jamk.fi

ExtremeAnalyticsin käyttöönotto ESSOTEssa

Antti Lauttaanaho

Opinnäytetyö
Marraskuu 2019
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Lauttaanaho, Antti	Opinnäytetyö, AMK	01.10.2019
	Sivumäärä	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
ExtremeAnalyticsin käyttöönotto ESSOTEssa

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Mika Rantonen, Karo Saharinen

Toimeksiantaja(t)
Etelä-Savon sosiaali- ja terveyspalvelut ESSOTE

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi Etelä-Savon sosiaali- ja terveyspalvelut ESSOTE. Opinnäytetyön tavoitteena oli käyttöönottaa yrityksen hankkima verkkoliikenteen analysointilaite ExtremeAnalytics. Käyttöönottoon liittyi laitteelle tehtävät konfiguraatiot, kuten verkkoalueisiin perustuvien lokaatioiden luonti, sovellusten ja palvelinten raporttinäkymät ja verkkoliikenteen raja-arvoihin perustuvat hälytykset.

Opinnäytetyön teoriaosuudessa käsitellään verkkoliikenteen monitorointia ja analysointia yleisesti sekä verkkoliikenteen analysointiin käytettyjä protokollia. Lisäksi teoriaosuudessa käsitellään OSI-mallin rakenne ja esitellään ExtremeAnalytics-laite toimintaperiaatteineen.

Opinnäytetyön toteutusvaiheessa selvitettiin aluksi toimeksiantajan kriittiset palvelut, jonka jälkeen pystyttiin luomaan tarvitut lokaatiot ja suunnittelemaan palvelukohtaiset raporttinäkymät. Lisäksi laitteelle luotiin sovellusten ja verkon vasteaikoihin perustuvia hälytyksiä sekä kartoitettiin potilastietojärjestelmä Effican vasteaikojen normaalitilanne.

Lopputulokseksi saatiin luotua toimeksiantajan haluamat raporttinäkymät kriittisistä palveluista ja selvitettyä potilastietojärjestelmä ProConsonaan liittynyt ongelmatilanne. Lisäksi kartoitettiin opinnäytetyöprojektin aikana havaittuja puutteita ExtremeAnalytics-laitteen käyttöliittymässä.

Avainsanat (asiasanat)
DPI, OSI-malli, verkkoliikenteen analysointi, ExtremeAnalytics

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Lauttaanaho, Antti	Bachelor's thesis	01.10.2019
		Language of publication: Finnish
	Number of pages	Permission for web publication: x

Title of publication

The deployment of ExtremeAnalytics in ESSOTE

Degree programme

Information and Communication Technology

Supervisor(s)

Rantonen, Mika, Saharinen, Karo

Assigned by

The South Savo Social and Health Care Authority (ESSOTE)

Abstract

The bachelor's thesis was assigned by the South Savo Social and Health Care Authority (ESSOTE). The purpose of the thesis was to deploy the network traffic analysis equipment ExtremeAnalytics the company had acquired. The deployment included device configurations such as a domain-based location creation, application and server report views, and alarms based on network traffic threshold values.

The theoretical part of the thesis deals with monitoring and analyzing in general and the protocols used for analyzing network traffic. In addition, the theory section discusses the structure of the OSI model and the ExtremeAnalytics device with its operation principles is presented.

In the thesis implementation phase, the assigner's critical services were first identified, after which it was possible to create the necessary locations and design service-specified report views. Additionally, application and network response time alarms were created for the device and the normal situation of the Effica patient information system was mapped.

As a result, the report views on critical services requested by the assigner were created and the problem with the ProConsona patient information system was resolved. In addition, shortcomings in the ExtremeAnalytics UI were identified during the thesis project.

Keywords/tags (subjects)

DPI, OSI-model, network traffic analysis, ExtremeAnalytics

Miscellaneous

Sisältö

Kuviot

Taulukot

Lyhenteet

AD	Active Directory
DPI	Deep Packet Inspection
ESSOTE	Etelä-Savon Sosiaali- ja Terveyspalvelut
IP	Internet Protocol
ICMP	Internet Control Message Protocol
MIB	Management Informartion Base
MPI	Medium Packet Inspection
OID	Object Identifier
OSI	Open Systems Interconnection
SNMP	Simply Network Management Protocol
SPI	Shallow Packet Inspection

1 Työn lähtökohdat

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi Etelä-Savon Sosiaali- ja Terveyspalvelut (ESSOTE), joka tarjoaa terveys- ja sosiaalipalveluita yli 100 000 asukkaalle Etelä-Savon alueella. ESSOTEn henkilöstöön kuului vuoden 2018 lopussa yli 3700 työntekijää ja sen liikevaihto oli n. 370 miljoonaa euroa, minkä ansiosta Mikkelin keskussairaala oli maan tuottavin sairaala kyseisenä vuonna, kun otetaan huomioon kaikki muu, paitsi psykiatrinen erikoissairaanhoito. (Tilinpäätös ja toimintakertomus 2018) ESSOTEn jäsenkuntiin kuuluvat Mikkelin lisäksi Hirvensalmi, Juva, Kangasniemi, Mäntyharju, Pertunmaa ja Puumala. (Ks. Kuvio 1.) Lisäksi erikoissairaanhoidon kautta ESSOTEen kuuluvat Joroinen ja Pieksämäki.

Kuvio 1. ESSOTEn jäsenkunnat (Jäsenkunnat 2016)

1.2 Tavoitteet

Opinnäytetyön tavoitteena oli käyttöönottaa ExtremeAnalytics -laite ESSOTEn verkossa ja hyödyntää sitä verkon ja sovellusten viiveiden analysointiin. Käyttöönottoon liittyi laitteella tehtävät konfiguroinnit, kuten mallipohjat ja valmiit analysointinäkymät. Tavoitteena oli saada laite niin hyvin käyttöön, että sitä pystyttiin käyttämään helposti ja vaivattomasti jokapäiväisessä työssä liittyen verkon valvontaan ja viiveiden analysointiin. Tavoitteena oli myös tutustua laitteen tarjoamiin mahdollisuuksiin luoda hälytyksiä ja käyttöön ottaa niitä. Lisäksi tavoitteena oli määrittää jonkin sovelluksen niin sanottu lähtökohta sovelluksen vasteajoille, jotta pystyttiin näkemään nopeasti, onko nykyinen verkkoliikenne normaalia vai epänormaalia.

1.3 Tutkimusmenetelmät

Opinnäytetyön toteutusosioon käytetty aineisto hankittiin pääsääntöisesti työskentelemällä työssä käytetyn laitteen parissa. Lisäksi toteutusosion aineistoa hankittiin toimeksiantajalta sekä paneutumalla ympäristössä käytettyihin sovelluksiin huolella. Teoriaosuuteen liittyvät aineistot hankittiin toimeksiantajalta, laitteen toimittajalta ja verkosta löydetyistä materiaaleista. Aineiston analysointiin pyrittiin käyttämään jo olemassa olevaa tietämystä aiheeseen liittyen sekä tarpeeksi laajaa katselmointia tutkittavaan asiaan.

2 OSI-malli

OSI-malli (Open Systems Interconnection) on ISOn (International Organization for Standardization) standardi numero ISO/IEC 7498-1, joka on julkaistu ensimmäisen kerran vuonna 1984, mutta sai nykyisen muotonsa vuonna 1994. (ISO/IEC 7498-1 1994). OSI-malli antaa käsityksen seitsemällä eri kerroksella siitä, miten eri protokollat pystyvät keskustelemaan toistensa kanssa. (Ks. Kuvio 2.)

Kuvio 2. OSI-malli

Fyysinen kerros sisältää datan kuljettamiseen tarkoitetut fyysiset laitteet, kuten kaapelit, kuidut ja kytkimet. Tällä tasolla data kulkee bitteinä, joten signaalista molempien päätelaitteiden täytyy erottaa, onko kyseessä yksi vai nolla. (What Is The OSI Model? n.d.)

Siirtokerros huolehtii saman verkon datan kuljetuksesta ja muuntaa fyysiseltä kerrokselta saadut bitit kehyksiksi (engl. frame). Siirtokerroksen tehtäviin kuuluu vastata verkon vuon- ja vianhallinnasta sekä ylläpitää fyysisesti kiinni toisissaan olevien laitteiden, kuten kytkimien, yhteyksiä. (What Is The OSI Model? n.d.)

Verkkokerroksen tehtävä on siirtää dataa kahden eri verkon välillä ja reitittää eli etsiä paras mahdollinen fyysinen reitti datan kuljettamiseen. Verkkokerros pilkkoo kuljetuskerrokselta saadut segmentit paketeiksi lähettäjän laitteessa ja kokoaa ne takaisin kokonaisuuksiksi vastaanottajan päässä. Verkkokerroksen laitteistoon kuuluvat reitittimet ja tason 3 kytkimet ja protokollat, kuten IPv4 ja IPv6. (What Is The OSI Model? n.d.)

Kuljetuskerros vastaa päästä päähän kahden laitteen kommunikoinnista. Kuljetuskerros ottaa datansa istuntokerrokselta ja pilkkoo ne osiin, segmenteiksi, ennen kuin ne lähetetään verkkokerrokselle. Vastaanottajan päässä kuljetuskerros taas kokoaa segmentit dataksi, jota istuntokerros ymmärtää. Kuljetuskerroksen tehtäviin kuuluu vian- ja vuonhallinta; se tarkistaa paketit vioilta ja kahdentumiselta (engl. duplication) ja tarvittaessa lähettää paketteja uudelleen, jos lähetys epäonnistuu. Yleisimmät kuljetuskerroksen protokollat ovat yhteydellinen TCP (Transmission Control Protocol) ja yhteydetön UDP (User Datagram Protocol). (What Is The OSI Model? n.d.)

Istuntokerroksen tehtävä on pitää kahden laitteen välinen istunto käynnissä. Istunnoksi kutsutaan sitä aikaväliä, kun osapuolten välinen yhteydenpito on käynnissä. Istuntokerron pitää huolen siitä, että istunto pysyy avoimena tarpeeksi pitkään, jotta kaikki datatieto saadaan vaihdettua. Tämän jälkeen istunto voidaan panna kiinni, jotta resursseja ei tuhlata. (What Is The OSI Model? n.d.)

Esityskerros valmistelee datan sellaiseksi, että sovelluskerros voi käyttää sitä. Esityskerros kääntää, salaa ja pakkaa datan. Koska toistensa kanssa kommunikoivat laitteet saattavat käyttää erilaisia koodaustekniikoita, on esityskerros välttämätön näiden välissä. (What Is The OSI Model? n.d.)

Sovelluskerros keskustelee suoraan loppukäyttäjän kanssa. Sovelluskerroksen sovelluksia ovat esimerkiksi verkkoselaimet ja sähköpostisovellukset, ja se sisältää näin ollen protokollia, kuten HTTP (Hypertext Transfer Protocol) ja SMTP (Simple Mail Transfer Protocol). Lisäksi sovelluskerros huolehtii autentikoinnista, yksityisyydestä ja palvelujen laadusta. (Raza 2018.)

3 Verkon analysointi

3.1 Liikenteen monitorointi

3.1.1 Yleisesti

Verkkoliikenteen monitoroinnilla tarkoitetaan verkonvalvontaa, jolla saadaan tieto siitä, kuka käyttää verkkoa, millä laitteilla verkkoa käytetään ja kuinka paljon liikennettä verkossa liikkuu. Monitoroinnilla pyritään löytämään epäkohtia verkkoliikenteestä, minkä seurauksena verkon suorituskyky, saatavuus tai turvallisuus voi kärsiä. Verkkoliikenteen monitorointi on todella helppo ja erittäin hyödyllinen tapa yrityksille valvoa jokapäiväistä verkkonsa käyttöä, koska nykyään on tarjolla yksinkertaisia ja helppokäyttöisiä, niin maksuttomia kuin maksullisiakin verkkoliikenteen monitorointiratkaisuja. Monitoroinnilla saadut tulokset, esimerkiksi verkosta löytyneen pullonkaulan korjaus, voi tapahtua todella nopeasti, jolloin monitorointia voidaan ajatella bisneskriittisestä näkökulmasta. Sijoituksella jonkinlaiseen monitorointivaihtoehtoon voidaan siis saada hyviä tuloksia pienessä ajassa, jolloin yrityksen liiketoiminta kiittää.

3.1.2 Vasteaika

Vasteajalla tarkoitetaan aikaväliä, jolloin tehtävä aloitetaan ja lopetetaan. Voidaan esimerkiksi ajatella, että työaseman käyttäjä menee jollekin verkkosivustolle, jolloin aloitus tapahtuu, kun verkkosivustoa aletaan ladata, ja lopetus silloin, kun verkkosivusto on ladattu. Vasteajat vaihtelevat paljon riippuen monista eri tekijöistä, kuten verkon viiveestä, verkkosivun koosta ja verkkopalvelimen kuormituksesta. Tekijöiden tilat voivat muuttua, mikä aiheuttaa vasteajan vaihtelun, vaikka suoritettava toiminto pysyisikin aina samana. (Response time (Networking) n.d.)

3.1.3 Hälytykset

Verkkoliikenteen hälytyksillä tarkoitetaan ilmoituksia, jolloin jokin ennalta määritetty laukaisin (eng. trigger) on saavutettu. Hälytykset ovat hyödyllisiä, kun halutaan tietää esimerkiksi jonkin tietyn palvelimen muistin kuormitusta tai palvelimen lämpötilaa. Toisaalta hälytyksiä voidaan myös asettaa verkkoliikenteeseen, jolloin esimerkiksi

tietyn sovelluksen vasteajat ovat saavuttaneet tietyn raja-arvon. Hälytysten tyypit voidaan esimerkiksi määritellä kriittisiin, virheisiin, varoituksiin ja muihin ilmoituksiin.

3.2 Verkon monitorointi

3.2.1 Yleisesti

Verkon monitoroinnilla tarkoitetaan apuvälinettä (laite/sovellus), jolla pystytään saamaan tietoa verkossa olevien laitteiden ja palveluiden tilasta. Verkon monitorointi mahdollistaa kriittisten laitteiden, kuten palvelimien, palomuurien, reitittimien ja kytkimien reaaliaikaisen tarkastelun ja ilmoittaa, jos niiden saatavuudessa tai suorituskyvyssä on poikkeamia. Verkon monitoroinnilla saadaan esimerkiksi nopeasti selvitettyä verkossa oleva pullonkaula. (Mitchell 2019.)

3.2.2 Ping

Ping on yksi perinteisistä verkon monitorointi työkaluista. Ping-testissä lähetetään ICMP (Internet Control Message Protocol) echo request -paketti kohdeosoitteeseen. Jos kohde on saatavilla, se vastaa ICMP echo reply -paketilla. Ping-työkalu löytyy lähes jokaisesta tietokoneesta. Kuviossa 3 on tehty ping-testi google.com -sivustolle. (Mitchell 2019.)

```
C:\Users\Annero>ping google.com

Pinging google.com [2a00:1450:400f:807::200e] with 32 bytes of data:
Reply from 2a00:1450:400f:807::200e: time=18ms
Reply from 2a00:1450:400f:807::200e: time=18ms
Reply from 2a00:1450:400f:807::200e: time=18ms
Reply from 2a00:1450:400f:807::200e: time=18ms

Ping statistics for 2a00:1450:400f:807::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 18ms, Average = 18ms
```

Kuvio 3. Ping-testi

3.2.3 SNMP

SNMP eli Simply Network Management Protocol on yksi tunnetuimmista ja käytetyimmistä verkon monitorointi protokollista. SNMP:sta on useita versiota, joista

ensimmäinen julkaistiin vuonna 1988. Nykyään yleisin käytetty versio on SNMPv3 sen tietoturvallisuuden vuoksi. SNMP:lla voidaan jakaa tietoa verkkolaitteiden kesken, vaikka laitteet olisivat erilaisia. (Oros 2016.)

SNMP:n arkkitehtuuri on yksinkertainen client-server malli. Serverit (managerit) ovat verkossa olevien laitteiden tietojen kerääjiä. Clientit (agents) ovat puolestaan mitä tahansa verkossa olevia laitteita, kuten tietokoneita, kytkimiä, reitittimiä, puhelimia ja tulostimia. Kun manageri kysyy agentilta tietoja, agentti katsoo vastauksen Management Informartion Basesta eli MIB:sta. MIB:ssa on lista arvoja, niin staattisia kuin muuttuvia. MIB kertoo vastauksensa OID:na eli Object Identifierina. Jokaisella komponentilla on oma OID:nsa ja OID voi olla joko skalaari tai taulukoitu. Skalaari on yksittäinen instanssi, kuten esimerkiksi laitteen valmistaja. Taulukoidulla tarkoitetaan OID:ta, jolla voi olla monta arvoa, kuten neliytiminen prosessori voi antaa neljä erilaista vastausta. (Parker 2016.)

3.3 Liikenteen perusarvojen laskeminen

Verkkoliikennettä analysoitaessa saadaan esille erilaisia diagrammeja, jotka perustuvat analysoitavaan dataan. Saaduista tuloksista voidaan laskea erilaisia arvoja, kuten (aritmeettinen)keskiarvo, keskihajonta ja varianssi. Näitä lukuja laskemalla saadaan tietoa siitä, minkälaiset vasteajat verkkoliikenteessä ovat normaaleja sillä hetkellä.

Keskiarvo lasketaan kaavalla (1), jossa x on mitattu arvo ja n on arvojen lukumäärä.

$$Ka = \frac{x_1+x_2+\cdots+x_n}{n} \quad (1)$$

Keskihajonta kertoo, kuinka paljon mitatut arvot poikkeavat keskimäärin keskiarvosta. Keskihajonta lasketaan kaavalla (2), jossa n on arvojen lukumäärä, x_i on mitattu arvo ja $\bar{x}$ on tulosten keskiarvo.

$$S = \sqrt{\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n}} \quad (2)$$

Varianssi on keskihajonnan neliö, joka kuvaa tulosten jakautuneisuutta keskiarvon ympäristöön. Varianssin ollessa suuri poikkeavat arvot paljon keskiarvosta, ja kun taas varianssi on pieni, poikkeamat keskiarvosta ovat pieniä. Varianssi lasketaan

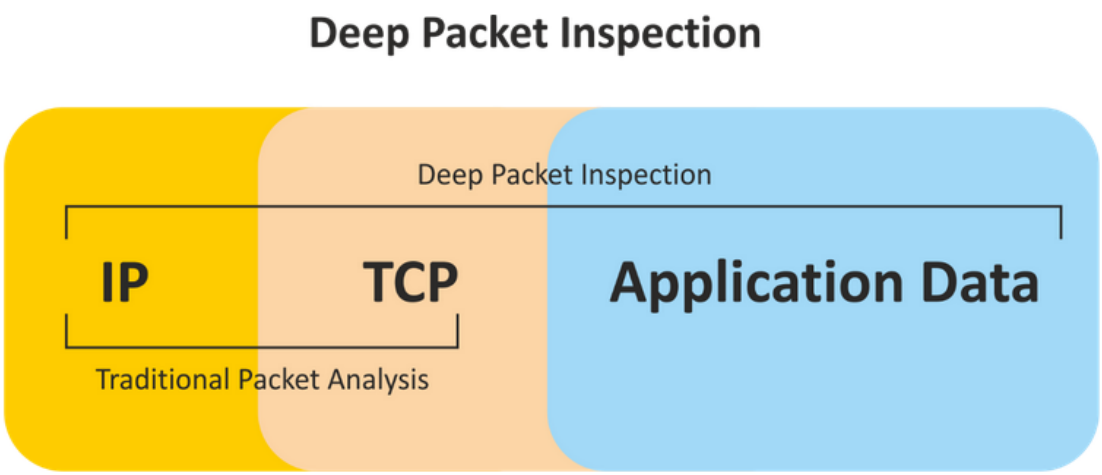
kaavalla (3), jossa n on arvojen lukumäärä, x_i on mitattu arvo ja $\bar{x}$ on tulosten keskiarvo. (Todennäköisyys ja tilastot n.d.)

$$S^2 = \frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n} \quad (3)$$

4 Pakettien analysointiprotokollat

4.1 Deep Packet Inspection

Deep Packet Inspection (DPI) on datapakettien analysointiin käytetty protokolla. DPI mahdollistaa datapakettien kokonaisvaltaisen analysoinnin ylätunnisteesta (engl. header) alatunnisteeseen (engl. footer). (Ks. Kuvio 4.) DPI on pakettien suodatustekniikka, jonka avulla voidaan tunnistaa, paikantaa, ryhmitellä, uudelleen reitittää ja estää liikennettä riippuen paketin datasisällöstä. DPI-protokolla toimii OSI-mallin (Open Systems Interconnection) sovelluskerroksella. (Rouse 2017.)



Kuvio 4. DPI:n sisältö (Saurabh 2017)

DPI mahdollistaa paketin syvemmän tarkastelun, kuten tiedon siitä, mistä sovelluksesta se on lähetetty ja mitä se sisältää. Protokolla pilkkoo headerin ja footerin pieniin osiin löytääkseen datasta tietyt merkkijonot ja muut yksityiskohdat, jotta paketti voidaan luokitella oikeaan ryhmään. DPI käyttää monia tapoja tutkia paketteja, mutta yleisimmät niistä ovat porttipohjaiset, staattiset ja automaatiopohjaiset tavat. Porttipohjaisessa tutkitaan paketin porttitietoja TCP/UDP -kehyksen headerissa, jolloin voidaan yhdistää tunnetut portit niitä käyttäviin

protokolliin. Staattisessa analysoinnissa keskitytään liikenteen luokitteluun paketin tavallisten tietojen, kuten pituuden ja porttitietojen perusteella. Automaatiopohjaisissa tavoissa analysoida dataa käytetään valmiita tilakoneita, joiden kautta data kierrätetään. Testaus alkaa alkutilasta, jolloin data kierrätetään automaattisen moottorin läpi, ja jos prosessi saadaan vietyä loppuun asti, voidaan tulkita, että paketti vastaa jotain jo tiedossa olevaa. (Saurabh 2017.)

4.2 Muut tekniikat

Ennen, kun tekniikka ei ollut vielä niin kehittynyttä ja verkkolaitteet olivat tehottomampia, pakettien analysointiin käytetyt tekniikat olivat Shallow Packet Inspection (SPI) ja Medium Packet Inspection (MPI).

4.2.1 Shallow Packet Inspection

SPI tarkastelee vain paketin header-osassa olevaa lähde- (engl. source) ja kohdeosoitetta (engl. destination) ja toimii näin ollen OSI-mallin neljännelle (siirto) kerrokselle asti. Koska SPI tarkastelee vain paketin headeria, pysyy yhteyden data anonyyminä, sillä paketin sisältöä ei huomioida analysoinnissa. Yksinkertaiset käyttöjärjestelmien palomuurit, kuten Windows XP:n ja Vistan, käyttävät SPI:a, koska sen avulla voidaan estää liikennettä ei halutuista IP-osoitteista (Internet Protocol). (Deep Packet Inspection n.d.)

SPI käsittelee lähettäjän ja vastaanottajan IP-osoitteita ja pakettien määrää, joihin viesti on pilkottu. Lisäksi SPI ottaa huomioon hyppyjen määrän, jonka paketti voi tehdä, kunnes reitittimet lopettavat reitittämästä sitä sekä synkronisoidun datan, joka mahdollistaa pakettien uudelleen kasaamisen muotoon, jotta dataa käsittelevä sovellus ymmärtäisi sitä. (Mt.)

4.2.2 Medium Packet Inspection

MPI on sovellusvälityspalvelin (engl. proxy) tai laite loppukäyttäjän ja oletusyhdyskäytävän (engl. gateway) välissä. MPI vertaa paketin data tyyppiä

valmiiksi luotuun listaan, jota pääkäyttäjät voivat helposti muokata, ja sen perusteella joko sallii tai estää liikenteen. MPI on SPI:a tehokkaampi, koska ei tarvita tiettyä listaa IP-osoitteista, vaan voidaan esimerkiksi estää videoiden tai kuvien katselu verkossa datan perusteella. Näin ollen MPI toimii OSI-mallin seitsemännelle eli sovellus -kerrokselle asti, koska se pystyy lukemaan paketin tietokuorman, kuten esimerkiksi tiedoston tyypin, esityskerrokselta ja sovelluksen komennot sovelluskerrokselta. MPI:n läpi voi kulkea hetkessä kymmenien tuhansien sovellusten paketteja, minkä vuoksi se skaalautuu suureen verkkoon huonosti, eikä tämän vuoksi ole kovin yleisesti käytössä. (Deep Packet Inspection n.d.)

5 Laitteisto

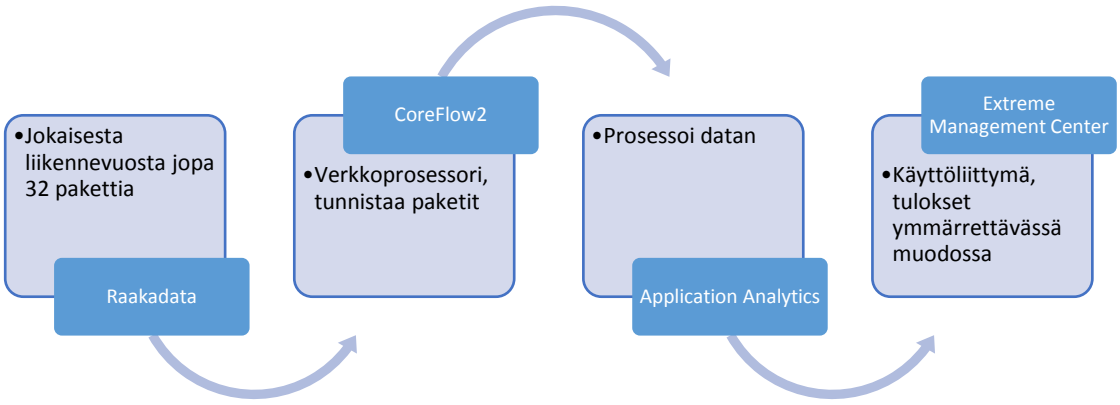
5.1 Yleistä

ExtremeAnalytics on Extreme Networksin kehittämä verkkomonitorointilaite, joka tarjoaa erinomaiset työkalut verkon viiveen analysointiin ja verkko-optimointiin. ExtremeAnalytics mahdollistaa OSI-mallin seitsemännen kerroksen näkyvyyden verkkoon. Laite asetetaan verkon sellaiseen kohtaan, jossa siihen voidaan peilata haluttu liikenne. ExtremeAnalytics mahdollistaa verkon hallinnoijan nähdä, mitä sovelluksia verkossa käytetään ja kuka niitä käyttää. Laitteen avulla saadaan selville sovellusten vasteaikoja, eli kauanko sovelluksen datalla kestää mennä palvelimelle ja takaisin. ExtremeAnalytics on oiva laite sellaisten verkossa olevien epäkohtien etsimiseen, jotka vaikuttavat verkon hitauteen ja toimimattomuuteen. (ExtremeAnalytics 2018.)

ExtremeAnalytics kokoaa kaiken keräämänsä datan käyttäjistä, laitteista ja sovelluksista yhteen datavarastoon, jolloin laitteelle karttuu laaja tietopohja siitä, mitä verkossa tapahtuu. ExtremeAnalyticsillä on mahdollista ottaa käyttöön virtuaalisensoreita, jolloin reaaliaikaista dataa saadaan myös mahdollisista VMware pohjaisista virtuaaliympäristöistä. Lisäksi Extremellä on vahva integraatio eri pilvipalveluiden, kuten Google Cloud Platformin, Amazon Web Servicesin ja Microsoft Azuren kanssa, jonka ansioista näiden tarkkailu ExtremeAnalytics-laitteella on myös mahdollista. (ExtremeAnalytics 2019.)

5.2 Toimintaperiaate

ExtremeAnalytics käyttää Deep Packet Inspection (DPI) -protokollaa ja monia erilaisia sormenjälkiä (engl. fingerprint) tunnistamaan liikennettä eri sovelluksista, niin paikallisista (esim. SAP, Exchange, SQL) kuin julkisistakin (esim. Google, Youtube, Facebook, P2P). ExtremeAnalytics ottaa kustakin uudesta liikennevuosta jopa 32 pakettia ja lähettää ne CoreFlow2:lle, joka on kustomoitu vuopohjainen verkkoprosessori. CoreFlow2:n sovelluskohtainen mikropiiri (engl. ASIC, Application Specific Integrated Circuit) tunnistaa sille lähetetyt paketit ja ohjaa ne Application Analytics -moottorille, jossa paketteihin lisätään alkuperäistä NetFlow-liikennettä, jolloin Application Analytics pystyy prosessoiman liikenteen ennen näkemättömällä laajuudella. Tämän jälkeen Application Analytics -moottori määrittelee sovelluksen, kerää datan, lisää tarvittavan kontekstin ja lähettää tiedon Extreme Management Centerille, jolloin verkon hallinnoija voi nähdä sen. (Ks. Kuvio 5.) Jos verkossa käytetään lisäksi laitteita, joissa on ExtremeXOS, niitä voidaan käyttää keräämään liikennevoita, mikä mahdollistaa tarkemman kuvan sovellusten käytöstä tutkitussa verkossa. (ExtremeAnalytics User Guide Version 8.2. 2019, 19.)



Kuvio 5. Toimintaperiaate

5.3 Hyödyt

Verrattuna perinteiseen tapaan analysoida verkossa käytettyjä palveluita ja käyttäjiä ExtremeAnalytics tarjoaa monenlaista apua. ExtremeAnalyticsin avulla nähdään

helposti, mitä sovelluksia verkossa käytetään ja kuka niitä käyttää. Verkon hallinnoija saa tärkeää tietoa siitä, miten sovelluksia käytetään ja tämän avulla käyttöä voidaan optimoida. Lisäksi, toisin kuin tavalliset menetelmät, ExtremeAnalyticsin tapa analysoida verkkoa ei rasita sitä. Laite asetetaan keskeiseen paikkaan verkkoa, jolloin ylimääräisiä kustannuksia ei tule. ExtremeAnalyticsin avulla voidaan myös estää sellaisten sovellusten käyttö verkossa, joita ei haluta siellä käytettävän. (ExtremeAnalytics 2018.)

5.4 Tekniset tiedot

ExtremeAnalytics-laite on yhden räkkiyksikön kokoinen palvelin, jonka tuote nimi on PV-A-305. Laitteeseen asennettaan tehtaalla kaikki valmiiksi, joten se on suoraan käyttövalmis. Laitteessa on kaksi 1Gbps verkkokorttia ja se pystyy suodattamaan jopa 1,3 miljoonaa tietovuota minuutissa. Laitteessa on 960GB SSd-levy ja virtalähde on kooltaan 750W. ExtremeAnalytics-laite painaa noin 13 kiloa. Lisäksi laitteen liitäntöihin kuuluu 5 USB-porttia, näyttöliitäntä VGA:lla ja sarjaportti RJ45:llä. (ExtremeAnalytics 2019.)

6 Toteutus

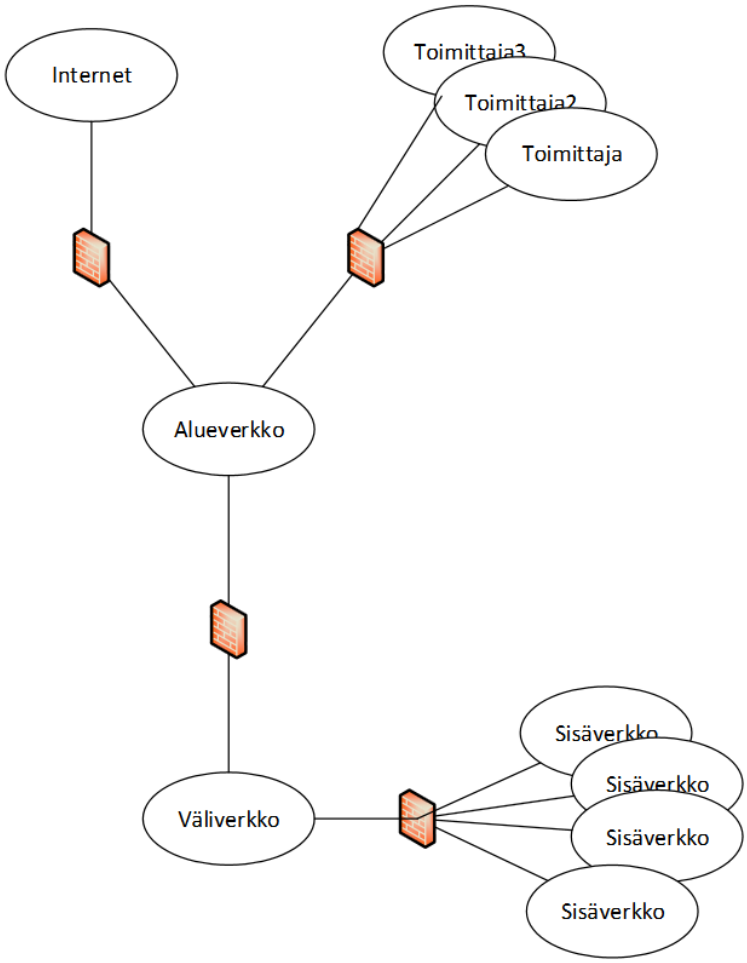
6.1 Tarkoitus

Tarkoituksena oli käyttöönottaa ExtremeAnalytics-laite ESSOTEn ympäristössä siten, että sitä voitiin hyödyntää ympäristössä käytettyjen sovellusten ja verkkokapasiteetin saatavuuteen liittyvissä asioissa, kuten palvelinten kuormitukseen, varsinkin jo olemassa olevissa ja äkillisissä ongelmatilanteissa. Toteutus aloitettiin selvittämällä toimeksiantajalle kriittiset palvelut, joiden perusteella tekeminen pystyttiin kohdentamaan. Sovellukset pantiin seurantaan palvelinten IP-osoitteiden ja joissain tapauksissa aliverkkojen perusteella. Lisäksi luotiin tarvittaessa laitteelle ennestään tuntemattomista sovelluksista sormenjäljet ja verkkoalueet ulkoverkossa oleville palvelimille. ExtremeAnalytics mahdollisti eri verkkorajapintojen tarkastelun, jolloin pystyttiin todentamaan eri palveluita vertailemalla, onko ongelmatilanteen sattuessa ko. ongelma omassa sisäverkossa vai jossain muualla, esimerkiksi palveluntarjoajan päässä.

6.2 Ympäristö

6.2.1 Yleistä

ESSOTEn verkkotopologia koostui kolmesta pääosasta: sisäverkoista, väliverkosta ja alueverkosta. (Ks. **Virhe. Viitteen lähdettä ei löytynyt.**Kuvio 6.) Työasemia ESSOTEssa oli noin 2700, josta kannettavia ja pöytätyöasemia oli noin 2400 ja loput 300 oli virtuaalipäätteitä eli Igeleitä. Käyttäjiä näillä työasemilla oli yhteensä noin 3500. Palvelimia ESSOTElla oli noin 150, josta osa oli fyysisinä ja osa virtuaalisina. Lisäksi palvelimista osa sijaitsi omassa alueverkossa ja osa toimittajien päässä. Palomuurit toimivat verkon reitityspisteinä, ja ne sijaitsivat niille kuvatuilla paikoilla erilaisin säännöin.



Kuvio 6. Verkkotopologia

6.2.2 Sisäverkko

Sisäverkot eli aliverkot sisälsivät käytössä olleet työasemat ja muut näihin verrattavissa olleet verkkoa tarvitsevat laitteet, kuten tulostimet, IP-puhelimet ja röntgenlaitteet. Kaikki sisäverkossa olevien laitteiden yhteydet kulkivat palomuurin kautta, ja työasemien väliset yhteydet oli estetty.

6.2.3 Väliverkko

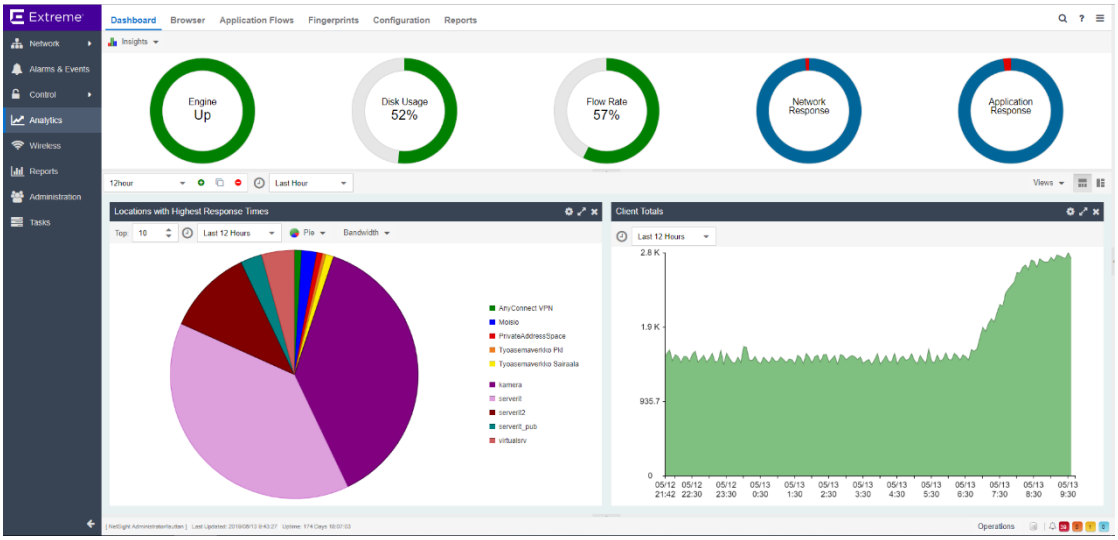
Väliverkkoon kuului ESSOTEn omat palvelimet, ja se toimi demilitarisoituna alueena (Demilitarized zone, DMZ). Väliverkossa yhdistyi sisäverkoista tulevat liikenteet, ja siitä ne ohjattiin joko takaisin päin tai uudelleen reititettiin edelleen alueverkkoon. ExtremeAnalytics-laite sijoitettiin sisäverkon ja väliverkon väliseen palomuuriin, jolloin se pystyi analysoimaan kaiken sinne asti päässeen liikenteen. Toisin sanoen ExtremeAnalytics oli kiinni päälinjassa (eng. core), jolloin siihen oli mahdollista peilata kaikki tarvittava liikenne.

6.2.4 Alueverkko

Alueverkossa yhdistyi väliverkosta tuleva liikenne, ja siitä oli mahdollista päästä verkko-operaattorin tarjoamien palomuurien läpi ESSOTElla käytössä olleiden palveluiden tarjoajiin sekä Internetiin. Lisäksi alueverkkoon reitittyi muualta, kuten muista sairaanhoitopiireistä, tulevat sisäverkkoyhteydet. Kaikki etäyhteydet reitittyivät niin ikään Internetiin kulkevan palomuurin lävitse. Internetiin ESSOTElla kuljettiin välityspalvelimen (eng. proxy) kautta.

6.3 Käyttöliittymä

ExtremeAnalyticsiä käytettiin sen selainpohjaisen käyttöliittymän, Extreme Management Centerin, kautta (ks. Kuvio 7). Käyttöliittymän vasemmassa kulmassa oli navigointipalkki, josta tärkeimmät välilehdet olivat Analytics, Reports ja Alarms & Events. Vaikka laite tarjosi paljon ominaisuuksia, käyttöliittymä oli saatu tarpeeksi yksinkertaiseksi, jotta kaikki tarvittava löytyi helposti.



Kuvio 7. Käyttöliittymä

6.3.1 Analytics

Analytics -välilehdellä tehdään kaikki analysointiin liittyvä. Kojelaudalla (eng. dashboard) nähdään verkon kuormitusta yleisesti ja siihen on mahdollista tehdä omia näkymiä. Browser (selain) tarjoaa mahdollisuuden tarkastella tiettyä sovellusta, päätelaitetta tai verkon osaa. Application flows näyttää kaikki laitteelle peilatut tietovuot reaaliaikaisesti. Fingerprints välilehdeltä nähdään laitteella olevat tunnisteet. Configuration tarjoaa mahdollisuuden erilaisiin konfiguraatioihin, kuten verkon lokaatioiden tunnistamiseen. Reports -välilehdeltä nähdään reaaliaikaista dataa esimerkiksi storagen tai protokollien kuormituksesta.

6.3.2 Application Flows

Application Flows -välilehdeltä nähtiin reaaliaikaisesti verkossa tapahtuvaa liikennettä. Jokainen päätelaitteen ja serverin välillä tapahtuva liikennöinti-istunto sisältää useita tietovoita ja näistä kaikista jää jälki application flows -välilehdelle. Välilehdeltä voi hakea esimerkiksi tiettyä päätelaitetta, serveriä tai sovellusta, jota halutaan tarkkailla. Välilehdeltä saadaan kokonaisvaltainen tieto liikenteestä; mikä päätelaite lähettää dataa mihinkin serveriin, mitä protokollaa ja porttia käytetään, mitä dataa lähetetään, tieto laitteiden lokaatioista verkossa vlanien perusteella ja paljon muuta dataa, kuten istunnon kesto ja pakettien määrä. Jos verkon ylläpitäjä

huomaa liikennettä, jota laite ei osaa luokitella, siitä voidaan luoda manuaalisesti sormenjälki (eng. fingerprint), jolloin tulevaisuudessa laite ymmärtää tällaisen liikenteen.

6.3.3 Reports

Reports välilehdellä luotiin raportteja halutuista kohteista. Analytics välilehdellä luodut raportit voitiin yhdistää kokonaisuuksiksi, jolloin saatiin halutut tapahtumat näkymään yhdellä kertaa. Yleensä haluttiin tehdä raportti, jossa samassa pohjassa näkyivät tietyn sovelluksen tai palvelimen vasteaika verkko- ja sovellustasolla.

6.3.4 Alarms & Events

ExtremeAnalyticssä oli mahdollista luoda erilaisia hälytyksiä tarpeiden mukaan. Hälytyksen lähteenä oli laite, rajapinta tai liityntäkohta (Access Point), joka oli hälytyksen laukaisija. Hälytykset lähtivät pois joko käsin kuittaamalla tai jos esimerkiksi yhteys laitteeseen katosi ja palasi uudelleen, hälytys kuittautui itsestään. ExtremeAnalyticsissä oli mahdollista tehdä kuusi erityyppistä hälytystä.

Custom Criteria Alarm
Hälytystyyppi, jossa voidaan määritellä todella tarkat kriteerit tapaukselle

Flow Alarm
Hälytys, jota käytetään raportoimaan verkkoliikenteen tietovoiden poikkeamista, jotka NetFlow huomaa. Hälytys laukeaa, kun vuomäärä vastaa konfiguroituja tietoja

Selected Trap Alarm
Hälytys, jonka konfiguroinnissa käytetään Extreme Management Centerissä olevia valmiita laitekohtaisia Trap ID:eita. Kun konfiguroitu ansa (eng. trap) ilmenee, hälytys laukeaa.

Severity Alarm

Vakavuuteen perustuva hälytys, joka ilmenee joko hätätapauksena, hälytyksenä, kriittisenä, virheenä, muistutuksena tai ilmoituksena (eng. Emergency, Alert, Critical, Error, Warning, Notice, Info). Hälytys konfiguroidaan valitsemalla joko tapahtuma (eng. event), trap tai molemmat, ja kun tämän vakavuusaste ilmenee, hälytys laukeaa.

Status Change Alarm

Hälytys tulee, kun laitteen toiminnallinen tila vaihtuu. ”Contact Lost” -hälytys tulee, kun yhteys laitteeseen on kadonnut. ”Contact Established” -hälytys puolestaan tulee, kun yhteys on palautunut. Molemmat näistä hälytyksistä tulevat, kun yhteys on kadonnut ja palautunut takaisin.

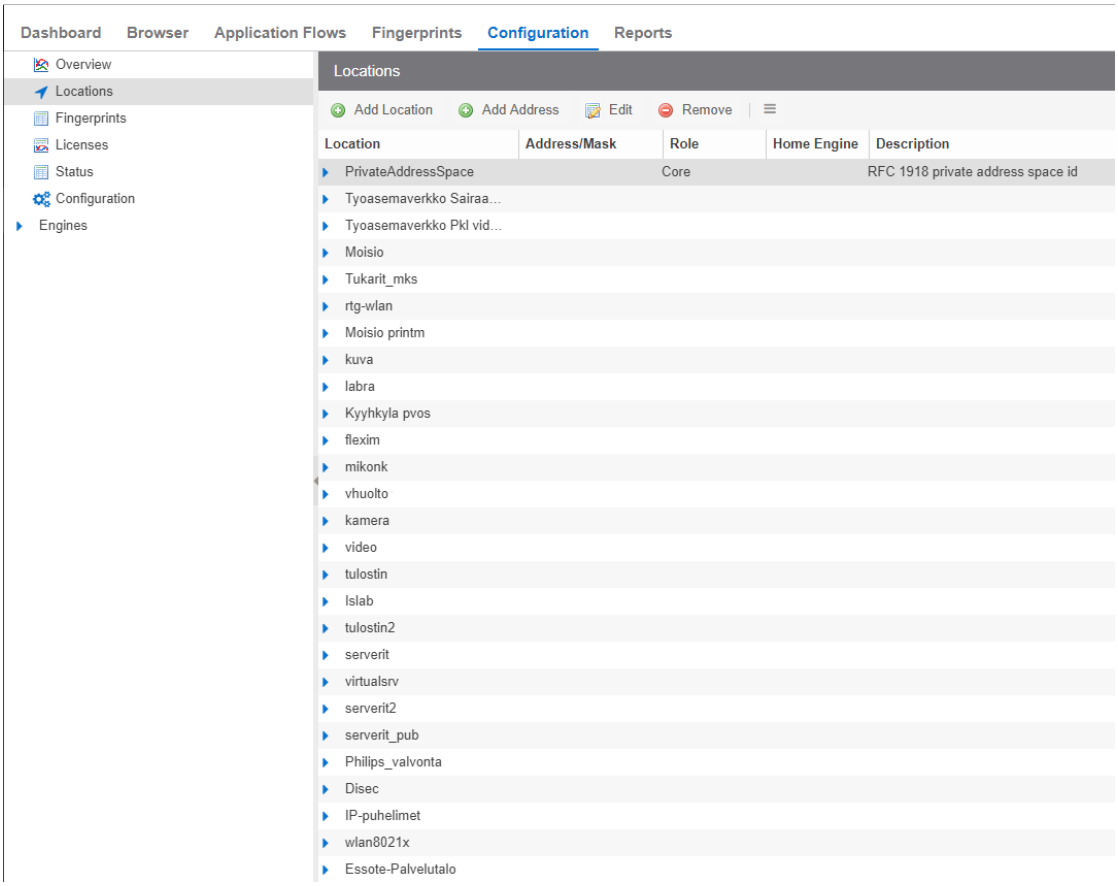
Threshold Alarm

Kun tietty arvo menee ennalta määritetylle arvoalueelle, tulee ”Threshold Alarm”. Esimerkiksi sovelluksen vasteajan raja-arvoksi on asetettu 100ms, kun tämä ylittyy, hälytys laukeaa.

6.4 Konfigurointi

6.4.1 Lokaatiot

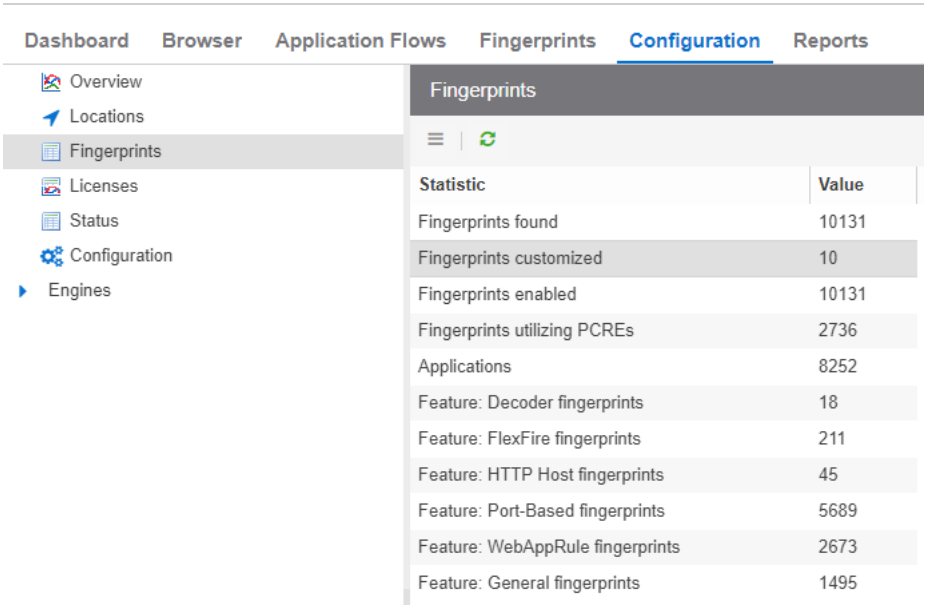
Jotta verkkoanalysointia voitiin lähteä kohdentamaan, oli luotava ensin lokaatioita. Lokaatiot luotiin tässä tapauksessa olemassa olevien vlanien ja ulkoisessa verkossa olevien palvelinsijaintien perusteella Configuration -välilehdeltä. (Ks. Kuvio 8.) Jotta lokaatioista saatiin kaapattua liikennettä, oli jokaisen aliverkon liikenne peilattava yrityksen runkoverkosta Analytics -laitteelle. Tämä helpotti myöhemmin tehtävää analysointia, jolloin voitiin esimerkiksi verrata Kangasniemellä olevan verkon kuormitusta Mikkelissä olevaan.



Kuvio 8. Lokaatiot

6.4.2 Fingerprints

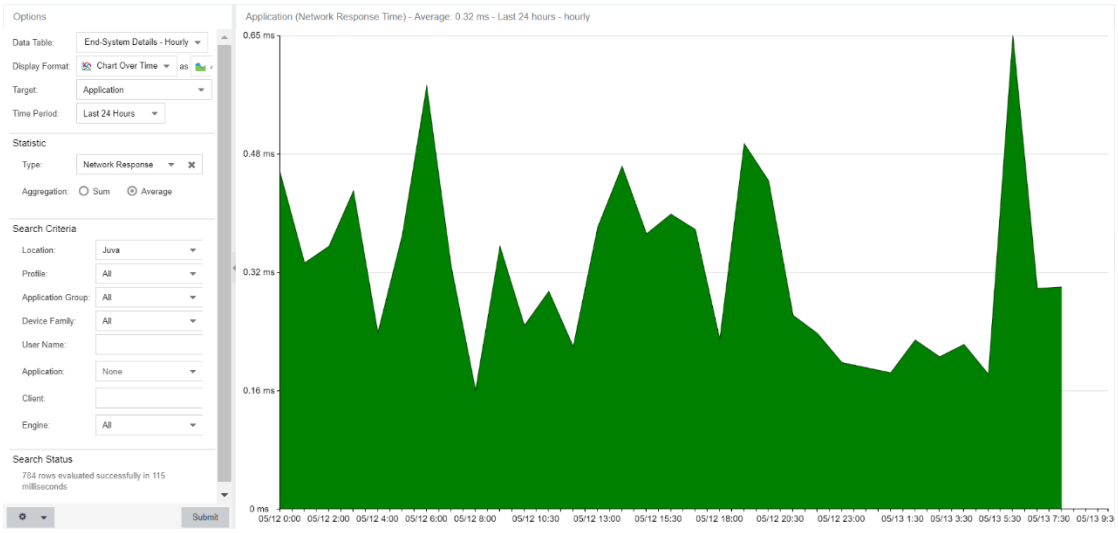
Fingerprintit ovat niin sanottuja kaavoja, joiden avulla voidaan määritellä mistä sovelluksesta on kyse. Fingerprinttejä voidaan luoda perustuen tietovuohon, sovellukseen, sovellusryhmään tai kohdeosoitteeseen. Extreme Analyticsillä on valmiita ”System Fingerprinttejä”, jotka ovat luotu yleisimmistä Extremen tietokantaan tallennetuista sovelluksista. System Fingerprinttejä on tällä hetkellä n. 10 000 ja lisää on tulossa koko ajan. (Ks. Kuvio 9.) Tuntemattomista sovelluksista järjestelmänvalvojan on helppo tehdä oma sormenjälkensä, josta tulee näin ollen ”Custom Fingerprint”. Esimerkiksi käytössä olleen potilastietojärjestelmän liikenne oli laitteelle tuntematonta, joten siitä tehtiin oma sormenjälkensä.



Kuvio 9. Sormenjäljet

6.5 Mallipohjat

Analyticsin Browser -välilehdellä voidaan luoda valmiita pohjia halutuista tapahtumista. Pohjan teko alkaa valitsemalla taulukon tyyppi, tarkasteltavan asian kohde ja aikajakso. Seuraavaksi valitaan statistiikan tyyppi, kuten sovelluksen tai verkon vasteaika, lähetetyt tai vastaanotetut paketit tai sovellusta käyttävien päätelaitteiden keskimääräinen lukumäärä. Viimeisenä määritellään hakukriteerit, joista tärkeimmät ovat ”Location”, ”Application” ja ”Client”. Näiden valintojen kautta voitiin hakea vaikkapa verkon keskimääräinen vasteaika tietyssä vlanissa tai tietyn sovelluksen keskimääräinen vasteaika tietyille käyttäjille ja tallentaa se pohjaksi. Kuvio 10 nähdään Juvan verkon vasteaika keskimäärin per päätelaite 24 tunnin ajalta. Haettu pohja voitiin tallentaa komponentiksi, josta niin ikään voitiin luoda uusi raporttinäkymä Reports-välilehdellä.



Kuvio 10. Raporttipohja

6.6 Palvelut

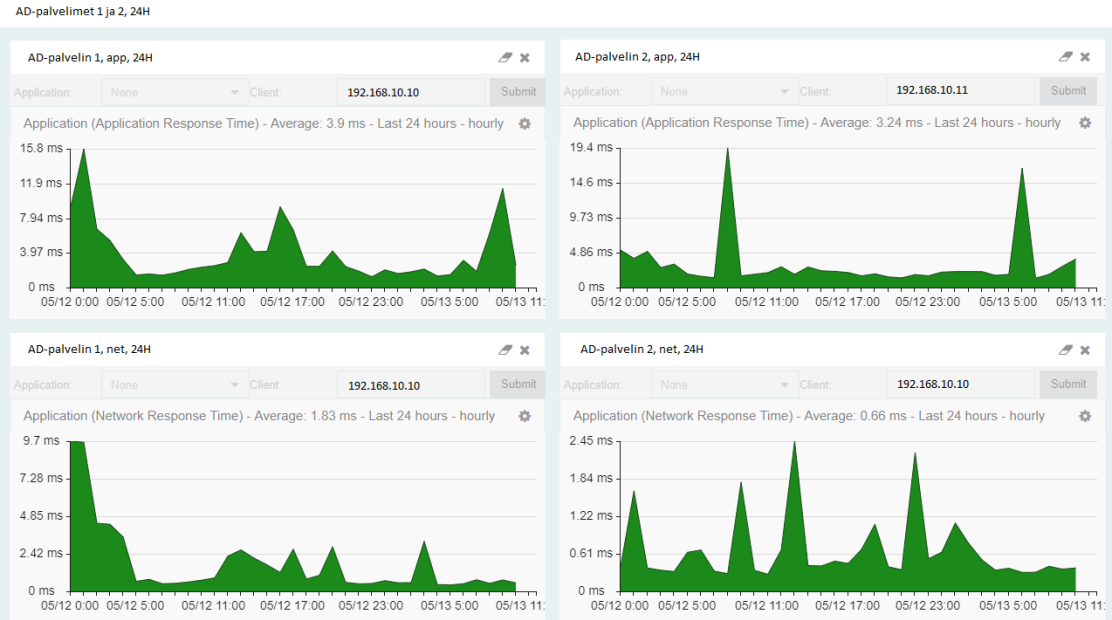
ESSOTE tarjoaa asiakkaillensa todella laajalla skaalalla terveyspalveluita, jonka takia kriittisiä palveluita oli paljon. Kriittisimmät palvelut olivat niitä, jotka vaikuttivat suoraan yrityksen liiketoimintaan, joita ilman työskentely olisi vaikeaa tai jopa mahdotonta. Tällaisia palveluita olivat mm. AD-palvelut, DNS ja käytössä oleva potilastietojärjestelmä. Muita kriittisiä palveluita olivat esimerkiksi levyjakopalvelut, SQL-palvelut, teho-osastolla käytettävät sovellukset, kulunvalvojajärjestelmä, kuvantamisen järjestelmät ja muut potilaiden tietoja käsittelevät palvelut.

6.6.1 Active Directory -palvelut

AD-palveluiden (Active Directory) toimimattomuus vaikuttaisi jokaisen yrityksen toimintaan dramaattisesti, siksi toimeksiantaja halusi luonnollisesti siitä reaaliaikaisen näkymän seurantaan. AD-palvelin oli kahdennettu, joten raporttipohjaan tuli kummankin palvelimen sovellus- ja verkkovasteajat seurantaan. (Ks. Kuvio 11.) Valvomossa katsoessa nähtäisiin heti, jos jommallakummalla palvelimella olisi virhetila päällä, vaikkakin AD:sta puhuttaessa vikatikettejä saattaisi tulla nopeasti palvelinrikon sattuessa.

Kuvio 11 AD-palvelimen 2 korkein piikki ajoittuu ajankohtaan, jolloin käyttäjät tulevat töihin. Kummatkin kuviossa nähtävät piikit ovat noin 7 aikaan aamulla. AD-palvelimet

oli konfiguroitu niin, että kummatkin pyrittiin kuormittamaan tasaisesti, jolloin mistä vaan sisäverkosta oli mahdollista ottaa yhteys jommallekummalle palvelimelle. AD-palvelimen 1 yöllä näkyvä piikki johtuu sille ajatetuista varmuuskopioista.

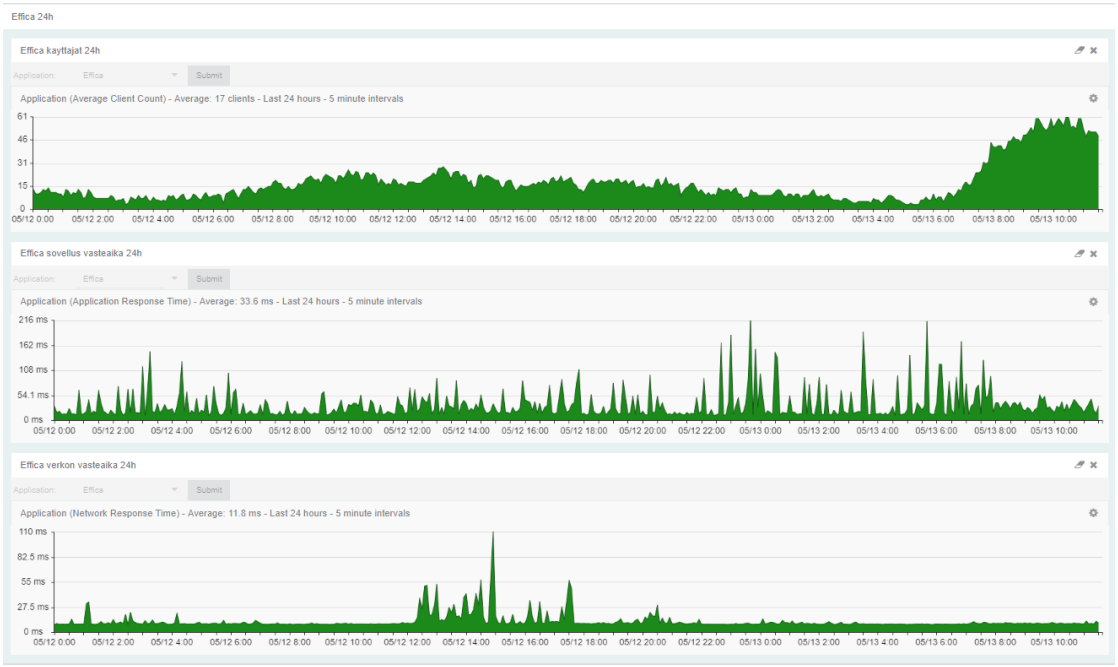


Kuvio 11. AD-palvelimet

6.6.2 Potilastietojärjestelmä Effica

Yksi kriittisimmistä palveluista oli käytössä oleva potilastietojärjestelmä Effica. Jos järjestelmään pääsy oli estynyt, potilaiden saama hoito saattoi kärsiä. Tämän vuoksi sovelluksella oli useita palvelimia, jolloin se oli redundanttinen. Palvelimet sijaitsivat ulkoverkossa. Potilastietojärjestelmän liikenne oli Extreme Analytics -laitteelle ennestään tuntematonta, jolloin siitä tehtiin oma sormenjälki. Liikennettä muodostui eri protokollista ja porteista, joten sormenjälki sisälsi useita komponentteja. Kun fingerprint oli valmis, voitiin miettiä, minkälainen raporttinäkymä haluttaisiin tehdä. Tärkeää oli saada tietää sovelluksen vasteaika sovellus- ja verkkotasolla. (Ks. Kuvio 12.) Lisäksi haluttiin tietää sovelluksen käyttäjämäärä, mistä pystyttiin tekemään vain suuntaa antava arvio, koska yrityksen ympäristössä oli käytössä virtuaalipäätteitä, jolloin yksi virtuaalipäätteiden palvelin nähtiin yhtenä käyttäjänä, vaikka todellisuudessa käyttäjiä saattoi olla yhdellä palvelimella jopa 30.

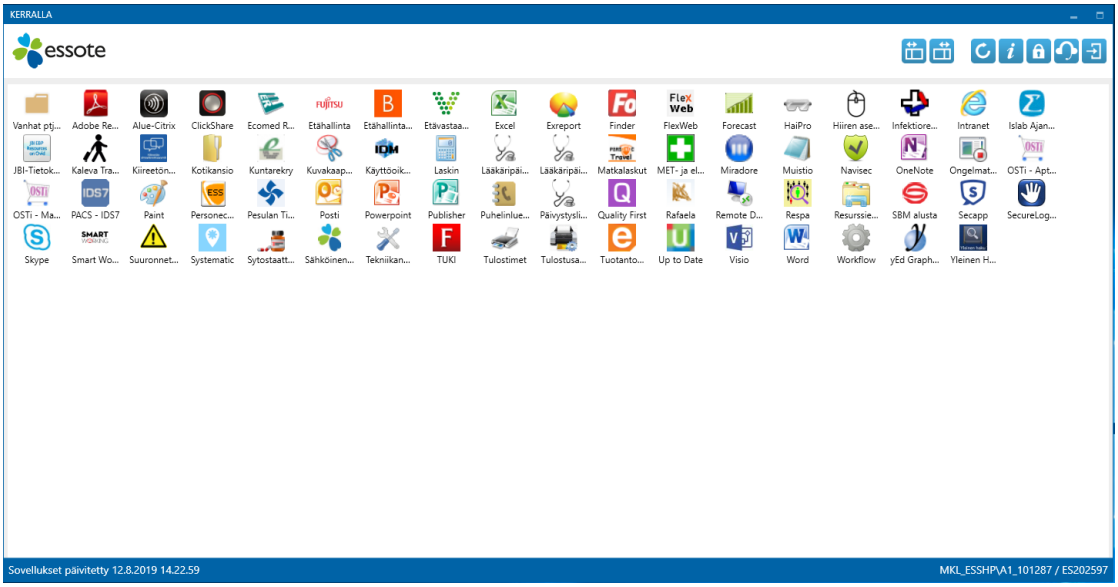
Kuvio 12 nähdään hyvin viikonlopun vaikutus sovellukseen. Käyttäjämäärä on noussut huomattavasti maanantaina 13.5, kun taas sunnuntaina 12.5 se on ollut alhaisempi. Sovelluksen vasteajat ovat puolestaan pysyneet suhteellisen samoina. Suurimmat piikit sovelluksen vasteajoissa johtuvat öisin noin klo. kolme ajettavista varmuuskopioista.



Kuvio 12. Potilastietojärjestelmä Effica

6.6.3 Kerralla-valikko

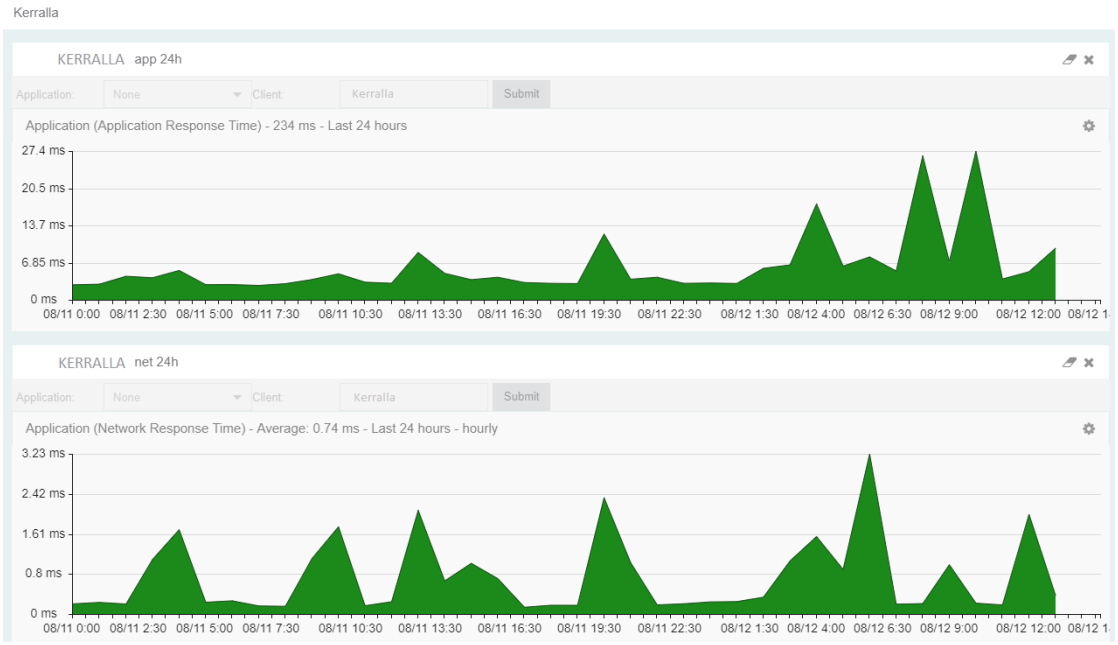
Kerralla-valikko oli ympäristössä käytetty sovellus, josta käyttäjät pääsivät kaikkialle tarvitsemiinsa palveluihin. Ympäristön työasemissa oli käytössä pääosin Windows 10 -käyttöjärjestelmä, jossa työpöydän käyttö oli estetty tavallisilta käyttäjiltä. Tämän vuoksi Kerralla-valikko oli erittäin kriittinen, sillä sen toimimattomuus esti, tai ainakin vaikeutti, käyttäjien pääsyn jokapäiväisiin, kriittisiin, sovelluksiin. Kerralla-valikko aukeaa aina työpöydälle, kun käyttäjä kirjautuu työasemalle. (Ks. Kerralla-valikkoKuvio 13.) Kerralla-valikko koostui yleisistä pikakuvakkeista, jotka näkyivät kaikille käyttäjille kuten mm. Intranet ja tulostusasetukset. Lisäksi oli mahdollista lisätä muita pikakuvakkeita niitä tarvitseville käyttäjille, kuten esimerkiksi pikakuvake tiettyyn sovellukseen tai linkki tarpeelliselle verkkosivustolle. Pikakuvakkeiden hallinta tapahtui AD:n kautta.



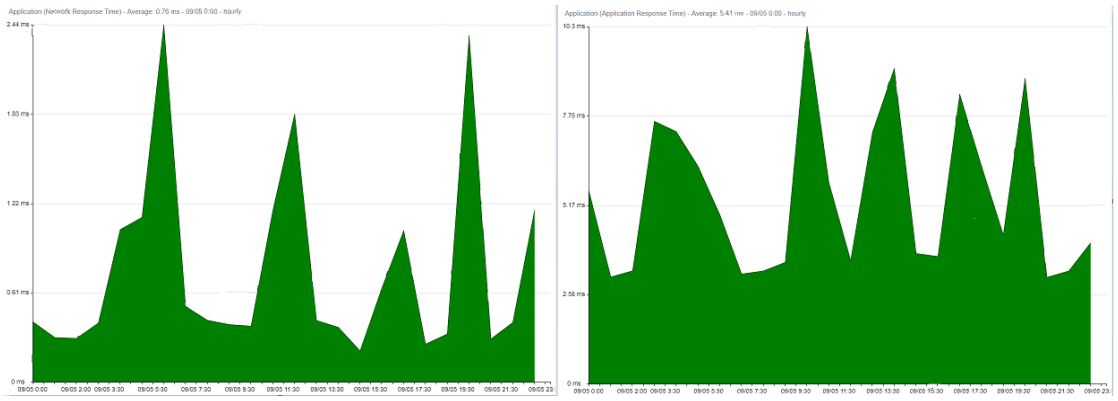
Kuvio 13. Kerralla-valikko

Kerralla-valikko otettiin myös valvontaan sovellus- ja verkonvasteen perusteella (ks. Kuvio 14). Kuviosta nähdään 24 tunnin otanta Kerralla-valikon toiminnasta. Kuviosta voidaan päätellä, että käyttäjien määrä on noussut noin kello seitsemän ja kahdeksan aikaan maanantaina 12.8., jolloin sovelluksen sovellusvasteessa näkyy piikki. Lisäksi 12.8. kello kymmenen on ollut häiriö Effican mediakeskuksessa, jolloin käyttäjien on täytynyt käynnistää Effica uudelleen kerralla -valikosta, jolloin palvelin on kuormittunut. Toisaalta taas sunnuntaina 11.8. käyttäjiä on todennäköisesti ollut vähemmän, sillä sovelluksen vasteajat ovat tuolloin olleet matalia

Kuvio 15 on vertailun vuoksi esitetty toinen graafi eri päivältä samasta sovelluksesta. Kummassakin kuviossa verkon vasteaikojen keskiarvot ovat lähes samat (0,74 ja 0,76ms). Vertailukuvassa (Ks. Kuvio 15) sovelluksen vasteaikojen korkeimmat piikit ovat olleet noin 8 ja 10 ms, kun taas Kuvio 14 korkeimmat piikit ovat olleet noin 27 ms, jolloin voitiin ajatella, että vertailukuvan tilanne on ns. normaali.



Kuvio 14. Kerralla-valikon valvonta



Kuvio 15. Kerrallan-valikon vertailu

6.6.4 Citrix

Kriittisiin palveluihin lukeutui myös ympäristössä käytössä olleet Citrix-palvelimet. Citrix-palvelimet sisälsivät Alue-Citrix -sovelluksen, sekä istunnot kevytpäätteiltä eli Igeleiltä.

Alue-Citrixin kautta pystyi käyttämään joitakin sovelluksia, kuten potilastietojärjestelmää. Potilastietojärjestelmän käyttö Alue-Citrixin kautta oli suotavaa etenkin, jos käyttäjä oli verkossa etäyhteydellä, koska verkkoyhteyden

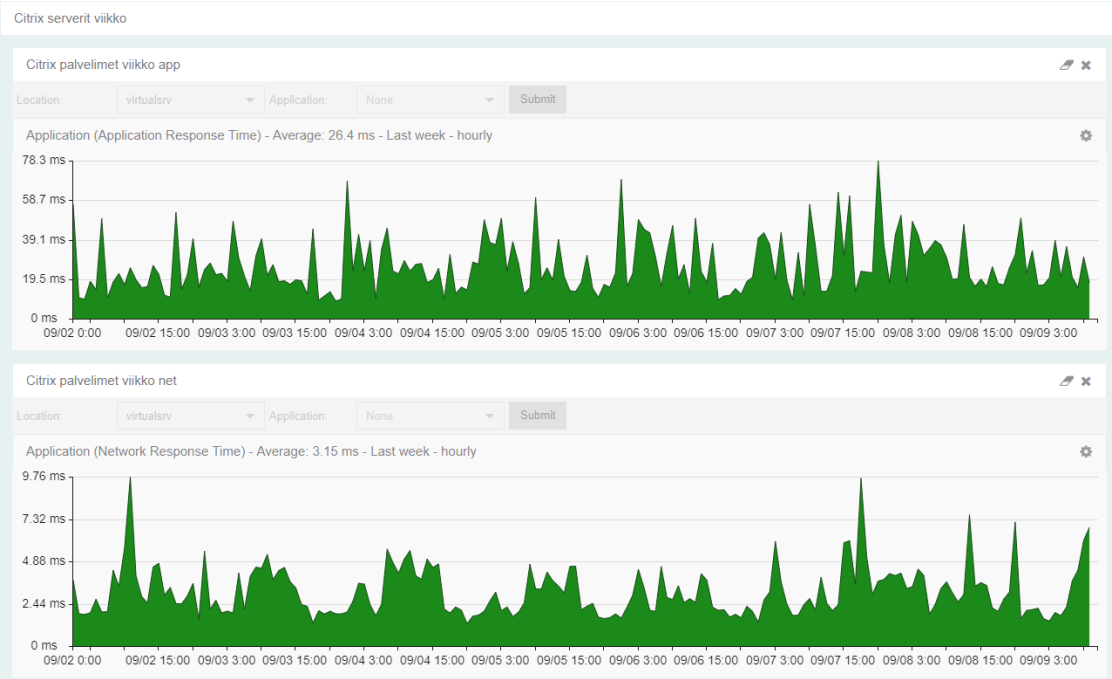
katketessa käyttäjän istunto jäi auki Citrix-palvelimelle, minkä seurauksena tallentamattomat työt eivät hävinneet heti.

Kevytpäätteet eli Igelit olivat työasemia (ks. Kuvio 16.), jotka loivat käyttäjälleen istunnon Citrix-palvelimille niille kirjauduttaessa. Käytännössä Igelit olivat ”tyhmiä” päätteitä, jotka käyttivät palvelinten resursseja. Kun käyttäjä kirjautui Igelille, Igel loi käyttäjälle istunnon yhdelle Citrix-palvelimelle. Igelille kirjauduttiin toimikortilla, jonka vuoksi käyttäjä saattoi kirjautua Igelille yhdellä osastolla, ottaa kortin mukaansa ja kirjautua uudelleen eri Igelille toisella osastolla. Käyttäjän istunto säilyi palvelimella koko tämän ajan ja kun hän missä tahansa vaiheessa kirjautui kevytpäätteelle, työpöytä näkymä säilyi sellaisenaan, mihin se oli jäänyt edellisellä kerralla.

Kuvio 16. Igel (Endpoint 2019).

Osa Citrix-palvelimista olivat fyysisiä ja osa virtuaalisia. Yksi palvelin pystyi käsittelemään jopa 30 istuntoa saman aikaisesti. Kuvio 17 on esitetty kootusti kaikkien Citrix-palvelinten vasteajat verkon ja sovellustason osalta viikon ajalta. Kaikista palvelimista tehtiin myös omat seurantanäkymät, jolloin pystyttiin paremmin seuraamaan niiden kuormitusta. Citrix-palvelimet haluttiin ottaa seurantaan niiden kriittisyyden vuoksi. Kriittisiä palvelimista teki kevytpäätteiden olemassaolo ja niiden jatkuva lisääntyminen ympäristössä sekä Alue-Citrixin käyttö. Alue-Citrixin kautta oli mahdollista käyttää esimerkiksi eri potilastietojärjestelmiä, kuten Effica ja ProConsonaa. Verkon vasteaikojen osalta tulokset näyttävät olevan viimeisen viikon

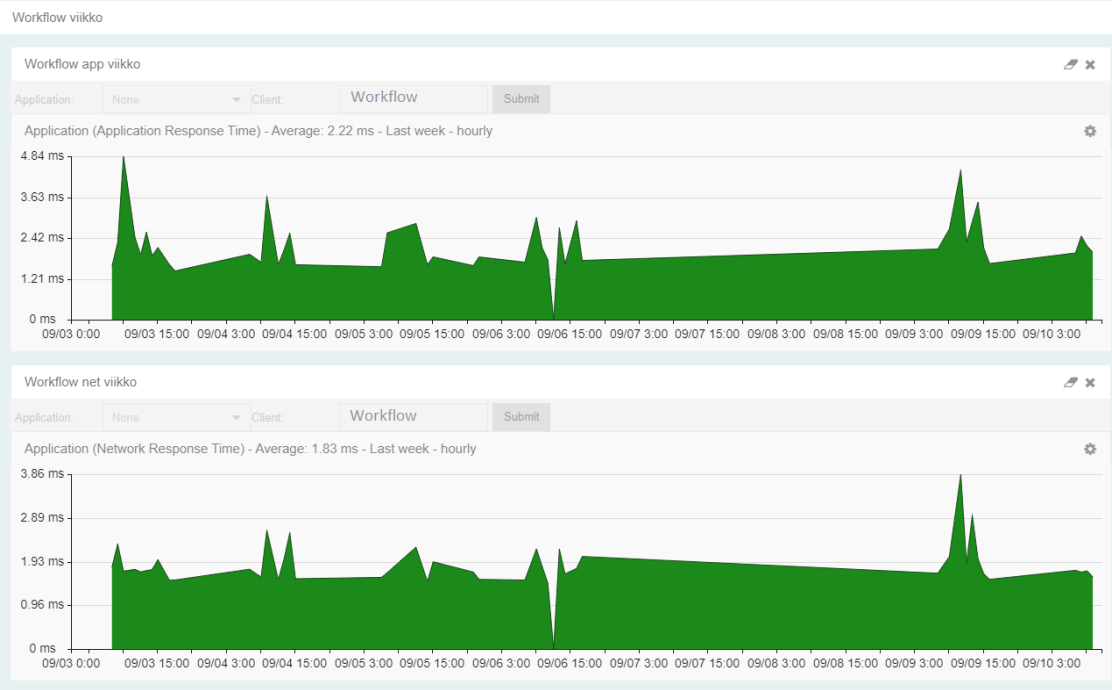
ajalta kunnossa. Myös sovelluksen vasteajat ovat kohtuullisen samalla tasolla eri päivien välillä.



Kuvio 17. Citrix-palvelimet

6.6.5 Workflow

Workflow on Aditro Oy:n toimittama sovellus, joka on tarkoitettu ostolaskujen tarkastamiseen, hyväksymiseen ja tiliöintiin. ESSOTE:lla Workflowta käytettiin Alue-Citrixin kautta. Workflow oli pääasiassa taloushallinnon työkalu, mutta myös muiden osastojen taloudesta vastaavat henkilöt kävivät hyväksymässä ja tarkistamassa laskuja siellä. Workflow otettiin seurantaan sen palvelimen IP-osoitteen perusteella (ks. Kuvio 18.) siksi, koska sovellus oli hidastellut käyttäjien mukaan satunnaisesti. Nopealla otannalla sovelluksessa ei havaittu ongelmia, mutta selvitys on edelleen käynnissä. Edellä mainitusta kuviosta voidaan havaita, että 6.9 noin kello 12 palvelu on ajettu alas. Alasajo johtui sovellukselle tehdystä huoltokatkosta. Korkeammat kuviossa havaittavat piikit johtuvat käyttäjämäärän kasvusta ja ajankohdat sijoittuvat noin kello 9:än.



Kuvio 18. Workflow

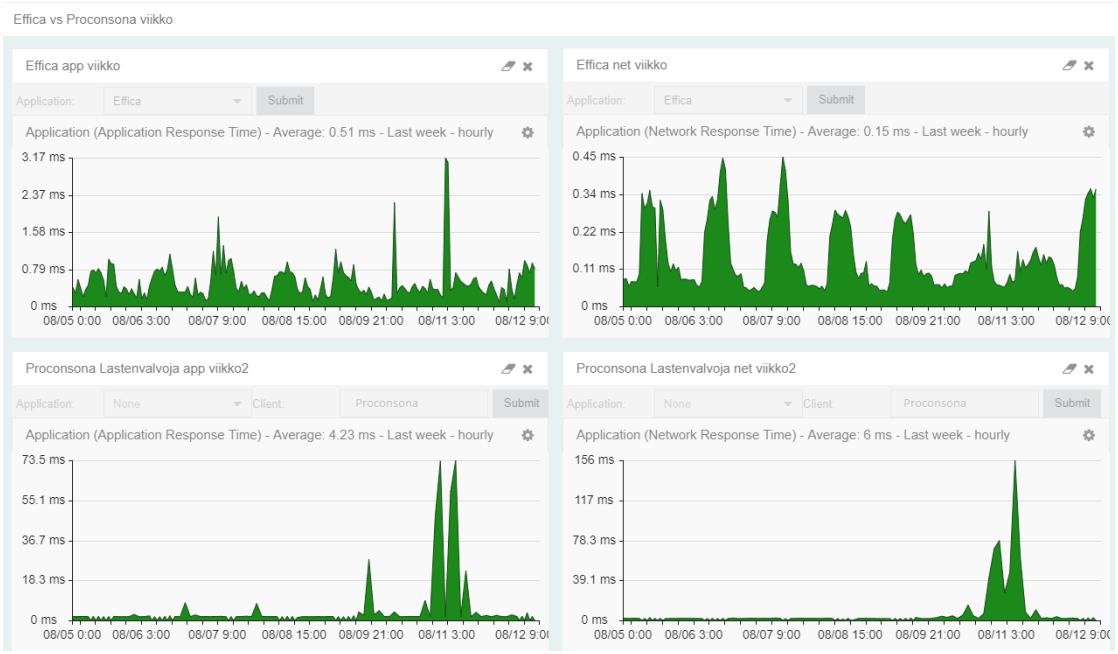
6.6.6 Muut sovellukset

Muihin sovelluksiin kuuluivat eri osastoilla, kuten esimerkiksi teho-osastolla, sosiaalityössä ja hallinnossa käytetyt sovellukset. Yleensä nämä sovellukset ottivat yhteyksiä yksittäisille palvelimille, joten helpoin tapa ottaa palvelut seurantaan oli tehdä yksi raporttipohja kutakin palvelua kohti. Tässä raporttipohjassa haluttiin nähdä liikenteen vasteaika sovellus- ja verkkotasolla ja tarkasteltava kohteena oli palvelimen IP-osoite.

6.7 Epäkohtien kartoitus

Laitteen käyttöönoton aikana saatiin käyttäjiltä ilmoituksia, että toisessa käytössä olleista potilastietojärjestelmistä ilmeni hitautta varsinkin lauantaisin. Kyseinen potilastietojärjestelmä, ProConsona, oli jo seurannassa, mutta siihen paneuduttiin entistä tarkemmin ilmoitusten jälkeen. Nopeasti ilmeni, että ProConsonassa oli huomattava piikki vasteajoissa sekä sovelluksen, että verkon osalta aina lauantaisin. (Ks. Kuvio 19.) Tämän jälkeen piti selvittää, oliko vika omassa verkossa vai jossain muualla, kuten esimerkiksi verkkopalveluiden tarjoajan tai sovellustoimittajan päässä. Selvitykseen lähdettiin ottamalla seurantaan samasta verkkoalueesta toinen

palvelu, tässä tapauksessa oli helppoa verrata toimintaa toiseen potilastietojärjestelmään, Efficaan. Efficaa käytettiin ympäristössä todella paljon enemmän kuin ProConsonaa, eikä sen hitauksista ollut tullut minkäänlaisia ilmoituksia. Myöskään seurantaan ottamalla kummatkin palvelut, Efficassa ei havaittu erityistä käyttäytymistä lauantain osalta, kun taas ProConsonassa lauantaisin oli huima piikki.



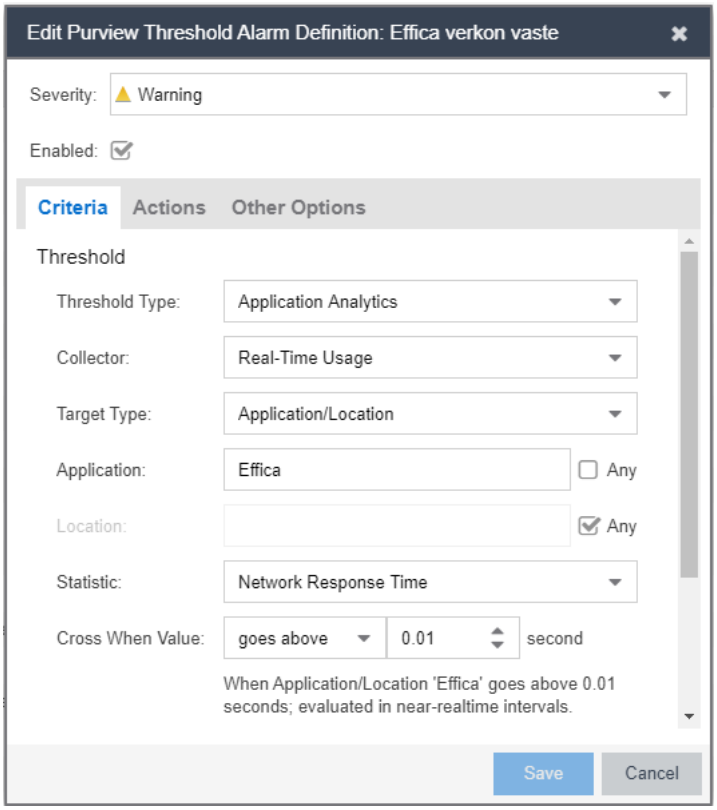
Kuvio 19. Effica vs Proconsona

Tämän jälkeen voitiin todeta, että ongelmat eivät olleet omassa sisäverkossa. Kummallakin potilastietojärjestelmällä oli eri toimittaja ja kumpikin sovellus reitittyi alueverkon kautta väliverkkoon ja sitä kautta sisäverkkoon. (Ks. Kuvio 6.) Tästä voitiin tehdä johtopäätös, että reitti Effican toimittajalta ESSOTE:n alueverkkoon oli kunnossa, kun taas ProConsonan reitti ei. Tuloksista ilmoitettiin ProConsonan toimittajalle, jolta vastaus ongelmiin tuli jonkun ajan kuluttua. ProConsonasta oli ajettu varmuuskopioita lauantai-sunnuntai välisenä aika, ja kun näiden ajamiseen tehtiin muutoksia, sovelluksen ja verkon viiveet hävisivät.

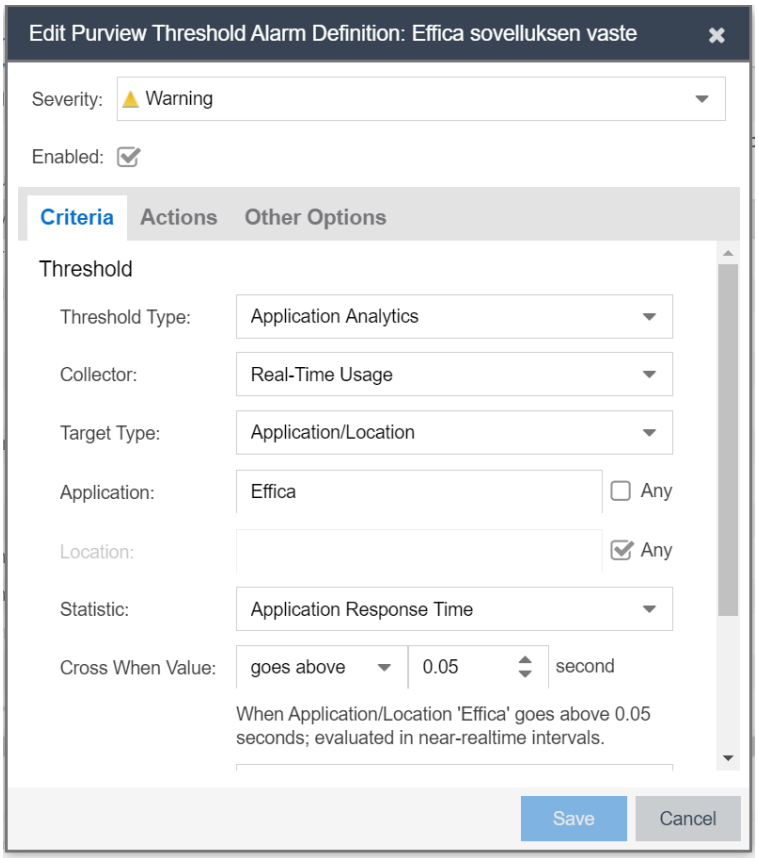
6.8 Hälytykset

6.8.1 Hälytysten konfigurointi

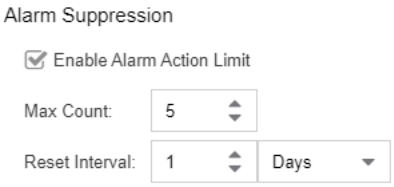
ExtremeAnalyticsissä oli muutamia valmiita hälytyksiä koskien esimerkiksi sovelluksen ja verkon vasteaikoja lokaatio kohtaisesti. Nämä eivät kuitenkaan antaneet tarpeeksi hyvää kuvaa mahdollisista akuuteista ongelmista, joten haluttiin luoda uusi hälytys koskien Effican käyttöä. Hälytysmalliksi valittiin ”Threshold Alarm”, joka luo hälytyksen, kun asetettu raja-arvo ylittyy. Hälytyksestä haluttiin tehdä niin kutsuttu huoltohälytys, jolloin raja-arvot asetettiin matalammalle. Tämän ansiosta oli mahdollista nähdä heti, jos jossain sisäverkossa vasteajat alkoivat nousta, jolloin tapaukseen oli mahdollista reagoida nopeasti. Hälytyksen vakavuudeksi valittiin tämän vuoksi ”Warning”. Keräilyajanjaksoksi valittiin ”Real-Time Usage”, jolloin hälytys tuli heti, jos raja-arvot ylittyivät. Kohteeksi valittiin ”Application/Location”, jolloin pystyttiin asettamaan tarkasteltavaksi sovellukseksi Effica. Hälytyksiä tehtiin kaksi: verkon vasteajalle (ks. Kuvio 20.) ja sovelluksen vasteajalle (ks. Kuvio 21). Verkon vasteajan raja-arvoksi asetettiin 10ms ja sovelluksen vasteajalle 50ms, koska sovelluksen normaalia käyttöä tarkastelemalla havaittiin, että tällaisia piikkejä tulee usein, kun käyttäjämäärät lisääntyvät. Lisäksi kummallekin hälytykselle asetettiin rajoitus, jolla samasta lokaatiosta tulevien hälytysten määrä rajattiin viiteen kappaleeseen ja tämä rajoitus nollattiin kerran päivässä. (Ks. Kuvio 22.)



Kuvio 20. Verkon vasteajan hälytyspohja



Kuvio 21. Sovelluksen vasteajan hälytyspohja



Kuvio 22. Rajoitusmääritykset

6.8.2 Sovellusten hälytysrajat

Kriittisille palveluille suunniteltiin hälytysrajat. Hälytysrajat ovat sovelluskohtaiset, sillä jokainen sovellus toimii eri tavalla, ja palvelimet sijaitsevat eri osissa verkkoa, jolloin ei voida määrittää yhtä tiettyä hälytysrajaa jokaiselle palvelulle. Taulukossa 1 on esitetty kriittisten sovellusten ja palvelinten hälytysrajat. Rajat on valittu sovellusten ja palveluiden keskimääräisten vasteaikojen perusteella sekä kartoittamalla jo tapahtuneita vasteaikojen vaihteluita.

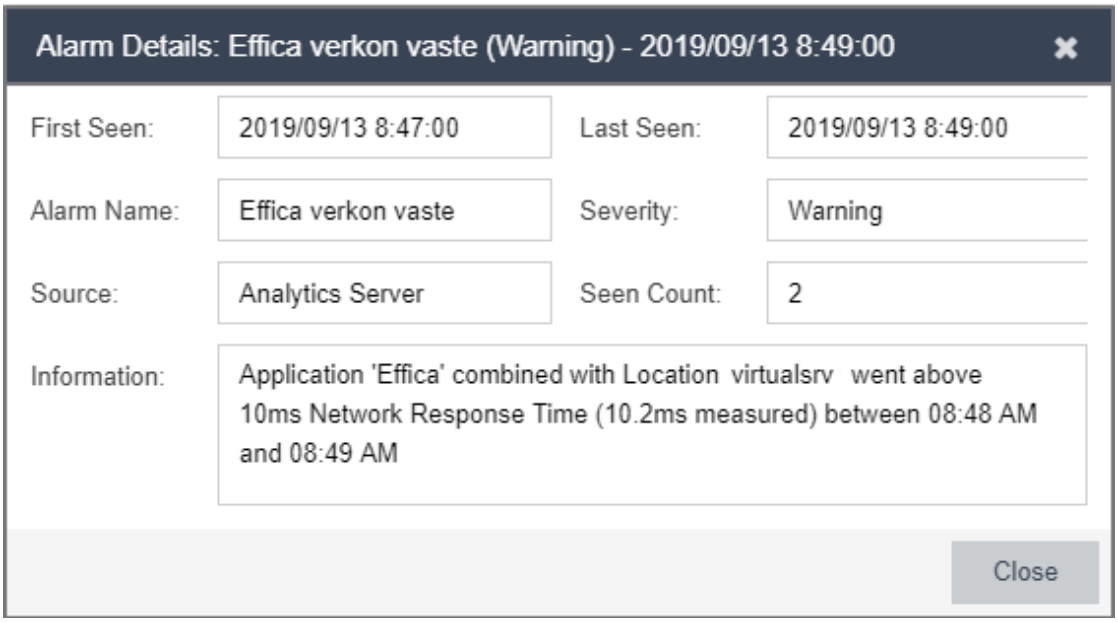
Taulukko 1. Hälytysrajat

Sovellus	**Sovelluksen vasteaika**	**Verkon vasteaika**
Effica	50ms	10ms
Proconsona	25ms	10ms
Teho-osaston sovellus	500ms	10ms
Citrix-palvelimet	60ms	10ms
AD-palvelimet	10ms	2ms
Kerralla-valikko	15ms	5ms

6.8.3 Hälytysten todentaminen

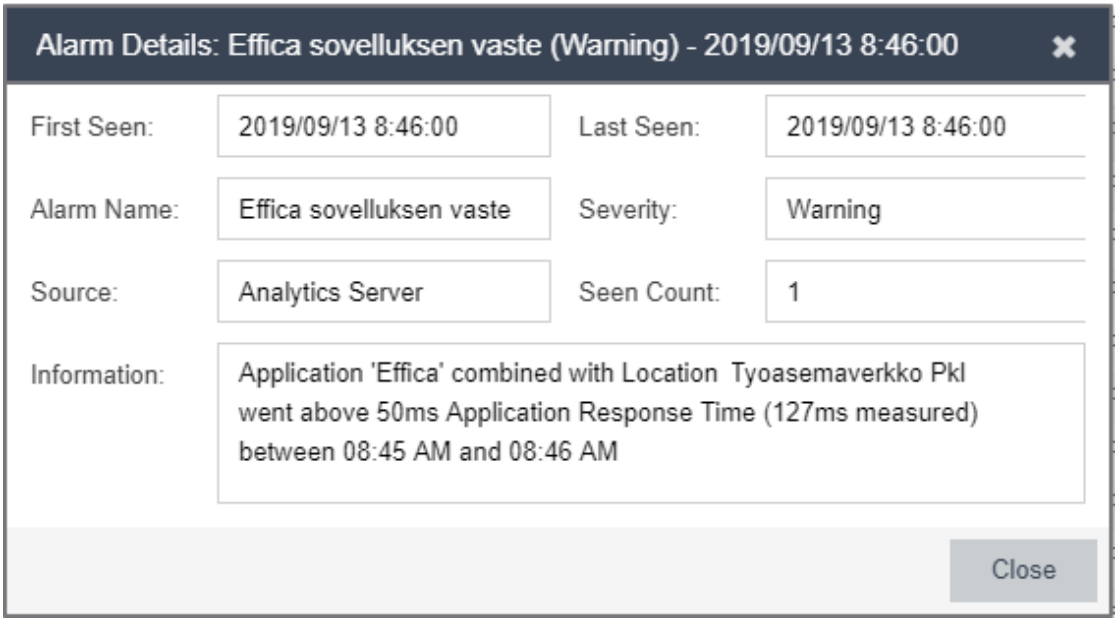
Hälytysten toimivuus todennettiin vielä katsomalla hälytyslistaa. Hyvin nopeasti hälytysten käyttöönoton jälkeen alkoi tulemaan osumia juuri tehtyihin hälytyspohjiin, jolloin voitiin todeta, että pohjat toimivat. Hälytyksestä ilmenee ajankohdat, jolloin raja-arvo on ylittynyt ensimmäisen kerran ja milloin viimeisimmäksi. Lisäksi hälytyksen tiedoissa lukee hälytyksen nimi, vakavuusaste, osumien lukumäärä ja tieto siitä, missä lokaatiossa kyseisen hälytyksen raja-arvo on ylittynyt ja kuinka suuri

vasteaika on ollut. Verkon vasteajalle saatiin heti osuma, jossa asetettu raja-arvo (10ms) oli ylittynyt 0,2 millisekunnilla ”virtualsrv” lokaatiossa. (Ks. Kuvio 23.)



Kuvio 23. Effican verkon vasteajan hälytys

Sovelluksen vasteajan raja-arvon ylittymistä ei myöskään tarvinnut kauaa odottaa. Raja-arvoksi asetettu 50ms ylittyi lokaatiossa ”Tyoasemaverkko Pkl” ja mitattu tulos oli 127ms. (Ks. Kuvio 24.) Koska ylitys oli yli tuplasti korkeampi, saattoi sovelluksen päässä olla jotain ongelmaa tai raja-arvo oli asetettu liian matalaksi.



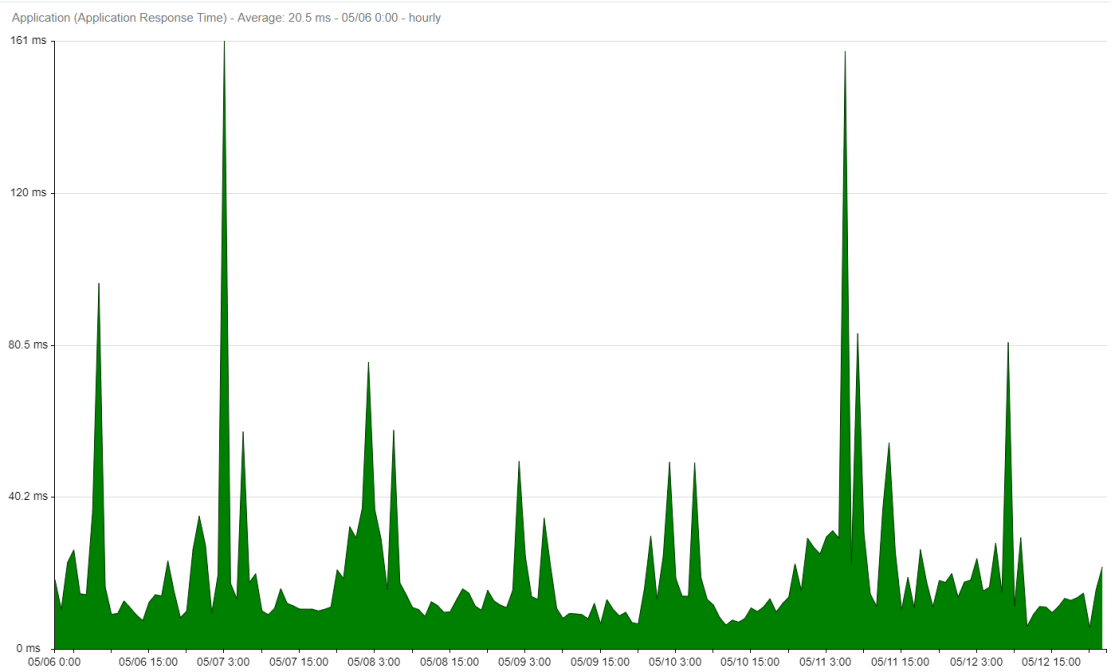
Kuvio 24. Effican sovelluksen vasteajan hälytys

7 Liikenteen normaalitilanne

7.1 Yleistä

Toimeksiantaja oli pyytänyt halutuista palveluista raporttinäkymät, jotka saatiin esille esimerkiksi valvomoon, mutta minkälainen liikennemäärä sitten oli normaalia? Selvät tapaukset oli helppo nähdä suoraan, jolloin esimerkiksi liikennettä ei näkynyt enää ollenkaan tai vasteajat poikkesivat yhtäkkiä todella paljon nykyisestä. Vasteajat vaihtelevat käyttäjämäärän mukaan, jonka vuoksi normaalin tilanteen hahmotteluun oli otettava tarpeeksi pitkä aikaväli. Tarkasteltavaksi ajanjaksoksi valittiin viikko, ja kohteeksi potilastietojärjestelmä Effican tietokanta. Tämä valittiin siksi, koska se oli ympäristössä eniten käytetyin palvelu ja sen toiminta oli erittäin tärkeää liiketoiminnan kannalta.

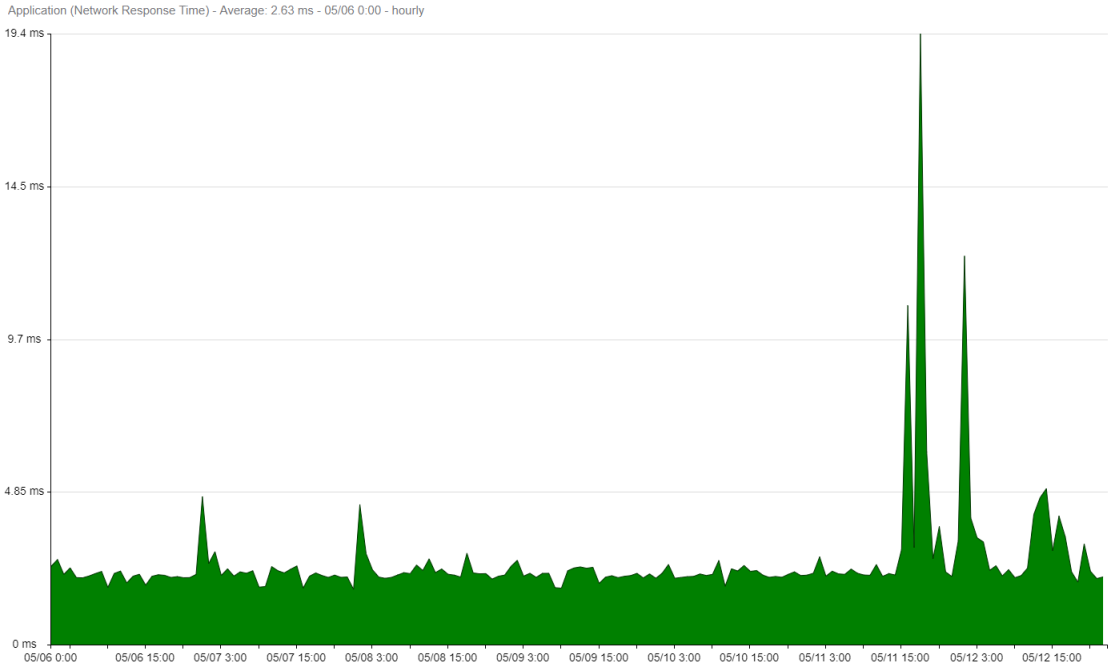
Kuvio 25 on esitetty potilastietojärjestelmän tietokannan sovellusvasteaika viikon ajalta. Vasteajat vaihtelevat käyttäjämäärien mukaan. Kuviosta nähtävät piikit vasteessa öisin johtuvat tietokannalle ajettavista varmuuskopioinneista.



Kuvio 25. Potilastietojärjestelmän tietokannan sovellusvasteaika

Kuvio 26 puolestaan nähdään potilastietojärjestelmän tietokannan verkon vasteaika saman viikon ajalta. Kuviosta voidaan todeta, että verkkoyhteys on ollut melko

tasainen koko viikon ajan. 11.5. kello 15 on kuitenkin tapahtunut jotain, mikä on aiheuttanut korkeampaa vasteaikaa, mutta tilanne on kuitenkin tasoittunut myöhemmin.

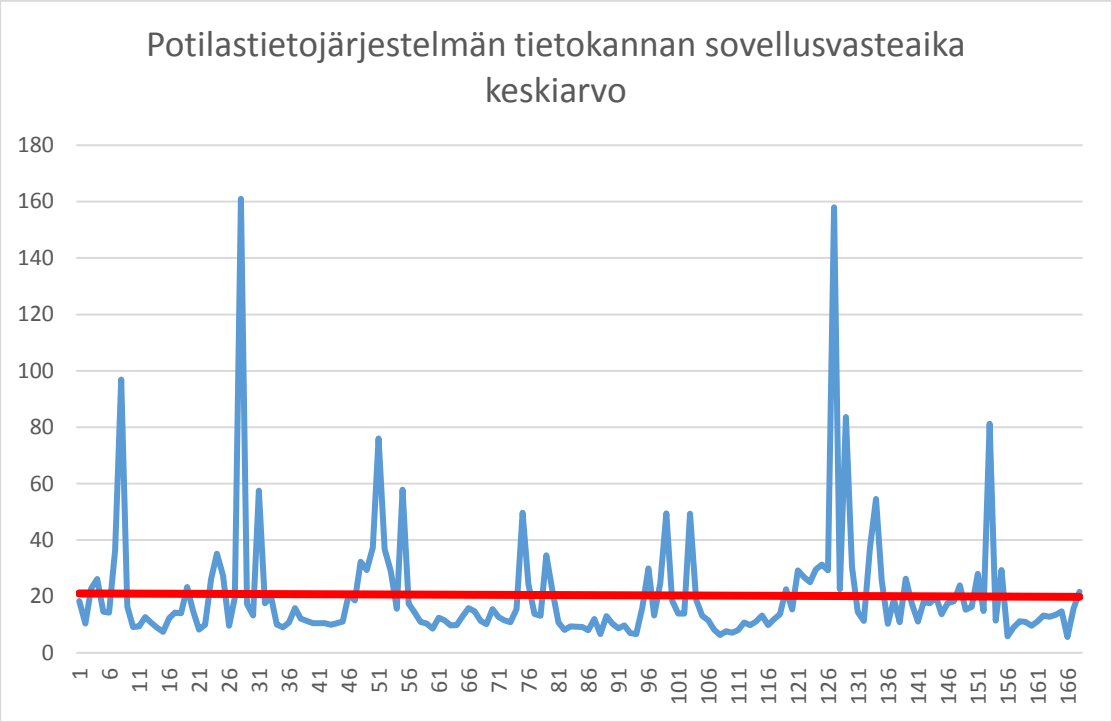


Kuvio 26. Potilastietojärjestelmän tietokannan verkkovasteaika

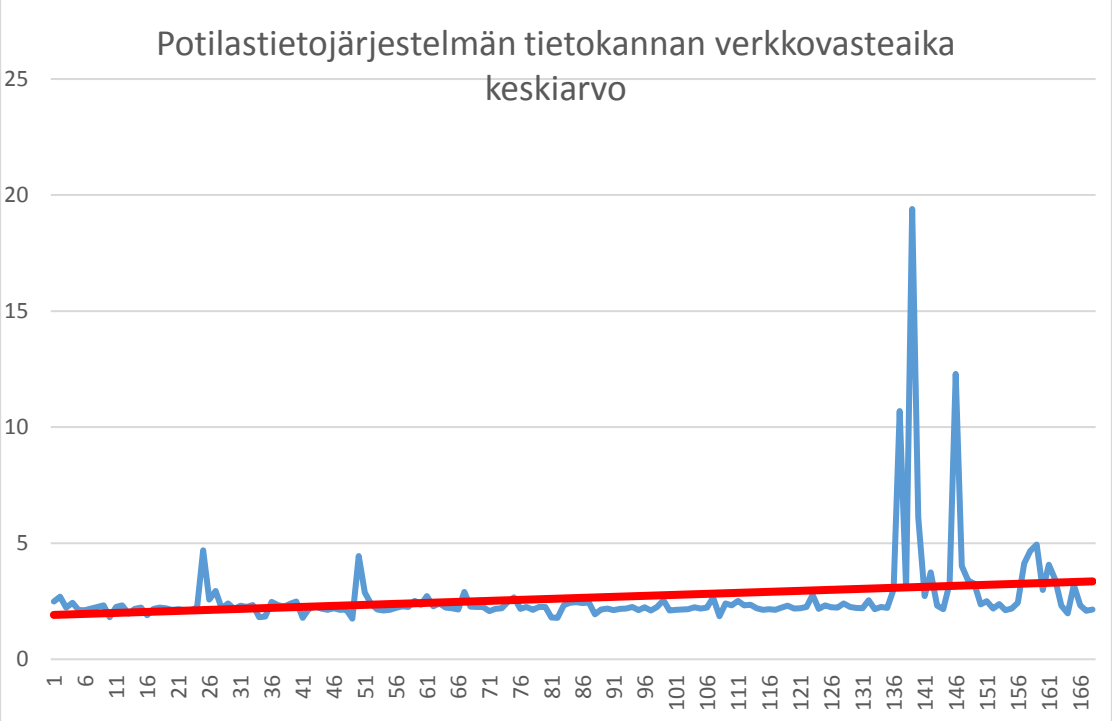
7.2 Keskiarvo

Hyvä lähtökohta määrittää normaali vasteaika-arvo oli laskea vasteaikojen keskiarvo. Keskiarvo laskettiin ottamalla liikennediagrammi viikon ajalta (ks. Kuvio 25. ja Kuvio 26.), johon Extreme Analytics laski jokaisen tunnin osalta keskiarvon liikenteen vasteajoista. Viikon ajalta saatiin hyvä kuva sovelluksen käyttöasteesta, koska luonnollisesti käyttöä on vähemmän öisin ja viikonloppuisin. Tämän pohjalta pystyttiin esimerkiksi asettamaan hälytysraja, jolloin kaikista keskiarvon ylittäneistä arvoista tuli huomautus. Keskiarvo laskettiin sekä sovellus-, että verkonvasteajoille.

Kuvio 27. ja Kuvio 28. on nähtävillä sovellus- ja verkkovasteajan keskiarvot punaisena viivana. Näytteitä viikon ajalta tuli yhteensä 168 kappaletta, yksi jokaiselta tunnilta. Sovellusvasteajan keskiarvoksi saatiin 20,47 ms ja verkon vasteajalle 2,63 ms.



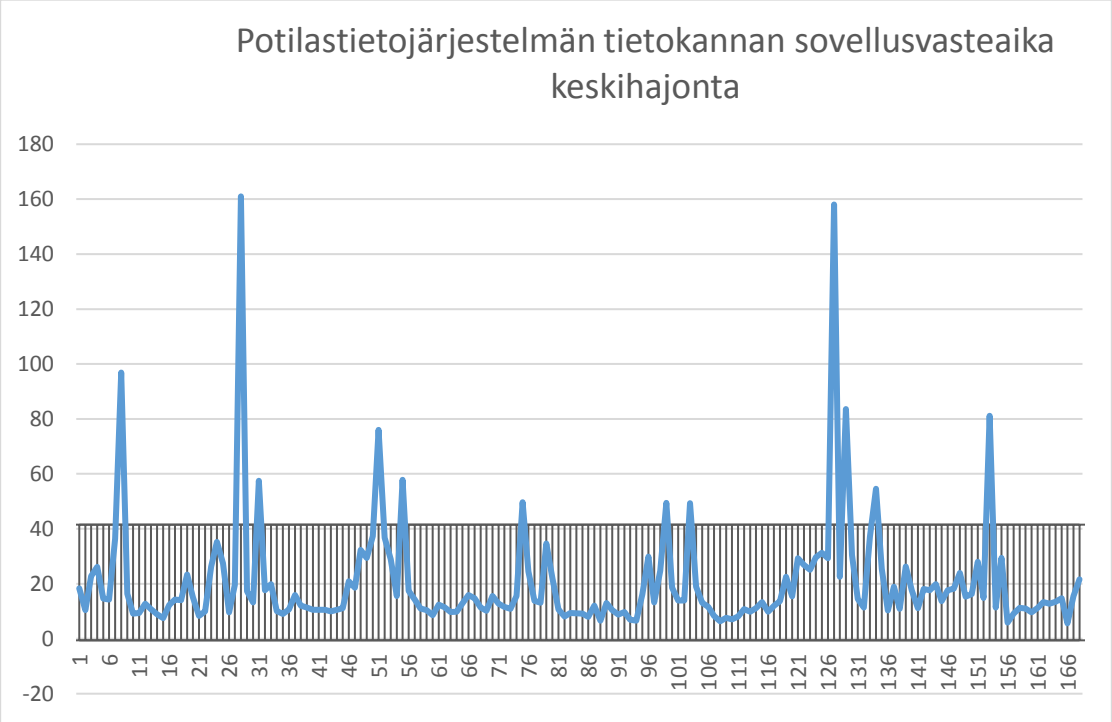
Kuvio 27. Potilastietojärjestelmän tietokannan sovellusvasteaika keskiarvo



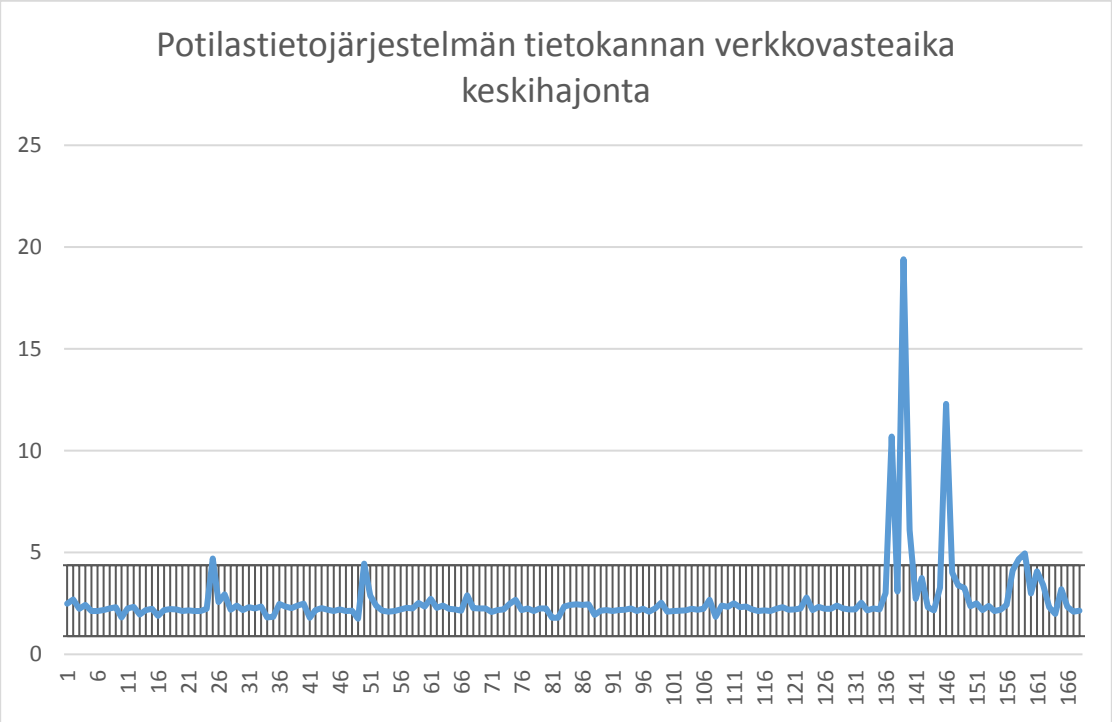
Kuvio 28. Potilastietojärjestelmän tietokannan verkkovasteaika keskiarvo

7.3 Keskihajonta

Keskihajonta kertoo, kuinka paljon arvot keskimäärin vaihtelevat keskiarvosta. Keskihajonta antaa paremman kuvan siitä, minkälaiset arvot ovat vielä niin sanotusti normaaleja, riippuen kuitenkin tilanteesta. Kuvio 29. ja Kuvio 30. nähdään sovellus- ja verkkovasteaikojen keskihajonnat kuvattuna harmaalla alueella. Keskihajonnaksi sovellusvasteajalle saatiin 21,05 ms ja verkkovasteajalle 1,74 ms. Tästä voitiin todeta, että harmaan alueen ulkopuolella olevat arvot vaativat selvitystä ja näiden pohjalta pystyttiin asettamaan rajat hälytyksille. Koska keskihajonnan ulkopuolella olevia arvoja ei ollut kovin paljon, voitiin ajatella, että tässä tapauksessa tilanne saattoi olla normaalia vakavampi.



Kuvio 29. Potilastietojärjestelmän tietokannan sovellusvasteaika keskihajonta



Kuvio 30. Potilastietojärjestelmän tietokannan verkkovasteaika keskihajonta

8 Yhteenveto

8.1 Pohdinta

Opinnäytetyön tavoitteena oli käyttöön ottaa ExtremeAnalytics -laite, joka oli hankittu yritykselle tarkoituksena saada tietoa verkossa olevista ongelmakohdista. Tavoitteena oli tehdä laitteelle konfiguraatioita liittyen käytössä olevien sovellusten, työasemien ja palvelinten tarkkailuun. Lisäksi tavoitteena oli tutustua laitteen tarjoamiin hälytysmahdollisuuksiin, ja hahmotella jonkin sovelluksen ns. normaalitilanne sovelluksen- ja verkon vasteaikojen osalta.

Tutkimustuloksina saatiin reaaliaikaisia näkymiä toimeksiantajan toivomista sovelluksista ja palvelimista. Lisäksi laitteelle tehdyt konfiguraatiot vahvistivat näkemystä sovelluksista, joista yrityksen henkilöstö oli tehnyt ilmoituksia. Konkreettisimpana asiana pystyttiin todistamaan laitteelle tehtyjen konfiguraatioiden perusteella, että potilastietojärjestelmä ProConsonassa oli hitautta lauantaisin.

Opinnäytetyö onnistuttiin toteuttamaan toimeksiantajan toivomalla tavalla. Alkuperäiseen suunnitelmaan, pelkästään sovellusten analysointinäkymien tekoon, saatiin lisäpotkua luomalla hälytyksiä ja kartoittamalla potilastietojärjestelmä Effican normaalitilanne sovelluksen ja verkon vasteaikojen osalta. Normaalitilanne antoi käsityksen asiasta tietämättömälle, minkälainen liikennemäärä on normaalia tavallisissa olosuhteissa.

ESSOTEn verkon hallinta oli ulkoistettu toiselle yritykselle, mikä aiheutti pieniä ongelmia. ExtremeAnalytics -laite kuului heidän laitekantaansa ja verkko- sekä palomuuriavaukset jouduttiin pyytämään ko. yrityksen kautta, mikä aiheutti viivettä työn toteutuksen kannalta.

Työn toteutus oli todella opettavaista ja mielenkiintoista, vaikka sitä joutuikin tutkimaan, suunnittelemaan ja toteuttamaan pääsääntöisesti omatoimisesti. Toimeksiantajan yhteyshenkilö oli kuitenkin mukana prosessissa todella tiiviisti ja innostuneesti, mikä motivoi tekemään työtä intensiivisesti. Lisäksi työn motivaattorina toimi tieto laitteen konkreettisesta avusta yritykselle ja vaikutusta sen liiketoimintaan. Kaiken kaikkiaan työn toteutus sujui mutkitta kaikkien osapuolten välillä ja toimeksiantaja oli todella tyytyväinen tuloksiin.

8.2 Jatkokehitys

Opinnäytetyötä tehdessä ExtremeAnalytics -laite ja sen käyttöliittymä tulivat tutuiksi, minkä johdosta konfiguraatio mahdollisuuksissa ilmeni kehitettävää. Kehitysehdotukset välitettiin toimeksiantajalle, joka välittää ne niin ikään laitteen toimittajalle.

Ensimmäiseksi kehitettävää ilmeni Analytics-välilehden Dashboard:ssa, jossa valmiiksi luotu hallintanäkymä ei pysynyt siinä muodossa, joka siihen jätettiin. Aina käyttöliittymän uudelleen avatessa Dashboard oli palautunut oletusnäkymään, mikä aiheutti lisätyötä. Lisäksi Analytics-välilehden Browser-osiossa tehty analysointinäkymä tyhjeni, jos käytiin jossain muussa käyttöliittymän osassa. Tämä

oli ärsyttävää, sillä esimerkiksi luotua näkymää saatettiin haluta käyttää eri IP-osoitteen hakuun, jolloin jouduttiin aloittamaan pohjan teko taas alusta.

Toiseksi raporttinäkymässä olisi suotavaa olla mahdollisuus valita päivämäärä halutulle näkymälle. Reports-välilehdeltä tarkasteltaessa haluttua näkymää se näkyi siinä ajanjaksossa, joka sille oli määritelty luontivaiheessa.

Viimeiseksi Alerts & Events -välilehden hälytysten luontiin kaivattiin selkeyttä. Hälytyksiä luodessa lokaation valinta täytyi kirjoittaa käsin. Tähän olisi hyvä esimerkiksi alasvetovalikko, jossa olisi listattuna laitteelle luodut lokaatioit. Nyt lokaation valinta oli hieman hankalaa, koska ei ollut tietoa siitä, pitääkö lokaation nimi olla täysin oikein kirjoitettu (isot ja pienet kirjaimet). Tämän vuoksi lokaation oikean nimen tarkistaminen vaati hälytysten luontisivun sulkemista, jolloin työtila tyhjeni, ja takaisin palatessa täytyi aloittaa alusta. Lisäksi, jos jo luodun hälytyksen nimi käytiin vaihtamassa, se ei muuttunut hälytyslistaan, vaikka konfiguraatiossa nimi muuttui.

Lähteet

Deep Packet Inspection. N.d. White paper deep packet inspectionista tec.gov.in -sivustolla. Viitattu 4.2.2019.
http://tec.gov.in/pdf/Studypaper/White%20paper%20on%20DPI.pdf

Endpoint. 2019. Tietoa igel päätteistä igel.com -sivustolla. Viitattu 18.8.2019.
https://www.igel.com/products-hardware/thin-client/

ExtremeAnalytics. 2018. ExtremeAnalyticsin esittelysivu extremenetworks.com -sivustolla. Viitattu 29.1.2019.
https://www.extremenetworks.com/product/extremeanalytics/

ExtremeAnalytics. 2019. Tietopaketti ExtremeAnalyticstä. Viitattu 1.10.2019.
https://kapost-files-prod.s3.amazonaws.com/kapost/55ba7c9e07003d9aab000394/studio/content/57bb6b44a703476ecf000760/published/extremeanalytics-data-sheet.pdf

ExtremeAnalytics User Guide Version 8.2. 2019. Käyttöopas ExtremeAnalyticsiin. Viitattu 8.4.2019.
https://documentation.extremenetworks.com/netsight/8.2/9035979-03_XMC_ExtremeAnalytics_User_Guide_8.2.pdf

ISO/IEC 7498-1:1994. 1994. ISO-standardi. Viitattu 25.3.2019.
https://www.iso.org/standard/20269.html

Jäsenkunnat. 2016. Karttakuva ESSOTEn jäsenkunnista ESSOTEn verkkosivuilla. Päivitetty 18.10.2016. Viitattu 29.1.2019. https://www.essote.fi/tietoa-meista/hallinto-ja-paatoksenteko/jasenkunnat/

Mitchell, B. 2019. Artikkeli verkon monitoroinnista lifewire.com -sivustolla. Viitattu 30.9.2019. https://www.lifewire.com/what-is-network-monitoring-817816

Oros, D. 2016. Artikkeli SNMP:sta auvik.com -sivustolla. Viitattu 30.9.2019.
https://www.auvik.com/franklymsp/blog/network-basics-what-is-snmp/

Parker, J. 2016. Artikkeli SNMP:sta pcwdld.com -sivustolla. Viitattu 30.9.2019.
https://www.pcwdld.com/what-is-snmp-and-tutorial

Raza, M. 2018. Blogi-kirjoitus OSI-mallista bmc.com -sivustolla. Viitattu 25.3.2019.
https://www.bmc.com/blogs/osi-model-7-layers/

Rouse, M. 2017. deep packet inspection (DPI). Artikkeli Deep packet inspectionista techtarget -sivustolla. Viitattu 4.2.2019.
https://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI

Response time (Networking). N.d. Artikkeli verkon vasteajasta what-when-how -sivustolla. Viivattu 3.6.2019. http://what-when-how.com/networking/response-time-networking/

Saurabh, A. 2017. A Guide to Deep Packet Inspection. Artikkeli DPI:stä catchpoint.com -sivustolla. Viitattu 4.2.2019. http://blog.catchpoint.com/2017/07/19/guide-deep-packet-inspection/

Tilinpäätös ja toimintakertomus 2018. 2018. Dokumentti ESSOTEn tilikaudesta 2018 ESSOTEn verkkosivuilla. Päivitetty 5.7.2019. Viitattu 16.9.2019. https://www.essote.fi/wp-content/uploads/sites/2/2019/07/tilinpaatos-ja-toimintakertomus-2018.pdf

Todennäköisyys ja tilastot. N.d. Opetusmateriaali opetushallinnon etälukio sivustolla. Viitattu 3.6.2019. http://www02.oph.fi/etalukio/pitka_matematiikka/kurssi6/maa6_teoria2.html#

What Is The OSI Model?. N.d. Artikkeli OSI-mallista cloudflare.com -verkkosivustolla. Viitattu 25.3.2019. https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/