LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Verkonvalvonta

Zabbix

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2017
Jukka Tuominen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

TUOMINEN, JUKKA:

Verkonvalvonta
Zabbix

Tietoliikennetekniikan opinnäytetyö, 43 sivua, 3 liitesivua

Kevät 2017

TIIVISTELMÄ

Tämä opinnäytetyö toteutettiin Lahden Ammattikorkeakoulussa keväällä 2017. Lahden Ammattikorkeakoululla on kolme toisistaan erillistä eri laitevalmistajien laitteistoilla toteutettua langatonta verkkoa. Nämä kolme verkkoa tulee yhdistää saman verkonvalvontasovelluksen alle ylläpidollisista syistä. Työn tavoitteena oli tutkia, asentaa ja tutustua NMS (Network Management System)-ohjelmistoihin, vertailla niitä keskenään verkonvalvonnan näkökulmasta ja valita määriteltyihin kriteereihin parhaiten soveltuva ohjelmisto.

Verkonvalvonnan tarkoitus on havaita hallittavassa verkossa tapahtuvia muutoksia, jotta ylläpito voi reagoida muutoksiin tarvittavalla tavalla. Verkonvalvontajärjestelmät käyttävät viestimiseen SNMP-protokollaa.

SNMP-protokollasta on kolme versiota. SNMP-protokolla käyttää UDP-protokollaa datan välitykseen managerin ja agentin välillä. SNMPv1 on saanut vuonna 1990 Internet-standard-statuksen. SNMPv3 on saanut Internet-standard-statuksen, ja se on tällä hetkellä käytettävä SNMP protokolla. SNMPv3 yhdisti edellisten versioiden parhaat puolet ja paransi protokollan turvallisuutta lisäämällä varmenteita viestintään.

Zabbix on maailmanlaajuinen, ilmainen täysin avoimeen lähdekoodiin perustuva yritystason verkonvalvontaohjelmisto, joka on suunniteltu IT-infrastruktuurin eri komponenttien suorituskyvyn ja ylläpidon monitorointiin. Sen kilpailija OpenNMS on myös maailmanlaajuinen, ilmainen täysin avoimeen lähdekoodiin perustuva ja kehitetty verkonvalvontaratkaisuksi. OpenNMS on jaettu kahteen eri versioon, jotka ovat Meridian ja Horizon. Työssä verkonvalvontaohjelmistolta vaaditut kriteerit täytti paremmin Zabbix.

Asiasanat: verkonvalvonta, NMS, SNMP, Zabbix, OpenNMS

Lahti University of Applied Sciences
Degree Programme in Information Technology

TUOMINEN, JUKKA:

Network Monitoring
Zabbix

Bachelor's Thesis in telecommunications, 43 pages, 3 pages of appendices

Spring 2017

ABSTRACT

This thesis was made for Lahti University of Applied Sciences. Lahti University of Applied Sciences has three independent wireless local area networks that need to be united within one network management system for administrative purposes. The purpose of the thesis was to investigate and install NMS (Network Management System) programs, compare them and select suitable software that meets the requirements of the customer.

The purpose of network monitoring is to detect changes in the system monitored so that adminitrators can react to them as required. Network Management Systems use the SNMP (Simple Network Management Protocol) protocol to transfer data.

There are three versions of the SNMP protocol. The SNMP protocol uses the UDP protocol to transfer data between manager and agent. SNMPv1 aquired Internet-standard status in year 1990. The newest version, SNMPv3 has also acquired the Internet-standard status and is the current version of SNMP. It united the best parts of the earlier versions and introduced better security of SNMP messaging via authorized messaging.

Zabbix is a free, global, enterprise-level NMS based totally on free source code. It is designed to monitor different IT infrastructure segments for example in processing. Its competitor OpenNMS is also a free, global, enterprise-level NMS solution based totally on free source code. OpenNMS has two versions, Meridian and Horizon. In this thesis Zabbix fulfilled the requirements needed for the network management system better than the other program.

Key words: Network Monitoring, NMS, SNMP, Zabbix, OpenNMS

SISÄLLYS

SANASTO JA LYHENTEET

SANASTO JA LYHENTEET

Admin	Järjestelmänvalvoja
Ad-hoc	Langattomien lähiverkkojen välinen yhteystapa. Laitteet liikennöivät keskenään ilman tukiaseman apua.
APT	Advanced Packaging Tool on ohjelmistopakettien asennukseen ja hallintaan käytetty apuohjelma.
CLNS	OSI Connectionless Network Service on yhteydetön paketinjakelupalvelu
Dashboard	Graafinen käyttöliittymä
DDP	AppleTalk Datagram Delivery Protocol, jonka päätehtävä on pakettien lähetys AppleTalk-verkkoprotokollassa.
HTTP	Hypertext Transfer Protocol on selainten ja web-sivustojen tiedonsiirtoon käyttämä protokolla.
IETF	Internet Engineering Task Force on Internet-protokollien standardoinnista vastaava organisaatio.
IP	Internet Protocol on protokolla, joka on Internetin toiminnan ydin. IP yhdistää internetiin liittyneitä laitteita palvelimiin ja sitä kautta toisiin käyttäjiin.
IPX	Novell Internet Packet Exchange on IP-protokollan tyyppinen protokolla, jonka etuna on pieni muistijälki. IPX oli laajalti käytössä 1980-luvun lopusta 1990-luvun puoliväliin.
LDAP	Lightweight Directory Access Protocol on verkkoprotokolla, jota käytetään hakemistopalveluissa. LDAP:n yleisin käyttötarkoitus on käyttäjäntunnistus ja käyttöoikeuksien tarkistaminen.

MAC	Medium Access Control on verkon varaamisen ja itse liikennöinnin hoitava osajärjestelmä. Toimii IEEE 802 -standardoidussa verkossa.
MIB	Management Information Base on virtuaalinen tietokanta, josta SNMP-protokollaa käyttävät sovellukset hakevat tietoa.
Node	Verkon komponentti
NMS	Network Management System on järjestelmä, jolla valvotaan hallinnoitavaa verkkoa.
OID	Object Identifier on esimerkiksi MIB:n käyttämä yksilöintitunnus. Sillä yksilöidään dataa esimerkiksi MIB:n kaltaisessa virtuaalisessa tietokannassa.
PHP	PHP: Hypertext Prepocessor on ohjelmointikieli, jota käytetään esimerkiksi dynaamisten web-sivujen luonnissa.
pre-shared key	WLAN-verkoissa tukiasemaan kirjauduttaessa käytettävä ennalta määritelty salasana
SNMP	Simple Network Management Protocol on verkkojen hallinnassa käytettävä tietoliikenneprotokolla.
SSH	Secure Shell Kryptograafinen verkkoprotokolla, jolla voidaan käyttää salattua yhteyttä salaamattomassa verkossa

TCP	Transmission Control Protocol on tietoliikenneprotokolla, jolla luodaan yhteyksiä tietokoneiden välille.
TLS	Transport Layer Security on salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
Topologia	Verkon rakenne, eli tapa, jolla verkon laitteet on liitetty toisiinsa
UDP	User Datagram Protocol on yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille mahdollistaakseen tiedonsiirron.

1 JOHDANTO

Verkonvalvontaa toteutetaan osana verkon ylläpitoa. Mitä isompi on verkko, sen monimutkaisempi ja vaikeampi on valvottava kokonaisuus. Verkonvalvontaan on kehitelty verkonvalvontasovelluksia, jotka auttavat verkon ylläpitäjää hallitsemaan ja valvomaan verkon eri segmenttejä ja osia, kuten reitittimiä ja kytkimiä. Verkonvalvontasovelluksella voidaan tarkastella esimerkiksi eri verkon segmenttien ruuhkautuneisuutta tai yksittäisten laitteiden lähettämää bittivirtaa sisään ja ulos verkosta.

Tämä opinnäytetyö toteutettiin Lahden Ammattikorkeakoulussa keväällä 2017. Lahden Ammattikorkeakoululla on kolme toisistaan erillistä eri laitevalmistajien laitteistoilla toteutettua langatonta verkkoa. Nämä kolme verkkoa tulisi yhdistää saman verkonvalvontasovelluksen alle ylläpidollisista syistä. Työn tavoitteena on tutkia, asentaa ja tutustua NMS (Network Management System)-ohjelmistoihin, vertailla niitä keskenään verkonvalvonnan näkökulmasta ja valita määriteltyihin kriteereihin parhaiten soveltuva ohjelmisto.

Työhön valikoituneet ohjelmistot ovat Zabbix ja OpenNMS. Molemmat verkonvalvontasovellukset ovat ilmaisia, joten niistä ei kerry ylläpidollisesti kustannuksia. Molemmat sovellukset käyttävät viestinnässään SNMP-protokollaa (Simple Network Management Protocol). Opinnäytetyössä tutustutaan myös SNMP-protokollan toimintaan ja historiaan.

2 VERKONVALVONTA

2.1 Verkonvalvonta yleisesti

Verkonvalvonnan tarkoitus on havainnoida hallittavassa verkossa tapahtuvia muutoksia. Muutokset ovat mahdollisesti käyttäjien, tai verkossa tapahtuneen vian aiheuttamia. Verkonvalvonnasta voidaan mainita esimerkkeinä suorituskyvyn ja virheiden havainnointi. (Solarwinds 2017.)

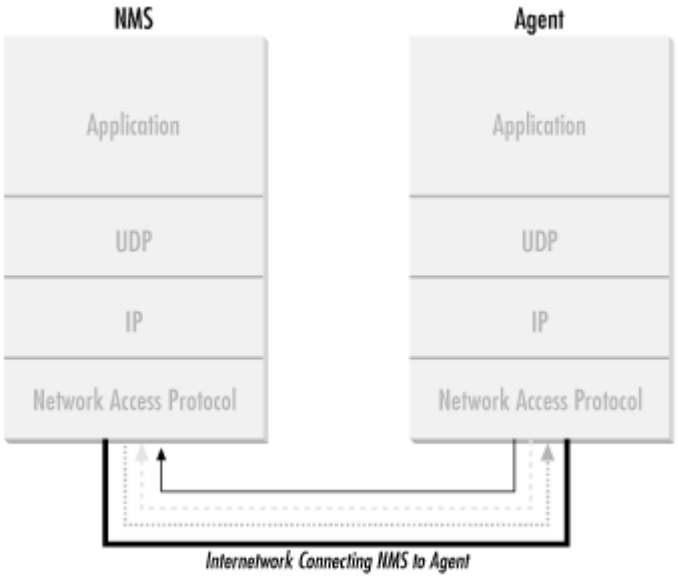
Suorituskyvyn valvonta on yksi kohteista verkonvalvonnassa. Suorituskykyä valvottaessa mittarina toimii esimerkiksi viestin siirron kesto käyttäjälle ja sen vastaukseen menevä aika, tai se paljonko verkkoa on vapaana käyttäjälle. Tämä tarkoittaa esimerkiksi verkon yksittäisen laitteen käyttöastetta ja liikenteen määrää. Mikäli käyttöaste nousee liian korkeaksi, ilmoittaa sovellus käyttäjälle verkon olevan vaarassa kaatua kuormittuvan laitteen vuoksi. Mikäli liian paljon dataa liikkuu yhden laitteen lävitse, on vaarana, että laite saattaa kuormituksen vuoksi ylikuumentua ja hajota, jolloin tieto ei enää kulje sen pisteen lävitse. Suorituskyvyn hallinnalla ei seurata verkon palveluja, vaan verkkoa ja verkon laitteita. (Solarwinds 2017.)

Virheiden havainnointi käsittelee laajempaa aluetta verkonvalvonnassa kuin suorituskyky. Virheiden havainnoinnista esimerkkinä voidaan kertoa kahden eri reitittimen välisen yhteyden katkeaminen. Yhteyden katkeaminen näkyy yksinkertaisena fyysisenä virheenä, kun yhteyttä laitteiden välille ei pystytä muodostamaan. Myös eri protokollatason virheet ovat mahdollisia, kuten esimerkiksi väärin määritelty reitti, joka aiheuttaa reitittimen lähettämään viestiä päättymättömässä kehässä lamauttaen näin laitteen toiminnan. (Solarwinds 2017.)

2.2 Simple Network Management Protocol

SNMP käyttää User Datagram Protocollaa (UDP) datan välitykseen managerin ja agentin välillä. UDP on valittu protokollaksi Transmission Control Protocollan (TCP) sijaan siksi, että UDP on yhteydetön, joka tarkoittaa, ettei agentilta managerille välistä yhteyttä rakenneta, kun pakettejä lähetetään edestakaisin. Yhteydettömyys tekee UDP:sta epäluotettavan, koska ei ole keinoa varmistaa, ovatko paketit päässeet perille ja tarvitseeko SNMP sovelluksen lähettää paketit uudelleen. Tämä on ratkaistu esimerkiksi yksinkertaisella aikarajalla, jonka umpeutuessa SNMP sovellus toteaa, ettei paketti ole päässyt perille, ja lähettää paketin uudelleen. Jos käy niin, ettei paketti mene perille, on mahdollista määritellä, kuinka monta kertaa paketti lähetetään uudelleen, jotta tapahtuma ei jää loputtomaan kierteeseen. (O'Reilly & Associates 2002a.)

UDP-protokollan käytön hyödyksi voidaan laskea, että UDP käyttää vähän verkkoa viestinnässään. Tämän vuoksi verkko ei rasitu pakettien uudelleen lähettämisestä UDP-protokollalla yhtä paljon, kuin TCP-protokollalla. UDP-protokolla käyttää porttia 161 lähettääkseen ja vastaanottaakseen pyyntöjä sekä porttia 162 vastaanottaakseen rajoituksia valvotuilta laitteilta. Jokaisen laitteen, joka käyttää SNMP-protokollaa, tulee käyttää näitä portteja oletuksena. Jos portteja on jostain syystä muutettu, tulee verkonvalvontaohjelmiston olla tietoinen näistä muutoksista, jotta viestit ohjautuvat oikeisiin portteihin. (O'Reilly & Associates 2002a.)

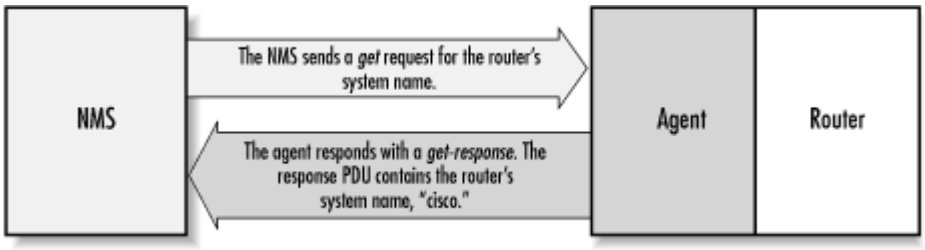


KUVIO 1. SNMP yhteys kuvattuna NMS sovelluksesta agenttiin (O'Reilly & Associates 2002a.)

Kuviossa 1 näytetään, kuinka TCP/IP yhteys laitteen ja internetin välillä muodostuu. Jokainen laite, joka haluaa muodostaa yhteyden internetiin, käyttää tätä yhteystapaa, jossa jokainen kerros käyttää tietoa suoraan alapuolella olevalta kerrokselta ja jakaa tiedon suoraan kerrosta ylemmäs. Selitettynä tämä tarkoittaa, että kun SNMP ohjelma lähettää viestin tai hälytyksen NMS ohjelmistolle, tapahtuu seuraavasti: Application kerros välittää palvelun käyttäjälle, joka voi olla esimerkiksi järjestelmänvalvoja, joka pyytää tilapäivitystä reitittimeltä. UDP kerros mahdollistaa yhteydettömässä tilassa kahden eri laitteen välisen viestinnän, joka suuntautuu joko porttiin 161 (query) tai 162 (trap). Trap on tässä tapauksessa hälytyksessä käytettävä portti. IP kerros yrittää seuraavaksi viedä SNMP viestin lähettäjältä vastaanottajalle, jonka tunnistaa vastaanottajan IP-osoitteen perusteella. Medium Access Control (MAC) on vastaanottajan fyysinen laite, joka varmistaa, että viesti välittyy oikeaan osoitteeseen. Tämän jälkeen tähän viesti kuitataan vastaanottajan toimesta, jolloin viesti kulkee saman reitin takaisin lähettäjälle, joka saa tiedon viestin perille pääsystä. (O'Reilly & Associates 2002b.)

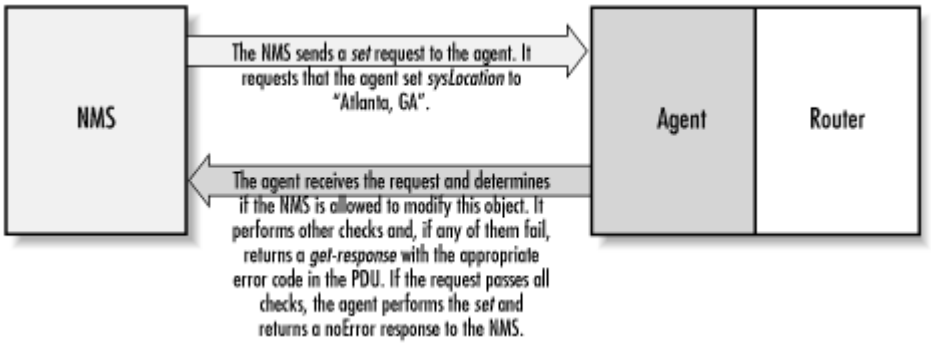
SNMP protokollan ensimmäinessä versiossa on neljän tyyppisiä viestejä, joilla tietoa lähetetään: GET, GET NEXT, SET ja TRAP. Protokollan

myöhemmissä vaiheissa on myös muita komentoja, mutta seuraavaksi käydään läpi nämä neljä alkuperäistä viestityyppiä. GET-pyyntö lähetetään NMS ohjelmasta esimerkiksi reitittimelle. Reititin antaa vastauksen SNMP agentille, joka palauttaa pyydetyn tiedon (kuvio 2). GET NEXT-pyynnöllä pyydetään järjestyksessä aina seuraavaa tietoa edeten ennalta määriteltyyn päätepisteeseen. (O'Reilly & Associates 2002b.)



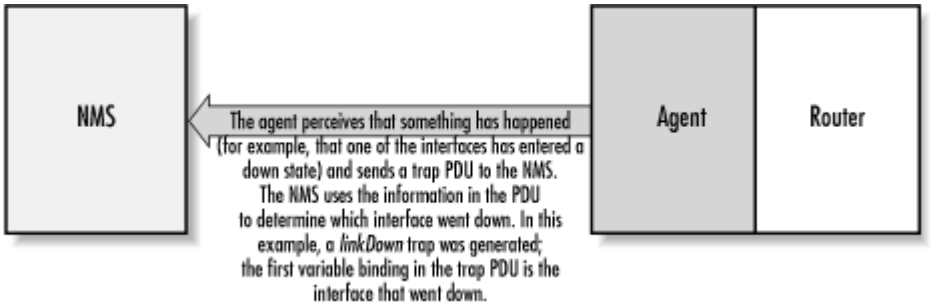
KUVIO 2. Kuva GET pyynnöstä reitittimelle, jossa pyydetään reitittimen nimeä (O'Reilly & Associates 2002b.)

SET komentoa käytetään, kun halutaan muuttaa jotain tietoa tietokannassa. SET komento etenee seuraavalla tavalla: NMS sovellus lähettää SET komennon päätelaitteelle. Päätelaite tarkastaa, onko komennon lähettäjällä oikeutta muuttaa tietokannassa olevaa tietoa. Mikäli komennon lähettäjällä ei ole oikeutta muuttaa tietokannassa olevaa tietoa, lähetetään komennon lähettäjällä asianmukainen virhevastaus. Mikäli komennon lähettäjällä on oikeus muuttaa tietoa, tieto muutetaan ja komennon lähettäjälle vastataan asianmukaisella ilmoituksella, että tiedon muutos on onnistunut (kuvio 3). (O'Reilly & Associates 2002b.)



KUVIO 3. Kuva SET komennosta käytännössä, jossa määritellään reitittimen sijainniksi ”Atlanta, GA” (O’Reilly & Associates 2002b.)

Viimeisenä komentona on TRAP. TRAP viesti on ilmoitus muuttuneesta tilanteesta järjestelmässä. Toisin kuin edellisissä viesteissä TRAP viestissä NMS järjestelmä ei ole lähettänyt kyselyä päätelaitteelle. TRAP viesti syntyy, kun esimerkiksi verkossa olevan reitittimen yksi porteista sammuu. Tällöin SNMP agentti lähettää viestin NMS järjestelmälle ilmoittaen, että portti on sammunut ja verkon ylläpitäjä saa ilmoituksen muutoksesta järjestelmässä (kuvio 4). (O’Reilly & Associates 2002b.)



KUVIO 4. Kuva TRAP komennosta, jossa SNMP Agentti ilmoittaa että reitittimen portti on sammunut (O’Reilly & Associates 2002b.)

Koska SNMP käyttää UDP-protokollaa viestinnässään on mahdollista, että viesti järjestelmän virheestä ei koskaan tavoita ylläpitäjää. Kun ohjelmisto saa TRAP viestin päätelaitteelta tulee ohjelmistolla olla mahdollisuus tulkita tuo viesti. Tämä tapahtuu selvittämällä viestin sisältö viestille määritellystä MIB:n (Management Information Base) OID:sta (Object

Identifier). Laitevalmistajat ovat määritelleet omille laitteilleen omat OID:t mahdollisille viesteille MIB tietokannassa. Tällä tavoin ylläpitäjän ei tarvitse tietää missä osassa verkkoa havaittu muutos tapahtuu, vaan viesti sisältää ilmoituksen minkälainen muutos ja missä järjestelmän laitteessa muutos on havaittu. (O'Reilly & Associates 2002b.)

2.2.1 SNMPv1

SNMPv1 on alkuperäinen versio SNMP:stä. Ensimmäinen versio käyttää protokollia, kuten UDP (User Datagram Protocol), IP (Internet Protocol), CLNS (OSI Connectionless Network Service), DDP (AppleTalk Datagram-Delivery Protocol sekä IPX (Novell Internet Packet Exchange). SNMPv1 on laajasti käytetty ja perustana verkonvalvonta-protokollalle.

Ensimmäisessä versiossa turvallisuus on toteutettu huonosti. Asiakasohjelmien varmennus toteutettiin ainoastaan selkokielisellä salasanalla. Se valjastettiin aikanaan käyttöön siinä uskossa, että internetiä aletaan käyttämään laajamittaisesti ja kaupallisesti. (RFC1157, 1990.)

2.2.2 SNMPv2

Toinen versio SNMP:stä toi parannuksia suorituskyvyssä, turvallisuudessa, luotettavuudessa ja isännältä isännälle – kommunikaatiossa. Toinen versio esitteli *GetBulkRequest* komennon, jolla pystyi hakemaan paljon dataa yhdellä pyynnöllä. Toinen toi myös mukanaan liian monimutkaisen suojauksen, jota ei hyväksytty yhteisön keskuudessa ja siitä tehtiin myöhemmin yhteisön kehittelemä ja käyttäjäpohjainen versio.

SNMPv2 agentti pystyy käyttäytymään proxyna SNMPv1 laitteen puolesta. Tämä tarkoittaa, että agentti ottaa verkonhallintajärjestelmältä vastaan pyynnöt, jotka on suunnattu SNMPv1 laitteelle. Proxy välittää pyynnöt

muuttumattomana SNMPv1 laitteelle, kerää datan itselleen ja kääntää viestin SNMPv2 muotoon. Tämän jälkeen viesti välitetään takaisin yhtenä ryppäänä verkonhallintajärjestelmälle.

Kaksikielinen SNMPv2 verkonhallintajärjestelmä tukee sekä SNMPv1:stä että SNMPv2:sta. Tukeakseen tätä, on hallintaohjelman otettava yhteys agenttiin. Verkonhallintajärjestelmä tutkii tietokannasta datan selvittääkseen onko se ensimmäistä vai toista versiota. Tämän jälkeen perustuen siihen kumpaa versiota data on agentti välittää tiedon verkonhallintajärjestelmälle oikealle versiolle käännettynä. (RFC1441, 1993.)

2.2.3 SNMPv3

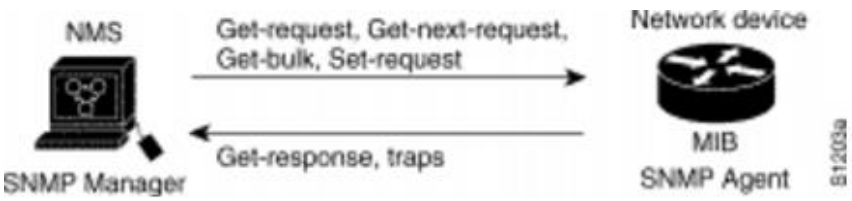
Viimeisin versio määriteltiin vuonna 2002. Kolmas versio on samalla niistä kaikkein tietoturvallisin. SNMPv3 kehitettiin paikkaamaan edellisten versioiden tietoturva-aukkoja, mutta ei tuonut muita parannuksia aiempiin versioihin nähden sisältäen vain tekstuaalisia parannuksia. SNMPv3 toi mukanaan tärkeitä turvallisuuteen liittyviä seikkoja:

- Viestin kryptaaminen estää paketin tarkastelua luvattomilta lähteiltä.
- Viesti kulkee koskemattomana perille.
- Viesti varmennetaan, jotta se on oikeasta lähteestä.

SNMPv3 tukee kaikkia ominaisuuksia, joita esiteltiin edellisissä versioissa. IETF (Internet Engineering Task Force) on tehnyt SNMPv3:sta internet standardin. Tämä tarkoittaa, että aiemmat versiot ovat vanhentuneet ja uusin korvannut ne. Internet standardin myöntäminen on korkein RFC-dokumentille myönnettävä standardi. (RFC2570, 1999.)

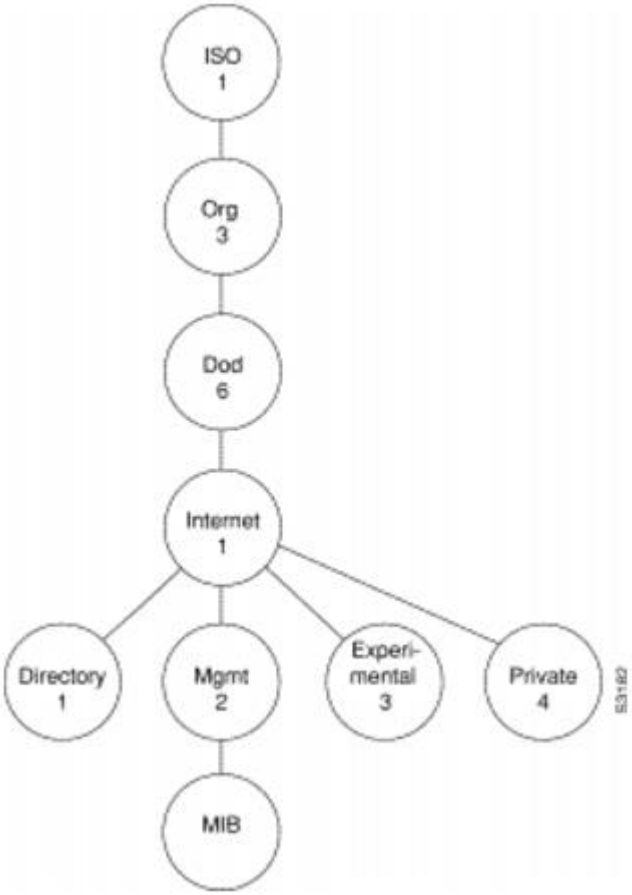
2.2.4 MIB

MIB (Management Information Base) on verkon virtuaalinen tietokanta. Management Information Base noudattaa puumallista hierarkiaa (kuvio 6). MIB:iin varastoidaan verkon laitteiden tietoja. MIB:n tiedot tunnistetaan OID:n (Object Identifier) avulla. NMS sovellukset voivat SNMP-protokollaa käyttäen hakea tietoja tietokannasta (kuvio 5). (Cisco 2007.)



KUVIO 5. SNMP agentti hakee dataa MIB tietokannasta (Cisco 2007.)

Tietokannan rakenteessa lähempänä juurta on yleisemmän tason informaatiota. Mitä kauemmas lähtöpisteestä mennään, sitä tarkempia ja yksityiskohtaisempia tietoja tietokantaan on varastoitu. Tietokannassa säilytetään esimerkiksi verkkoon liitetyn kytkimen sisään ja ulos suuntautuvien bittien lukumäärää. Tiedon tila muuttuu sisään ja ulos suuntautuvien bittien lisääntyessä ja NMS sovellus saa tästä tiedon SNMP-protokollan viestin välityksellä. (Cisco 2007.)



KUVIO 6. MIB tietokannan rakenteen havainnollistava kuva (Cisco 2007.)

3 ZABBIX

3.1 Zabbixin asennus

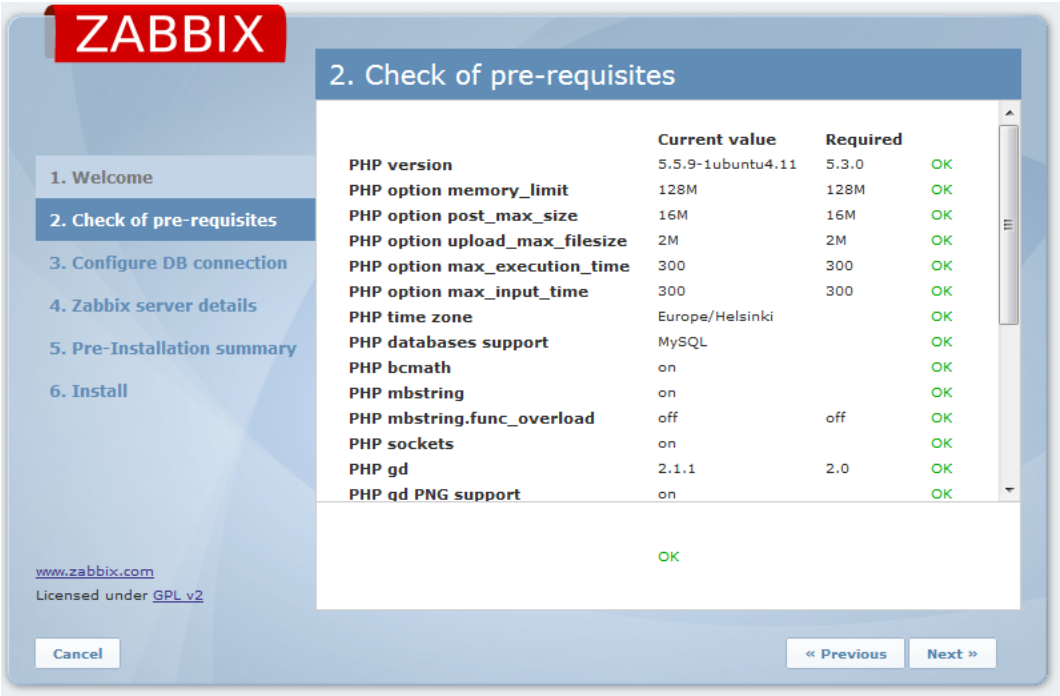
Zabbixin voi asentaa kolmella tapaa. Asennuksen voi tehdä jakelupaketeista, lataamalla uusimman lähdekoodin ja kääntämällä koodin itse, tai lataamalla virtuaalisovelluksen.

Tässä työssä asennettiin Zabbix version 2.4 jakelupaketeista Zabbixin materiaalipankista. Työssä käytettävä käyttöjärjestelmä on Linux Ubuntu 14.04.2 Server versio, joten työssä seurattiin kyseisen version asennusohjeita Zabbixin omasta manuaalista.

Työssä ei käydä läpi Linux Ubuntun yleistä käyttöä sekä asennusta. Mainittakoon, että työssä käytettiin vain tekstipohjaista käyttöliittymää virtuaalikoneen sisällä, koska graafiseen käyttöliittymään päästään käsiksi verkon yli. Esivalmisteluna Zabbixille peruspaketin lisäksi Ubuntuun asennettiin OpenSSH server ja Mail server. Näin pystytään käyttämään virtuaalikonetta myöhemmin etänä SSH (Secure Shell) yhteyden avulla ja mail serverin avulla Zabbix pystyy lähettämään sähköpostia käyttäjälle mikäli ohjelmisto esimerkiksi havaitsee verkosta tipahtaneen reitittimen, tai jotain muita laukaisimia mitä ohjelmistoon on asetettu.

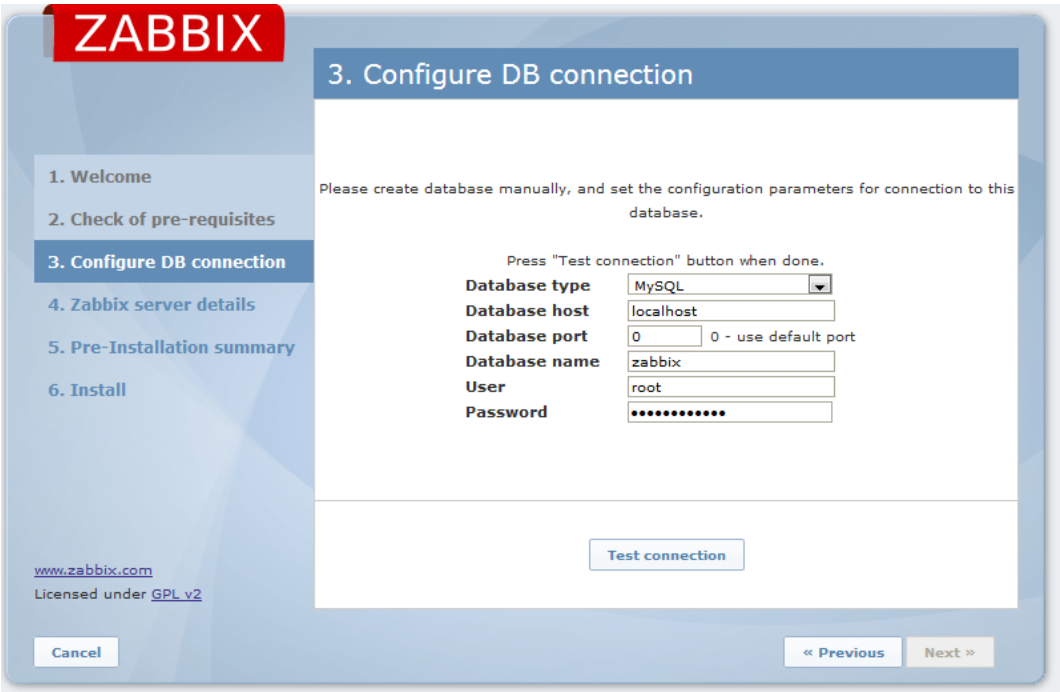
Tässä työssä Zabbix ja OpenNMS asennettiin virtuaalikoneeseen, koska käytössä ei ollut työlle omistettua tietokonetta. Tämä on toteutettu Oracle VM Virtualboxin avulla. Itse virtuaalikoneen määrittelyä, sekä käytettävän Ubuntu käyttöjärjestelmän asennusta ei käydä läpi tässä työssä. Työssä käytetty käyttöjärjestelmä on Ubuntu 14.04.2 Server versio.

Kun virtuaalikone, käyttöjärjestelmä, tarvittavat paketit ja palvelut on asennettu päästään Zabbixin asennukseen. Siirtymällä alustuksien jälkeen osoitteeseen 192.168.0.20/zabbix päästään Zabbix asennusvelhoon. Asennusvaihe on liitteessä 1 työn lopussa.



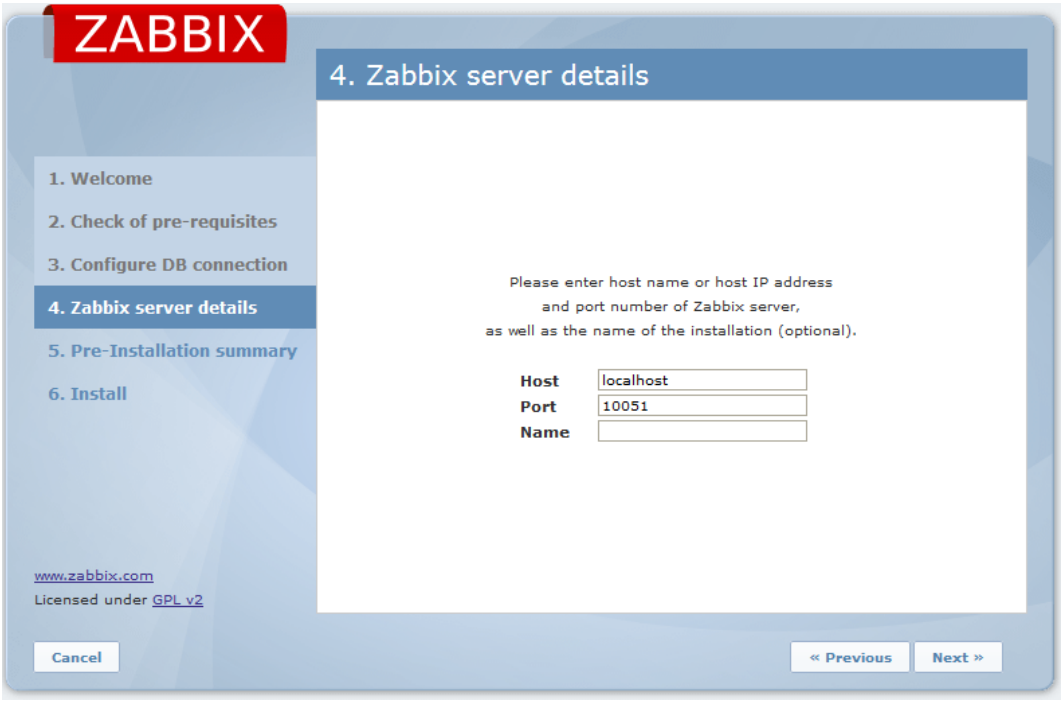
KUVIO 7. Zabbix asennusvelhon yhteensopivuustesti järjestelmän kanssa

Kun päästään tervetuloa-ikkunasta eteenpäin tullaan ensimmäiseksi testi-ikkunaan. Tässä vaiheessa Zabbix asennusvelho testaa ovatko kaikki tarvittavat palvelut kunnossa (kuvio 7). Mikäli kaikki on kunnossa ilmestyy keskelle valkoista aluetta ”OK” merkki ilmoittamaan, että asennuksessa voidaan siirtyä eteenpäin. Tämä tapahtuu painamalla ”Next” painiketta.



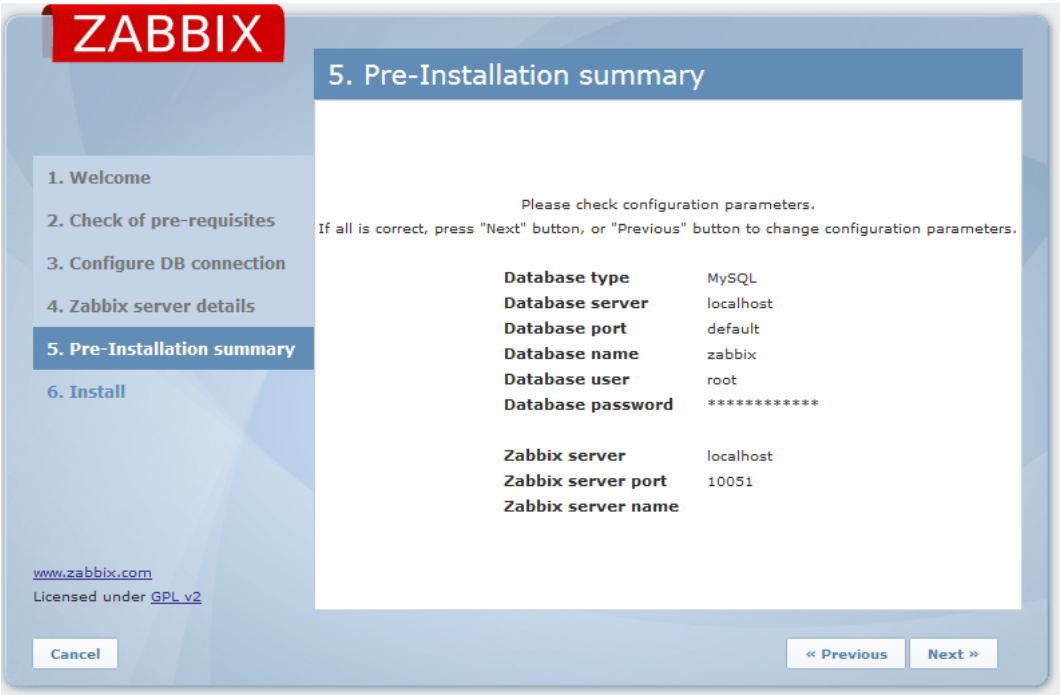
KUVIO 8. Tietokannan yhteysmäärittelyä

Seuraavassa ikkunassa meille aukeaa näkymä, jossa testataan Zabbixin ja MySQL serverin välistä yhteyttä (kuvio 8). Tähän tulee syöttää vain salasana, joka oltiin määritelty aiemmin tietokantapalvelun asennuksen yhteydessä. Tämän jälkeen yhteyttä testataan painamalla ”Test connection” näppäintä. Jos yhteys on kunnossa pomppaa testinappulan yläpuolelle vihreällä edellisen ruudun tapaan teksti ”OK” ja voidaan jatkaa eteenpäin painamalla ”Next”.



KUVIO 9. Zabbix serverin tietoja

Seuraavassa ikkunassa on mahdollista muuttaa itse Zabbix serverin tietoja (kuvio 9). Tässä asennuksessa niitä ei muutettu, vaan jatkettiin eteenpäin painamalla ”Next”.



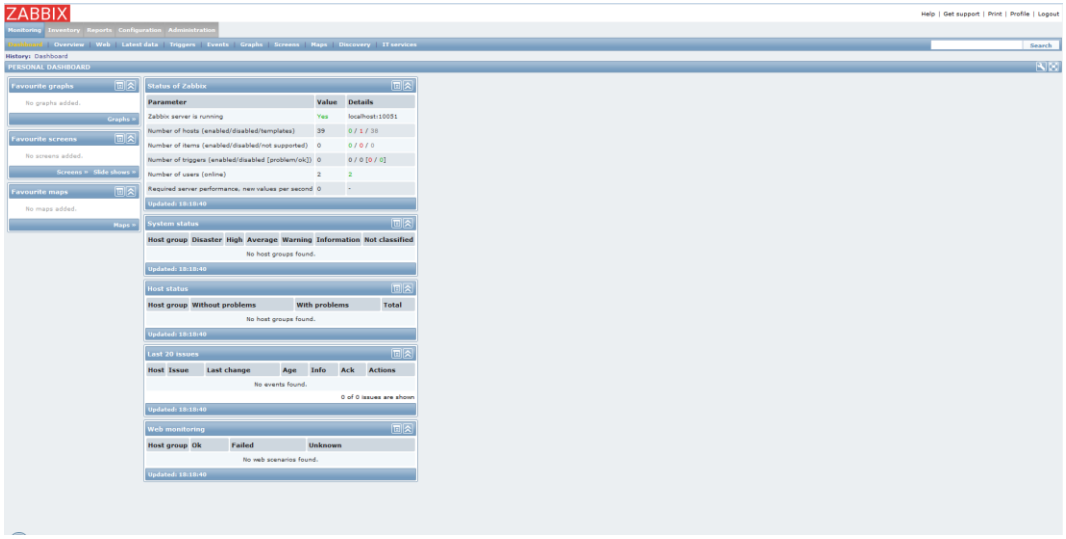
KUVIO 10. Yhteenveto asennuksesta

Viimeisessä ruudussa pyydetään vielä tarkistamaan, että asennusvelhon pyytämät tiedot ovat oikein ja kaikki asetukset ovat kunnossa (kuvio 10). Mikäli kaikki on kunnossa painetaan ”Next” ja viimeistellään asennus. Muussa tapauksessa painetaan ”Previous” ja muutetaan tarvittavat asetukset kuntoon ennen asennuksen viimeistelyä.

KUVIO 11. Zabbix serverin sisäänkirjautumisikkuna

Kun asennus on onnistuneesti suoritettu loppuun painetaan ”Finish” näppäintä ja voidaan kirjautua sisään Zabbixiin ensimmäistä kertaa (kuvio

11). Järjestelmään kirjautuakseen tarvitaan käyttäjätunnukset. Oletuksena Zabbixiin on asetettu käyttäjätunnukseksi ”Admin” ja salasanaksi ”zabbix”. Ohjelmistoon kirjaudutaan painamalla ”Sign In”. Huomioitavaa tässä vaiheessa on, että tietoturvan näkökulmasta salasanaa ei tulisi jättää oletusmuotoon, vaan muuttaa salasana ensimmäisen sisäänkirjautumisen yhteydessä halutuksi. Mikäli salasana jätetään muuttamatta on ulkopuolisten mahdollista yrittää arvata salasana oikein ja päästä vaikuttamaan järjestelmään.



KUVIO 12. Zabbix verkonvalvontajärjestelmän dashboard näkymä

Kirjautumalla ensimmäisen kerran onnistuneesti Zabbixiin päästään dashboard näkymään (kuvio 12). Dashboard näkymästä voi tarkastella tietoja verkosta ja näkymä on melko vapaasti muunneltavissa halutunlaiseksi, jotta myöhemmässä vaiheessa sisäänkirjautuessaan pystyy näkemään ensimmäiseksi verkon halutut tärkeimmät ja kriittisimmät tiedot.

3.2 Yleistä Zabbixista

Zabbix on maailmanlaajuinen, ilmainen täysin vapaaseen lähdekoodiin perustuva yritystason verkonvalvontaohjelmisto, joka on suunniteltu IT-

infrastruktuurin eri komponenttien suorituskyvyn ja ylläpidon monitorointiin. Zabbix yhtiön on perustanut vuonna 2005 latvialainen Alexei Vladishev. Ohjelmana se julkaistiin aiemmin jo vuonna 2001. Zabbixin käyttökohteita ovat Access Control, Application Developement, Business Analytics, Capacity, hallinnointi, Inventory ja turvallisuus. Yhtiö keskittyy palvelemaan isoja yhtiöitä, mutta samalla tavoite on pysyä parhaana vaihtoehtona keskisuurille ja pienille yhtiöille. (Zabbix 2016a.)

Käytettävyydeltään Zabbix on kehitelty optimoimaan yrityksen ajan ja rahan käyttöä, yksinkertaistamaan yrityksen osioiden hallintaa ja suunniteltu sujuvasti käytettäväksi. Zabbixiin julkaistaan myös sisältöä säännöllisin väliajoin. Zabbix on suunniteltu asiakaslähtöisesti täyttämään asiakkaan tarpeet ja yrityksen tärkeä kehitys strategia on pystyä täyttämään asiakkaan tarpeet. (Zabbix 2016a.)

3.3 Zabbixin toiminnot

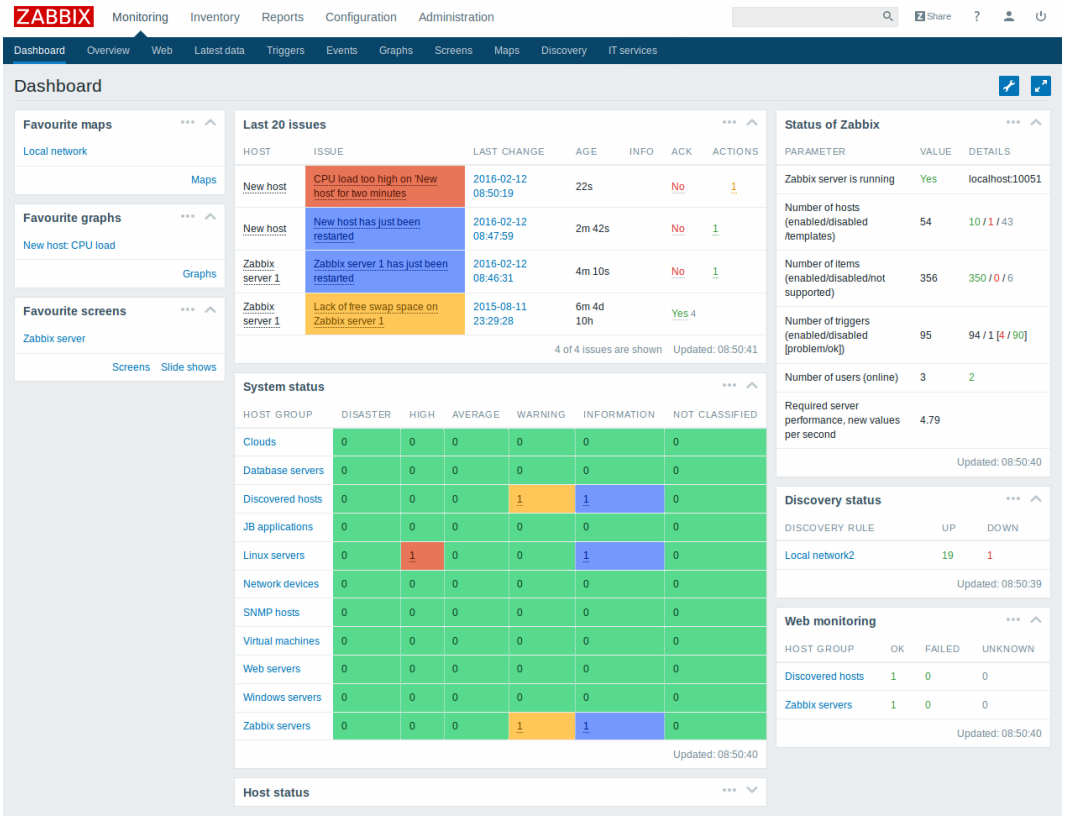
Työskenneltäessä Zabbixin pääasialliset toiminnot ovat datan kerääminen web monitoroinnin avulla, kerätyn datan tallentaminen ja hallinnointi. Zabbix antaa ilmoituksia verkon toiminnasta käyttäjälle ja käyttäjän on mahdollista koostaa datasta tarkasteltavia kaavioita, karttoja ja erilaisia taulukoita päänäytölle ja päänäytön eri osioihin. (Zabbix 2016a.)

Zabbix pystyy automaattisesti havaitsemaan verkkoon liitetyt laitteet ja analysoidulle datalle voidaan asettaa rajoja, jotka ylittyessään varoittavat käyttäjää käyttäjän määrittelemillä tavoilla. Zabbixia käytetään selainpohjaisella käyttöliittymällä suojatulla käyttäjätodennuksella ja käyttäjille voidaan asettaa rajoituksia. (Zabbix 2016a.)

3.3.1 Käyttöliittymä

Zabbixia käytetään PHP:lla (PHP: Hypertext Preprocessor) ohjelmoidulla graafisella verkkokäyttöliittymällä (kuvio 13). Graafisella käyttöliittymällä

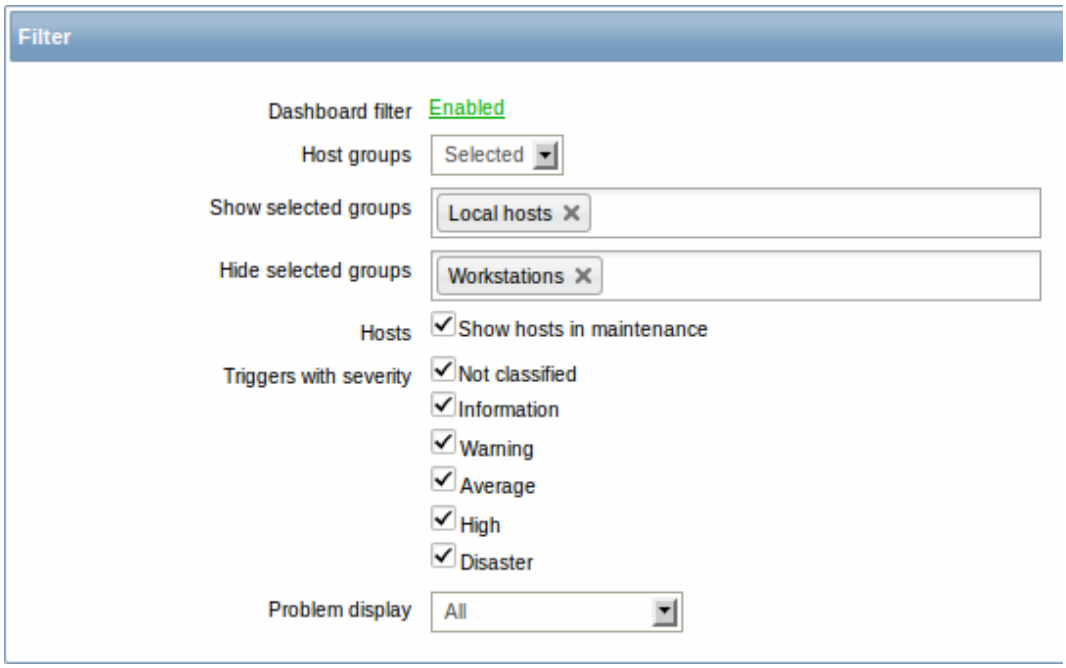
voidaan keskitetysti hallinnoida ja valvoa kerättyä dataa. Käyttöliittymässä tehdyt muutokset tulevat voimaan välittömästi, joten uudelleenkäynnistystä ei tarvita. Graafinen käyttöliittymä tukee kaikkia yleisesti suosituimpia selaimia (Google Chrome, Mozilla Firefox, Microsoft Explorer ja Opera). Zabbix saattaa toimia myös Safarilla. (Zabbix 2016h.)



KUVIO 13. Kuva Zabbixin käyttöliittymästä. Käyttöliittymän näkymää pystyy itse muokkaamaan haluamaansa suuntaan (Zabbix 2016h.)

Zabbixin käyttöliittymässä on käytössä globaalit ilmoitukset. Tämä tarkoittaa, ettei käyttäjän tarvitse olla läsnä siinä ikkunassa, josta ilmoitus tulee. Globaaleissa ilmoituksissa on käytössä sekä viestin näyttäminen, että äänimerkin anto. Mikäli ilmoitukset on otettu käyttöön pystyy käyttäjä itse määrittelemään aikarajan, jolloin ilmoitus poistuu näytöltä. Käyttäjälle on myös olemassa erilaisia ennalta rakennettuja teemoja, joilla käyttäjä voi personoida näkymänsä. Myös omien teemojen tekeminen on mahdollista. (Zabbix 2016h.)

Zabbixin käytön helpottamiseksi voidaan luoda templateja, eli malleja. Luoduilla malleilla saadaan aikaiseksi, että useamman samanlaisen laitteen samoille funktioille ei tarvitse tehdä jokaista määritystä käsin, vaan mallin voi asentaa templatena, jolloin useamman laitteen lisääminen verkkoon käy helpommin ja nopeammin. (Zabbix 2016h.)



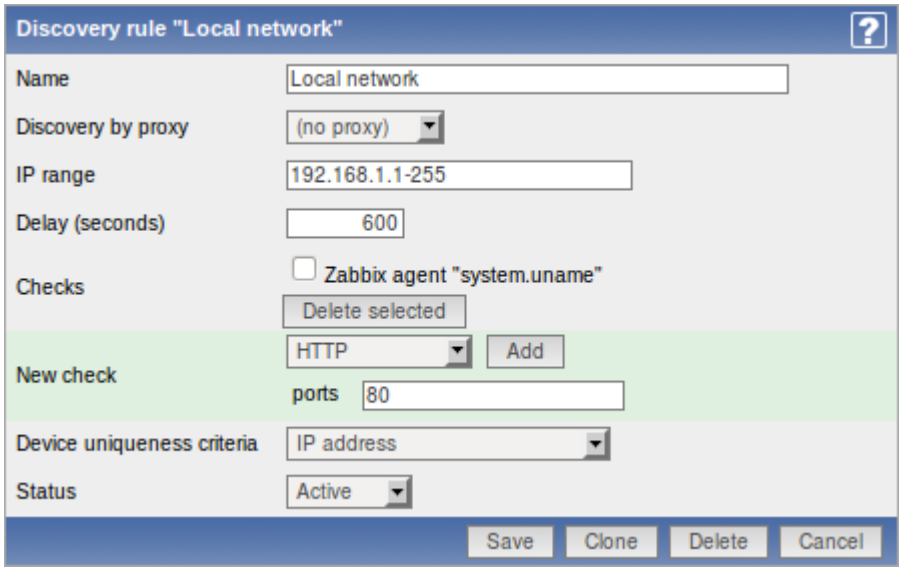
KUVIO 14. Zabbixin käyttöliittymän suodatin (Zabbix 2016h.)

Zabbixin käyttöliittymän näkymää pystyy muokkaamaan itselleen sopivaksi. Mikäli halutaan esimerkiksi suodattaa pois näkymästä tietyt laiteryhmät ja varoitukset (kuvio 14), voidaan se tehdä painamalla sinistä jakoavaimen kuvaa käyttöliittymän pääsivulla. Mikäli suodatinta käytetään käyttöliittymässä, muuttuu jakoavaimen kuva sinisestä oranssiksi. (Zabbix 2016h.)

3.3.2 Network Discovery

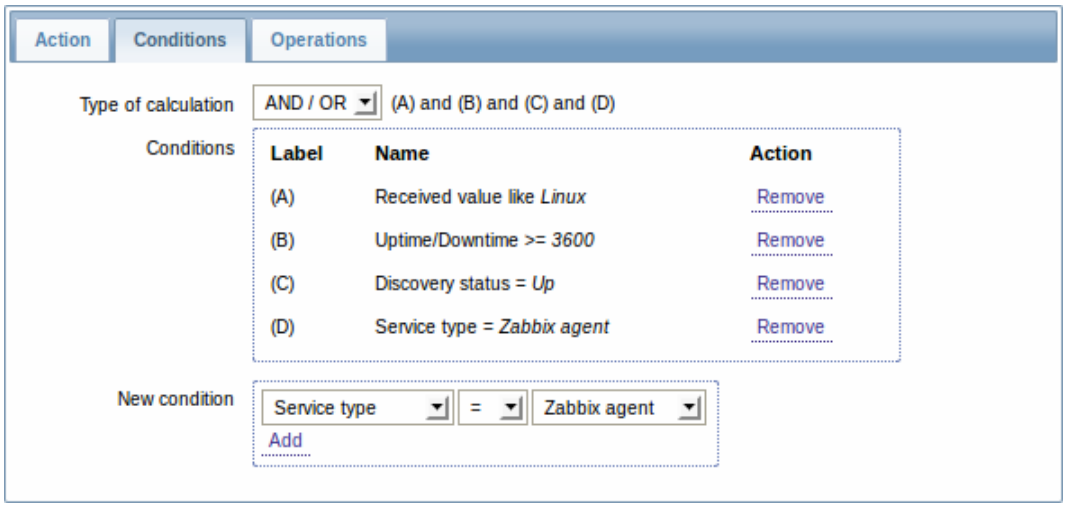
Zabbixista löytyy discovery tool, jolla löydetään verkon laitteet automaattisesti. Auto Discovery auttaa etsimään laitteita ja linkittämään ne oikeisiin malleihin automaattisesti. Auto Discovery käyttää laitteiden löytämiseen SNMP:tä, kuten esimerkiksi Zabbix agenttia. Auto Discovery

tehdään IP-osoite alueelle, jotta koko verkon SNMP laitteet löytyvät (kuvio 15). Kun käytettävä IP-alue on asetettu määritellään kuinka usein Zabbix Server ajaa network discoveryn, joka havaitsee verkon laitteet. Tämän jälkeen palvelu laitetaan päälle, jolloin verkon SNMP palvelua käyttävät laitteet tulisi löytyä automaattisesti mikäli ne ovat IP-osoite alueen sisäpuolella. (Zabbix 2016f.)



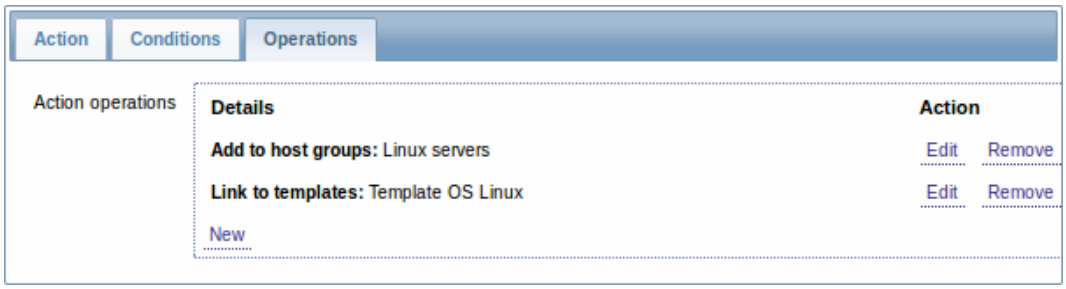
KUVIO 15. Havainnekuva Network Discoverysta, jolla etsitään verkon laitteita IP-osoitealueen avulla automaattisesti tietyn aikajakson (delay) välein (Zabbix 2016f.)

Verkon laitteilla tulee olla määriteltynä SNMP-ryhmä. Mikäli sitä ei ole tehty, joudutaan SNMP-ryhmä määrittelemään jokaiselle laitteelle käsin. Määrittelemällä SNMP-ryhmän päästään siis helpommalla. SNMP-host lukee määritellyn ryhmän templaten ja käyttää sitä, mikäli template on sama kuin hallittavalla laitteella. (Zabbix 2016f.)



KUVIO 16. Auto Discoveryn määrittelyikkuna, jossa määritellään ehtoja auto discovery toiminnolla löytyville verkon laitteille (Zabbix 2016f.)

Mikäli Auto Discovery löytää ennalta määritellyillä ehdoilla hakiessaan laitteilla, voidaan laitteille määritellä ehtoja millä perusteilla ne ryhmitellään ja järjestetään hierarkisesti omiin malleihinsa sopivasti. Lisäämällä ehto kohdasta ”Add” voidaan määritellä esimerkiksi, että mikäli kuvan osoittamalla tavalla serveri on Linux, lisätään serveri määritellyillä ehdoilla rakennettuun ryhmään (kuvio 16). (Zabbix 2016f.)



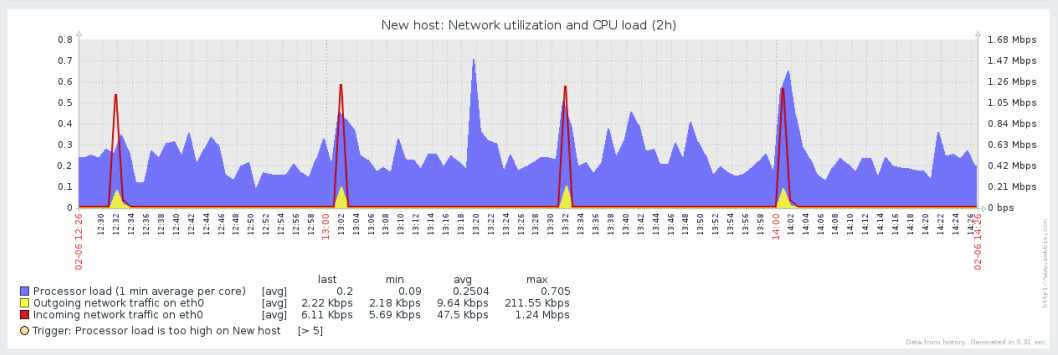
KUVIO 17. Mikäli Auto Discovery löytää laitteen ja löydetty laite täyttää määritellyt ehdot tapahtuu kuvassa ilmenevät toimenpiteet (Zabbix 2016f.)

Mikäli Auto Discovery löytää laitteen, joka vastaa ennalta määriteltyjä hakuehtoja määritellään tapahtumat, jotka ohjelma toteuttaa automaattisesti löydetylle laitteelle. Kuvion 17 osoittamalla tavalla, jos löydetty laite on Linux, lisätään laite Linux ryhmään ja luodaan valmiiksi rakennettu template nimeltään ”Template OS Linux”. (Zabbix 2016f.)

Edellä kuvatulla tavalla ohjelmisto havaitsee verkkoon liitetyt laitteet, kuten reitittimet ja kytkimet ja määrittelee laitteille ehtoihin perustuvat ryhmät. Jatkossa laitteistoja tarkastellessa on laitteille määritelty ennalta omat mallinsa, josta ylläpito pystyy tarkastelemaan haluamiaan tietoja. (Zabbix 2016f.)

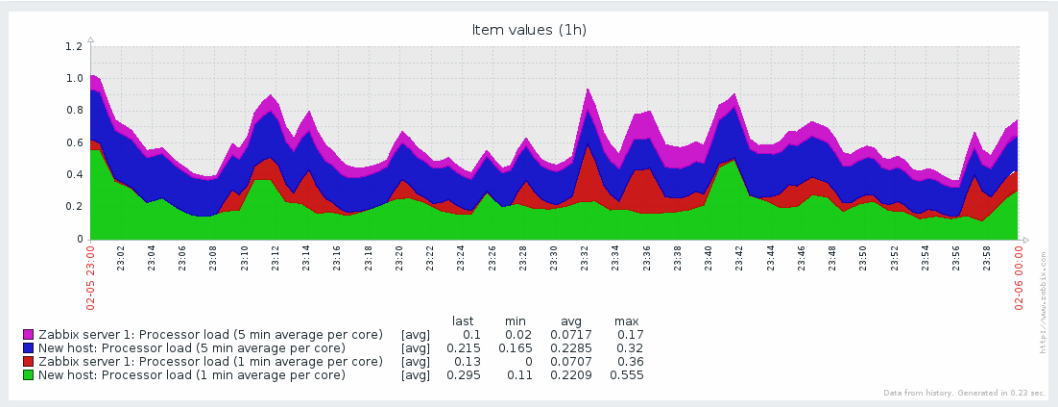
3.3.3 Kaaviot

Saadusta datasta on helppo muodostaa erilaisia kaavioita Zabbixin käyttöliittymään. Zabbix tarjoaa esimerkiksi automaattisesti luotuja kaavioita, jotka näyttävät esimerkiksi reitittimen käynnissä ollessa sen suorittimen käyttöasteen. (Zabbix 2016c.)



KUVIO 18. Kuva kaaviosta, jonka näytettävät elementit pystyy itse määrittelemään (Zabbix 2016c.)

Käyttäjä voi tehdä myös itse omia kaavioitaan (kuvio 18). Luomalla oman kaavion, käyttäjä voi itse määritellä datan, jonka haluaa kaavioon ja määritellä kuvaajan toimimaan eri laitteissa ajaen samaa käyttötarkoitusta. Esimerkkinä voitaisiin mainita reititin, josta näytetään sisään tuleva liikenne, ulos menevä liikenne ja suorittimen käyttöaste yhtäaikaa yhtenä kaaviona. (Zabbix 2016c.)

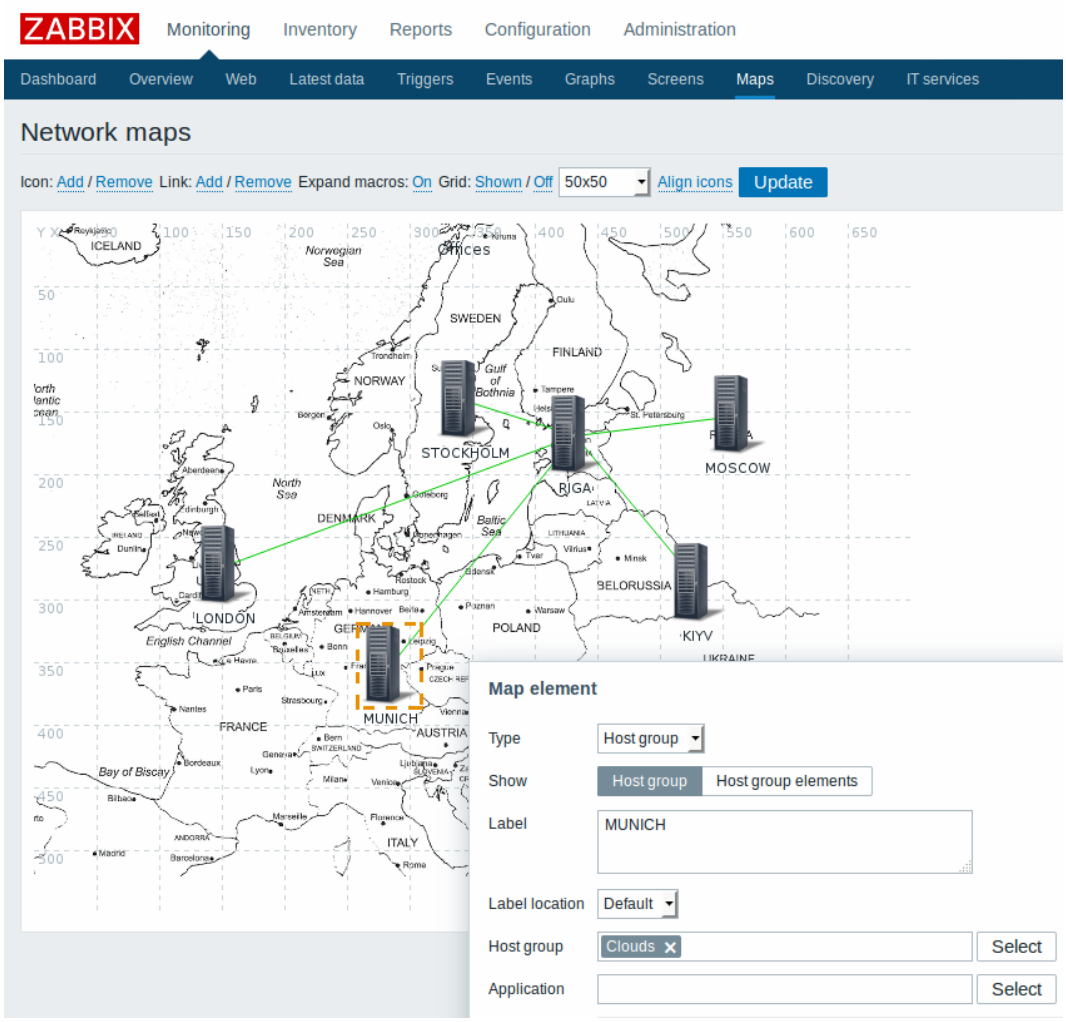


KUVIO 19. Kuva Ad-hoc kaaviosta (Zabbix 2016c.)

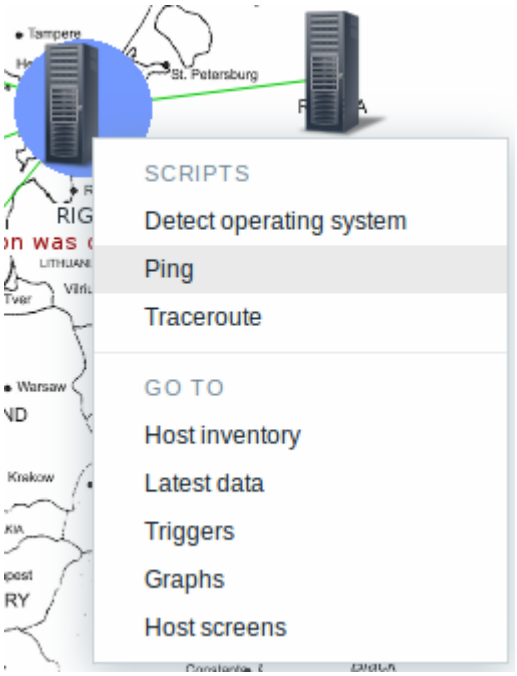
Ad-hoc kaaviot (kuvio 19) ovat pikavaihtoehto Zabbixin kaavioissa. Ad-hocilla voi nopeasti luoda usean eri datan yhteen niputtaman kaavion valitsemalla listasta eri datalähteitä, joita haluaa kaavioon tulevan. Tämä on paljon nopeampi vaihtoehto kuin edellä mainittu itse tehty kaavio, mutta silti kattavampi kuin ensimmäisenä mainittu simppeli kaavio. (Zabbix 2016c.)

3.3.4 Kartat

Kartta ominaisuus mahdollistaa kartan tekemisen monitoroidusta verkosta (kuvio 20). Näin käyttäjä saa kokonaiskuvan verkon rakenteesta. Karttaan voidaan liittää ennalta määritettyjä laukaisimia, jotka aktivoiduttuaan saavat kartan reagoimaan ja näyttämään, mitä verkossa tapahtuu. (Zabbix 2016e.)



KUVIO 20. Kuvite kuva karttanäkymästä monitoroidussa verkossa. Karttanäkymän taustan pystyy itse määrittelemään (Zabbix 2016e.)

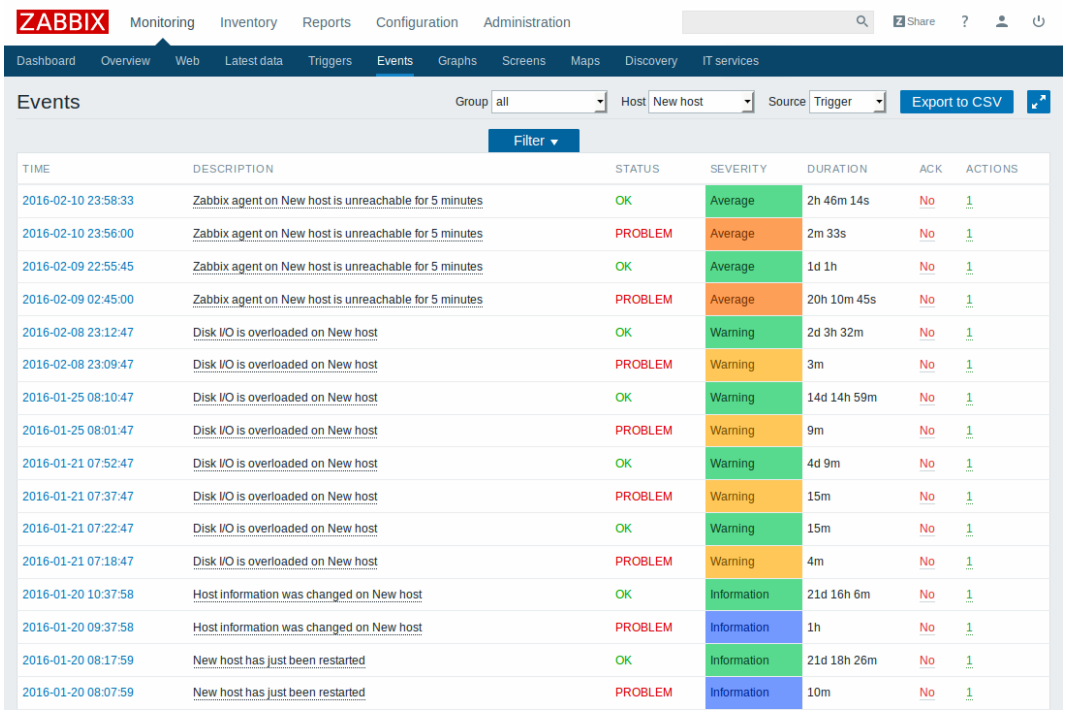


KUVIO 21. Klikkaamalla laitetta karttanäkymässä pääsee pikavalikkoon (Zabbix 2016e.)

Esimerkiksi verkon eri reitittimien välisien yhteyksien nopeutta tai suorittimien käyttöastetta pystyy seuraamaan reaaliajassa karttanäkymässä käyttäjän luomilla makrokomennoilla. Karttanäkymän laitteista voi myös nähdä millaisia laukaisimia niihin on asetettu. Karttanäkymässä laitetta klikkaamalla voi pikakomennoilla testata esimerkiksi mitä reittiä pitkin kytkin lähettää tiedon käyttäjälle (traceroute). Tästä ominaisuudesta on havainnollistava kuvio yläpuolella (kuvio 21). (Zabbix 2016e.)

3.3.5 Tapahtumat

Zabbix tallentaa kaikki tapahtumat tietokantaan (kuvio 22), josta käyttäjä voi katsoa niitä listana. Tietokannasta pystyy etsimään esimerkiksi vain tiettyjä tapahtumia, jotka sitten näytetään käyttäjälle niiden tapahtuma järjestyksessä. (Zabbix, 2016b.)



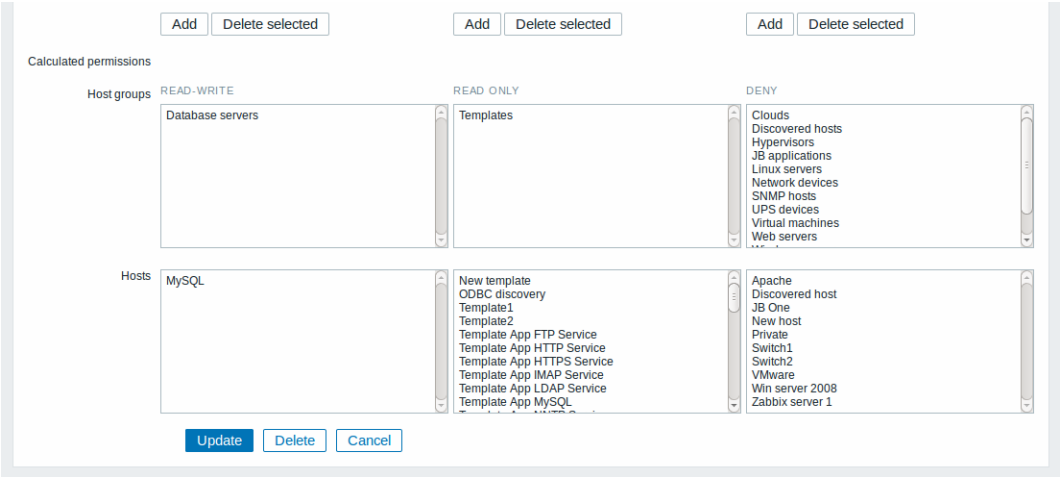
KUVIO 22. Kuvite kuva tapahtumaruudusta. Tietokantaan tallentuneet tapahtumat näytetään tässä ruudussa (Zabbix 2016b.)

Tapahtumien tarkoitus on ilmoittaa verkossa tapahtuneista muutoksista, joka voi vaikuttaa verkon toimintaan. Nämä muutokset voivat olla esimerkiksi käyttäjän ennalta määrittelemiä laukaisimia, jotka aktivoiduttuaan aiheuttavat tapahtuman josta käyttäjälle tulee ilmoitus. (Zabbix 2016b.)

3.4 Turvallisuus

Zabbixissa on joustava käyttäjän oikeuksien jako järjestelmä (kuvio 23), jolla voidaan määritellä käyttäjän oikeuksia yhdessä Zabbix asennuksessa, tai jaetussa ympäristössä. Zabbix listaa käyttäjät hierarkiassaan kolmella tavalla: Zabbix User, Zabbix Admin ja Zabbix Super Admin. Käyttäjäryhmälle voi asettaa kolmenlaisia oikeuksia: Luku- ja kirjoitusoikeus, vain lukuoikeus ja ryhmästä esto. Käyttäjäryhmät läpikäytynä tarkoittavat seuraavaa:

- Zabbix Userilla on pääsy monitorointiin. Käyttäjällä ei ole oikeuksia resursseihin oletuksena, mutta oikeudet voi muuttaa. Käyttäjäryhmien oikeudet tulee määritellä käyttäjäkohtaisesti.
- Zabbix Adminilla on pääsy monitorointiin ja asetuksiin. Käyttäjällä ei ole hallinnollisia oikeuksia oletuksena. Oikeudet käyttäjäryhmiin tulee määritellä käyttäjäkohtaisesti.
- Zabbix Super Adminilla on pääsy kaikkeen: monitorointiin, asetuksiin ja hallinnoimiseen. Käyttäjällä on luku- ja kirjoitusoikeus kaikkeen. Käyttäjän oikeuksia ei voi kumota estämällä pääsyä käyttäjäryhmiin. (Zabbix 2016g.)



KUVIO 23. Kuva näkymästä, jossa voidaan määritellä käyttäjäryhmien oikeuksia Zabbixissa (Zabbix 2016g.)

Zabbixin verkkokäyttöliittymä hyödyntää useita varmennusmenetelmiä, joita ovat muun muassa sisäinen tietokanta, HTTP (Hypertext Transfer Protocol) varmennus ja LDAP (Lightweight Directory Access Protocol) varmennus. Mikäli käytössä on LDAP varmennus ja varmennus jostain syystä estyy, käyttäjäryhmät voivat silti käyttää sisäistä varmennusta päästäkseen Zabbixin käyttöliittymään. (Zabbix 2016g.)

Zabbix käyttää komponenttien välillä salauksena TLS (Transport Layer Security) protokollan versiota 1.2. Sertifikaattiin ja ennalta jaettuun avaimeen (pre-shared key) perustuva salaus on Zabbixissa tuettu. Salaus

on Zabbixissa valinnaista ja määriteltävissä komponenttikohtaisesti. (Zabbix 2016g.)

4 OPENNMS

4.1 OpenNMS:stä yleisesti

OpenNMS ja Zabbix jakavat useita samoja ominaisuuksia. Molemmat ovat yritystason järjestelmiä ja ovat täysin ilmaisia ja kaikki kehitys on tehty avoimeen lähdekoodiin perustuen. OpenNMS on luotettava, muokattava, avoimeen lähdekoodiin perustuva ja kehitetty verkonvalvontaratkaisuksi. OpenNMS on jaettu kahteen eri versioon, jotka ovat Meridian ja Horizon.

Horizon versio on yrityksille, jotka haluavat pysyvyyttä ja pitkäaikaista tukea järjestelmälleen. Meridian versiossa tulee ensimmäisenä kaikki uudistukset ja Meridian on uusien teknologioiden ja IT-ratkaisujen monitorointiin mainio työkalu. Molemmat jakelut ovat rakennettu täysin vapaaseen lähdekoodiin. OpenNMS järjestelmän ominaisuuksina mainitaan helppo integroiminen, suorituskyvyn hallinnointi, palvelun varmuus, tapahtumakeskeisyys, topologian havainnointi ja varustelu. (OpenNMS 2016c.)

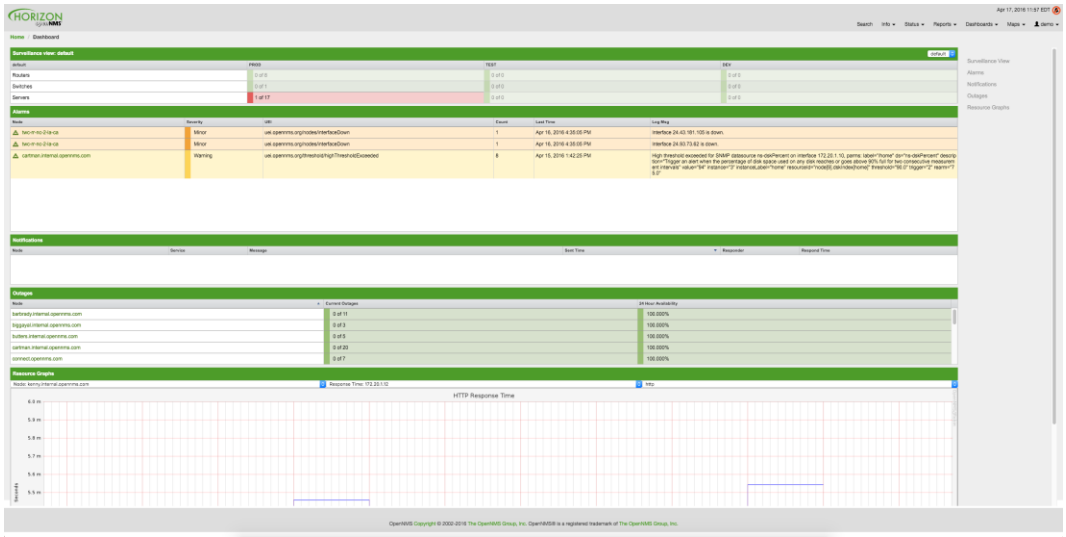
4.2 OpenNMS:n ominaisuuksia

Sovellusalusta on yrityskäyttöön soveltuva, integroitava, avoimeen lähdekoodiin perustuva ja sovellusalustasta voidaan rakentaa verkonvalvontatyökalu. OpenNMS:llä on aktiivinen yhteisö. Tässä työssä keskityttiin Horizon mallin toimintaan, koska se on pysyvyydensä ja pitkäaikaisen mallinsa mukaisesti ihanteellinen ratkaisu.

OpenNMS:n graafinen käyttöliittymä on hyvin muokattavissa oleva. Käyttöliittymän muokattavuus soveltuu eri käyttäjätasojen tarpeiden vastaamiseen. OpenNMS:n käyttöliittymän komponenteiksi on mainittu viisi osaa: valvontanäkymä, hälytykset, ilmoitukset, Node Status ja käytössä olevien resurssien kaavionäkymä. (OpenNMS 2016c.)

4.2.1 OpenNMS Horizon Dashboard

Valvontanäkymä antaa nopean ja tiivistetyn näkymän mitä verkossa tapahtuu valvonnan aikana (kuvio 24). Hälytykset kertovat asetettujen triggereiden ilmaisemia hälytyksiä, kun esimerkiksi reititin tai kytkin on lakannut toimimasta. Hälytyksessä kerrotaan muun muassa myös vian vakavuus ja lukumäärä, montako kertaa sama hälytys on tapahtunut. Ilmoituksissa kerrotaan verkon osan ja sen komponentin nimi, palvelu johon se on liitetty, tilaviesti komponentilta ja kuka sen on vastaanottanut ja reagoinut lähetettyyn ilmoitukseen. (OpenNMS 2016e.)

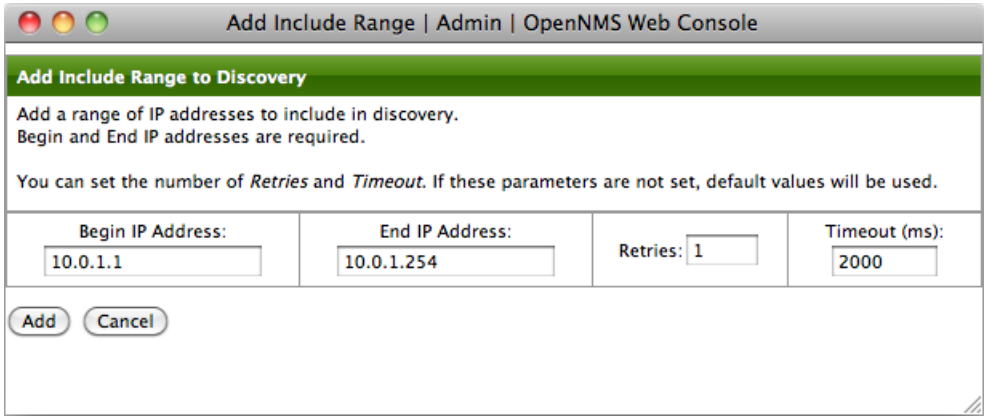


KUVIO 24. Käyttöliittymä, johon on asetettu toimintaan valvontanäkymä (OpenNMS 2016e.)

Node Status kertoo verkon komponenttien tilan, koska hälytykseen vastaaminen ei välttämättä tarkoita, että tilanne on ratkaistu. Node Statuksesta käyttöliittymässä näkee minkälaisessa tilassa verkon komponentit ovat. Kaavionäkymässä voidaan näyttää esimerkiksi Node Statuksien lukumäärä tiettynä kellonaikana. Tämä auttaa selvittämään kuinka paljon tapahtumia verkossa on ollut tiettynä kellonaikana, jolloin voidaan havaita esimerkiksi säännöllisiä häiriöitä verkon toiminnassa. (OpenNMS 2016e.)

4.2.2 Discovery

Discoveryllä OpenNMS löytää verkon osat ja komponentit. Discovery voidaan asettaa automaattiseksi, tai käyttää manuaalisena riippuen käytön järkevyydestä. Isommassa verkossa automaatiossa on omat hyötynsä, mutta suppean verkon hallinnointiin ei välttämättä tarvita kuin manuaalista verkon laitteiden havainnointia. (OpenNMS 2016a.)

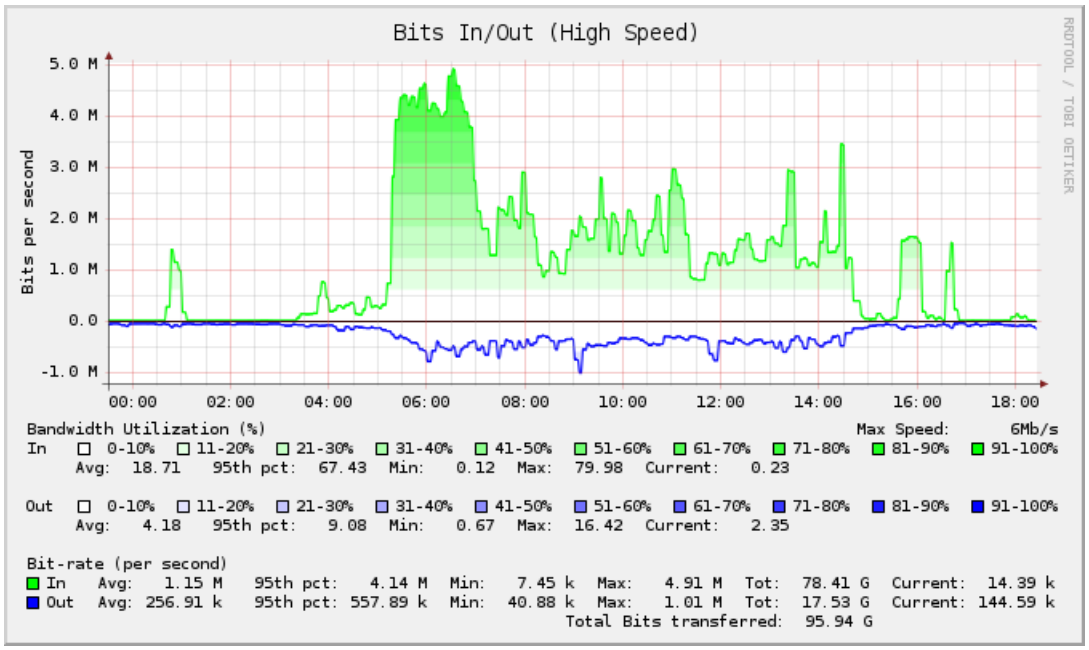


KUVIO 25. Kuva Discovery ominaisuuden käytöstä. Siinä syötetään IP-osoitealue ja jokaiseen IP-osoitteeseen käytettävä uusintayritysten lukumäärä sekä haun enimmäiskesto (OpenNMS 2016a.)

Automaattinen havainnointi toimii joko hakemalla laitteita IP-osoitealueen avulla (kuvio 25), sekä SNMP_communityn määrittelyllä. SNMP_community tarkoittaa, että verkon osan komponentilla on roolinsa mukaiset ominaisuudet ja OpenNMS valvoo tietyn roolin omaavan verkon komponentin tiettyjä valittuja osa-alueita. Esimerkiksi verkon reitittimen tai kytkimen yhteys toiseen reitittimeen tai kytkimeen. Yhteyden katketessa siitä ilmoitetaan verkon hallinnoijalle, joka reagoi siihen vaaditulla tavalla. (OpenNMS 2016a.)

4.2.3 Kaaviot

Versiosta 1.3.0 eteenpäin OpenNMS on tukenut graafisia kaavioita käyttöliittymässä (kuvio 26). Kaavioita pystyy muokkaamaan omiin käyttötarpeisiinsa ja OpenNMS:n omista dokumenteista löytyy ohjeita kaavioiden muodostamiseksi. (OpenNMS 2016d.)

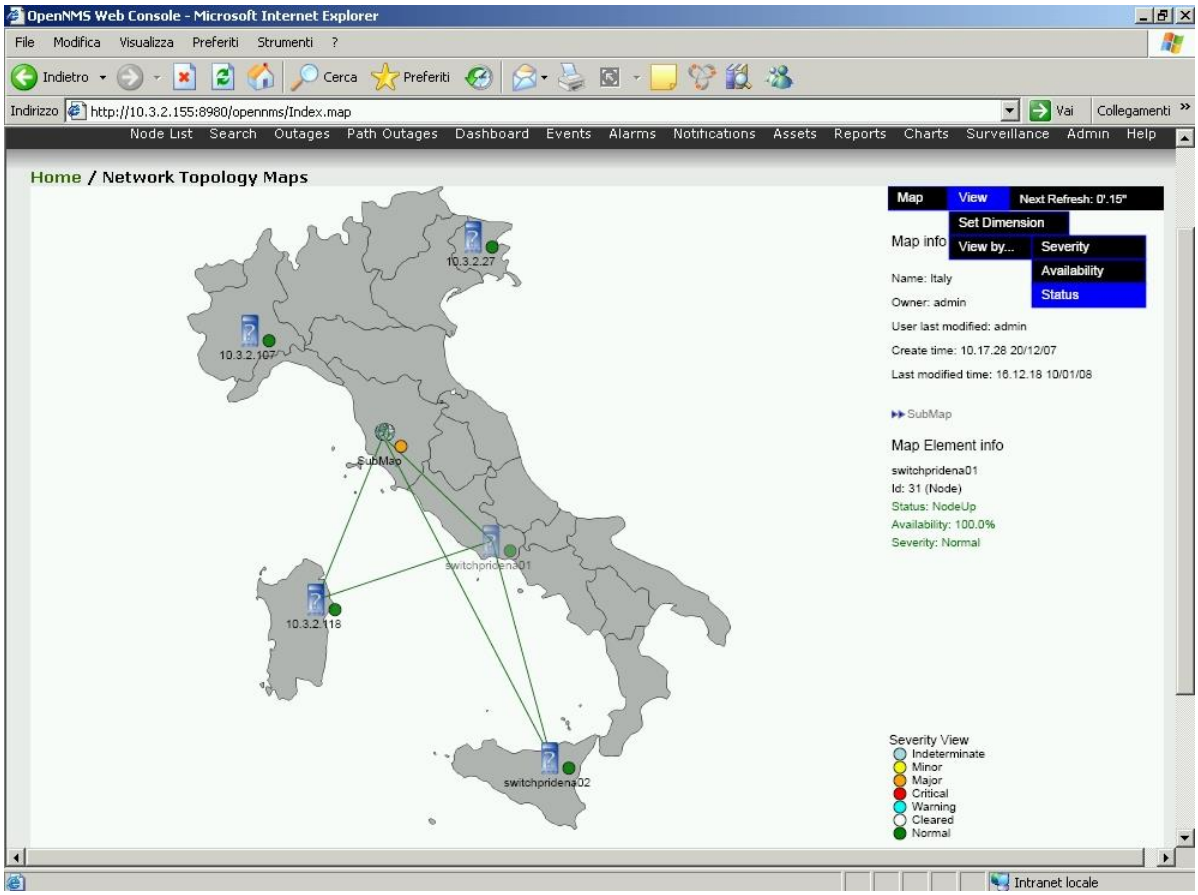


KUVIO 26. Kaavio, jossa kuvataan sisään tulevia ja ulos lähteviä bittejä verkon käyttöasteena (OpenNMS 2016d.)

OpenNMS:stä löytyy valmiiksi luotuja kaaviopohjia, joilla pystyy kuvaamaan esimerkiksi: mib2 arvoja, lämpötilaa, prosessorin kuormitusta ja levytilan käyttöastetta. NRTG (Near Real-Time Graphing), eli reaaliajassa määreen tarkkailu on mahdollista OpenNMS:ssä SNMP:tä käytettäessä. Tämä voi esimerkiksi olla prosessorin kuormituksen tarkkailua. (OpenNMS 2017.)

4.2.4 Kartat

OpenNMS:n karttojen avulla on mahdollista visuaalisesti hahmottaa verkon osien komponenttien väliset yhteydet ja tarkastella niitä, kuten käy ilmi yllä olevassa kuviossa (kuvio 27). Karttojen näkymää pystyy muokkaamaan. OpenNMS:ään kartat ovat tulleet oletuksena käyttöön vasta versiosta 1.7.0 ja niitä pystyvät tekemään, muokkaamaan ja poistamaan vain admin oikeuden omaavat käyttäjät. (OpenNMS 2016f.)



KUVIO 27. Kuva karttaominaisuudesta käytössä (OpenNMS 2016f.)

OpenNMS:ssä kartoilla voi olla alikarttoja. Kartoista luotavilla alikartoilla voidaan kuvailla verkon osia tarkasti. Esimerkkinä ominaisuudesta voidaan tarkastella yhden reitittimen takana olevia kytkimiä ja päätelaitteita. (OpenNMS 2016f.)

4.2.5 Tapahtumat

Tapahtumat ovat tärkeitä OpenNMS:n toiminnassa. Tapahtumat kertovat verkon tilanteista ja niiden tarkoitus on reagoida nimensä mukaisesti verkon osissa ja komponenteissa tapahtuviin tilanteisiin. (OpenNMS 2016b.)

Tapahtumasta kerrotaan määriteltyjä tietoja, jotka auttavat verkon hallinnoijaa reagoimaan tarvitulla tavalla verkon tapahtumaan. Tapahtumat listataan yksitellen lokitiedostoon, jotta yksittäisten tapahtumien tarkastelu on helpompaa. (OpenNMS, 2016b.)

4.3 Turvallisuus

OpenNMS suositellaan asennettavaksi mahdollisimman riisutulla versiolla tietokoneen käyttöjärjestelmästä. Tällä keinolla vältetään mahdollisien haavoittuvuuksien löytymistä ja OpenNMS:n valvonnan alaisena olevaan verkkoon pääsy. Suorituskyvyllisesti OpenNMS:n asentaminen ainoana palveluna tietokoneelle on suositeltua. Silloin prosessointitehoa ei käytetä mihinkään muuhun, kuin verkon tarkkailuun. Käyttäjätilien oikeuksien rajoittaminen parantaa verkon turvallisuutta. Kun käyttäjätilejä rajoitetaan vältytään turhilta toimenpiteiltä OpenNMS:n käytössä. (OpenNMS 2016g.)

Kun ohjelmiston asentaa ainoana komponenttina tietokoneeseen voidaan suorituskyky maksimoida ja verkon turvallisuudesta pitää parempaa huolta, kun kerätty data ei pääse vuotamaan verkon ulkopuolisille tahoille. Ohjelmiston oleminen ainoana komponenttina tietokoneessa edesauttaa myös verkkoon kytketyn palomuurin toimintaa. Tällöin palomuurin ei tarvitse valvoa usean ohjelman datan läpikulkua palomuurin lävitse. (OpenNMS 2016g.)

5 VERKONVALVONNAN VERTAILU

5.1 Verkonvalvontasovelluksen kriteerit

Verkonvalvontasovellukselta ei vaadita paljon ominaisuuksia, vaan enemmänkin perus ylläpitotoimintoja. Erikoisemmat toiminnot, joita ei tarvita tavallisessa ylläpitotilanteessa tehdään valmistajien omilla sovelluksilla. Vaadittavia kriteereitä ovat seuraavat:

- Sovelluksen tulee olla Unix-pohjainen.
- Sovelluksen tulee olla käytettävyysasteeltaan hyvä, jotta sitä voi käyttää myös opetustarkoituksessa.
- Sovellukseen tulee julkaista päivityksiä.
- Sovelluksesta on tarjolla dokumentointia.
- Sovelluksella on mahdollista lisätä ja poistaa tukiasemia.
- Sovelluksella on mahdollista määritellä tukiasemien perusasetukset (IP, SSID, kanava, ja niin edelleen...).
- Sovelluksella on mahdollista toteuttaa käyttäjämäärien laskemista.
- Sovelluksella on mahdollista toteuttaa käyttäjien liikennemäärän laskemista.
- Sovelluksella on mahdollista valvoa yksittäisen tukiaseman toimintaa, eli onko tukiasema esimerkiksi toiminnassa, tai vikatilassa.
- Sovelluksella on mahdollista toteuttaa verkkotopologiasta karttakuva, jotta vian ilmetessä ylläpidon on selkeämpi havaita missä vika on.

5.2 Sovellusten vertailu

Molemmilla sovelluksilla testattiin kriteerien vaatimia toimintoja. Kriteerien perusteella on tehty alla oleva taulukko (taulukko 1), jossa sovelluksia on

vertailtu ominaisuuksiltaan keskenään. Vertailu on toteutettu, jotta ominaisuuksien käytettävyyden eroavaisuuksia käyttäjälle saadaan esille.

Sovelluksia on vertailtu tietyissä osa-alueissa asteikolla Huono, Välttävä, Keskinkertainen, Hyvä, Erinomainen. Mikäli käytettävyyttä ei ole tarvinut mitata on sovelluksesta ilmoitettu ominaisuus joko Kyllä, tai Ei.

TAULUKKO 1. Verkonvalvontasovellusten ominaisuuksien vertailu

OHJELMA/OMINAISUUDET	Zabbix	OpenNMS
Käyttöjärjestelmä	Unix	Unix
Kieli	Englanti	Englanti
Päivitykset	Kyllä	Kyllä
Käytettävyys	Erinomainen	Keskinkertainen
Dokumentointi	Kyllä	Kyllä
Muokattavuus	Hyvä	Hyvä
Käyttöliittymä	WEB	WEB
Kartta	Hyvä	Hyvä
Graafit	Erinomainen	Hyvä
Hälytykset	Erinomainen	Erinomainen
OMINAISUUDET:		
Tukiaseman lisääminen ja poistaminen	Kyllä	Kyllä
Tukiaseman perusasetukset	Kyllä	Kyllä
Laskentatoimet	Kyllä	Kyllä

5.3 Yhteenveto verkonvalvontasovelluksista

Zabbixin ja OpenNMS:n välillä ei ollut juurikaan eroavaisuuksia yleisellä tasolla. Molemmat ovat ilmaisia, hyviä, luotettavia ja muokattavissa olevia yritystason verkonvalvontaohjelmistoja. Molemmilta sovelluksilta löytyy pitkä historia.

Asennettaessa Zabbix suoriutui tehtävästään OpenNMS:ää paremmin. OpenNMS:n kanssa ilmeni ongelmia postgreSQL:n ja muutaman komennon kanssa, mutta dokumentteja katsomalla ja yhteisön avulla ongelmista selvittiin kohtuullisen helposti. Zabbixin asennus oli hyvän dokumentoinnin ansiosta yksinkertaista, eikä postgreSQL aiheuttanut Zabbixin kanssa mitään ongelmia.

Molemmista sovelluksista löytyy ominaisuuksia, jotka auttavat käyttäjää verkonvalvonnassa. OpenNMS:stä löytyy enemmän ominaisuuksia, mikäli käytössä oleva verkko on laajempi ja tarkempia ominaisuuksia tarvitsee, mutta OpenNMS tuntui kankealta. Zabbixin ominaisuudet tulivat selkeästi ja ymmärrettävästi esille dokumenteista ja käytön aikana, minkä takia Zabbixin käyttäminen tuntui nopeammin luontevammalta

OpenNMS:ssä karttojen kerrosten sisäkarttojen olemassaolo teki vaikutuksen sen jäädessä ainoaksi paremmaksi ominaisuudeksi. Zabbixista löytyi parempi graafinen käyttöliittymä, joka on verkon valvonnallisesta näkökulmasta suuri yksittäinen tekijä. Tiedon pitää löytyä helposti ja nopeasti. Graafinen käyttöliittymä toimi Zabbixissa vaaditulla tavalla.

Ohjelmistojen vertailu käytettävyyden osalta päättyi melko yksipuoliseen tulokseen. OpenNMS:stä löytyy suuremmalle yritykselle tarpeellisia ominaisuuksia enemmän, mikäli esimerkiksi verkon valvonnassa tarvitaan verkon osan ja sen komponentin yksittäisten palvelujen valvontaa. Tätä ei

kuitenkaan työssä haettu. Ohjelmistossa panostettiin hyvään käytettävyyteen, joka oli Zabbixissa parempi.

Käytettävissä olevat dokumentit ja yhteisö olivat melko tasavertaiset. Zabbixissa yhteisön tukea löytyy kiitettävästi ja dokumentit ovat yksinkertaisesti ja hyvin ymmärrettävästi selitettyjä. OpenNMS:ssä dokumentteja löytyy paljon, mutta yleiskuva dokumenteista jää melko epäselväksi. Käyttäjän näkökulmasta tehdyt OpenNMS:n dokumentaatiot tuntuivat jäävän usein hyvin vajavaisiksi, koska ne ovat suunnattu ohjelmistoa paljon käyttäneille.

OpenNMS järjestää yhteisön tuen lisäksi maksullisia koulutuksia, mitkä ovat monelle kokemuksistaan kertoneelle tuoneet avun ongelmiin ja järjestelmän käytettävyyden ymmärtämiseen. Zabbix tarjoaa myös koulutusta, joten yksinään dokumenttien varaan käyttäjä ei kummankaan järjestelmän kanssa jää.

Molemmat sovellukset täyttivät vaaditut kriteerit, mutta tavoitteesta suoritui paremmin Zabbix. Näin ollen Zabbix valikoitui asiakkaan kanssa käyttöön kahdesta valittavana olevasta sovelluksesta. Valinnassa vaikutti edukseen Zabbixin parempi käytettävyysaste, sekä selkeämpi pääikkuna.

6 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli tutkia, asentaa, vertailla erilaisia NMS-ohjelmistoja ja valita asiakkaan tarpeisiin soveltuva ohjelmisto. Verkonvalvontaohjelmistot käyttävät SNMP-protokollaa keskustellakseen verkkoon kytkettyjen laitteiden kanssa. Työssä tutustuttiin myös SNMP-protokollan toimintaan ja historiaan.

Sovelluksen kriteereinä oli olla hyvä käytettävyysasteeltaan ja Unix-pohjainen. Sovellukseen täytyi tulla säännöllisesti päivityksiä, sekä opetuskäyttöä varten dokumentoinnin tuli olla kunnossa sovelluksen tarjoajan osalta. Verkonvalvontasovelluksella täytyi pystyä tekemään perus ylläpitotehtäviä, kuten laitteiden lisäämistä ja poistamista, sekä tavallisimpien ominaisuuksien valvontaa, joita ylläpidollisesti tarvitaan. Sovelluksella tuli pystyä piirtämään verkkotopologiasta havainnollistava kuva, jotta ylläpidolla on käsitys valvottavasta verkosta ja kyky vikatilanteessa paikantaa vian sijainti.

NMS-ohjelmistojen tutkiminen ja niiden käyttäminen toi ilmi, kuinka suuresta kokonaisuudesta verkonvalvonnassa on kyse ylläpidon näkökulmasta. Toimivalla ja järkevällä verkonvalvontasovelluksella on suuri merkitys ylläpidossa. Hyvin toteutettuna käytettävä ohjelmisto raportoi vikatilanteissa käyttäjää mahdollisesti reaaliajassa ja käytettävää tietoa voidaan soveltaa nopeasti käytäntöön. Verkon ylläpitäjälle tämä tarkoittaa vähemmän rikkoutuneita laitteistoja ja vähemmän ongelmatilanteita verkossa. Verkon käyttäjälle tämä tarkoittaa parempaa käytettävyyttä ja toimintavarmuutta.

Verkonvalvonta sovelluksella voidaan muodostaa yksityiskohtainen kuva verkon topologiasta, jolloin ylläpidolla on käsitys siitä, missä verkon eri laitteet sijaitsevat ja missä kunnossa valvottavat laitteet ovat. Tähän apuna löytyy verkonvalvonta sovelluksista löytyvät valmiit mallinnukset, sekä auto discovery toiminnot. Hyvä verkonvalvonta sovellus on selkeä ja helppokäyttöinen. Hyvästä verkonvalvonta sovelluksesta löytyy myös monipuoliset ominaisuudet mikäli hallittava verkko kasvaa, tai verkosta

tarvitsee muokata monitoroidakseen eri ominaisuuksia kuin lähtötilanteessa.

Vertailtaessa ohjelmistoja Zabbix erottautui vaihtoehdoista paremmaksi. Suurimpana erona vaihdoehdoista Zabbixissa oli parempi ja selkeämpi käytettävyys. Hyvä käytettävyys oli myös yksi vaadittavista kriteereistä. Verkonvalvonta sovelluksista löytyi paljon ominaisuuksia, mutta OpenNMS:n ominaisuuksia ei ollut selkeä käyttää. Ominaisuuksien lisääminen ohjelmistoon saattaa aiheuttaa sen, että ohjelmistosta tulee liian sekava ylläpitäjälle. Zabbixissa on paljon ominaisuuksia, mutta käytettävyyttä on myös ajateltu Zabbixin ollessa selkeämpi ja käytännöllisempi, kuin vertailtava OpenNMS.

Tekniikan kehittyminen nopeammaksi ja vaativammaksi tulee olemaan haastavaa laitevalmistajille ja sovelluskehittäjille. Siirtyminen käyttämään Ipv6 tekniikkaa tulee mullistamaan osan vanhalla tekniikalla tehdyistä ratkaisuista ja päivittäminen nykyaikaan tulee olemaan haastavaa. Vanhan laitteistokannan uusiminen ympäristölle vähän kuormittavalla tavalla tulee olemaan erittäin vaikeaa, joten ratkaisuja haetaan todennäköisesti kehittämällä sovellustasolla jo käytössä olevaa laitteistoa.

Toinen laitteistovalmistajien ja sovelluskehittäjien pullonkaula tulee olemaan koko ajan kasvava digitaalinen materiaali. Kun TV-yritykset ja suuret lehtipainot siirtävät materiaaliaan entistä enemmän verkkoon, tulee tätä dataa ylläpitävien laitteiden kestää todella suurta kuormitusta. Ylläpitäjälle tämä tarkoittaa kasvavaa laitteistoihin kohdistuvaa siirrettävän datan määrää ja rasitusta laitteiden kestokyvylle sekä verkon vikasietojärjestelmälle. Hallittavien verkkojen segmentointi järkevästi tulee olemaan varmasti yksi menettelytavoista, joilla ehkäistään verkon laitteistojen hajoaminen ja verkon lamaantuminen osittain, tai kokonaan pitkiksi ajoiksi.

Eri energialähteiden käytön hyödyntäminen tulee olemaan osa tulevaisuuden laitteisto- ja sovelluskehitystä. Koska käytettävän energian määrä kasvaa todella nopealla tahdilla tulee energiaa saada myös entistä

enemmän uusiutuvista energianlähteistä. Uusiutuvien energianlähteiden mahdollisimman tehokas hyödyntäminen on elintärkeää teknologia-alalle. Green ICT projektit ovatkin yksi tärkeimmistä kehityksen mahdollistajista ja niihin panostamalla laitevalmistajatkin hyötyvät uusimmista alan osaajista ja tekniikan innovaatioista.

Turvallisuus tulee olemaan suuri kehityskohta verkonvalvonnassa digitaalisen materiaalin kasvaessa. Verkonvalvonnan kehittäminen turvallisuuden kannalta on todella tärkeää, kun kyberrikollisuus on kokenut uuden aallon tekijöiden toimesta entistä näkyvämpää nousua tavallisen käyttäjän arkeen. Uutisointi suurienkin yhtiöiden verkko-ongelmista kasvattaa paineita verkonvalvonnassa ja laitteistokehityksessä. Jo olemassa olevien laitteistojen ongelmien ja puutteiden havaitseminen ja korjaaminen on tärkeää tietotekniikan turvallisuuden vaarantumisen ehkäisemiseksi.

LÄHTEET

Cisco 2007. Management Information Base Overview [viitattu 2.4.2017]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/pgw/7/mibs/guide/7MIB_Ch1.html

OpenNMS 2016a. OpenNMS Discovery [viitattu 25.11.2016]. Saatavissa: https://wiki.opennms.org/wiki/Discovery

OpenNMS 2016b. OpenNMS Events [viitattu 27.11.2016]. Saatavissa: https://docs.opennms.org/opennms/releases/latest/guide-admin/guide-admin.html#ga-events

OpenNMS 2016c. OpenNMS Front Page [viitattu 20.11.2016]. Saatavissa: https://www.opennms.org/en

OpenNMS 2016d. OpenNMS Graphs [viitattu 26.11.2016]. Saatavissa: https://wiki.opennms.org/wiki/Graph_Gallery

OpenNMS 2016e. OpenNMS Horizon Dashboard [viitattu 25.11.2016]. Saatavissa: https://docs.opennms.org/opennms/releases/latest/guide-user/guide-user.html#user-guide-dashboard

OpenNMS 2016f. OpenNMS Maps [viitattu 26.11.2016]. Saatavissa: https://wiki.opennms.org/wiki/Maps

OpenNMS 2016g. OpenNMS Security [viitattu 28.11.2016]. Saatavissa: https://wiki.opennms.org/wiki/Security_Considerations

OpenNMS 2017. OpenNMS NRTG [viitattu 20.4.2017]. Saatavissa: https://wiki.opennms.org/wiki/NRTG

O’Reilly & Associates 2002a. SNMP and UDP [viitattu 31.10.2016]. Saatavissa:

http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_01.htm#ahead-1

O'Reilly & Associates 2002b. SNMP Operations [viitattu 2.3.20171]. Saatavissa: https://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_06.htm

RFC1157, 1990. A Simple Network Management Protocol (SNMP) [viitattu 31.10.2016]. Saatavissa: https://tools.ietf.org/html/rfc1157

RFC1441, 1993. Introduction to Version 2 of the Internet-standard Network Management Framework [viitattu 31.10.2016]. Saatavissa: https://tools.ietf.org/html/rfc1441

RFC2570, 1999. Introduction to Version 3 of the Internet-standard Network Management Framework [viitattu 31.10.2016]. Saatavissa: https://tools.ietf.org/html/rfc2570

Solarwinds 2017. Basics of Network Monitoring [viitattu 19.5.2017]. Saatavissa: http://www.solarwinds.com/basics-of-network-monitoring

Zabbix 2016a. What is Zabbix [viitattu 08.11.2016]. Saatavissa: http://www.zabbix.com/product

Zabbix 2016b. Zabbix Event & Notification [viitattu 8.11.2016]. Saatavissa: http://www.zabbix.com/event_notification

Zabbix 2016c. Zabbix Graphs [viitattu 8.11.2016]. Saatavissa: http://www.zabbix.com/graphs

Zabbix 2016d. Zabbix Install from Packages [viitattu 20.11.2016]. Saatavissa: https://www.zabbix.com/documentation/2.4/manual/installation/install_from_packages

Zabbix 2016e. Zabbix Maps [viitattu 08.11.2016]. Saatavissa: http://www.zabbix.com/maps

Zabbix 2016f. Zabbix Network Discovery [viitattu 9.11.2016]. Saatavissa: http://www.zabbix.com/auto_discovery

Zabbix 2016g. Zabbix Security & Authentication [viitattu 8.11. 2016]. Saatavissa: http://www.zabbix.com/security_authentication

Zabbix 2016h. Zabbix Web Frontend [viitattu 8.11.2016]. Saatavissa: http://www.zabbix.com/zabbix_web_frontend

LIITE

Seuraavaksi käydään läpi vaiheittain Zabbixin asennus Ubuntulle: Ensiksi syötetään seuraavat komennot, joilla asennetaan materiaalipankin konfiguraatiopaketti. Tämä paketti sisältää apt (Advanced Packaging Tool) konfiguraatiotiedostot. Paketin asennuksien jälkeen haetaan päivitykset, jotta käytössämme olisi uusin versio.

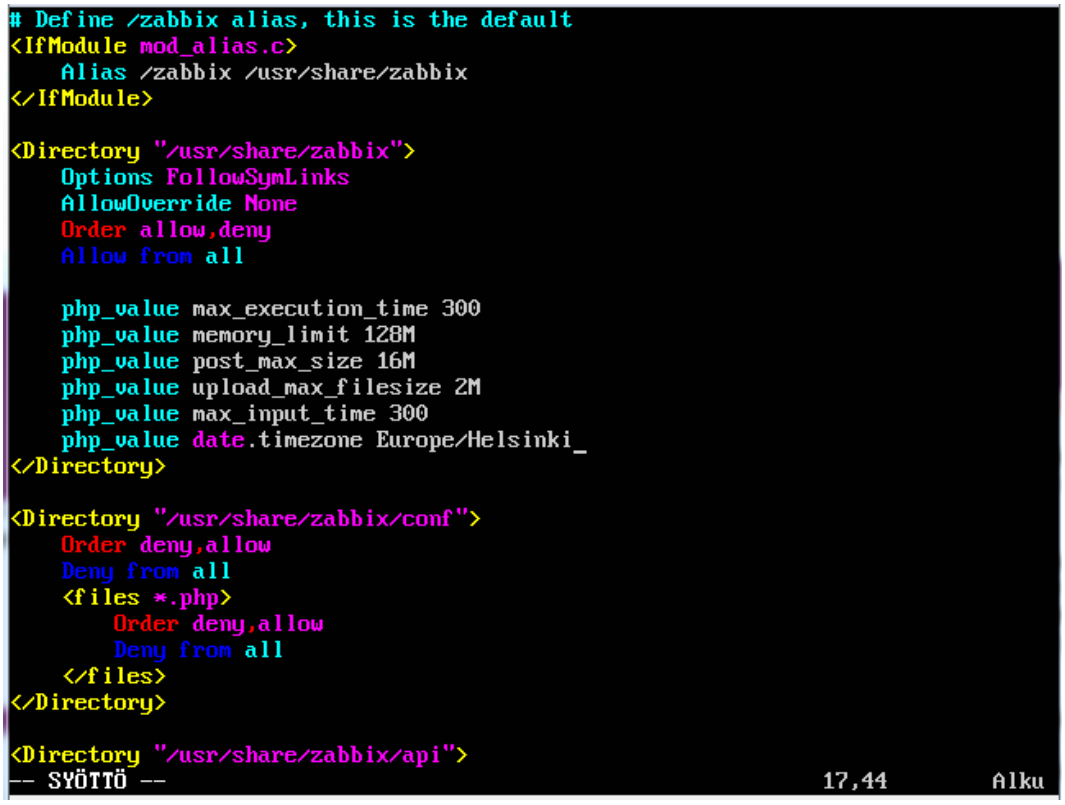
wget http://repo.zabbix.com/zabbix/2.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_2.4-1+trusty_all.deb

dpkg -i zabbix-release_2.4-1+trusty_all.deb

apt-get update

Tämän jälkeen asennetaan Zabbixin paketit. Näihin kuuluvat serveri, web käyttöliittymä ja mysql tietokanta.

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



KUVIO 1. Apachen konfiguraatioiden muutos käyttöliittymän PHP osion

osalta tiedostossa

Tämän jälkeen editoidaan Apachen konfiguraatiota web käyttöliittymän PHP osion osalta (kuvio 1). Osa PHP:n asetuksista on konfiguroitu oletuksena, mutta tärkeää on vaihtaa aikavyöhyke oikeaksi. Oletuksena aikavyöhykkeenä on yhtiön kotimaan Latvian pääkaupungin mukaan ”Europe/Riga”, mutta koska olemme Suomessa tähän muutetaan ”Europe/Helsinki”. Myöskin aikavyöhyke komennosta tulee ottaa kommentointi (#) pois, jotta asetus tulee voimaan. Alla on oletuksena oleva konfiguraatio:

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 date.timezone Europe/Riga

Kun aikavyöhyke on asetettu oikeaksi ja kommentointi on otettu asetuksista pois tulee apache web server palvelu käynnistää uudelleen. Tämä tapahtuu komennolla:

service apache2 restart

Tämän jälkeen voidaan siirtyä selaimella Zabbixin web käyttöliittymään (kuvio 2). Sinne pääsee osoitteella http://zabbix-frontend-hostname/zabbix. Oletuksena käyttäjänimi ja salasana ovat Admin ja Zabbix. (Zabbix 2016d.)

KUVIO 2. Zabbix ohjelmiston asennusvelhon aloitus ikkuna