Niina Koskinen

Tietoverkon palvelujen valvonta

Opinnäytetyö
Kevät 2017
SeAMK Tekniikka
Tietotekniikan tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoverkkotekniikka

Tekijä: Niina Koskinen

Työn nimi: Tietoverkon palvelujen valvonta

Ohjaaja: Alpo Anttonen

Vuosi: 2017 Sivumäärä: 41 Liitteiden lukumäärä: 1

Opinnäytetyön aiheena oli tutustua verkonhallinnan ja -valvonnan osa-alueisiin, tutkia palvelutasosopimuksia ja niiden merkitystä sekä tutustua tietotekniikan saralla yleistyvään palvelulähtöiseen ajatteluun, jossa tietoverkkojen tarjoamat ohjelmistot nähdään aiemmasta poiketen palveluina. Työ tehtiin yhteistyössä Etelä-Pohjanmaan sairaanhoitopiirin tietohallinnon kanssa.

Työn alussa käydään läpi tietoliikennemallit, tietoturvan peruskäsitteistöä sekä palvelulähtöistä ajattelua. Seuraavaksi tutkitaan palvelutasosopimuksia ja verkonhallintaa ja -valvontaa käsitteinä. Kantaa otetaan myös siihen, mitä asioita organisaation olisi hyvä dokumentoida.

Viimeisenä esitellään opinnäytetyön tekijän omasta kiinnostuksesta johtuen ELK Stack, kolmen yhdessä hyvin toimivan ohjelman yhteenliittymä, jolla voidaan esimerkiksi visualisoida Windowsin lokitiedostoja. Tämä ohjelmia koskeva tutustumisprosessi on liitteenä työn lopussa.

Avainsanat: verkonhallinta, verkonvalvonta, palvelutasosopimus, palvelulähtöisyys

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Data Communications Technology

Author: Niina Koskinen

Title of thesis: The supervision of services in information network

Supervisor: Alpo Anttonen

Year: 2017 Number of pages: 41 Number of appendices: 1

The goal of this thesis was to become acquainted with network management and supervision, to go through Service Level Agreements and to study service-oriented thinking, where applications are seen as services. The thesis was conducted in cooperation with the information management of Etelä-Pohjanmaan sairaanhoitopiiri.

First, the network reference models, the basic concepts of information security and service-oriented thinking were studied. Next the service level agreement, network management and network supervision were discussed. Sufficient network documentation was also gone through.

Last, ELK Stack was presented, due to the author's own interest. ELK Stack consists of three smaller programs. With the help of these programs it is possible to visualize, for example, Windows log files.

Keywords: network management, network supervision, Service Level Agreement, service orientation

SISÄLTÖ

Kuva- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

AQL-arvo	Acceptable Quality Limit, haluttu laatuarvo. Huonoin mahdollinen siedettävä palvelun taso.
ARP	Address Resolution protocol. Protokolla, joka kääntää Ethernet-verkossa IP-osoitteet MAC-osoitteiksi.
DHCP	Dynamic Host Control Protocol, protokolla, joka jakaa automaattisesti IP-osoitteet verkossa oleville laitteille.
DNS	Domain Name System, nimipalvelujärjestelmä, joka muuttaa internetosoitteet IP-osoitteiksi.
DSL	Digital Subscriber Line, nippu useampia tieoliikennetekniikoita, joiden avulla dataa siirretään puhelinlinjaa pitkin.
ELK Stack	Elasticsearch, Logstash ja Kibana, kolme avoimen lähdekoodin ohjelmaa, joiden avulla voidaan etsiä, hakea ja visualisoida dataa.
EPSHP	Etelä-Pohjanmaan sairaanhoitopiiri.
Frame Relay	Protokolla, jonka avulla voidaan siirtää dataa lähiverkkojen ja laajaverkkojen välillä.
FTP	File Transfer Protocol, kahden tietokoneen välisen datansiirron mahdollistava protokolla.
Fyysinen rakenne	Kuvaa, miten laitteet on yhdistetty kaapeleilla toisiinsa. Ei ota kantaa datan liikkumiseen laitteiden välillä.
GIF	Graphics Interchange Format, lyhyt, yleensä muutaman sekunnin mittainen liikkuva kuva.
Help desk	Tietotekniikka-asioissa neuvova tukipalvelu.

HTTP	Hypertext Transfer Protocol, internetpalvelimien ja selainten tiedonsiirtoon käyttämä protokolla.
Hot swap	Tekniikka, jonka avulla on mahdollista vaihtaa tai poistaa päällä olevan laitteen komponentti ilman että laitetta tarvitsee sammuttaa.
ICMP	Internet Control Message Protocol. Esimerkiksi reitittimet lähettävät virheilmoituksia tämän protokollan avulla.
IEEE.802.1	Kansainvälinen standardi, jota käytetään todentamiseen portin tarkkuudella WLAN- ja Ethernet-verkoissa.
Indeksointi	Helpotetaan tietynlaisten dokumenttien löytämistä ja tiedonhakua määrittelemällä sisältöä kuvaavia asiasanoja.
Intranet	Organisaation sisäiseen tiedonvälitykseen käytetty verkkopalvelu. Voidaan tarkoittaa myös organisaation lähiverkkoa.
IP-osoite	Verkossa laitteet yksilöivä numerosarja, jonka perusteella data löytää oikeaan laitteeseen.
IPv4	Internet Protocol version 4. IP-protokollan neljäs versio, joka reitittää nykyään suurimman osan internet-liikenteestä.
IPv6	Internet Protocol version 6. Uusin IP-protokollaversio, joka tulee jossain vaiheessa korvaamaan IPv4-version.
ISDN	Integrated Services Digital Network, nippu standardeja, joiden avulla voidaan siirtää yhtäaikaisesti ääntä, videota ja muuta data puhelinverkossa digitaalisesti
JPEG	Yleisin digikuvaformaatti.
Kaistanleveys	Kapasiteetti, jolla bittejä on mahdollista siirtää kahden eri laitteen tai ohjelman välillä.

Latenssi	Aika, joka datalta kuluu edestakaiseen matkaan.
Looginen rakenne	Kuvaa, millä tavoin ja mitä reittejä pitkin data siirtyy verkossa.
MAC-osoite	Media Access Control, osoite, joka yksilöi laitteen siirtoyhteyskerroksella. Ilmoitetaan heksadesimaaleina.
NetBIOS	Network Basic Input/Output System. Mahdollistaa kahden päätelaitteen kommunikoinnin lähiverkossa.
PNG	Kuvaformaatti, jolla on mahdollista rakentaa lähetetty kuva uudelleen täsmälleen samanlaiseksi.
PPP	Point-to-Point Protocol. Käytetään luomaan yhteys kahden noodin eli verkkolaitteen välille.
QoS	Quality of Service, tietoliikenteen luokitelu ja priorisointi. Tärkein osa liikenteestä päästetään läpi isommalla prioriteetillä, jolloin taataan sen laatu. Käytetään esimerkiksi verkkopelaamisessa tai videoneuvotteluissa.
RAID	Redundant Array of Independent Disks, käyttämällä useaa erillistä kiintolevyä kasvatetaan järjestelmän nopeutta ja vikasietoisuutta.
Redundanssi	Päällekkäisyys, ylimäärä. Verkossa on samaan tarkoitukseen ylimääräisiä laitteita, jolloin yhden rikkoutuessa muut jatkavat toimintaansa normaalisti.
SAP	Session Announcement Protocol. Sen avulla voidaan yleislähettää ryhmälähetyksen istuntotietoja.
SLO	Service Level Objective, olennainen osa palvelutasosopimusta: siinä määritellään, millä tavoin tarjotun palvelun tasoa mitataan.

SNMP Simple Network Management Protocol, protokolla, jonka avulla voidaan tarkkailla IP-verkkojen laitteita ja vaikuttaa niiden toimintaan muuttamalla konfiguraatioita.

Tarkistussumma Tiedonsiirrossa käytetty tarkistuskoodi, jonka perusteella voidaan todeta datan mahdollinen siirto- tai tallennusvirheistä johtuva epäeheys.

TCP Transfer Control Protocol, verkossa olevien tietokoneiden välistä liikennöintiä valvova protokolla. Pitää huolta siitä, että data saapuu vastaanottajalle oikeassa järjestyksessä.

UDP User Datagram Protocol, mahdollistaa tiedonsiirron laitteiden välillä ilman yhteyden muodostamista.

Vahva tunnistautuminen Käyttäjän henkilöllisyys varmistetaan kaksivaiheisesti, esimerkiksi verkkopankeissa käytetään käyttäjätunnusta ja henkilökohtaista, vaihtuvaa tunnuslukukorttia.

Varmuuskopiointi Toiminnalle välttämättömän tiedon kopioiminen ja varastoiminen, jotta se on mahdollista palauttaa virhetilanteen sattuessa.

1 JOHDANTO

1.1 Työn tausta

Tietoverkko ja siihen liittyvät resurssit sekä toiminnot ovat yhä yleisempiä ja kriittisempiä organisaation toiminnan kannalta. Verkkojen kasvaessa niistä tulee yhä alttiimpia vioille ja vikatilanteen sattuessa osa verkosta saattaa olla määräämättömän ajan alhaalla tai toimintataso voi laskea liian alhaiseksi. Tästä aiheutuu pahimmillaan toimintojen hidastumista ja ansionmenetyksia. Tällaisten suurten verkkojen ylläpito edellyttää organisaatiolta hyvin toteutettua verkonhallintaa. (Stallings 1997, 1.) Esimerkkinä mainittakoon sairaanhoitopiirin tapauksessa potilastietojärjestelmän toiminta, jonka ollessa alhaalla terveydenhoitoyksiköiden toiminta käytännössä seisahtuu kokonaan.

Eri käyttäjäryhmillä on yleensä hyvin erilaisia käsityksiä toimivasta verkonhallinnasta. Ylläpitäjät peräänkuuluttavat tietoverkon turvallisuutta ja kykyä seurata reaaliaikaisesti verkon tilaa, kuten vasteaikoja. Verkon skaalautuvuus ja muunneltavuus ovat tärkeitä, samoin kuin automaattisuus. Peruskäyttäjä taas haluaa, että heille ilmoitetaan heti viasta, joka vaikuttaa koneen tai laitteen toimintaan. (Hautaniemi 1994.)

1.2 Työn tavoite

Opinnäytetyön tavoitteena on käsitellä nykyistä tietotekniikan rakennemuutosta tietojärjestelmästä palveluihin, selvittää, miksi palvelutasosopimukset ovat nykyään entistä tärkeämmässä roolissa sekä käydä läpi verkonvalvonnan ja -hallinnan erilaisiin käytännöt. Esimerkkinä verkonvalvonnan ja -hallinnan saralta toimii ELK Stack-ohjelmiston tarkastelu.

1.3 Työn rakenne

Aluksi tutustutaan pääpiirteittäin tietoliikennemalleihin ja eri kerroksissa toimiviin protokolliin. Sen jälkeen tarkastelun kohteena ovat tietoturvan perusvaatimukset, verkon dokumentoinnin tärkeys ja palvelulähtöinen ajattelu sekä IT-palveluiden tasoa valvovat sopimukset. Lopussa tutustutaan vielä verkonhallinnan ja -valvonnan tärkeimpiin osa-alueisiin sekä ELK Stackiin, jolla on mahdollisuus valvoa verkkoa monipuolisesti. Viimeisinä ovat pohdinta ja johtopäätökset.

1.4 Organisaatioesittely

Etelä-Pohjanmaan sairaanhoitopiiri koostuu 18 jäsenkunnasta, joissa asukkaita on yhteensä noin 200 000. Sairaanhoitopiiri huolehtii yhteistyössä sosiaalitoimen kanssa asukkaiden perusterveydenhuollosta ja tuottaa myös erikoissairaanhoidollisia palveluita. Keskussairaala sijaitsee Senäjoella, lisäksi jäsenkunnissa on useita psykiatrisia avohoitoyksiköitä. (EPSHP [Viitattu 2.11.2016].) Vuonna 2014 sairaanhoitopiirin toimintakulut olivat 267 miljoonaa euroa. Henkilöstöä oli töissä vuonna 2014 noin 3300, mukaan laskettuna myös sijaisuudet. (EPSHP [Viitattu 3.11.2016].)

Organisaatio koostuu useasta toiminta-alueesta, jotka on jaettu edelleen vastuu- ja toimintayksiköihin. Tietohallinto toimii hallintopalveluiden toiminta-alueen alaisuudessa. (EPSHP [Viitattu 4.11.2016].)

2 TIETOLIIKENNEMALLIT

Vekon kautta käyttäjät pääsevät käsiksi useisiin ominaisuuksiin, kuten palvelimilla sijaitseviin sovelluksiin (Edwards & Bramante 2009, 5). Tässä luvussa tutustutaan tietoliikennemalleihin ja siihen, mitä muutoksia ja vaiheita data käy läpi liikkuessaan lähettäjältä vastaanottajalle.

2.1 TCP/IP

Internetissä tapahtuva tiedonsiirto pohjautuu TCP/IP-protokolliin. TCP-protokolla hoitaa siirrettävän datan pilkkomisen pienempiin osiin ja IP-protokolla vastaa siitä, että datapaketit pääsevät oikeaan kohteeseen. TCP/IP mahdollistaa useiden sovellusten, kuten etäkäytön, sähköpostin, internetselainten ja tiedostonsiirron käytön. (Edwards & Bramante 2009, 53, 55.)

2.2 OSI-malli

TCP/IP-mallin ohelle kehitetty OSI-malli kuvaa tiedonsiirtoprotokollat seitsemässä eri tasossa TCP/IP-mallin neljän kerroksen sijaan. OSI-malli kuvaa eri kerrosten välisen kommunikoinnin ja toiminnan ylemmän ja alemman kerroksen välillä, eli sen, miten data liikkuu päätelaitteelta toiselle. (Crawley 2012.) Kerroksiin viitataan yleensä numeron perusteella. Kerrokset on seuraavaksi esitelty numerojärjestyksessä seitsemännestä alkaen (Cisco [Viitattu 13.3.2017], 3.2.4.2).

Taulukko 1. OSI-mallin protokollat.
(Crawley 2012; Cisco [Viitattu 13.3.2017], 10.1.1.1)

OSI-malli	Protokollat
7. Sovelluskerros	**SNMP, HTTP, DNS**
6. Esitystapakerros	**GIF, JPEG, PNG**
5. Istuntokerros	**NetBIOS, SAP**
4. Kuljetuskerros	**TCP, UDP**
3. Verkkokerros	**IPv4, IPv6, ICMP, ARP**
2. Siirtoyhteyskerros	**PPP, Frame Relay**
1. Fyysinen kerros	**DSL, ISDN**

Seitsemäs kerros eli **sovelluskerros** on lähimpänä käyttäjää tarjoten rajapinnan sovellusten ja verkon välille, jotta datan siirto on mahdollista. Sovelluskerros mahdollistaa verkkoyhteyttä tarvitsevien kokonaisuuksien, kuten tiedonsiirron ja verkkopalvelujen toiminnan. (Crawley 2012.) Tunnettuja sovelluskerroksen protokollia ovat esimerkiksi HTTP (Hypertext Transfer Protocol), joka määrittelee tekstin, kuvien, videoiden ja muun multimedian esittämisen internetissä, ja DNS (Domain Name System), joka kääntää internetosoitteet IP-osoitteiksi (Cisco [Viitattu 13.3.2017], 10.1.1.3).

Esitystapakerroksen tehtävänä on valmistella alemmilta kerroksilta saapuva data sovelluskerroksen ymmärtämään muotoon. Tässä kerroksessa tapahtuu myös tarvittaessa datan salaaminen ja salauksen purku. (Crawley 2012.) Esimerkkejä esitystapakerroksen protokollista ovat GIF ja JPNG (Cisco [Viitattu 13.3.2017], 10.1.1.2).

Istuntokerros luo ja pitää yllä kohde- ja lähdesovellusten välisiä dialogeja, pitää ne aktiivisena ja uudelleenkäynnistää ne istunnot, jotka ovat olleet toimettomina tietyn aikaa tai keskeytyneet (Cisco [Viitattu 13.3.2017], 10.1.1.2). Istuntokerros kontrolloi lisäksi dupleksointia eli kahdentamista ja uudelleenkäynnistyksiä. Tällä kerroksella tapahtuu myös kättely, eli yhteyden luominen kahden laitteen välille. (Crawley 2012.)

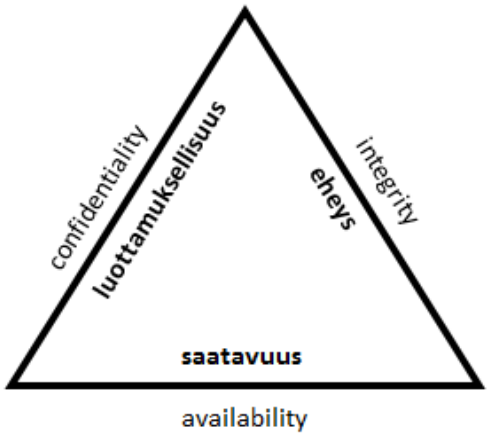
Kuljetuskerros huolehtii monen yhtäaikaisen yhteyden ylläpitämisestä, jotta useampi sovellus kykenee kommunikoimaan verkon yli samanaikaisesti (Cisco [Viitattu 13.3.2017], 9.1.1.1). Lisäksi kuljetuskerros huolehtii vuon ohjauksesta, luotettavsta datansiirrosta lähettäjän ja vastaanottajan välillä ja siitä, että data saapuu vastaanottajalle sopivissa osissa. Kuljetuskerroksen dataa kutsutaan segmenteiksi. Tunnetuimpia kuljetuskerroksen protokollia ovat TCP ja UDP. Ensiksi mainittua protokollaa käytetään, kun tarvitaan varmistusta datan perillepääsystä. TCP lähettää mahdollisesti kadonneen datan uudelleen kohteeseensa, samalla voi kuitenkin esiintyä hitautta. UDP on parempi vaihtoehto, kun latenssi on pakettihäviötä isompi ongelma, kuten esimerkiksi VoIP-puhelimissa ja verkkopelaamisessa. (Crawley 2012.)

Verkkokerros muodostaa yhteyden kahden eri verkossa olevan verkkoaseman välille. Reitittimet toimivat tässä kerroksessa ja määrittelevät, mitä kautta paketit toimitetaan vastaanottajalle. Dataa kutsutaan paketeiksi. (Crawley 2012.) Verkkokerros vaatii jokaiselle päätelaitteelle uniikin IP-osoitteen, jotta tietty laite on mahdollista identifioida. Tässä lisätään datapakettiin lähettävän ja vastaanottavan osapuolen IP-osoitetiedot ja datapaketin saapuessa kohteeseensa vastaanottajakone tarkistaa, vastaako datan IP-osoite sen omaa osoitetta. Mikäli näin on, IP-otsake poistetaan paketista ja paketti puretaan välitettäväksi alemmille kerroksille. (Cisco [Viitattu 13.3.2017], 6.1.1.1-6.1.1.3.)

Siirotyhteyskerros hoitaa kahden samassa verkossa olevan laitteen liikennöinnin. Tässä kerroksessa toimivat MAC-osoitteet ja Ethernet-protokolla. Siirtoyhteyskerros suorittaa myös virhehavainnointia ja -korjausta ja mahdollistaa luotettavan datansiirron. (Oulun yliopisto 2014/2015). Data on tässä kerroksessa nimeltään kehys (Crawley 2012).

Fyysisellä kerroksella määritellään tiedonsiirron laitteiden elektroniset ja fyysiset ominaisuudet, kuten oikeanlainen kaapelointi ja oikeat liittimet Dataa kutsutaan tässä kerroksessa biteiksi. Fyysinen kerros muuntaa siiroyhteyskerrokselta saapuneen datakehyksen vastaanottavan laitteen ymmärtämäksi signaalisarjaksi. (Crawley 2012.) Fyysisen kerroksen data jaetaan pääosin kolmeen eri muotoon: kuparikaapelissa signaalit ovat sähköisiä pulsseja, optisessa kaapelissa valoa ja langattomassa mikroaaltoja. (Cisco [Viitattu 13.3.2017], 4.1.2.1-4.1.2.2.)

3 TIETOTURVAN PERUSVAATIMUKSIA



Kuva 1. CIA-kolmio.
(Rouse 2014)

CIA-kolmio kuvaa osioita, joita pidetään perustavanlaatuisimpina asioina organisaation tuvallisuusnäkökulmasta katsottuna (Rouse 2014).

Luottamuksellisuus-termiä voidaan pitää osin verrattavana yksityisyyteen ja sen takia tehdään toimenpiteitä, joiden on tarkoitus estää tietoa päätymästä vääriin käsiin. Näihin toimenpiteisiin kuuluvat tietoihin pääsyn rajaaminen vain niille henkilöille, joille se on tarpeellista. Data voidaan myös erotella kategorioittain sen mukaan, kuinka vahingollista sen pääsy vääriin käsiin olisi ja määritellä suojaustoimenpiteet sen mukaan. Keinoja säilyttää datan luotettavuus ovat mm. datan kryptaus, käyttäjätunnukset ja vahva tunnistautuminen. (Rouse 2014.)

Tiedon eheys voidaan käsittää tiedon yhtenäisyytenä ja paikkaansapitävyytenä sen koko elinkaaren ajan. Dataan ei saa tullan siirron aikana muutoksia, eikä sitä saa päästä muuttamaan kukaan ulkopuolinen. Tämä pyritään varmistamaan kansioiden oikeuksilla ja pääsyn rajaamisella (esimerkiksi intranet, kampusten verkot). Ohjelmistojen versiokontrolli auttaa, ettei tieto muutu vahinogssa vanhan ohjelman takia. Lisäksi voidaan käyttää tarkistussummia eheyden varmistamiseen. Hyvä ja säännöllinen varmuuskopiointi suojaa organisaatiota tiedon menetykseltä. (Rouse 2014.)

Saatavuutta toteutetaan pitämällä laitteistot kunnossa ja korjaamalla tai korvaamalla ne heti vian sattuessa. Riittävä kaistanleveys, verkon pullonkaulojen välttäminen, redundanssi, RAID-järjestelmä ja nopea palautusohjelmisto auttavat tavoitteeseen pääsyssä. (Rouse 2014.)

4 VERKON DOKUMENTOINTI

Tietojärjestelmän muuttuvat nykyisin nopealla tahdilla ja muutosten perässä voi olla vaikea pysyä. On tärkeää dokumentoida ja merkitä ylös kaikki muutokset heti niiden tapahduttua, jotta verkon ylläpitäjät pysyvät ajan tasalla siitä, miten verkko on rakennettu. Huono dokumentointi voi johtaa hallitsemattomiin muutoksiin ja vianhallinnan hankaloitumiseen. Jokaisessa tietojärjestelmässä esiintyy jossain vaiheessa sen elinkaarta vikoja, eikä niitä voida täysin ehkäistä. On kuitenkin tärkeää pyrkiä ehkäisemään häiriöitä ja vikoja mahdollisimman tehokkaasti etukäteen. Vikatilanteiden tehokas selvittely vaatii ylläpitäjiltä riittävää tuntemusta järjestelmästä. Jaakohuhta (2005, 324-325) määrittelee ratkaisevat asiat, jotka organisaatiolla tulisi vähintään olla tiedossa:

- järjestelmän rakenteesta ajan tasalla oleva dokumentaatio
- tiedot laitteiden ja ohjelmistojen maahantuojista ja toimittajista
- tieto varaosien saatavuudesta
- tieto palveluiden saatavuudesta
- perusvälineet välittömien vikojen tunnistamiseksi
- taito tunnistaa ja korjata vikoja. (Jaakohuhta 2005, 324-325.)

Tässä yhteydessä kaikkia asiakirjoja, joista ilmenee tietojärjestelmän ajantasainen rakenne ja komponenttien toiminta, kutsutaan dokumentoinniksi. Jokainen organisaatio vastaa itse dokumentoinnin toteuttamisesta. Perusteellinen dokumentointi parantaa verkon käytettävyyttä vikaselvitysten lyhenemisellä, helpottuneella suunnittelulla, paremmalla turvallisuustasolla ja helpottuneella käyttöönotolla. Dokumentointi vie aikaa ja resursseja, mutta on hyödyksi siinä vaiheessa, kun jotain ikävää tapahtuu. Se jaetaan usein kahteen pääosaan: loogiseen ja fyysiseen dokumentaatioon. Ensiksi mainittu selventää millä tavoin data liikkuu verkossa, kun taas fyysinen rakenne kertoo, missä komponentit sijaitsevat. Organisaation kannalta keskeisiksi Jaakohuhta (2015, 325-327) luettelee mm. seuraavat kategoriat:

- kaapelointi
- johtotiet
- jakamot
- liitännät
- verkkolaitteiden konfiguraatiot
- WLAN-tukiasemat
- palvelimet

- sovellukset
- UPS-järjestelmät
- varmistusmenetelmät
- päätelaitteet
- laitteiden MAC- ja IP-osoitteet
- laitteiden käyttöjärjestelmäversiot. (Jaakohuhta 2015, 325-327.)

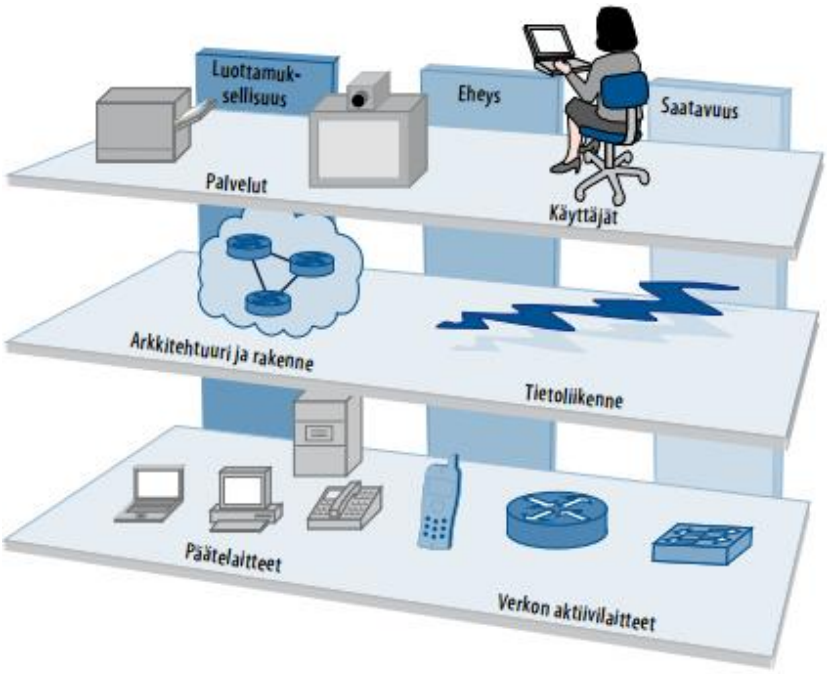
Dokumentointia aloitettaessa kannattaa kuitenkin harkita, mitkä tiedot ovat tarpeellisia. Vaarana on liika alkuinnostus, jonka jälkeen dokumentointi voi jäädä puolitiehen siitä aiheutuvan työmäärän vuoksi. Dokumentointitarkkuuden laajentaminen yhdenkin kohteen verran lisää työtaakkaa moninkertaisesti. (Jaakohuhta 2005, 326.) Hyvä dokumentaatio on mm. yhdenmukainen, sisältää asianmukaiset viittaukset muihin dokumentteihin, se on helposti muokattava, selkeä ja taloudellisesti koottu (Jaakohuhta 2005, 329).

5 PALVELULÄHTÖINEN AJATTELU

Varjo ja Lusch ovat vuonna 2004 (1-2) tuoneet esille markkinoinnin olevan murroksessa ja siirtyvän tuotekeskeisyydestä palvelukeskeisyyteen, jonka keskiössä ovat ihmissuhteet, aineettomuus ja kaupantekoprosessi. Tässä ajattelumallissa palvelun määritellään tarkoittavan erikoislaatuista kompetenssiä: taitoja ja tietoa, joita jokin taho voi hyödyntää. Resursseina pidetään aiemmasta käsityksestä poiketen myös ihmisen kyvykkyyttä suoriutua asioista. Tällöin resurssit eivät ole muuttumattomia. Palvelukeskeinen ajattelu sisältää ajatuksen jatkuvasta oppimisesta.

5.1 Palvelulähtöinen ajattelu tietotekniikassa

Tietotekniikankin saralla ollaan siirtymässä ajattelumalliin, jossa verkkoa kuvataan palvelulähtöisesti erillisten ohjelmistojen ja järjestelmien sijaan. Palvelulähtöisessä ajatusmallissa täytyy verkossa toteutua kolmannessa luvussa mainitut luottamuksellisuus, eheys ja saatavuus. Nämä on havainnollistettu kuvan 2 pystypalkkeina tarkoittaen, että kaikki verkon tasot toteuttavat osaltaan näitä vaatimuksia. Ajattelumallissa verkkolaitteilla ei ole perinteisiä rooleja, vaan palvelun toteuttamiseen voi osallistua useampikin palvelin tai asiakas. (Valtiovarainministeriö 2010, 29-30.)



Kuva 2. Luottamuksellisuus, eheys ja saatavuus verkon eri tasoilla. (Valtiovarainministeriö 2010, 29)

Tässä ajatusmallissa kaikki verkon resurssit, kuten sähköposti, intranet ja verkkotulostus ovat käyttäjän näkökulmasta palveluita. Käyttäjälle olennaista tietoa ovat palvelun tarkoitus, sinne pääsy ja sen käyttö. Palvelutasolla luottamuksellisuus ja eheys varmistetaan salauksella, lokituksella ja käyttäjähallinnalla palvelukohtaisesti. (Valtiovarainministeriö 2010, 30-31.)

Päätelaitteet tarjoavat rajapinnan, jonka kautta käyttäjä pääsee käsiksi verkon tarjoamiin palveluihin. Päätelaite voi myös olla osallisena palvelun tuottamisessa, mutta tämä ei näy käyttäjälle. Päätelaitteen käyttäjänhallinnan avulla varmistetaan eheys ja luottamuksellisuus, tarvittaessa käytetään myös salausta ja lokeja. Päätelaitteiden saatavuus varmistetaan käyttämällä verkossa toimivia palveluita, jolloin päätelaitteelta ei edellytetä vaativampaa logiikkaa. Mikäli tällaista logiikkaa vaaditaan, saatavuusongelmat hoidetaan varalaitejärjestelyllä. Verkossa on lisäksi aktiivilaitteita, joiden tarkoitus on mahdollistaa tiedonsiirto. Tässä tapauksessa saatavuus on varmistettava kahdennuksilla, hot-swap-komponenteilla sekä varmennetulla virransyötöllä. Luottamuksellisuuden ja eheyden kriteerit täytetään jälleen kerran käyttäjänhallinnalla ja rajaamalla asiattomien henkilöiden pääsy laitetiloihin. (Valtiovarainministeriö 2010, 30-31.)

Verkon fyysinen ja looginen rakenne voidaan nivoa yhteen verkon arkkitehtuurin käsitteeseen, joka käsittää verkon näistä osista muodostuvana kokonaisuutena. Loogiselta rakenteeltaan verkko voi koostua useammasta fyysisestä osasta, esimerkiksi lankaverkosta ja langattomasta verkosta. Fyysinen verkko taas voidaan pilkkoa useampaan itsenäiseen kokonaisuuteen, virtuaaliverkkoihin. (Valtiovarainministeriö 2010, 30-31.)

Reittien kahdennus ja hyvin vikoja sietävät, laadukkaat teknologiaratkaisut pitävät yllä tiedon saatavuutta. Kaapelien suojauksella ja muilla fyysisillä ratkaisuilla varmistetaan luottamuksellisuus ja eheys. (Valtiovarainministeriö 2010, 30-31.)

Verkkoon kytkettyjen laitteiden kommunikoinnin mahdollistaminen on verkon ydintehtävä. Tiedonsiirron välineinä palveluntarjoajan ja rajapinnan välillä toimivat tietoliikenneprotokollat. Saatavuuteen vaikuttavat huolella tehdyt, oikeat protokollavalinnat. Järkevästi toimiva reititysprotokolla osaa vikatilanteessa ohjata datapaketit kohteeseensa mahdollista vaihtoehtoista reittiä pitkin. Koska tavallisimmat TCP/IP-protokollat eivät takaa tiedon luottamuksellisuutta ja eheyttä, rinnalla käytetään erilaisia verkkoliikenteen salauskeinoja. Eheys varmistetaan ennen kahden osapuolen välistä tiedonsiirtoa tapahtuvalla tunnistautumisella. (Valtiovarainministeriö 2010, 30-31.)

5.2 Palvelu- ja tietojärjestelmäintegraatio sosiaali- ja terveyspalveluissa

Palveluintegraatiossa asiakas otetaan mukaan toimintaan ja hänet nähdään palvelun kehittämisen kannalta resurssina. Palveluintegraatio jaetaan vertikaaliseen ja horisontaaliseen integraatioon. Horisontaalinen palveluintegraatio on kyseessä, kun kaksi erillistä sosiaali- tai terveyspalveluorganisaatiota yhdistetään yhdeksi isommaksi toimivaksi kokonaisuudeksi vastaamaan asiakkaan palvelutarpeita. Laajemmin ajateltuna vertikaalinen integraatio pitää sisällään yhtenäisen palvelukokonaisuuden lisäksi sosiaali- ja terveyspalvelujen politiikkasuunnittelun, taloudelliset resurssit ja informaatio-ohjauksen. (Virtanen, Smedberg, Nykänen & Stenvall 2017, 6.)

Tietojärjestelmäintegraatiossa tavoitellaan tiedon siirtymistä saumattomasti tietojärjestelmästä toiseen niin vertikaalisten kuin horisontaalistenkin integraatioiden välillä. Kyse ei ole varsinaisesta tietojärjestelmien yhdistämisestä, kuten integraatio-sanana yleensä ymmärretään. Tietojärjestelmäintegraation jälkeenkin järjestelmät ovat edelleen erillisiä, mutta ne voivat kommunikoida keskenään ja vaihtaa tietoa. Esimerkkinä tästä on valtakunnallinen Kanta-palvelu, johon pyritään myöhemmin liittämään sosiaalihuollon valtakunnallinen arkistopalvelu. Näin saataisiin aikaan potilaiden asiakastiedot sisältävä yhtenäinen palvelu. Kannassa on puolestaan sertifioituna useita asiakastietojärjestelmiä. Palvelujärjestelmän uudistamisen näkökulmasta tietojärjestelmät nähdään palvelujen järjestämisen toteuttajina ja mahdollistajina. (Virtanen, Smedberg, Nykänen & Stenvall 2017, 6; 9.)

Kun halutaan kehittää tieotjärjestelmiä nykytarpeita vastaaviksi, on keskiössä johdonmukaisuus ja yhteiset tavoitteet. Kyse on pitkän aikavälin työstä, jossa on kiinnitettävä huomiota avoimiin rajapintoihin, eri järjestelmien väliseen vuoropuheluun sekä tiedon käytettävyyteen ja avoimuuteen yleisellä tasolla. (Virtanen, Smedberg, Nykänen & Stenvall 2017, 57.)

6 ULKOISTAMINEN JA SOPIMUKSET

IT-alalla on nykyisin tarjolla monia erilaisia ohjelmistoratkaisuja ja uuden teknologian tai ohjelman käyttöön ottaminen on aiempaa helpompaa. Uudistusten lomassa unohdetaan usein ajatella kauaskantoisemmin esimerkiksi sitä, miten uudistukset pitäisi ottaa huomioon liiketoimintamielessä. Tarvitaan korkeatasoisempia rakenteellisia muutoksia, jotta osataan arvioida tehokkaammin teknologian vaikutusta liiketoimintaan ja tehokkuuteen. Neljännessä luvussa käsitelty palvelulähtöinen ajattelu onkin seurausta tästä ilmiöstä. Kun palveluajattelua tuodaan yrityksiin, tarvitaan entistä tehokkaampia ja monipuolisempia tulosmittauksen menetelmiä määrittelemään, miten hyvin palvelu tuo lisäarvoa organisaatiolle. Yrityksen toimintaa ja palveluiden tasoa mitattiin aiemmin vain finanssinäkökulmasta, eikä se enää riitä. (McWhirter & Gaughan 2012, 12-13.)

Yhä harvempi organisaatio pystyy tarjoamaan ja toteuttamaan kaikki tarvittavat palvelut yksin. Ulkoistamisella tavoitellaan laadukkaampia palveluita ja kustannussäästöjä. Ulkoistamisen suurimmat riskit ovat, että aiemmin muualta tilatun tai itse toteutetun palvelun taso huononee, tai että tavoiteltuja kustannussäästöjä ei saavuteta. (Desai 2010, 12). Lisäksi paineet organisaatioita kohtaan ovat nykyisellään hyin suuria ja menestymisen takeeksi vaaditaan yhtenäinen strategia, jota toteutetaan saumattomasti (Okes 2013, 1).

6.1 Prosessiajattelu

Yksinkertaisimmillaan prosessi on sarja aktiviteetteja, joiden tarkoitus on muuttaa siihen käytetyt panokset saatavilla olevia resursseja hyödyntäen halutuksi lopputuotteeksi. Sairaalaympäristöön sopiva prosessiajattelun esimerkki voisi olla seuraavanlainen: toimeksiannon saajana toimii lääkärin vastaanotto, panoksena hoitoa tarvitseva potilas, itse prosessi sisältää diagnoosin teon ja sairauden hoidon ja lopputuotteena on hoidettu potilas. (Okes 2013, 3,5.)

6.2 Metriikka

Metriikka koostuu erilaisista mittaustuloksista, joilla esimerkiksi arvioidaan palvelun tehokkuutta ja toimintaa. Kerättyjen metriikkatietojen avulla voidaan kartoittaa, onko vaadittavat odotukset ja tavoitteet täytetty. Metriikka on arvokasta tietoa ja siitä voidaan hyötyä usealla tavalla: voidaan arvioida organisaation tai yrityksen kypsyyttä, muuttaa tai ohjata henkilökunnan käytöstä, löytää uusia kehitysmahdollisuuksia ja perustella muutoksia. Ilman minkäänlaisia mittaustuloksia prosessien senhetkisestä tehokkuudesta, perustuu päätöksenteko ja tieto marginaaliselle osalle ihmisistä ja pahimmassa tapauksessa vain arvailujen varaan. (McWhirter & Gaughan 2012, 7.)

Metriikka ei automaattisesti tuota lisäarvoa, vaan tulosten analysointi vaatii ymmärrystä kaivatuista tuloksista ja tavoitteista. Tämän takia metriikoille määritellään AQL-arvo eli haluttu laatuarvo. Tämän arvon tulee perustua palvelulta tai prosessilta odotettuihin asioihin. (McWhirter & Gaughan 2012, 7.)

6.3 Palvelutasosopimukset

SLA (Service Level Agreement) eli palvelutasosopimus on palveluntarjoajan ja palvelun hankkijan välinen sopimus, joka määrittelee palvelulta odotetun tason. Palvelutasosopimuksen päätarkoitus on määritellä, mitä tilaaja saa tilatessaan palvelun. Sopimus ei itsessään määrittele, miten palvelu tarjotaan tai toimitetaan. (Palo Alto Networks [Viitattu 21.1.2017].)

IT-alan palvelutasosopimuksissa otetaan huomioon myös QoS eli palvelun laatua mittaavat tekijät. Nykyisin SLA-sopimukset ovat arkipäivää kaikkien IT-palveluiden saralla: niitä käyttävät niin sovelluspalveluntarjoajat kuin help deskit. Tavoitellun palvelutason (SLO) mittarit tulevat useammilta eri osa-alueilta, kuten sovellusten- ja verkon hallinnasta. Lisäksi eri yritysten ratkaisevat parametrit vaihtelevat. Niitä ovat esimerkiksi saatavuus, suorituskyky, laitteiden toimintakelvottomuusaika, kaistanleveys ja vasteaika. Saatavilla on erilaisia SLA-sopimuspohjia, mutta ne sopivat sellaisinaan vain harvoille yrityksille. (Keller & Ludwig 2003, 57-58.)

Palvelutasosopimusta laativalla on oltava hyvä käsitys vaadituista ominaisuuksista sekä nykyisen palvelun tilasta hintoineen ja toimintamalleineen. Ymmärtämällä, miten sen hetkiset palvelut toimivat, on helpompi kertoa uudelle palveluntarjoajalle, mitä palvelulta kaivataan. Näin on myös helpompi varmistua siitä, että uusi palvelu on vähintään yhtä hyvä kuin nykyinen. (Desai 2010, 13.)

6.3.1 Koska palvelutasosopimusta tarvitaan?

Palvelutasosopimusta tarvitaan lähinnä silloin, kun hankitaan pitkäaikaisia, kalliita, monimutkaisia ja liiketoiminnan kannalta kriittisiä palveluita. Sopimuksella on mahdollista vaikuttaa palveluntarjoajaan määrittelemällä selkeästi halutut asiat ja painopisteet, jolloin palveluntarjoaja ymmärtää paremmin, mitkä asiat ovat erityisen tärkeitä. Organisaatioiden painopisteet ovat erilaisia, jolloin palveluratkaisut räätälöidään yrityskohtaisesti. Palvelutasosopimukseen vedoten voidaan myös hakea korvauksia, jos organisaation oma toiminta estyy riippuen palvelun huonosta tasosta. Ilman sopimusta siitä, minkälaisia palvelutasoa asiakas odottaa palveluntarjoajalta, asiakkaan on hyvin vaikea riitatilanteessa perustella, miksi ei ole tyytyväinen palveluun. SLA-sopimuksessa palvelu on pilkottu pienempiin osiin ja määritelty selkeästi, jolloin palveluntarjoaja ei voi perättömästi väittää saavuttaneensa vaadittuja kriteerejä, ellei niin ole oikeasti käynyt. (Desai 2010, 39-40.)

6.3.2 Palvelutasosopimuksen perusta

SLA-sopimusta suunniteltaessa on mietittävä, mitä hankittavalta palvelulta vähintään tarvitaan ja mitä organisaatio tarvitsee. Tämä prosessi mahdollistaa tehokkaamman tarjousten läpikäynnin. Seuraavaksi käydään läpi kysymyksiä, jotka helpottavat selvittämään edellä mainitut asiat. (Desai 2010, 49.)

Mitä palveluita organisaatiolla jo on? Uusia palveluja hankittaessa organisaatiolla täytyy olla tiedossa, mitä sen jo hankkimat palvelut sisältävät, mitä ne maksavat ja kuinka suurilta osin nämä palvelut täyttävät vaatimukset. Jo hankittuja palveluja läpikäytäessä kannattaa miettiä, mitkä niistä ovat hyödyllisimpiä, mitkä ongelmallisimpia ja mitä käytetään toistuvasti. Ilman näitä tietoja organisaatio ei

voi verrata nykyisiä palveluita ja kustannuksia mahdollisiin uusiin hankintoihin ja kustannuksiin. Tiedot auttavat mahdollisesti myös neuvotteluvaiheessa, sillä organisaatio voi neuvotella hinnoista vedoten jo tietyllä hinnalla ostettuun palveluun. Uusi palveluntarjoaja saattaa näiden tietojen puuttuessa olettaa, että organisaatio on hyvin tyytymätön senhetkisiin palveluihin ja voi nostaa hintoja. Väärinkäsityksiä voi syntyä myös virheellisistä oletuksista ja palveluntarjoaja saattaa pohjata tarjouksensa näihin oletuksiin, tarjoten liian monimutkaisia ja osaksi tarpeettomia palveluja. (Desai 2010, 49-52.)

Mitä palveluita organisaatiossa halutaan ja tarkemmin ottaen tarvitaan*?* Palvelutasosopimuksessa tulee mainita, mitä palvelu sisältää, mitä se ei sisällä, mitä lisäpalveluita voidaan tarjota ja millä hinnalla. Lisäksi tulee mainita, mitä lisäpalveluja ei ole mahdollista tarjota. Tässä kohdin organisaation on tärkeää ymmärtää, mitä se tarvitsee (minkälainen peruspalvelu tarvitaan) ja mitä se haluaa (mikä on palvelun ideaalinen tila). Organisaation täytyy lisäksi tietää, mistä palveluista se ei halua maksaa. (Desai 2010, 53.)

Onko sama palvelu saatavissa myös halvemmalla? Ei ole järkevää ajatella, että kustannussäästöjä syntyy ostamalla uusia palveluja. Mikäli yritys taas haluaa hankkia mahdollisesti paremman tasoisia palveluja, on todennäköistä, että ne ovat kalliimpia. Oleellinen kysymys onkin, paljonko rahaa organisaatio on valmis kuluttamaan parempaan palveluun? On tärkeää ymmärtää, että usein organisaatio tavoittelee parempia palveluita, muuten se ei kävisi neuvotteluja uuden palveluntarjoajan kanssa. Paremman palvelun määrittely ei kuitenkaan ole yksiselitteistä: se voi tarkoittaa esimerkiksi parempia vasteaikoja, ammattitaitoisempia työntekijöitä, parempia laitteistoja tai nopeampia ratkaisuja. Lähes aina tämä kaikki on kalliimpaa. Kuluihin täytyy myös laskea neuvotteluihin ja palvelutasosopimuksen tekoon kulutetut työtunnit. (Desai 2010, 56-57.)

Mistä organisaatio on vastuussa? On virheellistä ajatella, että palvelutasosopimus olisi yksisuuntainen siinä mielessä, että palveluntarjoaja on vastuussa sen toimittamisesta, organisaatio vain maksaa siitä. Jos organisaatio unohtaa oman vastuunsa ja luovuttaa suuren osan päätösvallastaan palveluntarjoajalle, voi ilmetä mittavia ongelmia. Organisaatio ei välttämättä pysy omien IT-järjestelmiensä perässä, eikä enää ymmärrä niiden konfiguraatiota ja toimintaa täysin. Näin organi-

saatio menettää kyvyn kontrolloida omia IT-ratkaisujaan sataprosenttisesti ja on täysin riippuvainen kolmannen osapuolen toimittamasta palvelusta. (Desai 2010, 58.)

7 VERKONHALLINTA JA -VALVONTA

Valtionhallinnon tietoturvallisuussuositukset asettavat organisaatiolle tiettyjä vaateita verkonhallintaa ja -valvontaa koskien. Jokainen käyttäjä osallistuu valvontaan raportoiden esimiehelleen tai tietohallinnolle huomaamistaan poikkeuksista ja ongelmista. Verkon ylläpitäjien täytyy ottaa huomioon, että kaikkien muutostöiden täytyy kirjautua lokeihin, verkon kokoonpanon on pysyttävä selvillä ja dokumenttien paikkaansapitävyys on tarkastettava säännöllisesti. Valvontaan liittyviä lokeja tulee seurata säännöllisesti ja seurata käytössä olevien ohjelmistojen hälytyslistoja mahdollisten poikkeuksien huomaamiseksi. Verkonvalvonnassa edellytetään käyttämään tarkoitukseen suunniteltua erillistä valvontaohjelmistoa, joka mahdollistaa verkkokomponenttien hallinnan yhdestä pisteestä ja auttaa paikallistamaan vikoja. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2010, 20-22.)

Organisaation edun mukaista on, että verkko pysyy hallinnassa kohtuullisin kustannuksin. Tätä tavoitetta ei ole helppo saavuttaa, sillä usein verkonhallinta perustuu kokemuksiin ja havaintoihin, joiden pohjalta tehdään päätelmiä painopisteiden asettamiseksi. (Jaakohuhta 2005, 309.)

7.1 Verkonhallinta ja -valvonta käsitteinä

Verkonhallinta voidaan jakaa erikseen verkonhallintaan ja verkonvalvontaan. Tässä tapauksessa verkonhallinnan katsotaan sisältävän IEEE.802.1-standardin viiden kohdan jaon mukaan turvallisuuden ja kokoonpanon hallinnan. Verkonvalvonnan taas katsotaan sisältävän suorituskyvyn, vikojen ja käytön hallinnan. (Stallings 1997, 57.)

7.2 Verkonhallinnan osa-alueet

Jaakohuhta (2005, 309, 311) jakaa verkonhallinnan kymmeneen osaan edellä mainitun viiden sijaan. Näihin tutustutaan seuraavissa luvuissa. Kymmenen määritellyn osan lisäksi verkonhallintaan voidaan myös sisällyttää yhdestoista osio, nimeltään teknologisen kehityksen hallinta (migration management). Tarkoituksena

on ottaa huomioon verkon tulevat laajentamistarpeet etukäteen, jolloin vältytään kalliilta, suunnittelemattomia uusintainvestointeja. (Jaakohuhta 2005, 309, 311.)

7.2.1 Vikojen hallinta (Fault Management)

Vikojen hallinta varmistaa, että jokainen verkkolaite sekä verkko kokonaisuutena toimii kuten pitää. Vikaantumisen sattuessa on olennaista selvittää ensiksi, missä vika on ja estää sen vaikutusalueen kasvaminen. Vian vaikutuksia minimoidaan muuttamalla verkon loogista rakennetta tai laitteiden asetuksia. Lopuksi vikaantunut laite korjataan tai vaihdetaan uuteen, jotta verkko voidaan palauttaa normaalitilaansa. Lisäksi vikojen hallintaan kuuluu käyttäjien pitäminen tilanteen tasalla. (Stallings 1997, 3-4.)

Jaakohuhta (2005, 309) painottaa vikojen ennaltaehkäisyä ja sisällyttää vikojenhallintaan lisäksi virhelokien ylläpidon, säännölliset diagnostiikkatestit ja niiden tuloksiin reagoimisen.

7.2.2 Laskutuksen hallinta (Accounting management)

Laskutuksen hallinta tunnetaan myös nimellä käytön hallinta. Ylläpitäjän täytyy kyetä seuraamaan, millä tavoin verkon resursseja käytetään. Peruskäyttäjä saattaa hyödyntää verkkoa tehottomasti tai ylittää käyttöoikeutensa kuormittaen verkkoa. On myös helpompi suunnitella mahdollista verkon laajentamista, kun tiedetään peruskäyttäjien aktiivisuus verkossa. Jotta käyttäjäjien pääsyä arkaluontoisiin tietoihin pystytään rajoittamaan, käytössä täytyy olla luotettava tunnistustapa. (Stallings 1997, 4-5.)

Joissain organisaatioissa on käytössä järjestelmä, jossa laskutetaan verkon käytöstä jopa projektitasolla. Usein tämä on organisaation sisäistä laskuttamista, jolloin raha siirtyy vain yksiköstä toiseen. Ylläpitäjän täytyy silti pystyä seuraamaan käyttäjäryhmien ja jopa yksittäisten käyttäjien toimintatapoja. (Jaakohuhta 2005, 310.)

7.2.3 Kokoonpanon hallinta (Configuration management)

Kokoonpanon hallintaan kuuluu verkon alustus ja tarvittaessa sen osan tai koko verkon sammuttaminen hallitusti, sekä verkkolaitteiden riippuvuuksien lisääminen ja päivittäminen verkon toiminnan aikana. Ylläpitäjällä täytyy olla kyky rekonfiguroida verkon asetukset tarvittaessa. (Stallings 1997, 5-6.)

Lisäksi kokoonpanon hallintaa on myös fyysisten ja loogisten attribuuttien, kuten reititysasetusten määrittely laitteille. Verkossa toimiville laitteille määritellään yksilölliset nimet hallinnan helpottamiseksi. (Jaakohuhta 2005, 310.)

7.2.4 Suorituskyvyn hallinta (Performance management)

Usein verkossa olevat laitteet käyttävät jaettuja resursseja, kuten levytilaa. Tällaiset seikat ovat usein reaaliajassa toimivien ohjelmien toiminnan kannalta kriittisiä. Suorituskykyä tarkkaillaan keräämällä raportteja esimerkiksi näiden laitteiden toiminnasta. Suorituskyvyn hallinta jaetaan verkkoliikenteen valvontaan, joka tarjoaa työkalut asetusten muokkaamiseen vastaamaan paremmin käyttäjien tarpeita, sekä hallintaan, joka käsittää verkon toiminnan tehostamisen. (Jaakohuhta 2005, 310.)

Suorituskykyä tarkkaillessa voidaan havaita ennen varsinaisten ongelmien aiheutumista esimerkiksi suoritustehon laskeminen sallitun tason alle, turha liikenne verkossa, kuinka hyvin verkon resursseja hyödynnetään, onko liikenteessä pullonkauloja ja onko vasteaika kasvanut (Stallings 1997, 6).

7.2.5 Turvallisuuden hallinta (Security management)

Auditointilokien ja muiden verkkolaitteista saatavien lokien tarkkailu on tärkeässä asemassa turvallisuuden hallinnasta puhuttaessa. Lisäksi tähän osioon kuuluu tietosuojaseikoista huolehtiminen, käyttäjätunnusten pääsyoikeudet ja salasanakäytäntöjen ylläpito. (Stallings 1997, 7.)

Turvallisuuden hallinnassa ei ole kyse varsinaisten käyttäjäoikeuksien määrittelystä, vaan siitä, kenellä on oikeus käyttää laitteita ja niiden tarjoamia palveluita (Jaakohuhta 2005, 310-311).

7.2.6 Dokumentointi (Documentation)

Verkon tehokas hallinta edellyttää ajantasaista dokumentointia, jotta pysytään ajan tasalla esimerkiksi verkon loogisesta ja fyysisestä rakenteesta. Varsinkin ison verkon hallinta ilman ajantasaisia dokumentteja on mahdotonta. (Jaakohuhta 2005, 311.)

7.2.7 Raportointi (Report)

Raportointi tarjoaa tietoa vekon tapahtumista ja niiden muutoksista. Lisäksi sen avulla saadaan tehtyä yhteenvetoja laitteiden kapasiteetin käytöstä ja vikatilanteista. (Jaakohuhta 2005, 311.)

7.2.8 Politiikan hallinta (Policy management)

Sovelluksille määritetään organisaation sisällä palveluluokka, jonka peusteella tärkeille sovelluksille annetaan enemmän verkkokapasiteettia. Käytössä voi olla erillinen politiikkapalvelin, johon on määritelty mm. se, ketkä saavat käyttää tiettyä ohjelmaa ja mihin kellonaikaan. (Jaakohuhta 2005, 167; 311.)

7.2.9 Huolto (Service)

Huolto tarkoittaa niitä kaikkia korjaustoimenpiteitä, joita tehdään laitteen rikkouduttua tai varotoimenpiteenä ennen vikatilannetta. Vian- ja kokoonpanon hallinta auttaa huomaamaan mahdolliset viat ja huollettavat kohteet, jolloin niihin voidaan puuttua ajoissa. (Jaakohuhta 2005, 311.)

7.2.10 Ylläpidon hallinta (Maintenance management)

Ylläpidon hallinta sisältää toimenpiteet, jolla pyritään takaamaan verkon toimintavarmuus esimerkiksi vikapäivystyksellä, varaosien hankkimisella ja palvelusopimuksilla. Tähtäimessä on vaikutusten ja taloudellisten menetysten minimointi ongelmatilanteiden sattuessa. (Jaakohuhta 2005, 311.)

7.2.11 Palveluiden hallinta (Services management)

Palveluiden hallinnalla varmistetaan luotettava verkkoympäristö, jossa palveluiden käytettävyys on hyvä, ja palvelut ovat mahdollisimman hyvin saatavilla oikeille käyttäjille myös järjestelmän vikatilanteessa (Jaakohuhta 2005, 311).

8 ELK STACK

Elasticsearch BV on Amsterdamissa vuonna 2012 perustettu yritys, joka haluaa tarjota reaaliaikaisia ratkaisuja IT-alan yritykselle koskien datan käsittelyä. Yrityksellä on työntekijöitä 32 maassa. Tunnetuin tuote on kolmen pienemmän ohjelman yhteenliittymä, ELK Stack. Ohjelmat ovat nimeltään Logstash, Elasticsearch ja Kibana. (Elasticsearch BV [Viitattu 21.3.2017].) Ne on esitelty lyhyesti alla.

8.1 Logstash

Logstash on avoimen lähdekoodin datankeruuväline reaaliaikaisilla datan prosessointityökaluilla. Dataa prosessoivan elementin tuloarvo on edellisen elementin lähtöarvo. Logstash pystyy yhdistelemään vertailukelvotonta dataa ja lähettämään ne haluttuun kohteeseen, kuten Elasticsearchiin ja siitä taas edelleen Kibanaan visualisointia varten. Logstash pystyy käsittelemään kaikkia lokitietoja, kuten web- ja palomuurilokeja tai jopa lukemaan dataa IoT-laitteista. (Logstash Introduction [Viitattu 21.3.2017].)

8.2 Elasticsearch

Elasticsearch mahdollistaa suurten datamäärien lähes reaaliaikaisen tallennuksen, hakemisen ja analysoinnin. Se on hyvin skaalautuva avoimen lähdekoodin haku- ja analysointimoottori. Elasticsearchia voi käyttää esimerkiksi verkkokaupan ylläpitäjä tallentamalla tuotekatalogin, jolloin Elasticsearchin avulla voidaan hakea tuotteita. Hakujen yhteyteen voidaan liittää myös erinäisiä ehtoja, kuten tuotteiden minimi- tai maksimihintoja. (Elasticsearch 5.0 [Viitattu 21.3.2017].)

Loki- tai transaktiodataa kerätessä halutaan myös analysoida saatuja tietoja, jotta löydetään trendejä, yhteenvetoja tai poikkeavuuksia. Tässä tapauksessa Elasticsearchia käytetään Logstash-ohjelman kanssa keräämään, kokoamaan ja jäsentämään dataa. (Elasticsearch 5.0 [Viitattu 21.3.2017].)

Elasticsearchin toimintaan liittyy muutama keskeinen käsite, jotka on lueteltu seuraavaksi (Elasticsearch 5.0 [Viitattu 20.3.2017]).

NRT eli Near Realtime tarkoittaa, että haun yhteydessä esiintyy pientä latenssia, yleensä yksi sekunti hakuehtojen ideksoinnista datan läpikäynnin aloittamiseen (Elasticsearch 5.0 [Viitattu 20.3.2017]).

Noodi on yksittäinen klusteriin kuuluva palvelin, joka varastoi datan ja osallistuu sekä indeksointiin että datan hakemiseen. Jokaiselle noodille annetaan oma uniikki nimi. (Elasticsearch 5.0 [Viitattu 20.3.2017].)

Klusteri on kokoelma noodeja, joka sisältävää kaiken datan ja mahdollistaa hakujen tekemisen kaikkien noodien tiedoista. Klusterilla on aina uniikki nimi, joka on oletuksena ”elasticsearch”. Uniikki nimi on tärkeä, sillä noodi voi liittyä klusteriin vain nimen perusteella. Klusteri voi yksinkertaisimmillaan koostua vain yhdestä noodista, toisaalta itsenäisiä klustereita voi olla useita. Klusterissa voi olla rajaton määrä noodeja. (Elasticsearch 5.0 [Viitattu 20.3.2017].)

Indeksi on kokoelma dokumentteja, joilla on joitain yhteneväisyyksiä. Esimerkiksi yksi indeksi voi olla asiakastietoja varten, yksi tuotetietoja varten jne. Indeksi määritellään nimellä, jossa ei saa olla isoja kirjaimia. Nimeä käytetään viittaamaan indeksiin hakuja, tietojen päivitystä, indeksointia tai poistamista suoritettaessa. Klusterille voi määrittää loputtoman paljon indeksejä. (Elasticsearch 5.0 [Viitattu 20.3.2017].)

Indeksi voi sisältää yhden tai useamman tyypin, jotka ovat itse määriteltävissä. Tyyppi on indeksin looginen osa tai kategoria. Esimerkiksi blogikirjoittaja voi säilöä omat tietonsa yhteen indeksiin, jossa käyttäjätiedot ovat samaa tyyppiä ja kommentit toista tyyppiä. (Elasticsearch 5.0 [Viitattu 20.3.2017].)

Dokumentti on indeksoitavan tiedon perusyksikkö. Järjestelmässä voi esimerkiksi yhtä asiakasta kohti olla yksi dokumentti, joka sisältää osoitetiedot, toinen yksittäiselle tuotteelle ja kolmas yksittäiselle tilaukselle. Saman tyyppisiä dokumentteja voi olla rajaton määrä. (Elasticsearch 5.0 [Viitattu 20.3.2017].)

8.3 Kibana

Kibana on avoimen lähdekoodin visualisointityökalu, joka on tarkoitettu toimimaan yhdessä Elasticsearchin kanssa. Kibanaa käytetään Elasticsearchin keräämän datan visualisointiin ja analysoimiseen. Ulkoasu perustuu tavalliseen selainohjelmaan. Datasta voi muotoilla Kibanan avulla erilaisia kaavioita. (Kibana User Guide [5.2] [Viitattu 21.3.2017].)

Kibana on yhteensopiva Linuxin, Darwinin ja Windowsin kanssa (Kibana User Guide [5.2] [Viitattu 22.3.2017]).

9 YHTEENVETO JA POHDINTA

Opinnäytetyön tavoitteena oli käsitellä Etelä-Pohjanmaan sairaanhoitopiirin tietohallinnon pyynnöstä palveluajattelua, selvittää, miksi palvelutasosopimukset ovat nykyään entistä tärkeämmässä roolissa sekä käydä läpi verkonhallinnan osa-alueet ja käytännöt sekä perustella, miksi huolellinen verkonhallinta ja -valvonta ovat entistä tärkeämmässä roolissa nykyään. Teknisen osaamisen lisäksi on tärkeä ymmärtää perusasiat myös sopimuksista ja dokumentoinnista, sillä insinöörin täytyy ottaa työssään huomioon myös lakisääteisyys ja vakiintuneet käytännöt ollakseen kokonaisvaltaisemmin hyödyksi työnantajalleen.

Työn tekijällä ei ollut aiempaa kokemusta verkonhallintasovelluksista ja ELK Stackiin tutustumisen halu syntyikin puhtaasti oman kiinnostuksen pohjalta. Yllättävää oli, että Kibanan käyttö vaati sen näennäisestä suoraviivaisuudesta ja selkeydestä huolimatta ehkä eniten opettelua, jotta dataa sai kuvattua mahdollisimman järkevällä ja hyödyllisellä tavalla. ELK Stack tarjoaa huomattavasti enemmän ominaisuuksia, kuin mitä oli mahdollista käsitellä tämän opinnäytetyön liitteessä.

ELK Stackilla on suosittelijana runsaasti suuria ulkomaisia organisaatioita ja tietoisuus tästä ohjelmistosta on vasta hiljalleen rantautumassa Suomeen, joten perusteellisempi tutustuminen ja käytön opettelu voisi helpottaa esimerkiksi oman alan töiden löytymisessä. Vastaavia ohjelmistoja on ollut jo aiemminkin, mutta ne ovat huomattavan kalliita.

LÄHTEET

Cisco. Ei päiväystä. CCNA R&S: Introduction to Networks. [Verkkokurssi]. Cisco Systems, Inc. [Viitattu 13.3.2017]. Saatavilla: https://www.netacad.com/group/landing/. Vaatii käyttöoikeuden.

Crawley, D. 2012. Understanding the OSI Reference Model. [Video]. Cisco Router Training 101. [Viitattu 15.3.2017]. Saatavilla: https://www.youtube.com/watch?v=sVDwG2RdJho

Desai, J. 2010. Service Level Agreements. A Legal and Practical Guide. [Verkkokirja.] IT Governance Publishing. [Viitattu 22.1.2017]. Saatavilla Ebsco eBook Academic Collection-tietokannaasta. Vaatii käyttöoikeuden.

Edwards, J. & Bramante, R. 2009. Networking Self-Teaching Guide. [Verkkokirja]. Indianapolis: Wiley Publishing. [Viitattu 19.3.2017]. Saatavilla Ebook Central Academic Complete-tietokannasta. Vaatii käyttöoikeuden.

Elasticsearch 5.0. Ei päiväystä. Elasticsearch Reference [5.2]. [www-sivu]. Basic Concepts. [Viitattu 20.3.2017]. Saatavilla: https://www.elastic.co/guide/en/elasticsearch/reference/current/_basic_concepts.html#_cluster

Elasticsearch 5.0. Ei päiväystä. Elasticsearch Reference [5.2]. [www-sivu]. Getting Started. [Viitattu 21.3.2017]. Saatavilla: https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started.html

Elasticsearch BV. Ei päiväystä. The Elastic Story. [www-sivu]. Elasticsearch BV. [Viitattu 21.3.2017]. Saatavilla: https://www.elastic.co/about

EPSHP. Ei päiväystä. Yleisesittely. [www-sivu]. Seinäjoki: Etelä-Pohjanmaan sairaanhoitopiiri. [Viitattu 2.11.2016]. Saatavilla: http://www.epshp.fi/yleisesittely

EPSHP. Ei päiväystä. Ihmisen terveyden tähden. [www-sivu]. Seinäjoki: Etelä-Pohjanmaan sairaanhoitopiiri. [Viitattu 3.11.2016]. Saatavilla: http://www.epshp.fi/files/111/Esittelydiat_EPSHP_2015.pdf

EPSHP. Ei päiväystä. Organisaatio ja rakenne. [www-sivu]. Seinäjoki: Etelä-Pohjanmaan sairaanhoitopiiri. [Viitattu 4.11.2016]. Saatavilla: http://www.epshp.fi/yleisesittely/organisaatio_ja_rakenne

Hautaniemi, M. 1994. [Diplomityö]. TKK/Atk-keskuksen verkon valvonta ja hallinta. Luku 2. Verkonhallinta. [Viitattu 22.1.2017]. Saatavilla: http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/verkonhallinta.html

Jaakohuhta, H. 2005. Lähiverkot-Ethernet. 4. uud. p. Helsinki: Edita Prima Oy.

Keller, A. & Ludwig, H. 2003. The WSLA Framework: Specifying and Monitoring Service Level Agreements for Web Services. [Verkkolehti]. Journal of Network and Systems Management. [Viitattu 25.1.2017]. Saatavilla ProQuest ABI/INFORM Collection-tietokannasta. Vaatii käyttöoikeuden.

Kibana User Guide [5.2]. Ei päiväystä. Introduction. [www-sivu]. Elasticsearch BV. [Viitattu 21.3.2017]. Saatavilla: https://www.elastic.co/guide/en/kibana/current/introduction.html

Kibana User Guide [5.2]. Ei päiväystä. Set Up Kibana. [www-sivu]. Elasticsearch BV. [Viitattu 22.3.2017]. Saatavilla: https://www.elastic.co/guide/en/kibana/current/setup.html

Logstash Introduction. Ei päiväystä. Logstash Reference [5.2]. [www-sivu]. Elasticsearch BV. [Viitattu 21.3.2017]. Saatavilla: https://www.elastic.co/guide/en/logstash/current/introduction.html

McWhirter, K. & Gaughan, T. 2012. The Definitive Guide to IT Service Metrics. [Verkkokirja]. IT Governance Publishing. [Viitattu 22.1.2017]. Saatavilla Ebsco eBook Academic Collection-tietokannasta. Vaatii käyttöoikeuden.

Okes, D. 2013. Performance Metrics: The Levers for Process Management. [Verkkokirja]. ASQ Quality Press. [Viitattu 23.1.2017]. Saatavilla ebrary Academic Complete-tietokannasta. Vaatii käyttöoikeuden.

Oulun yliopisto. 2014/2015. Siirtoyhteyskerros ja paikallisverkot. Tietojenkäsittelytieteiden laitos. [pdf-tiedosto]. Internet ja tietoverkot. [Viitattu 13.3.2017]. Saatavilla: https://noppa.oulu.fi/noppa/kurssi/811338a/luennot/811338A_siirtoyhteyskerros.pdf

Palo Alto Networks. Ei päiväystä. What is a service level agreement? [www-sivu]. Cyperpedia. [Viitattu 26.1.2017]. Saatavilla: https://www.paloaltonetworks.com/documentation/glossary/what-is-a-service-level-agreement-sla

Rouse, M. 2014. confidentiality, integrity, and availability (CIA triad). [www-sivu]. TechTarget. [Viitattu 19.3.2017]. Saatavilla: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Stallings, W. 1997. SNMP, SNMPv2, and RMON. 2. uud. p. Canada: Addison Wesley Longman, Inc.

Valtionhallinnon tietoturvallisuuden johtoryhmä. 2001. Valtionhallinnon lähiverkkojen tietoturvallisuus. Vahti-ohje. [www-sivu]. [Viitattu 2.3.2017]. Saatavilla: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7883adbf-de6f-4f38-8294-0c33b5969059&groupId=10128

Valtiovarainministeriö. 2010. Sisäverkko-ohje. [www-sivu]. Valtionhallinnon tietoturvallisuuden johtoryhmä. [Viitattu 25.2.2017]. Saatavilla: https://www.vahtiohje.fi/c/document_library/get_file?uuid=5084ce47-32bf-4025-bcc1-73fc2de4edad&groupId=10128

Vargo, S. & Lusch, R. 2004. Evolving to a New Dominant Logic for Marketing. [Lehtiartikkeli]. Journal of Marketing. [Viitattu 1.3.2017]. Saatavilla EBSCOhost Business Source Elite-tietokannasta. Vaatii käyttöoikeuden.

Virtanen, P., Smedberg, J., Nykänen, P. & Stenvall, J. 2017. Palvelu- ja asiakastietojärjestelmien integraation vaikutukset sosiaali- ja terveyspalveluissa. [www-sivu]. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja. [Viitattu 28.2.2017]. Saatavilla: http://tietokayttoon.fi/documents/10616/3866814/2_Palvelu-+ja+asiakastietoj%C3%A4rjestelmien+integraation+vaikutukset+sosiaali-+ja+terveyspalveluissa/bcc5b696-7e81-4121-b496-c9ac78be815e?version=1.0

LIITTEET

Liite 1. Elastic Stack -esimerkki

Niina Koskinen

ELK Stack–esimerkki

Liite 1

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SISÄLTÖ

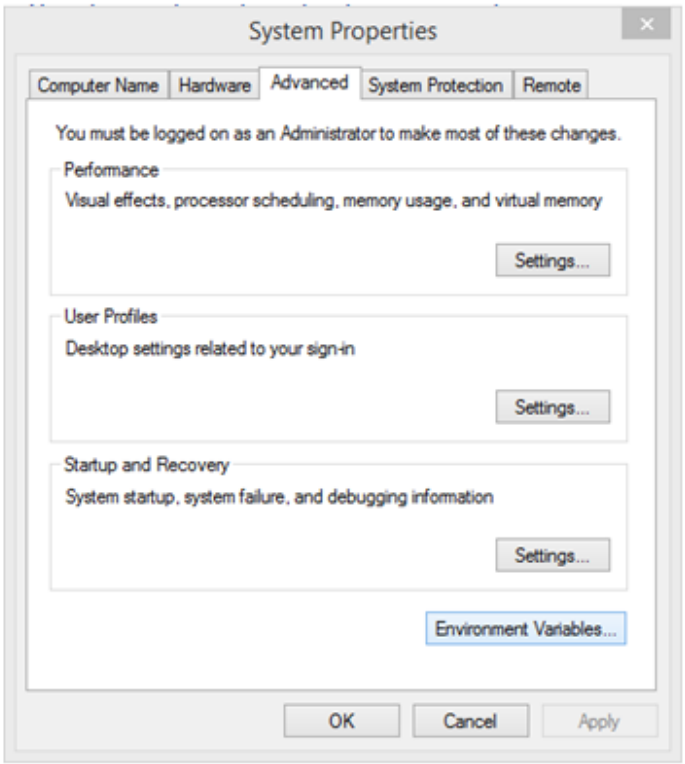
1 ESIASETUKSET

Tässä liitteessä tutustutaan pääpiirteittäin Elasticsearchin, Logstashin ja Kibanan toimintaan. Kaikki kolme ohjelmaa ovat ladattavissa ilmaiseksi sivulta https://www.elastic.co/products.

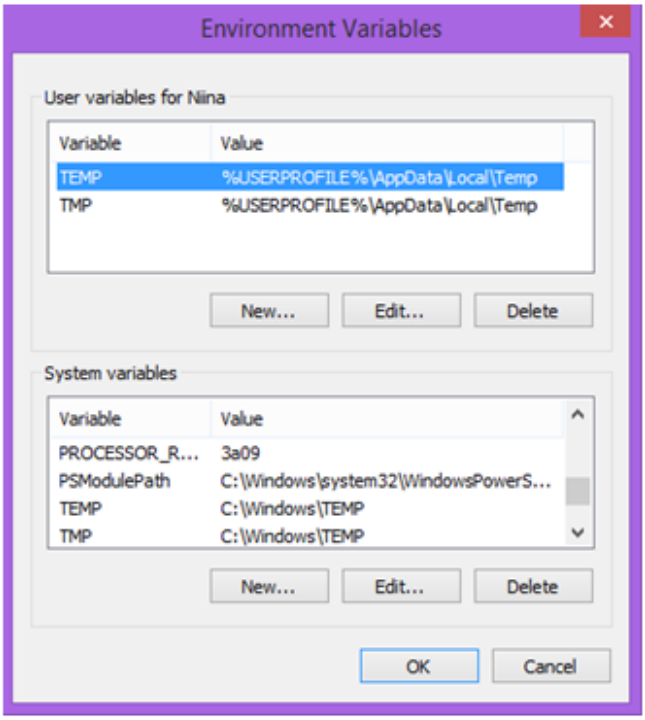
Elasticsearch vaatii toimiakseen vähintään Java SE development kit 8:n. Tätä opinnäytetyötä tehdessä suositeltiin erityisesti versiota 1.8.0_121.

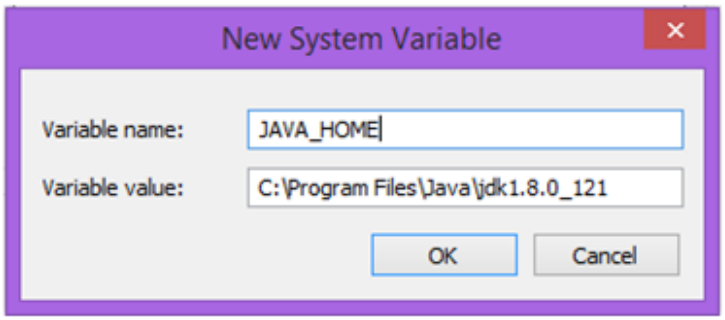
Seuraavaksi Java täytyy mennä asettamaan uudeksi system variableksi. Tämä tapahtuu navigoimalla seuraavasti:

Control Panel → System and Security →System → Advanced System Settings



Täältä valitaan Environment Variables…-painike.





Valitaan ”New...” ja kirjoitetaan seuraavat tiedot:

Varible name: JAVA_HOME
Variable value: tiedostopolku, jonne Java on asennettu

Painetaan OK.

Tähän liitteeseen ladattiin esimerkkidataksi sivustolta http://finance.yahoo.com/quote/AAPL/history?ltr=1 esimerkkidataa. Ladattu tiedosto on .csv-tyyppinen.

```
Date,Open,High,Low,Close,Volume,Adj Close
2017-03-23,141.259995,141.580002,140.610001,140.919998,20285700,140.919998
2017-03-22,139.850006,141.600006,139.759995,141.419998,25787600,141.419998
2017-03-21,142.110001,142.800003,139.729996,139.839996,39116800,139.839996
2017-03-20,140.399994,141.50,140.229996,141.460007,20213100,141.460007
2017-03-17,141.00,141.00,139.889999,139.990005,43597400,139.990005
2017-03-16,140.720001,141.020004,140.259995,140.690002,19132500,140.690002
2017-03-15,139.410004,140.75,139.029999,140.460007,25566800,140.460007
2017-03-14,139.300003,139.649994,138.839996,138.990005,15189700,138.990005
2017-03-13,138.850006,139.429993,138.820007,139.199997,17042400,139.199997
2017-03-10,139.25,139.360001,138.639999,139.139999,19488000,139.139999
2017-03-09,138.740005,138.789993,137.050003,138.679993,22065200,138.679993
2017-03-08,138.949997,139.800003,138.820007,139.00,18681800,139.00
2017-03-07,139.059998,139.979996,138.789993,139.520004,17267500,139.520004
2017-03-06,139.369995,139.770004,138.600006,139.339996,21155300,139.339996
2017-03-03,138.779999,139.830002,138.589996,139.779999,21108100,139.779999
2017-03-02,140.00,140.279999,138.759995,138.960007,26153300,138.960007
2017-03-01,137.889999,140.149994,137.600006,139.789993,36272400,139.789993
2017-02-28,137.080002,137.440002,136.699997,136.990005,23403500,136.990005
2017-02-27,137.139999,137.440002,136.279999,136.929993,20196400,136.929993
2017-02-24,135.910004,136.660004,135.279999,136.660004,21690900,136.660004
```

Tiedosto näyttää avattuna ylläolevan kuvan mukaiselta.

2 KONFIGURAATIOTIEDOSTO

Datan lukemiseksi csv.-tiedostosta täytyy Logstashille luoda konfiguraatiotiedosto. Tämä tiedosto luetaan samalla, kun Logstash käynnistetään.

```
input {
  file {
    path => "D:\Esimerkkidata\data.csv"
    start_position => "beginning"
  }
}
```

Konfiguraatiotiedoston input-osiossa kerrotaan path-kohdassa sen datatiedoston tiedostopolku, joka halutaan lukea. Lisäksi määritellään, että tiedoston luku aloitetaan alusta.

```
filter {
  csv {
      separator => ","
      columns => ["Date","Open","High","Low","Close","Volume","Adj Close"]
  }
  mutate {convert => ["High", "float"]}
  mutate {convert => ["Open", "float"]}
  mutate {convert => ["Low", "float"]}
  mutate {convert => ["Close", "float"]}
  mutate {convert => ["Volume", "float"]}
}
```

Filter-osio kertoo, missä muodossa luettava data on (csv). Tiedostomuodon sisälle määritellään, mitkä pystysarakkeet halutaan lukea. Kaikki tiedoston kentät muunnetaan float-muotoon, jotta Kibana osaa käsitellä niitä.

```
output {
    elasticsearch {
        action => "index"
        index => "esimerkki1"
        workers => 1
    }
    stdout {}
}
```

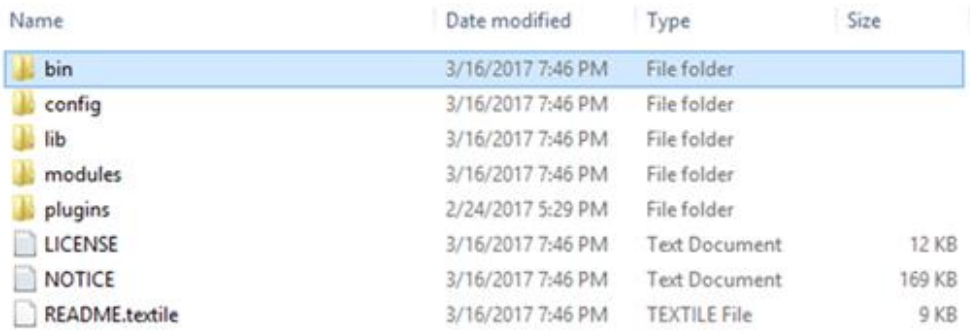
Output-osiossa kerrotaan ,että data lähetetään Elasticsearchille. Index-kohdassa annetaan tiedostolle nimi.

Tämä yllä esitetty esimerkkikonfiguraatio on mukailtu osoitteesta http://blog.webkid.io/visualize-datasets-with-elk/.

3 DATAN LUKU KIBANAAN

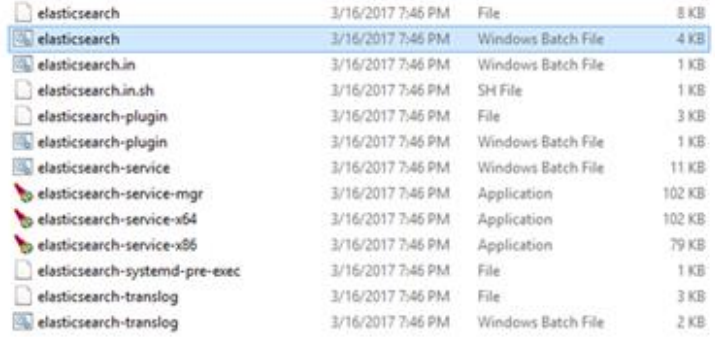
Seuraavaksi käynnistetään Elasticsearch.

Se tapahtuu navigoimalla kansioon, johon ohjelma on purettu. Alla olevassa kuvassa on kansiorakenne.



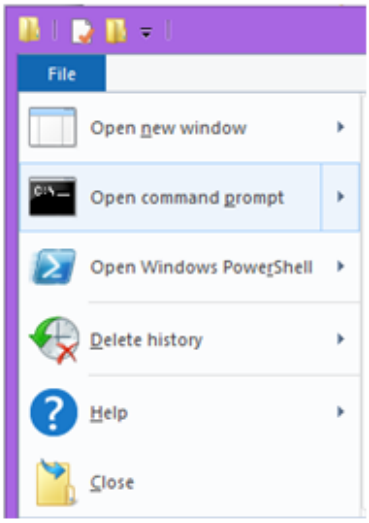
Name	Date modified	Type	Size
bin	3/16/2017 7:46 PM	File folder	
config	3/16/2017 7:46 PM	File folder	
lib	3/16/2017 7:46 PM	File folder	
modules	3/16/2017 7:46 PM	File folder	
plugins	2/24/2017 5:29 PM	File folder	
LICENSE	3/16/2017 7:46 PM	Text Document	12 KB
NOTICE	3/16/2017 7:46 PM	Text Document	169 KB
README.textile	3/16/2017 7:46 PM	TEXTILE File	9 KB

Ohjelman kansiosta löytyy bin-niminen kansio, jonka sisällä on ohjelman kanssa vastaavan niminen .bat -tyyppinen tiedosto.



elasticsearch	3/16/2017 7:46 PM	File	8 KB
elasticsearch	3/16/2017 7:46 PM	Windows Batch File	4 KB
elasticsearch.in	3/16/2017 7:46 PM	Windows Batch File	1 KB
elasticsearch.in.sh	3/16/2017 7:46 PM	SH File	1 KB
elasticsearch-plugin	3/16/2017 7:46 PM	File	3 KB
elasticsearch-plugin	3/16/2017 7:46 PM	Windows Batch File	1 KB
elasticsearch-service	3/16/2017 7:46 PM	Windows Batch File	11 KB
elasticsearch-service-mgr	3/16/2017 7:46 PM	Application	102 KB
elasticsearch-service-x64	3/16/2017 7:46 PM	Application	102 KB
elasticsearch-service-x86	3/16/2017 7:46 PM	Application	79 KB
elasticsearch-systemd-pre-exec	3/16/2017 7:46 PM	File	1 KB
elasticsearch-translog	3/16/2017 7:46 PM	File	3 KB
elasticsearch-translog	3/16/2017 7:46 PM	Windows Batch File	2 KB

Valitaan bat-tiedosto napauttamalla sitä kerran hiirellä.



Kansionäkymän vasemmasta yläreunasta valitaan “File” ja “Open command prompt”. Komentoriville kirjoitetaan tiedostopolun perään vielä “elasticsearch”.

```
elasticsearch
```

Elasticsearch käynnistyy. Jos kaikki menee hyvin, komentorivillä lukee ”started”.

Elasticsearch löytyy oletuksena osoitteesta localhost:9200.

Oletuksena sivulla on alla kuvatut tiedot.


```
{
  "name" : "atXDQUb",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "B7J3D4bAT7Gy1seWLWxKsw",
  "version" : {
    "number" : "5.2.2",
    "build_hash" : "f9d9b74",
    "build_date" : "2017-02-24T17:26:45.835Z",
    "build_snapshot" : false,
    "lucene_version" : "6.4.1"
  },
  "tagline" : "You Know, for Search"
}
```


Jätetään Elasticsearch päälle taustalle ja avataan Logstash aiemmin määritellyllä konfiguraatiolla.

Kuten Elasticsearchia käynnistettäessä, navigoidaan Logstashin bin-nimiseen kansioon ja avataan bat-tiedosto komentorivillä kirjoittamalla:

```
logstash –f “konfiguraatiotiedoston nimi.conf”
```

```
D:\logstash\bin>logstash -f esimerkki.conf
[2017-03-24T14:15:32,933][INFO ][logstash.outputs.elasticsearch]
[2017-03-24T14:15:32,937][INFO ][logstash.outputs.elasticsearch]
```

Jos kaikki toimii, komentoriville ilmestyy aikaleima. Seuraavaksi käynnistetään Kibana samaan tapaan kuin Elasticsearch.

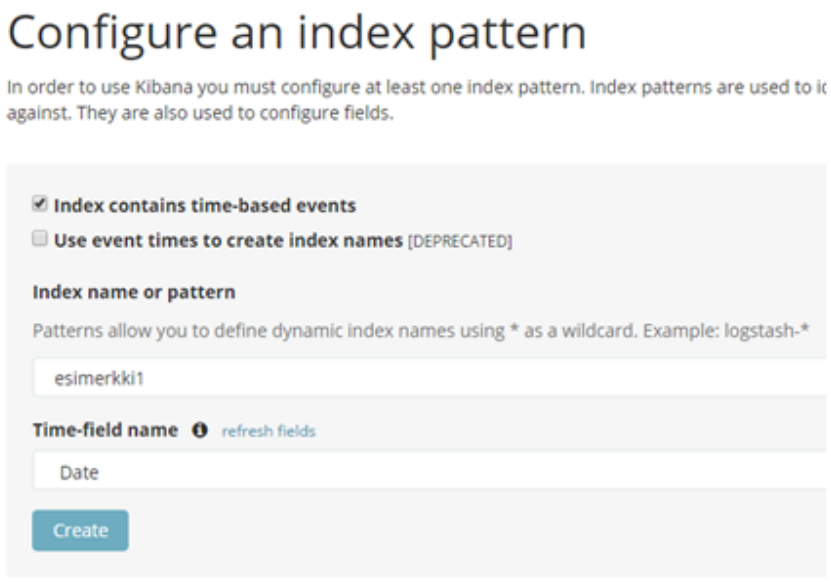
```
D:\kibana-5.2.2-windows-x86\kibana-5.2.2-windows-x86\bin>kibana
  log   [12:16:33.512] [info][status][plugin:kibana@5.2.2] Status
  log   [12:16:33.563] [info][status][plugin:elasticsearch@5.2.2
  log   [12:16:33.589] [info][status][plugin:console@5.2.2] Stat
  log   [12:16:33.924] [info][status][plugin:timelion@5.2.2] Sta
  log   [12:16:33.934] [info][listening] Server running at http:/
  log   [12:16:33.936] [info][status][ui settings] Status change
  log   [12:16:34.012] [info][status][plugin:elasticsearch@5.2.2
  log   [12:16:34.013] [info][status][ui settings] Status change
```

kibana

Nyt kaikki kolme ohjelmaa ovat päällä ja voidaan siirtyä datan visualisointiin.

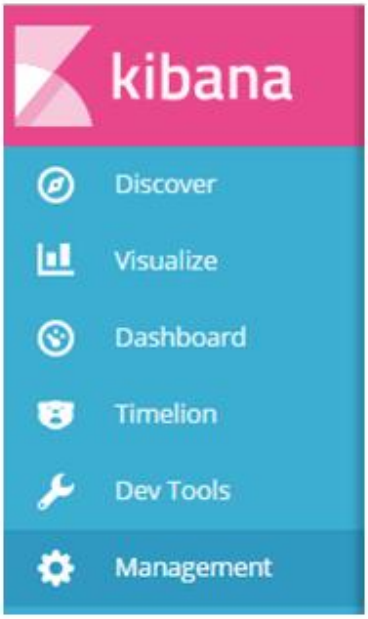
4 VISUALISOINTI KIBANAN AVULLA

Kibanan käyttöliittymä löytyy oletuksena osoitteesta localhost:5601.

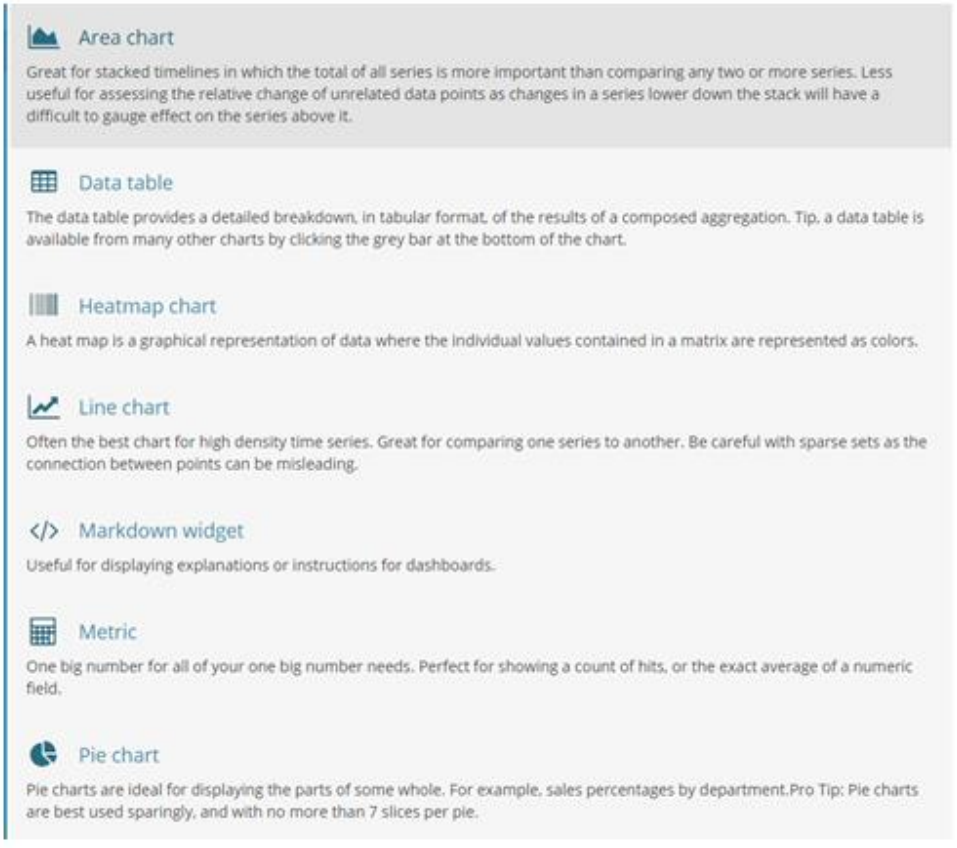


Aluksi täytyy määritellä, minkä nimisestä indeksistä halutaan visualisoida dataa. Tässä tarkoitetaan konfiguraatiotiedostossa määriteltyä index-kohtaa. Time field name-kohdassa määritellään, halutaanko dataa analysoida päivämäärän vai timestampin perusteella. Valitaan ”Date”-vaihtoehto ja painetaan ”Create”.

Seuraavaksi avautuvassa näkymässä on allekkain kaikki indeksit, jotka Elasticsearch on siirtänyt Kibanan luettavaksi.



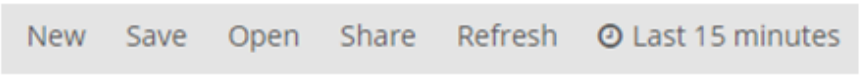
Tämän jälkeen navigoidaan vasemmalla puolella olevasta sivupalkista kohtaan “Visualize”.



Kibana tarjoaa useita erilaisia visualisointivaihtoehtoja. Valitaan esimerkiksi Metric”-vaihtoehto.

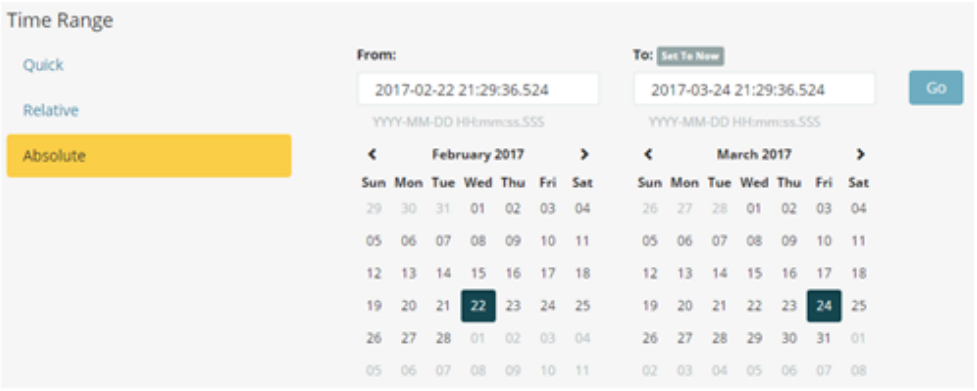
Valitaan indeksi, jonka dataa halutaan visualisoida.

Käyttöliittymän yläoikealla on alla kuvattu palkki.

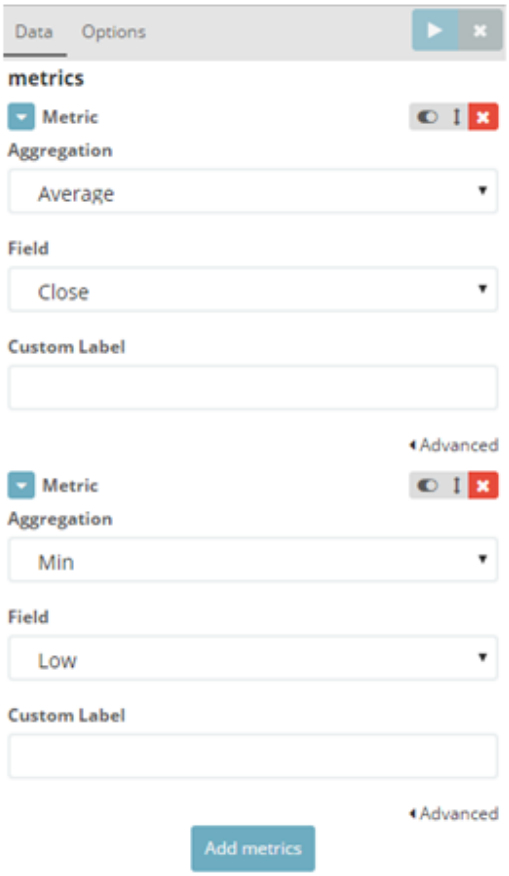


Aikaväli on oletuksena edellisen 15 minuutin ajalta. Mikäli visualisoitavaa dataa ei heti löydy, kannattaa aikaväli vaihtaa pidemmäksi. Tämän esimerkin päivämäärän perusteella luokiteltu data ei sovi oletusaikavälille.

Aikaväliä voi vaihtaa valmiiden vaihtoehtojen mukaan tai kalenterinäkymästä.

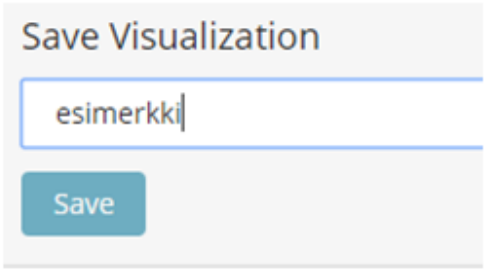


Dataa visualisoidessa voidaan valita useista vaihtoehdoista itselle tarpeellisimmat tiedot.



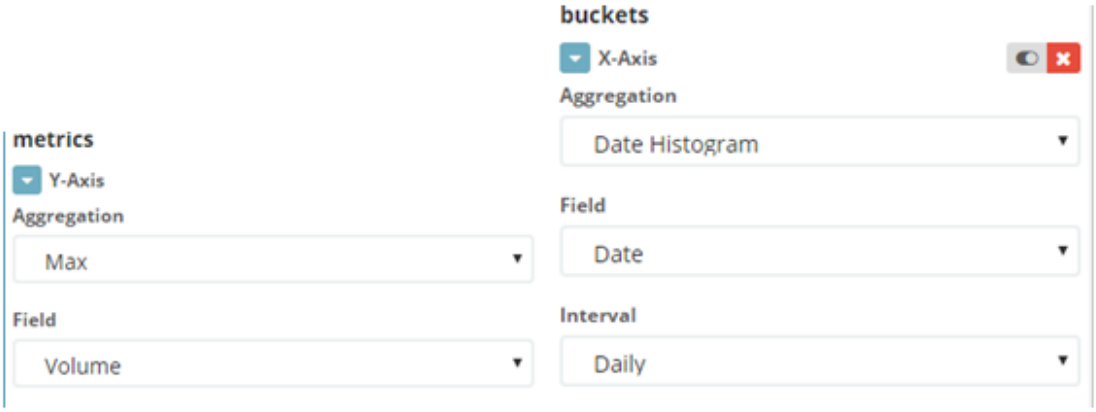
Tässä tapauksessa valittiin visualisoitavaksi lukujen keskiarvo Close-sarakkeesta ja minimiarvo Low-sarakkeesta.

Kibana esittää luvut ylläolevalla tavalla.



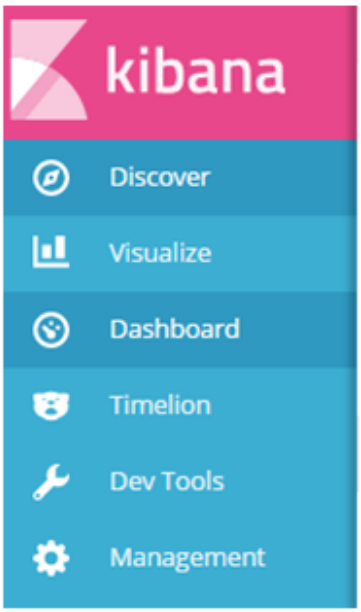
Halutun visualisoinnin voi tallentaa haluamallaan nimellä ylhäältä oikealta Save-napista.

Tallennuksen onnistuessa ikkunan yläreunassa lukee Visualization Editor: Saved Visualization "tiedostonimi".

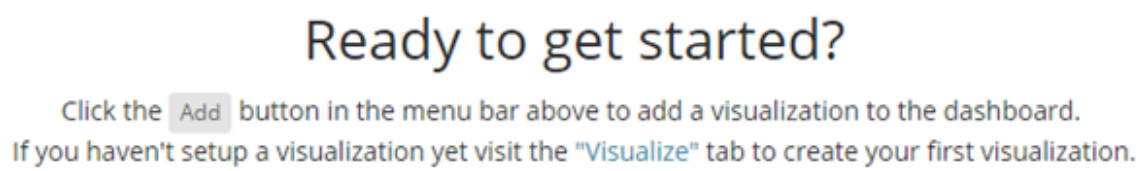


Toiseksi esimerkiksi lisättiin Vertical bar chart-tyyppinen taulukko. Y-akselille valittiin päivittäinen maksimiarvo Volume-sarakkeelta ja X-akselille laitettiin päivät.

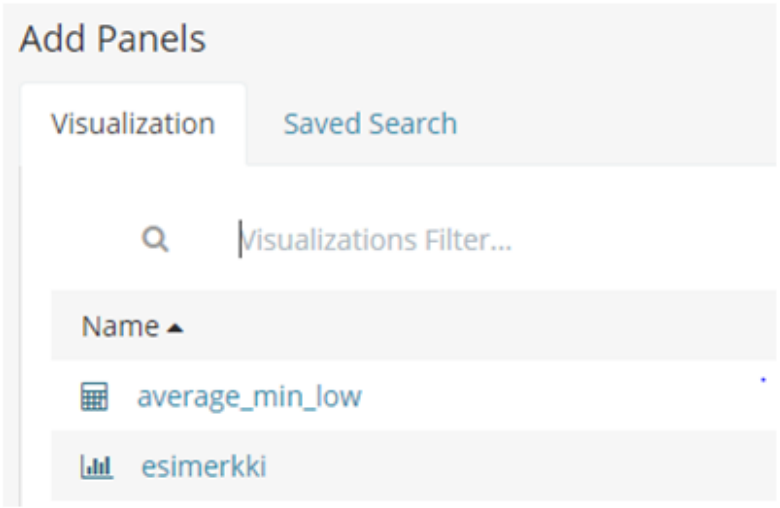
Tämäkin taulukko tallennettiin nimellä.



Dashboard-kohdassa voi yhdistellä taulukkoja ja muita visualisointeja haluamallaan tavalla, jotta kaikki tärkeimmät tiedot ovat nähtävissä heti kerralla.

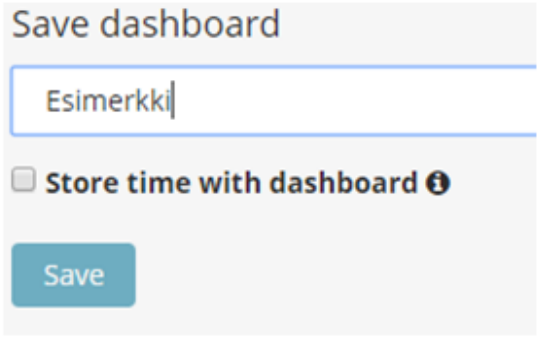


Napautetaan ”Add”-painiketta.



Tallennetut visualisoinnit näkyvät listassa. Siitä voi valita haluamansa Dashboard-näkymään.

Visualisoinnit voi järjestellä haluamallaan tavalla Dashboardille.



Dashboard tallennetaan yläoikealla olevasta ”Save”-painikkeesta.