Sakari Pieviläinen

Open Source -tietoturvatyökalujen vertailu verkonvalvonnassa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

29.4.2016

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Sakari Pieviläinen Open Source -tietoturvatyökalujen vertailu verkonvalvonnassa 33 sivua 29.4.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	yliopettaja Janne Salonen

Internetin käyttäjämäärien kasvu ja sisällön lisääntyminen ovat tuoneet mukanaan myös varjopuolia. Näitä ovat esimerkiksi verkkovakoilu, tietomurrot ja tietojenkalastelu. Tämän takia on tärkeää, että virustutkien, viruksentorjuntaohjelmistojen sekä muiden tähän liittyvien ohjelmistojen lisäksi verkkoa valvotaan ja pysytään ajan tasalla siitä, mitä verkossa liikkuu ja mitä siellä tulisi liikkua. Tällaisesta valvonnasta käytetään nimitystä verkonvalvonta. Tässä insinöörityössä perehdyttiin verkonvalvontaan tietoturvan näkökulmasta. Työssä on käyty läpi neljän eri verkonvalvontaohjelman asentaminen Ubuntu 14.04.3 LTS linux -työasemalle ja vertailtu, mitä verkon tietoturvasta voidaan nähdä milläkin ohjelmalla. Työssä on selvitetty myös, mikä ohjelmista on käyttöliittymältään helppokäyttöisin. Työssä käytettäviksi ohjelmistoiksi valittiin neljä avoimen lähdekoodin verkonvalvontaohjelmistoa: Zabbix, Observium, Icinga ja Cacti. Avoimen lähdekoodin ansiosta ohjelmat ovat hyvin saatavilla, kustannustehokkaita ja ennen kaikkea laadukkaita. Verkonvalvontaan liittyvän selvitystyön tekeminen edellyttää verkonvalvontaohjelmien käyttämien protokollien tuntemista, joihin on perehdytty työn alussa.

Kartoitustyön pohjalta voitiin päätyä johtopäätökseen, että verkonvalvontaohjelmiston valinnassa on olennaista se, mitä ohjelmalla halutaan tehdä ja minkälaiseen ympäristöön se asennetaan. Jos halutaan esimerkiksi ainoastaan katsella ja analysoida SNMP-dataa graafisessa muodossa, Cacti on tähän hyvä ohjelmisto. Icinga ja Zabbix olivat vertailtujen kohteiden monipuolisimmat ohjelmistot, joilla molemmilla pystytään toteuttamaan samat asiat. Zabbix ja Icinga eroavat kuitenkin toisistaan siinä, että Icingassa lisäosien merkitys on suurempi, kun taas Zabbix asentaa kaiken oletuksena. Jokaisessa verkonvalvontaohjelmistossa oli selkeä ja toimiva web-käyttöliittymä.

Insinöörityöaiheeseen perehtyminen tuotti työn tekijälle paljon uutta tietoa verkonvalvontaohjelmistoista. Laajan käsityksen saaminen ohjelmistojen käytöstä ja toiminnoista edellyttäisi työskentelyä ohjelmistojen parissa pidemmän aikaa ympäristössä, joka sisältäisi useita työasemia ja palvelimia.

Avainsanat	verkonvalvonta, avoin lähdekoodi, Zabbix, Icinga, Cacti, Observium

Author(s) Title Number of Pages Date	Sakari Pieviläinen Comparison of Open Source network monitoring software 33 pages 15 September 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Janne Salonen, Principal Lecturer

The object of this thesis was to explore four different open source based network monitoring software and install these four pieces of software to a Linux Ubuntu 14.04.3 LTS workstation.

The first half of the study goes through the protocols which these selected four pieces of network monitoring software use. Also, the basics of Intrusion Detection and Intrusion Prevention Systems are covered.

The thesis also addresses the issue of what are the benefits of using Open Source software compared to proprietary software.

The second half of the study focuses on going through the outlines of installing the four pieces of network monitoring software. One of these installations is a more in depth demo version of an installation which anybody with basic knowledge of Linux systems should be able to replicate.

Even though the selection of network monitoring software in this thesis is just a scratch of the surface the study provides basic understanding of network monitoring software and what it is capable of.

Finally, the study discusses how these four pieces of network monitoring software differ from each other and which software is best suited for which kind of application and environment.

Keywords	Network monitoring, Open source, Zabbix, Icinga, Cacti, Observium

Sisällys

Lyhenteet

CDP	Cisco Discovery Protocol. Cisco Systemsin kehittämä protokolla, jota käytetään verkossa olevien laitteiden tietojen keräämiseen.
CRC	Cyclic Redundancy Check. Virheen havaitsemiseen käytettävä koodi, jolla monitoroidaan datan eheyttä.
DDoS	Distributed Denial of Service. Hajautettu palvelunestohyökkäys.
EDP	Extreme Discovery Protocol. Extreme Networksin kehittämä protokolla, jota käytetään verkossa olevien laitteiden tietojen keräämiseen.
FDP	Foundry Discovery Protocol. Foundry Networksin kehittämä protokolla, jota käytetään verkossa olevien laitteiden tietojen keräämiseen.
FTP	File Transfer Protocol. Palvelimen ja asiakkaan väliseen tiedonsiirtoon käytettävä protokolla.
HIDS	Host Intrusion Detection System. Murronhavaitsemisjärjestelmä, jota ajetaan yksittäisellä työasemalla tai laitteella.
HIPS	Host Intrusion Prevention System. Murronestämisjärjestelmä, jota ajetaan yksittäisellä työasemalla tai laitteella.
HTML	Hypertext Markup Language. Hypertekstin kuvaamiseen käytettävä kieli.
HTTP	Hypertext Transfer Protocol. Hypertekstin siirtämiseen käytettävä protokolla.
ICMP	Internet Control Message Protocol. Internetprotokollan päällä toimiva protokolla, jota käytetään viestien lähettämiseen nopeasti koneelta toiselle.
IDS	Intrusion Detection System. Murronhavaitsemisjärjestelmä.

IMAP	Internet Message Access Protocol. Sähköpostiviestien lukemiseen käytettävä protokolla.
IP	Internet Protocol. Internetissä kulkevien IP-pakettien perille toimittamiseen käytettävä protokolla.
IPS	Intrusion Prevention System. Murronestämisjärjestelmä.
LLDP	Link Layer Discovery Protocol. Laitevalmistajariippumaton protokolla, jota käytetään verkossa olevien laitteiden tietojen keräämiseen.
MIB	Management Information Base. Laitteen määritelmien säilyttämiseen ja hallitsemiseen käytettävä tietokanta.
MRTG	Multi Router Traffic Grapher. Verkkolaitteiden monitorointitietoja ja verkon käyttöasteen tietoja graafisesti esittävä työkalu.
NBA	Network Behaviour Analysis. Murronestämisjärjestelmä, joka analysoi verkkoliikennettä ja pyrkii tunnistamaan uhat.
NIDS	Network Intrusion Detection System. Verkon solmukohtaan asennettava tunkeutujanhavaitsemisjärjestelmä.
NIPS	Network Intrusion Prevention System. Verkon solmukohtaan asennettava murronestämisjärjestelmä.
OSI	Open Systems Interconnection Model. Tiedonsiirtoprotokollien yhdistelmän kuvaamiseen käytettävä seitsemänkerroksinen malli.
POP	Post Office Protocol. Protokolla, jota asiakasohjelma käyttää sähköpostin hakemiseen.
RRD	Round-Robin Database Tool. Työkalu, jolla käsitellään aikasarjadataa, esimerkiksi verkon kaistaa, lämpötilaa tai prosessorin käyttöastetta.

SMTP	Simple Mail Transfer Protocol. Internetin standardiprotokolla sähköpostien siirtämiseen.
SNMP	Simple Network Management Protocol. Verkossa olevien laitteiden laitetietojen keräämiseen, hallitsemiseen ja muokkaamiseen käytettävä protokolla.
SSH	Secure Shell. Salatun yhteyden mahdollistava protokolla, joka tukee mm. etäkirjautumista.
TCP	Transmission Control Protocol. Internetin tärkeimpiä protokollia. Mahdollistaa okteteista koostuvan datavirran kahden päätepisteen välille.
UDP	User Datagram Protocol. Protokolla, joka mahdollistaa tiedonsiirron laitteiden välillä ilman erillistä yhteyden muodostamista.
WIPS	Wireless Intrusion Prevention System. Murronestämisjärjestelmä, joka monitoroi langattoman verkon liikennettä.

1 Johdanto

Tietoverkkojen ja niiden käyttäjien määrä on kasvanut voimakkaasti viimeisten kahdenkymmenen vuoden aikana. Esimerkiksi internetin käyttäjien määrä on kasvanut vuosien 1995 - 2015 välillä noin 16 miljoonasta käyttäjästä 3,37 miljardiin käyttäjään. Tämä kasvu selittyy mm. teknologian nopealla kehittymisellä viimeisten 20 vuoden aikana. Internetin käyttö ei rajoitu enää pelkästään langallisiin yhteyksiin sekä kannettaviin ja pöytäkoneisiin. Nykyisin internet on saatavilla myös langattomasti kannettavilla laitteilla, älypuhelimilla, tableteilla ja televisioilla. Myös internetyhteydet ovat nopeutuneet, ja suurimmalla osalla väestöstä on mahdollisuus päästä internetiin verkon laajentumisen ansiosta. Internetin fyysisten ominaisuuksien kehittymisen lisäksi myös palvelusovellusten määrän kasvu ja niiden sisältö ovat vaikuttaneet käyttäjämäärien kasvuun. Ihmisten arkea helpottavat internetpalvelut, esimerkiksi laskujen maksaminen tai lomamatkan tilaaminen omalta päätelaitteelta, tarjoavat joustavan, paikkaan ja aikaan sitoutumattoman tavan hoitaa asioita sähköisesti. Viime vuosina internetliikennettä on lisännyt merkittävästi myös sosiaalinen media. Internet ei ole enää pelkästään paikka, josta haetaan tietoa ja jossa hoidetaan asioita, vaan paikka, jossa myös sosiaalistutaan. [1.]

Internetin käyttäjämäärien kasvu ja sisällön lisääntyminen ovat tuoneet mukanaan myös varjopuolia. Näitä ovat esimerkiksi verkkovakoilu, tietomurrot ja tietojenkalastelu. Tämän takia on tärkeää, että virustutkien, viruksentorjuntaohjelmistojen sekä muiden tähän liittyvien ohjelmistojen lisäksi verkkoa valvotaan ja pysytään ajan tasalla siitä, mitä verkossa liikkuu ja mitä siellä tulisi liikkua. Tällaisesta valvonnasta käytetään nimitystä verkonvalvonta. Verkonvalvonnan avulla verkosta saadaan monenlaista tietoa, mutta yleisimpänä verkonvalvonnan syinä ovat verkon ongelmat, esimerkiksi verkon hitaus tai yhteyden katkeaminen. Tällaisissa tapauksissa verkonvalvonta on erittäin hyvä työväline, koska sillä voidaan etsiä tietoja verkossa olevista laitteista ja selvittää, aiheuttaako esimerkiksi kaatunut palvelin tai verkkolaite ongelman.

Tietoverkkojen tietoturvassa on kyse verkossa liikkuvan tiedon keräämisestä ja sen analysoimisesta epäilyttävän toiminnan havaitsemiseksi ja sen estämiseksi. Nykyaikaisissa verkoissa on jo valmiita tietoturvalaitteita, esimerkiksi palomuureja, mutta uusimmatkaan laitteet eivät aina takaa taitavan hyökkääjän pääsyä verkon sisään. Tietoturvan kannalta ovat olennaisia verkonvalvonnan tunkeutumisenhavaitsemis- ja murronestojärjestelmät eli IDS- ja IPS-järjestelmät, joilla kerätään ja analysoidaan verkko-

liikennettä. Ennaltaehkäisevä verkonvalvontatyö ja verkon tapahtumien jatkuva seuraaminen ovat verkkoturvallisuuden kannalta tärkeitä. Havahtuminen verkonvalvontaan vasta siinä vaiheessa, kun hyökkääjä on jo saanut valjastettua laitteen omaan palvelunestohyökkäykseensä, on liian myöhäistä.

Tässä insinöörityössä perehdytään verkonvalvontaan tietoturvan näkökulmasta. Työssä käydään läpi neljän eri verkonvalvontaohjelman asentaminen Ubuntu 14.04.3 LTS linux -työasemalle ja vertaillaan, mitä verkon tietoturvasta voidaan nähdä milläkin ohjelmalla. Työssä selvitetään myös, mikä ohjelmista on käyttöliittymältään helppokäyttöisin. Työssä käytettäviksi ohjelmistoiksi valittiin neljä avoimen lähdekoodin verkonvalvontaohjelmistoa: Zabbix, Observium, Icinga ja Cacti. Avoimen lähdekoodin ansiosta ohjelmat ovat hyvin saatavilla, kustannustehokkaita ja ennen kaikkea laadukkaita. Kuka tahansa voi muokata avointa lähdekoodia ja parannella sitä huomatessaan puutteita. Näin ollen ohjelmilla on huomattavasti enemmän kehittäjiä kuin suljetun lähdekoodin ohjelmilla. Mitä useampi käyttäjä pääsee tarkastelemaan lähdekoodia, sitä varmemmin koodista saadaan korjattua ongelmat. Verkonvalvontaan liittyvän selvitystyön tekeminen edellyttää verkonvalvontaohjelmien käyttämien protokollien tuntemista, joihin perehdytään työn alussa.

Työn loppuosassa vertaillaan avoimen lähdekoodin verkonvalvontaohjelmistojen asennusta ja käyttöönottoa sekä verkon tietoturvasta ohjelmistoilla nähtävissä olevia tietoja. Selvitystyön tavoitteena on saada tietoa verkonvalvonnassa hyödynnettävistä protokollista sekä siitä, mitä vaiheita verkonvalvontaohjelman asentaminen Ubuntu-työasemalle sisältää. Tavoitteena on myös, että avoimen lähdekoodin ohjelmistojen vertailutuloksia on mahdollista hyödyntää verkonvalvontaan parhaiten soveltuvan ohjelmiston valinnassa.

2 Verkonvalvontaohjelmien käyttämät protokollat

Kaikki verkossa tapahtuva liikenne tapahtuu protokollien sääntöjä noudattaen. Verkonvalvontaohjelmat etsivät protokollien avulla verkossa liikkuvaa dataa ja protokollatietoja. Tämän vuoksi protokollien sääntöjen ja toiminnan tunteminen on keskeistä.

2.1 Discovery-protokollat

Discovery- eli löydösprotokollia käytetään hankkimaan tietoa verkossa olevista laitteista. Löydösprotokollilla voidaan selvittää esimerkiksi se, mitä protokollia eri laitteet käyttävät ja millä alustalla laite toimii. Moni tietoverkkoihin erikoistunut laitevalmistaja on tehnyt laitteilleen oman discovery-protokollan, esimerkiksi Ciscon CDP (Cisco Discovery Protocol), Extreme Networksin EDP (Extreme Discovery Protocol), Foundry Networksin FDP (Foundry Discovery Protocol). Lisäksi löytyy myös laitevalmistajavapaa LLDP (Link Layer Discovery Protocol). Jokainen näistä protokollista toimii pitkälti samalla periaatteella. Kaikkien protokollien tarkoituksena on hankkia tietoa verkossa olevista laitteista. Cisco on yksi suurimmista verkkolaitevalmistajista, ja siksi tässä työssä perehdytään tarkemmin Ciscon CDP-protokollaan.

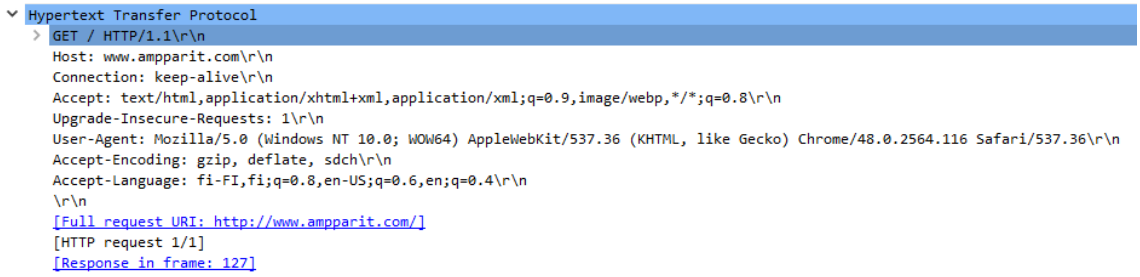
CDP eli Cisco Discovery Protocol on OSI-mallin siirtokerroksella toimiva protokolla, jonka kehittäjä on Cisco Systems. CDP-protokollaa pystytään ajamaan kaikissa Ciscon valmistamissa laitteissa, esimerkiksi reitittimissä ja kytkimissä. CDP-protokollaa käytetään tiedonhankkimiseen verkossa olevista laitteista, ja sillä saadaan selvitettyä esimerkiksi laitteiden IP-osoitteita ja käyttöjärjestelmätietoja. Koska CDP toimii OSI-mallin siirtokerroksella, se mahdollistaa tietojen hankkimisen myös sellaisten laitteiden välillä, jotka käyttävät OSI-mallin verkkokerroksella eri protokollia.

CDP toimii multicastin eli ryhmälähetyksen avulla. Ciscon laitteet lähettävät oletusarvoisesti 60 sekunnin välein CDP-ilmoituksen ryhmälähetyksenä kaikille verkon laitteille. Näitä CDP-ilmoituksia pystyvät vastaanottamaan verkkolaitteet, jotka tukevat CDP:tä (esimerkiksi Cisco Systemsin valmistamat kytkimet). Kun laite on vastaanottanut CDP-ilmoituksen, se tallentaa sen tauluun myöhempää tarkastelua varten ja merkitsee CDP-ilmoituksen lähettäneen laitteen naapurikseen. [2.] [3.]

2.2 HTTP-protokolla

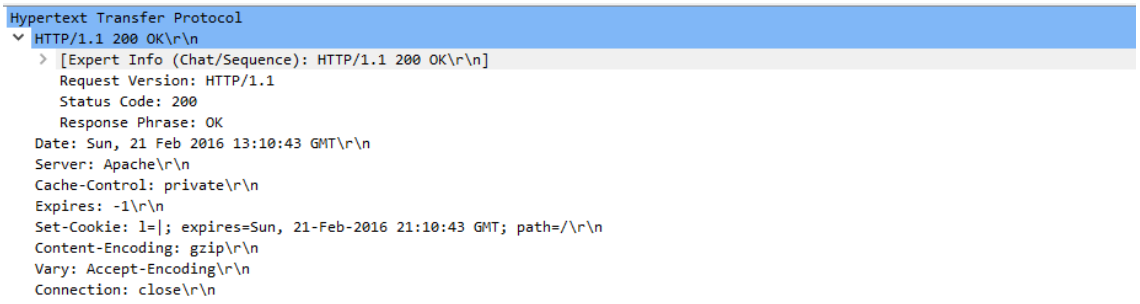
HTTP- eli hypertekstiprotokolla on OSI-mallin sovelluskerroksella toimiva protokolla, jota selain käyttää ottaakseen yhteyden www-palvelimeen ja hakeakseen esimerkiksi HTML-sivun. HTTP on World Wide Webin (www) tärkein protokolla ja perusta kaikelle world wide web -tietoliikenteelle. HTTP:n ensimmäinen yleisessä käytössä ollut versio oli HTTP/1.1 vuonna 1997. Tällä hetkellä uusin versio HTTP:stä on vuoden 2015 tou-

kokuussa julkaistu versio HTTP/2. HTTP toimii pyyntö-vastaus-periaatteella. Tavanomaisimmassa asiakasohjelman ja palvelimen välisessä istunnossa asiakasohjelma lähettää HTML-sivua haettaessa ensin TCP:n kautta HTTP GET -pyynnön palvelimelle. Vastauksena palvelin lähettää asiakasohjelmalle takaisin statuksensa ja pyydetyn HTML-sivun. [4.] [5.]



Kuva 1. HTTP GET -pyyntö Wiresharkilla tarkasteltuna

Alla on havainnollistettu tilannetta, jossa HTTP vastaa GET-pyyntöön lähettämällä statuksensa, ja HTML-sivu löytyisi tämän viestin body-osasta.



Kuva 2. HTTP vastaa GET-pyyntöön lähettämällä statuksensa

2.3 ICMP-protokolla

ICMP (Internet Control Message Protocol) on TCP/IP-pinon verkkokerroksella toimiva protokolla, jota käytetään verkon virhesanomien välittämiseen ja verkon diagnosointiin. Esimerkiksi ping- ja traceroute-käskyt hyödyntävät ICMP-protokollaa. ICMP:n kuljettamia virhesanomia ovat esimerkiksi palveluviestit tai tavoiteltu verkon laite ei ole saatavilla -viestit.

ICMP-viesti koostuu kolmesta eri osasta:

- Tyyppi (Type)
- Koodi (Code)
- Tarkistussumma (Checksum)

Tyyppi (Type) sisältää tiedon, minkälaisesta ICMP-viestistä on kyse. Tällaisia tyyppejä ovat esimerkiksi vastaus, laite ei saatavilla, pyyntö jne. Koodi sisältää tarkentavaa tietoa tyypistä. Jos kyseessä on esimerkiksi laite ei saatavilla -tyyppi, tällöin koodi tarkentaa, miksi laite ei ole saatavilla. Tähän liittyviä koodeja ovat esimerkiksi nämä: laite ei saatavilla, päämäärä laitteen verkko ei saatavilla, päämäärän protokolla ei saatavilla. Tarkastussumma on virheen tarkastusta varten ICMP-viestin headerista ja datasta laskettu summa, jolla voidaan tarkastaa ICMP-viestin oikeellisuus. [6; 7.]

2.4 SMTP-protokolla

SMTP (Simple Mail Transfer Protocol) on TCP/IP-pinon sovelluskerroksella toimiva protokolla, jota käytetään sähköpostiviestien lähettämiseen ja kuljettamiseen sähköpostipalvelimien välillä. SMTP-protokollalle on varattu TCP/UDP-portti 25. SMTP on tarkoitettu ainoastaan sähköpostiviestien lähettämistä varten, eli se ei nouda sähköpostiviestejä sähköpostipalvelimelta, vaan tätä toimintoa varten on muita protokollia, kuten esimerkiksi POP ja IMAP.

Normaalitilanteessa sähköpostiviestin lähettäminen tapahtuu niin, että lähettäjä kirjoittaa ensin viestin sähköpostiohjelmallaan, johon hän on laittanut vastaanottajaksi vastaanottajan sähköpostiosoitteen (esimerkiksi vastaanottaja@gmail.com). Kun lähettäjä painaa lähetä-painiketta, sähköpostiviesti lähtee vastaanottajan ja lähettäjän sähköpostiosoitteiden kanssa eteenpäin SMTP-palvelimelle. Tämän jälkeen SMTP-palvelin pilkkoo vastaanottajan sähköpostiosoitteen kahteen osaan: vastaanottaja ja gmail.com. SMTP-palvelin avaa sähköpostiviestin gmail.com-toimialuetiedon avulla TCP-yhteyden oikealle sähköpostipalvelimelle, minkä jälkeen lähettäjän sähköpostipalvelin siirtää sähköpostiviestin SMTP-protokollan avulla vastaanottajan sähköpostipalvelimelle. Tämän jälkeen vastaanottajan sähköpostipalvelin siirtää sähköpostiviestin vastaanottajan postilaatikkoon, jossa se säilyy siihen asti, kunnes vastaanottaja kirjautuu sähköpostiinsa sisään. Kun vastaanottaja kirjautuu sisään sähköpostiinsa, sähköpostin vastaanottamiseen tarkoitettu protokolla, esim. POP-protokolla, hakee sähköpostiviestin sähköpostipalvelimelta vastaanottajan työasemalle. [8.] [9.]

2.5 SNMP-protokolla

SNMP (Simple Network Management Protocol) on nimensä mukaisesti TCP/IP-verkkojen hallintaan käytettävä yksinkertainen protokolla, jolla saadaan selvitettyä tietoja verkossa olevista laitteista. Tiedot talletetaan kunkin laitteen Management Information Base (MIB) -tietokantaan. SNMP:n avulla esille saatuja tietoja ovat esimerkiksi lämpötila, tuuletinnopeus ja muu rautatieto. SNMP onkin erittäin hyödyllinen esimerkiksi tilanteessa, jossa valvotaan satoja palvelimia. Tämänkaltaisessa tilanteessa SNMP-protokollan välityksellä pystytään lähettämään järjestelmänvalvojan koneelle esimerkiksi tieto jonkin palvelimen kotelotuulettimen rikkoutumisesta. SNMP edellyttää, että järjestelmävalvojan koneelle asennetun SNMP-ohjelmiston lisäksi myös verkossa oleville valvottaville laitteille asennetaan SNMP-agent-ohjelma. Nykyisin SNMP on joissakin laitteissa myös sisäänrakennettuna, jolloin erillistä agent-ohjelmaa ei tarvita.

SNMP-viestejä on neljää eri tyyppiä: GET-, GETNEXT-, SET- ja TRAP. GET-viesteillä pyydetään tietoa toiselta verkossa olevalta laitteelta, johon on asennettu SNMP-agent. Tällöin saadaan selville esimerkiksi laitteessa olevan vapaan kovalevytilan määrä. GETNEXT-viesti on samantyyppinen kuin GET-viesti. Erona on se, että GETNEXT-viestillä pystytään selaamaan laitteen kaikki valvottavat objektit loogisessa järjestyksessä. SET-viestiä käytetään lähettämään agentille esimerkiksi muutettava arvo, jonka se tallentaa MIB-tietokantaan. Tämä edellyttää kirjoitusoikeuksia laitteen MIB-tietokantaan. TRAP-viestillä pystytään luomaan hälytyksiä agenteille. TRAP-viesti lähetetään esimerkiksi silloin kun agentti on asetettu valvomaan, ettei laitteen lämpötila nouse yli asetetun raja-arvon. Kun lämpötila nousee yli tämän asetetun raja-arvon, SNMP lähettää TRAP-viestin ilmoittaakseen asiasta esimerkiksi valvontakoneella järjestelmänvalvojan sähköpostiin tai johonkin muuhun kohteeseen, johon se on ohjelmoitu lähettämään ilmoitus. [10.] [11.]

2.6 SSH-protokolla

SSH (Secure Shell) on protokolla, joka mahdollistaa salatun yhteyden ottamisen verkossa oleviin laitteisiin salaamattoman verkon yli. Secure Shell -protokollalla pystytään esimerkiksi kirjautumaan sisään verkossa oleviin laitteisiin komentoriviyhteydellä ja suorittamaan niissä käskyjä. Secure Shell kehitettiin alun perin Telnetin ja muiden salaamattomia komentoriviyhteyksiä tarjoavien protokollien tietoturvallisemmaksi vaihto-

ehdoksi. Esimerkiksi Telnetissä salasanat liikkuvat verkossa selkokielisinä, jolloin kuka tahansa pystyy pakettianalyysin avulla selvittämään käyttäjien salasanoja.

Secure Shell -protokollaa pystytään käyttämään kahdella tavalla. Toisessa tavassa Secure Shell käyttää julkisen avaimen salaamista todentaakseen etäkoneen ja sallii sen todentaa käyttäjän, mikäli tämä on tarpeen. Toinen tapa on manuaalisesti luotu avainpari, joista toinen avain on julkinen ja toinen yksityinen. Tällöin julkinen avain jaetaan kaikille koneille, joihin käyttäjän tai ohjelman pitää päästä. Todennus toimii siten, että käyttäjällä olevaa yksityistä avainta ei koskaan jaeta kirjauduttavalle koneelle, vaan SSH vain varmentaa, että käyttäjällä on oikea julkinen avain ja siihen käyvä yksityinen avain.

Secure Shell -protokollaa käytetään koneelle etäkirjautumisen lisäksi myös salattuun tiedostojen siirtämiseen. Protokollan porttiohjaus mahdollistaa myös kaiken liikenteen ohjaamisen portin 22 läpi, jolloin pystytään ottamaan esimerkiksi kannettavalla laitteella etäyhteys kotona olevaan laitteeseen ja kierrättämään kaikki internetliikenne kotilaitteen kautta salatulla SSH-yhteydellä. Tällä tavoin pystytään suojaamaan verkkoliikennettä esimerkiksi kahvilan avointa wlan-yhteyttä käytettäessä. [12.]

2.7 TCP-protokolla

TCP (Transmission Control Protocol) on kaiken internetliikenteen tärkein protokolla. TCP mahdollistaa tavuista (8 bittiä) koostuvan datavirran kahden päätepisteen välillä, jossa dataa voi liikkua molempiin suuntiin samaan aikaan. TCP toimii OSI-mallin neljännellä kerroksella eli kuljetuskerroksella.

TCP-yhteydessä on kolme eri vaihetta. Yhteyden muodostaminen alkaa kolmitiekättelyllä, jossa yhteyden aloittaja ottaa yhteyden palvelimeen lähettämällä sille SYN-paketin. Tämän jälkeen palvelin lähettää yhteyden aloittajalle takaisin SYN/ACK-paketin, jolla palvelin tunnistaa, että SYN-paketti on vastaanotettu. Viimeisenä yhteyden aloittaja lähettää palvelimelle takaisin vielä ACK-paketin, jolla yhteyden aloittaja ilmoittaa palvelimelle, että SYN/ACK-paketti on vastaanotettu onnistuneesti. Tämän jälkeen TCP-yhteydessä alkaa itse tiedonsiirto. Tiedonsiirrossa on aina mahdollisuus, että paketti putoaa syystä tai toisesta välistä pois. Tämän vuoksi TCP-protokolla sisältää tiedonsiirtovaihetta varten myös useita mekanismeja, joilla varmistetaan datan ehe-

ys. Näitä mekanismeja ovat sekvenssinumerointi, tarkistussummat, ajastimet ja tunnistimet. TCP-protokolla mahdollistaa myös kaksisuuntaisen tiedonsiirron, jolloin tiedonsiirtovaiheessa ACK-pakettien mukana siirretään dataa myös palvelimelta asiakkaan suuntaan. [13.] [14.] [15.]

3 Tunkeutujanhavaitsemis- ja murronestämisjärjestelmät

Tietoturvan kannalta on tärkeää tietää, mitä laitteita verkossa tulisi olla. Verkon kautta tietoturvasta voidaan nähdä monia asioita: esimerkiksi laitteet, jotka ovat verkossa, mahdollisesti myös laitteet, joiden ei pitäisi olla verkossa, laitteiden ja prosessien tuleva ja lähtevä liikenne, sen oikeellisuus sekä laitteiden resurssien käyttö. Näiden tietojen avulla voidaan selvittää, missä laitteessa eri prosessit toimivat ja tulisiko niiden olla toiminnassa kyseisessä laitteessa, vai onko toiminnan taustalla mahdollisesti jokin tunkeutuja tai haittaohjelma.

3.1 Tunkeutujanhavaitsemisjärjestelmä (IDS)

IDS (Intrusion Detection System) eli tunkeutujanhavaitsemisjärjestelmän määrittely koskee laitetta tai ohjelmaa, joka monitoroi verkkoa tai laitetta haitallisen toiminnan tai käytäntörikkomusten varalta. Kun IDS havaitsee haitallisen toiminnan tai käytäntörikkomuksen verkossa tai laitteessa, se generoi tapahtumasta sähköisen raportin IDS:ää hallinnoivalle isäntälaitteelle. IDS jakautuu kahteen päätyyppiin: NIDS (Network Intrusion Detection Systems) ja HIDS (Host Intrusion Detection Systems). NIDS sijoitetaan verkon kannalta strategiseen kohtaan, missä se pääsee käsiksi kaikkien verkon sisällä olevien laitteiden lähtevään ja saapuvaan liikenteeseen. Esimerkki NIDS:n sijainti verkossa voisi olla palomuurin kanssa samassa verkon kohdassa, jolloin NIDS pystyisi monitoroimaan mahdollisia palomuuriin kohdistuvia hyökkäyksiä ja lähettämään raportteja niistä järjestelmänvalvojalle. HIDS-toimintoa ajetaan yksittäisellä työasemalla tai laitteella, ja se valvoo työaseman tai laitteen tulevaa ja lähtevää liikennettä. HIDS ottaa vedoksia olemassa olevista järjestelmätiedostoista ja vertaa niitä aikaisempiin vedoksiin. Mikäli järjestelmän kannalta kriittisiä tiedostoja on editoitu tai poistettu, HIDS lähettää asiasta hälytyksen järjestelmänvalvojalle. HIDS on käytössä esimerkiksi laitteissa, joissa on tärkeätä konfiguraation muuttumattomuus. [16.] [17.]

3.2 Murronestämisjärjestelmä (IPS)

IPS (Intrusion Prevention System) eli murronestämisjärjestelmän määrittely koskee verkkolaitetta, joka monitoroi verkkoa ja/tai työasemien ja laitteiden mahdollisia haitallisia toimia. IPS:n tärkein tehtävä on tunnistaa mahdollinen haitallinen toiminta, tehdä lokitiedosta tapahtuneesta, yrittää pysäyttää tai estää toiminta ja raportoida. IPS toimii siis laajalti samankaltaisesti kuin IDS, mutta verkkoliikenteen ja laitteiden toimintojen monitoroinnin lisäksi se pystyy tarvittaessa myös puuttumaan verkon tapahtumiin ennaltaehkäisemällä ja estämällä mahdolliset tunkeutujat sekä haitallisen toiminnan. Mikäli IPS huomaa verkossa epäilyttävää toimintaa, se pystyy lähettämään tapahtumasta hälytyksen, pudottamaan haitalliset paketit, nollaamaan yhteyden tai estämään liikenteen tunkeutujan IP-osoitteesta. Lisäksi IPS pystyy korjaamaan CRC (Cyclic Redundancy Check) -virhesanomia, eheyttämään pakettivirtoja, estämään TCP-sekvenssiongelmat ja puhdistamaan kuljetus- ja verkkokerroksen asetukset, joita ei haluta käyttää.

IPS-järjestelmät voidaan jakaa neljään eri luokkaan:

- NIPS (Network-based Intrusion Prevention System) monitoroi verkkoa haitallisen liikenteen varalta analysoimalla protokollien toimintaa.
- WIPS (Wireless Intrusion Prevention System) monitoroi langatonta verkkoa haitallisen verkkoliikenteen varalta analysoimalla langattoman verkon protokollien toimintaa.
- NBA (Network Behavior Analysis) analysoi liikennettä ja pyrkii tunnistamaan uhkat, jotka aiheuttavat epätavallista verkkoliikennettä. Esimerkiksi DDos- hyökkäykset, jotkin tietyt haittaohjelmat ja policy-rikkomukset.
- HIPS (Host-based Intrusion Prevention System) työasemalle asennettu ohjelma, joka monitoroi kyseistä työasemaa mahdollisen haitallisen toiminnan varalta analysoimalla työaseman sisällä tapahtuvia tapahtumia.

IPS-järjestelmät käyttävät tunkeutumisen havaitsemiseen kolmea eri metodia.

Signature-Based Detection toimii virustutkan tavoin monitoroimalla ja etsimällä liikenteestä ennalta tiedossa olevia hyökkäyksiä eli signatureja, joita se saa päivityksien muodossa säännöllisesti tietokantaansa. Metodi on erittäin tehokas tunnettujen hyökkäyksien torjunnassa, mutta toisaalta se on vain niin tehokas kuin sen viimeisin signature-tietokanta.

Statistical Anomaly-Based Detection eli poikkeamaan perustuva tunkeutumisen havaitseminen toimii siten, että IPS suodattaa IP-pakettien headerit ja päästää niistä läpi kaiken tunnetun liikenteen, esim. web-liikenteen organisaation web-palvelimelle, sähköpostiliikenteen organisaation sähköpostipalvelimelle ja siitä ulospäin, DNS-liikenteen organisaation DNS-palvelimelle jne. Metodi on osaavissa käsissä tehokas, ja sen etu Signature-Based Detection -havaitsemiseen verrattuna on se, että Anomaly-Based Detection pystyy pysäyttämään myös uudet tuntemattomat tunkeutumisyritykset. Toisaalta metodi vaatii käyttäjältään enemmän tietotaitoa, koska sille pitää jatkuvasti ”opettaa”, mikä on normaalia verkossa tapahtuvaa liikennettä.

Stateful Protocol Analysis Detection toimii analysoimalla protokollien (esimerkiksi DNS, FTP, HTTP, SMTP) toimintaa yhteyden ollessa käynnissä. IDS joka suorittaa Stateful Protocol -analysointia, tuntee protokollien toiminnan normaalitilanteessa ja hälyttää huomatessaan normaalista poikkeavaa liikennettä.

Suurin osa IPS-järjestelmistä käyttää yhtä kolmesta edellä mainitusta metodista tunkeutumisen tai tunkeutumisen yrityksen havaitsemiseen. [18.]

4 Vertailtavat verkonvalvontaohjelmat

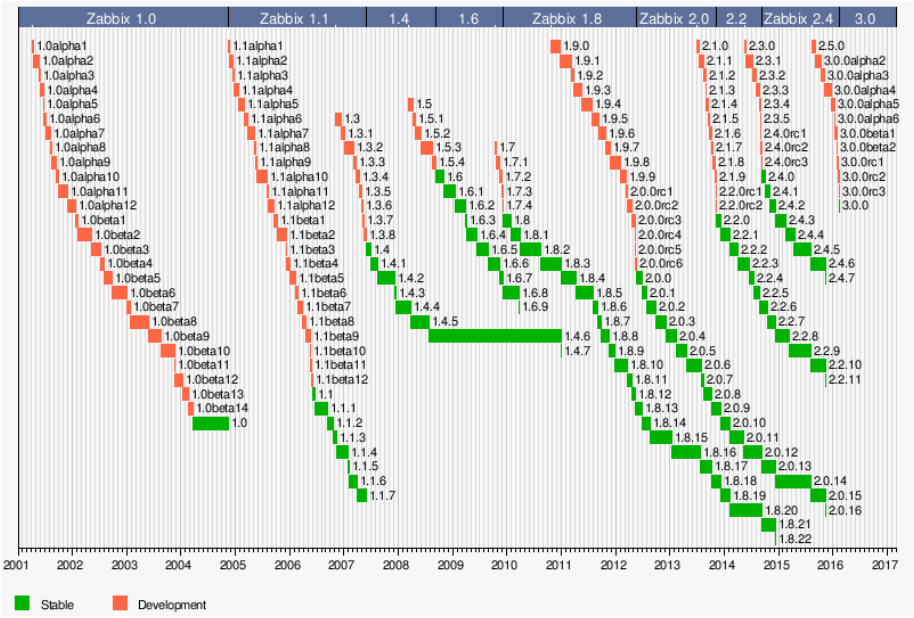
Työssä vertailtavat verkonvalvontaan käytettävät ohjelmistot ovat kaikki Open Source -ohjelmistoja eli avoimen lähdekoodin ohjelmistoja. Tähän päädyttiin, koska avoimen lähdekoodin ohjelmien käyttöön liittyy monia etuja, niin toiminnallisia kuin taloudellisia. Keskeisimpinä avoimen lähdekoodin etuina voidaan pitää tietoturvaa, ohjelmien räätälöintimahdollisuuksia, alustavapautta, yhteensopivuutta ja hintaa.

Avoimen lähdekoodin ohjelmistot ovat usein tietoturvallisia. Tämä selittyy sillä, että koodin ollessa avointa kuka tahansa käyttäjä voi tarkastella koodia. Mitä useampi tekee näin, sitä varmemmin koodista saadaan poistettua ongelmat. Tämän lisäksi avoimen lähdekoodin ohjelmat ovat hyvin räätälöitävissä kunkin käyttäjän omiin tarpeisiin. Koska koodia voi muokata kuka tahansa, ohjelmaa on helppo muokata omiin tarpeisiin sopivaksi. Avoimen lähdekoodin ohjelmistot eivät myöskään ole laitteistoon sidottuja, ja ne tukevat avoimia standardeja. Tällä saavutetaan se, että avoimen lähdekoodin ohjelmistot toimivat monilla eri alustoilla, ja ne ovat erittäin yhteensopivia. Myös ohjelmistojen hinta on yritysmaailmassa yksi tärkeimmistä syistä ohjelmistovalintoja tehtäessä.

Avoimen lähdekoodin ohjelmistojen kustannukset ovat huomattavasti pienempiä kuin suljettujen ohjelmistojen, mikä on avoimen lähdekoodin ohjelmistojen myyntivalttina tällä alueella.

4.1 Zabbix-ohjelmisto

Zabbix on vuonna 1998 Alexei Vladishevin alkuun laittama projekti, jonka tavoitteena oli luoda yrityskäyttöön soveltuva avoimeen lähdekoodin perustuva verkonvalvontaohjelmisto. Ensimmäinen vakaa versio julkaistiin vuonna 2004 nimellä Zabbix 1.0, ja tämän jälkeen Zabbix on edennyt vuoden 2016 versioon Zabbix 3.0. Vuonna 2005 perustettiin Zabbix-yritys ammattitaitoisen teknisen tuen takaamiseksi Zabbix-ohjelmistoille. Zabbix on tässä insinöörityössä käytetyistä verkonvalvontaohjelmista tunnetuin (kuvat 3 ja 4).



Kuva 3. Zabbixin eri versioiden aikajana. Version 1.1 jälkeen on otettu käyttöön kolminumeroiset kehitysversiot. [19.]

Kuva 4. Zabbixin levinneisyys [20]

Zabbix server -ohjelmisto on kirjoitettu C-kielellä, ja se sisältää myös PHP:llä toteutetun Web-käyttöliittymän. Monitorointidatan tallentamisessa Zabbix tukee MySQL-, Oracle-, SQlite- ja PostgreSQL-tietokantoja. Zabbix server tukee ainoastaan Linux/UNIX-käyttöjärjestelmiä, mutta sen agent-ohjelma voidaan asentaa Linux/UNIX-järjestelmien lisäksi myös Windowsille.

4.2 Observium-ohjelmisto

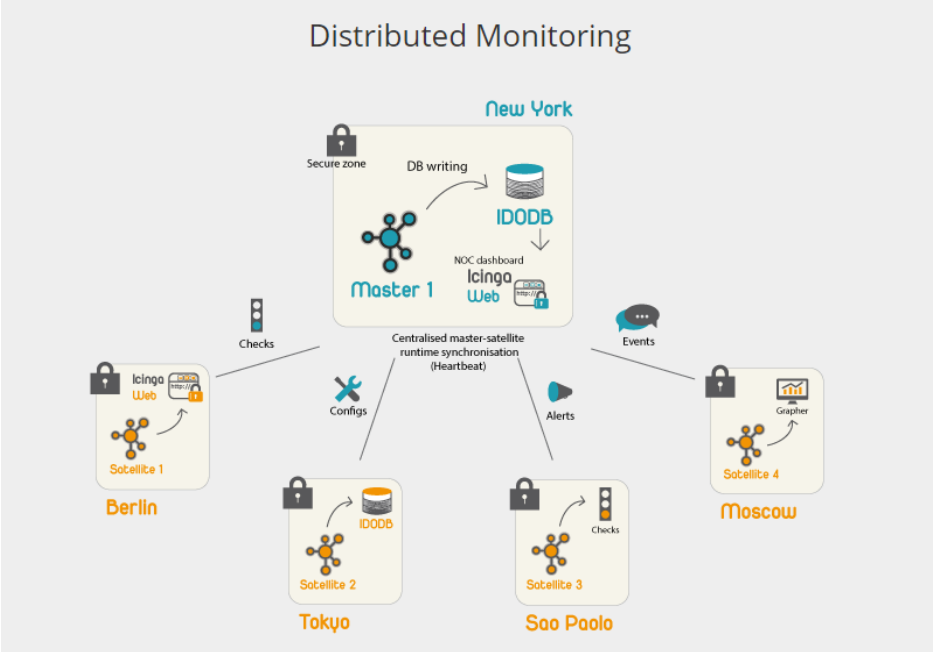
Observium sai alkunsa Adam Armstrongin luomasta koodista, jonka hän kirjoitti kartoittaakseen hänelle tuntematonta verkkoympäristöä. Koodi toimi piirtämällä kerätyn CDP-datan avulla kartan verkosta, joka mahdollisti laitteiden tietojen selaamisen klikkaamalla laitteita. Observium on historiansa aikana tunnettu myös nimillä Project Observer (2006 - 2008) ja ObserverNMS (2008 - 2010) ennen Observium nimen vakiintumista.

Observium on kirjoitettu PHP-kielellä, ja siitä on kaksi eri versiota: Observium Professional ja Observium Community Edition. Observium Professional on maksullinen versio, jonka tilaajat saavat aina uusimman version julkaisujen edetessä. Observium Community Edition on yhteisön ylläpitämä versio, jonka uusin versio ilmestyy puolen vuoden välein. [22.]

4.3 Icinga-ohjelmisto

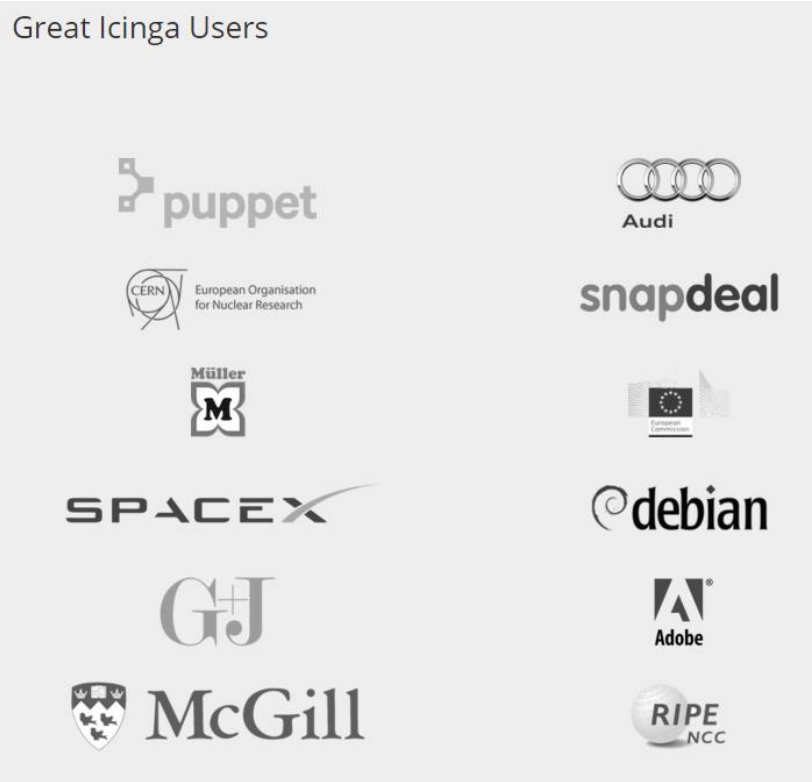
Icinga on alun perin Nagios-nimisen vapaaseen lähdekoodiin perustuvan verkonvalvontaohjelmiston kehityksessä vuonna 2009 tapahtunut forkkaus, eli Nagioksesta tehdystä kopiosta on alettu kehittää itsenäisenä projektina uutta ohjelmistoa Icingaa. Icingan perimmäinen tarkoitus on pyrkiä pääsemään Nagioksen kehityksessä ilmenneiden puutteiden yli ja lisäämään myös uusia ominaisuuksia, kuten Web 2.0 käyttöliittymän. Icinga pystyy monitoroimaan Linux- ja Windows-laitteita, mutta Icinga server toimii ainoastaan Linuxilla. Icinga on tähän työhön valikoituneista ohjelmistoista modulaarisin, ja monet ominaisuudet lisätään Icingaan erillisillä plugineilla. Icingan asennus on hieman monimutkaisempi kuin muiden työssä käytettyjen verkonvalvontaohjelmistojen. Tämän vuoksi työssä käydään Icingan esimerkkiasennus perusteellisemmin läpi.

Icingan etuna ovat muun muassa tietoturva ja redundanttisuus, jonka mahdollistaa Icingan komponenttien hajautettu asentaminen (kuva 5).



Kuva 5. Esimerkki Icingalla toteutetusta hajautetusta monitoroinnista [24]

Icinga on tässä työssä käytetyistä verkonvalvontaohjelmistoista toiseksi suosituin Zabbixin jälkeen. Icingaa on käytetty onnistuneesti suurissa yritysympäristöissä (kuva 6).



Kuva 6. Merkittäviä Icingaa käyttäviä yrityksiä [24]

4.4 Cacti-ohjelmisto

Cacti-ohjelmisto sai alkunsa vuonna 2001, kun Cactin luoja Ian Berry alkoi kehittää luontevampaa käyttöliittymää aikasarjadataa käsittelevälle RRD-työkalulle, joka käyttää SNMP:tä datan keräämiseen. Projektin keskeisimpänä tavoitteena oli tarjota RRD-työkalua heppokäyttöisempi työkalu, joka olisi samalla myös joustavampi kuin reitittimien monitorointitietojen ja verkonkäyttöasteen graafiseen esittämiseen suunniteltu MRTG. Cacti-ohjelmiston ensimmäinen versio julkaistiin kolme vuotta myöhemmin vuonna 2004. Tällä hetkellä uusin vakaa versio on 0.8.8g, joka julkaistiin vuonna 2016. Cacti on kirjoitettu käyttäen PHP:tä ja MySQL:ää. Muista tässä työssä käytetyistä verkonvalvontasovelluksista poiketen Cacti voidaan asentaa Linuxin lisäksi myös Windows-alustalle. [27.]

5 Verkonvalvontaohjelmistojen asentaminen

Tässä luvussa esitetään Zabbix-, Observium- ja Cacti-ohjelmistojen asentaminen pääpiirteittäin sekä Icinga-ohjelmiston asennus yksityiskohtaisempana esityksenä.

5.1 Zabbix-ohjelmiston asentaminen

Zabbix on mahdollista asentaa lähdekoodista tai suoraan asennuspaketeista. Tässä asennustyössä Zabbix asennetaan asennuspaketeista, jolloin säästytään lähdekoodin kääntämiseltä.

Zabbixin asentamisessa on kuusi eri vaihetta. Ensin asennetaan repositorio, josta asennustiedostot löytyvät. Tämä tapahtuu syöttämällä terminaliin seuraavat komennot:

```
# wget http://repo.zabbix.com/zabbix/3.0/ubuntu/pool/main/z/zabbix-
release/zabbix-release_3.0-1+trusty_all.deb
# dpkg -i zabbix-release_3.0-1+trusty_all.deb
# apt-get update
```

Seuraavaksi asennetaan Zabbix server ja web-käyttöliittymä sekä MySQL-tietokanta syöttämällä terminaliin nämä komennot:

```
# apt-get install zabbix-server-mysql zabbix-frontend-php
```

Vaihtoehtoisesti pelkkää Zabbix-agenttia varten syötettäisiin tämä komento:

```
# apt-get install zabbix-agent
```

Tässä vaiheessa on tarpeen luoda Zabbix-ohjelmistoa varten MySQL-tietokanta ja sille käyttäjä. Tämä tapahtuu syöttämällä seuraavat komennot:

```
# mysql -uroot -p<password>
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> grant all privileges on zabbix.* to zabbix@localhost identified by
'<password>';
mysql> quit;
# cd database/mysql
# mysql -uzabbix -p<password> zabbix < schema.sql
# mysql -uzabbix -p<password> zabbix < images.sql
# mysql -uzabbix -p<password> zabbix < data.sql
```

Kun MySQL-tietokanta on luotu, siihen tuodaan alustava schema ja data seuraavilla komennoilla:

```
# cd /usr/share/doc/zabbix-server-mysql
# zcat create.sql.gz | mysql -uroot zabbix
```

Tämän jälkeen muokataan Zabbixin tietokannan konfiguraatiotiedostoa vi-editorilla komennolla

```
# vi /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabbix
```

Tämän jälkeen Zabbix server -prosessi voidaan käynnistää komennolla

```
# service zabbix-server start
```

Lopuksi editoidaan Zabbix-käyttöliittymän PHP-konfiguraatioon

```
/etc/apache2/conf.d/zabbix
```

oikea aikavyöhyke ja otetaan kommenttimerkki pois käyttäen esimerkiksi vi-editoria. Tiedoston konfiguraation tulisi näyttää tältä:

```
php_value max_execution_time 300
php_value memory_limit 128M
php_value post_max_size 16M
php_value upload_max_filesize 2M
php_value max_input_time 300
php_value always_populate_raw_post_data -1
php_value date.timezone Europe/Riga
```

Lopuksi uudelleenkäynnistetään vielä Apache web server komennolla

```
# service apache2 restart
```

[21.]

5.2 Observium-ohjelmiston asentaminen

Observiumin Community Edition -ohjelmiston asentaminen tapahtuu terminalin kautta. Ensin asennetaan Observiumin tarvitsemat paketit syöttämällä käsky

```
# apt-get install libapache2-mod-php5 php5-cli php5-mysql php5-gd php5-mcrypt
php5-json php-pear snmp fping \ mysql-server mysql-client python-mysqldb
rrdtool subversion whois mtr-tiny ipmitool graphviz imagemagick
```

Observium asennukselle luodaan hakemisto ja siirrytään hakemistoon komennolla

```
# mkdir –p /opt/observium && cd /opt
```

Seuraavaksi ladataan Observiumin uusin .tar.gz-paketti ja puretaan se käskyillä

```
# wget http://www.observium.org/observium-community-latest.tar.gz
# tar zxvf observium-community-latest.tar.gz
```

Siirrytään hakemistoon observium komennolla

```
# cd observium
```

Kopioidaan oletuskonfiguraatiotiedosto komennolla

```
# cp config.php.default config.php
```

Tämän jälkeen on tarpeen muokata config.php-tiedostoon MySQL käyttäjänimi ja salasana. Tämä onnistuu esimerkiksi nano-tekstieditoria käyttäen seuraavalla komennolla:

```
# nano config.php
```

Seuraavaksi luodaan tietokanta komennoilla

```
# mysql -u root –p
<mysql root password>
mysql> CREATE DATABASE observium DEFAULT CHARACTER SET utf8 COLLATE
utf8_general_ci;
mysql> GRANT ALL PRIVILEGES ON observium.* TO 'observium'@'localhost' -> IDEN-
TIFIED BY '<observium db password>';
```

Tämän jälkeen tietokantaan tuodaan alustava schema komennolla

```
# ./discovery.php –u
```

Luodaan hakemistot, joihin Observium tallettaa logit ja RRD:t, ja määritetään hakemiston omistusoikeus komennoilla

```
# mkdir logs
```

```
# mkdir rrd
# chown www-data:www-data rrd
```

Seuraavaksi konfiguroidaan Apache muuttamalla tiedoston /etc/apache2/sites-available/default sisältö seuraavanlaiseksi käyttäen esimerkiksi nano-tekstieditoria:

```
<VirtualHost *:80>
            ServerAdmin webmaster@localhost
            DocumentRoot /opt/observium/html
            <FilesMatch \.php$>
                        SetHandler application/x-httpd-php
            </FilesMatch>
            <Directory />
                        Options FollowSymLinks
                        AllowOverride None
            </Directory>
            <Directory /opt/observium/html/>
                        DirectoryIndex index.php
                        Options Indexes FollowSymLinks MultiViews
                        AllowOverride All
                        Require all granted
            </Directory>
            ErrorLog ${APACHE_LOG_DIR}/error.log
            LogLevel warn
            CustomLog ${APACHE_LOG_DIR}/access.log combined
            ServerSignature On
</VirtualHost>
```

Seuraavaksi otetaan käyttöön php-kryptausmoduuli komennolla

```
# phpenmod mcrypt
```

Otetaan käyttöön a2en-moduulin päällekirjoitus ja uudelleenkäynnistetään apache frontend komennoilla

```
# a2enmod rewrite
# apache2ctl restart
```

Seuraavaksi lisätään Observiumille ensimmäinen käyttäjätili (Administrator tilille level on 10) ja ensimmäinen monitoroitava laite. Tämä tapahtuu komennoilla

```
# ./adduser.php <username> <password> <level>
# ./add_device.php <hostname> <community> v2c
```

Seuraavaksi ajetaan laitteiden discovery ja kiertokysely läpi, jotta saadaan ensimmäiset datat kerättyä verkosta. Tämä tapahtuu komennoilla

```
# ./discovery.php -h all
# ./poller.php -h all
```

Viimeiseksi ajastetaan vielä discoveryn ja kiertokyselyn ajaminen käyttäen hyväksi crontabia. Tämä tapahtuu luomalla uusi tiedosto /etc/cron.d/observium sisällöllä.

```
33 */6       * * *      root        /opt/observium/discovery.php -h all >>
/dev/null 2>&1

*/5 *        * * *      root         /opt/observium/discovery.php -h new >>
/dev/null 2>&1

*/5 *        * * *      root        /opt/observium/poller-wrapper.py 2 >>
/dev/null 2>&1
```

[23.]

5.3 Icinga-ohjelmiston asentaminen

Myös Icinga-ohjelmiston pystyy asentamaan lähdekoodista tai paketeista. Tässä työssä Icinga asennetaan paketeista syöttämällä terminaliin nämä komennot:

Ensin lisätään Icinga repositoriot ja päivitetään ne komennoilla

```
# add-apt-repository ppa:formorer/icinga
# apt-get update
```

Tämän jälkeen asennetaan Icinga komennolla

```
# apt-get install icinga2
```

Tämän jälkeen varmistetaan, että Icinga on käynnissä. Varmistus tehdään seuraavalla komennolla:

```
# service icinga2 status
```

Icingan pitäisi olla tässä vaiheessa käynnissä. Jos näin ei ole, voidaan Icinga käynnistää syöttämällä komento

```
# service icinga2 start
```

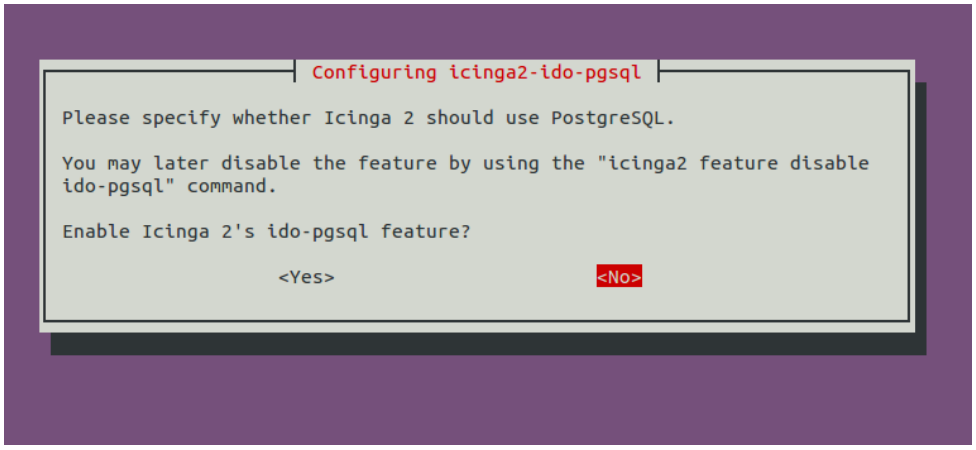
Tämän jälkeen Icingaan lisätään web-käyttöliittymä. Tässä työssä lisätään Web 2 -käyttöliittymä. Web 2 -käyttöliittymä vaatii toimiakseen myös tietokannan, joka on tässä työssä PostgreSQL. Lisäys tehdään komennolla

```
# apt-get install postgresql
```

Seuraavaksi asennetaan Icinga Data Output -paketti, jonka Icinga vaatii toimiakseen PostgreSQL:n kanssa. Tämä tapahtuu syöttämällä komento

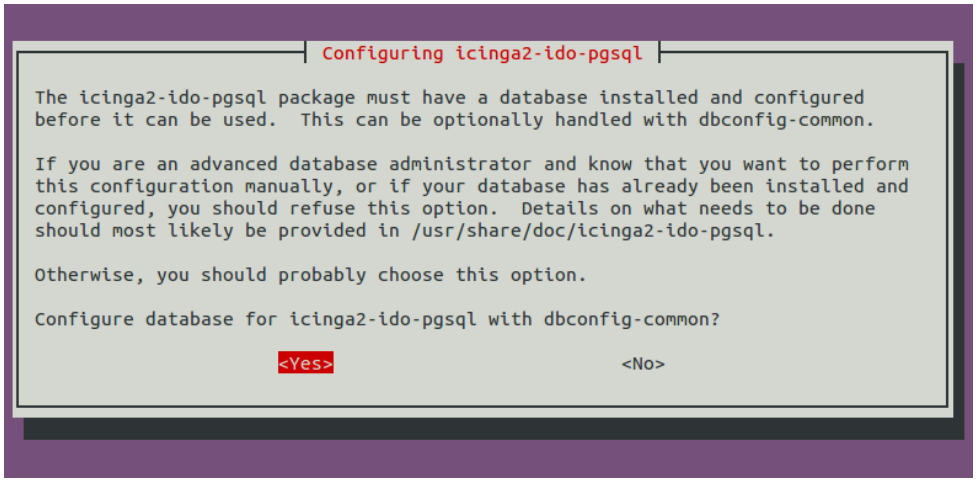
```
# apt-get install icinga2-ido-pgsql
```

Tässä vaiheessa asennus kysyy, halutaanko, että Icinga käyttää PostgreSQL-tietokantaa. Valitaan Yes-vaihtoehto (kuva 7).



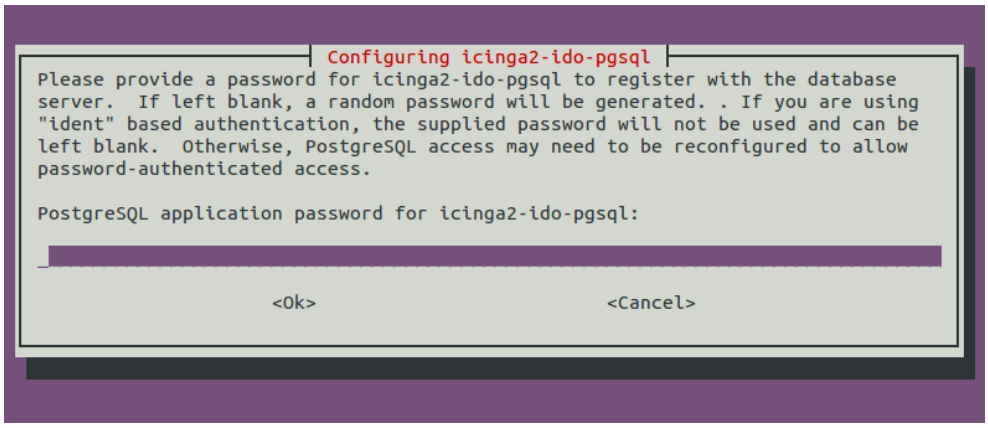
Kuva 7. Icingan konfigurointi käyttämään PostgreSQL-tietokantaa

Seuraavaksi asennus kysyy haluatko, että asennusohjelma konfiguroi tietokannan valmiiksi. Valitaan Yes (kuva 8).



Kuva 8. PostgreSQL -tietokannan asennus ja konfigurointi käyttäen dbconfig-common -toimintoa.

Lopuksi asennus kysyy vielä salasanaa tietokannalle (kuva 9). Tämän voi jättää myös tyhjäksi, jolloin ohjelma generoi salasanan itse.



Kuva 9. PostgreSQL-salasanan syöttäminen

Kun tietokanta on määritelty, se otetaan käyttöön Icingassa komennolla

```
# icinga2 feature enable ido-pgsql
```

Tässä vaiheessa kannattaa myös ottaa käyttöön komentomoduuli komennolla

```
# icinga2 feature enable command
```

Tässä vaiheessa Icinga täytyy uudelleenkäynnistää, jotta tehdyt muutokset astuvat voimaan. Tämä tapahtuu komennolla

```
# service icinga2 restart
```

Kun tietokanta on asennettu, päästään asentamaan itse Web 2 -käyttöliittymää. Ensin lisätään repositorio-avain ja repositorio, josta Web 2 -käyttöliittymä löytyy syöttämällä seuraavat komennot:

```
# wget -O - http://packages.icinga.org/icinga.key | apt-key add -
# add-apt-repository 'deb http://packages.icinga.org/ubuntu icinga-trusty
main'
```

Päivitetään vielä pakettihakemisto komennolla

```
# apt-get update
```

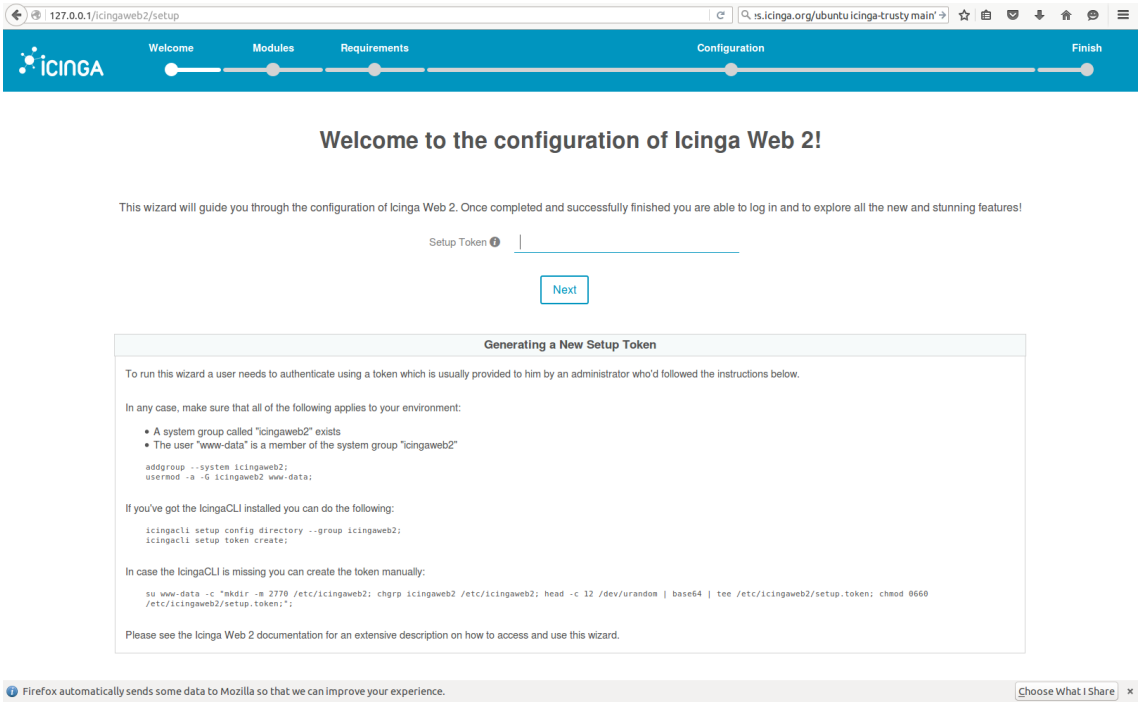
Lopuksi asennetaan itse Web 2 -käyttöliittymä komennolla

```
# apt-get install icingaweb2
```

Tämän jälkeen Web 2 -käyttöliittymä on saatavilla selaimella osoitteessa Icinga koneen IP-osoite/icingaweb2/setup, jossa asennus jatkuu. IP-osoitteen saa selville esimerkiksi syöttämällä terminaliin komennon

```
# ifconfig
```

Kun IP-osoite on selvitetty, siirrytään selaimella seuraavaan osoitteeseen: IP-osoite/icingaweb2/setup. Selaimen tulisi avata kuvassa 10 esitetyn kaltainen sivu.

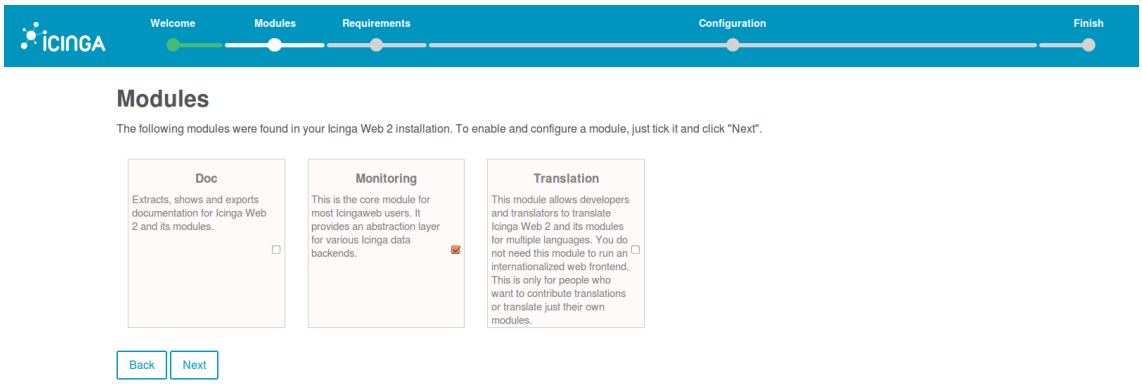


Kuva 10. Icinga Web 2 -käyttöliittymän konfiguraation aloitussivu

Sivu pyytää syöttämään asennus-tokenin, joka luodaan syöttämällä terminaliin komento

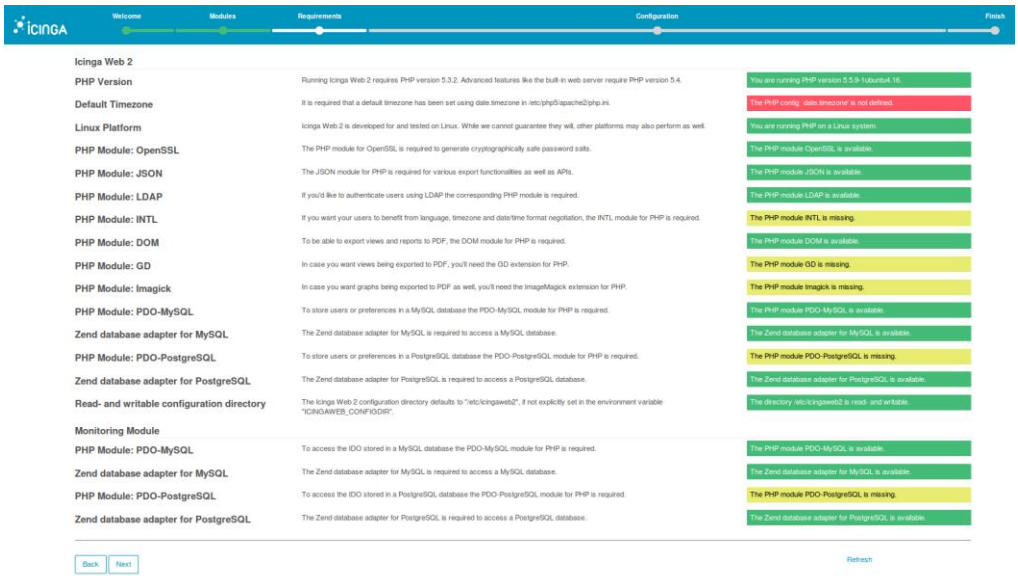
```
# icingacli setup token create
```

Seuraavassa ikkunassa asennus kysyy, mitkä moduulit otetaan käyttöön. Pidetään oletusvalinnat ja klikataan next (kuva 11).



Kuva 11. Web 2 -käyttöliittymään asennettavien moduulien valinta

Seuraavaksi aukeaa yhteenveto, joka näyttää, onko kaikki tarpeellinen Icingaa varten asennettu ja ajan tasalla. Icinga antaa tässä vaiheessa yhden punaisen virhesanoman ja viisi varoitusta (kuva 12).



Kuva 12. Icinga-asennuksen yhteenveto, jossa virheitä ja varoituksia.

Korjataan ensin punaisella merkitty virhesanoma ”The PHP config ’date.timezone’ is not defined”. Tämä korjataan muokkaamalla esimerkiksi nano-tekstieditorilla php.ini-tiedostoon oikea aikavyöhyke. Tämä tapahtuu komennolla

```
# nano /etc/php5/apache2/php.ini
```

Tiedostoon täytyy muokata aikavyöhykkeeksi Europe/Helsinki ja ottaa rivin edestä kommentointi eli puolipiste pois. Tämän jälkeen tallennetaan muutokset (kuva 13).

```
;;;;;;;;;;;;;;;;;;;
; Module Settings ;
;;;;;;;;;;;;;;;;;;;

[CLI Server]
; Whether the CLI web server uses ANSI color coding in its terminal output.
cli_server.color = On

[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
date.timezone = Europe/Helsinki

; http://php.net/date.default-latitude
;date.default_latitude = 31.7667

; http://php.net/date.default-longitude
;date.default_longitude = 35.2333
```

Kuva 13. Aikavyöhykkeen muokkaaminen php.ini-tiedostoon nano-tekstieditorilla

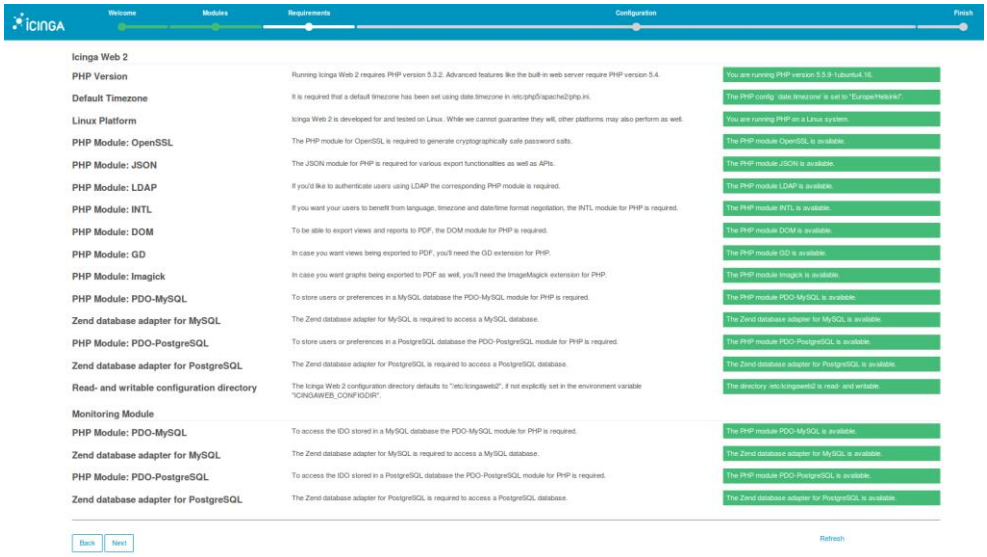
Seuraavaksi korjataan varoitukset asentamalla puuttuvat paketit komennolla

```
# apt-get install php5-json php5-gd php5-imagekick php5-pgsql php5-intl
```

Uudelleenkäynnistetään Apache syöttämällä komento

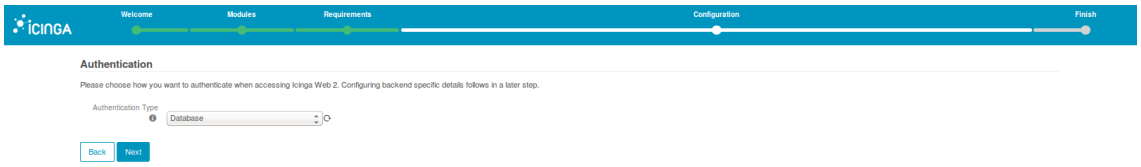
```
# service apache2 restart
```

Kun päivitetään selaimen sivu, kaikkien kohtien tulisi näyttää vihreää (kuva 14).



Kuva 14. Icinga-asennuksen yhteenveto virheiden ja varoituksien korjaamisen jälkeen

Seuraavassa ikkunassa kysytään todennustapaa. Valitaan Database ja siirrytään eteenpäin valitsemalla next (kuva 15).



Kuva 15. Web 2 -käyttöliittymän todennustavan valinta

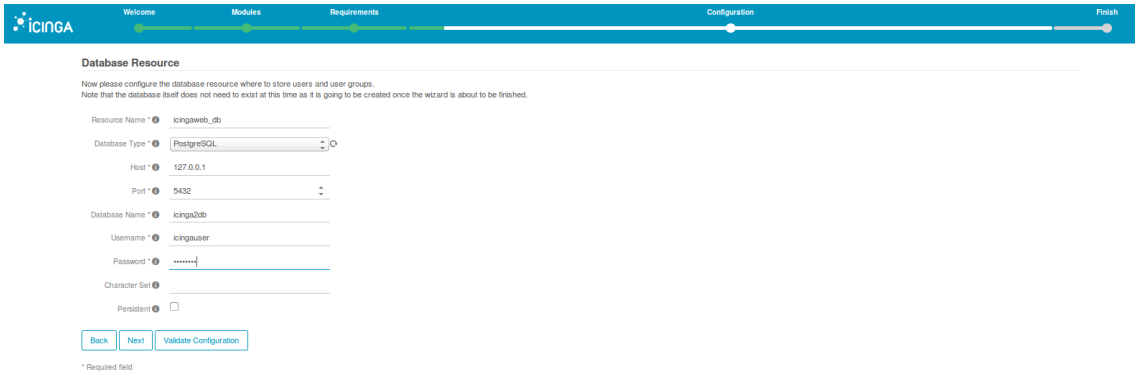
Seuraavaksi konfiguroidaan tietokanta valitsemalla tietokannan tyypiksi PostgreSQL ja asettamalla Hostiksi koneen IP-osoite. Port-kohta on valmiiksi 5432. Lopuksi nimetään tietokanta sekä käyttäjä ja syötetään käyttäjälle salasana.

Tässä vaiheessa kannattaa luoda käyttäjä ja tietokanta syöttämällä terminaliin komennot

```
# sudo –u  postgres psql –c ”CREATE ROLE käyttäjänimi WITH LOGIN PASSWORD
’salasana’”
```

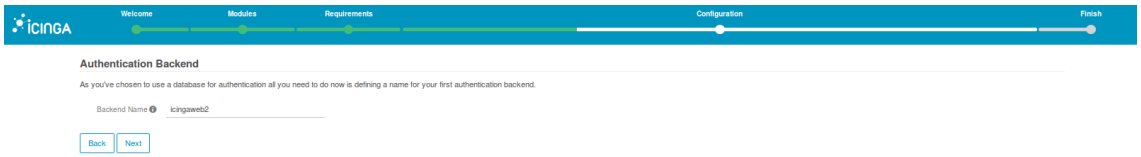
```
# sudo –u postgres createdb –O käyttäjänimi salasana
```

Tietokannan toimivuuden pystyy testaamaan painamalla selaimen sivulla Validate Configuration –painiketta (kuva 16).



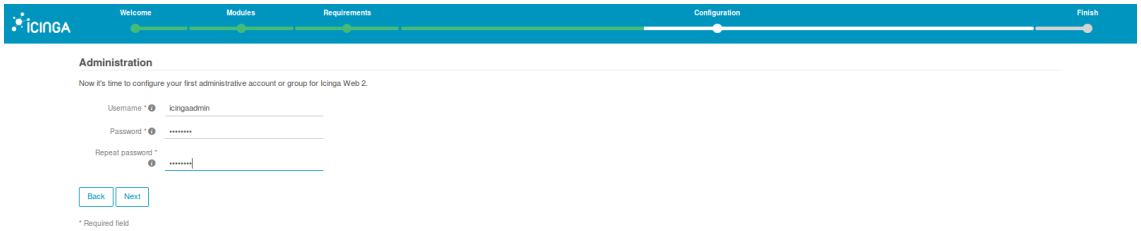
Kuva 16. Käytettävän tietokannan määrittäminen

Seuraavaksi asennus kysyy todennusmetodille nimeä. Käytetään oletusnimeä ja valitaan next (kuva 17).



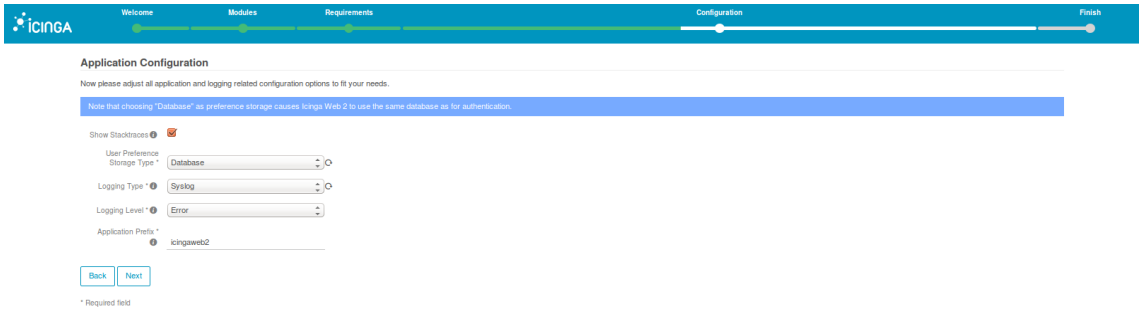
Kuva 17. Todennusmetodin nimeäminen

Seuraavaksi luodaan administrator-tili syöttämällä sille nimi, salasana ja salasanan vahvistus (kuva 18).



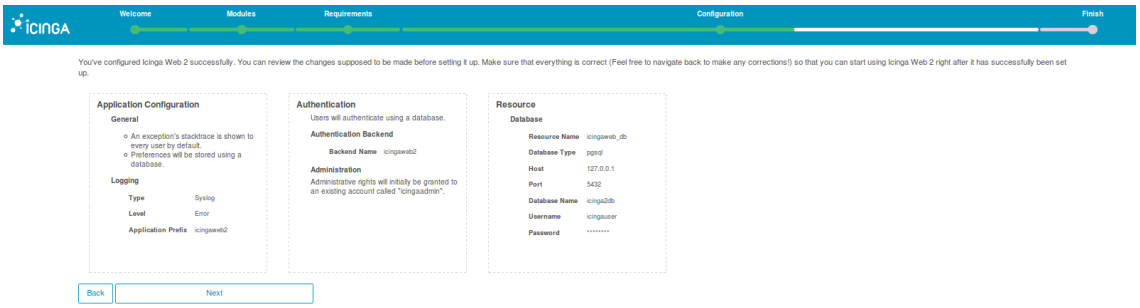
Kuva 18. Administrator-tilin luominen

Seuraavaksi asennus antaa muuttaa sovellukseen ja lokeihin liittyviä valintoja. Oletukset käyvät tässä vaiheessa (kuva 19).



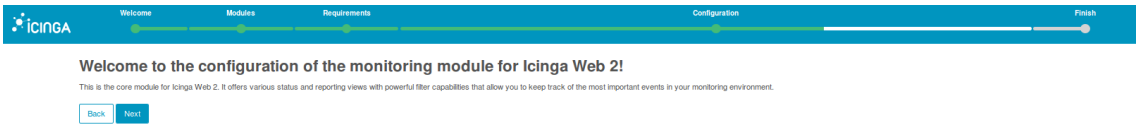
Kuva 19. Sovellukseen ja lokeihin liittyvien valintojen muuttaminen.

Kuvassa 20 näytetään yhteenveto tehdystä konfiguraatiosta.



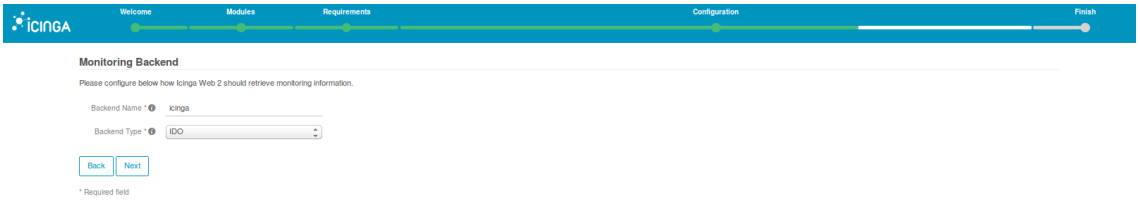
Kuva 20. Yhteenveto tehdyistä konfiguraatioasetuksista

Tämän jälkeen konfiguroidaan Icingan ja Web 2 -käyttöliittymän välinen yhteys (kuva 21).



Kuva 21. Icingan ja Web 2 -käyttöliittymän välisen yhteyden konfiguroinnin aloitusikkuna

Seuraavalla sivulla valitaan kuinka Web 2 -käyttöliittymä hakee verkonvalvontatietoja. Oletukset käyvät tässä vaiheessa (kuva 22).

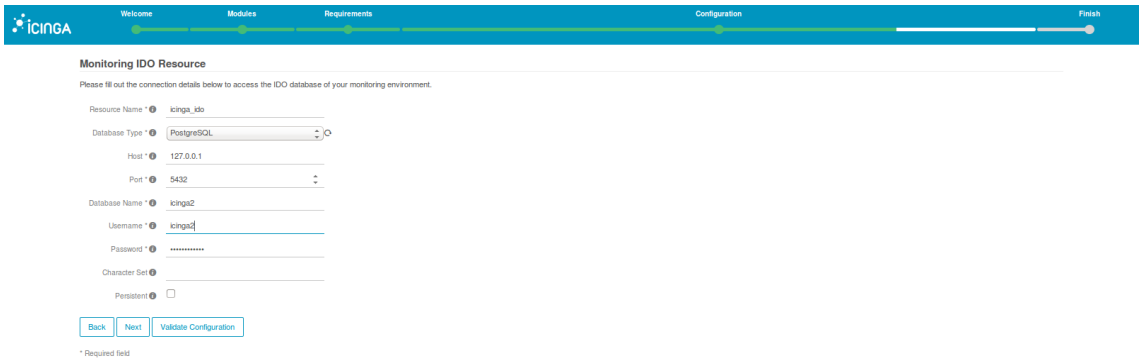


Kuva 22. Verkonvalvontatietojen hakemiseen liittyvien valintojen ikkuna.

Seuraavaksi asennus pyytää syöttämään tietoja, jotka Web 2 -käyttöliittymä tarvitsee päästäkseen käsiksi Icinga Data Output -tietokantaan. Nämä tiedot löytyvät tiedostosta ido-pgsql.conf, jota voi tarkastella esimerkiksi nano-tekstieditorilla komennolla

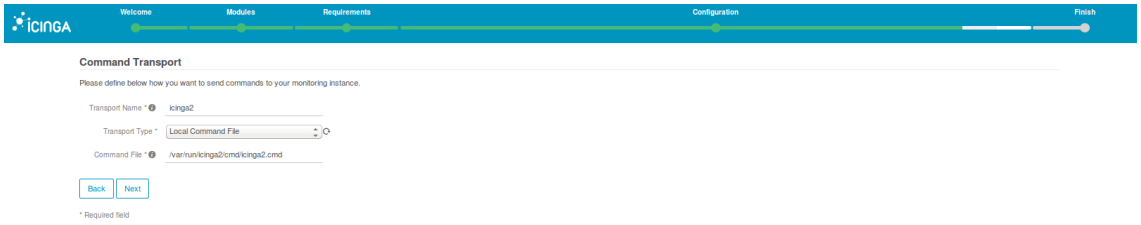
```
# nano /etc/icinga2/features-enabled/ido-pgsql.conf
```

Tarvittavat tiedot ovat tietokannan nimi, käyttäjänimi ja salasana. Syötettyjen tietojen oikeellisuuden pystyy tässä vaiheessa varmistamaan valitsemalla Validate Configuration (kuva 23).



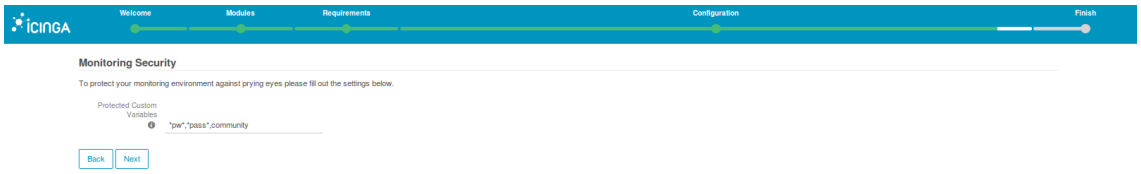
Kuva 23. Icinga Data Output -tietokantaan pääsyyn liittyvien tietojen täyttäminen

Seuraavaksi valitaan, kuinka monitorointikomentoja halutaan lähettää. Oletusarvot käyvät tässä vaiheessa (kuva 24).



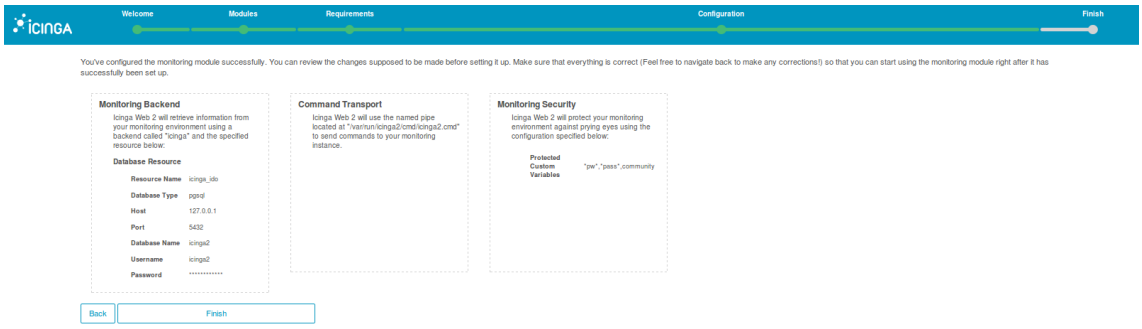
Kuva 24. Monitorointi komentojen lähettämiseen liittyvät valinnat.

Seuraavassa ikkunassa valitaan, mitkä monitorointiympäristön muuttujat halutaan suojata mahdolliselta urkinnalta. Oletusarvot käyvät tässä vaiheessa (kuva 25).



Kuva 25. Verkonvalvontaympäristön tietoturvaan liittyvät valinnat

Lopuksi asennus näyttää yhteenvedon Icingan ja Web 2 -käyttöliittymän välisen yhteyden konfiguraatiosta. Tätä on havainnollistettu kuvassa 26.



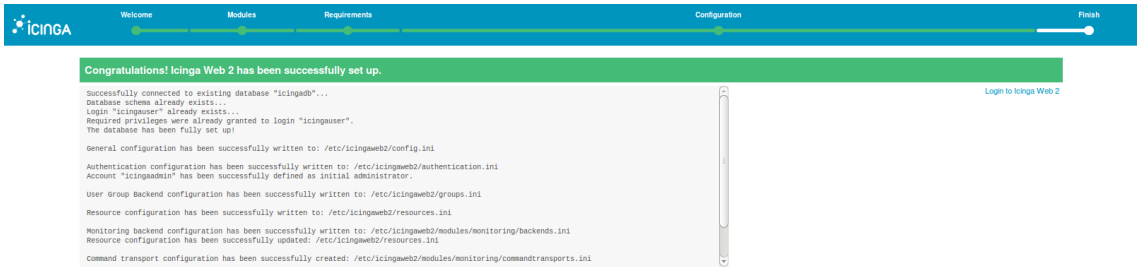
Kuva 26. Yhteenveto Icingan ja Web 2 -käyttöliittymän välisestä konfiguraatiosta

Valitaan finish, minkä jälkeen seuraava ikkuna näyttää, onnistuiko Icinga Web 2 -käyttöliittymän konfigurointi.

Konfigurointi ei onnistunut ensimmäisellä kerralla, vaan jouduttiin vielä antamaan icingaweb2-hakemiston omistajuuden www-data ryhmälle komennolla

```
# sudo chown –R www-data /etc/icingaweb2
```

Tämän jälkeen valitaan finish. Kuvasta 27 nähdään, että Icinga Web 2 -konfiguraatio on onnistunut.



Kuva 27. Icingan ja Web 2 -käyttöliittymän konfigurointi on onnistunut.

Seuraavaksi valitaan Login to Icinga Web 2 -linkki, josta päästään kirjautumissivulle (kuva 28).

Kuva 28. Icingan kirjautumisikkuna

Syötetään tunnukset, jotka luotiin kohdassa Administration, ja valitaan login. Päästään Icinga Web 2 -kotisivulle, jota on havainnollistettu kuvassa 29.

Kuva 29. Icinga Web 2 -kotisivu

[25.] [26.]

5.4 Cacti-ohjelmiston asentaminen

Cacti voidaan asentaa terminalin kautta asennuspaketeista. Ennen Cactin asennusta on kuitenkin asennettava Apache, MySQL, PHP, RRDtools ja SNMP/SNMPd, jotka Cacti vaatii toimiakseen. Tämä tapahtuu syöttämällä terminaliin seuraavat komennot:

```
# apt-get install apache2 mysql-server php5 libapache2-mod-php5

# apt-get install rrdtool
```

```
# apt-get install snmp snmpd
```

Tämän jälkeen voidaan siirtyä itse Cactin asennukseen. Cactin lisäksi asennettiin myös Cacti Spine -paketti, joka nopeuttaa Cactin kiertokyselyitä. Cacti ja Spine asennetaan paketeista syöttämällä terminaliin komennot

```
# apt-get install cacti cacti-spine
```

Tässä vaiheessa asennus esittää kolme kysymystä liittyen käytettävään webserveriin, tietokannan konfigurointiin ja MySQL: root -salasanaan. Vastataan Apache, Yes ja syötetään MySQL-salasana.

Tämän jälkeen on syytä käynnistää snmpd-palvelu komennolla

```
# /etc/init.d/snmpd start
```

Terminalin osalta asennus on nyt valmis, ja Cacti on saatavilla selaimella osoitteessa http://IP-osoitteesi/cacti. Asennus kysyy selaimessa vielä muutaman kysymyksen liittyen asennukseen. Näihin voi vastata oletuksilla. Tämän jälkeen Cactiin päästään kirjautumaan ensimmäistä kertaa sisään. Oletuksena käyttäjänimi ja salasana on admin. Nämä tulee vaihtaa ensimmäisen kirjautumisen yhteydessä. [28.]

6 Yhteenveto

Ohjelmistojen asennuksessa ilmeni jokaisen ohjelmiston osalta ongelmia. Valmistajien asennusdokumentit sisälsivät paljon tietoa, mutta verkonvalvontaohjelmistojen asennusvaiheessa on niin monia erilaisia vaihtoehtoja esimerkiksi tietokannan ja käyttöliittymän osalta, että asennuksen tekeminen pelkästään valmistajan asennusdokumenttien tuella voi olla ongelmallista. Hyvänä apuna asennustyössä olivat kolmansien osapuolien tekemät tutoriaalit, joita on melko hyvin saatavilla.

Työssä asennetuista ohjelmistoista Zabbix ja Icinga olivat kehittyneempiä ja kattavampia Observium-ohjelmistoon verrattuna. Cacti oli vertailussa olleista ohjelmistoista ominaisuuksiltaan vaatimattomin. Kartoitustyön pohjalta voidaan päätyä johtopäätökseen, että verkonvalvontaohjelmiston valinnassa on olennaista se, mitä ohjelmalla halutaan tehdä ja minkälaiseen ympäristöön se asennetaan. Jos halutaan esimerkiksi ainoas-

taan katsella ja analysoida SNMP-dataa graafisessa muodossa, Cacti on tähän tarkitukseen hyvä ohjelmisto. Observiumin etuna on, että Observiumin kotisivuilla pääsee testaamaan ohjelmistoa demoversiona ennen asennusta. Demoversio havainnollistaa hyvin ohjelmiston ominaisuuksia. Icinga ja Zabbix olivat vertailtujen kohteiden monipuolisimmat ohjelmistot, joilla molemmilla pystytään toteuttamaan samat asiat. Zabbix ja Icinga eroavat kuitenkin toisistaan siinä, että Icingassa lisäosien merkitys on suurempi, kun taas Zabbix asentaa kaiken oletuksena. Jokaisessa verkonvalvontaohjelmistossa oli selkeä ja toimiva web-käyttöliittymä. Icingan Web 2 -käyttöliittymä oli ulkonäöltään ja käytettävyydeltään nykyaikaisin, mutta ohjelmiston asennus oli vaativin. Muissakin ohjelmistoissa oli ongelmia, joiden selvittämisessä oli käytettävä superuser-oikeuksia tai kirjoitettava käsky itse kopioi ja liitä -menetelmän sijaan. Näin oli toimittava siksi, että joissakin tilanteissa internetistä kopioitu merkki ei kopioitunutkaan oikeana terminaliin.

Insinöörityötä aloitettaessa verkonvalvontaohjelmistot olivat työn tekijälle uusi aihepiiri. Aiempaa verkonvalvontaohjelmistojen käyttö- tai asennuskokemusta ei ollut. Linux-käyttöjärjestelmistä kokemusta oli jonkin verran, esimerkiksi perus-terminalissa käytettävät käskyt olivat tuttuja, vaikkakin niiden parissa toimimisesta oli kulunut aikaa. Siksi myös Linux-käyttöjärjestelmiin perehtyminen osoittautui hyödylliseksi. Insinöörityöaiheeseen perehtyminen tuotti työn tekijälle paljon uutta tietoa verkonvalvontaohjelmistoista. Laajan käsityksen saaminen ohjelmistojen käytöstä ja toiminnoista edellyttäisi työskentelyä ohjelmistojen parissa pidemmän aikaa ympäristössä, joka sisältäisi useita työasemia ja palvelimia.

Lähteet

1 Internet World Stats 2015. Verkkodokumentti. Internet World Stats. <http://www.internetworldstats.com/stats.htm> Luettu 2.4.2016.

2 Configuring Cisco Discovery Protocol. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf015.html> Luettu 20.2.2016.

3 Cisco Discovery Protocol. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol> Luettu 20.2.2016.

4 Hypertext Transfer Protocol. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol> Luettu 20.2.2016.

5 HTTP. Verkkodokumentti. Wikipedia. <https://fi.wikipedia.org/wiki/HTTP> Luettu 27.2.2016.

6 Internet Control Message Protocol. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol#Control_messages> Luettu 27.2.2016.

7 Internet Control Message Protocol (ICMP) Basics. Verkkodokumentti. Microsoft. <https://support.microsoft.com/en-us/kb/170292> Luettu 27.2.2016.

8 SMTP. Verkkodokumentti. Wikipedia. <https://fi.wikipedia.org/wiki/SMTP> Luettu 12.3.2016.

9 Simple Mail Transfer Protocol. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol> Luettu 12.3.2016.

10 SNMP. Verkkodokumentti. Wikipedia. <https://fi.wikipedia.org/wiki/SNMP> Luettu 12.3.2016.

11 Simple Network Management Protocol. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol> Luettu 19.3.2016.

12 Secure Shell. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Secure_Shell> Luettu 19.3.2016.

13 TCP. Verkkodokumentti. Wikipedia. <https://fi.wikipedia.org/wiki/TCP> Luettu 12.3.2016.

14 Transmission Control Protocol. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Transmission_Control_Protocol> Luettu 12.3.2016.

15 Networking 101: Understanding TCP, the Protocol. Verkkodokumentti. Enterprise Networking Planet. <http://www.enterprisenetworkingplanet.com/netsp/article.php/3593936/Networking-101--Understanding-TCP-the-Protocol.htm> Luettu 12.3.2016.

16 Signature-Based or Anomaly-Based Intrusion Detection: The Practice and Pitfalls. Verkkodokumentti. SC Magazine. <http://www.scmagazine.com/signature-based-or-anomaly-based-intrusion-detection-the-practice-and-pitfalls/article/30471/> Luettu 12.3.2016.

17 Intrusion detection system. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Intrusion_detection_system> Luettu 12.3.2016.

18 Intrusion prevention system. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Intrusion_prevention_system> Luettu 12.3.2016.

19 Zabbix versioiden aikajana. Verkkodokumentti. Wikipedia. <https://upload.wikimedia.org/wikipedia/en/timeline/f1a2fd30fc751fd4ac9ad81aa9f56464.png> 27.4.2016.

20 Kartta Zabbix asennuksista. Verkkodokumentti. Zabbix. <http://www.zabbix.com/map_of_zabbix_installations.php> 27.4.2016.

21 Zabbix Documentation 3.0 Installation from packages. Verkkodokumentti. Zabbix. <https://www.zabbix.com/documentation/3.0/manual/installation/install_from_packages> Luettu 23.4.2016.

22 Observium. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Observium> Luettu 27.4.2016.

23 Debian/Ubuntu Installation. Verkkodokumentti. Observium. <http://observium.org/docs/install_debian/> Luettu 25.4.2016.

24 Distributed monitoring, Great Icinga Users. Verkkodokumentti. Icinga. <https://www.icinga.org/> 27.4.2016.

25 Icinga 2 Documentation Installing Icinga. Verkkodokumentti. Icinga <http://docs.icinga.org/icinga2/latest/doc/module/icinga2/toc#!/icinga2/latest/doc/module/icinga2/chapter/getting-started#installing-icinga2> Luettu 25.4.2016.

26 Server monitoring with Icinga 2 – Part 1: the server (Ubuntu host). Verkkodokumentti. LowEndBox. <https://lowendbox.com/blog/server-monitoring-with-icinga-2-part-1-the-server-ubuntu-host/> Luettu 25.4.2016.

27 Cacti (software). Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Cacti_(software)> Luettu 28.4.2016.

28 How to install Cacti on Ubuntu 14.04/14.10. Verkkodokumentti. Unixmen. <http://www.unixmen.com/install-cacti-ubuntu-14-04/> Luettu 28.4.2016.