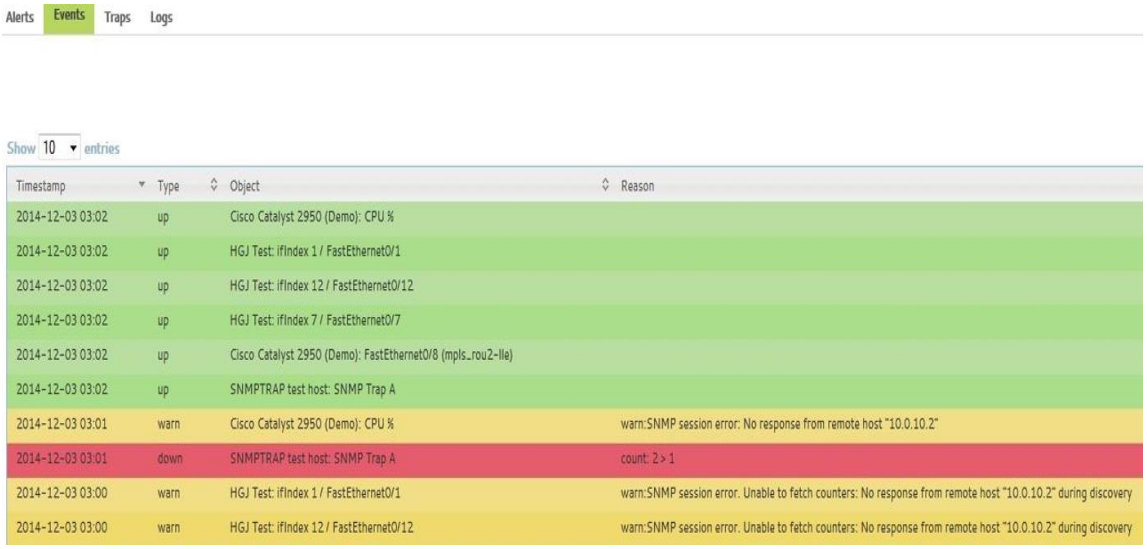
Hälytykset (Alerts)- välilehti näyttää kaikki järjestelmän tietoon tulevat varoitukset ja hälytykset. Yleisin hälytyksen aiheuttaja on hälytysraja-arvon ylittyminen tai laite ei vastaa. Hälytykset-välilehdessä on kuvattu tapahtumat ja virheet erivärisillä palkeilla.

Vihreä palkki kertoo tapahtumahistorian, jossa jokin laite on ollut hälytys/varoitus tilassa, mutta on itsestään alkanut vastaamaan kyselyihin. Keltainen palkki kertoo varoituksesta, jossa esimerkiksi laite ei vastaa SNMP-kyselyyn tai varoitus raja-arvo on ylitetty. Punainen palkki tarkoittaa hälytystilaa, jossa valvottavan kohteen katsotaan olevan alhaalla. Hälytysraja-arvo on ylittynyt tai yhteyttä ei saada muodostettua valvontakohteeseen. Kuviossa 6 on esimerkki Hälytykset-välilehdestä.



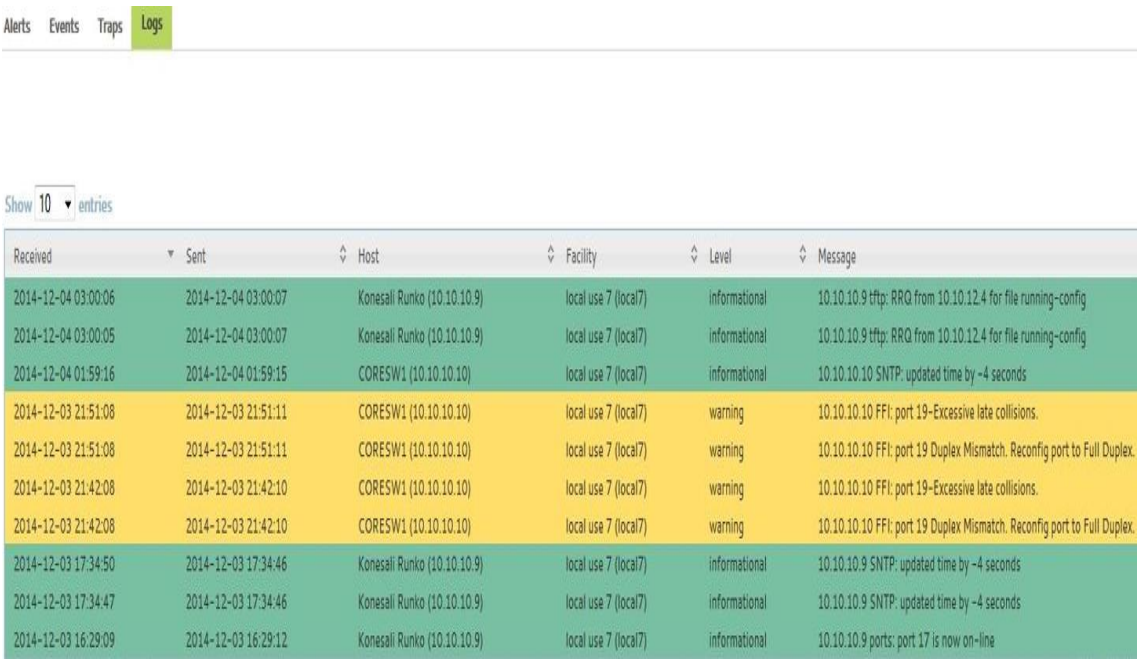
Kuvio 6. Hälytykset-välilehti (Qentinel NetEye 4.1.0 Administrator manual 2013.)

Tapahtumat (Events)-välilehti näyttää kaikki, mitä järjestelmässä on tapahtunut valvonnan aikana. Kuviossa 7 on esimerkki tapahtumat välilehdestä.



Kuvio 7. Tapahtumat-välilehti (Qentinel NetEye 4.1.0 Administrator manual 2013.)

Lokit (Logs)-välilehti näyttää kaikki järjestelmälokin viestit. Testien eri kategoriat vaikuttavat viestien näkyvyyteen Lokit-välilehdellä. Lokit-välilehden omat viestit ovat jaettu eri kategorioihin, jotka ovat: hätätila, hälytys, varoitus, huomio, info ja debug. Kuviossa 8 on esimerkki Lokit-välilehdestä. (Qentinel NetEye 4.1.0 Administrator manual 2013, 13.)



Kuvio 8. Lokit-välilehti (Qentinel NetEye 4.1.0 Administrator manual 2013.)

Trapit (Traps)-välilehti näyttää kaikki SNMP-Trap viestit, jotka ovat konfiguroitu vastaanotettaviksi. Välilehdeltä selviää milloin trapit on lähetetty, viestien alkuperä, OID (Object

Identifier) tieto ja viestin arvot. Kuviossa 9 on esimerkki Trapit-välilehdestä. (Qentinel NetEye 4.1.0 Administrator manual 2013, 12.)

Show 10 entries

Sent	Host	OID	Message
2014-12-04 03:00:07	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.3.7.11.29.0.2	RMON-MIB::eventDescription.130: "I 12/04/14 03:00:07 tftp: Transfer completed"
2014-12-04 03:00:06	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.3.7.11.29.0.2	RMON-MIB::eventDescription.129: "I 12/04/14 03:00:06 tftp: RRQ from 10.10.12.4 for file running-config"
2014-12-04 01:59:16	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.3.7.11.29.0.2	RMON-MIB::eventDescription.412: "I 12/04/14 01:59:15 SNTP: updated time by -4 seconds"
2014-12-03 21:51:08	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.14.12.1.0.5	enterprises.11.2.14.11.1.7.2.1.4.2552: 4 enterprises.11.2.14.11.1.7.2.1.5.2552: 2 enterprises.11.2.14.11.1.7 "http://10.10.14.10/cgi/fDetail?index=2552"
2014-12-03 21:42:08	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.14.12.1.0.5	enterprises.11.2.14.11.1.7.2.1.4.2550: 4 enterprises.11.2.14.11.1.7.2.1.5.2550: 2 enterprises.11.2.14.11.1.7 "http://10.10.14.10/cgi/fDetail?index=2550"
2014-12-03 11:58:22	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.3.7.11.29.0.2	RMON-MIB::eventDescription.75: "I 12/03/14 11:58:22 ports: port 22 is now on-line"
2014-12-03 11:58:19	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.3.7.11.29.0.2	RMON-MIB::eventDescription.76: "I 12/03/14 11:58:20 ports: port 22 is now off-line"
2014-12-03 10:59:20	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.3.7.11.29.0.2	RMON-MIB::eventDescription.412: "I 12/03/14 10:59:19 SNTP: updated time by -4 seconds"
2014-12-03 08:29:10	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.3.7.11.29.0.2	RMON-MIB::eventDescription.75: "I 12/03/14 08:29:13 ports: port 22 is now on-line"
2014-12-03 08:29:08	SNMPTRAP test host (10.10.12.10)	SNMPv2-SMI::enterprises.11.2.3.7.11.29.0.2	RMON-MIB::eventDescription.76: "I 12/03/14 08:29:11 ports: port 22 is now off-line"

Kuvio 9. Trapit-välilehti (Qentinel NetEye 4.1.0 Administrator manual 2013.)

6 VERKONVALVONNAN TOTEUTUS

6.1 Verkonvalvonnan suunnittelu

Verkonvalvonnan suunnittelu on tärkeä vaihe verkonvalvontaprosessia. On paljon mahdollisia hyviä ohjelmistoja, joista pitäisi löytää sopivin yrityksen käyttöön. Ohjelmassa tulee olla kattavat työkalut, jonka lisäksi sen tulee olla yksinkertainen ja helppokäyttöinen sekä kestää kahden organisaation verkkolaitteilta kerätyn datan määrä. Hyvä hinta-laatusuhde on edellytys verkonvalvontaohjelmiston hankinnassa. Omaa panostani suunnittelussa ei tarvittu, koska yhtiöt olivat jo ennen palkkaamistani päättäneet tulevan verkonvalvontajärjestelmän. Minun työni oli käyttöönottaa järjestelmä ja pitää sitä toiminnassa.

Opinnäytetyön käytännön osuus verkonvalvonnasta tehtiin kahdelle yhteistyötä tekevälle organisaatiolle. VSV-konsernin ja Rauman Energia Oy:n verkkolaitteille ja palveluille suunniteltiin yhteinen valvonta, joka kattoi satojen verkkolaitteiden kokoista verkkoa.

Verkonvalvontaohjelmiston käyttöönoton suunnittelussa ensimmäisenä huomioon on otettava kaikkein kriittisimmät valvontakohteet, jotka syötettäisiin ensimmäisenä järjestelmään. Yleensä kaikkein kriittisimpiä palveluita ovat yrityksen palvelimet. Lisäksi on hyvä miettiä valmiiksi mitä valvontatyökalua eri infrastruktuurien valvontaan käytetään. Esimerkiksi verkkolaitteita kannattaa valvoa ICMP Reachability-työkalulla, joka kertoo vastaako laite sekä ICMP Route Quality-työkalulla, joka kertoo verkkoliikenteen kuormituksen. Palvelimien valvonnassa kannattaa käyttää SNMP-pohjaisia työkaluja lisäksi hyväkseen. Näitä ovat esimerkiksi SNMP Memory Usage, SNMP Storage ja SNMP CPU Usage, jotka mittaavat palvelimelta sen muistin ja suorittimen käytön sekä levytilan. (Memonen 2016, 2.)

Verkkolaitteille tulee aluksi luoda hälytysrajat, joita tarvitsee muokata myöhemmin yrityksen liikenteen mukaisiksi. Kun kyse on kahdesta eri yhtiöstä, tulee molempien omat valvontakohteet eritellä verkonvalvontajärjestelmän omaan WWW-käyttöliittymään. Myös kaksi eri hälytysryhmää on luotava, jotta yhtiöt saisivat tiedon pelkästään omien valvontakohteidensa hälytyksistä. Taulukossa 1 on tarkemmin esitetty verkonvalvonnan suunnittelua.

Taulukko 1. Verkonvalvonnan suunnittelu.

Valvontasuunnitelma		
Kriittiset palvelut		
Palvelun yleiskuvaus		
Palvelun toteutus		
Palvelin laitteistojen kuvaus		
Lista palvelun tuottavista laitteista ja niiden tiedot		
	Laitteen rooli	
	IP-osoite	
	Käyttöjärjestelmä	
	Laitealusta	
Infastruktuurin valvonta		
Verkkolaitteet		
	Päälläolo (ICMP reachability)	
	Verkkoliikenteen kuormitus (SNMP Interface)	
Palvelimet		
	Päälläolo (ICMP reachability)	
	Reitin laatu (ICMP route quality)	
	Kapasiteetti valvonta (SNMP)	
		CPU kuorma (CPU Usage)
		Muistin käyttö (Memory Usage)
		Levy (Storage)
		Prosessit ja Windows palvelut
Palvelujen valvonta		
Palvelun saatavuus ja vasteaika (esim ping tai HTTP(S) kysely)		
Palveluporttien saatavuus ja vasteaika (TCP Port Status)		
Peruspalvelut		
	Nimipalvelin (Service DNS)	
	AD-kirjautuminen (Service LDAP)	
	DHCP (Service DHCP)	
	FTP (Service FTP)	
	Levyjaot (SMB)	
	SMTP (Service SMTP)	
Hälytysryhmät ja hälytys viiveet		
Erilliset ryhmät		
	Ryhmän henkilöt	
	Hälytysviive	

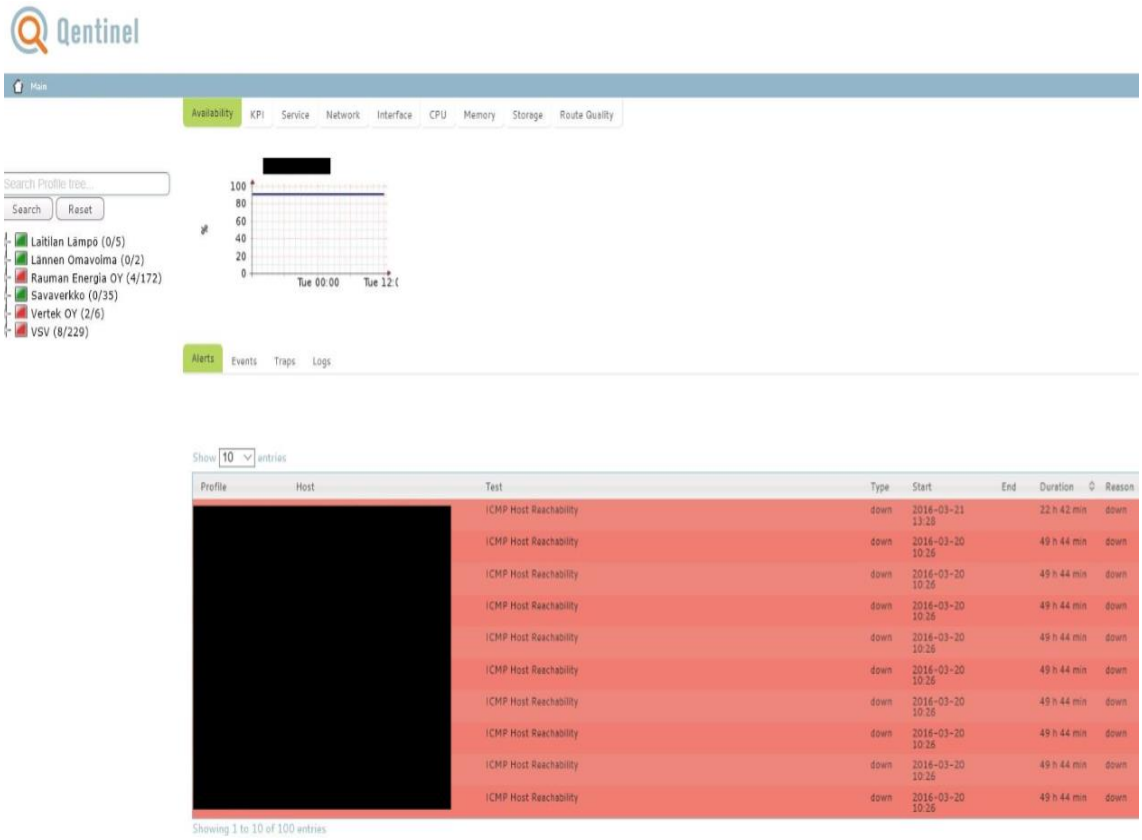
6.2 Järjestelmän käyttöönotto

Niin kuin mikä tahansa muu IT-järjestelmä, myös NetEye tarvitsee toimiakseen fyysisen laitteen, joka pyörittää järjestelmää. Qentinel Oy toimitti Vakka-Suomen Voima Oy:lle NetEyen palvelimen, joka minun tuli asentaa yrityksen tiloihin.

Varsinaisen käyttöönoton ensimmäisenä vaiheena tuli selvittää, mitkä olivat valvonta-kohteet ja mitä tietoa niistä haluttiin saada. Lisäksi tuli selvittää SNMP-protokollaa tukevista verkkolaitteista, että SNMP-kysely on sallittu sekä SNMP-yhteisönimi. Seuraava vaihe oli syöttää IP-osoiteavaruudet NetEyen palvelimeen, jonka jälkeen pystyttiin kytkemään laitteita valvontaan WWW-käyttöliittymässä.

WWW-käyttöliittymän käyttöönotto voitiin aloittaa edellisten toimenpiteiden jälkeen. Käyttöliittymän pääsivun luonti aloitettiin tekemällä jokaiselle yritykselle oma pääprofiili.

Pääprofiilit päädyttiin nimeämään luonnollisesti yritysten nimillä. Kun jokaisella yrityksellä oli oma pääprofiili, voitiin aloittaa aliprofiilien luonti, johon tulivat erikseen esimerkiksi palvelimet ja kytkimet. Kuviossa 10 on esitetty Qentinel NetEyen lopullinen pääsivu. Tietoturvasyistä mustalla palkilla on piilotettu kaikki kriittinen tieto, esimerkiksi IP-osoitteet ja valvontakohteiden nimet.



Kuvio 10. NetEyen lopullinen pääsivu.

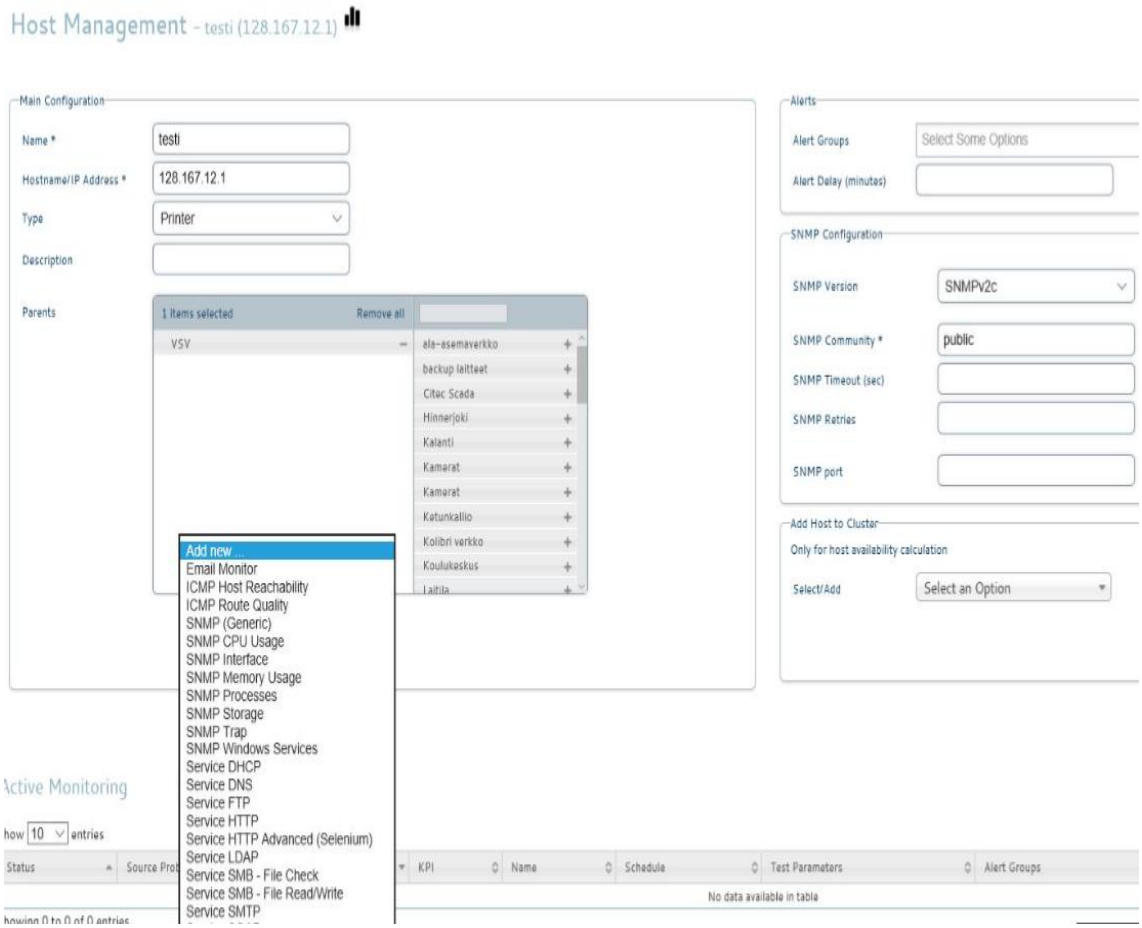
Kuten kuvion 10 alareunan ilmoitusnäkymästä voidaan todeta, on NetEye lähettänyt hälytyksiä eri verkkolaitteista verkonhallinnasta vastaavalle käyttäjälle. Kuviossa on pääsivun ylänäkymässä auki Availability-välilehti, joka kertoo käyttäjälle haluamiensa laitteiden saatavuuden. Lisäksi ylänäkymästä löytyvät myös KPI-, Service-, Network-, Interface-, CPU-, Storage- ja Route Quality-välilehdet. Välilehteä pystyy vaihtamaan painamalla välilehden nimen kohdalta. Kuviossa 11 on esimerkki laitteiden CPU-välilehdestä, joka antaa informaatiota käyttäjälle eri kohteiden suorittimen käytöstä.

Kuvio 11. CPU-välilehti.

Kuten voidaan kuviosta 11 todeta, on käyttäjän helppo yhdellä silmäyksellä nähdä kaikkien tarvittavien valvontakohteiden suorittimen käytöstä saatu informaatio. Tällä yhdellä silmäyksellä saadulla tiedolla verkonhallitsija pystyy tarvittaessa ryhtyä toimenpiteisiin.

6.3 Kohteiden lisäys

Kun valvontaan lisättävät laitteet ja niistä kerättävä informaatio oli selvillä, piti enää syöttää jokainen kohde erikseen järjestelmään. Kohteesta piti tietää laitteen nimi, IP-osoite ja SNMP-versio sekä SNMP-yhteisönimi. Tämän jälkeen laitteen lisäys NetEyen WWW-käyttöliittymässä oli mahdollista. Laitteen lisäykseen pääsee etusivun puunäkymästä klikkaamalla hiiren oikealla näppäimellä jotakin profiilia, ja valitsee kohdan ”Add host”. Add host-sivussa kohteelle syötetään nimi, IP-osoite, tyyppi, kuvaus kohteesta, SNMP-versio sekä SNMP-yhteisönimi. Halutessaan voi myös asettaa yksittäiselle laitteelle hälytysryhmän erikseen kohdasta Alert Groups. Kuviossa 12 on esitetty laitteen lisäyksen Add host-sivu.

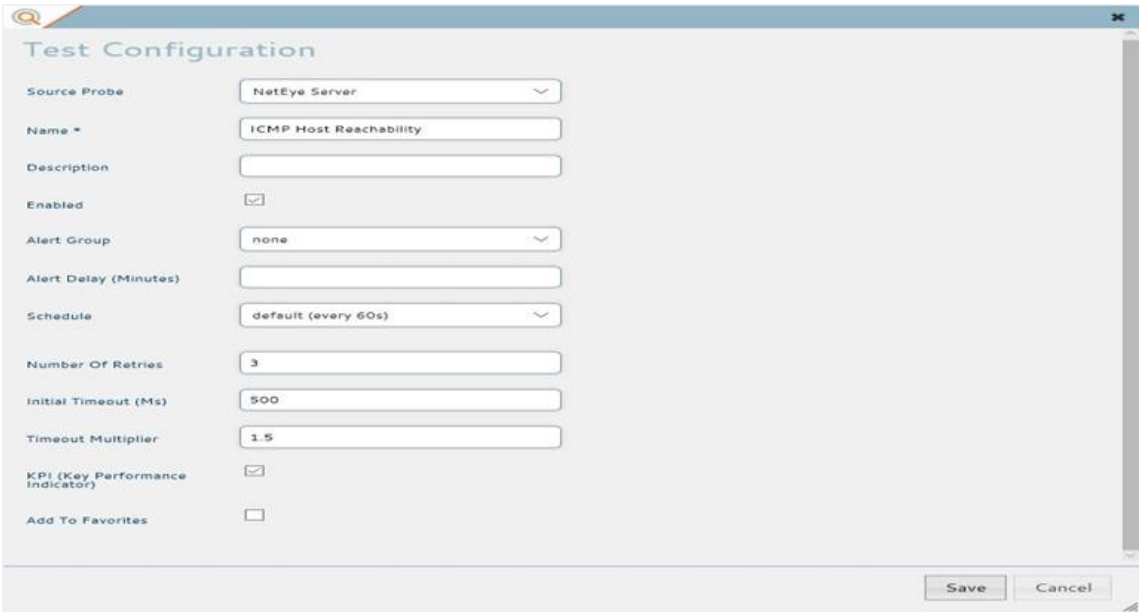


Kuvio 12. Add Host-sivu

Kun kohde on lisätty onnistuneesti järjestelmään, sille pitää luoda testejä, jotka keräävät varsinaista informaatiota. Testin pystyy luomaan kohteen alla olevasta pudotusvalikosta. Testejä on yhteensä 27, joista voi valita sopivan työkalun kohteen valvomiseen.

6.3.1 ICMP-testit

Opinnäytetyön käytännön osuudessa yleisimmät testit olivat ICMP Reachability ja Route Quality, joita käytettiin jokaisen kohteen valvonnassa. Kuviossa 13 on esimerkki ICMP Reachability-testin luomisesta.



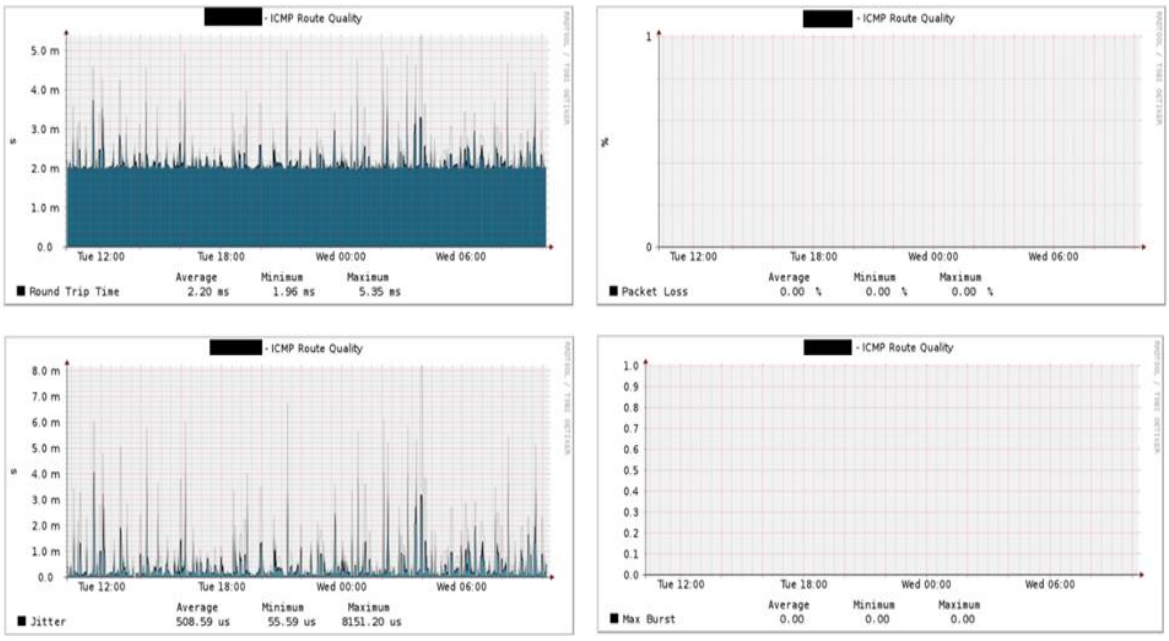
Kuvio 13. ICMP Reachability-testi

Testi kertoo käyttäjälle vastaako laite ICMP kyselyyn. ICMP Reachability-testissä kohteelle voidaan määrittää seuraavat asetukset:

- Source Probe, joka lähettää ICMP kyselyn kohteelle
- Name, joka on testin nimi
- Description, jossa voi täsmentää muille käyttäjille, mitä testi tekee
- Enable, josta testi kytketään aktiiviseksi
- Alert Group, jossa voi määrittää halutessaan hälytysryhmän, joka vastaanottaa vain ICMP Reachability hälytykset
- Alert Delay, jossa määritetään hälytyksen viive
- Schedule, jossa määritetään kuinka usein järjestelmä lähettää ICMP kyselyn kohteelle
- Number of retries, jossa määritetään kuinka monta uudelleenyritystä kohteelle lähetetään
- Initial timeout, jossa määritetään ICMP kyselyjen välinen aika millisekunteina. Voidaan valita 10 – 60 000 millisekunnin väliltä
- Timeout multiplier, jota käytetään laajentamaan ICMP kyselyjen välistä aikaa
- KPI, joka voidaan merkitä ruksilla, jos testin saatavuus halutaan etusivulle näkyville

- Add to favorites, jossa voi testin merkitä Favorites välilehdellä näkyväksi lempikohteeksi.

ICMP Route Quality oli toinen ICMP-testi, jota tämän opinnäytetyön käytännön osuudessa käytettiin. Testi antaa käyttäjälle laajempaa informaatiota kuin ICMP Reachability-testi. Se kertoo valitun kohteen prosentuaalisen paketti-hävikin (Packet Loss), latenssin (Round Trip Time) ja viiveen vaihtelun (Jitter). Kuviossa 14 on esitetty esimerkki kytkimen kuvaimista.



Kuvio 14. Kytkimen kuvaimet.

Kuten voidaan edellä olevasta kuviosta 14 huomata, kaikki paketit ovat löytäneet määränpään ja palanneet takaisin hallinta-asemalle. Tästä voidaan todeta, että kytkin toimii niin kuin pitääkin eikä järjestelmä lähetetä hälytyksiä.

6.3.2 SNMP-testit

ICMP-testien lisäksi SNMP-protokollaa tukeviin laitteisiin lisättiin SNMP-testejä. SNMP-testejä on järjestelmässä kahdeksan erilaista. Nämä testit ovat seuraavat:

- SNMP (Generic), jossa pystyy manuaalisesti määrittämään laitteen SNMP OID:n, jota halutaan valvoa

- SNMP CPU Usage, joka kertoo suorittimen prosentuaalisen käytön
- SNMP Interface, joka kertoo liikenteen määrän haluamassa verkkorajapinnassa
- SNMP Memory Usage, joka kertoo muistin prosentuaalisen käytön
- SNMP Processes, joka kertoo eri prosessien liikenteestä
- SNMP Trap, kertoo käyttäjälle mahdollisista toimintahäiriöistä liikenteessä.
- SNMP Windows Services, joka kertoo liikenteen Windowsin palveluista.

Yleisimmät SNMP-testit tässä opinnäytetyössä olivat SNMP CPU Usage, SNMP Interface, SNMP Memory Usage ja SNMP Storage. Kaikkia edellä mainittuja testejä käytettiin jokaisessa valvontaan lisätyssä palvelimessa. Jokaiseen SNMP-testiin tulee syöttää SNMP-versio ja SNMP-yhteisönimi. Kuviossa 15 on esimerkki palvelimen X SNMP-testien antamasta informaatiosta.

Kuvio 15. SNMP-testien antamat informaatiot.

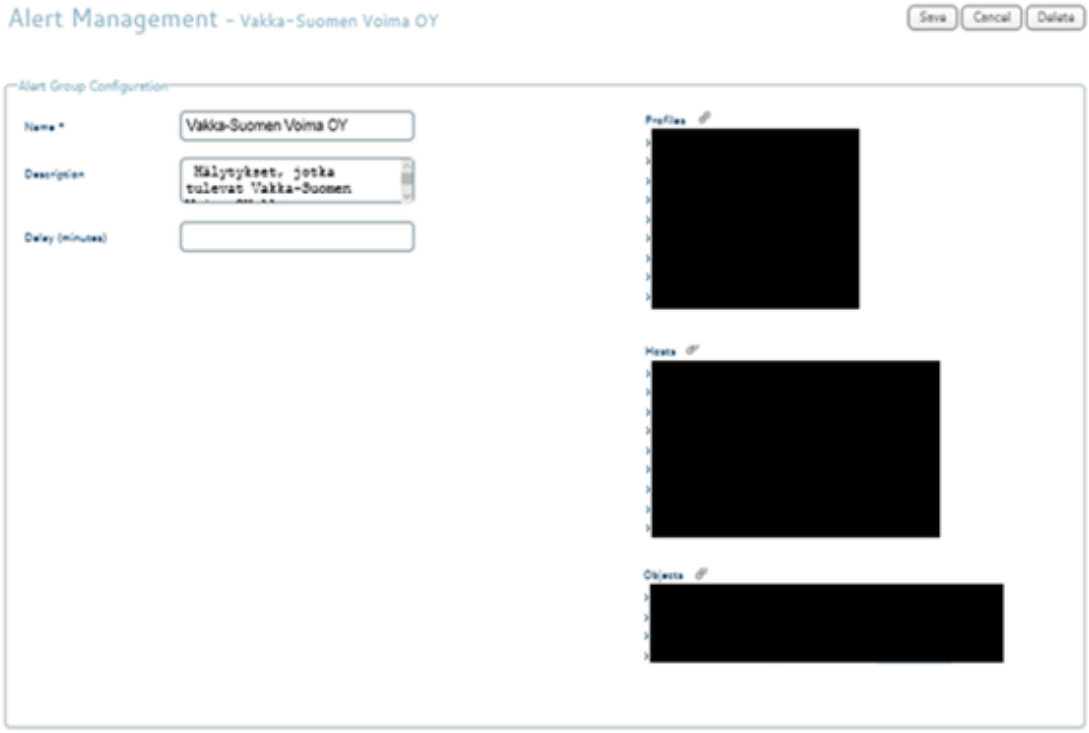
Kuten voidaan punaisesta viivasta todeta, sen suorittimen käytölle ja levytilan täyttymiselle on asetettu hälytysraja 95 %:iin. Mikäli palvelin käyttää siis suoritinta enemmän kuin 95 % tai, jos levytilaa on vähemmän kuin 5 % vapaana, lähtee siitä hälytys verkonhallitsijalle sähköpostiin, ja hän tietää ryhtyä tarvittaviin toimenpiteisiin.

6.3.3 Hälytykset

Kun kyse on kahdesta eri yhtiöstä on selvää, että molempien organisaatioiden omat verkonhallitsijat haluavat saada hälytyksiä vain omista valvontakohteistaan. Tämä onnistuu luomalla WWW-käyttöliittymästä kummallekin omat hälytysryhmänsä. Ennen hälytysryhmän luomista on luotava jokaiselle järjestelmän käyttäjälle oma profiili.

Profiili sisältää käyttäjän oman kirjautumisnimen ja salasanan, joilla kirjautuu järjestelmään. Tämän lisäksi asetuksiin tulee määrittää käyttäjän sähköpostiosoite, jonne halutut hälytykset järjestelmästä lähtevät.

Hälytysryhmän luonnissa tulee tietää, kuka verkonhallitsijoista saa minkäkin valvontakohteen hälytyksen. Jos esimerkiksi kaikki verkonhallitsijat voivat saada kaikki hälytykset, ei tarvitse luoda kuin yksi hälytysryhmä. Kuviossa 16 on esimerkki hälytysryhmästä.



Kuvio 16. Hälytysryhmänäkymä.

Hälytysryhmästä pystyy määrittämään muun muassa sen, minä päivinä hälytyksiä lähetetään ryhmän jäsenille. Esimerkiksi kesäloman ajaksi pystyy kytkemään jäsenen OFF-tilaan, jolloin hän ei saa hälytyksiä määriteltynä ajankohtana.

Kuten voidaan todeta kuviosta 16, hälytysryhmässä näkyy kaikki hälytysryhmään kuuluvat objektit, isännät ja profiilit. Nämä ovat sensuroituna kuviossa mustalla palkilla tietoturvasyistä. Kohdassa description on selvennetty käyttäjälle, mitä laitteita kyseiseen hälytysryhmään kuuluu.

7 POHDINTA

Opinnäytetyön tavoitteena oli käyttöönottaa Qentinel NetEye 4.1.0 verkonvalvontajärjestelmä VSV-konsernille ja Rauman Energia Oy:lle. Toimeksiantajan vanhan ohjelmiston tilalle tarvittiin laajempi ja monipuolisempi verkonvalvontajärjestelmä, joka antoi aikaisempaa enemmän informaatiota valvottavista kohteista. Valvottavia kohteita oli aluksi yli tuhat, joista karsittiin pois noin puolet, koska NetEye-palvelin kuormittui liikaa ja se lähetti hälytyksiä laitteista, joista hälytyksiä ei koettu tarvitsevan.

Verkonvalvonnasta ja protokollien toiminnasta sekä itse järjestelmästä NetEye piti hankkia tietoa ennen järjestelmän käyttöönottoa. Kävin läpi verkonvalvontaa käsitteleviä opinnäytetöitä, englanninkielisiä artikkeleita ja Wikipedia-sivuja perehtyessäni aiheeseen, johon en ollut aiemmin tarkemmin tutustunut. Tämä pohjatyö auttoi minua ymmärtämään, mitä olin tekemässä.

Seuraavana vaiheena oli tutustuminen järjestelmään. Qentinel Oy oli sopinut yhdessä Vakka-Suomen Voima Oy:n sekä Rauman Energia Oy:n kanssa, että menisin kahdeksi päiväksi Qentinel Oy:n konttorille opettelemaan järjestelmän käyttöä ja ylläpitoa. Koulutuksessa kävimme läpi aivan kaiken, mitä järjestelmällä voitiin tehdä. Sain heiltä erittäin hyvän koulutuksen, jonka jälkeen pystyin omin päin käyttöönottamaan järjestelmän sekä ylläpitämään sitä. Koulutuksen lisäksi NetEyen käyttäjän opas oli apuna ottaessani järjestelmää käyttöön.

Kun verkonvalvonta termi ei enää ollut pelkkää utopiaa minulle sekä tiesin mikä NetEye on ja kuinka käyttää sitä, niin voitiin aloittaa verkonvalvonnan suunnittelu. Kävimme toimeksiantajan kanssa läpi, mitä kohteita valvontaan määritetään. Sain IP-osoite listan, jossa oli kaikki tarvittavat tiedot valvontakohteista. Kun valvontakohteet olivat tiedossa, tuli päättää mitä työkalua niiden valvonnassa käytettäisiin, ja minkälaiset hälytysrajat näille määritettäisiin. Päädyimme valitsemaan jokaiseen valvontakohteeseen ICMP Reachability- ja ICMP Route Quality-testit, jonka lisäksi palvelimille ja kytkimille SNMP-pohjaiset työkalut.

Tämän jälkeen alkoi varsinainen käyttöönotto vaihe. Valvottavien kohteiden lisääminen järjestelmään oli melko mekaanista suorittamista, jossa ei juurikaan ongelmia ilmennyt. Valvottavasta kohteesta lisättiin järjestelmään vain sen nimi, IP-osoite, kuvaus ja mahdollinen SNMP-versio ja yhteisönimi, jonka jälkeen NetEye-palvelin lähti keräämää tietoa

kohteesta. Kun NetEye oli kerännyt informaatiota valvottavista kohteista muutaman viikon ajalta, voitiin hälytysrajoja muokata toimeksiantajalle sopivammiksi.

Ongelmia työssä ei juurikaan ilmennyt, mutta jokaisessa työssä on aina jotakin korjattavaa. Mielestäni aikaa säästääkseen tässä työssä olisi voinut asettaa hälytysrajat vasta silloin, kun NetEye-palvelin oli jo hieman kerännyt informaatiota valvontakohteiden liikenteestä. Lisäksi alkuun lisätyt ICMP Route Quality-testin hälytysrajat olisi voinut jättää asettamatta kokonaan, koska se lähetti eniten turhia hälytyksiä.

Kokonaisuutena voi sanoa opinnäytetyön olleen onnistunut. Järjestelmä saatiin onnistuneesti käyttöönotettua. NetEye kerää nyt toimeksiantajalle aikaisempaa verkonvalvontaohjelmistoa enemmän informaatiota valvontakohteista sekä hälyttää verkonhallitsijaa tarvittaessa. Henkilökohtaisesti sain opinnäytetyöstä valtavasti lisätietoa verkoista ja niiden toiminnasta sekä itse verkonvalvonnasta. Tästä on hyvä lähteä jatkamaan ja jalostamaan oppia verkkojen parissa.

LÄHTEET

Anttila, A. 2000. TCP/IP-tekniikka. Helsinki: Helsinki Media.

Cisco 2016a. SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches). Viitattu 3.5.2016. http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-inf-req-review.html.

Cisco 2016b. SNMPv2c. Viitattu 3.5.2016 https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv2c.pdf.

Cisco 2016c. SNMP version 3. Viitattu 13.2.2016. http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html.

Cisco 2016. Network Management Basics. http://docwiki.cisco.com/wiki/Network_Management_Basics#Figure:_A_Typical.

Cinia Group Oy 2016. Kriittisten tietoliikenneverkkojen valvonta paranee, Qentinel ja Corenet yhteistyöhön. Viitattu 7.4.2016 http://cinia.fi/fi/ajankohtaista/kriittisten-tietoliikenneverkkojen-valvonta-paranee-qentinel-ja-corenet-yhteisty%C3%B6h%C3%B6n.

Haikonen, J., Hlinovsky, J. & Paju, A. 2000. Verkonhallinta. Viitattu 22.4.2016 http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/47/.

Hautaniemi, M. 1994. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. Diplomityö. Aalto-yliopiston teknillinen korkeakoulu, Tietotekniikan osasto. Viitattu 22.4.2016. http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/thesis.html.

Held, G. 2003. Ethernet networks: Design, Implementation, Operation and Management. 4th Edition Chichester: Wiley, cop.

Jaakohuhta, H. 2005. Lähiverkot – Ethernet: ethernet-tekniikan soveltaminen käytännössä. Helsinki: IT Press. Viitattu 6.2.2016.

Keogh, J. 2001. Verkkotekniikat – tehokas hallinta. Helsinki: Edita. Viitattu 17.2.2016.

Lummevaara, V. 2008. SNMP V3 Verkonhallinta & Cisco Works. Viitattu 19.2.2016. https://www.theseus.fi/bitstream/handle/10024/740/Lummevaara%20Vesa.pdf?sequence=1.

Memonen, M. 2014. Parhaat käytönnät - Verkonvalvonta. Viitattu 26.2.2016. https://info.funet.fi/wiki/download/attachments/28410624/BCP-AF-Verkonvalvonta-FINAL-2011-05.pdf?api=v2.

Microsoft. 2016. Internet Control Message Protocol (ICMP) Basics. Viitattu 3.5.2016. https://support.microsoft.com/en-us/kb/170292

Miller, M. 2009. Manage Your Network by Working Smarter. Viitattu 3.5.2016. http://www.enterprisenetworkingplanet.com/netsysm/article.php/3815311/Manage-Your-Network-by-Working-Smarter.htm

Nash, K. & Behr, A. 2007. Netwok Monitoring Definition and Solutions. Viitattu 15.2.2016. http://www.cio.com/article/2438133/networking/network-monitoring-definition-and-solutions.html.

Net-SNMP. 2016. FAQ: General 13. Viitattu 3.5.2016. http://www.net-snmp.org/wiki/index.php/FAQ:General_13

Puska, M. 2000. Lähiverkkojen tekniikka. 2, uudistettu painos. Jyväskylä: Gummerus Kirjapaino Oy. Viitattu 15.2.2016.

Ogletree, T; Muellerin, S; & Ilkka, J. Verkot. 2001. Helsinki: IT Press.

Qentinel Oy 2016. Qentinel NetEye- Näkyvyyttä ICT-palveluihin. Viitattu 2.3.2016. http://www.qentinel.com/fi/qentinel-neteye-naekyvyyttae-ict-palveluihin.

Qentinel NetEye 4.1.0 Administrator manual. 2013.

Rauman Energia Oy. 2016. Rauman Energia Oy. Viitattu 19.3.2016. http://www.raumanenergia.fi/yritys/reo/fi_FI/index/.

Suunnittelutoimisto Enertel Oy. 2016. Yrtitys. Viitattu 22.4.2016. http://www.enertel.fi/yritys.php.

TCP/IP Guide. 2016. SNMP Version 2 (SNMPv2) Message Formats. Viitattu 3.5.2016. http://www.tcpipguide.com/free/t_SNMPVersion2SNMPv2MessageFormats.htm.

Vakka-Suomen Voima Oy. 2016. VSV-konserni. Viitattu 19.3.2016. http://www.vsv.fi/yritys/fi_FI/vsv-konserni/.

Wikipedia. 2016a. FCAPS. Viitattu 3.5.2016. https://en.wikipedia.org/wiki/FCAPS.

Wikipedia. 2016b. Internet Control Message Protocol. Viitattu 22.4.2016. https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol