VAPAIDEN VERKONVALVONTAOHJELMISTOJEN VERTAILU JA TESTAUS

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Riihimäki, 31.5.2012

Lasse-Tapani Ketola

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

RIIHIMÄKI
Tietotekniikan koulutusohjelma

Tekijä Lasse-Tapani Ketola **Vuosi** 2012

Työn nimi Vapaiden verkonvalvontaohjelmistojen vertailu ja testaus

TIIVISTELMÄ

Tämän työn tarkoituksena oli perehtyä tarjolla oleviin vapaisiin eli avoimeen lähdekoodiin perustuviin verkonvalvontaohjelmistoihin. Verkonvalvontaohjelmistoista on viime vuosina tehty lukuisia opinnäytetöitä. Monet niistä käsittelevät Nagios-verkonvalvontaohjelmistoa tai SNMP:n hyödyntämistä.

Tässä työssä vertailtiin kymmentä verkonvalvontaohjelmistoa. Vertailu perustui ohjelmistojen dokumentaatioon ja valmistajan kotisivuillaan ilmoittamiin tietoihin. Erilaisista toteutustavoista ja painotuksista huolimatta lähes kaikki vertaillut ohjelmistot olivat ominaisuuksiltaan monipuolisia ja keskenään hyvin samankaltaisia.

Kahta vertailuun valittua ohjelmistoa, AlienVault OSSIM:a ja Zenoss Corea, testattiin suljetussa testiympäristössä. Testauksen tarkoituksena oli todentaa ohjelmistojen ominaisuuksien toiminnallisuus käytännössä. Testit pyrittiin toteuttamaan ohjelmistojen dokumentoinnin avulla. AlienVaultin kohdalla tästä oli poikettava monessa tilanteessa. Zenossin osalta testi kyettiin toteuttamaan pääsääntöisesti dokumentaation avulla.

Testauksen painopiste oli valvonnan aloittamisessa sekä vian- ja suorituskyvynhallintaan liittyvien parametrien tarkkailussa. AlienVault sisälsi Nagios-ohjelmiston ja siksi tarvittavat asetukset tehtiin suurelta osin komentoriviltä eri asetustiedostoihin. Zenoss hyödynsi päämenetelmänä SNMP:tä. Koska Zenossiin oli saatavilla laitekohtaisia lisäosia, joissa oli tehty valmiiksi tarvittavat asetukset, ei asetuksien käsin muokkaamiseen ollut juurikaan tarvetta.

Erilaisista toteutustavoista huolimatta kummatkin ohjelmistot kykenivät toteuttamaan lähes kaikki testitapaukset. Mahdollista jatkotutkimusta voi suunnata esimerkiksi ohjelmistojen suorituskykyyn tai tapahtumien yksityiskohtaisempaan käsittelyyn ja raportointiin.

Avainsanat verkonhallinta, verkonvalvonta, avoin lähdekoodi, vapaat ohjelmistot

Sivut 46 s. + liitteet 20 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

Riihimäki
Degree Programme in Information Technology

Author Lasse-Tapani Ketola **Year** 2012

Subject of Bachelor's thesis Comparison and testing of open source network monitoring software products

ABSTRACT

The purpose of this thesis was to become acquainted with open source network monitoring software. Several theses on this theme have been published in recent years. Many of them deal with Nagios monitoring software or exploiting SNMP.

In this thesis ten network monitoring software products were compared with each other. The comparison was based on their documentation and other information that was presented in their home pages. Despite the different solutions and emphasis used in these products, almost every one of them was versatile, and they were all similar.

Two products, that were included in the comparison, were tested in a closed test environment. They were AlienVault OSSIM and Zenoss Core. The purpose of the test was to verify the functionality of their features in practice. It was attempted that the tests were implemented by only using their documentation. Additional information was needed in many cases concerning AlienVault but with Zenoss its documentation was mainly adequate.

The emphasis of the test was on the initial setup and monitoring parameters related to fault and performance management. AlienVault used Nagios as the main tool in availability monitoring. Therefore the necessary settings had to be modified directly to the configuration files by using a command-line interface. Zenoss used SNMP as its main method. Because device specific plug-ins were available for Zenoss, there was almost no need to adjust the settings manually. The plug-ins included readymade configuration for monitored devices.

Despite the different solutions both products could fulfil almost every test case. A possible subject for further research could be testing of the products' performance or event handling and reporting thoroughly.

Keywords network management, network monitoring, open source code, open source software

Pages 46 p. + appendices 20 p.

TERMIT JA LYHENTEET

Agentti	Sovellus, joka kerää tietoa hallittavasta laitteesta tai sitä ympäröivästä verkosta.
AT	Address Translation. Osoitteenmuunnos.
Avoin lähdekoodi	Vapaasti tutustuttavissa ja muokattavissa oleva sovelluksen lähdekoodi.
CSV	Comma Separated Values. Tiedostomuoto, jossa taulukkomuotoinen tieto tallennetaan tekstitiedostoon.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jonka tehtävänä on jakaa IP-osoite ja muita asetuksia lähiverkkoon liittyvälle uudelle laitteelle.
DNS	Domain Name Service. Nimipalvelu.
EGP	Exterior Gateway Protocol. Vanhentunut autonomisten järjestelmien yhdistämiseen tarkoitettu protokolla.
FMS	Flexible Monitoring System. Joustava valvontajärjestelmä.
GNU	GNU's Not Unix. Free Software Foundationin hallinnoima projekti, jonka tarkoituksena on kehittää täysin vapaa käyttöjärjestelmä. Projektin tuottamia ohjelmia käytetään esimerkiksi Linux-ytimen ympärille rakennetuissa käyttöjärjestelmissä.
GPL	General Public License. GNU-projektin tarpeisiin luotu avoimen lähdekoodin sovellusten julkaisuun tarkoitettu lisenssi.
Hallinnoitava objekti	Verkkomallin kerros, yksittäinen yhteys tai verkkolaitteen yksittäinen komponentti tai jokin abstrakti ominaisuus.
Hallinta-asema	Työasema, johon asennetulla verkonhallintasovelluksella valvotaan ja hallinnoidaan verkkoa.
HTML	Hypertext Markup Language. Kuvauskieli.
ICMP	Internet Control Message Protocol. TCP/IP-mallin kontrolliprotokolla.
IETF	Internet Engineering Task Force. Internet-protokollien standardisoinnista vastaava organisaatio.
IP	Internet Protocol. TCP/IP-mallin Internet-kerroksen protokolla.
ISO	International Organisation for Standardization. Kansainvälinen standardisoimisjärjestö.

ISO-levykuva	Pakkaamaton arkistotiedosto, jossa useista tiedostoista muokataan yksi tiedosto.
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector. Kansainvälisen televiestintäliiton telestandardisointisektori.
Keruuyksikkö	ks. agentti
Korrelointi	Tapahtumien välisen riippuvuuden tutkiminen.
Loki	Tapahtumarekisteri, johon kerätään tapahtumahistoria.
MAC	Media Access Control. OSI-mallin 2. kerros.
MGMT	Management. Hallinta.
MIB	Management Information Base. Hallinnoitavien objektien ja niitä määrittävien ominaisuuksien kokoelma.
MRTG	Multi Router Traffic Grapher. Valvontatyökalu, joka esittää SNMP:llä kerättyä parametritietoa graafisessa muodossa.
NMS	Network Management System. Verkonhallintajärjestelmä.
Normalisointi	Päällekkäisten tapahtumien poistaminen.
OID	Object Identifier. Yksilöintitunnus, jota käytetään MIB:ssä objektien ja ominaisuuksien tunnistamiseen.
Olio	Tietorakenne, joka sisältää toisiinsa liittyvää tietoa ja toiminnallisuutta.
OSI-malli	Open System Interconnection Reference Model. Seitsemänkerroksinen tietoliikenteen käsitemalli.
OSSEC	Open Source Host-based Intrusion Detection System. Avoimeen lähdekoodiin perustuva turvallisuusvalvontajärjestelmä.
OSSIM	Open Source Security Information Management. Avoimeen lähdekoodiin perustuva turvallisuusvalvontajärjestelmä.
PDF	Portable Document Format. Ohjelmistoriippumaton tiedostomuoto.
PHP	PHP: Hypertext Preprocessor. Yleiskäyttöinen komentosarjakieli.
Poll	Hallinta-aseman ja agentin välinen kysely-vastausoperaatio.

RFC	Request for Comments. IETF:n julkaisema muistio, joka voi olla standardi tai muu ohjeistus.
RMON	Remote Monitoring. MIB:n laajennus, joka mahdollistaa verkon valvonnan ja analysoinnin etäkäyttöisesti.
RRDTool	Round Robin Database Tool. Aikasarjamuotoisen tiedon, kuten prosessorin kuormitus tai lämpötila, käsittelyyn tarkoitettu työkalu.
SIEM	Security Information and Event Management. Verkon turvallisuuteen liittyvän tiedon ja tapahtumien hallinta.
SMI	Structure of Management Information. MIB:n tietorakenne.
SNMP	Simple Network Management Protocol. Verkonhallintaprotokolla, joka määrittelee hallintasovellusten toiminnot sekä raportin sisällön ja lähettämisen.
SQL	Structured Query Language. Relaatiotietokantojen hallintaan tarkoitettu ohjelmointikieli.
SSH	Secure Shell. Salatun tietoliikenteen protokolla.
TCP	Transmission Control Protocol. TCP/IP-mallin kuljetuskerroksen yhteydellinen protokolla.
Tikettijärjestelmä	Vikailmoitustenhallintajärjestelmä.
Trap	Agentin lähettämä sanoma hallinta-asemalle kynnysarvon ylittymisestä.
UDP	User Datagram Protocol. TCP/IP-mallin kuljetuskerroksen yhteydetön protokolla.
Vapaa ohjelmisto	Avoimeen lähdekoodiin perustuvien ohjelmien kokonaisuus.
Verkonhallinta	Työkalujen ja menetelmien kokonaisuus, jonka tarkoituksena on hallinnoida, koordinoida ja valvoa tiedonsiirtoresursseja ja -aktiviteettia.
Verkonhallintajärjestelmä	Laite- ja sovelluskokonaisuus, jolla hallinnoidaan verkkoa.
Verkonhallintaympäristö	Verkkoympäristön osa, joka sisältää kyvyn valvoa verkkoa ja kerätä informaatiota verkosta sekä kyvyn ylläpitää tietoisuutta tiedonsiirtoresurssien tilanteesta ja raportoida siitä tarvittavalla tavalla.
Verkonvalvonta	Laitteiden tilaan, verkon käyttöön ja verkon eri osien kuormitukseen liittyvän tiedon keräämistä, käsittelyä ja esittämistä.

Verkonvalvontajärjestelmä	Verkonhallintajärjestelmä, jonka ensisijaisena tarkoituksena on kerätä tietoa verkkolaitteiden tilasta, verkon käytöstä ja verkon eri osien liikennemääristä.
WMI	Windows Management Instrumentation. Windows-koneiden hallintaan tarkoitettu laajennusosa Windows Driver Modeliin.
WWW	World Wide Web. Hypertekstijärjestelmä, joka on käytettävissä Internetin kautta.
XML	Extensible Markup Language. Kuvauskieli.
XMPP	Extensible Messaging and Presence Protocol. Pikaviestintään tarkoitettu avoin protokolla.
ZenPack	Zenoss Core -ohjelmiston nimitys lisäosalle, joka sisältää muun muassa valmiit laite- tai laiteryhmäkohtaiset asetusmääritykset ja/tai valmiita raporttipohjia.

SISÄLLYS

1 JOHDANTO

Verkonhallinnan keskeisenä tavoitteena on mahdollistaa verkon käyttäjäorganisaation tarvitsemien palveluiden keskeytymätön toiminta. Laajojen verkkojen toimintaa on mahdotonta hallita tehokkaasti ilman keskitettyä verkonhallintaa. Vikaantumisista ja verkon liiallisesta kuormittumisesta johtuvat palvelukatkokset voidaan ennakoida ja jopa ehkäistä valvontatyökalujen avulla.

Tämän työn tarkoituksena on perehtyä tarjolla oleviin vapaisiin eli avoimeen lähdekoodiin perustuviin verkonvalvontaohjelmistoihin. Haettaessa kustannustehokkaita ratkaisuja vapaat ohjelmistot ovat varteenotettava vaihtoehto.

Verkonvalvontaohjelmistoista on viime vuosina tehty lukuisia opinnäytetöitä. Monet niistä keskittyvät Nagios-verkonvalvontaohjelmistoon tai SNMP:n hyödyntämiseen. Jonkin verran on tehty opinnäytetöitä myös muihin ohjelmistoihin liittyen. Tässä työssä vertaillaan useampia järjestelmiä rinnan yleisellä tasolla ilman varsinaista kohdeverkkoa.

Ohjelmistoja vertaillaan dokumentaation ja valmistajan ilmoittamien tietojen perusteella. Kahta vertailuun otettua ohjelmistoa testataan käytännössä suljetussa yksinkertaisessa testiverkossa. Testauksen tarkoituksena on todentaa dokumentaatiossa ja muissa tiedoissa ilmoitettujen ominaisuuksien toiminnallisuus käytännössä.

Tässä työssä tarkastellaan ainoastaan ilmaisia ohjelmistoja. Tarkastelun painopiste on suorituskyvyn ja vikojen hallintaan liittyvässä verkonvalvonnassa. Siksi turvallisuuslokien tarkastelu on rajattu tämän työn ulkopuolelle. Valvonnan kohteina ovat lähiverkon verkkolaitteet, palvelimet ja palvelut.

Tässä työssä vastataan seuraaviin pääkysymyksiin: millaisia avoimeen lähdekoodiin perustuvia verkonvalvontatyökaluja on olemassa, miten ohjelmistot eroavat ominaisuuksiltaan toisistaan ja miten lähiverkko on valvottavissa näillä ohjelmistoilla. Ensimmäisen pääkysymyksen tarkoituksena on selvittää eri ohjelmistojen tarkempaa käyttötarkoitusta ja mitä niillä voidaan seurata. Sen lisäksi tarkastellaan ohjelmistojen asettamia vaatimuksia laitteistokokoonpanolle ja muille tarvittaville sovelluksille. Kokonaiskuvan muodostamiseksi kartoitetaan erilaisia tukivaihtoehtoja ja ohjelmistojen kehitystahtia.

Toisen pääkysymyksen osa-alueita ovat ohjelmiston asentaminen, käyttöliittymä, keräysmenetelmät, tiedon käsittely ja hälytysmenetelmät. Kolmanteen pääkysymykseen vastattaessa tarkastellaan mitä toimenpiteitä vaaditaan valvonnan aloittamiseksi, millä tavoin ohjelmistojen asetuksia muokataan, miten ohjelmisto ilmaisee poikkeustilanteet ja millaisia raportteja ohjelmisto tuottaa. Näihin kysymyksiin kyetään vastaamaan tarkemmin ainoastaan testattujen ohjelmistojen osalta. Muiden osalta voidaan vastata perustietojen osalta toiseen pääkysymykseen.

Työn lopputuloksena syntyy käsitys ohjelmistojen soveltuvuudesta verkonvalvontaan sekä niiden keskinäisistä eroista. Saatujen tulosten perusteella on mahdollista valita soveltuvin järjestelmä tiettyyn käyttötarkoitukseen ja -ympäristöön.

2 VERKONHALLINTA

Verkonhallinta on laaja kokonaisuus, jota voidaan tarkastella useasta eri näkökulmasta. Tässä luvussa tarkastelun lähtökohtana on Kansainvälisen televiestintäliiton telestandardisointisektorin (ITU-T) suositus X.700 (1992). Verkonhallintaympäristölle ominaiset piirteet vaihtelevat jonkin verran sen mukaan, mihin tarkoitukseen verkkoa käytetään ja millainen yhteisö verkkoa käyttää. Tämä vaikuttaa myös verkonhallintaan käytettävien järjestelmien valintaan. Järjestelmien teknisiin ratkaisuihin liittyviä käsitteitä avataan luvun loppupuolella.

Verkonhallinnalla tarkoitetaan työkalujen ja menetelmien kokonaisuutta, jonka tarkoituksena on hallinnoida, koordinoida ja valvoa tiedonsiirtoresursseja ja -aktiviteettia. Sen tavoitteena on tukea loppukäyttäjää mahdollistamalla luotettava ja taloudellinen tiedonsiirto. Verkonhallinnan avulla tulee kyetä reagoimaan muuttuneisiin tarpeisiin tiedonsiirtoyhteyksiin ja -kapasiteettiin liittyen. Tämä edellyttää syvällistä tuntemusta hallittavasta tiedonsiirtoverkosta ja sen kautta kulkevasta tavanomaisesta verkkoliikenteen määrästä ja laadusta verkon eri osissa. (Recommendation X.700:1992, 2–3.)

2.1 Verkonhallinnan osa-alueet

ITU-T:n suosituksen X.700 (1992, 3) mukaan OSI-mallin mukaisen verkon hallinta jaetaan toiminnallisesti viiteen osa-alueeseen:

- vikojen hallintaan
- käytön hallintaan
- kokoonpanon hallintaan
- suorituskyvyn hallintaan
- turvallisuuden hallintaan.

Vika on tapahtuma, joka estää verkon normaalin toiminnan. Vikojen hallinta voidaan edelleen jakaa vian havaitsemiseen, eristämiseen ja korjaamiseen. Vikojen hallintaan liittyviä toimenpiteitä ovat virhelokien ylläpitäminen ja tutkiminen, vikailmoituksiin reagoiminen, vikojen jäljittäminen ja tunnistaminen, diagnostiikkatestien suorittaminen ja vian korjaaminen. (Recommendation X.700:1992, 4.)

Virhelokeihin tallentuu laitteen tai palvelun toimintaan liittyvät virheelliset tapahtumat. Vikailmoitus voi olla esimerkiksi valon syttyminen laitteen etupaneelissa tai verkonhallintatyökalun tuottama hälytys joko järjestelmän käyttöliittymässä tai sen välittämä viesti havaitusta viasta sähköpostiin tai puhelimeen. Vikailmoitusten ja lokitietojen perusteella vika ja sen sijainti yksilöidään. Tämän varmentamiseen voidaan käyttää joko yksittäiseen laitteeseen kuuluvia tai erillisiä diagnostiikkatyökaluja. Vian eristämiseen ja korjaamiseen on mahdollista hyödyntää laitteiden sisäisiä ominaisuuksia. (Jaakohuhta 2005, 309.)

Käytön hallinnan sijaan pitäisi täsmällisemmin käännettynä puhua laskutuksen hallinnasta. Tämä osa-alue mahdollistaa verkkoresurssien käyttöön liittyvien kustannusten yksilöimisen ja sen perusteella käyttäjien laskuttamisen. Siihen sisältyy käyttäjien tiedottaminen syntyneistä kuluista tai käytetystä resurssista sekä laskutusrajojen ja tariffien määrittäminen. Toiminta voi liittyä myös sisäiseen laskutukseen, jossa asiakkaina ovat esimerkiksi yrityksen eri osastot. Laskutusta varten kerätty tieto tarjoaa verkon ylläpitäjälle tietoa resurssien käytöstä käyttäjäryhmä- tai jopa käyttäjätasolla. Siksi tässä on käytetty termiä käytön hallinta. (Recommendation X.700:1992, 4; Jaakohuhta 2005, 310.)

Kokoonpanon hallinta käsittää verkon fyysisten ja loogisten olioiden käsittelyn ja yksilöimisen. Kokoonpanon hallinnalla kerätään verkosta sellaista tietoa, jonka perusteella voidaan alustaa, käynnistää ja poistaa olioita. Tiedon perusteella huomataan myös verkossa tapahtuvat muutokset. Yksilöiminen tapahtuu liittämällä nimet hallittaviin olioihin. (Recommendation X.700: 1992, 4; Jaakohuhta 2005, 310.)

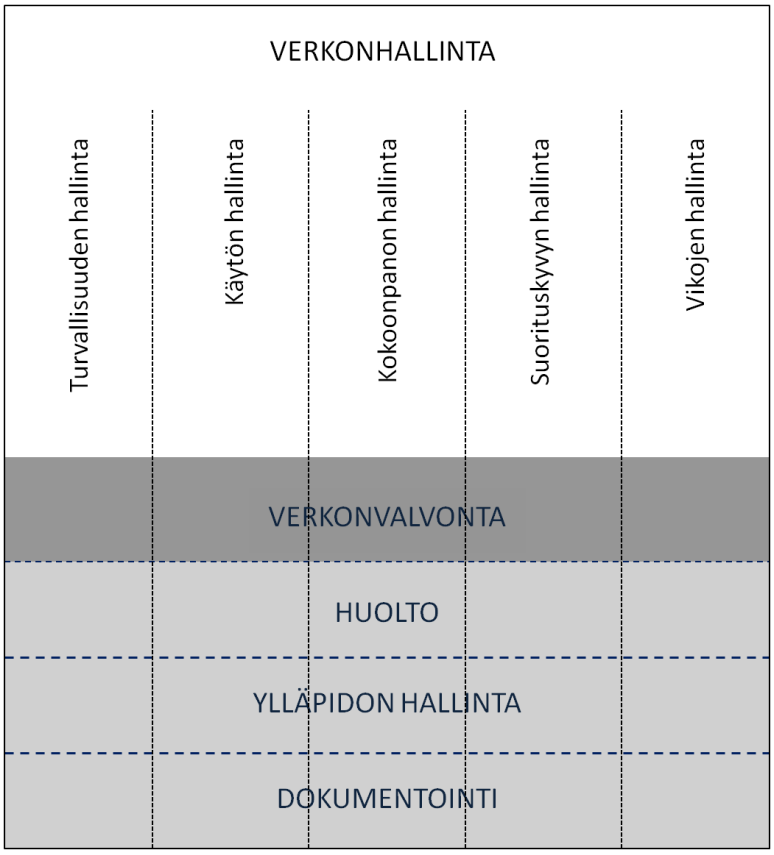
Suorituskyvyn hallinnan tarkoituksena on arvioida verkkoympäristön resurssien käyttäytymistä ja tiedonsiirron kuormitusta verkon eri osissa. Suorituskyvyn hallinnan toimenpiteisiin kuuluu tilastotiedon kerääminen, järjestelmälokien ylläpitäminen ja tutkiminen, verkon tai sen osan käyttäytymisen määrittäminen eri tilanteissa sekä verkkoasetusten säätäminen tarvittaessa. Verkon kokoonpanon muuttuessa määrittelyt tulee tehdä tarvittavilta osin uudestaan. Verkkoasetusten säätämisen osalta suorituskyvyn hallinta menee osin päällekkäin kokoonpanon hallinnan kanssa. Luonteeltaan se on kuitenkin enemmän verkon virittämistä kuin varsinaisesti kokoonpanon muokkaamista. (Recommendation X.700:1992, 4; Jaakohuhta 2005, 310.)

Turvallisuuden hallinnan tarkoituksena on tukea vallitsevia turvallisuuskäytäntöjä. Siihen kuuluu turvallisuuteen liittyvien mekanismien luominen, poistaminen ja valvonta, turvallisuuteen liittyvän informaation jakaminen sekä turvallisuuspoikkeamista raportointi. Turvallisuuden hallinnalla ei tässä yhteydessä tarkoiteta järjestelmien sisäisiä käyttäjä- ja käyttäjäryhmäkohtaisten oikeuksien määrittämistä. Turvallisuuden hallinnan painopiste on siinä, kuka tai ketkä ovat oikeutettuja käyttämään eri laitteita ja palveluita ja mistä heillä on oikeus näitä käyttää. (Recommendation X.700:1992, 4; Jaakohuhta 2005, 310.)

Jaakohuhdan mallissa (2005, 309–311) verkonhallinta on jaettu kymmeneen osa-alueeseen. Siinä politiikan hallinta, dokumentointi, raportointi, huolto ja ylläpidon hallinta on eriytetty omiksi osa-alueiksi. Politiikan hallinnalla tarkoitetaan eri palveluiden tärkeyden määrittämistä ja tärkeiden sovellusten ja palveluiden asettamista etuoikeutettuun asemaan verkkoresurssien käytössä. Dokumentointia voidaan pitää jokaisen suosituksessa X.700 (1992) esitetyn osa-alueen perustana. Kolme viimeistä osa-aluetta voidaan mieltää toimenpiteiksi, joita muiden osa-alueiden tuloksena on syntynyt.

Valvonta voidaan vastaavalla tavalla mieltää osa-alueeksi, joka liittyy kaikkiin suosituksen X.700 (1992) mukaisiin osa-alueisiin. Yhdellä valvontajärjestelyllä on mahdollista tuottaa tietoa eri osa-alueiden tarpeisiin. Verkonvalvonnalla tarkoitetaan tässä työssä laitteiden tilaan, verkon käyttöön ja verkon eri osien kuormitukseen liittyvän tiedon keräämistä, käsittelyä ja esittämistä. Siihen sisältyy myös poikkeustilanteista ilmoittaminen palauttavien toimenpiteiden käynnistämiseksi.

Kuvassa 1 on esitetty verkonhallinnan eri osa-alueet. Kuvion perustana on suosituksen X.700 (1992) mukainen jako. Kuvaa on täydennetty Jaakohuhdan mallin (2005, 309–311) käsitteillä.



Kuva 1. Verkonhallinnan osa-alueet ja niiden liittyminen toisiinsa

2.2 Verkonhallintaympäristö

Verkonhallintaympäristö on osa koko verkkoympäristöä. Se sisältää kyvyn valvoa verkkoa ja kerätä informaatiota verkosta sekä kyvyn ylläpitää tietoisuutta tiedonsiirtoresurssien tilanteesta ja raportoida siitä tarvittavalla tavalla. Verkkoympäristön yksittäisillä järjestelmillä voi olla verkonhallintaan liittyviä vastuita, kuten järjestelmän itsenäinen hallinta. Järjestelmän tulee kuitenkin toimia yhteistyössä muiden järjestelmien kanssa vähintään tiedonvaihdon osalta, jotta kokonaisverkonhallintaan liittyviä toimenpiteitä on mahdollisuus suorittaa. (Recommendation X.700:1992, 2–3.)

Verkkoympäristölle ja sen myötä verkonhallintaympäristölle asetettavat vaatimukset vaihtelevat verkonkäyttäjän mukaan. Eri ympäristöissä verkonhallinnan osa-alueet painottuvat eri tavoin. Verkonhallintaympäristön käytännön toteutukseen vaikuttavat paitsi nämä painotukset myös verkon käyttötarkoitus ja käytössä olevat resurssit. Taulukossa 1 verkonkäyttäjät on jaoteltu karkeasti viiteen ryhmään. Taulukossa on yleistäen arvioitu, miten eri resursseihin ja toiminnan luonteeseen liittyvät tekijät painottuvat kunkin ryhmän osalta.

Taulukko 1. Verkonkäyttäjien resurssien ja tarpeiden arviointi käyttäjäryhmittäin

Ominaisuus	Yksityis-käyttö	Pien-yritys	Suur-yritys	Julkinen sektori	Opetus-käyttö
keskeytymätön toiminta	ei tärkeä	kriittinen	kriittinen	tärkeä	melko tärkeä
oma osaaminen	kyllä	ei	kyllä	kyllä	kyllä
järjestelmän käyttäjäkohtainen muokkaaminen	mahdol-linen	ei	mahdol-linen	mahdol-linen	mahdol-linen
tukipalvelun tarve	ei	kyllä	kyllä	kyllä	ei
hankinta- ja ylläpitokustannukset	kriittinen	kriittinen	tärkeä	tärkeä	kriittinen

Yksityiskäytöllä tarkoitetaan tässä harrastustoimintaa, jolla ei ole kaupallisia tarkoitusperiä. Verkon vikaantuminen tai palveluiden käytön estyminen ei aiheuta taloudellisia tappioita. Käyttäjällä on lähtökohtaisesti aiempaa osaamista tietojärjestelmistä ja tietoliikenteestä. Järjestelmien muokkaamiselle juuri kyseistä verkkoa varten ei välttämättä ole tarvetta, mutta järjestelmien perehtymiseen liittyen voi löytyä kiinnostusta niiden jatkokehittämiselle. Erilliselle tukipalvelulle ei ole tarvetta, koska apua ongelmatilanteisiin löytyy Internetistä lukuisilta foorumeilta. Koska kyseessä on harrastustoiminta, hankinta- ja ylläpitokustannukset halutaan pitää mahdollisimman alhaisina.

Yritystoiminta on jaettu kahteen ryhmään. Pienyritysten koko liiketoiminta voi olla riippuvainen verkon toiminnasta ja sen vikaantuminen voi tuottaa merkittäviä taloudellisia tappioita. Näissä yrityksissä ei välttämättä ole omaa verkonhallintahenkilöstöä eikä tietotaitoa verkonhallintaan. Useimmiten käytetään valmiita ratkaisuja, joissa käyttäjän vastuulla olevien toimenpiteiden tarve on mahdollisimman vähäinen. Pelkkä Internet-foorumien tarjoama tuki ei riitä, vaan asiantuntija-apua on oltava tarvittaessa saatavissa. Koko verkon ylläpito on mahdollisesti ulkoistettu. Yrityksellä ei välttämättä ole mahdollisuutta panostaa merkittävästi ydinliiketoiminnan ulkopuolisiin osa-alueisiin, joten valitun ratkaisun tulisi olla mahdollisimman edullinen.

Suuryrityksen toiminta on usein jakautunut useisiin toimipisteisiin jopa ympäri maailmaa ja sen verkkoympäristö pitää sisällään lukuisia verkkosegmenttejä ja tärkeimmät yhteydet on varmennettu. Siksi on epätodennäköistä, että koko verkon toiminta estyisi kerrallaan. Tärkeimpien palveluiden toimimattomuus voi kuitenkin aiheuttaa katkoksia tuotantoon ja tuottaa merkittäviä taloudellisia tappioita. Suuryrityksillä on useimmiten oma tekninen tuki verkonhallintaan, vaikka osa toiminnoista olisikin ulkoistettu. Yrityksen verkossa voi olla toteutettuna joitakin erityisratkaisuja. Siksi on mahdollista, että verkonhallintajärjestelmääkin joudutaan muokkaamaan näiden ratkaisujen mukaisesti. Jotta tietoverkosta johtuvat tuotantokatkokset jäisivät mahdollisimman vähäisiksi, yrityksellä on hankalimmissa ongelmatilanteissa tarve ulkopuoliseen asiantuntija-apuun omasta osaamisesta huolimatta. Kokonaisratkaisun tuleekin olla mahdollisimman edullinen, mutta verkon keskeytyksettömään toimintaan ollaan valmiita panostamaan.

Julkisen sektorin toimijoille verkon toimimattomuudesta aiheutuvat palvelukatkokset ovat kiusallisia, mutta ne eivät yleensä aiheuta merkittäviä taloudellisia tappioita. Nämä toimijat ovat usein suuryrityksen kaltaisia verkkoratkaisujen ja resurssien osalta. Julkisen sektorin tekemät hankinnat ovat kuitenkin tiukasti säädeltyjä. Siksi hankinta- ja ylläpitokustannukset ovat yksi merkittävin hankintoihin vaikuttava tekijä.

Tietotekniikan koulutusta antavien oppilaitosten opetuskäyttöön tarkoitetut verkkoympäristöt asettuvat yksityiskäytön ja julkisen sektorin väliin. Verkon keskeytyksetön toiminta on keskeinen tekijä opetustavoitteiden täyttymisen kannalta, mutta tavoitteisiin on mahdollista päästä vaihtoehtoisilla ratkaisuilla. Verkkoa ylläpitävällä henkilöstöllä on todennäköisesti vankka ammattitaito ja siinä voidaan hyödyntää myös oppilaiden osaamista. Verkon kehitystoiminta on yritysverkkoihin verrattuna mahdollisesti nopeatempoisempaa ja niihin voidaan opetustarkoituksia varten toteuttaa erityisratkaisuja. Tällöin on myös mahdollista, että verkonhallintaan käytettävää järjestelmääkin halutaan muokata täyttämään erityisratkaisujen asettamat vaatimukset. Erillistä tukipalvelua ei yleensä tarvita, vaan ratkaisuja voidaan hakea esimerkiksi opinnäytetöiden avulla. Määrärahat verkon kehittämiseen ja ylläpitoon voivat olla hyvinkin rajalliset.

2.3 Verkonhallintajärjestelmä

Verkonhallintajärjestelmällä tarkoitetaan laite- ja ohjelmistokokonaisuutta, joilla hallinnoidaan verkkoa. Käytännön verkonhallintaa voi tehdä laitteiden ja ohjelmistojen hallintaominaisuuksien avulla. Työmäärän pienentämiseksi ja verkonhallintaympäristön yhtenäistämiseksi on tarjolla tähän tarkoitettuja järjestelmiä sekä ilmaisena että maksullisena. Järjestelmien toiminta painottuu tavallisesti tiettyihin verkonhallinnan osa-alueisiin. (Recommendation X.700:1992, 4; Jaakohuhta 2005, 324.)

Verkonvalvontajärjestelmällä tarkoitetaan tässä työssä verkonhallintajärjestelmää, jonka ensisijaisena tarkoituksena on kerätä tietoa verkkolaitteiden tilasta, verkon käytöstä ja verkon eri osien liikennemääristä. Yleiskäyttöiset järjestelmät mahdollistavat useiden eri valmistajien tai eri käyt-

töjärjestelmiin perustuvien laitteiden valvonnan. Ne voivat sisältää myös joitakin menetelmiä laitteiden ja verkon tilan muuttamiseksi. Esimerkiksi vikatilanteissa voidaan järjestelmän avulla käynnistää laite tai yksittäinen liityntä uudelleen. Järjestelmän ominaisuuksia on usein mahdollista laajentaa erillisillä lisäosilla.

Työkalut voidaan jakaa lisensointitavan perusteella kahteen kategoriaan: suljettuun ja avoimeen lähdekoodiin perustuvat ohjelmistot. Suljettuun lähdekoodiin perustuvien järjestelmien lähdekoodi ei ole yleisesti saatavilla ja tutkittavissa. Näiden ohjelmistojen lisenssiehdoissa määritetään, kuinka moneen työasemaan ohjelmisto voidaan asentaa tai kuinka monta yhtäaikaista käyttäjää sovelluksella voi olla. Lopulliset kustannukset määräytyvät sen mukaan minkälaisia tukipalveluita sisällytetään hankintaan. Suljettuun lähdekoodiin perustuvien ilmaisohjelmien käyttöehdoissa voi olla lisäksi rajoituksia, jotka estävät niiden käyttämisen kaupallisiin tarkoituksiin. Ilmaissovellukset ovat usein ominaisuuksiltaan rajatumpia kuin maksulliset versiot eikä niihin välttämättä ole tarjolla tukipalveluita. Näiden tarkoituksena on mahdollistaa järjestelmään tutustuminen ennen hankintapäätöstä.

Avoimeen lähdekoodiin perustuvien vapaiden ohjelmistojen lähdekoodi on vapaasti kaikkien saatavissa ja siksi kuka tahansa voi muokata sovelluksia. GNU General Public License (GPL) on yksi yleisesti käytetty lisenssi vapaissa sovelluksissa. Se takaa lisenssin käyttäjälle mahdollisuuden muunnella ohjelmistoa ja jakaa vapaasti muunneltua ohjelmistoa. Muunneltuja ohjelmistoja jaettaessa niiden käyttäjille tulee taata samat oikeudet kuin alkuperäisen ohjelman käyttäjilläkin. Siksi muunnellun ohjelmistonkin tulee noudattaa tätä lisenssiä. Lisenssiehtojen mukaan ohjelmiston lähdekoodi on sisällytettävä sovelluspakettiin tai se on oltava muuten saatavilla. Lisenssin käyttö tarkoittaa sitä, että ohjelmistoon voi vapaasti yhdistää osia muista vastaavaa lisenssiä käyttävistä ohjelmistoista ja alkuperäisen ohjelmiston kehittämisessä voi hyödyntää siitä muunneltuja komponentteja. Lisenssiä käyttävillä ohjelmistoilla ei ole mitään takuuehtoja. (GNU General Public License 2007.)

GNU General Public Licensen käyttö ohjelmiston lisenssinä ei estä sen maksullista jakelua, kunhan lisenssiehtoja noudatetaan eli vapaus muokkaamiseen ja edelleenjakeluun säilyy. Syynä maksulliseen jakeluun voi olla halu tarjota samalla tukipalveluita kouluttamiseen ja ylläpitoon. (GNU General Public License 2007.)

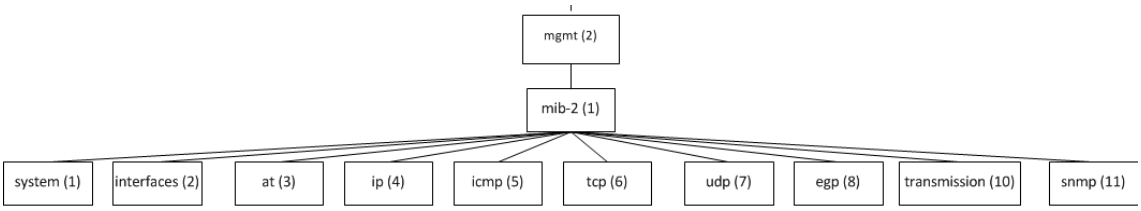
2.4 Tekniseen toteuttamiseen liittyvät käsitteet

Management Information Base (MIB), Simple Network Management Protocol (SNMP) ja Remote Monitoring (RMON) ovat verkonhallintaan keskeisesti liittyviä teknisiä käsitteitä. Ne ovat kiinteästi sidoksissa toisiinsa.

MIB on järjestelmään sisältyvien hallinnoitavien objektien ja niitä määrittävien ominaisuuksien kokoelma. Hallinnoitava objekti voi olla verkkomallin kerros, yksittäinen yhteys tai verkkolaitteen yksittäinen komponentti tai jokin abstrakti ominaisuus. (Recommendation X.700:1992, 3.) Ni-

mensä mukaisesti MIB on tietokanta, joka määrittelee hallittavien objektien hierarkkisen rakenteen. Niitä on laajuudeltaan kaksi eri versiota MIB-1 ja MIB-2. (Jaakohuhta 2005, 315).

MIB:n tietorakennetta kutsutaan nimellä Structure of Management Information (SMI). Se tarjoaa keinot sekä luoda että tunnistaa tietotyyppejä ja tiedon esitystapoja. Tietotyyppeihin kuuluu kokonaislukuarvoja, verkko-osoitteita, laskureita, mittausarvoja, aikaleimoja ja taulukoita. Objektien tunnistamisen helpottamiseksi ne nimetään tietorakenteen määrittelyjen mukaisesti. Tämän puumaisen rakenteen pääominaisuuksien määrittelystä vastaa Kansainvälinen standardoimisjärjestö (ISO). Alemman tason ominaisuuksien määrittely on muiden organisaatioiden ja laitevalmistajien vastuulla. MIB:n perusobjektiryhmät on esitetty kuvassa 2. Kuvion puurakenne alkaa yhtä tasoa ylempää esittäen sen ryhmän, johon MIB kuuluu. Muut SMI:n osat on jätetty kuviosta pois. Kunkin ryhmän perässä on sen SMI-tunniste. (Jaakohuhta 2005, 315–316.)



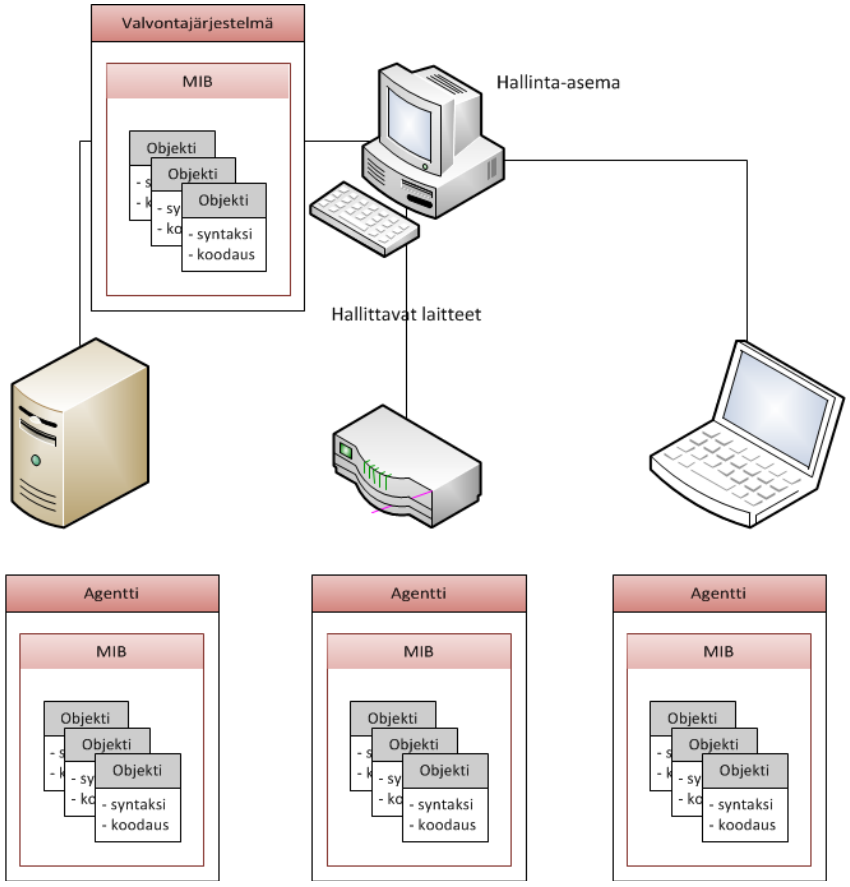
Kuva 2. MIB-2-puurakenne (Mauro & Schmidt 2001c)

System-alaryhmä kuvaa hallittavat laitteet. Siihen kuuluvia objekteja ovat muun muassa järjestelmän käynnissäoloaika ja järjestelmän nimi. Interfaces-ryhmään kuuluvat objektit tarkkailevat jokaisen verkkoliitynnän tilaa ja liikennettä. Ryhmä AT pitää sisällään osoitteenmuunnoksiin liittyvät objektit. Ryhmä on vanhentunut, mutta se on sisällytetty MIB-2:een yhteensopivuussyistä. Transmission-ryhmä sisältää tiedonsiirtomedian tunnistamiseen liittyvät objektit. Muut ryhmät pitävät sisällään kunkin protokollan mukaisen liikenteen tarkkailuun liittyvät objektit. Ryhmä, jonka tunniste on 9, ei ole enää käytössä. (Mauro & Schmidt 2001c; RFC1213:1991, 4–12.)

SNMP on laajasti käytössä oleva verkonhallintakäytäntö, joka määrittelee hallintaohjelmistojen toiminnot sekä raportin sisällön ja lähettämisen. SNMP on sovellustason protokolla. Sen ensimmäinen versio, SNMPv1 julkaistiin vuonna 1990, toinen versio, SNMPv2, on vuodelta 1993 ja viimeisimmän version, SNMPv3, julkaisuvuosi on 2002. Näistä viimeisin versio paikkaa aiempien versioiden tietoturvapuutteita (Mauro & Schmidt 2001f). Muita uusia toiminnallisuuksia siinä ei ole, vaan se tukee täysin aiempien versioiden toiminnallisuuksia. Protokolla on määritelty Internet Engineering Task Forcen (IETF) Request for Comments (RFC) -dokumenteissa. SNMP on suunniteltu valmistajariippumattomaksi protokollaksi. (Jaakohuhta 2005, 312.)

SNMP-käyttöympäristö on esitetty kuvassa 3. SNMP-tuetuissa laitteissa on agentti eli sovellus, joka kerää tietoa hallittavasta laitteesta tai sitä ympäröivästä verkosta. Agentista voidaan käyttää myös nimitystä keruuyk-

sikkö. Agentti kerää tallentamansa tiedot MIB-tiedostoon. Niille laitteille, joista SNMP-tuki puuttuu, on käytettävissä välityspalvelinagentti eli erillinen SNMP-tuen ja agentin sisältävä laite. Agenttien keräämä tieto välitetään hallinta-asemalle SNMP-muodossa UDP-tietosähkeinä. Kerätyn tiedon käsittelemiseksi hallinta-asemaan on oltava asennettuna valvontasovellus, jossa on SNMP-tuki. (Jaakohuhta 2005, 312–313; STD62 (RFC3411):2002, 4.)



Kuva 3. SNMP-käyttöympäristö (Hakala & Vainio 2002, 270; Jaakohuhta 2005, 313)

Hallinta-aseman ja agenttien välinen viestintä tapahtuu kysely-vaste-periaatteella (poll). Näiden viestien lähettämiseksi ja vastaanottamiseksi käytetään hallinta-aseman porttia 161. Hallinta-asemalta voidaan muuttaa laitteiden hallintaparametrien arvoja ja tilaa. Parametreille voidaan määritellä kynnysarvo, jonka ylitys tai alitus aiheuttaa hälytyksen. Tällöin laitteessa toimiva agentti lähettää sanoman (trap) kynnysarvon ylittämisestä tai alittamisesta ilman erillistä kyselyä hallinta-asemalle MIB-moduulissa määriteltyjen tapahtumatietojen mukaisesti. Nämä viestit käyttävät hallinta-aseman porttia 162. Hälytyksen voi aiheuttaa esimerkiksi liian suuri liikennemäärä tai tietyn yhteysvälin katkeaminen. SNMP-operaatiot on esitetty taulukossa 2. (Jaakohuhta 2005, 314; Mauro & Schmidt 2001a.)

Taulukko 2. SNMP-operaatiot (Mauro & Schmidt 2001d; STD62 (RFC3416):2002, 6)

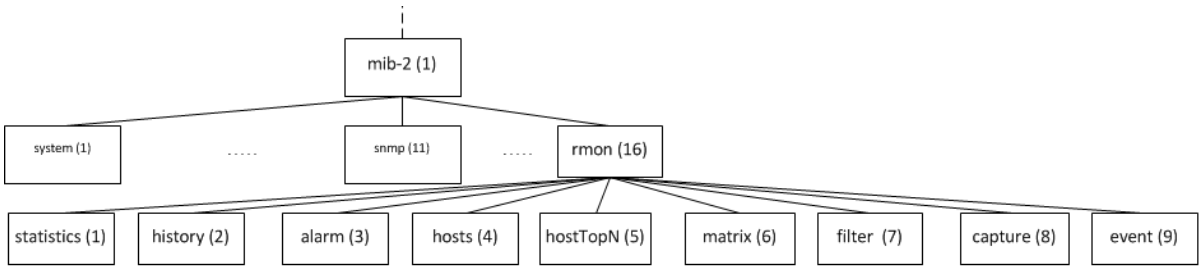
Operaatio	Käyttötarkoitus
GetRequest	Hallinta-aseman kysely agentille halutun muuttujan arvosta
GetNextRequest	Hallinta-aseman kysely agentille usean muuttujan arvosta kerrallaan
GetBulkRequest (SNMPv2)	Hallinta-aseman kysely agentille taulukkomuuttujien arvosta kerrallaan
SetRequest	Hallinta-aseman pyyntö agentille hallinnoitavan objektin arvon muuttamisesta tai uuden objektin luomisesta
Response	Agentin vastaus hallinta-aseman kyselyyn
SNMPv2-Trap (SNMPv2)	Agentin ilmoitus hallinta-asemalle kynnysarvon ylittymisestä
Notification (SNMPv2)	SNMPv1 trap-viestien yhteensovittamiseen tarkoitettu operaatio
InformRequest (SNMPv2)	Hallinta-asemien väliseen kommunikointiin tarkoitettu operaatio
Report (SNMPv2)	Pääosin SNMP-viestien prosessointiin liittyvien ongelmien ilmoittamiseen SNMP-laitteiden välillä

Operaatioihin liittyy lisäksi lisämääreitä, joilla määritellään esimerkiksi kyselyiden osalta, mistä objektista on kyse. Response-operaatioon liittyy 18 virheilmoitusta, joilla kerrotaan mistä syystä pyydettyä arvoa ei välitetty tai haluttua muutosta ei tehty. SNMPv1:n trap-viestin rakenne poikkesi get- ja set-viesteistä. SNMPv2:ssa viestin rakenne muutettiin vastaavaksi kuin get- ja set-viesteissä. Notification-operaatiolla muunnetaan SNMPv1:n trap-viestit vastaamaan muiden viestien rakennetta. Inform-operaatiota voidaan käyttää myös hälytysten välittämiseen agentilta hallinta-asemalle. Tällöin agentti saa kuittauksen hälytyksen perillemenosta. Report-operaatio määriteltiin SNMPv2:n luonnoksessa, mutta se otettiin käyttöön vasta SNMPv3:ssa. (Mauro & Schmidt 2001d.)

SNMPv1 ja SNMPv2 määrittävät hallintaoikeuksia yhteisöjen avulla. Niitä on kolmea eri tyyppiä: vain luku, luku ja kirjoitus sekä trap. Vain luku -yhteisö antaa nimensä mukaisesti oikeuden lukea tietueiden arvoja, mutta se ei mahdollista tietojen muokkaamista. Luku ja kirjoitus -yhteisö sallii edellä mainitun lisäksi muokata tietoja, kuten nollata laskureita ja jopa muuttaa laitteen asetuksia. Trap-yhteisö sallii trap-viestien vastaanottamisen. Yhteisöjen nimeämisessä ja nimien käsittelyssä on huomioitava, että yhteisön nimi on käytännössä salasana. Siksi uutta laitetta käyttöönotettaessa tulee huomioida, että oletusnimet on syytä vaihtaa ennen laitteen liittämistä tuotantoverkkoon. (Mauro & Schmidt 2001b.)

Vaikka SNMP-viestit itsessään kuormittavat verkkoa vain vähän, SNMP-liikennettä syntyy melko paljon. Hallinta-aseman on jatkuvasti lähetettävä kyselyitä agenteille verkon toiminnan seuraamiseksi. Kerätyt tiedot on siirrettävä historiakantaan, jotta ne ovat käytettävissä analyyseihin. Tämä aiheuttaa hallinta-aseman kuormittumista. (Jaakohuhta 2005, 314.)

RMON on vuonna 1995 kehitetty MIB:n laajennus, jonka tarkoituksena on vähentää verkonhallinnan synnyttämää kuormitusta. RMON:a käytettäessä hallinta-asema tutkii agentteja vasta, kun niillä on jotakin kerrottavaa. RMON mahdollistaa historiaan perustuvan tilastollisen tiedon keräämisen verkkosegmenteissä agenttien avulla. Vaikka yhteys agentin ja hallinta-aseman välillä katkeaisikin, agentti pystyy keräämään tilastotietoa ja tallentamaan sen myöhempää lähetystä varten. Kuvassa 4 on esitetty laajennuksen puurakenne yhdeksän RMON1:n määrittämän alaryhmän osalta. (Jaakohuhta 2005, 314–319; RFC4502:2006, 2–3.)



Kuva 4. RMON1-puurakenne (Jaakohuhta 2005, 318)

Statistics-ryhmä kerää tilastotietoa, kuten kehyksiin liittyvää tietoa, Ethernetistä. History-ryhmään kuuluu tapahtumahistorian keräämiseen liittyviä objekteja. Alarm-ryhmä seuraa laskureita muodostaen niistä hälytyksiä kynnysarvojen ylittyessä. Tämä ryhmä ei toimi ilman Filter- ja Event-ryhmiä. Hosts-ryhmän objektit liittyvät lähiverkossa olevien laitteiden tietojen keräämiseen. Kerättävät tiedot liittyvät muun muassa MAC-osoitteisiin, kehyskokoihin ja liikennetyyppeihin. HostTopN-ryhmä kerää tietoa eniten kuormittaneista MAC-osoitteista. Mittausperusteeksi voidaan määrittää esimerkiksi pakettimäärä tai virheet. Seuraava ryhmä, Matrix, pitää sisällään objektit, jotka liittyvät MAC-osoitteiden keskinäisen liikenteen seurantaan. Filter-ryhmän objekteilla ohjataan kehysten keräystä, kun Capture-ryhmän objektien tehtävänä on kerätä kehyksiä. Event-ryhmän objekteilla ohjataan tapahtumat, jotka ylittävät hälytysrajan, joko erilliseen lokitiedostoon tai SNMP-virityksen käynnistämiseen. (Jaakohuhta 2005, 314–319; STD59 (RFC2819):2000, 4–15.) RMON2:ssa alaryhmien määrä lisääntyy kymmenellä (RFC4502:2006, 13). Näiden ryhmien sisältämien objektien avulla analysointimahdollisuudet laajenevat OSI-mallin verkko- ja sovelluskerroksiin (Mauro & Schmidt 2001e).

3 VERKONVALVONTAAN TARKOITETUT OHJELMISTOT

Tässä luvussa vertaillaan verkonvalvontaohjelmistoja luvun alussa esiteltävien kriteerien perusteella. Tämän jälkeen käydään läpi keskeisiä havaintoja vertailtavista ohjelmistoista. Vertailun tulokset on kokonaisuudessaan esitetty liitteessä 1. Luvun loppupuolella esitellään testaukseen valittavien ohjelmistojen valintaan vaikuttaneet tekijät ja testattavat ohjelmistot.

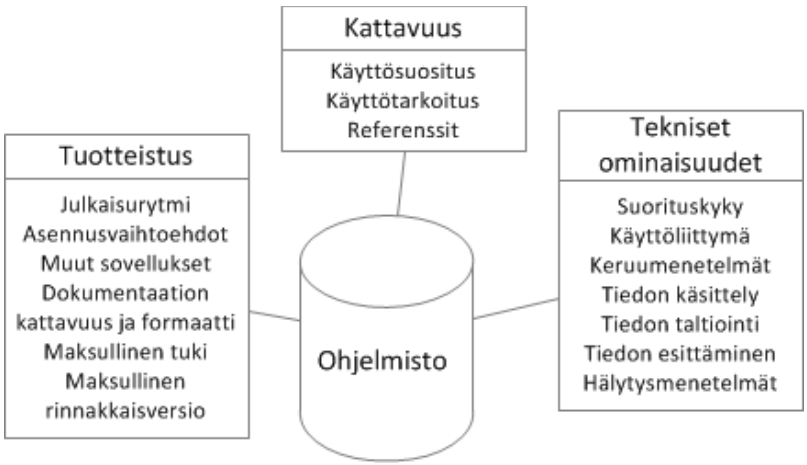
3.1 Vertailtavat ohjelmistot ja ominaisuudet

Alustavaan kartoitukseen käytettiin aiheeseen liittyviä opinnäytetöitä ja aihetta käsitteleviä sähköisiä artikkeleita. Kartoituksen perusteella vertailuun valittiin kymmenen ohjelmistoa, jotka olivat

- AlienVault OSSIM (jatkossa AlienVault)
- Cacti
- Centreon
- Nagios Core (jatkossa Nagios)
- OpenNMS
- Pandora FMS (jatkossa Pandora)
- Shinken
- Syslog-ng
- Zabbix ja
- Zenoss Core (jatkossa Zenoss).

Näistä Centreon ja Shinken perustuivat Nagiokseen. Centreon tarkoitettiin alun perin Nagioksen käyttöliittymäksi (Centreon n.d.d) ja Shinken Nagioksen ytimeksi (Shinken n.d.f). Kumpikin projekti on myöhemmin laajentunut itsenäiseksi valvontaohjelmistoksi.

Vertailtavat ominaisuudet valittiin siten, että niiden avulla on mahdollista tarkastella ohjelmistoja eri näkökulmista. Kutakin ohjelmistoa vertailtiin omana kokonaisuutenaan eikä mahdollista yhteiskäyttöä muiden ohjelmistojen kanssa huomioitu. Ominaisuudet ryhmiteltiin kuvan 5 mukaisesti kolmeen ryhmään: kattavuus, tuotteistus ja tekniset ominaisuudet.



Kuva 5. Vertailtavat ominaisuudet

Kattavuuteen liittyvien ominaisuuksien tarkoituksena oli selvittää, mihin eri käyttötarkoituksiin ohjelmisto soveltuu sekä missä yrityksissä ja yhteisöissä ohjelmisto on käytössä. Käyttösuosituksella tarkoitetaan sitä käyttötarkoitusta, minkä valmistaja ilmoitti ohjelmistolleen. Tämä käyttötarkoitus ei välttämättä noudata luvussa 2 esiteltyä verkonhallinnan jakoa. Käyttötarkoituksen tarkemmassa tarkastelussa keskityttiin sellaisiin tekijöihin, jotka liittyvät kokoonpanon, vikojen ja suorituskyvyn hallintaan sisältyvään verkonvalvontaan. Muihin osa-alueisiin liittyviä ominaisuuksia ei tässä vertailussa huomioitu. Käyttäjien osalta huomioitiin vain ne yritykset ja yhteisöt, jotka on mainittu referensseinä valmistajien ilmoittamissa tiedoissa.

Tuotteistukseen sisältyvien ominaisuuksien avulla pyrittiin selvittämään, kuinka aktiivisesti ohjelmistoa kehitetään, miten ohjelmistoon voi tutustua ja ottaa käyttöön sekä kuinka kattavasti ohjelmiston käyttäjän on mahdollisuus saada tukea sen käytössä. Julkaisurytmin avulla pyrittiin arvioimaan ohjelmistojen kehitystahtia. Liian tiheä julkaisurytmi voi aiheuttaa sen, että uusia toiminnallisuuksia ei ole ehditty riittävästi testata. Huonosti toimiva ohjelmistoversio voi itsessään aiheuttaa verkon käytettävyyden alenemista. Liian harvaan julkaisurytmiin voi olla syynä esimerkiksi riittämättömät resurssit ohjelmiston kehityksessä. Harva julkaisurytmi voi aiheuttaa sen, että ohjelmisto jää jälkeen käyttäjän tietoverkon yleisestä kehityksestä, eikä vastaa enää sille asetettuja vaatimuksia. Näiden oletusten pohjalta optimitilanteena pidettiin yhdestä kahteen uutta versiota vuodessa. Uusilla versioilla tässä tarkoitetaan sellaisia julkaisuja, joihin sisältyi virheiden korjausten lisäksi jotakin uutta toiminnallisuutta.

Parhaimmillaan ohjelmistoon voi tutustua testiympäristössä, johon on pääsy valmistajan sivuilta. Toisaalta tutustumista helpottaa valmiiksi rakennetut virtuaalikoneet. Jälkimmäisessä tapauksessa testiympäristö on oltava käyttäjällä itsellään valmiina. Asennusvaihtoehdoissa ei erikseen mainita asentamista lähdekoodista. Ohjelmistoissa käytetyn lisenssin vuoksi se on kaikkiin saatavilla. Agenttien ja muiden lisäosien asentamisvaihtoehtoja ei ole otettu huomioon. Perusohjelmiston osalta lähtökohtana oli, että asennusalustan käyttöjärjestelmänä olisi jokin Linux-jakelu. Lisäksi selvitettiin tarvitseeko ohjelmisto toimiakseen muita ohjelmia asennuspakettiin sisältyvien lisäksi.

Ensisijaisena tukena ohjelmiston käyttäjällä on usein siihen liittyvä dokumentaatio. Keskeisimpinä asioina dokumentaatiossa pidettiin jonkinlaista järjestelmäkuvausta, ohjelmiston asettamia vaatimuksia alustan kokoonpanolle ja muiden ohjelmien käytölle, asennusohjeita sekä ohjeita perusasetusten tekemiselle. Järjestelmäkuvaus auttaa ohjelmiston käyttäjää hahmottamaan sen toimintaperiaatteen ja ymmärtämään mahdolliset rajoitukset sen käytölle. Alustan suorituskykyvaatimukset ja tarvittavat muut ohjelmat on tiedettävä, jotta ohjelmistoa voi ylipäänsä käyttää tehokkaasti.

Asennus- ja käyttöohjeiden avulla ohjelmiston käyttäjä pystyy saattamaan ohjelmiston käyttökuntoon. Syvällisempään perehtymiseen ja asetuksien muokkaamiseen käyttäjillä on lähtökohtaisesti mahdollisuus hakea tietoa kehittäjäyhteisön keskustelupalstalta. Tätä vaihtoehtoa ei ole vertailussa

erikseen huomioitu. Vertailussa huomioitiin myös onko dokumentointi saatavilla erikseen ladattavana pdf-tiedostona vai ainoastaan online-muodossa.

Ohjelmiston käyttöä voidaan tehostaa valmistajan tai sen yhteistyökumppaneiden tarjoamalla koulutuksella tai ylläpitoon liittyvällä tuella. Tämä maksullisen tuen mahdollisuus osoittaa osaltaan valmistajan sitoutumista ohjelmistoon. Lisäominaisuuksia vaativille käyttäjille voi olla tarjolla maksullinen rinnakkaisversio, joka tarjoaa mahdollisesti ohjelmiston käyttöä helpottavia ratkaisuja, kuten eri lisäosien parempaa integrointia, sekä uusia toiminnallisuuksia esimerkiksi hajautetun verkon valvontaan. Vaikka vertailun kohteena olivatkin vapaat ohjelmistot, maksulliset palvelut ja rinnakkaiset ohjelmistot mahdollistavat lahjoitusvaroja vakaamman tulonlähteen vapaiden ohjelmistojen tuotekehitykseen. Siksi myös maksullisen tuen mahdollisuutta ja rinnakkaisen maksullisen ohjelmiston olemassa oloa tutkittiin vertailussa.

Teknisiä ominaisuuksia vertailemalla pyrittiin selvittämään ohjelmistojen toiminnallisia eroja. Suorituskyvyllä tarkoitetaan tiedon käsittelynopeutta joko bitteinä tai tapahtumina aikayksikköä kohden. Ohjelmiston käytettävyyttä parantavana tekijänä nähtiin selainpohjaisen käyttöliittymän olemassaolo. Tiedonkeruuseen on mahdollista käyttää kohdejärjestelmiin asennettavia ohjelmallisia agentteja tai eri protokollien ominaisuuksia eli agentitonta tapaa. Vaikka SNMP käyttääkin agentteja tiedonkeruuseen, useimpiin laitteisiin on sellainen integroitu valmiiksi, eikä erillisiä asennuksia edellytetä. Siksi SNMP huomioitiin vertailussa omana menetelmänään. Verkkoon asennettavia valvontaan tarkoitettuja fyysisiä lisälaitteita ei tässä vertailussa huomioitu.

Kerätyn tiedon käsittelyn ja taltioinnin osalta selvitettiin, miten eri ohjelmistot käsittelevät keräämiään lokeja ja tapahtumia ennen analysointia ja esittämistä. Keskeisiä tiedon käsittelyyn liittyviä termejä ovat korrelointi ja normalisointi. Korreloinnilla tutkitaan tapahtumien välisiä riippuvuuksia, kun taas normalisoinnilla ehkäistään saman tiedon tallentaminen kahteen kertaan eli poistetaan päällekkäiset tapahtumat. Tallentamisen osalta selvitettiin tallennetaanko tiedot tietokantaan vai tavallisiin tiedostoihin.

Tiedon esittämiseen ja raportointiin liittyen vertailtiin kuinka ohjelmiston keräämä ja prosessoima tieto on käyttäjien käytettävissä. Vertailussa huomioitiin paitsi tilastollisen tiedon esittäminen myös tiedon esittäminen erilaisten graafien ja verkkokartan avulla. Esitetyn tiedon ja raportoinnin käytettävyyttä lisäävinä tekijöinä nähtiin mahdollisuutta niiden tallentamiseen muidenkin ohjelmien ymmärtämässä muodossa sekä ohjelmistoon liittyvä vikailmoitustenhallinta- eli tikettijärjestelmä, jonka avulla voidaan seurata ohjelmiston tuottamille ilmoituksille suoritettuja toimenpiteitä. Ulkoisiin viestimiin, kuten sähköpostiin tai puhelimeen, ohjatut hälytykset poikkeavista tapahtumista parantavat ohjelmiston käytettävyyttä.

3.2 Kattavuus

Valmistajat esittelivät ohjelmiston käyttötarkoitusta monin eri ilmaisuin. Niissä painotettiin esimerkiksi ohjelmiston skaalautuvuutta, kokonaisvaltaista valvontaa tai liiketoimintalähtöistä lähestymistapaa. Useimpien vertailuun valittujen ohjelmistojen kohdalla käyttötarkoitukseksi mainittiin eri ilmaisuista huolimatta yleisesti verkonvalvonta.

Kolme ohjelmistoa erosi käyttötarkoitukseltaan muista. Syslog-ng oli käyttötarkoitukseltaan suppein. Se oli tarkoitettu pelkästään lokitietojen käsittelyyn osana laajempaa verkonvalvontakokonaisuutta. Cacti oli monipuolisuudeltaan samalla tasolla muiden kanssa. Sen pääasiallinen tarkoitus oli esittää kerättyä tietoa visualisesti graafeina. AlienVault poikkesi käyttötarkoitukseltaan selvimmin muista vertailun ohjelmistoista. Se oli mahdollisten verkkohyökkäysten ja luvattomien tunkeutumisyritysten havaitsemiseen ja estämiseen tarkoitettu työkalu. Käyttötarkoituksestaan huolimatta siinä oli myös verkon ja verkkolaitteiden valvontaan tarvittavia ominaisuuksia. (AlienVault LC 2012a; The Cacti Group n.d.a; The syslog-ng Open Source Edition 3.3 Administrator Guide 2012, 1).

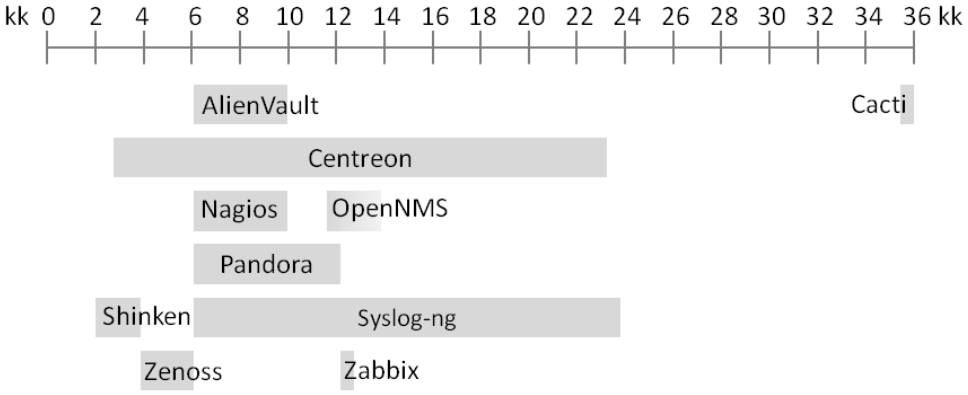
Kuva 6. Ohjelmistojen kattavuus

Kuvassa 6 on esitetty tarkemmin käyttötarkoitukseen liittyvien ominaisuuksien sisältymistä eri ohjelmistoihin. Puolet ohjelmistoista oli sellaisia, että niihin sisältyivät kaikki vertailtavat käyttötarkoitukseen liittyvät ominaisuudet. Cactin, Centreonin ja Nagioksen ainoana puutteena oli laitteiden automaattiseen tunnistamisen puute. Vaikka Pandoraan periaatteessa sisältyikin kaikki tarkastellut ominaisuudet, ohjekirjan mukaan sitä ei ollut varsinaisesti tarkoitettu lokien keräykseen ja käsittelyyn eikä tapahtumien analysointiin. Syslog-ng ei suppean käyttötarkoituksensa lisäksi sisältänyt muita tarkasteltuja ominaisuuksia. (AlienVault LC 2012a; Lorenzo n.d.b, 2–3; Cacti Group n.d.e; Berry, Roman, Adams, Pasnak, Conner, Scheck & Braun 2010, 12; Centreon n.d.c; Nagios Core Version 3.x Documentation 2010, 4; OpenNMS Group 2011a; Pandora FMS Administrator's guide v4.0 2011, 18–19; Shinken n.d.c; The syslog-ng Open Source Edition 3.3 Administrator Guide 2012, 1; Zabbix SIA 2012; Zenoss Administration 2010, 1–4.)

Referenssien osalta ohjelmistot voitiin jakaa kolmeen ryhmään. Ensimmäiseen ryhmään kuuluivat AlienVault, Centreon, Nagios, OpenNMS, syslog-ng ja Zenoss. Näiden valmistajat joko mainitsivat ohjelmistoaan käyttävät yritykset ja yhteisöt tai esittelivät niitä hieman kattavammin. (AlienVault LC n.d.c; Centreon n.d.e; Nagios Enterprises LLC n.d.a; OpenNMS Group n.d.a; The syslog-ng Open Source Edition 3.3 Administrator Guide 2012, 2; Zenoss Inc n.d.e.) Seuraavaan ryhmään kuuluivat Pandora ja Zabbix, joiden kotisivuilla mainittiin käyttäjistä vain ylimalkaisesti. Yksittäisiä käyttäjiä ei ollut nimetty, vaan referenssinä käytettiin ohjelmiston latausten määrää. (Pandora FMS n.d.e; Zabbix SIA 2012.) Kolmanteen ryhmään kuuluneet Cacti ja Shinken eivät tarjonneet minkäänlaisia referenssejä käyttäjistä. Koska vertailun kohteena olivat vapaat ohjelmistot, valmistajan voi olla lähes mahdoton tietää ohjelmistonsa käyttäjiä. Referenssien ilmoittaminen korreloi seuraavassa alaluvussa käsiteltävän maksullisen tuen mahdollisuuden kanssa.

3.3 Tuotetuki

Ohjelmistojen uusien versioiden julkaisuvälin määrittäminen lähdeaineiston perusteella ei ollut täysin yksiselitteistä. Joillakin ohjelmistoilla uusia versioita on ilmestynyt varsin usein, mutta kyseisten ohjelmistojen kohdalle ainakin osa niistä oli ainoastaan virheenkorjaukseen liittyviä päivityksiä. Kuvassa 7 on esitetty arvio ohjelmistojen kehitystahdista niiden eri versioiden julkaisuajankohtien perusteella. Joidenkin ohjelmien kohdalla vaihteluväli oli edellä mainitusta syystä melko suuri. Nopein julkaisutahti on ollut Shinkenillä ja Zenossilla. Uusia versioita on julkaistu muutaman kuukauden välein. Toista ääripäätä edustaa Cacti, jonka uutta versiota on saanut odotella mahdollisesti jopa kolmen vuoden ajan. (AlienVault LC 2012c; The Cacti Group. n.d.d; Centreon n.d.g; Sourceforge 2012a; Sourceforge 2012b; Sourceforge 2012c; Sourceforge n.d; Shinken n.d.d; BalaBit IT Security Ltd n.d.e; Zabbix SIA n.d.c.)



Kuva 7. Ohjelmistojen uusien versioiden julkaisuväli

Centreonille, OpenNMS:lle, Pandoralle ja Shinkenille oli tarjolla kaikille avoin testiympäristö, johon pääsi tutustumaan valmistajan kotisivuilta. Ne tarjosivat ensivaikutelman ohjelmiston käyttöliittymästä ja toimintaperiaatteesta. Niiden avulla sai melko hyvän käsityksen, millaisia tiedon esitystapoja ohjelmistoon sisältyy. Niiden perusteella ei kuitenkaan saanut

kunnollista käsitystä ohjelmiston asetuksien säätämisestä ja niiden vaikutuksesta ohjelmiston toimintaan. (Centreon n.d.k; OpenNMS Group n.d.d; Pandora FMS n.d.b; Shinken n.d.h.)

Ohjelmistoihin oli tarjolla vaihteleva määrä asennusvaihtoehtoja lähdekoodista asentamisen lisäksi. Parhaimmillaan niille oli tarjolla käyttövalmis virtuaalikone. Toista ääripäätä edusti ainoastaan itse ohjelmiston sisältävä sovelluspaketti, jonka lisäksi oli asennettava muita ohjelmia. AlienVault poikkesi asennusvaihtoehdoiltaan muista. Ainoa vaihtoehto lähdekoodin lisäksi oli iso-tiedosto. Se sisälsi ohjelmiston lisäksi myös käyttöjärjestelmän, joka asentui aina ohjelmiston yhteydessä. (AlienVault LC 2012c.) Kaikki ohjelmistot tarvitsivat toimiakseen muita ohjelmia. Yleisimmin tarvittiin jokin tietokantaohjelma. Ainoastaan Nagios ja Shinken tallensivat tiedot lokitiedostoihin (Nagios Core Version 3.x Documentation 2010, 4; Shinken n.d.b). Jotkin ohjelmistoista tarvitsivat erillisen www-palvelimen ja toisissa se oli sisällytetty ohjelmistoon. Monissa tapauksissa tarvittavat ohjelmat oli sisällytetty asennuspakettiin.

Ohjelmistojen lisensointitavan ja avoimuuden vuoksi oli hieman yllättävää, että Centreonin dokumentointia ei ollut saatavissa online-muodossa. Vastaavia tietoja löytyi valmistajan Internet-sivuilta, mutta kootumpaa dokumentointia oli saatavissa vain pdf-tiedostoina. Muille ohjelmistoille oli saatavissa ainakin osittainen online-dokumentointi. Sen rinnalla tarjottiin dokumentteja pdf-tiedostoina lukuun ottamatta OpenNMS:ää ja Shinkeniä. Zabbix tarjosi pdf-dokumentteja vain vanhemmista versioista. Sen online-dokumentit oli kuitenkin saatavissa helposti tulostettavana versiona. (Centreon n.d.f; OpenNMS Group 2012a; Shinken 2012b; Zabbix SIA n.d.a.)

Dokumentaation sisältö oli pääsääntöisesti varsin kattava. Lähes kaikkien ohjelmistojen dokumentaatioon oli sisällytetty järjestelmäkuvaus, vaatimukset ohjelmiston asentamiselle, asennusohjeet ja peruskäyttöön vaadittavat asetukset. Dokumentaatioltaan suppein oli Centreon, jolle oli saatavilla ainoastaan asennusohjeet ja ohjeet perusasetuksista. Edellä mainitut dokumentit olivat tosin tarkoitettu maksulliselle Centreon Enterprise Serverille. Järjestelmäkuvauskin oli tarjolla valmistajan kotisivuilla toisaalla. Muutamien muiden ohjelmistojen dokumentointi sisälsi myös maksullisen version ominaisuuksia, mutta niistä oli selkeästi erikseen mainittu. (Centreon n.d.a; Centreon n.d.d.)

Vain Cactin ja Shinkenin käyttäjien tukena oli ainoastaan dokumentaatio ja yhteisön keskustelupalsta. Muilla ohjelmistoille oli tarjolla maksullisia tukipalveluita. Maksullista suljetun lähdekoodin versiota tarjottiin AlienVaultista, Centreonista, Nagioksesta, Pandorasta, syslog-ng:stä ja Zenossista. (AlienVault LC n.d.a; AlienVault LC n.d.b; Centreon n.d.b; Centreon n.d.j; Centreon n.d.i; Nagios Enterprises LLC n.d.d; Nagios Enterprises LLC n.d.e; OpenNMS Group n.d.b; Pandora FMS n.d.a; Pandora FMS Administrator's guide v4.0 2011, 20; BalaBit IT Security Ltd n.d.b; BalaBit IT Security Ltd n.d.e; Zabbix SIA 2012; Zenoss Inc n.d.b; Zenoss Inc n.d.d.)

3.4 Tekniset ominaisuudet

Vertailluista ohjelmistoista syslog-ng luotti komentorivipohjaiseen käyttöliittymään. Muihin ohjelmistoihin sisältyi selainpohjainen graafinen käyttöliittymä. Tosin Nagioksessa se oli valinnainen ja sitä käytettiin lähinnä tiedon esittämiseen. Siinä asetusten muokkaaminen tapahtui suoraan asetustiedostoihin komentorivin kautta. Cactissa komentoriviä käytettiin komentosarjojen muokkaamiseen. (Lorenzo n.d.b, 6; Berry ym. 2010; Centreon n.d.c; Nagios Core Version 3.x Documentation 2010, 4; OpenNMS Group 2011a; Pandora FMS Administrator's guide v4.0 2011, 27–28; Shinken n.d.c; The syslog-ng Open Source Edition 3.3 Administrator Guide 2012; Zabbix SIA 2012; Zenoss Administration 2010, 1.)

Suurin osa ohjelmistoista käytti tiedonkeruuseen useita eri menetelmiä. Valikoimaan kuuluivat niin SNMP-kyselyt ja trap-viestit, kohdelaitteeseen asennettavat agentit kuin kohdeverkossa käytettävien protokollien hyödyntäminenkin. Tästä poikkeuksen tekivät Cacti, syslog-ng ja Zenoss. Cactin kerrottiin määrittävän tietolähteet komentosarjojen avulla hyödyntäen muun muassa SNMP:tä. Zenossin korostettiin käyttävän agentitonta tiedonkeruu tapaa eli se hyödynsi SNMP:n ohella eri protokollien ominaisuuksia tiedonkeruuta varten muodostettavissa kyselyissä. Syslog-ng käytti ainoastaan kohdelaitteeseen asennettavaa agenttia lokiviestien keräämiseen ja välittämiseen. (Berry ym. 2010, 12; The syslog-ng Open Source Edition 3.3 Administrator Guide 2012, 5; Zenoss Administration 2010, 2.)

Kerätyn tiedon käsittelystä kerrottiin ohjelmistojen dokumenteissa ja kotisivuilla varsin vaihtelevasti. Joidenkin ohjelmistojen kohdalla menetelmistä ei kerrottu selkeästi. Ne ohjelmistot, joiden tiedonkeruumenetelmiä esiteltiin, käyttivät yleisimmin joko korrelointia, normalisointia tai molempia. Näiden lisäksi AlienVaultin ja syslog-ng:n ilmoitettiin käyttävän luokittelua tiedon merkittävyyden arviointiin. AlienVaultin menetelmiin sisältyi myös tarkkailtavien verkkojen profilointi. Kerätyn tiedon perusteella se loi kullekin verkkosegmentille käyttöprofiilin muun muassa liikenteen määrän ja laadun perusteella. Syslog-ng:ssä oli mahdollista jäsennellä lokitietoja eli järjestellä niiden kentät toiseen järjestykseen. Menetelmä mahdollistaa eri lähteistä kerättyjen lokitietojen yhdenmukaistamisen. (AlienVault Unified SIEM. System Description. Version 1.0 n.d.; Lorenzo n.d.b, 118; The syslog-ng Open Source Edition 3.3 Administrator Guide 2012.)

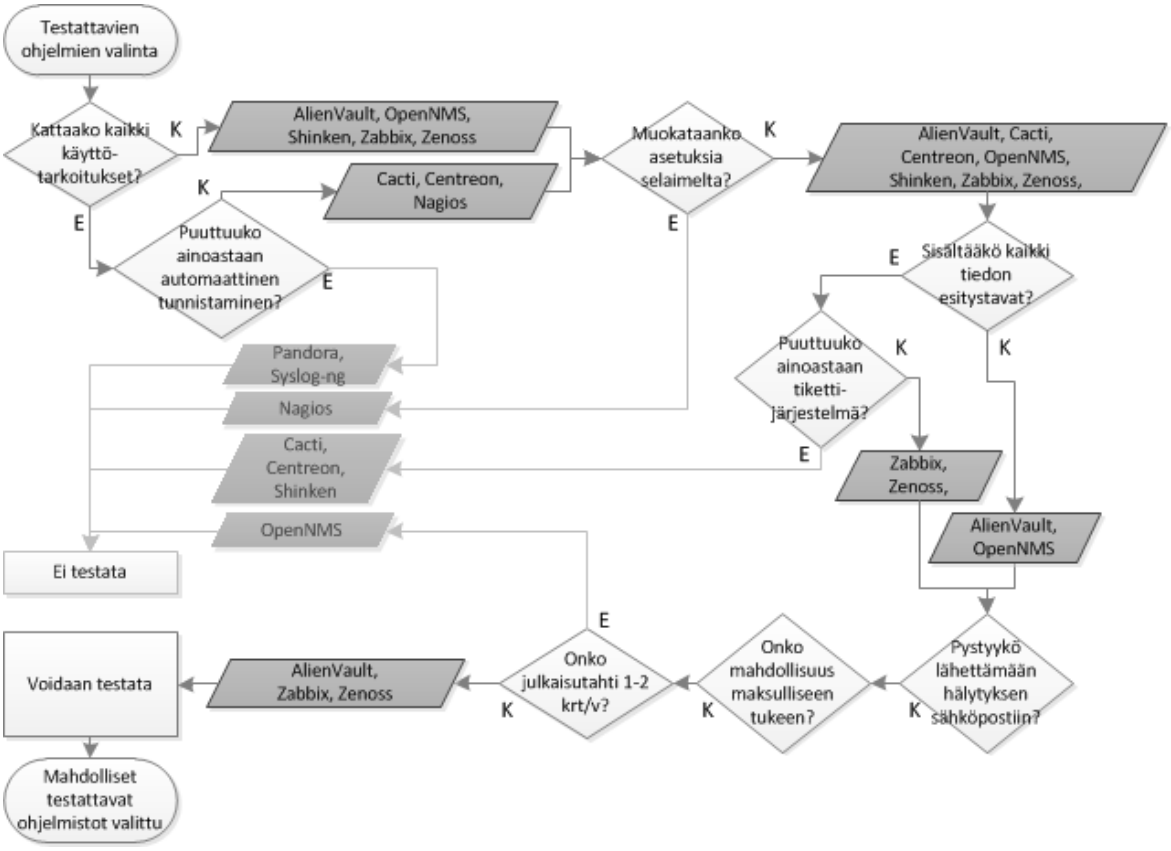
Tiedon esittämistavoiltaan suppein oli syslog-ng. Graafisen käyttöliittymän puutteen vuoksi tietoa voitiin esittää korkeintaan taulukkomuodossa. Muissa ohjelmistoissa tietoa esiteltiin taulukoiden lisäksi erilaisina graafeina ja useimmissa myös verkkokartan avulla. AlienVaultin, Centreonin ja OpenNMS:n kohdalla oli maininta tikettijärjestelmästä. Ohjelmien avoimuuden vuoksi ei ole poissuljettua, että myös muihin ohjelmistoihin voitaisiin luoda vastaava lisäosa. Kuusi ohjelmistoa mahdollisti raporttien tallentamisen erilliseen tiedostoon siirrettäväksi esimerkiksi taulukkolaskentaohjelmaan tai lähetettäväksi sähköpostin liitteenä. (AlienVault Unified SIEM. System Description. Version 1.0. n.d.; Lorenzo n.d.b; Berry ym. 2010, 44; Centreon n.d.c; Nagios Core Version 3.x Documentation 2010, 321; OpenNMS Group 2011a; Pandora FMS Administrator's guide

v4.0 2011, 11–12; Shinken n.d.g; Zabbix SIA 2012; Zenoss Administration 2010.)

Cactista ja syslog-ng:stä puuttui mahdollisuus lähettää hälytyksiä ulkoiseen viestimeen. Muiden ohjelmistojen osalta hälytys voitiin välittää ainakin sähköpostiin. Tämän lisäksi vaihtoehtoina olivat tekstiviesti, hakulaite, toiminnan määrittäminen komentosarjan avulla ja XMPP. (Lorenzo n.d.b, 127; Centreon n.d.c; Nagios Core Version 3.x Documentation 2010, 4; Nagios Enterprises LLC n.d.c; OpenNMS Group 2011a; Pandora FMS Administrator's guide v4.0 2011, 25; Shinken n.d.c; Zabbix SIA 2012; Zenoss Administration 2010, 18.) XMPP on pikaviestintään tarkoitettu avoin teknologia (XMPP Standards Foundation 2010). Hälytystapana sähköposti on varsin kattava ja mahdollistaa hälytysten vastaanottamisen myös puhelimeen. Hakulaitteen tai tekstiviestin merkitys korostuu aikakriittisissä yhteys- tai palvelukatkoksissa.

3.5 Testaukseen valitut ohjelmistot

Testaukseen haluttiin valita mahdollisimman monipuoliset ohjelmistot. Valinnassa painotettiin ohjelmiston käyttötarkoitusta, mahdollisuutta muokata asetuksia selaimella, tiedon esittämistapoja, mahdollisuutta tuottaa hälytyksiä vähintään sähköpostiin, mahdollisuutta maksulliseen tukeen ja julkaisuväliä. Kriteereitä tarkasteltiin edellä mainitussa järjestyksessä siten, että kriteerin puuttuminen aiheutti ohjelmiston jäämisen testauksen ulkopuolelle. Valintaprosessi on esitetty kuvassa 8.



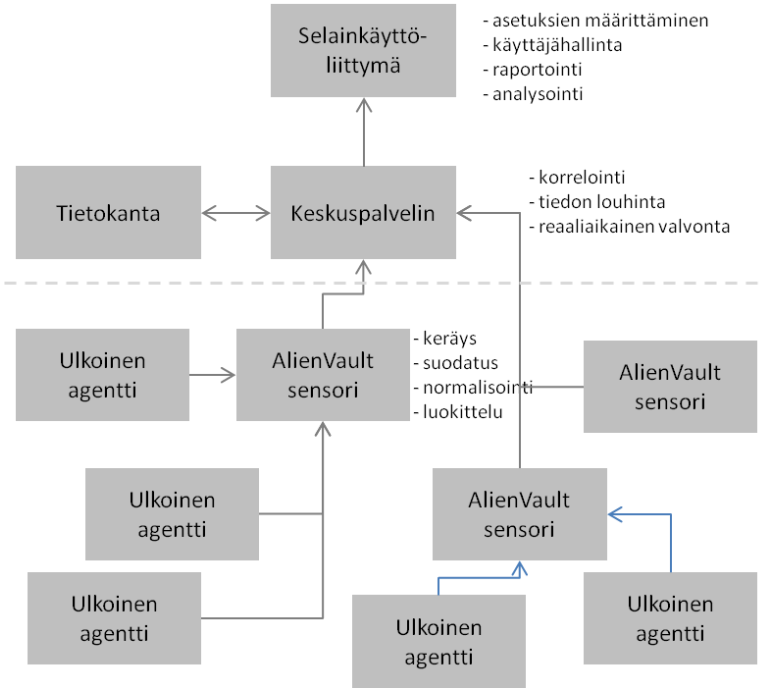
Kuva 8. Testattavien ohjelmistojen valinta

Käyttötarkoituksen osalta kohdelaitteiden automaattisen tunnistamisen puuttumista ei pidetty poissulkevana tekijänä, jos ohjelmisto kattoi kaikki muut osa-alueet. Pandoralla ja syslog-ng:llä oli useampia puutteita, joten ne pudotettiin pois. Jäljelle jääneistä Nagios pudotettiin pois selainkäyttöliittymän vuoksi, koska se on tarkoitettu lähinnä kerätyn tiedon tarkasteluun.

Ainoastaan kaksi vertailun ohjelmistoista, AlienVault ja OpenNMS, kattoivat kaikki vertailussa tarkastellut tiedon esitystavat. Kahden muun osalta puutteena oli tikettijärjestelmä. Sitä ei kuitenkaan pidetty poissulkevana tekijänä. Neljä jäljelle jäänyttä ohjelmistoa kattoivat kaksi seuraavaa kriteeriä. Viimeisen kriteerin, julkaisuvälin, kohdalla pudotettiin OpenNMS hieman liian hitaan tahdin vuoksi.

Valintaprosessin läpäisseiden ohjelmistojen erot olivat pieniä. Näistä testaukseen valittiin AlienVault ja Zenoss. AlienVaultin valintaa puolsi se, että ohjelmisto täytti valintakriteerit ilman puutteita. Zenoss valittiin, koska se ei käytä SNMP:tä lukuun ottamatta muita agentteja tiedonkeruuseen.

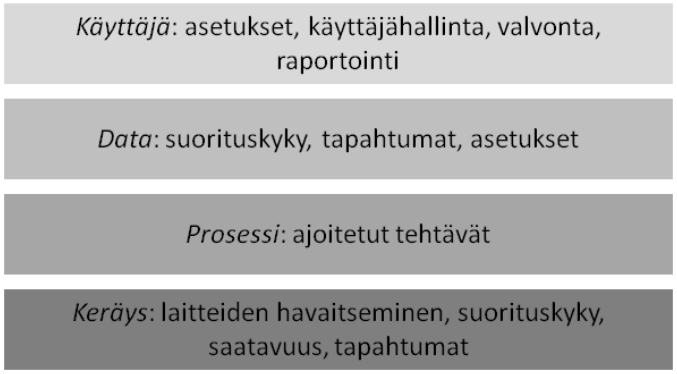
AlienVaultin toimintaperiaate on esitetty kuvassa 9. Siinä ei ole huomioitu ohjelmiston turvallisuusvalvontaan liittyviä toimintoja. AlienVaultin osakokonaisuuksiin kuuluvat sensori, agentit, keskuspalvelin, tietokanta ja selainkäyttöliittymä. Sensori on kuhunkin verkkosegmenttiin asennettava ohjelmisto. Se suodattaa, luokittelee ja normalisoi tiedon ennen kuin lähettää sen keskuspalvelimelle. Sensori sisältyy AlienVaultin asennusmediaan. Tämän lisäksi AlienVault käyttää erikseen kohdelaitteisiin asennettavia agentteja. Nämä eivät sisälly AlienVaultin asennusmediaan. Keskuspalvelin korreloi tapahtumat ja tallentaa ne tietokantaan. Selainkäyttöliittymän avulla hallinnoidaan kokonaisuutta. (Lorenzo n.d.b, 3–6.)



Kuva 9. AlienVaultin toimintaperiaate (Lorenzo n.d.b, 3–6; AlienVault Unified SIEM. System Description. Version 1.0 n.d)

AlienVaultissa on hyödynnetty tehokkaasti vapaiden ohjelmien lisenssien tarjoamia mahdollisuuksia – siihen on integroitu useita vapaita valvontatyökaluja. Sen sensoriin on sisällytetty useita tunnettuja työkaluja, joista verkon suorituskyvyn sekä laitteiden ja palveluiden tilan valvonnan osalta keskeisiä ovat ntop, OSSEC ja Nagios sekä Nfsen, Nfdump ja Fprobe -yhdistelmä. (Lorenzo n.d.a, 6, Lorenzo n.d.b, 151.)

Zenossin toimintaperiaatteena on ohjelmiston kaikkien komponenttien asentaminen samalle alustalle, koska erillisiä agentteja ei käytetä. Ohjelmiston arkkitehtuuri on esitetty kuvassa 10. Keräyskerroksen tehtävänä on kerätä tietoa sekä laitteista että itse verkosta. Tiedon keräämiseen laitteilta käytetään SNMP:tä, SSH:ta ja WMI:tä. Raakadatan normalisointiin käytetään erilaisia liitännäisiä. Verkon käytettävyyden ja suorituskyvyn seurantaan käytetään useita eri protokollia. Kerätty tieto tallennetaan RRD-tiedostoihin. Prosessikerros toimii linkkinä keräys- ja datakerroksen välillä sekä suorittaa jaksottaisia tehtäviä. Datakerroksessa tieto taltioidaan kolmella eri tavalla: RRD-tiedostoihin tallennetaan suorituskykyyn liittyviä tietoja, tapahtumat tallennetaan MySQL-tietokantaan ja kokoonpano- ja asetustiedot omaan tietokantaansa. Käyttäjäkerros esittää datakerroksen tiedot halutussa muodossa selainkäyttöliittymän avulla. (Zenoss Administration 2010, 3–4.)



Kuva 10. Zenossin arkkitehtuuri (Zenoss Administration 2010, 3–4)

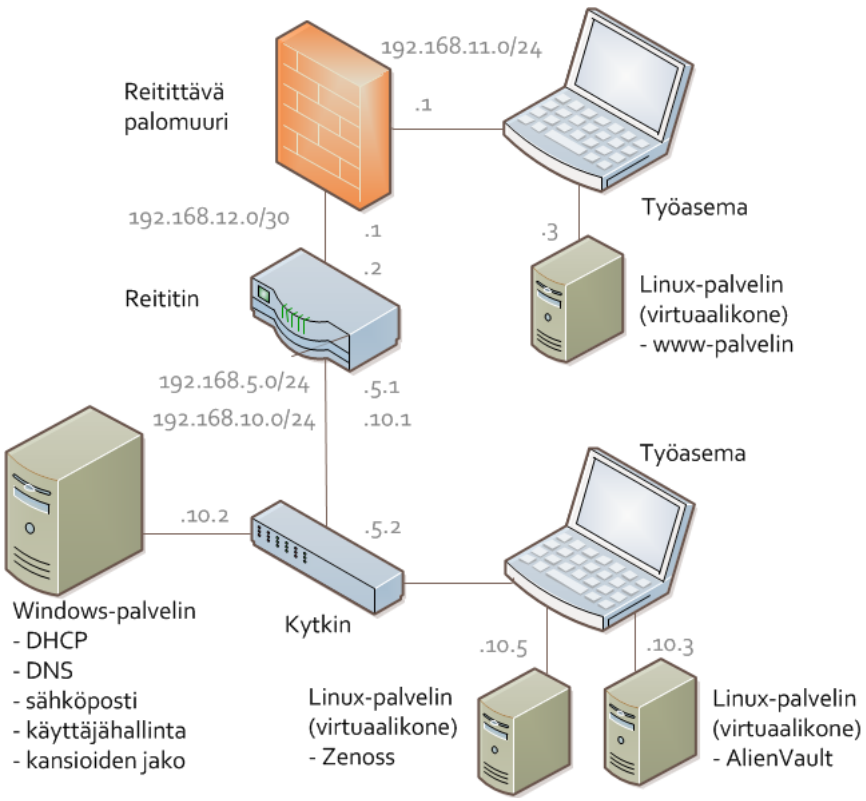
Vaikka Zenossin osalta korostetaan agentitonta keräystapaa, tähän ei kaikissa tilanteissa päästä. Windows-palvelimien osalta mainitaan, että suorituskykyyn liittyvien parametrien valvonta SNMP:llä edellyttää erillisen agentin asentamista. Samoin järjestelmälokien kerääminen Windows-palvelimelta edellyttää erillistä agenttia. (Zenoss Administration 2010, 32.)

4 OHJELMISTOJEN TESTAUS

Tässä luvussa esitellään testausjärjestelyt ja sen toteuttaminen. Ohjelmistojen testaamiseen käytettiin erillistä verkkoa, josta on kerrottu tarkemmin ensimmäisessä alaluvussa. Kummastakin ohjelmistosta käytettiin testauksen aikana viimeisintä saatavilla olevaa vakaata 64-bittistä versiota. AlienVaultista testattiin versiota 3.1 ja Zenossista versiota 3.2.1. Asentaminen ja testauksen aikaiset toimenpiteet toteutettiin mahdollisimman tarkasti ohjekirjojen mukaisesti. Keskeisimmät AlienVaultin käyttöön liittyvät ohjekirjat olivat Alienvault Installation Guide ja AlienVault Users Manual (Lorenzo n.d.a, Lorenzo n.d.b). Zenossin osalta keskeisimmät ohjekirjat olivat Zenoss Core Installation (2010), Getting Started with Zenoss (2010) ja Zenoss Administration (2010).

4.1 Testiympäristö

Ohjelmistoja testattiin kuvan 11 mukaisessa suljetussa ympäristössä. Ympäristö rakennettiin siten, että siinä oli eri valmistajien verkkolaitteita sekä eri käyttöjärjestelmällä toimivia palvelimia. Reitittävä palomuuri oli Juniperin valmistama, reititin Ciscon ja kytkin Hewlett & Packardin. Virtuaalikoneiden luomiseen käytettiin VirtualBox-virtualisointiohjelmaa.



Kuva 11. Testiympäristö

Palomuurin sisäpuolella olevaan lähiverkkoon liitettiin Windows-palvelin ja työasema. Toinen työasema sijoitettiin palomuurin ulkopuolelle ja siihen asennettiin virtuaalinen Linux-palvelin Ubuntu-käyttöjärjestelmällä. Palvelimissa otettiin käyttöön kuvassa 11 mainitut palvelut. Sähköpostipalvelin toteutettiin erillisellä käyttöjärjestelmään kuulumattomalla ohjel-

malla. Ympäristössä käytettiin yhtä toimialuetta, johon sisältyi kaksi erillistä osoitealuetta – yksi sisäverkkoon ja yksi palomuurin ulkopuolelle. Verkon aikapalvelimena käytettiin palomuuria.

4.2 Ohjelmistojen asentaminen

Kummallekin ohjelmistolle luotiin virtuaalikone. Asentaminen suoritettiin testiympäristön ulkopuolella. Asentamisen aikana oli käytössä Internet-yhteys, jotta ohjelmistot oli helppo päivittää eri komponenttien uusimmilla versioilla ennen testaamista. Asentamisen ja päivittämisen jälkeen virtuaalikoneet siirrettiin testiympäristöön sisäverkossa olleeseen työasemaan.

AlienVaultille suositellaan muistin määräksi vähintään neljä gigatavua (Lorenzo n.d.a, 10). Käytettäessä Zenossia alle 250 laitteen tarkkailuun tarvitaan valmistajan mukaan vähintään neljä gigatavua muistia ja 300 gigatavun kiintolevy (Zenoss Core Installation 2010, 1). Käytettävissä olleiden fyysisten tietokoneiden suorituskyvystä johtuen virtuaalikoneille annettiin käyttöön 1920 megatavua keskusmuistia ja 256 gigatavun kiintolevy. AlienVaultia varten luotuun koneeseen ei asennettu käyttöjärjestelmää, sillä se sisältyi ohjelmiston asennuspakettiin. Zenossia varten luotuun koneeseen asennettiin 64-bittinen Ubuntu Server -käyttöjärjestelmä.

AlienVaultin asennustavaksi valittiin automaattinen asennus. Asennusohjelma pyysi määrittämään kyseisen koneen, oletusyhdyskäytävän ja nimipalvelimen osoitetiedot sekä root-käyttäjän salasanan. Asennusvaiheessa käytettiin tilapäisiä osoitetietoja, jotka muutettiin asentamisen jälkeen vastaamaan testiympäristön osoitteita. Tämän lisäksi asennusvaiheessa määriteltiin levyn osiointi ja ohjelmiston päivittäminen. Asentaminen kesti noin puoli tuntia.

AlienVaultin asetustiedot oli koottu yhteen tekstitiedostoon. Asetuksia voitiin muuttaa komentoriviltä millä tahansa tekstieditorilla tai käyttämällä ossim-setup-komentoa. Jälkimmäinen tapa on kokemattomalle käyttäjälle turvallisempi, sillä se avaa pienen valikkopohjaisen ohjelman, jolla haluttuja asetuksia voi muuttaa. (Lorenzo n.d.a, 41.)

Tässä testissä jälkimmäisellä tavalla määritettiin valvottavat verkot, otettiin käyttöön muutamia liitännäisiä ilmaisemiseen ja valvontaan sekä päivitettiin ohjelmisto. Uusia versioita eri komponentteihin löytyi sen verran runsaasti, että asennusvaiheen aikainen päivittäminen ei todennäköisesti onnistunut. Tämän lisäksi suoraan ohjelmiston omaan asetustiedostoon täytyi muuttaa hallintaosoite ja selainohjelman osoite. Tätä ei tarvitse tehdä, jos jo asennusvaiheessa määritetään käytettävät osoitteet. Oikeat verkkoasetukset ja aikapalvelimen tiedot määritettiin käyttöjärjestelmän omiin asetustiedostoihin. Asennuksen jälkeen tehdyt asetusmuutokset on esitelty tarkemmin liitteessä 2.

Zenossin asennuspaketiksi valittiin kaikki komponentit sisältävä Debian-asennuspaketti. Asentaminen suoritettiin dpkg-komennolla. Asentaminen kesti parikymmentä minuuttia eikä sen aikana tarvinnut tehdä muita toimenpiteitä.

Asentamisen jälkeen säädettiin järjestelmää asennusohjeen mukaisesti. Näihin toimenpiteisiin sisältyivät ZEO-tietokannan pakkaaminen sekä MySQL-tietokannan ja Zope-sovelluspalvelimen säätäminen. ZEO-tietokanta tallentaa tiedot kaikista ohjelmistoilla suoritetuista toimenpiteistä. Jotta tietokanta toimisi tehokkaasti, suositellaan vanhat toimenpiteet poistettavaksi tietokannasta säännöllisesti cron-ajastuspalvelun avulla. MySQL-tietokannan suorituskyvyn parantamiseksi käytettiin ohjeessa mainittuja käytettävän muistin määrään liittyviä oletusasetuksia. (Zenoss Core Installation 2010, 28–29.)

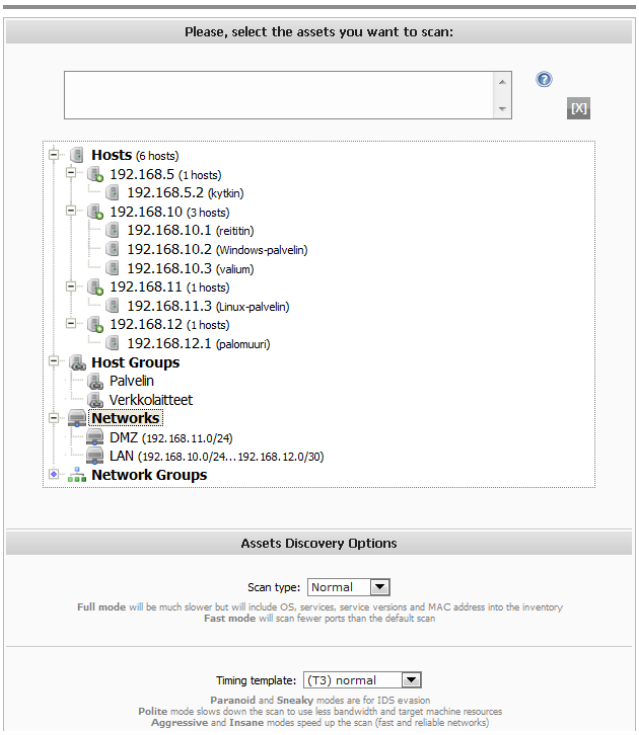
Zenossin selainkäyttöliittymä toimii Zope-sovelluspalvelimessa ja siksi palvelimen suorituskyky vaikuttaa ohjelmiston käytettävyyteen merkittävästi. Ohje suosittelee palvelimen asetuksien muokkaamista käytössä olevaan ympäristöön. Osa tarvittavista arvoista on mainittu suoraan ohjeessa ja osa arvoista on laskettava ympäristön mukaan. Näidenkin laskeminen on opastettu asennusohjeessa. Asennuksen jälkeen tehdyt asetusmuutokset on esitelty tarkemmin liitteessä 3. (Zenoss Core Installation 2010, 29–30.)

4.3 Testauksen toteutus

Testiympäristöön siirtämisen jälkeen käynnistettiin ohjelmistojen selainkäyttöliittymä ja aloitettiin asetusten muokkaaminen testiverkon valvontaan soveltuvaksi. Testaussuunnitelma on esitelty liitteessä 4.

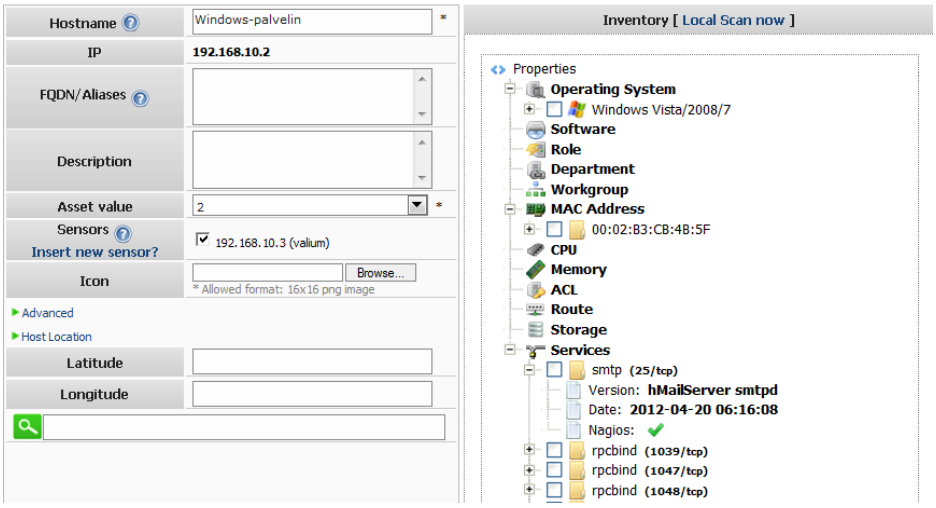
4.3.1 AlienVault

Aloitettaessa AlienVaultin käyttö määritettiin valvottavat verkot selainkäyttöliittymässä uudelleen, sillä ne eivät näkyneet verkkolistauksessa. Valvottavat laitteet oli mahdollista lisätä käsin tai etsiä hakuohjelmana käytetyn nMapin avulla. Kuvassa 12 on esitetty näkymä laitteiden etsintään käytetystä osiosta. Ohjelmisto löysi testiympäristön laitteita hakuohjelmallaan, mutta haku hidasti ohjelmistoa melko paljon. Pari kertaa koko ohjelmisto jouduttiin käynnistämään uudelleen. Hidastumisen syynä oli todennäköisesti alustana käytetyn virtuaalikoneen liian vähäinen muisti. Toiminnon kuormittavuutta pienennettiin hakemalla osa laitteista yksitellen niiden osoitteen perusteella. Tavallisia työasemia ei tässä testissä haluttu valvoa, joten ne poistettiin listalta.



Kuva 12. Näkymä AlienVaultin laitteiden etsintään käytetystä osiosta (Kuvakaappaus ohjelmiston käyttöliittymästä)

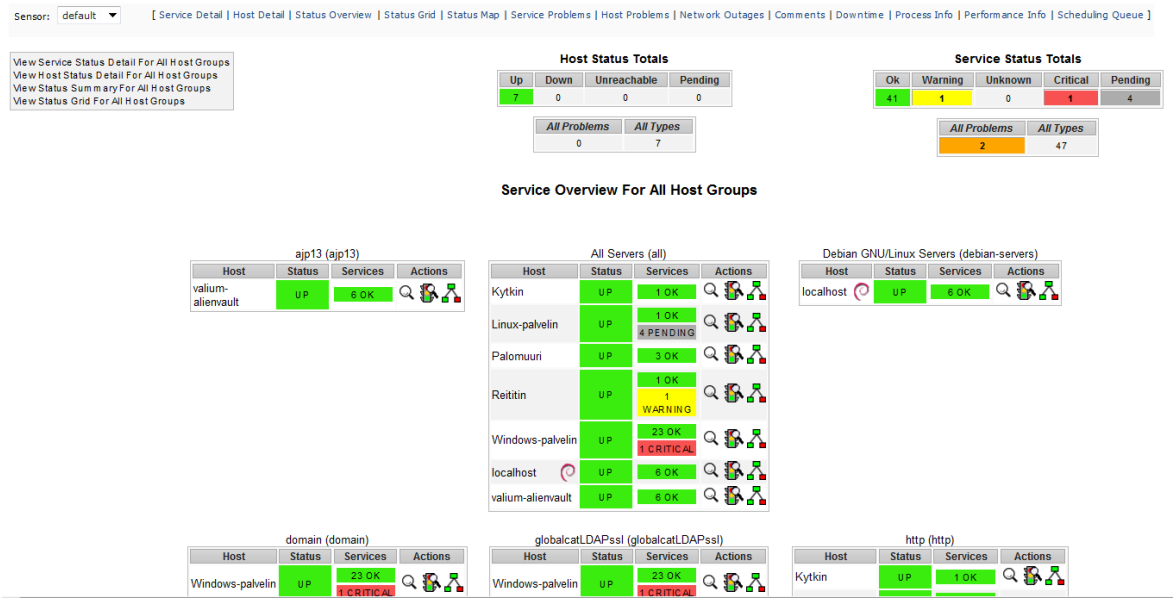
Haun avulla ohjelmisto keräsi laitteista käyttöjärjestelmän tiedot, verkkokortin fyysiset osoitteet ja laitteissa käytössä olevat palvelut kuvan 13 mukaisesti. Päivitettäessä hakutuloksia tietokantaan määritettiin kaikki laitteet Nagioksen valvottavaksi. Laitekohtainen haku kuvan 13 oikeassa reunassa ei lisännyt laitteesta saatavaa tietoa, mutta poisti Nagioksen käytöstä. Se voitiin palauttaa käyttöön ainoastaan poistamalla laite ja hakemalla se uudestaan hakutoiminnolla. Laitteiden hakuun ja Nagioksen käyttöönottoon liittyvät ohjeet ja esimerkkikuvat eivät täysin täsmänneet testatun version kanssa. Ilmeisesti ohjelmiston maksullinen versio tuo joitakin lisäominaisuuksia Nagioksen käyttöön liittyen, vaikka sitä ei ohjeissa mainittukaan. (Lorenzo n.d.a, 89–93, 195–197.)



Kuva 13. AlienVaultin esittämät tiedot valvottavasta laitteesta (Kuvakaappaus ohjelmiston käyttöliittymästä)

Valvottavia laitteita ja verkkoja ei pystynyt tarkastelemaan verkkokuvan avulla. AlienVaultissa oli mahdollisuus hyödyntää karttapohjaa, mutta sen tarkastelu jätettiin tämän testin ulkopuolelle.

Saatavuus-osiona toimi käytännössä Nagioksen graafinen käyttöliittymä. Esimerkki näkymästä on kuvassa 14. Siinä tarkkailtavien laitteiden ja niissä käytettävien palveluiden tila esitetään värikoodein ja sanoin. Tilatietoja pystyi tarkastelemaan yksityiskohtaisemmin eri välilehdillä. Nagioksen käyttö edellytti, että valvottaville palvelimille oli asennettu Nagios-agentti. Windows- ja Linux-ympäristöön oli kumpaankin omat agenttinsa. (Nagios Core Version 3.x Documentation 2010.)



Kuva 14. Esimerkki AlienVaultin esittämistä laitteiden ja palveluiden tilatiedoista (Kuvakaappaus ohjelmiston käyttöliittymästä)

Jotta laitteiden kuormitukseen ja liitäntöihin liittyvää tietoa kyettiin valvomaan, täytyi Nagioksen asetuksiin tehdä muutoksia. Asetusmuutokset täytyi tehdä komentoriviltä asetustiedostoihin. Testin aikana AlienVaultissa käytetyt asetukset on esitelty liitteessä 2. Tarvittavat muutokset ohjeistettiin Nagioksen ohjekirjassa. Tiedostojen oikeat sijainnit oli selvitettävä tutkimalla AlienVaultin kansiorakennetta, joka poikkesi Nagioksen käyttämästä. Myös käytetyt tiedostot ja niiden sisältämät asetukset poikkesivat hieman Nagioksen käyttämästä. (Nagios Core Version 3.x Documentation 2010.)

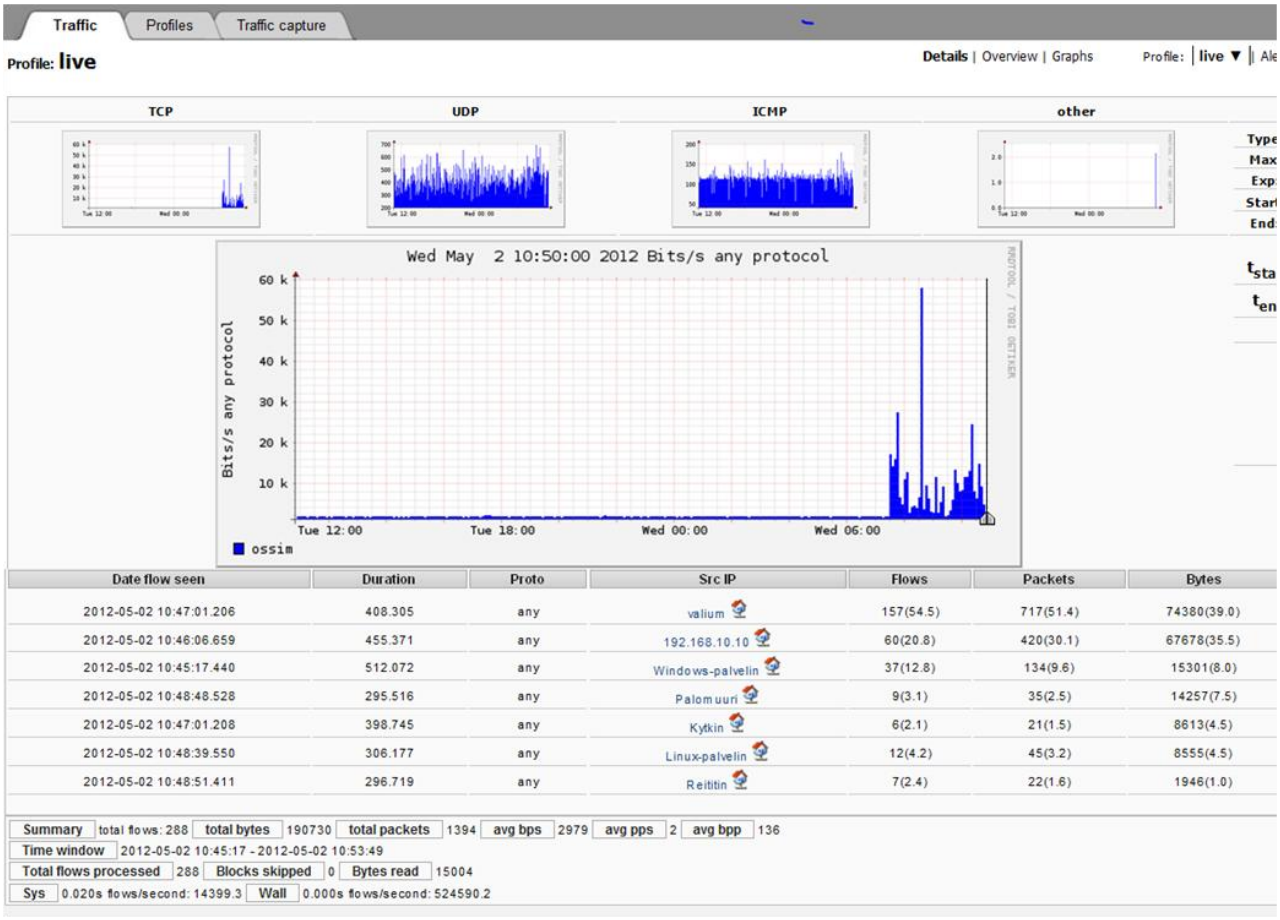
AlienVault loi jokaiselle laitteelle oman asetustiedostonsa todennäköisesti siinä vaiheessa, kun ne määriteltiin Nagioksen valvottavaksi. Niihin tehdyt muutokset säilyivät tallentamisen jälkeen vain hetken. Ne ehtivät päivittymään selainkäyttöliittymän Saatavuus-osioon, mutta hävisivät parin minuutin kuluttua. Samoin kyseinen tiedosto oli palautunut ennalleen. Ilmeisesti ohjelmisto muutti näiden tiedostojen sisältöä säännöllisesti eivätkä käyttäjän tekemät muutokset säilyneet.

Siksi jokaiselle laitteelle luotiin uusi tiedosto eri laitenimellä, johon lisättiin määrittelyt kuormituksen ja liitäntöjen valvomiseksi. Määrittelyissä hyödynnettiin ohjelmiston sisältämiä Nagioksen esimerkkitiedostoja. Luotujen tiedostojen määrittämät tiedot näkyivät selainkäyttöliittymän Saatavuus-osiossa omina laitteinaan, mikä teki näkymästä hieman sekavan. Vastaavasti tällä tavalla lisätyt laitteet eivät näkyneet valvottavien laitteiden listalla. Tehtyjen muutosten jälkeen tuli käynnistää Nagios uudelleen, jotta muutokset astuivat voimaan.

Tehdyistä asetuksista huolimatta Windows-palvelimen kuormitus- ja levynkäyttötietoja ei saatu näkymään oikein selainkäyttöliittymässä. Sen sijaan komentoriviltä suoritetut komentosarjat tuottivat tuloksen, joten palvelimeen asennettu agentti oli toiminnassa. Kyseistä ongelmaa ei onnistuttu ratkaisemaan testin aikana. Samoin verkkolaitteiden liitäntäkohtaisten liikennemäärien ja kuormituksen seuraaminen MRTG-lisäosan avulla ei onnistunut halutulla tavalla. Lisäosan luomia kuvaajia pystyi tarkkailemaan sen omalla html-sivulla, mutta AlienVaultin käyttöliittymän kautta se ei onnistunut. Syynä oli se, että ohjelmisto ei kyennyt luomaan tarvittavia lokitiedostoja todennäköisesti käyttöoikeuksiin liittyvien ristiriitojen vuoksi. Näitä ei onnistuttu testin aikana ratkaisemaan.

AlienVaultissa oli mahdollista kerätä kohdelaitteiden tuottamia lokitietoja useammalla menetelmällä. Näistä käytettiin syslog-liitännäistä ja OSSEC-lisäosaa. Tarvittavia asetusmäärityksiä ei kuitenkaan ehditty kunnolla tekemään, joten lokien tuottaman tiedon hyödyntämistä ei ehditty todentamaan.

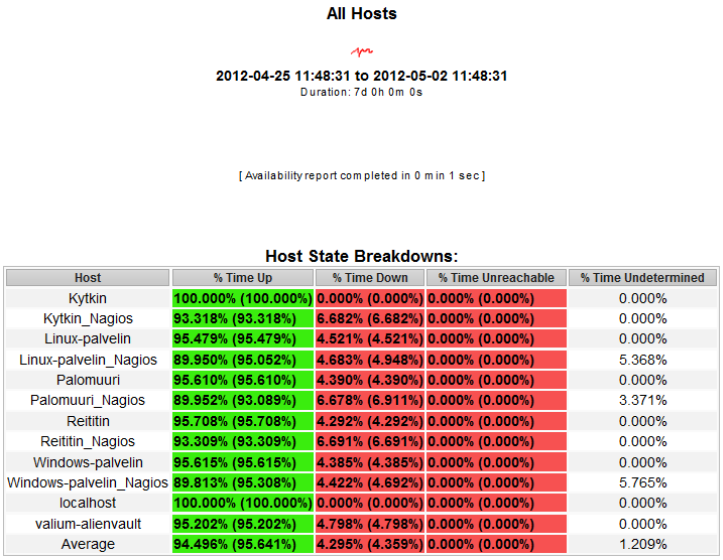
Kuormituksen seurantaan AlienVault käytti Nfdump ja Fprobe-lisäosia. Niiden tuottamaa tietoa seurattiin Network-osiona toimineesta nfsen-käyttöliittymästä. (Lorenzo n.d.b, 151.) Esimerkki osion näkymästä on esitetty kuvassa 15. Liikennemääriä pystyi seuraamaan halutulta ajanjaksolta joko protokollakohtaisesta tai kokonaismäärän näyttävästä graafistaeri näkökulmista. Lisäksi tuloksia pystyi suodattamaan siten, että laitekohtaisia kuormituksia pystyi seuraamaan listauksena, Kuormituksen seuraaminen ei edellyttänyt erillisiä asetusmäärittelyjä ohjelmistossa tai seurattavissa laitteissa.



Kuva 15. Esimerkki AlienVaultin tuottamasta tiedosta verkon kuormituksen seuraamiseksi (Kuvakaappaus ohjelmiston käyttöliittymästä)

Testiympäristö tuotti valtavasti tapahtumia AlienVaultiin. Jotta ohjelmisto saatiin tuottamaan hälytyksiä halutuista tapahtumista, oli muodostettava käytänteitä ja niihin liittyviä toimenpiteitä. Luotaessa käytännettä rajattiin eri parametrien, kuten lähde- ja kohdeosoite, avulla hälytyksen aiheuttavat tapahtumat. Käytänteeseen liitetty tapahtuma oli esimerkiksi tiketin avaaminen tai hälytys sähköpostiin. Testissä todettiin kumpikin toimenpide toimivaksi. Toimenpidettä luotaessa voitiin määritellä, mitä tapahtuman tietoja esimerkiksi sähköpostiviestiin liitettiin. Yhteen käytänteeseen on mahdollista liittää useita toimenpiteitä.

Raportointi-osiossa oli lähinnä ohjelmiston varsinaiseen käyttötarkoitukseen liittyviä vakiomuotoisia raporttipohjia. Ne luotiin halutulta ajanjaksolta sekä Word- että pdf-muodossa. Jälkimmäinen oli mahdollista lähettää myös haluttuun sähköpostiosoitteeseen. Osiossa pystyi luomaan myös laitekohtaisia raportteja. Verkon ja sen laitteiden tilaan liittyviä raportteja oli mahdollista luoda Saatavuus-osiona toimivasta Nagioksen käyttöliittymästä. Raportoitava tieto näytettiin joko listauksena tai graafeina. Esimerkiksi laitekohtaisia tapahtumia oli mahdollista tarkastella listana kun taas laitteen tilaa pystyi tarkastelemaan graafina. Esimerkki raportista on kuvassa 16. Osa raporteista oli mahdollista luoda csv-muodossa. Sitä ei ollut suoraan mahdollista tallentaa kyseisessä muodossa, vaan raportin tiedot oli tallennusta varten kopioitava käyttöliittymästä haluttuun tiedostoon.



All Hosts

2012-04-25 11:48:31 to 2012-05-02 11:48:31
Duration: 7d 0h 0m 0s

[Availability report completed in 0 min 1 sec]

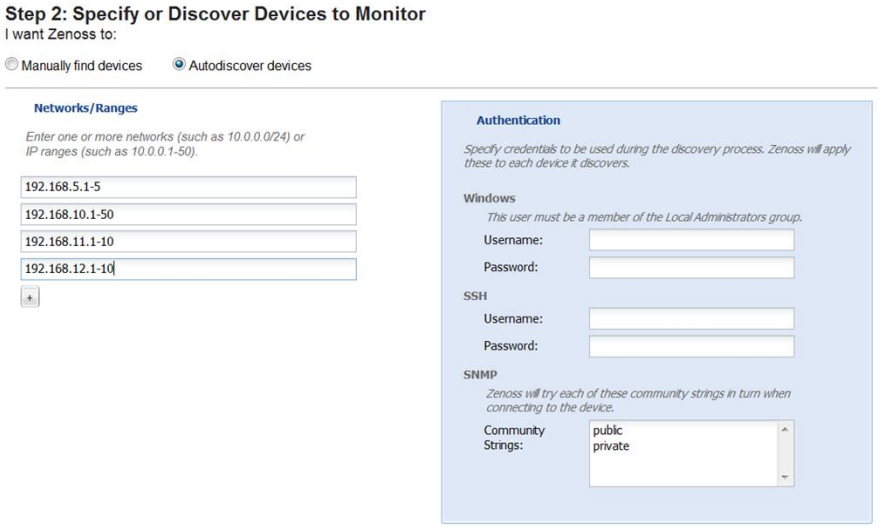
Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Kytkin	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Kytkin_Nagios	93.318% (93.318%)	6.682% (6.682%)	0.000% (0.000%)	0.000%
Linux-palvelin	95.479% (95.479%)	4.521% (4.521%)	0.000% (0.000%)	0.000%
Linux-palvelin_Nagios	89.950% (95.052%)	4.683% (4.948%)	0.000% (0.000%)	5.368%
Palomuuri	95.610% (95.610%)	4.390% (4.390%)	0.000% (0.000%)	0.000%
Palomuuri_Nagios	89.952% (93.089%)	6.678% (6.911%)	0.000% (0.000%)	3.371%
Reititin	95.708% (95.708%)	4.292% (4.292%)	0.000% (0.000%)	0.000%
Reititin_Nagios	93.309% (93.309%)	6.691% (6.691%)	0.000% (0.000%)	0.000%
Windows-palvelin	95.615% (95.615%)	4.385% (4.385%)	0.000% (0.000%)	0.000%
Windows-palvelin_Nagios	89.813% (95.308%)	4.422% (4.692%)	0.000% (0.000%)	5.765%
localhost	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
valium-alienvault	95.202% (95.202%)	4.798% (4.798%)	0.000% (0.000%)	0.000%
Average	94.496% (95.641%)	4.295% (4.359%)	0.000% (0.000%)	1.209%

Kuva 16. Esimerkki AlienVaultin tuottamasta raportista (Kuvakaappaus ohjelmiston käyttöliittymästä)

4.3.2 Zenoss

Avattaessa Zenossin selainkäyttöliittymä ensimmäisen kerran tuli näkyviin asetusvelho, jolla määriteltiin pääkäyttäjän salasana, yksi tavanomainen käyttäjä sekä etsittiin verkkoja ja verkkolaitteita. Esimerkki näkymästä on kuvassa 17. Laitteiden etsintään käytettiin automaattista toimintoa. Etsittäväksi alueeksi määriteltiin testiympäristön aliverkot. Menetelmänä käytettiin SNMP:tä. Ennen tätä varmistettiin, että testiympäristön laitteilla oli oikeat SNMP-asetukset.



Step 2: Specify or Discover Devices to Monitor
I want Zenoss to:

Manually find devices Autodiscover devices

Networks/Ranges

Enter one or more networks (such as 10.0.0.0/24) or IP ranges (such as 10.0.0.1-50).

192.168.5.1-5
192.168.10.1-50
192.168.11.1-10
192.168.12.1-10

Authentication

Specify credentials to be used during the discovery process. Zenoss will apply these to each device it discovers.

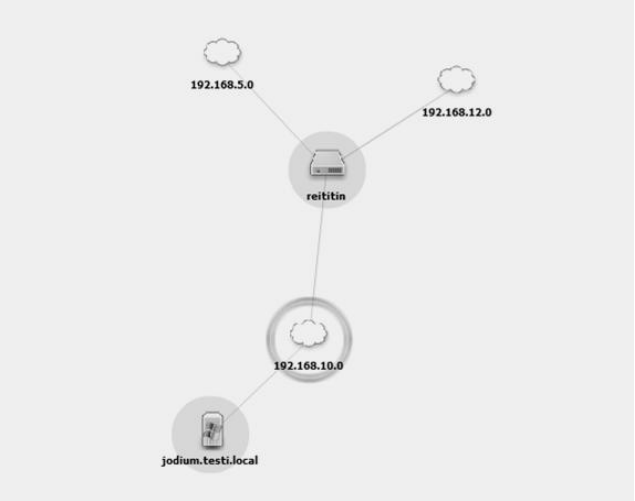
Windows
This user must be a member of the Local Administrators group.
Username:
Password:

SSH
Username:
Password:

SNMP
Zenoss will try each of these community strings in turn when connecting to the device.
Community Strings: public private

Kuva 17. Zenossin asetusvelho (Kuvakaappaus ohjelmiston käyttöliittymästä)

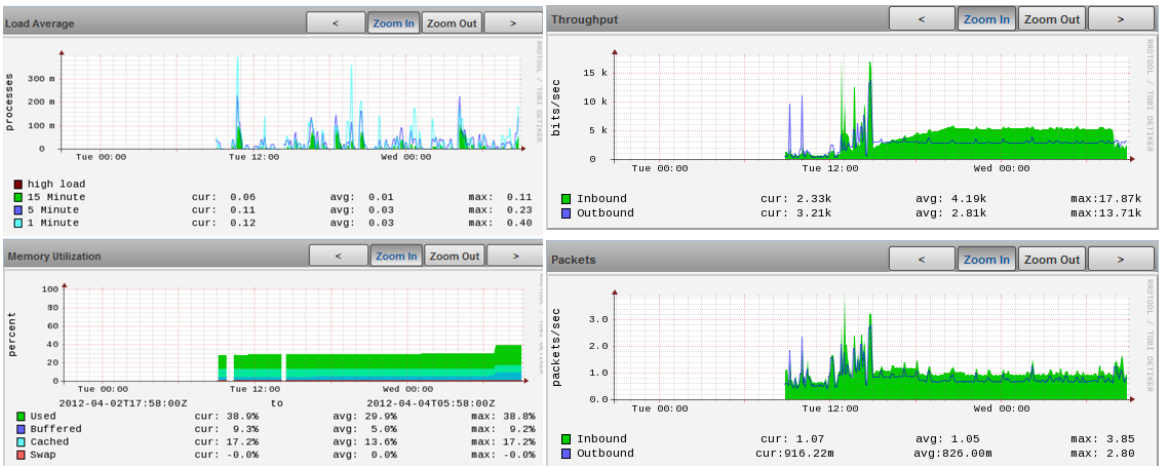
Kaikki testiympäristön laitteet löytyivät tällä menetelmällä. Tavallisia työasemia ei haluttu tässä testissä valvoa, joten ne poistettiin laitelistalta. Tuloksia pystyi tarkastelemaan myös verkkokartan avulla, jossa näkyi kerrallaan yhteen aliverkkoon kuuluvat laitteet. Esimerkki näkymästä on kuvassa 18.



Kuva 18. Esimerkki Zenossin luomasta verkkokartasta (Kuvakaappaus ohjelmiston käyttöliittymästä)

Kaikki löydetyt laitteet kuuluivat aluksi Discovered-luokkaan. Tällöin niistä pystyi näkemään käyttöjärjestelmään ja kokoonpanoon liittyviä perustietoja, verkkoliitäntöjen määrän, laadun ja tilan sekä reititystietoja. Liitäntöihin liittyvää suorituskykytietoa esitettiin myös graafien avulla. Laitteiden löytämisen jälkeen kukin laite siirrettiin Zenossin toimintaperiaatteen mukaisesti oikean laiteluokan alle. Testin aikana käytetyt laiteluokat ja muut Zenossiin tehdyt asetusmuutokset on esitelty liitteessä 3.

Laitteiden siirtämisen jälkeen reitittimelle ja Linux-palvelimelle ilmestyi kuormitukseen ja muistiin liittyviä graafeja. Esimerkki graafeista on esitetty kuvassa 19. Palomuuri, kytkin ja Windows-palvelin vaativat tietolähdeasetuksien muokkaamista. Asetusten muokkaamisessa hyödynnettiin valmistajan Internet-sivustolla saatavissa olleita valmiita ZenPack-lisäosia, jotka sisälsivät tarvittavat luokkakohtaiset asetukset (Zenoss Inc n.d.f).



Kuva 19. Zenossin tuottamia graafeja: vasemmassa reunassa palvelimen kuormitukseen liittyviä ja oikeassa reunassa reitittimen yhden liitännän liikenteeseen liittyviä graafeja (Yhdistelmä kuvakaappauksista ohjelmiston käyttöliittymästä)

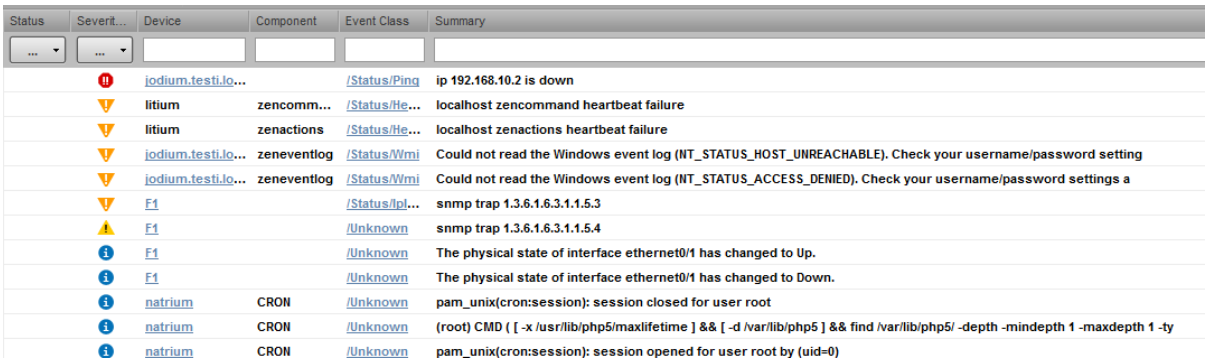
Lisäosien asentamisen jälkeen täytyi vähintään Zope-sovelluspalvelin käynnistää uudestaan, mutta joissakin tapauksissa oli käynnistettävä koko Zenoss-ohjelmisto uudelleen. Tätä ei pystynyt tekemään selainkäyttöliittymän kautta, vaan ainoastaan palvelimen komentoriviltä zenoss-käyttäjänä. Jotta muutokset vaikuttivat laitteista saatavaan informaatioon, tarvittavat laitteet oli mallinnettava uudestaan. Toimenpiteen suorittaminen käynnistettiin valikosta ja sen etenemistä oli mahdollista seurata käyttöliittymään avautuneesta komentorivi-ikkunasta.

Windowsin SNMP-agentti ei palauttanut palvelimen suorituskykyyn liittyvää tietoa. Zenoss suositteli, että Windows-palvelimelle olisi asennettu kolmannen osapuolen SNMP-agentti. (Getting Started with Zenoss 2010, 19.) Zenossiin oli saatavilla myös juuri tätä tarkoitusta varten laadittu lisäosa, joka ei vaatinut erillisiä asennuksia kohdelaitteeseen. Testissä käytettiin kyseistä lisäosaa. Myös palomuurille löytyi sopiva lisäosa, jonka avulla saatiin suorituskykytiedot näkyviin.

Kytkimelle oli tarjolla ainoastaan vanhemmilla ohjelmistoversioilla testattu lisäosa, joka saatiin asennettua myös testissä käytettyyn ohjelmistoversioon. Siinä olleet tietolähteet eivät kuitenkaan toimineet todennäköisesti virheellisten objektitunnisteiden määrittelyjen vuoksi. Tunnisteita yritettiin korjata oikeaksi muun muassa foorumilta löytyneiden ohjeiden avulla, mutta suorituskykytietoja ei saatu näkymään. (Zenoss Inc, 2008)

Zenoss näytti laitekohtaisella välilehdellä laitteen liitäntöjen tilan mallinnushetkellä. Laite tuli mallintaa uudelleen aina, kun sen siirrettiin toiseen luokkaan tai luokkaan tehtiin muutoksia. Mallinnuksen avulla kaikki luokkaan liittyvät ominaisuudet otettiin käyttöön. Välilehdeltä pystyi seuraamaan graafien avulla liitäntäkohtaisia suorituskykytietoja. Liitännän tilatieto ei tässä näkymässä kuitenkaan muuttunut esimerkiksi yhteyskatkoksen aikana, vaan ainoastaan laitteen mallintamisen jälkeen.

Liitäntöjen tilaa voitiin seurata erilaisten tapahtumien avulla. Yhteyden katketessa tai otettaessa liitäntä pois käytöstä Zenoss loi siitä tapahtuman muun muassa SNMP:n trap-viestin tai järjestelmälokin avulla. Järjestelmälokien käsittelyn mahdollistamiseksi, testiympäristön laitteiden järjestelmälokitiedot ohjattiin Zenoss-palvelimelle. Kolmantena tapana testattiin käyttäjäyhteisön sivuilta löytyneen dokumentin mukaan luotua SNMP-kyselyä, jolla saatiin sama informaatio (Zenoss Inc 2011). Esimerkki Zenossin tapahtumanäkymästä on kuvassa 20.



Status	Severit...	Device	Component	Event Class	Summary
		jodium.testi.lo...		/Status/Ping	ip 192.168.10.2 is down
		litium	zencomm...	/Status/He...	localhost zencommand heartbeat failure
		litium	zenactions	/Status/He...	localhost zenactions heartbeat failure
		jodium.testi.lo...	zeneventlog	/Status/Wmi	Could not read the Windows event log (NT_STATUS_HOST_UNREACHABLE). Check your username/password setting
		jodium.testi.lo...	zeneventlog	/Status/Wmi	Could not read the Windows event log (NT_STATUS_ACCESS_DENIED). Check your username/password settings a
		F1		/Status/Ipl...	snmp trap 1.3.6.1.6.3.1.1.5.3
		F1		/Unknown	snmp trap 1.3.6.1.6.3.1.1.5.4
		F1		/Unknown	The physical state of interface ethernet0/1 has changed to Up.
		F1		/Unknown	The physical state of interface ethernet0/1 has changed to Down.
		natrium	CRON	/Unknown	pam_unix(cron:session): session closed for user root
		natrium	CRON	/Unknown	(root) CMD ([-x /usr/lib/php5/maxlifetime] && [-d /var/lib/php5] && find /var/lib/php5/ -depth -mindepth 1 -maxdepth 1 -ty
		natrium	CRON	/Unknown	pam_unix(cron:session): session opened for user root by (uid=0)

Kuva 20. Esimerkki Zenossin luomista tapahtumista (Kuvakaappaus ohjelmiston käyttöliittymästä)

Reitittimessä käytetyt virtuaaliliitännät synnyttivät testin aikana toistuvasti tapahtumailmoituksen, vaikka niiden tilassa ei tapahtunut muutoksia. Niihin liittyvät graafit vaikuttivat tuottavan oikeaa tietoa. Tapahtumailmoituksen johtuivat keskustelupalstan mukaan siitä, että laitteen virtuaaliliitännät eivät tue samoja SNMP-objekteja kuin fyysiset liitännät. Koska liitäntöjen seuraamiseen käytettiin oletusmallipohjaa, aiheuttivat puuttuvat objektit toistuvasti ilmoituksen SNMP-kyselyn yhteydessä. Ilmoitusten syntyminen on todennäköisesti mahdollista estää käyttämällä virtuaaliliitännöille erillistä mallipohjaa. Tässä testissä erillisen mallipohjan käyttöä ei testattu. (Zenoss Inc 2009.)

Koko verkkosegmentin liikennemäärän seuraamiseen ei löytynyt mainintoja ohjekirjoissa tai foorumilla. Eri liitäntöjen liikennemääriä oli mahdollista valvoa, mutta kytkimeen liittyneet ongelmat estivät kokonaiskuormituksen valvonnan todentamisen.

Windows-palvelimessa käytössä olevien palveluiden tilaa pystyttiin seuraamaan erillisen lisäosan avulla. Palvelut oli sijoitettu omalle välilehdelleen laitetiedoissa ja toisin kuin liitäntöjen osalta niiden tilatieto päivittyi tässä näkymässä automaattisesti. Vastaavasti Linux-palvelin ei vaatinut erillisiä lisäosia palvelun tilan havaitsemiseen. Palveluiden tilan valvontaan voitiin hyödyntää myös järjestelmälokien tapahtumatietoja. Testissä sekä lisäosan että järjestelmälokien tuottamat tapahtumat todettiin toimivaksi kummallakin palvelimella palvelukatkoksen yhteydessä.

Testin aikaisista tapahtumista haluttiin saada ilmoitus myös sähköpostiin. Hälytyssäännöt olivat käyttäjäkohtaisia ja ne luotiin käyttäjän asetuksissa omalla välilehdellään. Oletusarvoisesti hälytykset lähetettiin siihen sähköpostiosoitteeseen, joka oli määritelty käyttäjätiedoissa. Hälytyssäännön asetuksissa voitiin määritellä myös vaihtoehtoinen osoite hälytyksille. Hälytysviestin sisältöä oli mahdollista muokata haluamallaan tavalla. Tässä testissä käytettiin oletusviestiä. Viestissä ilmoitettiin samat tiedot tapahtumasta kuin Zenossin Tapahtumat-välilehdelläkin. Lisäksi siinä oli linkit tapahtuman kuittaamiseen, poistamiseen ja yksityiskohtien tarkasteluun.

Zenossissa oli useita valmiita raporttipohjia, joiden lisäksi oli mahdollista luoda omia raporttipohjia. Valmiit raportit olivat pääosin listauksia esimerkiksi koko verkon liitännöistä ja niiden tilasta tai verkossa käytettävis-

tä palveluista. Kuvassa 21 on esimerkki ohjelmiston luomasta raportista. Zenossissa oli mahdollista luoda myös graafipohjaisia raportteja. Ainakin listamuotoiset raportit oli mahdollista tallentaa csv-tiedostoon. Raporttien lisäksi ohjelmiston tuottamat tapahtumat oli mahdollista tallentaa joko csv- tai xml-tiedostoon.


All Devices

Name	Class	Product	State	Ping	Snmp
F1	/Network/Router/Firewall	.1.3.6.1.4.1.3224.1.52	Production	Up	Up
R1.testi.local	/Network/Router/Cisco	2821	Production	Up	Up
S1	/Network/Switch/HP	.1.3.6.1.4.1.11.2.3.7.11.104	Production	Up	Up
iodium.testi.local	/Server/Windows/2 Processors	.1.3.6.1.4.1.311.1.1.3.1.3	Production	8	Up
natrium	/Server/Linux	Net-SNMP Agent	Production	Up	Up

export all

Kuva 21. Esimerkki Zenossin luomasta raportista (Kuvakaappaus ohjelmiston käyttöliittymästä)

4.4 Tulokset

Ohjelmistojen asentaminen oli varsin yksinkertaista. Zenossin asentaminen onnistui yhdellä komennolla, mutta sen jälkeen oli tarpeellista tehdä muutamia säätötoimenpiteitä. AlienVaultin asennusprosessi kesti jonkin verran pitempään, koska samalla asennettiin käyttöjärjestelmä. Asentamisvaiheessa määriteltiin käyttöjärjestelmän asentamiseen liittyvien parametrien lisäksi verkkoasetuksia ja valvottavan ympäristön aliverkot.

Kummankin ohjelmiston alustana käytettiin samanlaisia virtuaalikoneita. Niiden muistin määrä oli vähimmäissuosituksia pienempi. Tästä ei ollut merkittävää haittaa testaukselle. AlienVaultin osalta se esti laitteiden automaattisen etsinnän koko ympäristöstä kerrallaan. Seurauksena oli ohjelmiston merkittävä hidastuminen ja jopa kaatuminen. Laitteet voitiin käytännössä hakea vain laite kerrallaan. Muilta osin muistin määrä ei vaikuttanut ohjelmiston käyttöön. Zenossin käyttöliittymässä ilmeni testauksen loppuvaiheilla jonkin verran hitautta. Ilmiö liittyi mahdollisesti käytettyyn työasemaan, sillä käytettäessä ohjelmistoa toiselta työasemalta liittymä toimi normaalisti.

Dokumentaation perusteella kummastakin ohjelmistosta olisi pitänyt löytyä testatut ominaisuudet. Paria poikkeusta lukuun ottamatta näin olikin. Tiivistelmä testien tuloksista on esitetty taulukossa 3. Tuloksia on käsitelty tarkemmin liitteessä 5.

Taulukko 3. Tiivistelmä testituloksista

Toiminto	AlienVault	Zenoss
Laitteiden automaattinen löytäminen	kyllä	kyllä
Verkon kokoonpanon esittäminen verkkokuvana	ei	kyllä
Ohjelmiston asetusten muokkaaminen pelkästään selainkäyttöliittymästä	ei	ei
Laitteiden perusparametrien valvonta	kyllä	kyllä
Verkkolaitteen liitäntäkohtainen valvonta	kyllä	kyllä
Palvelimen palvelu-/protokollakohtainen valvonta	kyllä	kyllä
Verkkosegmentin kuormituksen valvonta	kyllä	– [a]
Verkkolaitteen vikaantumisen valvonta	kyllä	kyllä
Yhteyskatkoksen havaitseminen	kyllä	kyllä
Palvelun katkeamisen havaitseminen	kyllä	kyllä
Hälytyksen välittäminen sähköpostiin	kyllä	kyllä
Raporttien vienti ohjelmistosta	kyllä	kyllä

Huom.
a Ei kyetty todentamaan

Kumpikin ohjelmisto kykenee löytämään laitteet määritetystä osoiteavaruudesta automaattisen hakutoiminnon avulla. AlienVaultissa tämän menetelmän perusteella oli mahdollista valvoa ainoastaan laitteissa käytössä olevia palveluita. Muiden parametrien valvomiseksi laitteet oli lisättävä manuaalisesti komentoriviltä. Zenossin hakutoiminto jäi laitteiden löytymisen jälkeenkin toimintaan ja seurasi valvottavan verkon kokoonpanossa tapahtuneita muutoksia reaaliaikaisesti, jos prosessia ei erikseen pysäyttänyt. Zenoss kykeni piirtämään etsinnän tulosten avulla verkkokuvan, jossa oli mahdollista tarkastella yhtä aliverkkoa kerrallaan. AlienVaultissa ei tätä mahdollisuutta ollut.

Kumpaakaan ohjelmistoa ei pystynyt käyttämään puhtaasti selainkäyttöliittymän avulla. Zenossissa komentoriviä tarvittiin lähes ainoastaan asennuksen jälkeen säädettäessä sen eri komponentteja. AlienVaultissa alkuvaiheen asetusmäärittelyt oli tehtävä Zenossin tapaan komentoriviltä. Ohjelmistossa käytettiin laitteiden valvontaan Nagiosta eikä asetusten muokkaamista varten ollut tehty muutoksia sen käyttöliittymään. Siksi myös suurin osa valvottaviin laitteisiin liittyvistä asetuksista tehtiin komentoriviltä. Asetustiedostot olivat käytännössä tekstitiedostoja, joihin oli mahdollista niiden muodollisesta rakenteesta huolimatta syöttää mitä tietoa tahansa. Siksi muokkauksen aikana tehdyt virheet tekivät pahimmillaan koko tiedostosta toimimattoman. Kummallekin ohjelmistolle oli tarjolla kohtuullisen selkeät ohjeet komentoriviltä tehtäviä asetuksia varten, joiden avulla pystyi tekemään tarpeelliset muutokset, vaikka tiedostojen yksityiskohtaista rakennetta ei tunnettukaan.

Testitapausten vaatimat asetusmäärittelyt onnistuivat Zenossilla lähes kokonaan saatavilla olleiden lisäosien avulla. AlienVaultissa määrittelyitä jouduttiin muokkaamaan enemmän, mutta niissäkin pystyi hyödyntämään ohjelmistoon sisältyneiden mallitiedostojen sisältöä.

Testin aikaisista ongelmista huolimatta kumpikin ohjelmisto kykeni valvomaan testiympäristöä kattavasti ja havaitsemaan siinä ilmenneet vikatilanteet. Ongelmat eivät johtuneet ominaisuuksien puutteesta, vaan kohdelaitteesta tai käytetystä lisäosasta tai agentista. Tästä syystä Zenossin osalta jäi todentamatta sen kyky verkkosegmentin kuormituksen valvontaan.

Testin perusteella valvottavien laitteiden järjestelmälokien tapahtumat eivät tuottaneet lisäarvoa testitapausten todentamiseen, vaikka ne olivatkin kummankin ohjelmiston käytettävissä. Tarvittava informaatio esimerkiksi vikatilanteista oli mahdollista saada muilla menetelmillä. Sen sijaan vian etsintään ja ongelmatilanteiden ratkaisuun ne tarjosivat hyödyllistä lisätietoa.

Kumpikin ohjelmisto pystyi välittämään hälytyksen halutuista tapahtumista sähköpostitse ylläpitäjälle. Lähetettävän sähköpostin sisältö oli mahdollista määritellä halutunlaiseksi ja eri sääntöjen avulla pystyi luomaan käyttäjäkohtaisia hälytyksiä.

AlienVaultin ohjekirjat esittelivät kattavasti ohjelmiston ominaisuuksia painottuen varsinaiseen käyttötarkoitukseen – tunkeutumisen estoon ja tunnistamiseen. Laitteiden löytämiseen ja valvonnan aloittamiseen liittyvä ohjeistus oli testauksen perusteella puutteellista. Ohjeissa esitetyt näkymät ja toimintojen sijainnit käyttöliittymässä poikkesivat testatusta versiosta. Eroista huolimatta ohjeet olivat helposti hahmotettavissa lukuun ottamatta Nagiokseen liittyviä asetuksia. Niihin löytyi tukea Nagioksen ohjekirjoista.

AlienVaultin dokumentointi oli valtaosin laadittu kaupalliseen versioon perustuen. Avoimeen lähdekoodiin perustuvan version osalta viitattiin samaan dokumentointiin. Ohjekirjoissa oli erikseen mainittu ominaisuuksista, jotka olivat saatavilla ainoastaan kaupallisessa versiossa. Testauksen perusteella eri versioiden valikkorakenne ja joidenkin osioiden näkymät ja toiminnallisuus poikkesivat toisistaan muutenkin kuin ohjekirjoissa mainituissa kohdissa.

Zenossin ohjekirjat olivat varsin kattavia ja selkeitä. Ohjeet painottuivat Windows- ja Linux-palvelimien ja niissä käytettävien palveluiden valvontaan verkkolaitteiden jäädessä varsin vähälle huomiolle. Muiden tietolähteiden käyttö testin aikana oli varsin vähäistä. Muutamissa kohdissa oli ratkaisua etsittävä muista lähteistä. Valmistajan kysymyksiä ja vastauksia -palsta sekä käyttäjäyhteisön foorumi auttoivat näissä tilanteissa.

Kummankin ohjelmiston selainkäyttöliittymät olivat selkeitä käyttää ja toiminnot olivat loogisesti ryhmitelty. Avausnäkymä sisälsi yhteenvedon verkon tilasta ja käyttäjän oli mahdollista muokata sen sisältöä. AlienVaultissa valvottavan verkon kokonaistila oli helpompi hahmottaa kuin

Zenossissa. AlienVaultissa Nagioksen näkymästä pystyi näkemään niin laitteiden, niiden liitäntöjen kuin niissä käytettyjen palveluiden tilan yhdellä silmäyksellä.

Zenossissa näki laitteisiin liittyvien tapahtumien määrän ja laitteen tilan laitevalikossa, mutta eri parametrien tilaa pystyi tarkkailemaan laite kerrallaan laitekohtaisista tiedoista. Ohjelmistossa oli mahdollista luoda raportti, jossa kaikki seurattavat parametrit olivat samassa listassa tilatietoineen. Se ei kuitenkaan ollut yhtä havainnollinen kuin AlienVaultissa käytetty esitystapa.

Tapahtumanäkymä oli Zenossissa AlienVaultia selkeämpi. Tämä johtui osaksi siitä, että AlienVault tuotti oletusasetuksilla runsaasti enemmän tapahtumia kuin Zenoss. Zenossissa oli monille eri parametreille luotu hälytysrajat oletusarvoilla. Osa näistä sisältyi käytettyihin lisäosiin. Yhteyskatkokset ja muut vakavat vikatilanteet tuottivat oletusasetuksilla hälytyksen aiheuttavan tapahtuman. AlienVaultissa mikään tapahtuma ei tuottanut oletusarvoilla hälytystä ohjelmistossa, vaan hälytyssäännöt oli luotava erikseen. Toisaalta Nagioksen havainnollinen näkymä korvasi osin tätä tilannetta.

5 YHTEENVETO

Luotaessa verkonhallintajärjestelmää on määritettävä mitä verkonhallinnan osa-alueita on tarkoituksenmukaista painottaa ja käytettävät työkalut on valittava sen mukaisesti. Valvonta on keskeinen osa verkonhallintaa ja liittyy jokaiseen osa-alueeseen. Kattava ja tarkoituksenmukainen verkonvalvonta tuottaa tietoa verkon kuormituksesta eri tilanteissa ja mahdollistaa verkossa tapahtuviin muutoksiin reagoinnin ja parhaimmillaan palvelukatkokset voidaan ennaltaehkäistä.

Jo muutamasta laitteesta koostuvan verkon valvonta on työlästä ilman siihen tarkoitukseen sopivia työkaluja. Haettaessa kustannustehokkaita ratkaisuja avoimeen lähdekoodiin perustuvat ohjelmistot muodostavat houkuttelevan vaihtoehdon. Niiden käyttäjä voi vapaasti muokata ohjelmistoa vastaamaan omia tarpeita. Toisaalta muiden tekemät muokkaukset ovat vapaasti hyödynnettävissä, eikä kaikkea tarvitse tehdä itse. Ohjelmistoihin ei sisälly minkäänlaista takuuta tai tukipalveluja. Useisiin ohjelmistoihin on tarpeen vaatiessa mahdollista saada maksullisia tukipalveluja, kuten koulutusta tai järjestelmän ylläpitoon liittyvää neuvontaa.

Tässä työssä toteutettuun vertailuun pyrittiin valitsemaan mahdollisimman monipuolisia ohjelmistoja. Muutamaa poikkeusta lukuun ottamatta ohjelmistot kattoivat lähes kaikki vertaillut käyttötarkoitukset. Ohjelmistojen dokumentaatio oli pääsääntöisesti kattava ja selkeä. Dokumentoinnin perusteella ohjelmistoilla oli erilaisia lähestymistapoja verkonvalvontaan, mutta ominaisuuksiltaan useimmat vertaillut ohjelmistot olivat samankaltaisia. Osa vertailuun valituista ohjelmistoista perustui toiseen vertailtavaan ohjelmistoon tai niissä oli mahdollisuus hyödyntää toisen ohjelmiston liitännäisiä, mikä on täysin ohjelmistoissa käytettävän lisenssin mukaista.

Valintaprosessin perusteella testaukseen kelpuutettavia ohjelmistoja oli kolme. Testattavat ohjelmistot valittiin näiden joukosta niiden erilaisen toimintaperiaatteen perusteella. AlienVault oli ensisijaisesti verkkoon tunkeutumisen havaitsemiseen ja estämiseen tarkoitettu ohjelmisto, johon oli integroitu useita verkonvalvontatyökaluja. Ohjelmisto käytti SNMP:n ohella muita agentteja tiedon keruuseen. Zenoss puolestaan oli tarkoitettu nimenomaan verkonvalvontaan ja sen yhtenä päämenetelmänä tiedonkeruussa oli SNMP. Se ei pääsääntöisesti käyttänyt erillisiä agentteja.

Ohjelmistojen testaus toteutettiin sitä varten luodussa suljetussa verkkoympäristössä. Testauksen tarkoituksena oli todentaa vertailussa mainitut ominaisuudet ja toiminnallisuudet liitteessä 4 esitetyn suunnitelman mukaisesti. Kummankin ohjelmiston testauksessa kohdattiin ongelmia, joita ei pystytty testaukseen käytettävissä olevan ajan puitteissa ratkaisemaan. Ongelmat eivät kuitenkaan olleet niin merkittäviä, että ne olisivat vaikuttaneet testauksen toteuttamiseen. Ainoastaan verkkosegmentin kuormituksen valvonnan ei Zenossin osalta pystytty todentamaan testauksen aikana ilmenneiden ongelmien vuoksi. Kumpikaan testatuista ohjelmistoista ei läpäissyt kaikkia testitapauksia. Kyseiset testitapaukset liittyivät lähinnä

ohjelmistojen käyttötapaan ja tiedon visualisointiin eikä niillä ollut vaikutusta niiden toimintaan.

Ohjelmistojen käyttöönotto ja valvonnan aloittaminen oli melko vaivatonta ja nopeaa. Zenossiin on saatavilla valmiita lisäosia, joissa oli valmiit laitekohtaiset asetukset. AlienVaultissa vastaavien asetusten muokkaaminen vaati jonkin verran perehtymistä Nagios-ohjelmistoon. Koska AlienVaultissa käytettiin Nagioksen graafista käyttöliittymää sellaisenaan, suuri osa asetusmäärittelyistä oli tehtävä komentoriviltä. Tämän perusteella AlienVault ei olisi läpäissyt valintaprosessia. Dokumentaatiosta sai kuitenkin vaikutelman, että tähän ei olisi ollut tarvetta. Molempien testattujen ohjelmistojen osalta niiden yksityiskohtainen säätäminen voi olla aikaa vievää. Valvottavien parametrien valinta ja hälytysrajojen määrittäminen vaativat hyvää kohdeverkon tuntemusta.

Testauksen aikana havaituista puutteista huolimatta ohjelmistojen käyttöä voisi harkita lähes kaikkien luvussa 2 esitettyjen käyttäjäryhmien tarpeisiin. Osaamistarpeista johtuen ohjelmistot eivät välttämättä sovellu pienyritysten tarpeisiin. Yksityis- ja opetuskäytössä ohjelmistot tarjoavat erinomaisen mahdollisuuden perehtyä verkonvalvontaan ilman ohjelmistokustannuksia. Käyttäjäyhteisöjen foorumit tarjoavat apua moniin ongelmatilanteisiin eikä maksullisille tukipalveluille ole tarvetta. Suurempien yritysten ja julkisen sektorin osalta ohjelmistojen käyttöönotto ja kriittisten palveluiden keskeytymätön toiminta edellyttänee maksullisen koulutuksen hankkimista ja jonkinlaista maksullista tukipalvelua.

Mahdollisia jatkotutkimusaiheita ovat muun muassa ohjelmistojen suorituskyvyn todentaminen kuormitustesteillä, kuormittuvan tai katkonaisesti toimivan palvelun havaitseminen, hajautetun verkon valvonta sekä syvällisempi perehtyminen tapahtumien käsittelyyn ja raportointiin. Jatkotutkimuksia tehdessä on hyvä olla tiedossa kohdeympäristö, jossa ohjelmistoa tullaan käyttämään.

LÄHTEET

AlienVault LC. 2012a. AlienVault Community Overview. Viitattu 2.2.2012. http://www.alienvault.com/community

AlienVault LC. 2012b. AlienVault Technical Documentation. Viitattu 2.2.2012. http://alienvault.com/community/technical-documentation

AlienVault LC. 2012c. Download AlienVault Open Source SIEM. Viitattu 2.2.2012. http://www.alienvault.com/download-ossim

AlienVault LC. n.d.a. AlienVault Solutions. Viitattu 23.2.2012. http://www.alienvault.com/solutions/unified-security-management-platform/

AlienVault LC. n.d.b. Case Studies. Viitattu 23.2.2012. http://www.alienvault.com/solutions/services-subscriptions/

AlienVault LC. n.d.c. Services & Subscriptions. Viitattu 23.2.2012. http://www.alienvault.com/c-suite/case-studies/

AlienVault Unified SIEM. System Description. Version 1.0. n.d. AlienVault LC. Viitattu 2.2.2012. http://alienvault.com/docs/AlienVault_Unified_System_Description_1.0.pdf

BalaBit IT Security Ltd. n.d.a. Documentation. Viitattu 2.2.2012. http://www.balabit.com/support/documentation

BalaBit IT Security Ltd. n.d.b. New generation logging. Viitattu 2.2.2012. http://www.balabit.com/network-security/syslog-ng

BalaBit IT Security Ltd. n.d.c. Projects using syslog-ng. Viitattu 2.2.2012. http://www.balabit.com/network-security/syslog-ng/opensource-logging-system/overview/references

BalaBit IT Security Ltd. n.d.d. Server side. Viitattu 2.2.2012. http://www.balabit.com/network-security/syslog-ng/opensource-logging-system/features/server_side#flex4

BalaBit IT Security Ltd. n.d.e. Support of syslog-ng versions. Viitattu 2.2.2012. http://www.balabit.com/network-security/syslog-ng/opensource-logging-system/support?utm_source=syslog-ng-ose-guide-admin-en&utm_medium=pdf-guide&utm_campaign=syslog-ng-ose-guide-admin-en

Berry, I., Roman, T., Adams, L., Pasnak, J., Conner, J., Scheck, R. & Braun, A. 2010. The Cacti Manual. The Cacti Group. Viitattu 3.2.2012. http://www.cacti.net/downloads/docs/pdf/manual.pdf

Centreon. n.d.a. Centreon Architecture. Viitattu 4.2.2012. http://www.centreon.com/Content-Products-IT-network-monitoring/architecture

Centreon. n.d.b. Centreon Entreprise Server. Viitattu 4.2.2012. http://www.centreon.com/Content-products/centreon-entreprise-server

Centreon. n.d.c. Centreon features in detail. Viitattu 4.2.2012. http://www.centreon.com/Content-Products-IT-network-monitoring/features-in-detail-centreon

Centreon. n.d.d. Centreon: Monitoring and supervision of hardware and software systems. Viitattu 7.2.2012. http://www.centreon.com/Content-products/it-infrastructure-and-application-monitoring-centreon

Centreon. n.d.e. Customers and testimonials. Viitattu 4.2.2012 http://www.centreon.com/Customers/testimonials

Centreon. n.d.f. Documentation for Centreon Enterprise Server. Viitattu 4.2.2012. http://www.centreon.com/Content-Products-Entreprise-Server/documentation

Centreon. n.d.g. Download Centreon. Viitattu 4.2.2012. http://www.centreon.com/Content-Download/donwload-centreon-monitoring-tools

Centreon. n.d.h. Supported Software and requirements. Viitattu 4.2.2012. http://www.centreon.com/Content-Products-IT-network-monitoring/supported-software-and-requirements

Centreon. n.d.i. Support for Centreon. Viitattu 4.2.2012. http://www.centreon.com/Content-Services/support

Centreon. n.d.j. The Centreon Software Suite is a set of modular software programs designed for managing and controlling your information systems. Viitattu 4.2.2012. http://www.centreon.com/Home-products/products-centreon

Centreon. n.d.k. Welcome to the Centreon Demonstration Platform. Viitattu 4.2.2012. http://www.centreon.com/Content-products/demo

Getting Started with Zenoss. 2010. Annapolis: Zenoss Inc. Viitattu 4.2.2012. http://ignum.dl.sourceforge.net/project/zenoss/Documentation/Getting Started/Getting_Started_01-092010-3.0-v02.pdf

GNU General Public License 2007. Version 3. Viitattu 21.1.2012. http://www.gnu.org/licenses/gpl-3.0.html.

Hakala, M. & Vainio, M. 2002. Tietoverkon rakentaminen. Jyväskylä: Docendo Finland.

Jaakohuhta, H. 2005. Lähiverkot – Ethernet. 4. uud. p. Helsinki: Edita Publishing.

Lorenzo, J. n.d.a. Alienvault Installation Guide. Version 1.0. Campbell: AlienVault LC. Viitattu 2.2.2012.
http://alienvault.com/docs/Installation_Guide.pdf

Lorenzo, J. n.d.b. AlienVault Users Manual. Version 1.0. Campbell: AlienVault LC. Viitattu 2.2.2012.
http://alienvault.com/docs/Alienvault_Users_Manual_1.0.pdf

Mauro, D. & Schmidt, K. 2001a. Essential SNMP. 1. p. Chapter 2. A Closer Look at SNMP. Sebastobol: O'Reilly & Associates. Viitattu 24.1.2012.
http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_01.htm

Mauro, D. & Schmidt, K. 2001b. Essential SNMP. 1. p. 2.2. SNMP Communities. Sebastobol: O'Reilly & Associates. Viitattu 24.1.2012. http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_02.htm

Mauro, D. & Schmidt, K. 2001c. Essential SNMP. 1. p. 2.5. A Closer Look at MIB-II. Sebastobol: O'Reilly & Associates. Viitattu 26.1.2012. http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_05.htm

Mauro, D. & Schmidt, K. 2001d. Essential SNMP. 1. p. 2.6. SNMP Operations. Sebastobol: O'Reilly & Associates. Viitattu 27.1.2012. http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_06.htm

Mauro, D. & Schmidt, K. 2001e. Essential SNMP. 1. p. 2.8. Remote Monitoring Revisited. Sebastobol: O'Reilly & Associates. Viitattu 27.1.2012.
http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_08.htm

Mauro, D. & Schmidt, K. 2001f. Essential SNMP. 1. p. Appendix F. SNMPv3. Sebastobol: O'Reilly & Associates. Viitattu 24.1.2012. http://docstore.mik.ua/orelly/networking_2ndEd/snmp/appf_01.htm

Nagios Core Version 3.x Documentation. 2010. Nagios Core Development Team and Community Contributors. Viitattu 4.2.2012. http://nagios.sourceforge.net/docs/nagioscore-3-en.pdf

Nagios Enterprises LLC. n.d.a. Customers and users. Viitattu 4.2.2012. http://www.nagios.com/users

Nagios Enterprises LLC. n.d.b. Nagios Core Manuals. Viitattu 4.2.2012. http://library.nagios.com/library/products/nagioscore/manuals/

Nagios Enterprises LLC. n.d.c. Nagios Features. Viitattu 4.2.2012. Nagios Enterprises LLC. Viitattu 4.2.2012. http://www.nagios.org/about/features

Nagios Enterprises LLC. n.d.d. Nagios Support. Viitattu 4.2.2012.
http://www.nagios.org/support
Nagios Enterprises LLC. n.d.e. Nagios XI. Viitattu 4.2.2012.
http://www.nagios.com/products/nagiosxi

Nagios Enterprises LLC. n.d.f. Thanks for Downloading Nagios Core. Viitattu 4.2.2012. http://www.nagios.org/download/core/thanks/

OpenNMS Group. 2011a. Features in OpenNMS 1.8 Stable Release Train. Viitattu 2.2.2012. http://www.opennms.org/wiki/Features_List

OpenNMS Group. 2011b. Main Page. Viitattu 2.2.2012. http://www.opennms.org/wiki/Main_Page

OpenNMS Group. 2011c. Vmware-evaluation. Viitattu 3.2.2012. http://www.opennms.org/wiki/Vmware-evaluation

OpenNMS Group. 2012a. Docu-overview. Viitattu 2.2.2012. http://www.opennms.org/wiki/Docu-overview

OpenNMS Group. 2012b. Tutorial Installation. Viitattu 3.2.2012. http://www.opennms.org/wiki/Tutorial_Installation

OpenNMS Group. n.d.a. Archive for the 'Customer Stories' Category. Viitattu 6.2.2012. http://www.opennms.com/category/testimonials/

OpenNMS Group. n.d.b. Get Support. Viitattu 2.2.2012. http://www.opennms.org/get-support/

OpenNMS Group. n.d.c. Installation:Debian. Viitattu 6.2.2012. http://www.opennms.org/wiki/Installation:Debian

OpenNMS Group. n.d.d. Welcome to the OpenNMS Demo. Viitattu 6.2.2012. http://demo.opennms.org/opennms/login.jsp

Pandora FMS. n.d.a. Community & support. Viitattu 3.2.2012. http://pandorafms.org/index.php?sec=project&sec2=support&lng=en

Pandora FMS. n.d.b. Demo On-line. Viitattu 3.2.2012. http://pandorafms.org/index.php?sec=project&sec2=demo&lng=en

Pandora FMS. n.d.c. Documentation. Viitattu 3.2.2012. http://pandorafms.org/index.php?sec=project&sec2=documentation&lng=en

Pandora FMS. n.d.d. Downloads. Viitattu 3.2.2012. http://pandorafms.org/index.php?sec=project&sec2=downloads&lng=en

Pandora FMS. n.d.e. Who uses Pandora FMS? Viitattu 3.2.2012. http://pandorafms.org/index.php?sec=project&sec2=who_uses_pandora&lng=en

Pandora FMS Administrator's guide v4.0. 2011. Artica Soluciones Tecnológicas. Viitattu 3.2.2012. http://sourceforge.net/projects/pandora/files/Pandora%20FMS%204.0/Final/DOC/PandoraFMS_4.0_Manual_EN.pdf/download

Recommendation X.700. 1992. Management Framework for Open Systems Interconnection (OSI) for CCITT Applications. Geneve: International Telecommunication Union's Telecommunication Standardization Sector. Viitattu 14.1.2012.
http://www.itu.int/itu-t/recommendations/index.aspx?ser=X

RFC1213. 1991. Management Information Base for Network Management of TCP/IP-based internets: MIB-II. Fremont: Internet Engineering Task Force. Viitattu 26.1.2012. http://www.ietf.org/rfc/rfc1213.txt

RFC4502. 2006. Remote Network Monitoring Management Information Base Version 2. Fremont: Internet Engineering Task Force. Viitattu 27.1.2012. http://www.ietf.org/rfc/rfc4502.txt

Shinken. 2012a. start. Viitattu 6.2.2012.
http://www.shinken-monitoring.org/wiki/start

Shinken. 2012b. Welcome to the Shinken Documentation Wiki. Viitattu 6.2.2012. http://www.shinken-monitoring.org/wiki/

Shinken. n.d.a. Download. Viitattu 6.2.2012.
http://www.shinken-monitoring.org/download/

Shinken. n.d.b. Chapter 1. About Shinken. Viitattu 6.2.2012.
http://www.shinken-monitoring.org/wiki/official/about

Shinken. n.d.c. Features. Viitattu 6.2.2012.
http://www.shinken-monitoring.org/features/

Shinken. n.d.d. News. Viitattu 6.2.2012.
http://www.shinken-monitoring.org/category/news/

Shinken. n.d.e. Part II. Getting Started. Viitattu 6.2.2012.
http://www.shinken-monitoring.org/wiki/official/part-gettingstarted

Shinken. n.d.f. Project. Viitattu 7.2.2012.
http://www.shinken-monitoring.org/project/

Shinken. n.d.g. Screenshots. Viitattu 6.2.2012.
http://www.shinken-monitoring.org/screenshots/

Shinken. n.d.h. Welcome on Shinken WebUI-Beta.
Viitattu 6.2.2012. http://demo-shinken.web4all.fr/user/login

Shinken. n.d.i. What is in Shiken, not in Nagios...and vice versa. Viitattu 6.2.2012. http://www.shinken-monitoring.org/what-is-in-shinken-not-in-nagios-and-vice-versa/

Sourceforge. 2012a. OpenNMS. Viitattu 6.2.2012.
http://sourceforge.net/projects/opennms/files/OpenNMS/old/

Sourceforge. 2012b. Pandora FMS. Viitattu 3.2.2012. http://sourceforge.net/projects/pandora/files/

Sourceforge. 2012c. Zenoss. Viitattu 4.2.2012. http://sourceforge.net/projects/zenoss/files/

Sourceforge. n.d. Nagios. Viitattu 4.2.2012. http://nagios.svn.sourceforge.net/viewvc/nagios/nagioscore/trunk/Changelog?view=markup

STD59 (RFC2819). 2000. Remote Network Monitoring Management Information Base. Fremont: Internet Engineering Task Force. Viitattu 27.1.2012. http://www.ietf.org/rfc/rfc2819.txt

STD62 (RFC3411). 2002. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. Fremont: Internet Engineering Task Force. Viitattu 26.1.2012. http://www.ietf.org/rfc/rfc3411.txt

STD62 (RFC3416). 2002. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP). Fremont: Internet Engineering Task Force. Viitattu 24.1.2012. http://www.ietf.org/rfc/rfc3416.txt

The Cacti Group. n.d.a. About Cacti. Viitattu 3.2.2012. http://www.cacti.net/index.php

The Cacti Group. n.d.b. Documentation. Viitattu 3.2.2012. http://www.cacti.net/documentation.php

The Cacti Group. n.d.c. Download Cacti. Viitattu 3.2.2012. http://www.cacti.net/download_cacti.php

The Cacti Group. n.d.d. Index of /downloads. Viitattu 3.2.2012. http://www.cacti.net/downloads/

The Cacti Group. n.d.e. What is Cacti? Viitattu 3.2.2012. http://www.cacti.net/what_is_cacti.php

The syslog-ng Open Source Edition 3.3 Administrator Guide. 2012. BalaBit IT Security Ltd. Viitattu 2.2.2012. http://www.balabit.com/sites/default/files/documents/syslog-ng-ose-3.3-guides/syslog-ng-ose-v3.3-guide-admin-en.pdf

XMPP Standards Foundation. 2010. About. Viitattu 13.2.2012. http://xmpp.org/about-xmpp/

Zabbix SIA. 2012. Zabbix 1.8 Manual. Viitattu 3.2.2012. http://www.zabbix.com/documentation/1.8/complete

Zabbix SIA. n.d.a. Documentation. Viitattu 3.2.2012. http://www.zabbix.com/documentation.php

Zabbix SIA. n.d.b. Download. Viitattu 3.2.2012.
http://www.zabbix.com/download.php

Zabbix SIA. n.d.c. Download old releases. Viitattu 3.2.2012.
http://www.zabbix.com/download2.php

Zabbix SIA. n.d.d. Features. Viitattu 3.2.2012.
http://www.zabbix.com/features.php

Zenoss Administration. 2010. Annapolis: Zenoss Inc. pdf-tiedosto. Viitattu 4.2.2012.
http://community.zenoss.org/community/documentation/official_documentation/zenoss-guide

Zenoss Core Installation. 2010. Annapolis: Zenoss Inc. Viitattu 4.2.2012.
http://switch.dl.sourceforge.net/project/zenoss/Documentation/zenoss-3.0.x-docs/zendocs-3.0.3/Zenoss_Core_Installation_04-102010-3.0-v05.pdf

Zenoss Inc. 2008. Procurve switches Viitattu 22.3.2012.
http://community.zenoss.org/thread/4264?decorator=print&displayFullThread=true

Zenoss Inc. 2009. Zenperfsnmp and Cisco subinterfaces.
Viitattu 22.3.2012. http://community.zenoss.org/message/35188

Zenoss Inc. 2011. Polling Interface Status. Viitattu 22.3.2012.
community.zenoss.org/docs/DOC-2494

Zenoss Inc. n.d.a. About Zenoss. Viitattu 4.2.2012.
http://community.zenoss.org/community/documentation

Zenoss Inc. n.d.b. Documentation. Viitattu 4.2.2012.
http://community.zenoss.org/community/about

Zenoss Inc. n.d.c. Downloads. Viitattu 4.2.2012.
http://community.zenoss.org/docs/DOC-3240?noregister

Zenoss Inc. n.d.d. Partners. Viitattu 4.2.2012.
http://community.zenoss.org/community/partners

Zenoss Inc. n.d.e. Success Stories. Viitattu 4.2.2012.
http://community.zenoss.org/community/about/success_stories

Zenoss Inc. n.d.f. ZenPacks. Viitattu 6.4.2012.
http://community.zenoss.org/community/zenpacks

OHJELMISTOJEN KOKONAISVERTAILU

Taustatiedot ja kattavuus

Ominaisuus	AlienVault OSSIM	Cacti	Centreon	Nagios Core	OpenNMS	Pandora FMS	Shinken	syslog-ng	Zabbix	Zenoss Core
Vertailtava versio	3.1	0.8.7i	2.3.4	3.3.1	1.8.17	4.0.1	0.8.1	3.3	1.8.10	3.2.1
Tukija	AlienVault	-	Merethis	Nagios Enterprises	OpenNMS Group	Ártica Soluciones Tecnológicas	-	BalaBit IT Security	Zabbix SIA	Zenoss Inc.
Käyttösuositus	tunkeutumisen esto	tiedon graafinen esittäminen	verkonvalvonta	verkonvalvonta	verkonvalvonta	verkonvalvonta	verkonvalvonta	lokien keräys ja keskitetty taltiointi	verkonvalvonta	verkonvalvonta
Käyttötarkoitus										
– automaattinen tunnistaminen	x	-	-	-	x	x	x	-	x	x
– lokit	x	x	x	x	x	x[a]	x	x	x	x
– suorituskyky	x	x	x	x	x	x	x	-	x	x
– liikennemäärä	x	x	x	x	x	x	x	-	x	x
– analysointi	x	x	x	x	x	-	x	-	x	x
Referenssit	mm. Telefonica, Metro de Madrid, Spanish Army, Los Angelesin, Marquette University	-	mm. IBM, Thales, Zeiss, BT, Fraunhofer	mm. American Public Media, DHL, Linksys, McAfee, Telia, Siemens, Sony, Philips	The Pennsylvania State Milton S. Hershey Medical Center, City of Grapevine, Texas	-	-	Allianz Hungary Insurance Co., Navisite Inc., Svenska Handelsbanken AB, Swedish National Debt Office	-	Geeknet, Competitive Local Exchange Carriers (CLEC), International Broadcast Corporation, webAJ

Huomautukset
a Vain pieniä määriä

Tuotteistus

Ominaisuus	AlienVault OSSIM	Cacti	Centreon	Nagios Core	OpenNMS	Pandora FMS	Shinken	syslog-ng	Zabbix	Zenoss Core
julkaisuväli	6–10 kk	3 v	4–24 kk	6–10 kk	yli 1 v	6–12 kk	2–4 kk	6–24 kk	1 v	4–6 kk
online demo	-[b]	-	x	-	x	x	x	-	-	-
asennusvaihtoehdot										
– iso-tiedosto	x	-	-	-	-	x	-	-	x[c]	-
– sovelluspaketti	-	x	x	x	x	x	x	x	x	x
– asennusohjelma	-	-	-	-	-	-	-	x		x
– oletuksena käyttöjärjestelmässä	-	-	-	-	-	-	-	x	-	-
– virtuaalikone	-	-	-	-	x[c]	x	x[d]	-	x[c]	x
muiden sovelluksien tarve	-	RRDTool, MySQL, PHP, www-palvelin	MySQL, Apache, PHP, Perl	Web-palvelin	SQL ,Oracle Java Development Kit	MySQL, Perl	Python	SQL	tietokantasovellus, Apache, PHP	MySQL
dokumentaation kattavuus										
– järjestelmäkuvaus	x	-	x[e]	x	-	x	x	x	x	x
– vaatimukset	x	x	-	x	x	x	x	x	x	x
– asentaminen	x	x	x	x	x	x	x	x	x	x
– perusasetukset	x	x	x	x	x	x	x	x	x	x
dokumentointitapa										
– html	x	x	-	x	x	x	x	x	x	x
– pdf	x	x	x	x	-	x	-	x	x[f]	x
maksullisen tuen saatavuus	x	-	x	x	x	x	-	x	x	x
rinnalla maksullinen versio	x	-	x	x	-	x	-	x	-	x

Huomautukset

b Maksulliseen versioon löytyy
c Vain testikäyttöön
d Vertailuhetkellä vanhentunut
e Löytyy erikseen kotisivuilta
f Vain vanhemmat versiot, uudemmat tulostettavissa

Tekniset ominaisuudet

Ominaisuus	AlienVault OSSIM	Cacti	Centreon	Nagios Core	OpenNMS	Pandora FMS	Shinken	syslog-ng	Zabbix	Zenoss Core
suorituskyky	miljoonia tapahtumia päivässä	?	?	?	?	?	Yli 100000 tarkastusta/ 5min	500000 viestiä sekunnissa, 24GB raakada-taa tunnissa	?	?
käyttöliittymävaihtoehdot										
– komentorivi	-	x	-	x	-	-	-	x	-	-
– selain	x	x	x	x[g]	x	x	x	-	x	x
tiedonkeruumenetelmät										
– agentiton	x	x	x	x	x	x	x	-	x	x
– agentti	x	-	x	x	x	x	x	x	x	-
– SNMP	x	x	x	x	x	x	x	-	x	x
kerätyn tiedon käsittely	tapahtumien luokittelu, korrelointi ja normalisointi, verkkojen profilointi	?	?	?	tapahtumien korrelointi ja normalisointi	tapahtumien normalisointi	tapahtumien korrelointi	luokittelu, korrelointi ja jäsentely	?	tapahtumien korrelointi ja normalisointi
tiedon taltiointi										
– tietokanta	MySQL	MySQL+RRD	MySQL	-	PostgreSQL	MySQL	-	MSSQL, MySQL, Oracle, Post-greSQL tai SQLite	IBM DB2, MySQL, Oracle, Post-greSQL tai SQLite	MySQL+RRD
– tiedostot	-	-	-	x	-	-	x	-	-	-

Huomautukset
g Lähinnä tiedon lukemiseen, asetukset komentoriviltä tiedostoihin

(jatkuu)

(jatkuu)

Ominaisuus	AlienVault OSSIM	Cacti	Centreon	Nagios Core	OpenNMS	Pandora FMS	Shinken	syslog-ng	Zabbix	Zenoss Core
tiedon esittäminen										
– graafit	x	x	x	x	x	x	x	-	x	x
– taulukot	x	x	x	x	x	x	x	-	x	x
– verkkokartta	x	-	-	-	x	x	x	-	x	x
– tikettijärjestelmä	x	-	x	-	x	-	-	-	-	-
– raportin tallennus	pdf, HTML, Excel, Word, csv, NBE	HTML, kuva	csv	-	XML	-	-	-	XML	XML, csv
hälytysmenetelmät										
– sähköposti	x	-	x	x	x	x	x	-	x	x
– XMPP	-	-	-	-	x	x	-	-	x	-
– tekstiviesti	-	-	x	x	-	x	x	-	x	-
– komentosarja	-	-	-	x	x	x	x	-	x	-
– hakulaite	-	-	-	x	x	-	x	-	-	x
Muuta	käyttää syslog-ng:tä ja Nagiosta		Nagiokseen perustuva	paljon liitännäisiä saatavilla	käyttää Nagioksen liitännäisiä	mahdollisuus liittää myös fyysisiä agentteja	Nagiokseen perustuva	sisältyy AlienVaultin metodeihin		mahdollisuus käyttää Nagios- ja Cacti-liitännäisiä

Vertailussa käytetyt lähteet

AlienVault OSSIM
- AlienVault LC 2012a
- AlienVault LC 2012b
- AlienVault LC 2012c
- AlienVault LC n.d.a
- AlienVault LC n.d.b
- AlienVault LC n.d.c
- AlienVault Unified SIEM. System Description. Version 1.0 n.d
- Lorenzo n.d.a
- Lorenzo n.d.b

Cacti
- Berry ym. 2010
- The Cacti Group n.d.a
- The Cacti Group n.d.b
- The Cacti Group n.d.c
- The Cacti Group n.d.d
- The Cacti Group n.d.e

Centreon
- Centreon n.d.a
- Centreon n.d.b
- Centreon n.d.c
- Centreon n.d.d
- Centreon n.d.e
- Centreon n.d.f
- Centreon n.d.g
- Centreon n.d.h
- Centreon n.d.i
- Centreon n.d.j
- Centreon n.d.k

Nagios Core
- Nagios Core Version 3.x Documentation 2010
- Nagios Enterprises LLC n.d.a
- Nagios Enterprises LLC n.d.b
- Nagios Enterprises LLC n.d.c
- Nagios Enterprises LLC n.d.d
- Nagios Enterprises LLC n.d.e
- Nagios Enterprises LLC n.d.f
- Sourceforge n.d.

OpenNMS
- OpenNMS Group 2011a
- OpenNMS Group 2011b
- OpenNMS Group 2011c
- OpenNMS Group 2012a
- OpenNMS Group 2012b
- OpenNMS Group n.d.a
- OpenNMS Group n.d.b
- OpenNMS Group n.d.c
- OpenNMS Group n.d.d
- Sourceforge 2012a

Pandora FMS
- Pandora FMS Administrator's guide v4.0 2011
- Pandora FMS n.d.a
- Pandora FMS n.d.b
- Pandora FMS n.d.c
- Pandora FMS n.d.d
- Pandora FMS n.d.e
- Sourceforge 2012b

Shinken
- Shinken 2012a
- Shinken 2012b
- Shinken n.d.a
- Shinken n.d.b
- Shinken n.d.c
- Shinken n.d.d
- Shinken n.d.e
- Shinken n.d.g
- Shinken n.d.h
- Shinken n.d.i

syslog-ng
- BalaBit IT Security Ltd n.d.a
- BalaBit IT Security Ltd n.d.b
- BalaBit IT Security Ltd n.d.c
- BalaBit IT Security Ltd n.d.d
- BalaBit IT Security Ltd n.d.e
- The syslog-ng Open Source Edition 3.3 Administrator

Zabbix
- Zabbix SIA 2012
- Zabbix SIA n.d.a
- Zabbix SIA n.d.b
- Zabbix SIA n.d.c
- Zabbix SIA n.d.d

Zenoss Core
- Sourceforge 2012c
- Zenoss Administration 2010
- Zenoss Core Installation 2010
- Zenoss Inc n.d.a
- Zenoss Inc n.d.b
- Zenoss Inc n.d.c
- Zenoss Inc n.d.d
- Zenoss Inc n.d.e

ALIENVAULTIN ASETUKSET TESTAUKSEN AIKANA

Testauksen aikana käytettiin ohjelmiston oletusasetuksia pois lukien alla olevat poikkeukset.

Komentoriviltä tehdyt asetukset

ossim-setup-komennolla avautuvan valikon kautta tehdyt muutokset

- Configure Network: testiympäristön verkot
- Enable detector plug-ins (lisättiin): apache, cisco-router, dhcp, nagios, nessus, nessus-detectors, netscreen-firewall, netscreen-manager, syslog.

Tiedosto /etc/ossim/ossim_setup.conf
Tiedostoon muutettiin alla olevat tiedot:

```
admin_ip: 192.168.10.3
framework_ip: 192.168.10.3
domain=testi.local
email_notify=muser1@testi.local
mailserver_relay=192.168.10.2
mailserver_relay_port=25
ntp_server=192.168.12.1
```

Tiedosto /var/ossec/bin/manage_agent
Tiedostoon tehtiin seuraavat muutokset:

- lisätty agentti:
  *hostname: jodium
  *IP-address: 192.168.10.2
  *ID: 002
- extract key for agent 002
- lisätty agentti:
  *hostname: natrium
  *IP-address: 192.168.11.3
  *ID: 003
- extract key for agent 003

AlienVaultin asetukset selaimelta

Valvottavat verkot

- testiympäristön verkot
- kaikille verkoille: Enable Nagios

Valvottavat laitteet

- etsintä Nmapilla (Assets > Asset Discovery)
  - *Full Scan
  - *Normal
- kaikille laitteille: Enable Nagios
- RRD Profile
  - *verkkolaitteille: Default
  - *palvelimille: Server

Sähköpostipalvelimen asetukset

- From Address: tätä varten luotu sähköpostiosoite
- SMTP Server IP Address: Windows-palvelimen osoite
- SMTP Server Port: 25

Hälytysasetukset

- Policy:
  - *Source: Any
  - *Destination: Any
  - *Port Group: Any
  - *DS Group: Availability, Level Info 0, Level Info 1, Level Info 2, Windows Events
  - *Sensors: Any
  - *Time Range Mon 0h - Sun 23 h
  - *Targets: Any
  - *Set Priority: 5
- Action:
  - *email
  - *ticket

Nagios-asetukset

Nagioksen asetustiedostoihin tehtiin useita muutoksia ja luotiin myös uusia tiedostoja. Asetustiedoston rivin jatkuminen tässä tekstissä toisella rivillä on merkitty \-merkillä.

Tiedostoon /etc/nagios3/nagios.cfg
Tiedoston eräs rivi muokattiin alla olevan mukaiseksi.

```
cfg_dir=/etc/nagios3/conf.d
```

Tiedostoon /etc/nagios3/commands.cfg
Tiedostoon lisättiin määritelmä

```
define command{
        command_name          check_nrpe
        command_line          $USER1$/check_nrpe -H \
                              $HOSTADDRESS$ -c $ARG1$
        }
```

Kansio /etc/nagios3/conf.d
Kansioon luotiin alla olevat tiedostot sisältöineen:

- generic-switch.cfg

```
define host{
        name                  generic-switch
        use                   generic-host
        check_period          24x7
        check_interval        5
        retry_interval        1
        max_check_attempts    10
        check_command         check-host-alive
        notification_period   24x7
        notification_interval 30
        notification_options  d,r
        contact_groups        admins
        register              0
        }
```

- generic-server.cfg

```
define host{
        name                  windows-server
        use                   generic-host
        check_period          24x7
        check_interval        5
        retry_interval        1
        max_check_attempts    10
        check_command         check-host-alive
        notification_period   24x7
        notification_interval 30
        notification_options  d,r
        contact_groups        admins
        hostgroups            Windows-servers
        register              0
        }
```

```
define host{
        name                    linux-server
        use                     generic-host
        check_period            24x7
        check_interval          5
        retry_interval          1
        max_check_attempts      10
        check_command           check-host-alive
        notification_period     workhours
        notification_interval   120
        notification_options    d,u,r
        contact_groups          admins
        register                0
        }
```

– switch.cfg

```
define host{
        use                     generic-switch
        host_name               Kytkin_Nagios
        alias                   Kytkin
        address                 192.168.5.2
        hostgroups              switches
        }
define hostgroup{
        hostgroup_name          switches
        alias                   Network Switches
        }
define service{
        use                     generic-service
        host_name               Kytkin_Nagios
        service_description     PING
        check_command       check_ping!200.0,20%!600.0,60%
        normal_check_interval 5
        retry_check_interval  1
        }
define service{
        use                     generic-service
        host_name               Kytkin_Nagios
        service_description     Uptime
        check_command check_snmp!-C public -o sysUpTime.0
        }
define service{
        use                     generic-service
        host_name               Kytkin_Nagios
        service_description     Port 16 Link Status
        check_command           check_snmp!-C public -o \
                      ifOperStatus.16 -r 1 -m RFC1213-MIB
        }
define service{
        use                     generic-service
        host_name               Kytkin_Nagios
        service_description     Port 13 Link Status
        check_command           check_snmp!-C public -o \
                        ifOperStatus.13 -r 1 RFC1213-MIB
        }
```

```
define service{
        use                     generic-service
        host_name               Kytkin_Nagios
        service_description     Port 17 Link Status
        check_command           check_snmp!-C public -o \
                              ifOperStatus.17 -r 1 RFC1213-MIB
        }
define service{
        use                     generic-service
        host_name               Kytkin_Nagios
        service_description     Disk Space
        check_command           check_all_disks!20%!10%
        }
define service{
        use                     generic-service
        host_name               Kytkin_Nagios
        service_description     Current Users
        check_command           check_users!20!50
        }
define service{
        use                     generic-service
        host_name               Kytkin_Nagios
        service_description     Total Processes
        check_command           check_procs!250!400
        }
define service{
        use                     generic-service
        host_name               Kytkin_Nagios
        service_description     Current Load
        check_command check_load!5.0!4.0!3.0!10.0!6.0!4.0
        }
```

– router.cfg

```
define host{
        use                     generic-switch
        host_name               Reititin_Nagios
        alias                   Reititin
        address                 192.168.10.1
        hostgroups              switches
        }
define hostgroup{
        hostgroup_name          routers
        alias                   Network Routers
        }
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     PING
        check_command       check_ping!200.0,20%!600.0,60%
        normal_check_interval 5
        retry_check_interval  1
        }
```

```
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     Uptime
        check_command check_snmp!-C public -o sysUpTime.0
        }
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     Port 1 Link Status
        check_command           check_snmp!-C public -o \
                        ifOperStatus.1 -r 1 -m RFC1213-MIB
        }
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     Port 1 Link Status
        check_command           check_snmp!-C public -o \
                        ifOperStatus.2 -r 1 -m RFC1213-MIB
        }
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     Port 1 Bandwidth Usage
        check_command check_local_mrtgtraf!/var/log/mrtg\
                /192.168.10.1_1.log!AVG!1000000,1000000!\
                5000000,5000000!10
        }
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     Disk Space
        check_command           check_all_disks!20%!10%
        }
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     Current Users
        check_command           check_users!20!50
        }
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     Total Processes
        check_command           check_procs!250!400
        }
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     Current Load
        check_command check_load!5.0!4.0!3.0!10.0!6.0!4.0
        }
```

– firewall.cfg

```
define host{
        use                     generic-switch
        host_name               Palomuuri_Nagios
        alias                   Palomuuri
        address                 192.168.12.1
        hostgroups              switches
        }
define service{
        use                     generic-service
        host_name               Palomuuri_Nagios
        service_description     PING
        check_command check_ping!200.0,20%!600.0,60%
        normal_check_interval 5
        retry_check_interval  1
        }
define service{
        use                     generic-service
        host_name               Reititin_Nagios
        service_description     Uptime
        check_command check_snmp!-C public -o sysUpTime.0
        }
define service{
        use                     generic-service
        host_name               Palomuuri_Nagios
        service_description     Port 1 Link Status
        check_command           check_snmp!-C public -o \
                        ifOperStatus.1 -r 1 -m RFC1213-MIB
        }
define service{
        use                     generic-service
        host_name               Palomuuri_Nagios
        service_description     Port 2 Link Status
        check_command           check_snmp!-C public -o \
                        ifOperStatus.2 -r 1 -m RFC1213-MIB
        }
define service{
        use                     generic-service
        host_name               Palomuuri_Nagios
        service_description     Port 1 Bandwidth Usage
        check_command check_local_mrtgtraf!/var/lib/mrtg\
                /192.168.10.1_1.log!AVG!1000000,1000000!\
                5000000,5000000!10
        }
define service{
        use                     generic-service
        host_name               Palomuuri_Nagios
        service_description     Disk Space
        check_command           check_all_disks!20%!10%
        }
```

```
define service{
        use                     generic-service
        host_name               Palomuuri_Nagios
        service_description     Current Users
        check_command           check_users!20!50
        }
define service{
        use                     generic-service
        host_name               Palomuuri_Nagios
        service_description     Total Processes
        check_command           check_procs!250!400
        }
define service{
        use                     generic-service
        host_name               Palomuuri_Nagios
        service_description     Current Load
        check_command check_load!5.0!4.0!3.0!10.0!6.0!4.0
        }
```

- windows.cfg

```
define host{
        use                     windows-server
        host_name               Windows-palvelin_Nagios
        alias                   Windows-palvelin
        address                 192.168.10.2
        }
define hostgroup{
        hostgroup_name          windows-servers
        alias                   Windows Servers
        }
define service{
        use                     generic-service
        host_name               Windows-palvelin_Nagios
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }
define service{
        use                     generic-service
        host_name               Windows-palvelin_Nagios
        service_description     Uptime
        check_command           check_nt!UPTIME
        }
define service{
        use                     generic-service
        host_name               Windows-palvelin_Nagios
        service_description     CPU Load
        check_command           check_nt!CPULOAD! \
                                -l 5,80,90,10,80,90
        }
define service{
        use                     generic-service
        host_name               Windows-palvelin_Nagios
        service_description     C:\ Drive Space
        check_command           check_nt!USEDDISKSPACE!\
                                -l c -w 80 -c 90
        }
```

– linux.cfg

```
define host{
        use                     linux-server
        host_name               Linux-palvelin_Nagios
        alias                   Linux-palvelin
        address                 192.168.11.3
        }
define service{
        use                     generic-service
        host_name               Linux-palvelin_Nagios
        service_description     CPU Load
        check_command           check_nrpe!check_load
        }
define service{
        use                     generic-service
        host_name               Linux-palvelin_Nagios
        service_description     /dev/sda2 Free Space
        check_command           check_nrpe!check_sda2
        }
```

Tiedosto check_nrpe
Tiedosto kopioitiin kansiosta /usr/local/nagios/libexec kansioon /usr/lib/nagios/plugins.

MRTG-asetukset

Asetustiedoston rivin jatkuminen tässä tekstissä toisella rivillä on merkitty \-merkillä.

MRTG-lisäosan käyttöönottamiseksi luotiin kansio /var/www/html/mrtg ja siirrettiin tiedosto mrtg.cfg kansiosta /etc kansioon /etc/mrtg.

Tiedoston mrtg.cfg muutokset

```
RunAsDaemon: yes
Interval: 5
LogDir: /var/log/mrtg
```

Asetusten viimeistelemiseksi suoritetut komennot

```
cfgmaker --global 'WorkDir:/var/www/mrtg' -global \
'Options[_]: bits,growright' -output /etc/mrtg/mrtg.cfg \
public@192.168.10.1
indexmaker --output=/var/www/mrtg/index.html \
/etc/mrtg/mrtg.cfg
env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg
```

Ajoitetun tehtävän luominen
Lopuksi annetttiin komento cron ja lisättiin seuraava rivi:

```
0,50,10,15,20,25,30,35,40,45,50,55 * * * * env LANG=C \
/usr/bin/mrtg /etc/mrtg/mrtg.cfg --logging \
/var/log/mrtg.log
```

ZENOSSIN ASETUKSET TESTAUKSEN AIKANA

Komponenttien säätäminen ennen valvonnan aloittamista

ZEO-tietokannan ajoitettu pakkaaminen
Käyttäjänä zenoss annettiin komento cron ja lisättiin seuraavat rivit:

```
#Pack database every Monday morning at 2am
0 2 * * 1 bash -lc "$ZENHOME/bin/zeopack.py -h localhost \
-p 8100 >> /tmp/logfile.log 2>&1"
```

Asetustiedoston rivin jatkuminen tässä tekstissä toisella rivillä on merkitty \-merkillä.

MySQL-tietokannan asetusten muokkaaminen
Tiedostoon /etc/mysql/my.cnf lisättiin rivit:

```
innodb_buffer_pool_size = 256M
innodb_additional_mem_pool_size = 32M
```

Ohjeessa poluksi mainitaan /etc/my.cnf, mutta tässä tapauksessa oikea polku oli yllä oleva (Zenoss Core Installation 2010, 28).

Zope-sovelluspalvelimen asetusten muokkaaminen
Tiedostoon /usr/local/zenoss/zenoss/etc/zope.conf lisättiin rivit ennen kohtaa `<zodb_db main>`:

```
server-threads 4
python-check-interval 1500
```

Saman tiedoston alla olevaan kohtaan lisättiin lukuarvot.

```
<zodb_db main>
  ...
  cache-size 10000
  <zeoclient>
    ...
    cache-size 100 MB
    ...
```

Käytetyt arvot määritettiin ohjeen mukaan (Zenoss Core Installation 2010, 29–30).

Testiympäristössä käytetyt asetukset

Testauksen aikana käytettiin ohjelmiston oletusasetuksia pois lukien alla mainitut asetukset.

Käytetyt laiteluokat laitteittain:
- palomuuri: /Network/FireWall, lisätty template Juniper Performance
- reititin:/Network/Router/Cisco
- kytkin:/Network/Switch/HP, lisätty template HP Procurve
- Windows-palvelin: /Server/Windows/2 Processors
- Linux-palvelin: /Server/Linux

Asennetut ZenPackit:
- ZenPacks.community.JuniperPerformance-1.0-py2.6.egg
- ZenPacks.Nova.WinServiceSNMP-1.0-py2.6.egg, josta memory threshold value poistettiin, virheilmoituksen vuoksi
- ZenPacks.Nova.Windows.SNMPPerfMonitor-1.6-py2.6.egg
- ZenPacks.networking.HPProcurve-1.1.egg

Hälytyssääntö testikäyttäjälle:
- Enabled: True
- Severity: Info
- Send clear messages: True

Muut asetukset:
- SMTP Host: Windows-palvelimen koko domain-nimi
- From Address for Emails: tätä varten luotu sähköpostiosoite
- zopeurl: http://192.168.10.5:8080
- Event/Status/IpInterface --> Transform (ei toiminut)

```
if evt.summary.startswith('treshold of operational sta-
tus '):
        if evt.severity > 0:
          evt.summary = "interface operationally down"
          evt.message = "interface operationally down"
        else:
          evt.summary = "interface operationally up"
          evt.message = "interface operationally up"
```

- ethernetCsmacd ja ethernetCsmacd_64
  *Data Source: ifOperStatus
    - RRDmin 0
    - RRDmax 10
  *MinMaxTreshold: operational status
    - min value 1
    - max value 1

TESTAUSSUUNNITELMA

ID	Testitapaus	Liittyy	Tutkimuskysymys	Testaustapa
1	Laitteiden löytäminen	Valvonnan aloittaminen	Löytääkö ohjelmisto verkkolaitteet ja palvelimet automaattisesti vai onko ne lisättävä manuaalisesti?	Etsitään kohdelaitteet ohjelmistokohtaisen ohjeen mukaan.
2	Verkon kokoonpanon esittäminen	Tiedon esittäminen	Pystyykö ohjelmisto esittämään verkon rakenteen graafisesti?	Laitteiden lisäämisen jälkeen tarkastetaan käyttöliittymän esitystavat.
3	Ohjelmiston asetusten muokkaaminen	Valvonnan aloittaminen ja ohjelmiston käyttö	Onnistuuko ohjelmiston asetusten muokkaaminen pelkästään selainkäyttöliittymästä?	Havainnoidaan muiden kohtien ohessa.
4	Laitteiden perus-parametrien valvonta	Suorituskyvyn hallinta	Pystyykö ohjelmisto valvomaan laitteen kuormitusta ja levytilaa reaaliaikaisesti?	Tarkastetaan, voidaanko ohjelmiston asetuksia muokata siten, että kohdelaitteen prosessorin, muistin ja levytilan käyttöön liittyvää tietoa esitetään joko numeerisessa tai graafisessa muodossa ajan suhteen.
5a	Verkkolaitteen liitäntöjen valvonta	Vikojen hallinta	Pystyykö ohjelmisto valvomaan verkkolaitteen tilaa liitäntäkohtaisesti?	Tarkastetaan, voidaanko ohjelmiston asetuksia muokata siten, että kohdelaitteen liitäntöjen tila esitetään joko tekstinä tai symbolina.
5b	Palvelimen palveluiden valvonta	Vikojen hallinta	Pystyykö ohjelmisto valvomaan laitteen palveluiden tilaa?	Tarkastetaan, voidaanko ohjelmiston asetuksia muokata siten, että kohdelaitteessa käytössä olevien palveluiden tila esitetään joko tekstinä tai symbolina.

(jatkuu)

(jatkuu)

ID	Testitapaus	Liittyy	Tutkimuskysymys	Testaustapa
6	Verkko-segmentin kuormituksen valvonta	Suorituskyvyn hallinta	Pystyykö ohjelmisto seuraamaan verkkosegmentin kokonaisliikennemäärää?	Tarkastetaan, voidaanko ohjelmiston asetuksia muokata siten, että valvottavan verkkosegmentin kokonaisliikennemäärä esitetään joko numeerisesti tai graafisesti.
7a	Verkkolaitteen vikaantumisen valvonta	Vikojen hallinta	Pystyykö ohjelmisto havaitsemaan reaaliaikaisesti verkkolaitteen vikaantumisen?	Sammutetaan palomuuri ja tarkkaillaan ohjelmiston toimintaa.
7b	Yhteyskatkoksen havaitseminen	Vikojen hallinta	Pystyykö ohjelmisto havaitsemaan reaaliaikaisesti yhteyskatkoksen?	Irrotetaan kaapeli yhdestä kytkimen liitännästä ja tarkkaillaan ohjelmiston toimintaa.
7c	Palvelukatkoksen havaitseminen	Vikojen hallinta	Pystyykö ohjelmisto havaitsemaan reaaliaikaisesti palvelun katkeamisen?	Pysäytetään Linux-palvelimen Apache-palvelu ja Windows-palvelimen DHCP-palvelu, jonka jälkeen tarkkaillaan ohjelmiston toimintaa.
8	Hälytyksen välittäminen sähköpostiin	Vikojen hallinta	Pystyykö ohjelmisto välittämään hälytyksen haluttuun sähköpostiosoitteeseen kohdan 7 tapahtumista?	Tarkastetaan, voidaanko ohjelmiston asetuksia muokata siten, että halutuista tapahtumista ilmoitetaan sähköpostitse.
9	Tiedon esittäminen	Suorituskyvyn hallinta/Vikojen hallinta	Miten ohjelmisto pystyy esittämään tietoa muihin kohtiin liittyen?	Tutkitaan ohjelmiston raportointitapoja muihin kohtiin liittyen.
10	Raporttien vienti ohjelmistosta	Raportointi	Miten ohjelmistosta voi viedä raportin ulos?	Tarkastetaan, voidaanko ohjelmiston tuottamia raportteja tallentaa XML-, HTML-, pdf- , csv- tai toimistosovellusten käyttämässä tiedostomuodossa.

TESTAUKSEN TULOKSET

ID	Testitapaus	Tutkimuskysymys	AlienVault	Zenoss
1	Laitteiden löytäminen	Löytääkö ohjelmisto verkkolaitteet ja palvelimet automaattisesti vai onko ne lisättävä manuaalisesti?	Kyllä. Etsintää varten määritettiin verkot, joista etsitään ja kuinka yksityiskohtaisesti laitteita tutkitaan.	Kyllä. Etsintää varten määritettiin verkot, joista etsitään ja menetelmäksi valittiin SNMP.
2	Verkon kokoonpanon esittäminen	Pystyykö ohjelmisto esittämään verkon rakenteen graafisesti?	Ei	Kyllä. Rakenne esitettiin korkeintaan verkkosegmentti kerrallaan.
3	Ohjelmiston asetusten muokkaaminen	Onnistuuko ohjelmiston asetusten muokkaaminen pelkästään selainkäyttöliittymästä?	Ei. Sensorin asetukset, verkkoasetukset ja Nagioksen asetukset on tehtävä komentorivillä.	Ei. Ohjelmiston asentamisen jälkeen tehtävät säätötoimenpiteet oli suoritettava komentorivillä, kuten koko ohjelmiston uudelleenkäynnistys.
4	Laitteiden perusparametrien valvonta	Pystyykö ohjelmisto valvomaan laitteen kuormitusta ja levytilaa reaaliaikaisesti?	Kyllä. Windows-palvelimen valvonta onnistui ainoastaan komentoriviltä. Ongelma johtui todennäköisesti käytetystä agentista.	Kyllä. Kytkimen valvonta ei onnistunut. Ongelma johtui todennäköisesti käytetystä kytkimestä.
5a	Verkkolaitteen liitäntöjen valvonta	Pystyykö ohjelmisto valvomaan verkkolaitteen tilaa liitäntäkohtaisesti?	Kyllä. Liitännän kuormitustietoa ei saatu näkyviin. Ongelma johtui todennäköisesti ratkaisemattomista käyttöoikeusrajoituksista.	Kyllä. Liitännän tilan muutokset näkyvät vain Tapahtumat-välilehdellä.
5b	Palvelimen palveluiden valvonta	Pystyykö ohjelmisto valvomaan laitteen palveluiden tilaa?	Kyllä.	Kyllä.

(jatkuu)

(jatkuu)

ID	Testitapaus	Tutkimuskysymys	AlienVault	Zenoss
6	Verkko-segmentin kuormituksen valvonta	Pystyykö ohjelmisto seuraamaan verkkosegmentin kokonaisliikennemäärää?	Kyllä.	Ei pystytty todentamaan kytkimeen liittyneiden ongelmien vuoksi.
7a	Verkkolaitteen vikaantumisen valvonta	Pystyykö ohjelmisto havaitsemaan reaaliaikaisesti verkkolaitteen vikaantumisen?	Kyllä.	Kyllä.
7b	Yhteyskatkoksen havaitseminen	Pystyykö ohjelmisto havaitsemaan reaaliaikaisesti yhteyskatkoksen?	Kyllä.	Kyllä.
7c	Palvelukatkoksen havaitseminen	Pystyykö ohjelmisto havaitsemaan reaaliaikaisesti palvelun katkeamisen?	Kyllä. Windows-palvelin todennettiin sähköpostipalvelulla, DHCP ei ollut seurannassa oletuksena eikä sitä ehditty määrittämään seurattavaksi.	Kyllä.
8	Hälytyksen välittäminen sähköpostiin	Pystyykö ohjelmisto välittämään hälytyksen haluttuun sähköpostiosoitteeseen kohdan 7 tapahtumista?	Kyllä. Hälytyssääntöjä pystyi muokkaamaan useamman eri parametrin suhteen.	Kyllä. Hälytyssäännöt olivat käyttäjäkohtaisia.
9	Tiedon esittäminen	Miten ohjelmisto pystyy esittämään tietoa muihin kohtiin liittyen?	Listauksena värikoodein kuormitus, laitteiden, liitäntöjen ja palveluiden tila sekä graafeina verkon kuormitus.	Listauksena laitteiden, liitäntöjen ja palveluiden tila sekä graafeina kuormitus- ja käyttöastetiedot.
10	Raporttien vienti ohjelmistosta	Miten ohjelmistosta voi viedä raportin ulos?	Raportit joko rtf- tai pdf-tiedostona. Jälkimmäisen voi lähettää suoraan sähköpostitse. Saatavuustiedot csv-muodossa (ei tallennu suoraan tiedostoon).	Tapahtumat joko XML- tai csv-tiedostona, raportit csv-tiedostona.