



JÄRJESTELMIEN VALVONNAN SUUNNITTELU JA TOTEUTUS

Ilkka Rautiainen

Opinnäytetyö

Syyskuu 2009

Teknologiayksikkö



**JYVÄSKYLÄN
AMMATTIKORKEAKOULU**

Tekijä(t) RAUTIAINEN, Ilkka	Julkaisun laji Opinnäytetyö	
	Sivumäärä 91	Julkaisun kieli suomi
	Luottamuksellisuus <input type="checkbox"/> Salainen _____ saakka	
Työn nimi JÄRJESTELMIEN VALVONNAN SUUNNITTELU JA TOTEUTUS		
Koulutusohjelma Tietoverkkotekniikan koulutusohjelma		
Työn ohjaaja(t) RANTONEN, Mika		
Toimeksiantaja(t) Pieksämäen kaupunki TIKKANEN, Tommi		
Tiivistelmä <p>Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa Pieksämäen kaupungille valvontajärjestelmä valvonnan ulkopuolella olleille verkon laitteille, joista suurin osa oli Windows-palvelimia. Työssä vertailtiin neljää avointa valvontaohjelmistoa. Toteutusta varten valittiin Zenoss Core -valvontaohjelma, joka asennettiin Debian GNU/Linux -käyttöjärjestelmään. Valvottavat laitteet liitettiin valvontaohjelmaan ja seurantaan käytettiin pääasiassa Simple Network Management Protocol- ja Windows Management Instrumentation -tekniikoita. Järjestelmä rakennettiin niin, että valvontaliikenne oli tarvittaessa salattua tai salauksen käyttöönottoon oli valmius.</p> <p>Työssä otettiin käyttöön useita valvontaohjelmaan asennettavia lisäosia, jotka mahdollistivat laitteen tai toiminnon tarkemman seuraamisen. Tällaisia olivat lisäosat mm. UPS-laitteille ja Exchange-sähköpostipalvelimelle. Joitakin lisätoimintoja lisättiin myös itse luomalla kokonaan uusia asetusohjelmia.</p> <p>Käyttöön otettu valvontaohjelma havaittiin monipuoliseksi ja hyvin muokattavissa olevaksi. Laitteiden liittäminen valvontaan ja lisäosien käyttöönotto oli kuitenkin paljon aikaa vievä toimenpide. Valvontaympäristön jatkokehitykselle, mm. lisäämällä uusia lisäosia, jäikin paljon mahdollisuuksia. Toimeksiantaja halusi myös ohjelman käytöstä ohjeistuksen, joka on työn liitteenä.</p>		
Avainsanat (asiasanat) avoin lähdekoodi, monitorointi, SNMP, verkonhallinta, Zenoss		
Muut tiedot Liitteenä käyttöohje, 48 sivua.		

Author(s) RAUTIAINEN, Ilkka	Type of Publication Bachelor's Thesis	
	Pages 91	Language Finnish
	Confidential <input type="checkbox"/> Until _____	
Title PLANNING AND IMPLEMENTATION OF SYSTEM MONITORING		
Degree Programme Information Technology / Data Network Technology		
Supervisor(s) RANTONEN, Mika		
Commissioner(s), contact person Town of Pieksämäki TIKKANEN, Tommi		
Abstract <p>The thesis was assigned by the town of Pieksämäki and its objective was to plan and implement system monitoring for devices in the town's network. For network management and monitoring the town had previously implemented HP ProCurve Manager tool and most network devices were monitored by that program. Most devices outside monitoring were Windows servers. Four open source system monitoring tools were compared and the tool chosen was Zenoss Core. It was installed on server running Debian GNU/Linux operating system. Devices to be monitored were then added to Zenoss. Most important techniques used for monitoring were Simple Network Management Protocol and Windows Management Instrumentation. The encryption of monitoring traffic was implemented when necessary.</p> <p>Several ZenPacks, packages that extend the functionality of Zenoss, were also installed. For example, one implemented ZenPack was for monitoring a specific UPS model and another for Microsoft's Exchange Server. Some functions were also added by creating new monitoring templates from scratch.</p> <p>The monitoring tool implemented proved to be versatile and extensible. Testing and implementing a complete monitoring system was also proved to be time-consuming and many possibilities were left for further extending the system. The assigner also wanted to have instructions for usage of the Zenoss program. These instructions can be found in the appendices of the thesis.</p>		
Keywords network management, open source software, SNMP, system monitoring, Zenoss		
Miscellaneous Usage instructions attached, 48 pages.		

SISÄLTÖ

LYHENTEET JA KÄSITTEET	4
1 TYÖN LÄHTÖKOHDAT	7
1.1 Toimeksiantaja	7
1.2 Alkutilanne ja tavoitteet	7
2 KÄYTETTYJEN TEKNIKOIDEN ESITTELY	8
2.1 Simple Network Management Protocol	8
2.1.1 Hallintatietokanta (Management Information Base).....	9
2.1.2 SNMP:n versiot	11
2.2 Windows Management Instrumentation	12
3 SUUNNITTELU	13
3.1 Yleistä	13
3.2 Avoimen lähdekoodin ohjelmat	14
3.3 Lisenssi	15
3.4 Ohjelmiston valinta	16
3.5 Hyperic HQ Open Source.....	16
3.6 OpenNMS.....	17
3.7 Pandora FMS.....	18
4 ZENOSS CORE.....	18
4.1 Yleistä	18
4.2 Laitteistovaatimukset.....	19
4.3 Rakenne.....	20

4.3.1	Zenossin käyttämät ohjelmat.....	20
4.3.2	Daemonit	22
4.4	Luokat	24
4.5	Tapahtumat (Events)	25
4.6	Lisäosat (ZenPacks)	26
5	TOTEUTUS	26
5.1	Palvelin	26
5.2	Käyttöjärjestelmä.....	27
5.3	Perusosat	27
5.4	Asetukset	28
5.4.1	Yleistä.....	28
5.4.2	Windows.....	29
5.4.3	Linux	32
5.4.4	Muut laitteet	32
5.5	Lisäosat.....	33
5.6	Asetuspohjat	36
6	POHDINTA	37
6.1	Yleistä	37
6.2	Ongelmat	37
6.3	Kehitysmahdollisuudet	38
	LÄHTEET.....	39
	LIITTEET	43
	Liite 1. Zenoss Core -käyttöohje	43

KUVIOT

KUVIO 1. SNMP:n rakenne.	9
KUVIO 2. MIB-puun hierarkkista rakennetta	10
KUVIO 3. Zenoss Coren web-käyttöliittymän päänäkymä Firefox-selaimella....	21
KUVIO 4. Zenoss-ohjelman rakenne	22
KUVIO 5. Zenossin Daemons-välilehti	23
KUVIO 6. Zenossin Event console -toiminto	26
KUVIO 7. Laitteen Status-välilehti Zenossissa	30
KUVIO 8. Laitteen OS-välilehti Zenossissa.....	31
KUVIO 9. MIB:n tutkimista Zenoss-ohjelmassa MIB browser -lisäosalla	34

LYHENTEET JA KÄSITTEET

AES	Advanced Encryption Standard. Salausmenetelmä.
Daemon	Linux-käyttöjärjestelmässä taustalla ajettava palvelu.
DCOM	Distributed Component Object Model. WMI:n käyttämä siirtoprotokolla.
DES	Data Encryption Standard. Salausmenetelmä.
DHCP	Dynamic Host Control Protocol. Protokolla verkkoasetusten automaattiseen jakeluun ja hakuun.
DMZ	Demilitarised Zone. Tietoverkossa sisä- ja ulko- verkko välissä sijaitseva alue.
GNU/Linux	Käyttöjärjestelmä, joka koostuu GNU-projektin tekemistä perusosista sekä Linux-ytimeistä. Kun tekstissä puhutaan pelkästä Linuxista, sillä tarkoitetaan GNU/Linuxia.
HTTP	Hypertext Transfer Protocol. WWW:ssä käytetty siirtoprotokolla.
IETF	Internet Engineering Task Force. Järjestö, joka vastaa Internet-tekniikoiden standardoinnista.
IOPS	Input/output Operation Per Second. Ilmaisee esim. kiintolevyn luku- ja kirjoitusaktiiviteetin yhden sekunnin aikana.
Linux	Ks. GNU/Linux
LVM	Logical Volume Management. Monipuolisemman levynhallinnan mahdollistava tekniikka.

MD5	Message-Digest algorithm 5. Tiivistealgoritmi, jota käytetään mm. pakettien eheyden varmistamiseen.
MIB	Management Information Base. SNMP:n hallintatietokanta.
NTP	Network Time Protocol. Protokolla ajan synkronointiin.
OID	Object Identifier. Yksittäisen MIB:n olion tunnus.
RAID	Redundant Array of Independent Disks. Kiintolevyjen suorituskkyä ja vikasietoisuutta kasvattamaan luotu tekniikka.
RFC	Request For Comments. IETF:n julkaisema asiakirja, jossa määritellään jokin Internetiä suoraan tai epäsuoraan koskeva tekninen osa-alue.
RPM	Nopeuden yksikkö, kierrosta minuutissa.
RSA	Salausmenetelmä. Lyhennys johdettu kehittäjien sukunimien alkukirjaimista.
SDSL	Symmetric Digital Subscriber Line. DSL-tekniikka, jossa lähetys- ja vastaanottoaikaista toimivat samalla nopeudella.
SMI	Structure of Management Information. Kuvaa SNMP:n hallintatiedon rakenteen.
SNMP	Simple Network Management Protocol. Tekniikka verkonhallintaan ja -valvontaan.

SNMP-yhteisönimi	SNMP community name. Salasana, jota käytetään SNMP:n kahdessa ensimmäisessä versiossa.
SSH	Secure Shell. Protokollaa käytetään salatun yhteyden muodostamiseen laitteeseen.
SSL	Secure Sockets Layer. TLS:n edeltäjä.
TCP	Transmission Control Protocol. IP:n päällä toimiva yhteydellinen siirtoprotokolla, joka tarkistaa pakettien perillemenon.
TLS	Transport Layer Security. Salausprotokolla WWW-sivujen siirtoa varten.
UDP	User Datagram Protocol. IP:n päällä toimiva yhteydetön siirtoprotokolla, joka ei tarkista pakettien perillemeno.
UPS	Uninterrupted Power Supply. Järjestelmä, jonka tehtävä on taata laitteille katkeamaton ja tasainen virransyöttö.
WMI	Windows Management Instrumentation. Hallintaan tarkoitettu Windowsin laajennus.
x86	Intelin kehittämä käytetyin suoritinarkkitehtuuri.
ZODB	Zope Object Database. Sovelluspalvelin Zopen tietokanta.

1 TYÖN LÄHTÖKOHDAT

1.1 Toimeksiantaja

Työn toimeksiantaja Pieksämäki on n. 20 700 asukkaan (Pieksämäki 2009) kaupunki Itä-Suomen läänissä. Sen tietohallintoyksikköön kuuluu tällä hetkellä tietohallinto-päällikkö, pääsuunnittelija, suunnittelija, asiantuntija sekä neljä tukihenkilöä.

1.2 Alkutilanne ja tavoitteet

Kaupungin tietoverkossa laitevalmistaja HP:n kytkimiä sekä tukiasemia valvotaan ja hallitaan keskitetysti ProCurve Manager -ohjelman avulla. Tämän valvonnan ulkopuolella oli toista sataa sekalaista verkon laitetta. Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa valvonnan ulkopuolella oleville verkon laitteille – palvelimille, SDSL (Symmetric Digital Subscriber Line) -laitteille, UPS (Uninterrupted Power Supply) -laitteille, verkkotulostimille ja -kopiokoneille – keskitetty monitorointijärjestelmä. Aikaisessa suunnitteluvaiheessa tulostimet ja kopiokoneet jäivät vaatimuslistalta pois, sillä niitä varten löydettiin Xeroxin valmistama erityisesti tulostimien valvontaan ja hallintaan tarkoitettu ohjelma.

Toimeksiantaja asetti valvontajärjestelmälle joitakin minimivaatimuksia. Sen haluttiin olevan riittävän monipuolinen, jotta esimerkiksi palvelimen kiintolevytilan täytyessä järjestelmä voisi lähettää sähköpostin ylläpitäjälle. Lisäksi haluttiin, että valvontaliikenne salattaisiin mahdollisimman suurilta osin. Työn aikana toimeksiantajan puolelta ilmeni halukkuutta saada ohjeistusta valvontaohjelman peruskäytöstä. Tämä ohjeistus on opinnäytetyön liitteenä 1, johon viitataan tekstissä nimellä ohjekirjaliite. Toimeksiantaja halusi myös, että järjestelmän toimintoja esiteltäisiin päällisin puolin kaupungin tietohallinnolle. Tässä opinnäytetyöraportissa laitteiden nimet, osoitteet, salasana ja muut vastaavat tiedot on muutettu tai peitetty. Tekstissä komentorivin syöte ja asetustiedostojen sisältö on kirjoitettu eri kirjasinlajilla. Lisäksi komentorivin syötteessä käyttäjän antamat komennot on **vahvistettu**.

2 KÄYTETTYJEN TEKNIKOIDEN ESITTELY

2.1 Simple Network Management Protocol

Käsite Simple Network Management Protocol (SNMP) voi tarkoittaa kahta asiaa. Ensimmäinen se on, kuten nimestä voi päätellä, siirtoprotokolla, joka määrittelee tavan, jolla laitteet viestivät keskenään. Toisessa tulkinnassa SNMP käsittää kaikki valvonnan mahdollistavat osat, mukaanlukien varsinaisen SNMP-protokollan. (Kozierok 2005.) Tätä kokonaisuutta kutsutaan nimellä Internet standard management framework ja sen rakenteen osat määritellään seuraavasti:

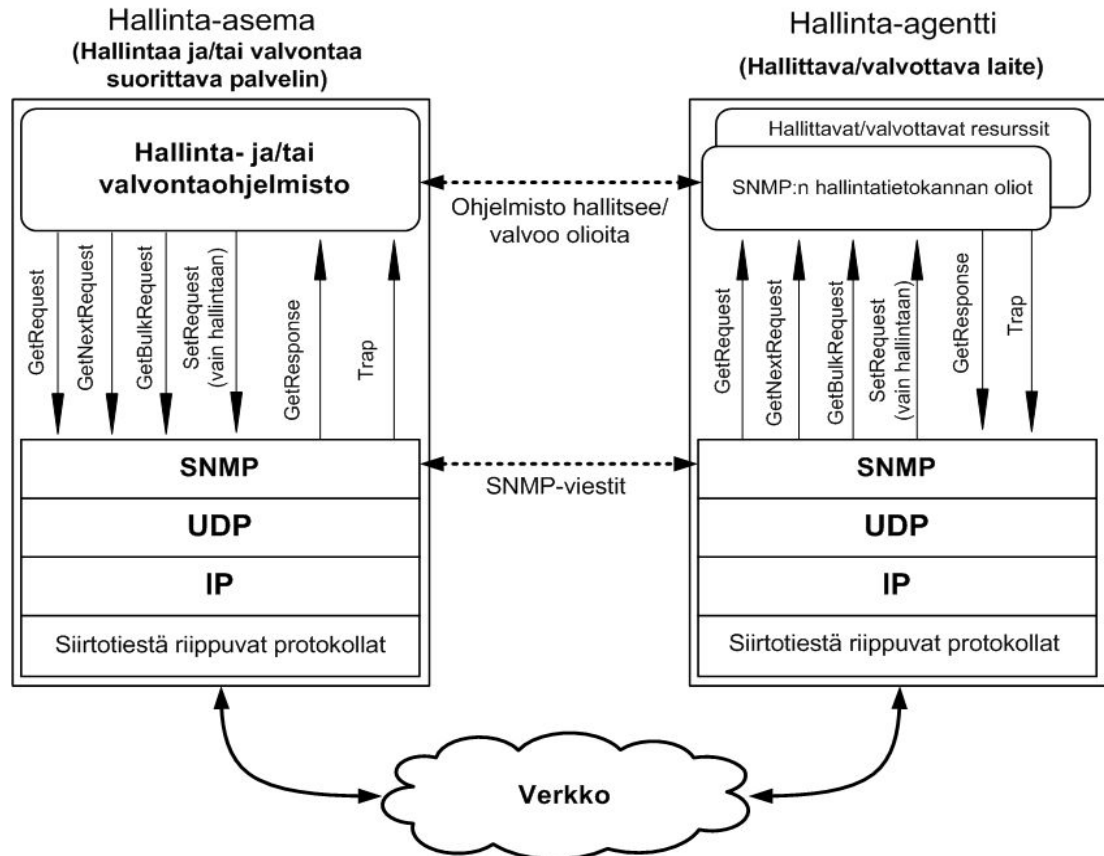
- tiedon esitystapa
- hallintatietojen määrittely
- protokollan määrittely
- tietoturva ja hallinta. (RFC 3410, 3.)

Nämä osat määriteltiin kolmessa Internet Engineering Task Forcen (IETF) julkaisemassa Request For Comments (RFC) -dokumentissa, 1155, 1212 ja 1157. Näiden kolmen dokumentin muodostama kokonaisuutta kutsutaan alkuperäiseksi Internet standard network management frameworkiksi, eli SNMP:n versioksi 1. Ensimmäinen dokumenteista, RFC 1155, määritteli tiedon esitystavan, nimeltään Structure of Management Information (SMI), jonka tarkoitus oli määrittellä hallintatietokannan (Management Information Base eli MIB) hallittavien olioiden rakenne ja ominaisuudet. RFC 1212 puolestaan määritteli SMI:n kanssa yhteensopivasti tarkemmin MIB-moduulien rakenteen. RFC:ssä 1157 määriteltiin SNMP-protokolla, joka huolehtii näiden olioiden käsittelystä. Samalla siinä käsiteltiin SNMP:n tietoturvaa ja hallintaa. Tämä perusrakenne on pysynyt vastaavana myöhemmissäkin SNMP:n versioissa. (RFC 3410, 4.)

SNMP-protokolla käyttää IP:n (Internet Protocol) päällä toimivaa yhteydetöntä User Datagram Protocol (UDP) -protokollaa, joka ei tarkista viestien perillemeno.

SNMP:n käyttämä oletusportti on 161 ja porttia 162 käytetään viesteihin joita kutsutaan Trapeiksi. SNMP-valvontatoteutuksen perusosat ovat valvontaohjelmiston sisältävä hallinta-asema, valvottava laite eli hallinta-agentti, SNMP-protokolla tietojen

vaihtoon aseman ja agentin välillä sekä tiedot hallinta-agentin sisältämistä valvottavista resursseista hallintatietokannan muodossa (RFC 3410, 3). Tämä rakenne on esitetty kuviossa 1.



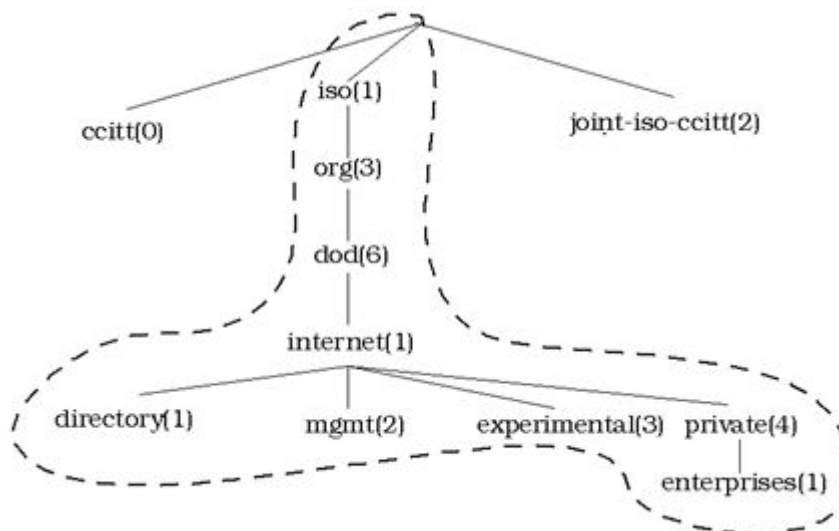
KUVIO 1. SNMP:n rakenne. Muokattu Hautaniemen (1994) kuvasta, joka perustuu Stallingsin (1993) esitykseen.

2.1.1 Hallintatietokanta (Management Information Base)

SNMP:tä tukeva laite (hallinta-agentti) ylläpitää tietokantaa, joka sisältää tietoa laitteesta. Tätä muuttujien puumaista kokoelmaa kutsutaan nimellä Management Information Base eli hallintatietokanta. SNMP-valvontaa suorittava palvelin (hallinta-asema) voi hakea tämän tietokannan muuttujia (Get-viestit) tai seurattava laite voi oma-aloitteisesti lähettää viestin muutoksesta valvontapalvelimelle (Trap- ja Inform-viestit). SNMP mahdollistaa myös muuttujien arvon asettamisen (Set-viestit), mutta tässä työssä tavoitteena on ainoastaan valvonta, eli tietojen lukeminen ja vastaanottaminen.

SNMP:n ensimmäisessä versiossa oli määritelty ainoastaan yksi hallintatietokanta, joka päivittyi myöhemmin MIB-II-versioon RFC:ssä 1213. Nämä tietokannat sisältävät laitteesta tietoa varsin yleisellä tasolla, keskittyen lähinnä verkko-ominaisuuksiin. Toisen MIB-version julkaisun jälkeen luovuttiin käytännöstä, jossa kaikki hallittava tieto oli määritelty yhden RFC-dokumentin määrittelemässä hallintatietokannassa (RFC 3410, 5). RFC-dokumentteina on tämän jälkeen ilmestynyt paljon hallintatietokantoja, jotka keskittyvät kuvaamaan ainoastaan yhden tarkemman osa-alueen, kuten RFC 1628 UPS-laitteiden tai RFC 3805 tulostimien, hallintatietokannat. IETF:n julkaisemien RFC-dokumenttien lisäksi hallintatietokantoja voivat määrittellä myös valmistajat itse omille laitteilleen ja ohjelmilleen.

Hallintatietokannan olioon voi viitata numeerisella olion tunnuksella (Object Identifier eli OID) tai olion sanallisella kuvauksella (Object Descriptor) (RFC 1155, 9). Kaikki SNMP:n hallittavat tiedot löytyvät olion 1.3.6.1 (iso.org.dod.internet) alta (ks. kuvio 2). Tarkemmin määriteltynä OID 1.3.6.1.2, joka sanallisesti kuvattuna on iso.org.dod.internet.mgmt, sisältää IETF:n RFC-dokumenteissa määrittelemät hallintatietokannat ja 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprises) laitevalmistajien tekemät määrittelyt omille laitteilleen.



KUVIO 2. MIB-puun hierarkkista rakennetta. (Hautaniemi 1994.)

2.1.2 SNMP:n versiot

Ensimmäisen SNMP-version määrytykset julkaistiin RFC-dokumenteissa vuonna 1988 ja toisen 1996. SNMP:n kahdessa ensimmäisessä versiossa käytetään osapuolten todentamiseen eli autentikointiin SNMP-yhteisönimeä. Salasanaa vastaava yhteisönimi kulkee salaamattomana verkon yli ja on täten helposti ulkopuolisen luettavissa mikäli tällainen pääsee seuraamaan verkon liikennettä. Tämä on ongelma erityisesti siinä tapauksessa kun yhteisönimi antaa laitteeseen kirjoitusoikeudet, ts. kun laitteen asetusten muutokset ovat mahdollisia.

Toiseen versioon oli tavoitteena saada parannusta SNMP:n huonoon tietoturvaan, mutta siinä se ei onnistunut. SNMPv2 teki kuitenkin lukuisia pienempiä parannuksia, kuten laajensi tietotyyppejä mahdollistamaan suuremmat arvot. SNMP:n toiseen versioon tuotiin myös Inform-niminen viesti. (RFC 3410, 7.) Inform- viesti vastaa toiminnaltaan Trap- viestiä pienellä parannuksella. Siinä missä Trap- viestin perillemeno ei varmisteta, Inform- viestiä lähetetään niin kauan kunnes valvontapalvelin vahvistaa ottaneensa viestin vastaan. Käytössä olevaa, yhteisöpohjaista (Community-based) SNMP:n toista versiota kutsutaan nimellä v2c. Lisäksi on julkaistu muitakin SNMPv2-versioita, kuten RFC 1910:ssä määritelty tietoturvatoteutuksen sisältävä käyttäjöpohjainen (User-based) v2u. Vaikka näille muille versioille ei laajaa hyväksyntää tullutkaan, ehdotuksia käytettiin hyväksi seuraavaa SNMP:n versiota määrittäessä. (RFC 3410, 8.)

Vuonna 2002 julkaistu versio 3 toi viimein ratkaisun aiempien versioiden suurimpaan ongelmaan ja paransi SNMP:n tietoturvaa. RFC 3414:ssä esiteltiin SNMPv3:n käyttäjöpohjainen tietoturvamalli (User-based Security Model, USM). Se mahdollistaa kolme käytettävää tietoturvatasoa:

- **noAuthNoPriv**, joka autentikoi ainoastaan käyttäjänimen perusteella. Vastaa aiempien SNMP-versioiden yhteisönimipohjaista todentamistapaa.
- **authNoPriv**, joka autentikoi käyttäjänimen sekä autentikointisalasanan perusteella. Salasana ei kulje verkossa selväkielisenä, vaan salasanasta ja SNMP- viestistä lasketaan MD5- tai SHA-algoritmia käyttäen tiiviste, joka lähetetään SNMP-paketin mukana ja jota verrataan määränpäässä alkuperäiseen. Tiivis-

teen avulla voidaan myös varmistaa tiedon eheys, eli havaitaan jos saapunut viesti ei ole sama kuin lähtiessä. (RFC 3414, 50 - 51, 56 - 57.)

- **authPriv**, joka autentikoi kuten authNoPriv, mutta lisää tiedon yksityisyyden (Privacy). RFC 3414:ssä määritellään salaus käyttäen Data Encryption Standard (DES) -salausmenetelmää, mutta se ei rajaa muita salausmenetelmiä pois. Esimerkiksi Advanced Encryption Standard (AES) on mahdollinen ja yleisesti käytössä. Salattava osa on SNMP-paketin hyötykuorma (payload). (RFC 3414, 7, 62.) Salauksella varmistetaan, että ulkopuolinen ei pääse tietoon käsiksi, eli se toteuttaa tiedon luottamuksellisuutta.

2.2 Windows Management Instrumentation

Microsoftin Windows Management Instrumentation (WMI) on Windows-käyttöjärjestelmien hallintaa varten kehitetty laajennus. Sen pohjana on Distributed Management Task Force -organisaation julkaisema Web-Based Enterprise Management (WBEM) -kokonaisuus, jonka tarkoitus on yhtenäistää hajautettujen ympäristöjen (Distributed computing environment) hallintaa (Web-Based Enterprise Management 2009). Samaan tekniikkaan perustuva hallintaratkaisu on käytössä useimmilla muillakin käyttöjärjestelmävalmistajilla. WMI koostuu kolmesta osasta, jotka ovat

- mekanismi hallintatiedon sisältävien olioiden määritysten säilytykselle
- DLL-kirjastot, jotka keräävät ja välittävät varsinaisen tiedon olioille
- COM/DCOM-protokolla hallintatiedon hakemiseen ja levittämiseen. (Windows Management Instrumentation: background and overview 2000.)

Windowsin Component Object Model (COM) -osaa käytetään sisäisesti ja Distributed Component Object Model (DCOM) -osaa, joka on COM:n laajennus, etäyhteyksien muodostamiseen (DCOM technical overview 1996). DCOM käyttää porttia 135 yhteyden muodostukseen, jonka jälkeen se valitsee käytettävän portin dynaamisesti väliltä 1024–65 535 (Nelson 1998). Palomureille tämä on ongelmallista ja käytettäviä portteja onkin käytännössä rajattava Windowsin rekisteriä muokkaamalla. Rekisterin

muokkaus on kuvattu on kuvattu ohjekirjaliitteen kappaleessa 5.3.1. Kun valvonta-ohjelma hakee tietoja WMI:llä, se käyttää autentikointiin NTLM-protokollaa, joka käyttää haaste-vastine (challenge-response) -menetelmää. NTLM ei lähetä salasanaa verkon yli selväkielisenä, vaan hallinta-agentti lähettää hallinta-asemalle haasteena (challenge) 16-tavuisen satunnaisluvun, jonka hallinta-asema salaa käyttäen salasanan tiivistettä (hash). Tämä tiiviste lähetetään vastineena (response) hallinta-agentille, joka vertaa sitä itse samalla salasanan tiivisteellä salaamaansa satunnaislukuun. Jos hallinta-aseman ja hallinta-agentin laskemat tulokset ovat samat, autentikointi onnistuu. (Microsoft NTLM 2009.)

WMI:n kautta haettavia tietoja voivat olla esimerkiksi lokit ja suorituskykytiedot käyttöjärjestelmästä. Käytännössä kaikista Microsoftin merkityksellisistä sovelluksista, kuten Active Directory -hakemistopalvelusta ja SQL-tietokannasta, voidaan hakea tietoa WMI:n kautta. Myös muut valmistajat voivat tehdä Windows-sovelluksilleen WMI-toteutuksen. Valvonnan kannalta palvelu täydentää hyvin SNMP:n tarjoamia tietoja.

3 SUUNNITTELU

3.1 Yleistä

Verkonhallintaa ja -valvontaa varten kaupungin tietohallinnolla oli käytössään edellisvuonna käyttöönotettu HP ProCurve Manager (PCM) -ohjelma (Pellonpää 2008). Valvonnan lisäksi PCM-ohjelmalla on myös mahdollista muuttaa järjestelmään liitettyjen kytkimien sekä tukiasemien asetuksia keskitetysti. Nyt PCM-ohjelman rinnalle käyttöönotettavan valvontaohjelmiston pääasiallinen tehtävä on järjestelmien valvonta (system monitoring). Sen on valvottava laitteiden toimintaa mm. seuraamalla niiden kuormitusta, havaittava mahdollisia laitevikoja ja monitoroitava tärkeitä palveluita. Suurin osa valvontaan liitettävistä laitteista on Windows-palvelimia, joten näiden seurantaan on kiinnitettävä erityistä huomiota.

Valvontaohjelmalla ei ole tarkoitus muokata mitään seurattavan laitteen asetuksia, joten sille riittävät laitteisiin pelkät lukuoikeudet. Lisäksi kaikki seurattavat laitteet sijaitsevat ulkopuolisilta suojusta sisäverkossa. Poikkeuksena tähän ovat demilitarisoidulla vyöhykkeellä (DMZ) sisäverkon ulkorajalla sijaitsevat palvelimet, kuten WWW-palvelin. Mikäli ulkopuolinen pääsisi kaupungin sisäverkkoon seuraamaan salaamatonta SNMP-liikennettä, hän voisi saada selville vain luku -oikeuksilla varustetun SNMP-yhteisönimen, mitä ei voi pitää todennäköisenä eikä edes kovin vakavana uhkana. Lisäsuojaa tätä vastaan voi kuitenkin vielä saada sallimalla SNMP-yhteydet ainoastaan valvontaohjelman palvelimelta. Kaupungin verkossa laajalti käytössä olevat Windows-palvelimet eivät suoraan tue SNMP:n versiota 3, ja sen ottaminen käyttöön on suhteellisen mutkikasta. Salauksen mahdollistavan SNMPv3:n käyttöönotto jokaiseen mahdolliseen laitteeseen ei näistä syistä ollut tavoitteena, vaan sen käyttö Windows-palvelimissa oli tavoitteena ainostaan erityisellä DMZ-alueella.

Koska yksikään Windows-versio ei tue SNMP:n versiota 3, oli sen käytölle etsittävä vaihtoehtoinen toteutustapa. Muutamit valmistajat myyvät Windowsin SNMP-toteutuksen kokonaan korvaavaa ratkaisua. Tällainen Windowsin kiinteän osan kokonaan korvaaminen maksullisella ohjelmistolla ei kuitenkaan houkutellut. Toinen mahdollisuus oli jättää Windowsin oma SNMP-palvelu paikoilleen ja välittää kaikki SNMP-kyselyt sille erillisen versio 3:a tukevan välityspalvelun avulla. Lähinnä Linux-puolella käytössä oleva Net-SNMP oli asennettavissa myös Windowsiin ja siitä löytyi tämä haettu välitysmahdollisuus (Net-SNMP - Readme.win32 2007). Net-SNMP siis asennettiin SNMPv3:a tarvitseviin Windows-koneisiin, ja sen kautta hoidettiin yhteydet salattuna valvontapalvelimeen.

3.2 Avoimen lähdekoodin ohjelmat

Dubien (2007) artikkelissa mainitun Gartnerin tutkimuksen mukaan verkohallintaohjelmistoissa 55 prosentin yhteenlaskettua markkinaosuutta pitivät vuonna 2007 hallussaan epävirallisesti suureksi nelikoksi kutsutut isot valmistajat IBM, HP, BMC ja CA. Näiden valmistajien tuotteet ovat kehittyneet pitkän kehityskaarensa kuluessa monipuolisiksi, mutta ovat myös melko kalliita ja usein ylimitoitettuja pienempien ympäristöjen hallinta- ja valvontatarpeisiin. Neljän suuren ja pienempien haastajien jouk-

koon on 2000-luvun aikana ilmestynyt uusia yrittäjiä, joiden taktiikkana on tarjota ohjelma ja sen lähdekoodi vapaasti lisenssillä, jonka käyttöehdot ovat hyvin sallivat. Kun itse ohjelma tarjotaan ilmaiseksi, voidaan tavoitella hyötyjä, joita avoin lähdekoodi mahdollistaa. Yksi saavutettava etu voi olla tuotteen parantuminen, kun kuka tahansa voi sitä tutkia ja tehdä ohjelmaan omia parannuksiaan. Yleinen ansaintamalli on myös tarjota suppeampi versio ohjelmasta ilmaiseksi ja antaa maksua vastaan tuotetukea sekä laajennuksia ohjelmaan. Osaavalle käyttäjälle lähdekoodin tutkimisen ja muokkaamisen mahdollisuus voi tuoda lukuisia etuja, kuten ohjelman räätälöinnin omiin tarpeisiin sekä ohjelmointivirheiden tai tietoturvahaukien nopean korjaamisen joko itse tai muiden käyttäjien avustuksella.

Ilmaiseksi ladatulla tuotteella ei luonnollisesti voi olla perinteistä tuotetukea. Ellei maksullista tuotetukea ole tarjolla tai siitä ei haluta maksaa, tärkeäksi avoimen lähdekoodin ohjelmiston valinnassa muodostuu tuotteen käyttäjäyhteisön aktiivisuuden huomioiminen. Muuten hyvästä ohjelmasta ei ole iloa, jos vastaan tulevista ongelmista ei saa tietoa mistään tai ohjelmaan ei saa lisätoimintoja muuten kuin itse tekemällä. Eräs hyvä tapa tarkistaa nopeasti käyttäjäkunnan aktiivisuus on seurata ohjelman omia keskustelualueita.

3.3 Lisenssi

Kaikki vertailussa olleet ohjelmat käyttävät samaa GNU General Public License (GPL) 2.0 -lisenssiä. Sen tärkeimpiä kohtia ovat

- ohjelmaa saa käyttää, muokata ja levittää vapaasti
- levitettävästä versiosta on ilmentävä ohjelmaan tehdyt muutokset, muokattu lähdekoodi on oltava saatavissa ja muokatun version on käytettävä samaa GPL-lisenssiä kuin alkuperäinen ohjelma
- ohjelmalla ei ole minkäänlaista takuuta. (GNU General Public License, version 2 1991.)

3.4 Ohjelmiston valinta

Vertailuun otetuista neljästä valvontaohjelmasta Hyperic HQ Open Source sekä Zenoss Core vaikuttivat kokonaisuutena parhaimmilta. Ohjeistus on tärkeä osa mitä tahansa hiemankin monimutkaisempaa ohjelmaa ja näiden valmistajien dokumentaatio vakuutti. Erityisesti Zenossilla oli tarjolla selkeät ohjekirjat, joihin oli panostettu. Sen sijaan OpenNMS antoi tällä osa-alueella heikoimman vaikutelman tarjoten lähinnä hajanaisen artikkelikokoelmaa muistuttavan ohjeistuksen. Pandora FMS:n käyttäjistä suuri osa vaikutti olevan espanjankielisiä, mikä väistämättä vaikuttaa tiedon saantiin, varsinkin kun ohjelma ei käyttäjämäärällään kilpaile Hypericin tai Zenossin kanssa. Hyperic HQ Open Sourcen agenttipohjainen valvontaratkaisu vaikutti lupaavalta, mutta avoimen version pahasti karsitut raportti- ja hälytystoiminnot vaikuttivat siihen, että Zenoss Core valittiin järjestelmään asennettavaksi valvontaohjelmaksi. Zenoss Core vaikutti kaikin puolin lupaavalta. Sen vahvuuksia olivat

- aktiivinen ja runsaslukuinen käyttäjäyhteisö
- monipuolinen laajennusvara
- hyvä ohjeistus
- monipuoliset hälytys- ja raportointitoiminnot
- miellyttävä ja selkeä käyttöliittymä sekä ulkoasu.

3.5 Hyperic HQ Open Source

Java-pohjaisesta Hyperic HQ -valvontaohjelmasta on tarjolla avoimen lähdekoodin ilmainen versio sekä maksullinen Enterprise-versio. Ohjelma on saatavissa yleisimmille käyttöjärjestelmille, myös Windowsille. Se on rakennettu JBoss-sovelluspalvelimen päälle ja käyttää tietojen tallennukseen PostgreSQL-tietokantaa. (Hyperic HQ 4.0 product tour 2009.)

Hyperic HQ:n monipuolisempi seuranta edellyttää, että jokaiselle seurattavalle palvelimelle asennetaan oma pieni ohjelmansa, Hyperic-agentti. Tämä agentti hoitaa tie-

donkeruun palvelimelta ja välittää sen Hyperic-palvelimelle. Agentti ei välitä siitä onko seurantalpalvelin saatavilla, vaan se kerää tietoa jatkuvasti. Kun seurantalpalvelimeen saadaan seuraavan kerran yhteys, agentti välittää tällä välin kerätyt tiedot Hyperic-palvelimelle. Maksulliseen versioon verrattuna ilmaista versiota on karsittu melko paljon, mm. tässä ympäristössä tärkeäksi koetut hälytys- ja raportointitoiminnot vaikuttavat ilmaisversiossa huomattavasti suppeammilta. Hyperic HQ:n mukana tulee lisäohjelmia eli plug-inejä useita yleisiä palvelinohjelmia varten, mm. IIS:ää, Apachea, Active Directorya ja SQL:ää. Ohjelmalla on melko paljon käyttäjiä, ja joitakin käyttäjien tekemiä lisäosia on myös ladattavissa. (Hyperic HQ 4.0 product tour 2009.) Elokuussa 2009 virtualisointiohjelmistovalmistaja VMware ilmoitti ostaneensa Hypericiä kehittävän SpringSource-yhtiön (VMware to acquire SpringSource 2009).

3.6 OpenNMS

Hypericin tavoin myös OpenNMS-valvontaohjelma on ohjelmoitu suurimmaksi osaksi Javalla ja sekin käyttää PostgreSQL:ää tietokantanaan. Ohjelma ilmoittaa tukevansa suoraan kuutta eri Linux-jakelua, Windowsia, Mac OS X:ää sekä Solarista. Sen voi kuitenkin saada toimimaan millä tahansa Javan kehityspaketin (SDK) versiota 1.4 tukevalla alustalla. (OpenNMS - FAQ-about 2009.)

OpenNMS:n kotisivut ja dokumentaatio on rakennettu kokonaan helposti muokattavan MediaWiki-pohjan alle. Kunnollisia ohjekirjoja ei löydy helposti, vaan ohjeistus on erillisinä Wiki-artikkeleina. Dokumentoinnin etusivulla ilmoitetaankin suoraan, että ohjeistus ei ole niin hyvää kuin se voisi olla (OpenNMS - documentation 2007). Käyttäjien apua siis kaivataan artikkeleiden luomiseen ja parantamiseen. Ohjelman kokeilu on vaivatonta, sillä kuka tahansa voi testata ohjelmaa suoraan web-selaimella tarkoitusta varten pystytetyssä testiympäristössä. OpenNMS:n asetuksia säilytetään erillisissä Extensible Markup Language (XML) -tiedostoissa. Näiden muokkaaminen onnistuu suurimmaksi osaksi myös graafisen web-käyttöliittymän kautta (Curry 2008, 97). Curry (2008, 98) myös mainitsee huonona puolena Java-lokitiedostot, joista on vaikeaa löytää mitään hyödyllistä tietoa.

3.7 Pandora FMS

Pääosin Perl-kielellä ohjelmoitu Pandora Flexible Monitoring System käyttää Hyperic HQ:n tavoin agenttia, joka asennetaan jokaiselle seurattavalle palvelimelle. Nämä agentit ilmoittavat seurattavilta palvelimilta kerättyjä tietoja Pandora FMS - palvelimelle oletuksena salatun SSH-yhteyden kautta. Tuettuja käyttöjärjestelmiä ei selkeästi ilmoiteta, mutta lähdekoodin lisäksi ainakin Debianille ja VMwarelle tarkoitettut paketit löytyvät. Ohjelma käyttää MySQL-tietokantaa tietojen tallennukseen. (Introduction to Pandora FMS 2008.) Vaikka ohjelman dokumentaation viralliseksi kieleksi ilmoitetaan englanti, ohjelma on espanjalainen ja suuri osa käyttäjistä on espanjankielisiä. Tämä ilmenee hyvin ohjelman keskustelualueella, jolta tuntuu olevan vaikeampaa saada tietoa englanniksi. OpenNMS-ohjelman tavoin Pandoraa on myös mahdollista kokeilla verkkoselaimen kautta kaikille avoimessa testiympäristössä. Myös Pandoraa myydään maksullisena Enterprise-versiona, joka lisää joitakin lisäominaisuuksia sekä tuotetuen.

4 ZENOSS CORE

4.1 Yleistä

Zenoss-ohjelman kehityksen aloitti vuonna 2002 Erik Dahl ja vuonna 2005 perustettiin yhtiö nimeltä Zenoss Inc (Zenoss team - Management 2009). Yhtiön toiminta-ajatus on sama kuin Hypericin tuotteessa; tarjolla on riisutumpi avoimen lähdekoodin Core-versio sekä maksullinen enemmän ominaisuuksia tarjoava Enterprise-versio. Jatkossa pelkästä Zenossista puhuttaessa viitataan nyt käyttöönotettuun Core-versioon.

Zenoss on agentiton verkon- ja järjestelmänvalvontatyökalu. Tämä tarkoittaa, että Zenossilla ei ole omaa, jokaiselle seurattavalle laitteelle asennettavaa lisäohjelmaa kuten Hypericilla ja Pandoralla, vaan se kerää tietonsa työkaluilla jotka usein ovat jo valmiina seurattavalla laitteella. Käytännössä täysin agentitonta valvontaa ei ole, sillä jokainen kunnolliseen seurantaan liitettävä laite lähes poikkeuksetta vaatii vähintään

muutoksia asetuksiin, pahimmillaan myös useiden lisäohjelmien asennusta. Ohjelma tukee laitteiden seurantaan SNMP:n kaikilla versioilla, Windowsin WMI:llä, SSH:lla, Telnetillä sekä Pingillä. Ainakaan versio 2.4.2 ei vielä tue SNMP:n versio 3:n Trap- tai Inform-viestejä. Zenoss tukee myös Googlen karttapalvelu Google Mapsin integrointia käyttöliittymään, mutta sen ilmaista versiota ei voi käyttää yrityksen sisäverkossa (Google Maps/Google Earth APIs terms of service 2009).

4.2 Laitteistovaatimukset

Zenoss Core on asennettavissa lähdekoodista mille tahansa Linuxille, Solaris 10:lle tai FreeBSD:lle. Ladattavissa ovat myös jakelukohtaiset stack-asennuspaketit, jotka sisältävät valmiiksi kaiken tarpeellisen, kuten MySQL:n. Nämä ovat saatavissa seuraaville käyttöjärjestelmille sekä 32- että 64-bittisinä, tarkoitettuna vain x86-suoritinarkkitehtuurille:

- Red Hat Enterprise Linux 4 ja 5
- CentOS 4 ja 5
- Fedora 9 ja 10
- SUSE Enterprise 10
- openSUSE 10.3 ja 11.1
- Debian 5
- Ubuntu Server 6.06 ja 8.04
- Mac OS X 10.5, vain 32-bittisenä.

Lisäksi löytyvät VMware-virtuaaliympäristöön tarkoitettut valmiit Appliance-paketit Windowsille, Linuxille sekä Mac OS X:lle. (Zenoss - downloads 2009.) Virallisia vaatimuksia laitteiston komponenteille Zenoss ei anna, mutta suuntaa antavina voidaan pitää seuraavia:

Korkeintaan 250 seurattavaa laitetta:

- 4 GB keskusmuistia

- Core 2 Duo E6300 1.86/1066 RTL
- 75 GB:n kiintolevy.

Enemmän kuin 250 seurattavaa laitetta:

- 8 GB keskusmuistia
- Xeon 5120 DC 1.86/1066/4 MB
- neljä kappaletta 75 GB:n kiintolevyjä kahtena RAID-1-parina. (Badger 2008.)

Näistä vaatimuksista ei yksin vielä voi päätellä paljonkaan, sillä laite voi kevyimmillään olla ainoastaan Ping-seurannassa, mikä vie palvelimen tehoja hyvin vähän.

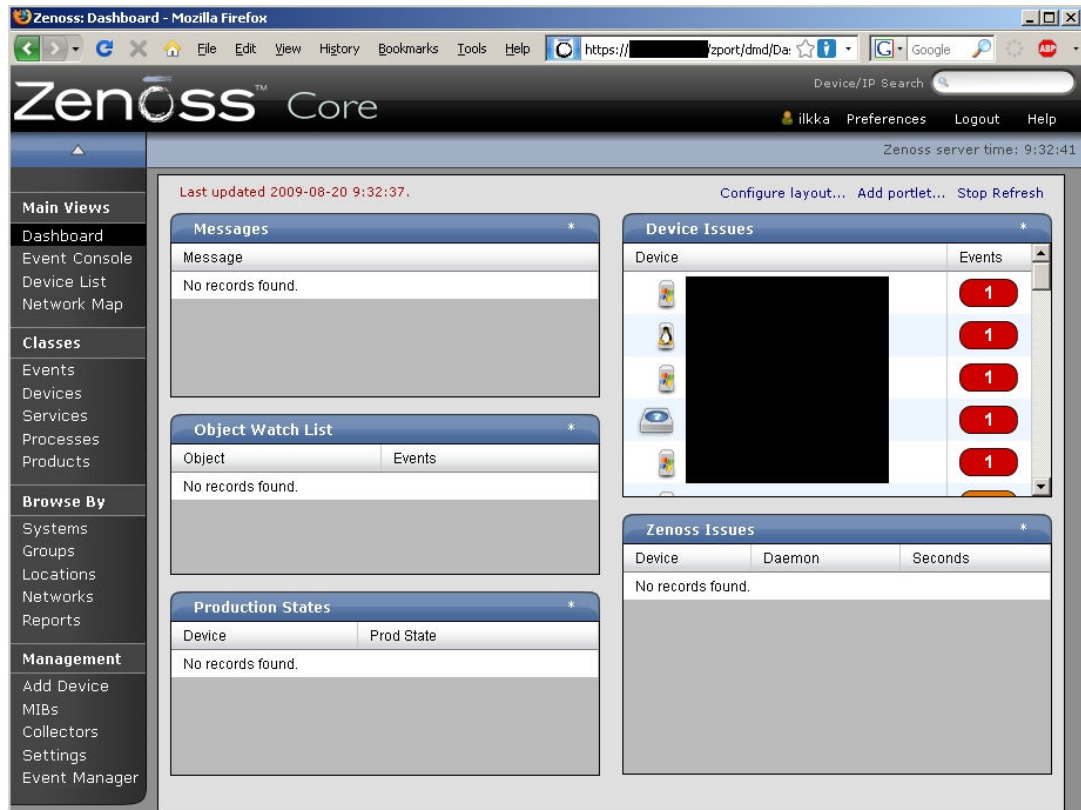
Useimmiten laitteen seuranta taas tarkoittaa seurantaa usealla eri protokollalla, ja voi sisältää mm. lokien keräystä, tarkempaa ohjelmien toiminnan sekä lämpötilojen ja kiintolevytilan seurantaa. Zenossia hallitaan web-käyttöliittymän kautta, minkä luvataan toimivan tarkoitettulla tavalla vain Firefoxin versiolla 3 sekä Internet Explorer 7:llä (Zenoss - downloads 2009).

4.3 Rakenne

4.3.1 Zenossin käyttämät ohjelmat

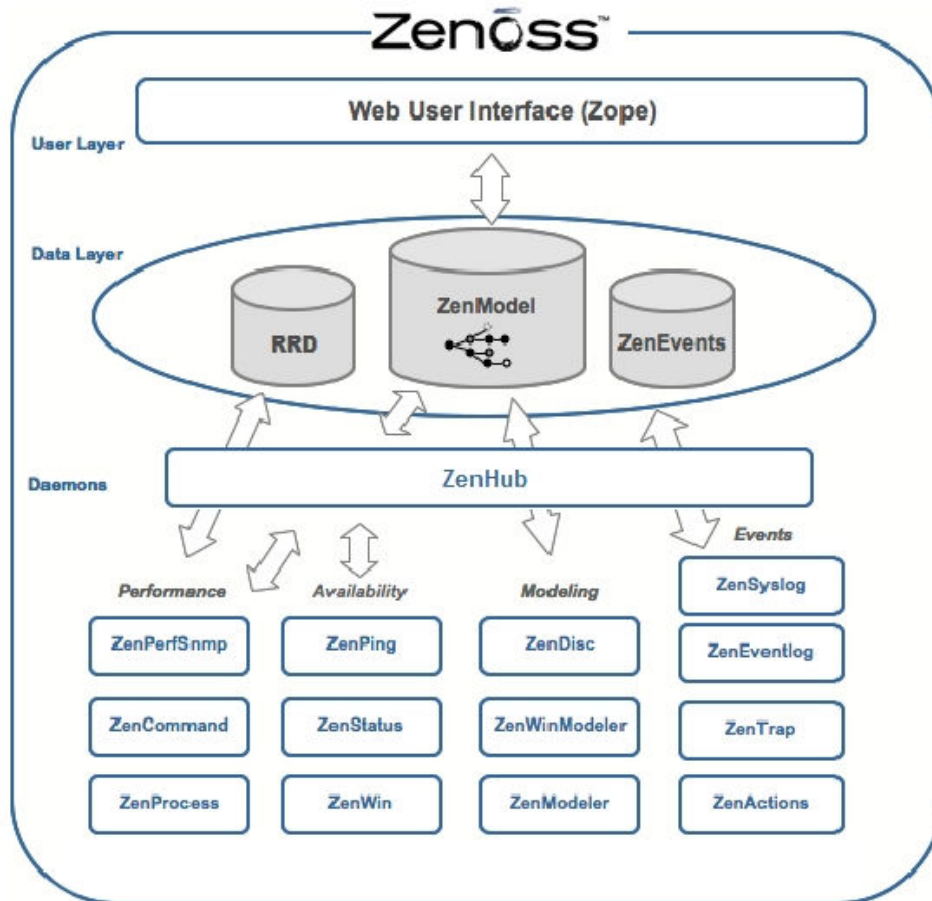
Python-kielellä ohjelmoitu Zenoss on rakennettu avoimien ohjelmistojen päälle. Niistä tärkeimmät ovat

- **Zope**, joka on niin ikään Python-kielellä tehty sovelluspalvelin. Zenoss-ohjelmassa sen varassa toimii käyttäjälle järjestelmän näkyvin osa, graafinen web-käyttöliittymä (ks. kuvio 3). Tästä muodostuu käyttäjäkerros (User layer) (ks. kuvio 4). Zopella on oma tietokantansa, Zope Object Database (ZODB), joka sisältää mm. laitekohtaiset asetukset. (Zenoss Developer's guide for version 2.4, 24.)



KUVIO 3. Zenoss Coren web-käyttöliittymän päänäkymä Firefox-selaimella.

- **MySQL**, joka on maailman suosituin avoimen lähdekoodin tietokantaohjelmisto (About MySQL 2009). Zenoss käyttää MySQL-tietokantaa tapahtumien (Events) tallennukseen (Zenoss Developer's guide for version 2.4, 25). Kuviossa 4 MySQL-tietokanta sijaitsee tietokerroksella (Data layer).
- **RRDtool** (Round Robin Database tool), joka tallentaa Zenossin keräämät tiedot ja piirtää tallennettujen tietojen pohjalta niistä kuvaajat (Zenoss Developer's guide for version 2.4, 27). Kuviossa 4 RRD-tietokanta sijaitsee tietokerroksella (Data layer).
- **Twisted**-verkkototeutus, jota Zenoss käyttää määrittämään kuinka järjestelmä hoitaa liikennöinnin seurattaviin laitteisiin ja Zenossin omiin daemoneihin (Zenoss Developer's guide for version 2.4, 51).



KUVIO 4. Zenoss-ohjelman rakenne. (Zenoss Developer's guide for version 2.4, 2)

4.3.2 Daemonit

Kuviossa 4 esitetyn rakenteen alimmalla tasolla ovat Zenossin daemonit. Daemonit ovat ohjelmia, joista jokainen on erikoistunut yhteen tiettyyn tehtävään. Daemoneita voidaan käynnistää tai pysäyttää, niiden lokeja voidaan katsoa ja asetuksia muuttaa ohjelman web-käyttöliittymässä Daemons-välilehdeltä (ks. kuvio 5).

Settings Commands Users ZenPacks Jobs Menus Portlets Daemons Versions Backups									
Zenoss Daemons									
Zenoss Daemon	PID	Log File	Configuration		State	Actions			
zeoctl	2449	view log	view config	edit config	●	Restart	Stop		
zopectl	2453	view log	view config	edit config	●	Restart	Stop		
zenhub	2482	view log	view config	edit config	●	Restart	Stop		
zenjobs	2521	view log	view config	edit config	●	Restart	Stop		
zenping	2576	view log	view config	edit config	●	Restart	Stop		
zensyslog	2623	view log	view config	edit config	●	Restart	Stop		
zenstatus	2629	view log	view config	edit config	●	Restart	Stop		
zenactions	2659	view log	view config	edit config	●	Restart	Stop		
zentrap	2732	view log	view config	edit config	●	Restart	Stop		
zenmodeler	2746	view log	view config	edit config	●	Restart	Stop		
zenperfsnmp	2771	view log	view config	edit config	●	Restart	Stop		
zencommand	2797	view log	view config	edit config	●	Restart	Stop		
zenprocess	2830	view log	view config	edit config	●	Restart	Stop		
zenwin	2869	view log	view config	edit config	●	Restart	Stop		
zeneventlog	2908	view log	view config	edit config	●	Restart	Stop		

KUVIO 5. Zenossin Daemons-välilehti.

- **ZenHub** on daemoneista raskaimman kuormituksen alla. Sen tärkein tehtävä on toimia Zope- ja MySQL-tietokantojen sekä RRD-tiedostojen että daemoneiden välittäjänä (Zenoss Developer's guide for version 2.4, 56).
- **Zeoctl**, ZEO on Zopen ja Zopen tietokannan ZODB:n välinen kerros. Zeoctl käynnistää ja pysäyttää ZODB:n (Zenoss Developer's guide for version 2.4, 24).
- **Zopectl** käynnistää ja pysäyttää Zope-sovelluspalvelimen.
- **ZenJobs**-daemonille toimitetaan tehtävät, joiden käynnistämisestä se huolehtii, esim. uusien laitteiden etsiminen.
- **ZenPerfSnmp** suorittaa säännöllisin väliajoin keräyksen seurattavien laitteiden tilasta SNMP:n kautta.
- **ZenCommand** huolehtii Nagios- ja Cacti-lisäohjelmien suorittamisesta joko paikallisesti tai etänä SSH:n avulla.
- **ZenProcess** vastaa palvelimien prosessien seurannasta.

- **ZenPing** valvoo laitteita Internet Control Message Protocol (ICMP) -viesteillä, eli pingaamalla.
- **ZenStatus** vastaa palvelimien TCP-palveluiden seurannasta.
- **ZenWin** vastaa Windowsin palveluiden WMI-seurannasta.
- **ZenDisc** vastaa uusien laitteiden etsimisestä.
- **ZenModeler** kerää tietoja laitteiden asetuksista SNMP:n, SSH:n ja Telnetin kautta.
- **ZenSyslog** ottaa vastaan ja käsittelee Syslog-viestit, esim. Linuxista tai Windowsiin asennetulta Syslog-palvelimelta.
- **ZenEventlog** ottaa vastaan ja käsittelee WMI:n kautta tulevat Windowsin lokipalvelun lähettämät viestit.
- **ZenTrap** ottaa vastaan ja käsittelee SNMP:n Trap-viestit.
- **ZenActions** vastaa siitä, että asetetut hälytykset toimivat (esim. sähköposti lähtee ylläpidolle). (Zenoss Developer's guide for version 2.4, 3.)

4.4 Luokat

Zenoss-järjestelmä käyttää ryhmittelyä, jossa tapahtumat, laitteet, palvelut ja tuotteet on jaoteltu hierarkkisesti luokkiin. Esimerkiksi laitteiden pääsivu sisältää karkean jaotelun, jossa alaluokat ovat mm. verkko, palvelin ja tulostin. Tästä etenemällä palvelinluokkaan päästään sivulle, jossa laitteet entisestään tarkentuvat Windows-, Linux- tai joksikin muuksi palvelimeksi. Tarkempia asetuksia varten voidaan vielä esimerkiksi /Devices /Server /Windows -luokan alle luoda uusia ryhmiä. Tällainen luokkajako helpottaa asetusten muokkaamista, sillä ylemmälle luokalle tehty asetukset periytyy automaattisesti sen alla oleville luokille ja laitteille, ellei erikseen muuta ole määritelty.

Samantyylinen jako on Products-sivulla, jolta voi selata koneille asennettuja ohjelmia ja laitteita. Pääsivu listaa kaikki valmistajat. Yksittäisen valmistajan sivulle jatkamalla nähdään kaikki kyseisen valmistajan ohjelmat sekä laitteet. Yksittäisen tuotteen sivulta näkyy vielä missä palvelimissa ohjelma tai laite on asennettuna.

4.5 Tapahtumat (Events)

Kun seurattavassa laitteessa tapahtuu jotakin, Zenoss ilmoittaa siitä luomalla tapahtuman. Tapahtumat näkyvät kunkin laitteen Events-välilehdellä, ja kullekin tapahtumalle on määritelty vakavuusaste kriittisestä (Critical) normaaliin (Clear) sekä luokka. Välilehdelle kerätään niin käyttöjärjestelmien lokeista suoraan haetut kuin Zenossin itse generoimatkin tiedot. Eri vakavuusasteet on eroteltu välilehdellä värein ja vähemmän vakavat tapahtumat voi myös suodattaa pois näkyvistä. Käyttöliittymän pääsivulta avattava Event console -niminen toiminto kerää kaikkien seurattavien laitteiden tapahtumat yhdelle sivulle (ks. kuvio 6). Kerättyjä tapahtumia voi myös tarkastella luokkajaon mukaan, esim. /Devices /Power /UPS -luokan tapahtumista nähdään kaikkien UPS-laitteiden tapahtumat. Tapahtumien vakavuusasteet ovat tärkeitä määrittäessä sähköpostiin tehtäviä hälytyksiä. Hälytyksiä käsitellään tarkemmin ohjekirjalitteen kappaleessa 10.

The screenshot shows the Zenoss Event console interface. At the top, there are filters for 'Sev' (Severity) and 'State' (Acknowledged), and a 'Stop' button with a counter of 60. Below the filters, there are options to 'Select: All None Acknowledged Unacknowledged' and a page indicator '1-14 of 156'. The main table has columns: device, component, eventClass, summary, firstTime, lastTime, and count. The table is sorted by 'count' in descending order. Callouts provide instructions: 'Click the column header to sort by that category. Click again to toggle between ascending and descending sort order.' and 'Filter by event severity' and 'Filter by event state'. A 'Click to view event details' callout points to a magnifying glass icon in the 'count' column.

device	component	eventClass	summary	firstTime	lastTime	count
localhost		/Status/	Devices/win2003.zenoss.loc not up	2008/08/15 10:43:38.000	2008/08/18 07:43:29.000	829
	Browser	/Status/-WinService	Windows Service 'Browser' is down	2008/08/06 14:25:43.000	2008/08/16 04:01:47.000	13392
	Browser	/Status/-WinService	Windows Service 'Browser' is down	2008/08/06 14:24:44.000	2008/08/16 04:01:47.000	
		/Status/Ping	ip 10.175.211.134 is down	2008/08/15 15:16:46.000	2008/08/15 15:26:46.000	11
adtran-204.zenoss.loc		/Status/Ping	ip 10.204.210.2 is down	2008/08/04 08:06:25.000	2008/08/18 04:38:13.000	5814
vista-dev-vm02.zenoss.loc	Netlogon	/Status/-WinService	Windows Service 'Netlogon' is down	2008/08/06 14:18:41.000	2008/08/14 04:02:33.000	11089
Ubuntu-Oracle		/Status/Ping	ip 10.175.211.116 is down	2008/08/04 08:06:22.000	2008/08/04 10:23:06.000	138
sourceforge.net		/SourceForge	threshold of zenossvncommits not met: current value 0.00	2008/08/05 16:55:35.000	2008/08/18 07:44:39.000	2831
HP7354E0	snmp	/Status/Snmp	snmp agent down	2008/08/08 15:35:33.000	2008/08/18 07:43:29.000	2242
apcups.zenoss.loc	snmp	/Status/Snmp	snmp agent down	2008/08/09 09:05:44.000	2008/08/18 07:43:29.000	2032
s-sql2005.zenoss.loc	snmp	/Status/Snmp	snmp agent down	2008/08/13 09:26:10.000	2008/08/18 07:43:29.000	1422
s-exch2007-64_demo.zenoss.loc	snmp	/Status/Snmp	snmp agent down	2008/08/13 09:26:16.000	2008/08/18 07:43:29.000	1422
austinbot.zenoss.loc	snmp	/Status/Snmp	snmp agent down	2008/08/09 09:05:44.000	2008/08/18 07:43:29.000	2032

KUVIO 6. Zenossin Event console -toiminto. (Zenoss Administration for version 2.4.2, 17.)

4.6 Lisäosat (ZenPacks)

Zenossille on saatavilla ZenPackeja, lisäosia, jotka lisäävät sen ominaisuuksia. Lisäosat jakautuvat Zenossin itse ylläpitämiin Core-lisäosiin ja käyttäjien tekemiin Community-lisäosiin. Tyypillinen ZenPack lisää mahdollisuuden seurata tarkemmin jotakin ohjelmaa tai laitetta, mutta myös sen omaan käyttöliittymään tehtyjä muokkauksia on saatavilla. Zenoss sisältää tuen myös Nagios- ja Cacti-valvontaohjelmia varten tehdyille lisäohjelmille (plug-init).

5 TOTEUTUS

5.1 Palvelin

Valvontaohjelmistoa pyörittäväksi palvelimeksi otettiin aiemmin WWW-palvelimena toiminut HP ProLiant ML350 G3. Sen tärkeimmät komponentit olivat

- Intel Xeon 2,8 GHz -suoritin
- 4 GB keskusmuistia (alussa 2 GB)
- 2 kpl 10 000 RPM:n SCSI-väyläisiä 72,8 GB:n kiintolevyjä
- HP SmartArray 641 -RAID-ohjain.

RAID (Redundant Array of Independent Disks) -ohjaimen asetuksissa otettiin käyttöön laitteistopohjainen RAID-1. Tämä RAID-tila on peilaava, joten palvelimen molemmilla levyillä on koko ajan sama sisältö. Jos toinen levy hajoaa, jäljellä oleva levy voi jatkaa toimintaansa normaalisti.

5.2 Käyttöjärjestelmä

Palvelimen käyttöjärjestelmäksi valittiin Debian GNU/Linux 5.0, koodinimeltään Lenny. Valintaan vaikutti se, että tämä Linux-jakelu oli ollut käytössä joissakin aiemmin asennetuissa kaupungin palvelimissa, joten se oli suhteellisen tuttu tietohallinnon ylläpitäjille. Käyttöjärjestelmä asennettiin perusasennuksena, ilman graafista käyttöliittymää tai muuta ylimääräistä. Asennuksessa otettiin käyttöön Logical Volume Management (LVM), joka mahdollistaa monipuolisemman levyjen hallinnan, kuten levyosion koon muuttamisen jopa sen ollessa käytössä. Ennen valvontaohjelmiston asennusta käyttöjärjestelmän perusasetukset oli laitettava kuntoon. Tämä sisälsi verkon asetukset, Network Time Protocol (NTP) -aikapalvelun käyttöönoton sekä Secure Shell (SSH) -hallintayhteyden luonnin.

5.3 Perusosat

Käyttöjärjestelmän perusasetusten jälkeen asennettiin itse valvontaohjelma, Zenoss Core, jonka uusin versio asennushetkellä oli 2.4.2. Ohjelman asentaminen ja käynnistäminen oli yksinkertaista eikä ongelmia tullut vastaan. Asennus on kuvattu ohjekirjalitteen (liite 1) kappaleessa 2. Oletuksena Zenoss käyttää salaamatonta HTTP-yhteyttä web-käyttöliittymän yhteyksiin. Yhteys haluttiin kuitenkin salatuksi, joten käyttöön otettiin Apache-web-palvelin. Sen tehtävä on toimia välityspalvelimena, jo-

hon Zenossin web-käyttöliittymän käyttäjät ottavat salatun Transport Layer Security (TLS) -yhteyden, sekä välittää tämä liikenne eteenpäin sovelluspalvelin Zopelle.

Apachen asennuksen jälkeen luotiin Zenoss-palvelimelle salattua yhteyttä varten varmenne. Salaukseen käytetään julkisen avaimen järjestelmää (Public Key Infrastructure), jossa palvelimella on yksityinen salausavaimensa ja siihen yhteydessä oleva laite salaa viestinsä yksityisestä avaimesta johdetulla julkisella avaimella. Varmen- teen, joka hyväksytään otettaessa yhteys web-selaimella ensimmäisen kerran palveli- meen, mukana toimitetaan julkinen salausavain. Apachen asennus, asetukset varmen- teelle sekä välityspalvelimeksi asettaminen on kuvattu ohjekirjaliitteen kappaleessa 3.

5.4 Asetukset

5.4.1 Yleistä

Edellisessä kappaleessa kuvailtiin ohjelman perusosien asennus. Suurin osa työstä kuitenkin käsitti varsinaisen sisällön saamisen pystytetyn rungon päälle. Ohjekirjaliite (liite 1) keskittyy pääasiassa näiden toimenpiteiden tarkempaan kuvaamiseen. Ensimmäinen vaihe järjestelmän pystytyksen jälkeen oli verkkojen läpikäyminen ja seurattavien laitteiden lisääminen järjestelmään, minkä jälkeen laitteiden SNMP- ja WMI- asetukset oli määriteltävä sekä siirtoprotokollien tarvitsemat portit avattava palomuu- rista. Järjestelmään tarvittavia lisäosia kartoitettiin, testattiin ja otettiin käyttöön. Li- säksi luotiin itse asetuspohjilla UPS-laitteille, lämpömittareille sekä Dynamic Host Control Protocol (DHCP) -palvelimille SNMP:tä käyttävä seuranta.

Yleissääntönä voisi sanoa, että kaikesta Zenossin keräämästä numeerisesta datasta, mm. virtalähteiden jännitteet, tuulettimien kierrosnopeudet, kiintolevyjen kirjoitus- ja lukuvirheet, se myös piirtää kuvaajat. Siispä yksittäisen komponentin sivulta voi näh- dä historiallista tietoa komponentista. Esimerkiksi C:\-kiintolevyosion kuvaajasta näh- dään levytilan käytön kehitys pitkältä aikaväliltä. Tätä tietoa taas voidaan käyttää apu- na arvioitaessa milloin osio täyttyy. Raportit, joiden avulla voidaan koota samalle si- vulle mitä tahansa tietoa monesta eri laitteesta, helpottavat tällaista ennakoivaa seu- rantaa huomattavasti.

5.4.2 Windows

Windowsissa käyttöön otettiin tarpeen mukaan joko SNMP:n versio 2c tai 3. 2c-version käyttöönotto on helppoa, sillä Windows tukee sitä suoraan. Tarvittavat asetukset, yhteisönimen muutos ja oikeudet, voidaan muuttaa suoraan Windowsin palvelunhallinnasta. Salatun liikenteen mahdollistavaa SNMPv3:a varten Windows-palvelimelle on asennettava välityspalvelimeksi Net-SNMP-ohjelma, joka vaatii myös OpenSSL:n asennuksen. Windows-palvelimelle asennetun Net-SNMP:n ainoa tehtävä on liikennöidä salatusti Zenoss-palvelimen kanssa ja välittää tämä liikenne paikallisesti Windowsin omalle SNMP-agentille sen ymmärtämässä salaamattomassa muodossa. Trap-viesteihin Net-SNMP:tä ei käytetä, sillä Zenoss ei tue versio 3:n Trap-viestejä. SNMP:n käyttöönotto Windows-palvelimessa on kuvattu tarkemmin ohjekirjaliitteen kappaleissa 5.1 ja 5.2. Kun SNMP-asetukset ovat kunnossa, nähdään Zenossissa Windows-koneista suoraan seuraavia tietoja:

- laitteen Status-välilehdeltä (ks. kuvio 7) perustiedot kuten käyttöjärjestelmäversio sekä käynnissäoloaika
- verkkoliitännät ja niiden tarjoamat reitit, sekä kuvaajat yksittäisten verkkokorttien liikennemääristä ja virheistä (ks. kuvio 8, Interfaces ja Routes)
- kiintolevyosiot ja niiden tilankäyttö (ks. kuvio 8, File systems)
- yksittäinen käyttöjärjestelmän prosessi tai IP-palvelu voidaan määritellä seurattavaksi, jolloin voidaan seurata, kuinka paljon prosessi käyttää suoritinta ja muistia sekä havaitaan mahdollinen prosessin kaatuminen (ks. kuvio 8, kohdat OS processes ja IP services)
- lista asennetuista ohjelmista laitteen Software-välilehdellä
- SNMP-kyselyillä tietonsa hakevien lisäosien ja asetuspohjien tarjoamat tiedot, joista enemmän lisäosia käsittelevässä kappaleessa 5.5.

The screenshot displays the Zenoss Status interface for a specific device. At the top, there are navigation tabs: Status, OS, Hardware, Software, Events, Perf, and Edit. The main content is divided into two primary sections: Device Status and Device Information.

Device Status: This section shows the device's overall health. The status is 'Up', indicated by a green circle. A vertical stack of colored circles (red, orange, yellow, blue, grey, green) represents different levels of severity. Key metrics include:

- Availability: 100.000%
- Uptime: Unknown
- State: Production
- Priority: Normal
- Locks: None
- Last Change: 2009/08/20 11:42:11
- Last Collection: 2009/08/20 11:42:12
- First Seen: 2009/06/26 15:03:48

 A table lists components and their status:

Component Type	Status
cpqSm2Cntlr	●
IpRouteEntry	●
HPPowerSupply	●
cpqDaCntlr	●
HPsdFan	●

Device Information: This section provides detailed metadata about the device.

- Organizers:** Location (None), Groups (None), Systems (None), Collector (localhost).
- OS:** Tag #, Serial #, HW Make (HP), HW Model (ProLiant DL380 G5), OS Make (Microsoft), OS Version (Microsoft Windows Server 2003, Standard Edition Service Pack 2).
- Rack Slot:** Name, Contact, Location.
- Description:** Hardware: x86 Family 6 Model 15 Stepping 6 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
- Comments:** (Empty field)
- Links:** (Empty field)

KUVIO 7. Laitteen Status-välilehti Zenossissa.

Asentamalla SNMP Informant -laajennuksen Windowsiin voi SNMP:n kautta saada vielä lisää tietoa. Laajennus asennettiin vain Domain Controller -palvelimiin, joissa WMI-seurantaa ei otettu käyttöön. SNMP Informantin kautta saadaan kuvaajat laitteen Perf-välilehdelle suorittimen ja keskusmuistin käytöstä sekä sivutuksesta (paging).

/Devices /Server /Windows /SNMPv1_2_WMI_ /HP ProLiant / Zenoss server time: 14:26:00

Status OS Hardware Software Events Perf Edit

Interfaces Monitored

Select: All None

Name	IP Address	Network	MAC	O	A	M	Lock
<input type="checkbox"/> HP NC7761 Gigabit Server Adapter				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> MS TCP Loopback interface	127.0.0.1/8			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

1 of 2 < > show all Page Size 40 ok

IP Services Monitored

Name	Proto	Port	Ips	Description	Status	M	Lock
1 of 0 < > show all Page Size 40 ok							

Win Services Monitored

Caption	StartMode	StartName	Name	Status	M	Lock
<input type="checkbox"/> DHCP Server	Auto	LocalSystem	DHCPServer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

1 of 1 < > DHCP Server > > show all Page Size 40 ok

OS Processes Monitored

Name	Class	Restarts	Fail Severity	Status	M	Lock
1 of 0 < > show all Page Size 40 ok						

File Systems

Mount	Total bytes	Used bytes	Free bytes	% Util	M	Lock
<input type="checkbox"/> C:\ Label: Serial Number 588d0c4a	33.9GB	11.4GB	22.5GB	33	<input checked="" type="checkbox"/>	

Routes

Select: All None

Destination	NextHop	Interface	Protocol	Type	Lock
<input type="checkbox"/> 0.0.0.0/0		HP NC7761 Gigabit Server Adapter	netmgmt	indirect	
<input type="checkbox"/>		HP NC7761 Gigabit Server Adapter	local	direct	
<input type="checkbox"/> 127.0.0.0/8	(None)	MS TCP Loopback interface	local	direct	
<input type="checkbox"/> 224.0.0.0/4		HP NC7761 Gigabit Server Adapter	local	direct	

KUVIO 8. Laitteen OS-välilehti Zenossissa.

WMI-seurantaa varten, mikäli välissä oli palomuri, määriteltiin Windows-palvelimelle DCOM-protokollan käyttämät portit. Nämä Windowsin rekisteriin määriteltävät portit on muutoksen jälkeen vielä avattava palomuurista. Tämän jälkeen palvelimelle on luotava käyttäjä, jolla on riittävästi oikeuksia WMI-seurantaa varten. Järjestelmänvalvojatason käyttäjä on luonnollisesti tällainen, mutta teoriassa mahdollista on myös käyttäjän, jolla on vain juuri sen tarvitsemat oikeudet, luominen. Tämä on kuitenkin työlästä, eikä tulos ole välttämättä odotetunlainen. Tässä työssä onkin luotu ainoastaan järjestelmänvalvojan oikeuksilla varustettuja WMI-käyttäjää. Kun WMI-käyttäjä on luotu palvelimen päähän, täytyy seuranta ottaa käyttöön Zenoss-palvelimen web-käyttöliittymässä muokkaamalla laitteen zProperties-sivua. WMI-seurannan käyttöönotto on kuvattu tarkemmin ohjekirjaliitteen kappaleessa 5.3. Sillä saadaan käyttöön seuraavia lisäominaisuuksia:

- laitteen Events-välilehdelle saadaan tapahtumat suoraan Windowsin omista lokeista
- Windows-palveluiden seuranta (ks. kuvio 8, osio Win services, jossa SNMP- ja WMI-seurannassa olevaan Windows-palvelimeen on lisätty seurattavaksi Windowsin palvelu DHCP-palvelin)
- WMI-kyselyillä tietonsa hakevien lisäosien ja asetuspohjien tarjoamat tiedot, joista enemmän lisäosia käsittelevässä kappaleessa 5.5.

5.4.3 Linux

SNMP:tä varten Linux-palvelimille asennettiin Net-SNMP- ja OpenSSL-ohjelmat. SNMPv3:n käyttöönotto Linuxissa on Windowsia yksinkertaisempaa, sillä käyttäjien luontiin voidaan käyttää net-snmp-config-komentoa ja Net-SNMP:n rinnalla ei ole käytössä toista SNMP-agenttia. Seurannan käyttöönotto on kuvattu ohjekirjaliitteen kappaleessa 6. SNMP:n kautta saadaan Linux-palvelimista tietoja, jotka ovat samat kuin Windows-palvelimesta pelkällä SNMP:llä haetut tiedot, lukuun ottamatta listaa asennetuista ohjelmista. Lisäksi Linux-palvelimilta saadaan Perf-välilehdelle myös neljä suorituskykykuvaajaa, sisältäen suorittimen ja muistin käyttöasteen sekä kuormituksen ja kiintolevyn käytön (ks. ohjekirjaliitteen kuvio 4).

5.4.4 Muut laitteet

Palvelimissa SNMP-asetusten muutokset voivat olla työläitä. Sen sijaan UPS- ja SDSL-laitteissa sekä muissa sekalaisissa laitteissa, kuten lämpömittareissa, tarvittavat muutokset ovat lähes aina yksinkertaisia. Näistä laitteista ei yleensä löydy tukea SNMP:n versiolle 3 ja ainoat mahdolliset muutokset ovat SNMP-yhteisönimet ja Trap-viestien kohdeosoitteet. Haaste muodostuukin Zenoss-ohjelman päässä, sillä vähänkin erikoisemmat laitteet antavat suoraan ainoastaan suppeat perustiedot. Asennettavilla lisäosilla voi saada lisää tietoa näkyville, kuten Powerwaren UPS-laitteen tapauksessa. Jos sopivaa lisäosaa ei löydy, esimerkkinä Newaven UPS-laite, sopiva asetus pohja on tehtävä itse.

5.5 Lisäosat

Lisää ominaisuuksia seurantaan haettiin asentamalla Zenoss-ohjelmaan lisäosia eli ZenPackeja. Lisäosat käyttävät tietojen hakemiseen yleensä joko SNMP:tä tai WMI:tä ja ne voivat vaatia myös lisämuutoksia palvelimen päähän normaalien SNMP- ja WMI-asetusten lisäksi. Seuraavissa kappaleissa on esitelty tärkeimmät käyttöönotetut lisäosat.

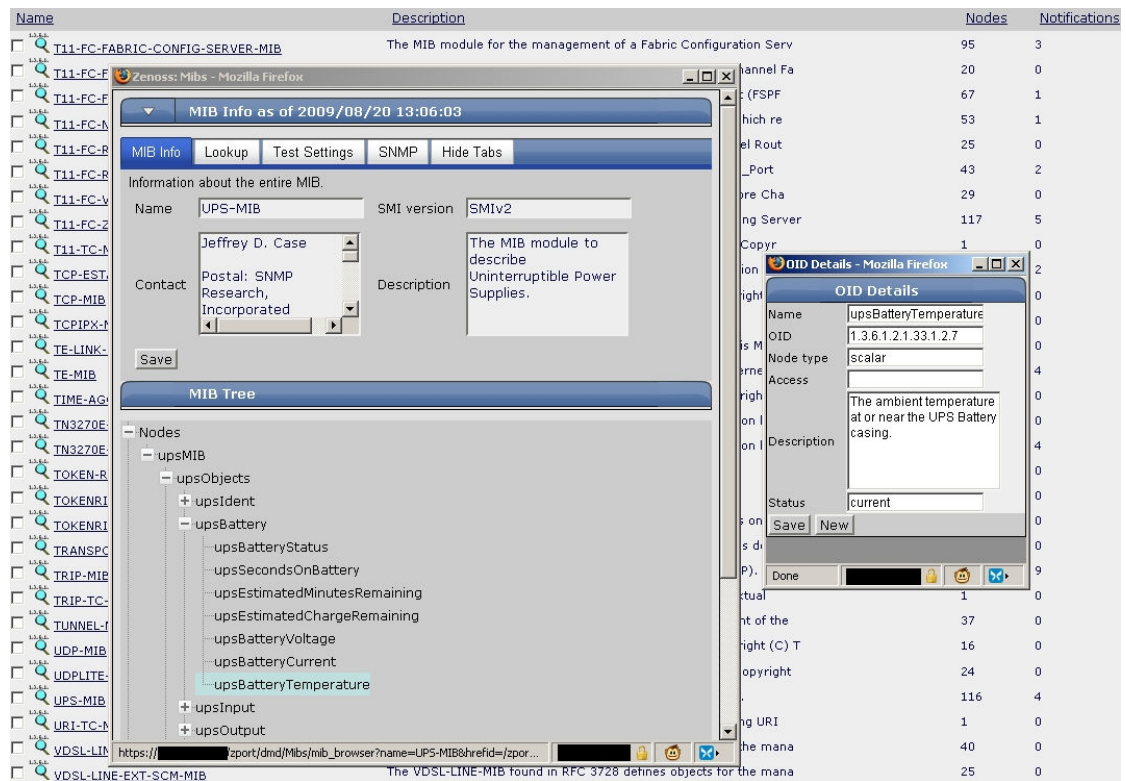
Apache monitor seuraa Linuxiin tai Windowsiin asennetun Apache-web-palvelimen tilaa ja piirtää siitä neljä kuvaajaa laitteen Perf-välilehdelle. Lisäosan toiminta vaatii muutoksia Apache-palvelimen asetustiedostoon, minkä jälkeen palvelin ylläpitää käyttötilastoa web-sivuna, jota Zenossiin asennettu Apache monitor seuraa HTTP-protokollan avulla. Lisäosan käyttöönotto on kuvattu tarkemmin ohjekirjaliitteen kappaleessa 7.2 ja liitteen kuviossa 7 näytetään lisäosalla saatavat kuvaajat.

Dell monitor on suunniteltu antamaan lisää tietoja Dellin palvelimista SNMP:n kautta. Lisäosan toiminta vaatii Dell-palvelimeen asennetun Dell OpenManage -ohjelman. Laitteen Hardware-välilehdelle tulevat lisätiedot haetaan suoraan OpenManagen ylläpitämistä tiedoista. Lisäosalla nähdään mm. palvelimen osien mallit, tuulettimien ja virtalähteiden tilat sekä fyysiset kiintolevyt ja näiden loogiset asemat (RAID-tilat). Lisäosan käyttöönotto on kuvattu tarkemmin ohjekirjaliitteen kappaleessa 7.3 ja liitteen kuviossa 8 näytetään esimerkki lisäosalla saatavista lisätiedoista Hardware-välilehdeltä.

HP ProLiant ZenPack muistuttaa toiminnaltaan hyvin paljon Dell monitor -lisäosaa. Sen tehtävä on hakea SNMP:llä HP ProLiant -palvelimeen asennetusta HP Insight Management Agents -ohjelmasta lisää tietoja laitteistosta laitteen Hardware-välilehdelle. Saatavat tiedot ovat lähes samat kuin Dellin palvelimissa. Lisäosan käyttöönotto on kuvattu tarkemmin ohjekirjaliitteen kappaleessa 7.4 ja liitteen kuviossa 9 näytetään esimerkki lisäosalla saatavista lisätiedoista Hardware-välilehdeltä.

MIB browser lisää Zenossin käyttöliittymään mahdollisuuden tarkastella hallintatietokantoja eli MIB-tiedostoja ja lisää ominaisuuksia niiden hallintaan. Zenoss käyttää järjestelmään ladattuja MIB-tiedostoja SNMP:n Trap-viestien kääntämiseen tapahtumalokissa OID-numerosarjoista sanallisiksi kuvauksiksi. Lisäosan avulla on myös

mahdollista ladata MIB-tiedosto suoraan järjestelmään pelkän web-osoitteen perusteella. Kuviossa 9 on esitetty lisäosan toimintaa MIB-selaimena.



KUVIO 9. MIB:n tutkimista Zenoss-ohjelmassa MIB browser -lisäosalla.

Microsoft IIS kerää tietoa Microsoftin Internet Information Services (IIS) -palvelimen käytöstä WMI:llä kolmeen suorituskykykuvaajaan laitteen Perf-välilehdelle. Ohjekirjaliitteen kuviossa 10 on esitetty IIS-seurannassa olevan laitteen tarjoamat kuvaajat.

Powerware UPS seuraa Powerwaren valmistaman UPS-laitteen toimintaa SNMP:llä. Laitteen Perf-välilehdelle saatavat viisi kuvaajaa sisältävät mm. arvion jäljellä olevasta varausajasta sekä lämpötilan. Kuvaajat on esitetty ohjekirjaliitteen kuviossa 11.

SQL 2000/2005 Server performance seuraa WMI:n avulla Microsoftin SQL-tietokantaohjelmiston toimintaa ja piirtää tiedot kuuteen kuvaajaan laitteen Perf-välilehdelle. Lisäosan käyttöönottoa varten oli korvattava Zenossin mukana toimitettu Winexe-ohjelman versio uudemmalla ja muokattava lisäosan käyttämää Perl-skriptiä

viittaamaan uuteen Winexe-versioon. Lisäosalla saatavat kuvaajat on esitetty ohjekirjaliitteen kuviossa 12 ja käyttöönotto kappaleessa 7.7.

Windows WMI device template liitettiin kaikkiin WMI-seurannassa oleviin Windows-palvelimiin. Se kysyy suorittimen käyttöasteen SNMP:n kautta sekä vapaan keskusmuistin määrän, kiintolevyn jonon ja sivutuksen WMI:n kautta. Tiedoista piirretään kuvaajat laitteen Perf-välilehdelle. Lisäosan käyttämä skripti toimi ainoastaan SNMP:n versioilla 1 ja 2. Koska skriptin ajama Snmpwalk-komento on hieman erilainen SNMP:n versiosta riippuen, muokattiin skripti yhteensopivaksi kaikille versioille. Uusi skripti kysyy SNMP-versiota laitteen asetussivulta (zProperties), minkä perusteella valitaan ajettava komento. Tarkemmin lisäosan käyttöönotto on kuvattu ohjekirjaliitteen kappaleessa 7.8 ja sen tarjoamat kuvaajat liitteen kuviossa 13.

WMI Exchange monitor seuraa Microsoftin Exchange-sähköpostipalvelinta. Laitteen Perf-välilehdelle piirretyt kuvaajat sisältävät käyttäjien ja erilaisten pyyntöjen määrän sekä palvelimen Intelligent Message Filtering (IMF) -suodatustoiminnon seurannan. Käyttöönotossa oli muokattava lisäosan skriptiä hakemaan Wmic-ohjelmaa oikeasta paikasta. Käyttöönotto on kuvattu tarkemmin ohjekirjaliitteen kappaleessa 7.9. Lisäosan tarjoamat kuvaajat, lukuun ottamatta IMF-toimintoa, on esitetty liitteen kuviossa 14.

WMI performance monitor hakee WMI:n kautta monipuolisesti tietoa suorittimen ja muistin käyttöasteesta, kiintolevyn jonosta, muistin sivutuksesta, IOPS:stä, eli kiintolevyn luku- ja kirjoitusaktiiviteetista sekunnin aikana, ja koneeseen muodostetuista yhteyksistä. Lisäosa ei kuitenkaan käyttöönotettuna toiminut odotetulla tavalla, ja monet sen tuloksista olivat vääristyneitä. Korvaajaksi asennettiin aiemmin esitelty vähemmän ominaisuuksia sisältävä Windows WMI device template -lisäosa. WMI performance monitor -lisäosasta käyttöön jätettiin kuitenkin osa, joka seuraa palvelimeen muodostettujen etäyhteyksien määrää. Toiminnosta oli hyötyä Citrix-ympäristöä ylläpitävien palvelimien seurannassa. Käyttöönotto on kuvattu ohjekirjaliitteen kappaleessa 7.10 ja liitteen kuviossa 15 esitetään esimerkkikuvaaja palvelimeen muodostetuista yhteyksistä.

5.6 Asetuspohjat

Joillekin laitteille ja toiminnoille ei löytynyt valmista lisäosaa. Uusien asetuspojhien luonti oli varsin helppoa pienen totuttelun jälkeen. Esimerkki uuden asetuspojhian luonnista on esitetty ohjekirjaliitteen kappaleessa 8.1. Käyttöönnotossa luotiin itse kolme erilaista asetuspojhjaa.

Newaven valmistama UPS-laite käytti IETF:n RFC 1628 -dokumentissa määrittelemää UPS-MIB:tä. MIB-tiedostoa tutkittiin erillisellä MIB-selaimella ja sen perusteella valittiin haettavat tiedot. Tiedot, kuten lämpötila ja jäljellä oleva varaus, lisättiin uuteen asetuspojhiaan. Halutuille arvoille lisättiin kynnsarvot, ja tiedot sekä kynnsarvot lisättiin lopuksi kuvaajiin. Lopputuloksena asetuspojhja piirtää tiedot kuuteen kuvaajaan laitteen Perf-välilehdelle. UPS-laitteen asetuspojhja on kuvattu ohjekirjaliitteen kuviossa 23 ja sen piirtämistä kuvaajista kolme kuviossa 24.

Kaupungin verkossa oli käytössä useita Windows- ja Linux-pohjaisia DHCP-palvelimia. Näille tehtiin yksinkertainen seuranta, joka ilmoittaa varattujen ja vapaana olevien osoitteiden määrän. Windows-palvelimilta nämä tiedot saa kysytyä suoraan SNMP:n avulla, mutta Linux-palvelimille oli asennettava erillinen Dhcp-snmpd-skripti. Kuvaajan värejä muokattiin niin, että vapaat osoitteet näkyvät erottuvat selkeästi vihreällä värillään. DHCP-seurannan luonti on kuvattu ohjekirjaliitteen kappaleessa 8.2 ja kuviossa 25 esitetään kuvaaja, jonka asetuspojhja luo laitteen Perf-välilehdelle.

Eri palvelinhuonetiloissa sijaitsevat lämpömittarit käyttävät omaa, Comet Systems -valmistajan määrittelemää, hallintatietokantaansa. Luotu asetuspojhja seuraa lämpötilaa sekä hälytyksen tilaa. Kynnsarvoja ei säädetty, sillä hälytykset sähköpostiin tulevat suoraan lämpömittarilta. Asetuspojhian tarkoituksena on ainoastaan kerätä ja näyttää lämpötilan historiatietoa, mitä ei mittarin omilla työkaluilla voi tehdä. Luotu asetuspojhja on esitetty ohjekirjaliitteen kuviossa 27.

6 POHDINTA

6.1 Yleistä

Työn toteutus täytti tehtävälle asetetut vaatimukset. Valittu ohjelma on monipuolinen ja se on laajennettavissa varsin pitkälle. Toimeksiantaja piti hyvänä erityisesti ohjelman Event console -ominaisuutta, joka kerää kaikkien laitteiden tapahtumat yhdelle sivulle. Vaikka Zenossin käyttöliittymä on selkeä ja looginen, sen kunnollinen hallinta vaatii toki oman opettelunsa. Ohjelmasta saa kuitenkin oikein käytettynä hyvän avun laitteiden seurantaan ja vikojen nopeaan havaitsemiseen ja ennakointiin. Jos järjestelmä osoittautuu käyttökelpoiseksi ja toimintoja halutaan laajentaa, mahdollista on myös ohjelmiston asentaminen tehokkaamalle palvelimelle.

Jälkeenpäin ajateltuna oli hyvä, että verkkotulostimet sekä kopiokoneet putosivat työn vaatimuslistalta pois, sillä kaikki niiden tarjoama tieto olisi vaikuttanut edelleen heikentävästi Zenoss-palvelimen suorituskykyyn ja samalla vaikuttanut myös muiden palvelimien seurantaan. Kaikki toteutukseen käytetyt ohjelmat olivat ilmaisia, joten pystyitin vastaavan, tosin luonnollisesti pienemmän, valvontaympäristön myös omaan kotiini. Tässä testiympäristössä oli hyvä kokeilla joitakin kaavailtuja ominaisuuksia, kuten Net-SNMP:tä Windowsissa, ennen niiden asentamista tuotantokäytössä olleisiin palvelimiin.

6.2 Ongelmat

Uusia laitteita ja ominaisuuksia vähitellen lisättäessä huomattiin web-käyttöliittymässä toiminnan hidastumista. Tarkastelemalla palvelimen itse itsestään keräämiä suorituskykykuvaajia pääteltiin, että muistin lisääminen voisi auttaa ongelmaan. Selkeästi se auttoi, tämän jälkeenkin tosin esiintyi välillä pientä viivettä kommentojen käsittelyssä. Zenoss varaa toimintoihinsa paljon keskusmuistia ja nykyisen neljän gigatavun muistin voi sanoa olevan todella tehokkaassa käytössä.

WMI performance monitor -lisäosa ehti olla melko kauan testikäytössä, kunnes huomattiin, että monet sen tuottamista kuvaajista olivat vääristyneitä. Tämä lisäosa jouduttiin lähes kokonaan korvaamaan suppeamilla ominaisuuksilla varustetulla Windows WMI device template -lisäosalla. Lisäksi HP ProLiant ZenPack -lisäosassa on virhe kynnyksarvoissa, jotka vaikuttavat kiintolevyjen virheiden seurantaan. Ongelman voi kiertää muuttamalla itse kynnyksarvoja ongelmia aiheuttavien laitteiden kohdalla.

Joihinkin Windows-palvelimiin ei saatu toimivaa WMI-toteutusta, vaan yhteydenottoyritykset päättyivät virhekoodiin, jonka epäiltiin viittaavan jonkinlaiseen Windowsin sisäiseen WMI-ongelmaan. Zenossin Zenhub-daemonin lokia tutkiessa huomattiin, että välillä Zenoss ei pääse käyttämään MySQL-tietokantaansa aikakatkaisun vuoksi. Tämä pyrittiin estämään kaksinkertaistamalla MySQL:n aikakatkaisun aika MySQL:n konfigurointitiedostoa muokkaamalla.

6.3 Kehitysmahdollisuudet

Zenoss Core tarjoaa paljon ominaisuuksia, joihin tässä työssä ei kunnolla ehditty tutustua, kuten Linux-lokien keräyksen Syslog-palvelun kautta tai seurannan SSH-protokollan avulla. Uusia ZenPack-lisäosia julkaistaan jatkuvasti. Tätä kirjoitettaessa viimeisimmän kuukauden aikana oli julkaistu käyttäjien tekemiä uusia lisäosia kymmenen kappaletta. Uusilla lisäosilla voi korvata nyt käytössä olevia tai lisätä valvontajärjestelmään kokonaan uusia ominaisuuksia.

LÄHTEET

About MySQL. 2009. MySQL-ohjelman kotisivu. Viitattu 8.8.2009.

<http://www.mysql.com/about>.

Badger, M. 2008. Ote kirjasta Zenoss Core network and system monitoring. Viitattu

4.8.2009. <http://www.packtpub.com/article/installation-of-zenoss-core>.

Curry, J. 2008. Open source management options. Julkaistu 30.9.2008. Viitattu

11.8.2009. <http://www.skills-1st.co.uk/papers/jcurry.html>, Open Source Management Options.

Dastrup, J.C. 2008a. Advanced WMI Exchange monitor ZenPack for Zenoss Core.

Julkaistu 31.3.2008. Viitattu 6.7.2009. <http://blog.dastrup.com/?p=26>.

Dastrup, J.C. 2008b. Advanced WMI performance monitor ZenPack for Zenoss Core.

Julkaistu 26.3.2008. Viitattu 6.7.2009. <http://blog.dastrup.com/?p=13>.

DCOM technical overview. 1996. Microsoftin Developer network -sivu. Viitattu

20.8.2009. <http://msdn.microsoft.com/en-us/library/ms809340.aspx>.

Dubie, D. 2007. Management heavies get poor grades in Gartner survey. Julkaistu

3.5.2007. Viitattu 20.8.2009. <http://www.networkworld.com/news/2007/050307-management-gartner.html>.

GNU General Public License, version 2. 1991. GNU-projektin kotisivu. Viitattu

8.8.2009. <http://www.gnu.org/licenses/old-licenses/gpl-2.0.html>.

Google Maps/Google Earth APIs terms of service. 2009. Googlen kotisivu. Päivitetty

27.5.2009. Viitattu 4.8.2009. <http://code.google.com/intl/fi/apis/maps/terms.html>.

Hautaniemi, M. 1994. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. Dip-

lomityö. Teknillinen korkeakoulu, tietotekniikan osasto. Viitattu 20.8.2009.

<http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/diplomityo.book.html>, 4.2.2
Yleiskuva SNMP-protokollan arkkitehtuurista.

Hyperic HQ 4.0 product tour. 2009. Hyperic HQ -ohjelman kotisivu. Viitattu 10.8.2009. <http://support.hyperic.com/display/DOC/HQ+Documentation>, Product tour.

Introduction to Pandora FMS. 2008. Pandora FMS -ohjelman kotisivu. Päivitetty 8.12.2008. Viitattu 12.6.2009.
http://openideas.info/wiki/index.php?title=Pandora_2.0:Documentation_en:Introduction.

Kozierok, C.M. 2005. The TCP/IP guide. Päivitetty 20.9.2005. Viitattu 9.8.2009.
http://www.tcpiptide.com/free/t_TCP/IPInternetStandardManagementFrameworkArchitecture.htm.

Levitte, R. n.d. OpenSSL - howto certificates. Viitattu 29.6.2009.
<http://www.openssl.org/docs/HOWTO/certificates.txt>.

Microsoft NTLM. 2009. Microsoftin Developer network -sivu. Viitattu 21.8.2009.
<http://msdn.microsoft.com/en-us/library/aa378749%28VS.85%29.aspx>.

Nelson, M. 1998. Using Distributed COM with firewalls. Microsoftin Developer network -sivu. Julkaistu 20.6.1998. Viitattu 14.7.2009. <http://msdn.microsoft.com/en-us/library/ms809327.aspx>.

Net-SNMP - Readme.win32. 2007. Net-SNMP-ohjelman kotisivu. Päivitetty 2.3.2007. Viitattu 20.6.2009. <http://www.net-snmp.org>, documentation, readme.win32.

Net-SNMP readme files. 2007. Net-SNMP-ohjelman kotisivu. Päivitetty 2.3.2007. Viitattu 15.7.2009. <http://net-snmp.sourceforge.net>, documentation.

OpenNMS - documentation. 2007. OpenNMS-ohjelman kotisivu. Päivitetty 18.5.2007. Viitattu 10.8.2009. <http://www.opennms.org/wiki/Documentation>.

OpenNMS - FAQ-about. 2009. OpenNMS-ohjelman kotisivu. Päivitetty 7.6.2009. Viitattu 10.8.2009. <http://www.opennms.org/wiki/FAQ-About>.

Pellonpää, J. 2008. Verkonhallintaohjelmiston käyttöönotto. Opinnäytetyö. Jyväskylän ammattikorkeakoulu, tekniikka ja liikenne, informaatioteknologian instituutti, tietotekniikan koulutusohjelma.

Pieksämäki. 2009. Pieksämäen kaupungin www-sivut. Viitattu 16.7.2009. <http://www.pieksamaki.fi/kaupunki>.

RFC 1155. 1990. Structure and identification of management information for TCP/IP-based Internets. Internet Engineering Task Force.

RFC 3410. 2002. Introduction and applicability statements for Internet standard management framework. Internet Engineering Task Force.

RFC 3414. 2002. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). Internet Engineering Task Force.

Ribak, J. n.d. Generating an SSL certificate with Apache+mod_ssl. Viitattu 29.6.2009. <http://slacksite.com/apache/certificate.php>.

VMware to acquire SpringSource. 2009. VMware-valmistajan kotisivu. Julkaistu 10.8.2009. Viitattu 22.8.2009. <http://www.vmware.com/company/news/releases/springsource.html>.

Web-Based Enterprise Management. 2009. Distributed Management Task Force, Inc. Viitattu 15.8.2009. <http://www.dmtf.org/standards/wbem>.

Win32_NTLogEvent class. 2009. Microsoftin Developer network -sivu. Viitattu 18.8.2009. [http://msdn.microsoft.com/en-us/library/aa394226\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa394226(VS.85).aspx).

Windows Management Instrumentation: background and overview. 2000. Microsoftin Developer network -sivu. Viitattu 15.8.2009. <http://msdn.microsoft.com/en-us/library/ms811553.aspx>.

Zenoss Administration for version 2.4.2. 2009. Zenoss-ohjelman kotisivu. Viitattu 4.8.2009. <http://www.zenoss.com/community/docs>, Zenoss Administration Guide PDF.

Zenoss Developer's guide for version 2.4. 2009. Zenoss-ohjelman kotisivu. Viitattu 8.8.2009. <http://www.zenoss.com/community/docs>, Zenoss Developer's Guide PDF.

Zenoss documentation. 2009. Zenoss-ohjelman kotisivu. Viitattu 28.6. 2009. <http://www.zenoss.com>, community, documentation.

Zenoss - downloads. 2009. Zenoss-ohjelman kotisivu. Viitattu 4.8.2009. <http://www.zenoss.com/download/links?creg=null>.

Zenoss team - Management. 2009. Zenoss-ohjelman kotisivu. Viitattu 4.8.2009. <http://www.zenoss.com/about/team>.

ZenPack project site. 2009. Zenoss-ohjelman kotisivu. Viitattu 2.7.2009. <http://www.zenoss.com>, community, ZenPacks.

LIITTEET

Liite 1. Zenoss Core -käyttöohje

Zenoss Core -käyttöohje

SISÄLTÖ

1	YLEISTÄ	48
2	ZENOSS-ASENNUS	48
3	APACHE-ASENNUS	50
3.1	Varmenne	50
3.2	Välityspalvelimeksi muuttaminen	50
4	LAITTEEN LISÄÄMINEN	51
5	WINDOWS-SEURANTA	52
5.1	SNMPv2c.....	52
5.2	SNMPv3 ja Net-SNMP.....	52
5.3	WMI.....	56
5.3.1	Asetukset palomuuria varten	56
5.3.2	Käyttäjän luonti	56
5.3.3	Toiminnan testaus	57
6	LINUX-SEURANTA.....	57
6.1	SNMPv2c.....	59
6.2	SNMPv3.....	59
7	ASENNETUT LISÄOSAT (ZENPACKS).....	60
7.1	Yleistä	60
7.2	Apache monitor	62
7.3	Dell monitor	63
7.4	HP ProLiant ZenPack.....	65
7.5	Microsoft IIS	66
7.6	Powerware UPS	67
7.7	SQL 2000/2005 Server performance	69
7.7.1	Muokkaukset	70
7.7.2	Käyttöönotto.....	70
7.8	Windows WMI device template	71
7.9	WMI Exchange monitor	72

7.10	WMI performance monitor.....	74
7.11	Muut lisäosat.....	75
8	ASETUSPOHJAT (TEMPLATES).....	75
8.1	Asetuspohjan luonti.....	75
8.1.1	Laitteen MIB:tä ei tiedetä.....	75
8.1.2	Laitteen MIB tiedetään.....	76
8.1.3	Uusi asetuspohja.....	78
8.1.4	Valmis asetuspohja.....	82
8.2	DHCP-palvelimen seuranta.....	84
8.2.1	Windows.....	84
8.2.2	Linux	84
8.3	Comet Systems P8510 -lämpömittarit	85
9	RAPORTIT (REPORTS)	86
10	HÄLYTYKSET (ALERTING RULES).....	88
11	OHJELMAN OMAT LOKIT	90
12	VARMUUSKOPIOINTI JA PÄIVITYS	90

KUVIOT

KUVIO 1. Laiteluokan päävalikko.....	48
KUVIO 2. SNMP-asetukset Windowsissa.....	53
KUVIO 3. Trap-asetukset Windowsissa.	54
KUVIO 4. Linux-palvelimen suorituskykykuvaajat.....	58
KUVIO 5. Lämpötilan seurannan toimivuuden testaus.....	61
KUVIO 6. Snmpwalk-komennolla haettu lämpötilan arvo.....	61
KUVIO 7. Apache monitor -lisäosan tuottamat kuvaajat.....	62
KUVIO 8. Dell Monitor -lisäosan antamat lisätiedot.....	64
KUVIO 9. HP ProLiant ZenPack -lisäosan antamat lisätiedot.	66
KUVIO 10. Microsoft IIS -lisäosan tuottamat kuvaajat.	67
KUVIO 11. Powerware UPS -lisäosan tuottamat kuvaajat.....	68
KUVIO 12. SQL 2000/2005 Server Performance -lisäosan tuottamat kuvaajat..	70
KUVIO 13. Windows WMI Device Template -lisäosan tuottamat kuvaajat.....	71
KUVIO 14. WMI Exchange Monitor -lisäosan tuottamat kuvaajat.	73
KUVIO 15. WMI performance monitor -lisäosan tuottama kuvaaja palvelimeen muodostetuista yhteyksistä.....	74
KUVIO 16. Mib-2-olion sijainti MIB-puussa.	76
KUVIO 17. iReasoningin MIB-selain.	77
KUVIO 18. Uusi tyhjä asetuspohja.	78
KUVIO 19. SNMP-tietolähde.....	79

KUVIO 20. Kynnysarvon asetus.....	79
KUVIO 21. Kuvaajan sivu.....	80
KUVIO 22. Kuvaajan tarkemmat asetukset.....	81
KUVIO 23. RFC 1628:ssa määriteltyä UPS-MIB:tä käyttävän UPS-laitteen valmis asetus pohja.....	82
KUVIO 24. Valmiin UPS-asetuspohjan luomia kuvaajia.....	83
KUVIO 26. Asetuspohjan tietolähteiksi lisätyt Linux-palvelimen DHCP-tiedot.	85
KUVIO 27. Lämpömittarin asetus pohja.....	86
KUVIO 28. Raporttien pääsivu.....	87
KUVIO 29. Kuvaajaraportin luonti.	87
KUVIO 30. Uuden hälytyksen asetusten muokkaus.	89

1 YLEISTÄ

Tämän ohjeen Zenossia koskevat ohjeet perustuvat valmistajan omiin käyttöoppaisiin, työstä saatuihin omiin käyttökokemuksiin sekä ohjelman keskustelualueelta löytyneisiin vihjeisiin. Zenossin tuottamista omista ohjekirjoista Administration guide ja Extended monitoring guide (Zenoss documentation 2009) käyvät läpi kiitettävästi suurimman osan järjestelmän asetuksista ja ominaisuuksista. Tämä ohje ei yritä korvata näitä ohjekirjoja, vaan keskittyy erityisesti kuvaamaan tämän asennuksen ominaisuuksia ja asetuksia. Läpikäytyt lisäosien ja asetus pohjien muokkaukset toimivat samalla esimerkkeinä, joista voi hakea vinkkejä uusien ominaisuuksien asennuksessa tarvittaviin muutoksiin. Lisäosat on haettu Zenossin omalta ZenPack-sivulta (ZenPack project site 2009) lukuunottamatta kahta lisäosaa, joista on mainittu erikseen. Net-SNMP:tä koskevan ohjeistuksen apuna ovat olleet ohjeet Readme.snmpv3 ja Readme.win32 (Net-SNMP readme files 2007).

Palvelimia lukuunottamatta SNMP-asetusten muutokset laitepäässä ovat yleensä hyvin yksinkertaisia, joten UPS- ja SDSL-laitteiden sekä lämpömittareiden SNMP-asetuksia, eli lähinnä yhteisönimen vaihtamista ja osoitetta johon Trap-viestit lähetetään, ei kuvailla tässä ohjeessa. Kaikki Zenossin toimintaan liittyvät komentorivin komennot suoritetaan zenoss-nimisellä käyttäjällä. \$ZENHOME, joka esiintyy usein skripteissä ja ohjeissa, viittaa Zenossin asennuskansioon, joka tässä asennuksessa on /usr/local/zenoss/zenoss, ja se on määritelty zenoss-käyttäjän kotihakemistossa tiedostossa .bash_profile.

Tekstissä symboli ▾ viittaa päävalikon punaisella ympyröityyn kohtaan kuviossa 1. Tämä painike avaa lisää toimintoja mahdollistavan lisävalikon. Punaisia *-merkkejä on käytetty ilmaisemaan, että tarkempi tieto kohdasta löytyy tekstistä myöhemmin.



KUVIO 1. Laiteluokan päävalikko.

2 ZENOSS-ASENNUS

Asennusta varten Debianin /etc/apt/sources.list-tiedostoon oli lisättävä asennuslähteeksi Zenossin pakettivarasto (repository). Tämän jälkeen ohjelman asennus suoritettiin hakemalla kaikki ohjelman tarvitsemat riippuvuudet sisältävä paketti Zenoss-stack:

```

zenoss:~# apt-get install zenoss-stack
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  zenoss-stack
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 132MB of archives.
After this operation, 450MB of additional disk space will be
used.
WARNING: The following packages cannot be authenticated!
  zenoss-stack
Install these packages without verification [y/N]? y
Get:1 http://dev.zenoss.org main/stable zenoss-stack 2.4.2-0
[132MB]
Fetched 132MB in 4min20s (506kB/s)
Selecting previously deselected package zenoss-stack.
(Reading database ... 19135 files and directories currently
installed.)
Unpacking zenoss-stack (from .../zenoss-stack_2.4.2-0_i386.deb)
...
Setting up zenoss-stack (2.4.2-0) ...
zenoss:~#

```

Zenossin asennuttua ohjelma on valmis käynnistettäväksi:

```

zenoss:/# /etc/init.d/zenoss-stack start
nohup: redirecting stderr to stdout
Starting mysqld.bin daemon with databases from
/usr/local/zenoss/mysql/data
/usr/local/zenoss/mysql/scripts/ctl.sh : mysql  started at port
3307
Daemon: zeoctl . daemon process started, pid=4478
Daemon: zopectl . daemon process started, pid=4482
Daemon: zenhub starting...
Daemon: zenjobs starting...
Daemon: zenping starting...
Daemon: zensyslog starting...
Daemon: zenstatus starting...
Daemon: zenactions starting...
Daemon: zentrap starting...
Daemon: zenmodeler starting...
Daemon: zenperfsnmp starting...
Daemon: zencommand starting...
Daemon: zenprocess starting...
Daemon: zenwin starting...
Daemon: zeneventlog starting...
zenoss:/#

```

Ohjelman käynnistyksen jälkeen palvelimeen voi ottaa yhteyden web-selaimen kautta. Zope vastaa oletuksena portista 8080. Tämä yhteys ei kuitenkaan ole salattu, joten väliin oli asennettava Apache-web-palvelin.

3 APACHE-ASENNUS

Apache asennetaan komennolla `apt-get install apache2`, minkä jälkeen voidaan siirtyä varmenteen luontiin. Ennen varmenteen luontia on asennettava myös OpenSSL-ohjelma.

3.1 Varmenne

Varmenteen luontiohje perustuu Ribakin (n.d.) ja Levitten (n.d.) ohjeisiin. TLS-yhteyttä varten Zenoss-palvelimelle on luotava varmenne. Tämä aloitetaan luomalla OpenSSL-ohjelmalla yksityinen avain.

```
openssl genrsa -out /etc/ssl/private/privkey.pem 2048
```

Edellinen käsky loi 2048-bittisen yksityisen RSA-avaimen. Tämän jälkeen luodaan varmennepyyntötiedosto käyttäen juuri luotua yksityistä avainta. Käskyn antamisen jälkeen kysytään varmenteelle annettavia X.509-asetuksia, jotka sisältävät mm. varmenteen haltijan nimen.

```
openssl req -new -key /etc/ssl/private/privkey.pem -out /etc/ssl/certs/cert.csr
```

Näin luodun varmennepyyntötiedoston voi lähettää allekirjoitettavaksi jollekin ulkopuoliselle taholle tai sen voi allekirjoittaa itse. Koska palvelin on ainoastaan tietohallinnon sisäisessä käytössä, ei ole erityistä syytä olla allekirjoittamatta varmennepyyntöä itse.

```
openssl x509 -req -days 1825 -in /etc/ssl/certs/cert.csr -signkey /etc/ssl/private/privkey.pem -out /etc/ssl/certs/server.crt
```

Edellinen käsky loi viisi vuotta voimassa olevan server.crt-nimisen itseallekirjoitetun varmenteen. Yksityinen privkey.pem-avain saa olla ainoastaan root-käyttäjän luettavissa.

3.2 Välityspalvelimeksi muuttaminen

Kun Apache on asennettu ja käynnistetty, se vastaa ulkoa tuleviin HTTP-yhteyksiin oletuksena suoraan portista 80, mikä ei ole tarkoitus. Muokataan tiedostoa `/etc/apache2/sites-available/default-ssl` seuraavasti:

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    SSLEngine on
    SSLProxyEngine on
    SSLCertificateFile /etc/ssl/certs/server.crt
```

```

        SSLCertificateKeyFile /etc/ssl/private/privkey.pem
        RewriteEngine On
        RewriteRule ^/(.*) http://<Zenoss-palvelimen osoi-
te>:8080/VirtualHostBase/https/<Zenoss-palvelimen osoi-
te>:443/VirtualHostRoot/$1 [L,P]
    </VirtualHost>
</IfModule>

```

Tiedosto kytkee päälle Apachessa salaukseen tarvittavat toiminnot sekä määrittää käytetyt varmenne- ja yksityinen avain -tiedostot. Se myös käskää palvelimen porttiin 443 (HTTPS-liikenne) tulevan liikenteen ohjattavaksi paikalliseen porttiin 8080 (Zope). Tiedosto otetaan vielä käyttöön luomalla siihen symbolinen linkki:

```

ln -s /etc/apache2/sites-available/default-ssl
/etc/apache2/sites-enabled/000-default-ssl

```

Apachen /etc/apache2/httpd.conf-tiedostoa on vielä muokattava seuraavasti:

```

ServerName <Zenoss-palvelimen domain-nimi (FQDN)>
LoadModule rewrite_module
/usr/lib/apache2/modules/mod_rewrite.so
LoadModule ssl_module /usr/lib/apache2/modules/mod_ssl.so
LoadModule proxy_module /usr/lib/apache2/modules/mod_proxy.so
LoadModule proxy_http_module
/usr/lib/apache2/modules/mod_proxy_http.so
Redirect permanent / https://<Zenoss-palvelimen osoite>

```

Tässä ladataan Apacheen välityspalvelin- ja salaustoimintoihin tarvittavat moduulit. Viimeisellä rivillä määritellään myös, että porttiin 80 tulevat yhteydet ohjataan porttiin 443. Zenossin web-käyttöliittymään pääsyyn tämän jälkeen siis riittää, että kirjoittaa osoitteeksi palvelimen osoitteen ilman porttia, jolloin muodostuu salattu TLS-yhteys.

4 LAITTEEN LISÄÄMINEN

Seurattavaksi haluttava laite lisätään Zenossiin päävalikon Add device-painikkeesta. Oletuksena avautuu sivu, josta lisätään yksittäinen laite. Laite voidaan lisätä joko IP-osoitteen tai DNS-nimen perusteella. Helpointa laitteen lisääminen on, jos lisättävälle laitteelle on valmiiksi mietittynä ja luotuna sopiva luokka. Tällöin laite perii asetukset automaattisesti luokalta eikä laitekohtaista säätöä tarvita.

Toinen vaihtoehto on käyttää Easy add -toimintoa. Tämä toiminto ei ole kovin monipuolinen, ja sen käyttö lieneekin järkevintä vain alussa, kokonaan uusia verkkoja skannattaessa.

5 WINDOWS-SEURANTA

SNMP käyttää oletuksena liikennöintiin UDP-porttia 161 sekä Trap-viesteihin porttia 162. WMI on hieman monimutkaisempi ja siitä on kerrottu erikseen WMI-otsikon alla. SNMP:n version 3 toteutus vaatii Windowsissa Net-SNMP-ohjelman asennuksen.

5.1 SNMPv2c

1. Asennetaan Windowsin SNMP-palvelu, jos sitä ei ole jo asennettu.
2. Windowsin palvelunhallinnassa SNMP-asetuksia muokataan niin, että luodaan vain luku -oikeuksilla varustettu yhteisönimi. SNMP-paketit sallitaan vain Zenoss-palvelimelta.
3. Trap-asetuksiin lisätään valittu yhteisönimi ja trap-viestien kohteeksi laitetaan Zenoss-palvelin.
4. Testataan toimivuus Zenoss-palvelimelta komennolla

```
snmpwalk -v2c -c<SNMP-yhteisönimi> <Windows-palvelimen
osoite> sysDescr.0
```

Jos kaikki on kunnossa, edellinen komento palauttaa esimerkiksi Windows Server 2003 -palvelimelta rivin

```
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15
Model 2 Stepping 7 AT/AT COMPATIBLE - Software: Windows
Version 5.2 (Build 3790 Multiprocessor Free)
```

5. Zenossin web-käyttöliittymässä SNMPv2c:tä käyttävään laitteeseen tai laiteluokkaan määritetään seuraavat asetukset zProperties-sivulla:

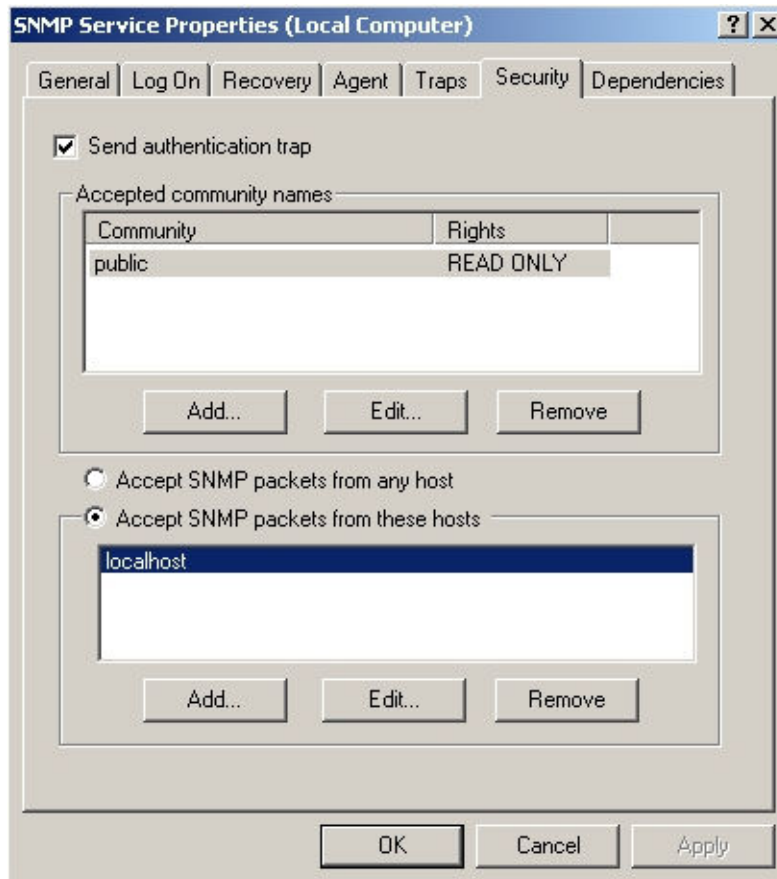
- zSnmpCommunity: <SNMP-yhteisönimi>
- zSnmpPort: <SNMPv1/2c-portti, oletus 161>
- zSnmpVer: v2c

5.2 SNMPv3 ja Net-SNMP

1. Ennen Net-SNMP:n asennusta Windows-palvelimella on oltava asennettuna OpenSSL, joka puolestaan vaatii Microsoftin Visual C++ 2008 -kirjastot.

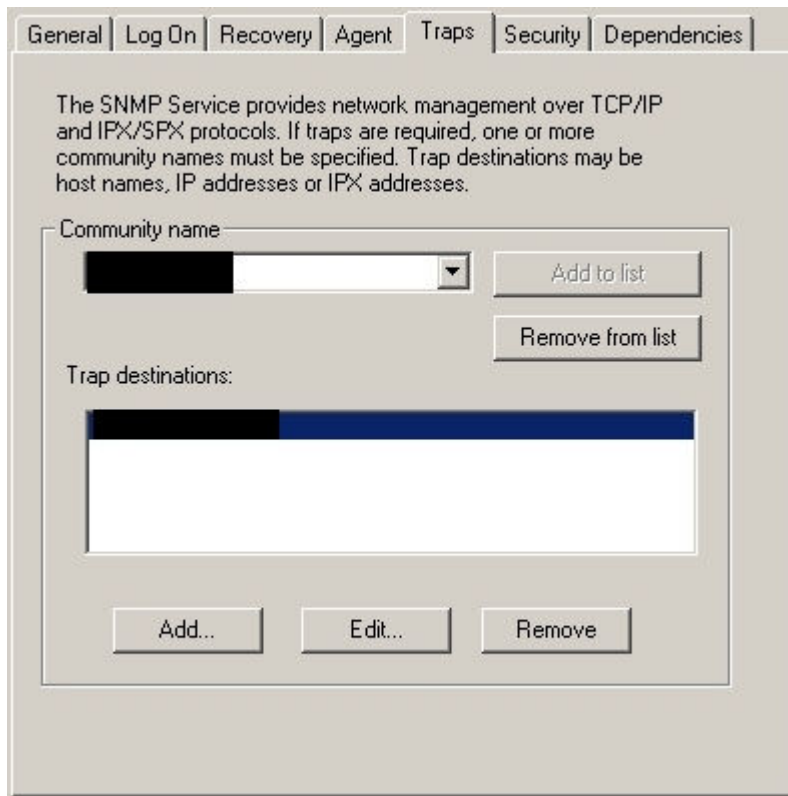
2. Asennetaan Net-SNMP:n SSL-tuen sisältävä versio. Ohjelman Trap-osan voi jättää asentamatta, sillä Trap-viestien lähetykseen käytetään suoraan Windowsin omaa Trap-palvelua.

3. Asennetaan Windowsin oma SNMP-palvelu jos sitä ei jo ole asennettu. Sekä SNMP-palvelu että SNMP-Trap-palvelu laitetaan päälle Windowsin palvelunhallinnassa. SNMP-palvelun asetuksia muokataan niin, että yhteydet palveluun ovat sallittuja vain paikalliselta koneelta. Lisäksi kohdassa "Accepted community names" on oltava vain luku -oikeuksilla varustettu yhteisönimi.



KUVIO 2. SNMP-asetukset Windowsissa.

Trap-asetuksiin lisätään kohteeksi Zenoss-palvelimen osoite. Yhteisönimen on täsmätävä Zenossin käyttämän nimen kanssa.



KUVIO 3. Trap-asetukset Windowsissa.

4. Luodaan tiedosto <Net-SNMP:n asennushakemisto>\usr\etc\snmp\snmpd.conf ja siihen seuraavat rivit:

```
agentaddress udp:<SNMPv3-portti>
rouser <SNMPv3-käyttäjänimi>priv
proxy -v 1 -c <paikallinen SNMP-yhteisönimi> localhost:161
.1.3
createUser <SNMPv3-käyttäjänimi> MD5 "<SNMPv3:n MD5-
salasana>" DES "<SNMPv3:n DES-salasana>"
```

Missä

- **agentaddress** määrittää missä portissa Net-SNMP-palvelu kuuntelee SNMP-yhteyksiä
- **rouser <SNMPv3-käyttäjänimi>priv** määrittää että käyttäjällä <SNMPv3-käyttäjänimi> on vain luku -oikeudet sekä pääsy järjestelmään vain kun autentikointi ja viestien salaus on päällä
- **proxy** määrittää, että kaikki SNMP-liikenne ohjataan eteenpäin Windowsin omalle SNMP-palvelulle porttiin 161
- **createUser** luo SNMPv3-käyttäjän ja määrittää sille salasanat

5. Rekisteröidään Net-SNMP Windowsin palveluksi komennolla

```
"<Net-SNMP:n asennushakemisto>\usr\bin\snmpd.exe" -
register -Lf "<Net-SNMP:n asennushakemis-
to>\usr\log\snmpd.log" -
Ivacm_conf,proxy,pass,pass_persist,usmUser,usmConf,setSerialNo
```

Missä

- **-register** rekisteröi ohjelman Windowsin palveluksi
- **-Lf** määrittää mihin ohjelman lokitiedosto luodaan
- **-I** määrittää ladattavat Net-SNMP:n moduulit. Tässä ladataan kaikki sekä välityspalvelintoiminnon että SNMPv3:n vaatimat moduulit.

6. Käynnistetään Net-SNMP Windowsin palvelujenhallinnasta.

7. Ohjelma säilyttää salasanat salattuna tiedostossa <Net-SNMP:n asennushakemisto>\usr\snmp\persist\snmpd.conf. Tämän vuoksi <Net-SNMP:n asennushakemisto>\usr\etc\snmp\snmpd.conf-tiedostosta on poistettava selväkielinen rivi

```
createUser <SNMPv3-käyttäjänimi> MD5 "<SNMPv3:n MD5-
salasana>" DES "<SNMPv3:n DES-salasana>"
```

8. Testataan toimivuus Zenoss-palvelimelta komennolla

```
snmpwalk -v3 -u<SNMPv3-käyttäjänimi> -l authPriv -a MD5 -A
<SNMPv3:n MD5-salasana> -x DES -X <SNMPv3:n DES-salasana>
<Windows-palvelimen osoite>:<SNMPv3-portti> sysDescr.0
```

Jos kaikki on kunnossa, edellinen komento palauttaa vastaavan rivin kuin SNMPv2c-ohjeen kohdassa 4.

9. Zenossin web-käyttöliittymässä SNMPv3:a käyttävään laitteeseen tai laiteluokkaan määritetään seuraavat asetukset zProperties-sivulla:

- zSnmpAuthPassword: <SNMPv3:n MD5-salasana>
- zSnmpAuthType: MD5
- zSnmpPort: <SNMPv3-portti>
- zSnmpPrivPassword: <SNMPv3:n DES-salasana>
- zSnmpPrivType: DES
- zSnmpSecurityName: <SNMPv3-käyttäjänimi>
- zSnmpVer: v3

Trap-viestien vastaanottoa varten määritetään vielä zSnmpCommunity. Se säädetään samaksi kuin kuvion 3 valikossa.

5.3 WMI

5.3.1 Asetukset palomuuria varten

Nelsonin (1998) ohjeen mukaan WMI:n DCOM-protokollan käyttämät portit voi määrittellä Windowsin rekisteriin Regedt32.exe-ohjelmalla. Luodaan HKEY_LOCAL_MACHINES\Software\Microsoft\Rpc\Internet-rekisteriavain, johon luodaan uusi

- moniosainen arvo REG_MULTI_SZ nimeltään Ports, arvossa määritellään käytettävät portit erotettuna väliviivalla, esim. 5000-5100
- merkkijonoarvo REG_SZ nimeltään PortsInternetAvailable, arvoksi määritellään Y
- merkkijonoarvo REG_SZ nimeltään UseInternetPorts, arvoksi määritellään Y.

5.3.2 Käyttäjän luonti

Windows-palvelimelle luodaan järjestelmänvalvojan oikeuksilla varustettu WMI-käyttäjä. Zenoss-palvelimen web-käyttöliittymässä WMI:tä käyttävään laitteeseen tai laiteluokkaan määritetään seuraavat asetukset zProperties-sivulla:

- zWinEventlog: True
- zWinEventlogMinSeverity: *
- zWinPassword: <WMI-käyttäjän salasana>
- zWinUser: <WMI-käyttäjän nimi muodossa toimialue\käyttäjänimi> **
- zWmiMonitorIgnore: False

* zWinEventlogMinSeverity-kohdassa määritellään mitkä lokit kerätään. Tämän kohdan arvo voi olla numero yhdestä viiteen, missä

1. Virhe (Error)
2. Varoitus (Warning)
3. Tietoja (Information)
4. Suojaus, onnistuneiden valvonta (Security audit success)
5. Suojaus, epäonnistuneiden valvonta (Security audit failure).
(Win32_NTLogEvent class 2009.)

Esimerkiksi jos arvoksi määritellään 3, Zenoss kerää ja näyttää ainoastaan tasojen 3, 2 ja 1 lokit.

** Jos WMI-käyttäjä on paikallinen, käytetään toimialueen tilalla pistettä.

5.3.3 Toiminnan testaus

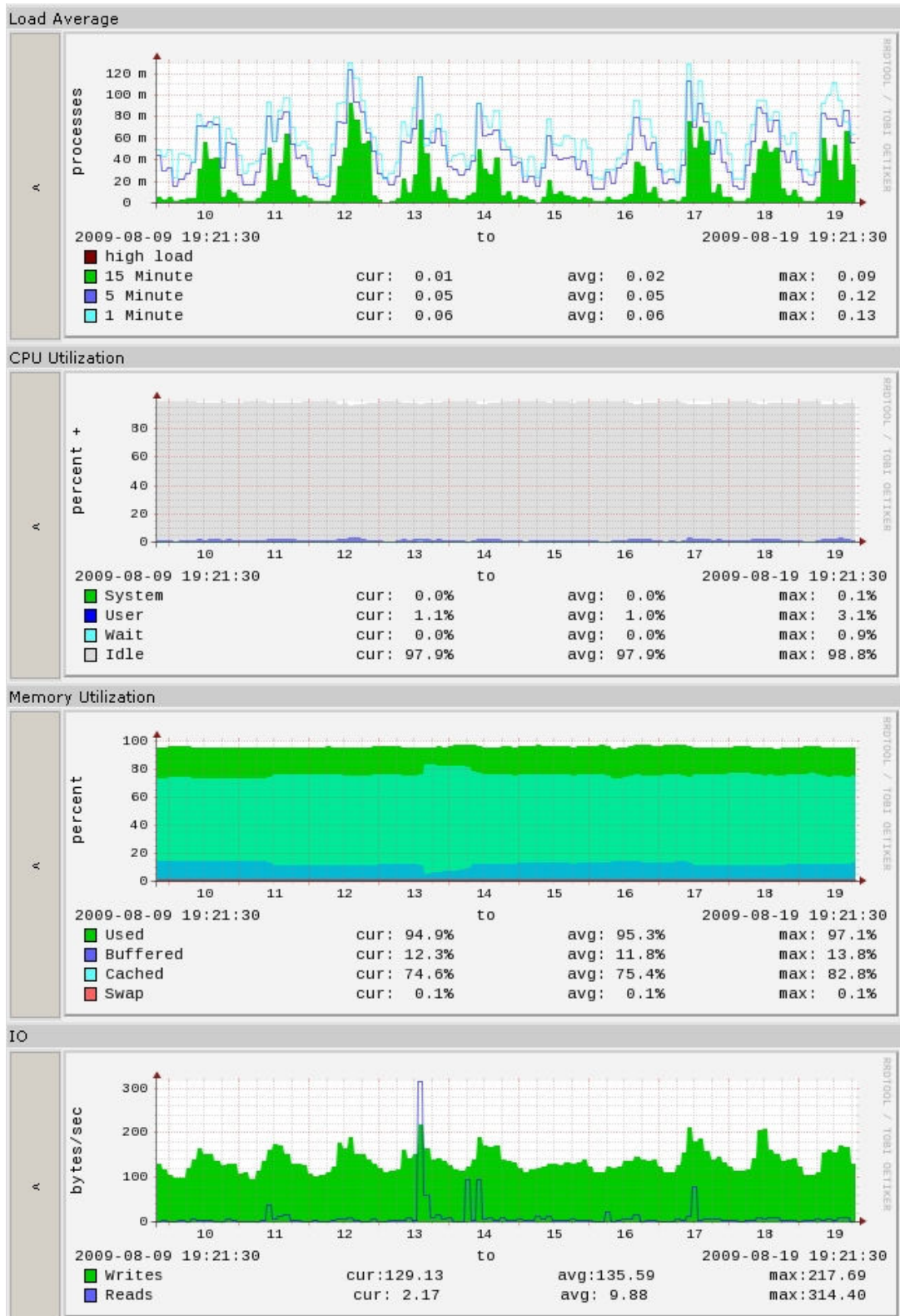
Zenoss-palvelimen komentoriviltä WMI-yhteyden toimivuutta voidaan testata Wmic-ohjelman avulla. Hakemistoon /bin on luotu symbolinen linkki viittamaan ohjelman alkuperäiseen sijaintiin /usr/local/zenoss/zenoss/bin/wmic, joten ohjelmaa voi käyttää pelkällä wmic-komennolla.

```
wmic -U '<toimialue>\<WMI-käyttäjän nimi>%<WMI-käyttäjän  
salasana>' //<Windows-palvelimen osoite> "select Name from  
Win32_ComputerSystem"
```

Jos yhteys toimii, tämä komento palauttaa palvelimen nimen. Muussa tapauksessa komento palauttaa yleensä virheen numeron tai sanallisen kuvauksen virheestä, joiden avulla voi etsiä vian syytä.

6 LINUX-SEURANTA

Zenossissa /Devices /Server /Linux -laiteluokkaan lisätyt laitteet käyttävät automaattisesti Device-nimistä asetuspohjaa, joka hakee kuvion 4 suorituskykykuvaajat Net-SNMP:tä käyttävältä Linux-palvelimelta. Seuraavissa ohjeissa kuvataan Net-SNMP:n käyttöönotto Linuxissa.



KUVIO 4. Linux-palvelimen suorituskykykuvaajat.

6.1 SNMPv2c

Tämä ohje kuvaa yksinkertaisen asennuksen, SNMP:n versiota 3 suositellaan käytettäväksi.

1. Asennetaan Snmpd.

2. Tiedostoon snmpd.conf lisätään seuraavat rivit:

```
rocommunity <SNMP-yhteisönimi>
trapcommunity <SNMP-yhteisönimi>
trap2sink <Zenoss-palvelimen osoite>
```

3. Käynnistetään snmpd-palvelu uudelleen komennolla

```
/etc/init.d/snmpd restart
```

4. Testataan kuten Windowsin SNMPv2c kappaleen 5.1 kohdassa 4. Zenossiin tehtävät muutokset ovat samat kuin Windowsissa, ks. kohta 5.

6.2 SNMPv3

1. Asennetaan Snmpd ja OpenSSL.

2. Luodaan vain luku -oikeuksilla varustettu SNMPv3-käyttäjä komennolla

```
net-snmp-config --create-snmpv3-user -ro -a MD5 -A "<MD5-
salasana>" -x DES -X "<DES-salasana>" <SNMPv3-
käyttäjänimi>
```

3. Komento loi rivin

```
rouser <SNMPv3-käyttäjänimi>
```

tiedostoon /usr/share/snmp/snmpd.conf. Lisätään tämän rivin perään vielä

```
priv
```

Nyt palvelu sallii yhteyden vain kun molemmat salasanat on määritetty, eli kun sekä autentikointi että yksityisyys ovat päällä.

Trap-viestejä varten tiedostoon lisätään vielä rivit

```
trapcommunity <SNMP-yhteisönimi>
trap2sink <Zenoss-palvelimen osoite>
```

4. Käynnistetään snmpd-palvelu komennolla

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

5. Testataan toimivuus Zenoss-palvelimelta komennolla

```
snmpwalk -v3 -u<SNMPv3-käyttäjänimi> -l authPriv -a MD5 -A
<SNMPv3:n MD5-salasana> -x DES -X <SNMPv3:n DES-salasana> <Win-
dows-palvelimen osoite>:<SNMPv3-portti> sysDescr.0
```

Jos komento palauttaa koneen nimen ja muuta tietoa, palvelu toimii ja voidaan siirtyä suoraan ohjeen kohtaan 8. Jos palvelu ei vastaa, on mahdollista että ulkoa tulevat yhteydet on estetty. Ks. kohdat 6 ja 7.

6. Joissakin Linux-jakeluissa, esimerkiksi Debianissa ja Ubuntussa, snmpd-palvelu ei oletuksena kuuntele ulkopuolelta tulevia paketteja. Tässä tapauksessa tiedoston /etc/default/snmpd rivistä

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p
/var/run/snmpd.pid 127.0.0.1'
```

täytyy vielä poistaa 127.0.0.1.

7. Käynnistetään snmpd-palvelu uudelleen komennolla

```
/etc/init.d/snmpd restart
```

8. Zenossin web-käyttöliittymässä tehtävät muutokset ovat samat kuin Windowsin SNMPv3:n asennuksessa. Ks. kappale 5.2, SNMPv3 ja Net-SNMP, kohta 9.

7 ASENNETUT LISÄOSAT (ZENPACKS)

7.1 Yleistä

Järjestelmään asennettuja lisäosia hallitaan web-käyttöliittymän sivulta Settings → ZenPacks. Sivulta lisäosia voidaan asentaa, poistaa tai luoda. Ladatut lisäosat ovat joko egg- tai zip-muodossa. Molemmat käyvät suoraan asennettaviksi tätä kautta, paketteja ei siis tarvitse purkaa ennen asennusta. Asennuksen voi suorittaa myös komentoriviltä komennolla `zenpack --install [paketin nimi]`. Komentoriviltä asennus kannattaa lähinnä silloin kun asennettava paketti on suuri, esim. HP:n MIB:t. Usein asennuksen jälkeen on Zope käynnistettävä uudelleen. Se tehdään sivulta Settings → Daemons, kohdasta restart zopectl.

Ennen lisäosan lopullista sitomista laitteeseen sen toimivuus kannattaa testata. Tämä tapahtuu Settings → ZenPacks -sivulla menemällä ensin testattavan lisäosan sivulle. Tältä sivulta näkyy lisäosan sisältämät tiedostot. Kohdasta "ZenPack provides" valitaan joku datasources-nimen sisältävä kohta (ks. kuvio 5).

Data Source

State at time: 2009/08/10 10:07:41

Name	ambientTemp
Source Type	SNMP
Enabled	True
OID	1.3.6.1.4.1.534.1.6.1
Type	GAUGE
RRD Min	
RRD Max	
Create Cmd	
Aliases	

Save

Test Against Device: [REDACTED] Test

KUVIO 5. Lämpötilan seurannan toimivuuden testaus.

Esimerkiksi kuviossa 5 esitetty paketin osa kysyy laitteen lämpötilaa. Test against device -kohtaan käy laitteen IP-osoite tai laitenimi. Tämän jälkeen lähetetään kysely painamalla Test-nappia.

Data Source

Command Output

```
Executing command
snmpwalk -c [REDACTED] -v1 [REDACTED] 1.3.6.1.4.1.534.1.6.1
against [REDACTED]
SNMPv2-SMI::enterprises.534.1.6.1.0 = INTEGER: 27
DONE in 0 seconds
```

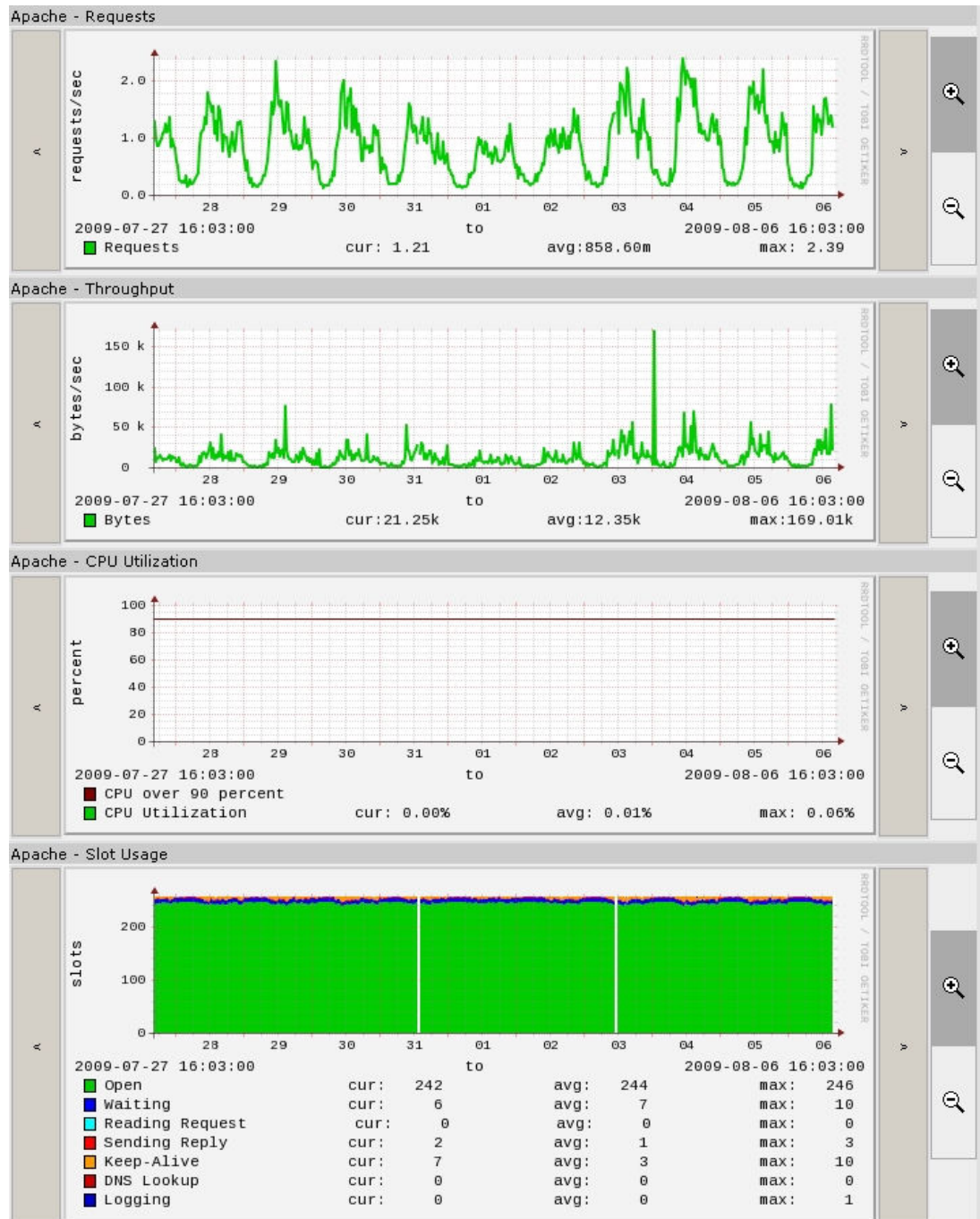
KUVIO 6. Snmpwalk-komennolla haettu lämpötilan arvo.

Jos kysely toimii, se palauttaa arvon. Esimerkiksi kuviossa 6 kysely palautti kokonaisluvun (integer) 27. Virhetapauksissa komento antaa ilmoituksen, josta voi yleensä päätellä onko vika seurattavan laitteen päässä vai Zenossin sisällä.

Yleisin tapa ottaa lisäosa käyttöön on valita laiteluokan tai yksittäisen laitteen Templates-sivulta Bind templates. Avautuvasta ikkunasta valitaan lisäosan/asetuspohjan nimi. CTRL-nappia pohjassa pitäen valitaan laitteeseen sidottavat asetuspohjat. Mikäli lisäosan käyttöönotto poikkeaa tästä, on siitä mainittu erikseen lisäosan kohdalla.

7.2 Apache monitor

Lisäosa kuuluu Zenossin toimittamiin Core-ZenPackeihin. Sen tarkoituksena on seurata Apache-web-palvelimen kuormitusta. Seuranta tapahtuu suoraan HTTP-protokollalla. Palvelin luo web-sivun, jossa se ylläpitää tietoa palvelimen käytöstä. Zenoss hakee tiedot suoraan tältä sivulta.



KUVIO 7. Apache monitor -lisäosan tuottamat kuvaajat.

Apache-palvelimen httpd.conf-asetustiedostoa on muokattava. Siinä otetaan käyttöön seuraavat rivit:

```
ExtendedStatus on
<Location /server-status>
SetHandler server-status
Order deny,allow
Deny from all
Allow from <Zenoss-palvelimen osoite>
</Location>
```

Tämän jälkeen Apache käynnistetään uudelleen. Seurannan toiminnan voi tarkistaa Zenoss-palvelimelta menemällä esim. Links-selaimella osoitteeseen <http://<Apache-palvelimen osoite>/server-status?auto>. Sivulla pitäisi näkyä tilastotietoa Apachen käytöstä. Tämän jälkeen Apache-asetuspohjan voi normaalisti liittää seurattavaan palvelimeen Zenossin web-käyttöliittymässä.

7.3 Dell monitor

Lisäosa antaa lisätietoja Dellin palvelimista SNMP:n kautta. Se sisältää myös Dellin MIB:t trap-viestien tulkintaa varten ja toimii kunnolla vain jos Advanced device details -lisäosa on asennettu Zenossiin.

▼ Status OS **Hardware** Software Events Perf Edit

Memory

Memory	4.0GB	Swap	unknown
--------	-------	------	---------

CPUs

Socket	Manufacturer	Model	Cores	Speed	Ext Speed	L1	L2	Volts	
1	Intel	Intel Xeon CPU E5410	2.33GHz Stepping 6	4	2333 MHz	1333 MHz	128 KB	12288 KB	1400 mV

Hard Disks

Name	Bay	Model	Type	Speed	Size	Status
Backplane Physical Disk 0 0 0	0	DELL MAX3073RC	SAS	0	72.7GB	●
Backplane Physical Disk 0 0 1	1	DELL MAX3073RC	SAS	0	72.7GB	●
Backplane Physical Disk 0 0 2	2	DELL MAX3073RC	SAS	0	72.7GB	●
Backplane Physical Disk 0 0 3	3	DELL MAX3073RC	SAS	0	72.7GB	●

Fans

Name	Type	Speed	Status
System Board FAN 1 RPM	Fan	5254Lpm	●
System Board FAN 2 RPM	Fan	5245Lpm	●
System Board FAN 3 RPM	Fan	5287Lpm	●
System Board FAN 4 RPM	Fan	5325Lpm	●

Power Supplies

Name	Type	Watts	Voltage	Status
PS 1 Status	AC	750	226V	●
PS 2 Status	AC	750	228V	●

Temperature Sensors

Name	Temperature	Status
System Board Ambient Temp	22C / 71F	●

Memory Modules

Board.Slot	Type	Frequency	Speed	Size	Status
1.1	DDR3	0MHz	1.50 ns	1.0GB	●
1.2	DDR3	0MHz	1.50 ns	1.0GB	●
1.3	DDR3	0MHz	1.50 ns	1.0GB	●
1.4	DDR3	0MHz	1.50 ns	1.0GB	●

Logical Disks

Name	OS Name	Type	Stripe Size	Size	Status
Virtual Disk 0	Windows Disk 0	RAID1	64.0KB	72.7GB	●
Virtual Disk 1	Windows Disk 1	RAID1	64.0KB	72.7GB	●

Expansion Cards

Slot	Manufacturer	Model	Status
4	Intel	Intel Corporation 5000X Chipset Memory Controller Hub	●
5	Broadcom	Broadcom BCM5708C NetXtreme II GigE (LOM)	●
6	Dell	DELL PERC 6 i Integrated	●
7	Intel	Intel Corporation 5000 Series Chipset PCI Express x8 Port 4-5	●
8	Intel	Intel Corporation 5000 Series Chipset PCI Express x4 Port 5	●
9	Intel	Intel Corporation 5000 Series Chipset PCI Express x8 Port 6-7	●
10	Intel	Intel Corporation 5000 Series Chipset PCI Express x4 Port 7	●
11	Broadcom	Broadcom BCM5708C NetXtreme II GigE (LOM)	●
12	Intel	Intel Corporation 631xESB 632xESB 3100 Chipset UHCI USB Controller 1	●
13	Intel	Intel Corporation 631xESB 632xESB IDE Controller	●
14	Intel	Intel Corporation 6311ESB 6321ESB PCI Express Downstream Port E2	●
15	ATI	ATI Technologies Inc Radeon Graphics Adapter	●

1 of 12 < > 4 show all Page Size 40 ok

KUVIO 8. Dell Monitor -lisäosan antamat lisätiedot.

Palvelimessa on oltava asennettuna Dell OpenManage -ohjelma.

Lisäosa otetaan käyttöön menemällä laiteluokan tai yksittäisen laitteen kohtaan More → Collector plugins. Alemmasta Plugins-kohdasta valitaan Add fields ja siirretään kaikki community.snmp.Dell-alkuiset pluginit ylempään ikkunaan. Tämän jälkeen tallennetaan siirto painamalla Save.

Käytössä olevista plugineista on poistettava zenoss.snmp.CpuMap.

7.4 HP ProLiant ZenPack

Tämä lisäosa antaa lisätietoa HP:n ProLiant-palvelimista SNMP:n kautta. Se toimii kunnolla vain jos Advanced device details -lisäosa on asennettu Zenossiin.

Status	OS	Hardware	Software	Events	Perf	Edit		
Memory								
Memory	3.5GB	Swap	unknown					
CPUS								
Socket	Manufacturer	Model	Cores	Speed	Ext Speed	L1	L2	Volts
1	Intel	Intel Xeon	1	3400 MHz	800 MHz	0 KB	1024 KB	0 mV
2	Intel	Intel Xeon	1	3400 MHz	800 MHz	0 KB	1024 KB	0 mV
Hard Disks								
Name	Bay	Model	Type	Speed	Size	Status		
HardDisk2_128	0	COMPAQ BF03688284	SCSI	15K	36.4GB			
HardDisk2_129	1	COMPAQ BF03688284	SCSI	15K	36.4GB			
Fans								
Name	Type	Speed	Status					
cpu1	Spin Detect	Normal						
cpu2	Spin Detect	Normal						
system1	Spin Detect	Normal						
system2	Spin Detect	Normal						
Power Supplies								
Name	Type	Watts	Voltage	Status				
PSU0_1	Hot-pluggable Power Supply	0	unknown					
PSU0_2	Hot-pluggable Power Supply	0	unknown					
Temperature Sensors								
Name	Temperature	Status						
cpu1	43C / 109F							
cpu2	43C / 109F							
system1	44C / 111F							
Memory Modules								
Board.Slot	Type	Frequency	Speed	Size	Status			
0.1	DIMM	333MHz	3ns	512.0MB				
0.2	DIMM	333MHz	3ns	512.0MB				
0.3	DIMM	333MHz	3ns	2.0GB				
0.4	DIMM	333MHz	3ns	2.0GB				

Logical Disks					
Name	OS Name	Type	Stripe Size	Size	Status
LogicalDisk2_1	Disk 0	RAID1	128.0KB	36.4GB	

Expansion Cards			
Slot	Manufacturer	Model	Status
0	Unknown	Standard IDE Controller	
0	HP	HP NC7761 Gigabit Server Adapter	
0	HP	HP 64-Bit 133MHz PCI-X 2CH Ultra320 HBA	
0	HP	HP 64-Bit 133MHz PCI-X 2CH Ultra320 HBA	
6	HP	HP Smart Array 641 Controller	

KUVIO 9. HP ProLiant ZenPack -lisäosan antamat lisätiedot.

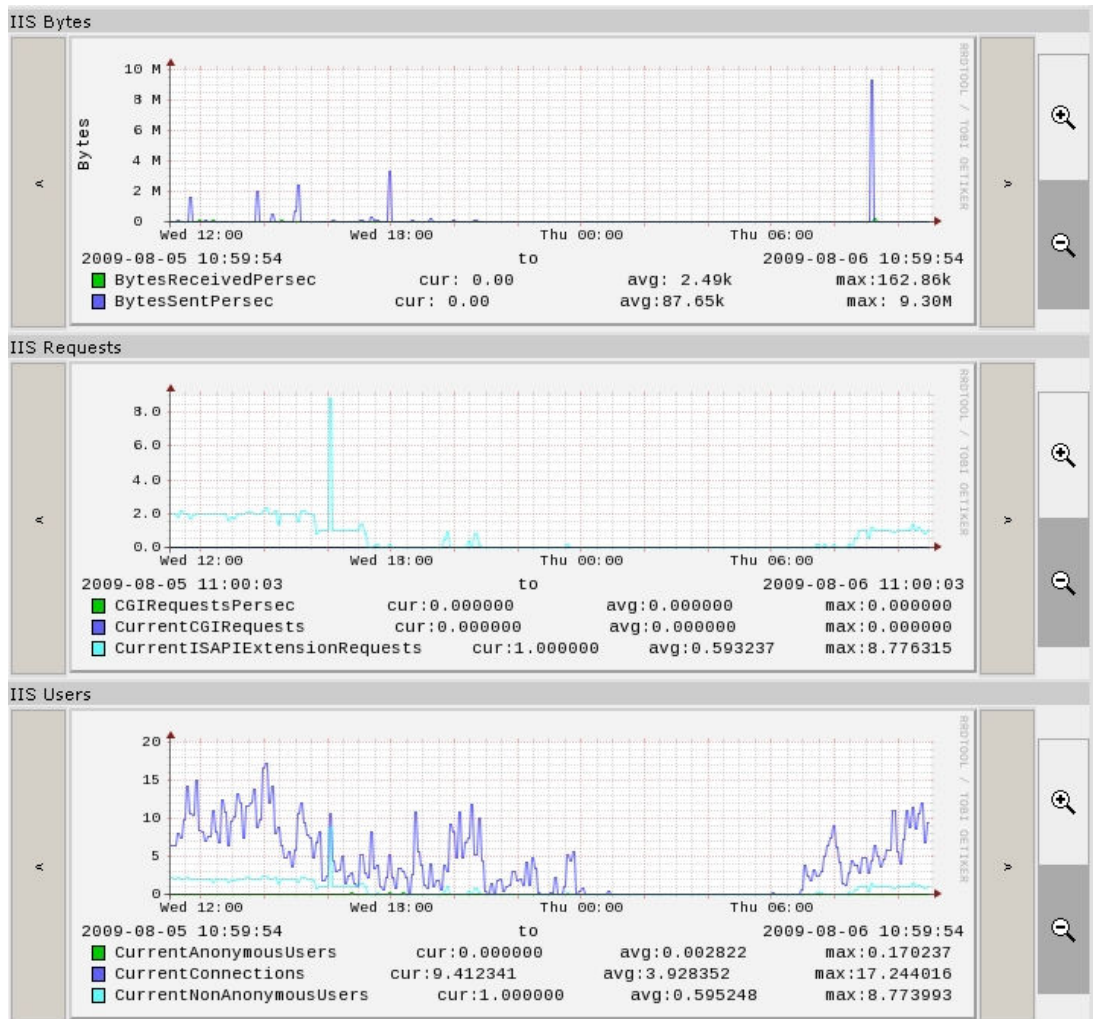
Palvelimessa on oltava asennettuna HP Insight Management Agents -ohjelma.

Lisäosa otetaan käyttöön menemällä laiteluokan tai yksittäisen laitteen kohtaan More → Collector plugins. Alemmasta Plugins-kohdasta valitaan Add fields ja siirretään kaikki community.snmp.HP-alkuiset pluginit ylempään ikkunaan. Tämän jälkeen tallennetaan siirto painamalla Save.

Käytössä olevista plugineista on poistettava zenoss.snmp.CpuMap. Tämän jälkeen on järjestystä vaihdettava niin, että community.snmp.HPHardDiskMap, community.snmp.HPLogicalDiskMap ja community.snmp.HPExpansionCardMap ovat viimeisinä.

7.5 Microsoft IIS

Lisäosan tarkoituksena on kerätä tietoa Microsoftin IIS-palvelimen käytöstä WMI:n kautta.



KUVIO 10. Microsoft IIS -lisäosan tuottamat kuvaajat.

7.6 Powerware UPS

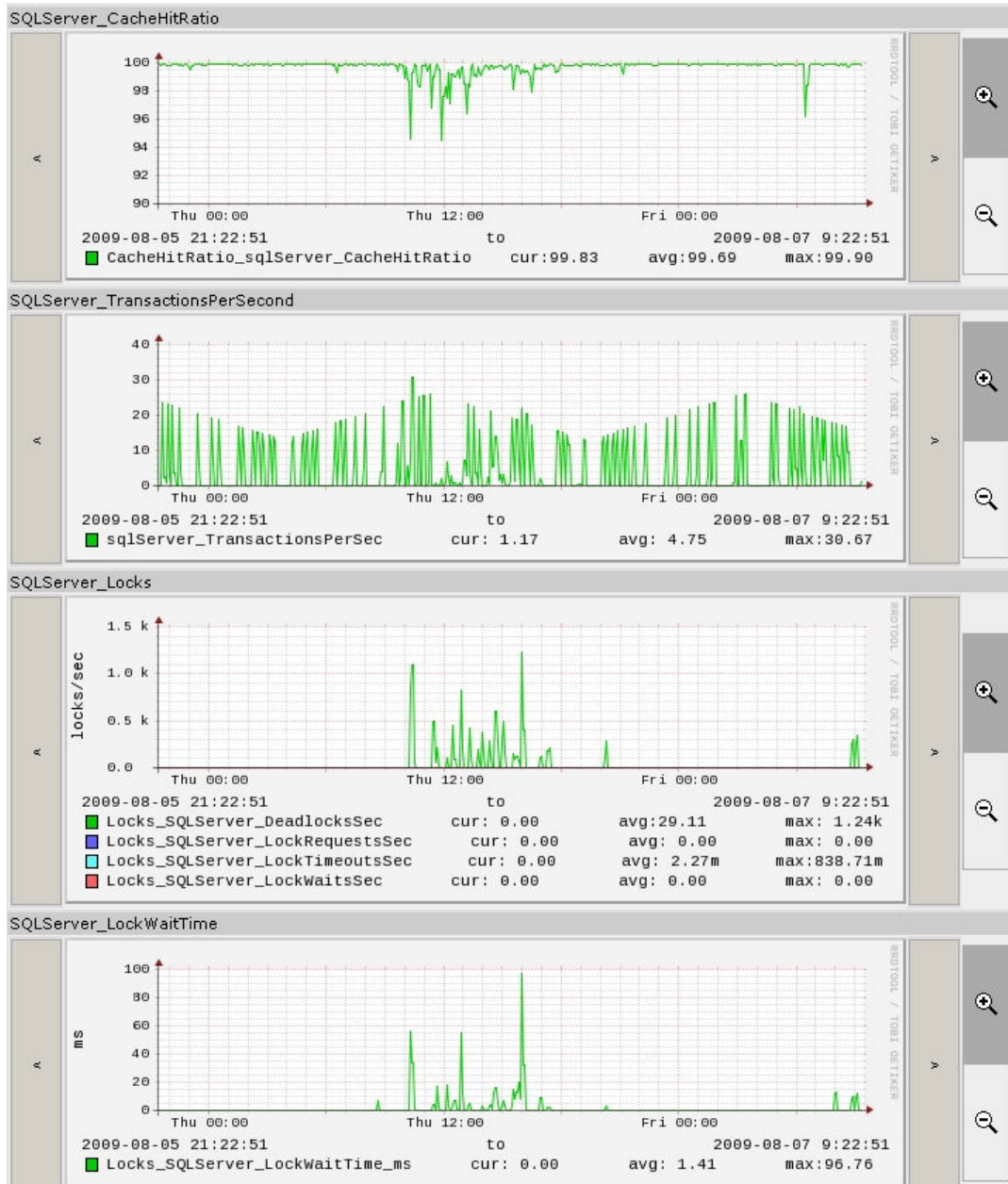
UPS-valmistaja Powerware käyttää laitteidensa SNMP-valvontaan omaa hallintatietokantaansa. Tämä lisäosa mahdollistaa Powerwaren UPS-laitteiden seurannan.

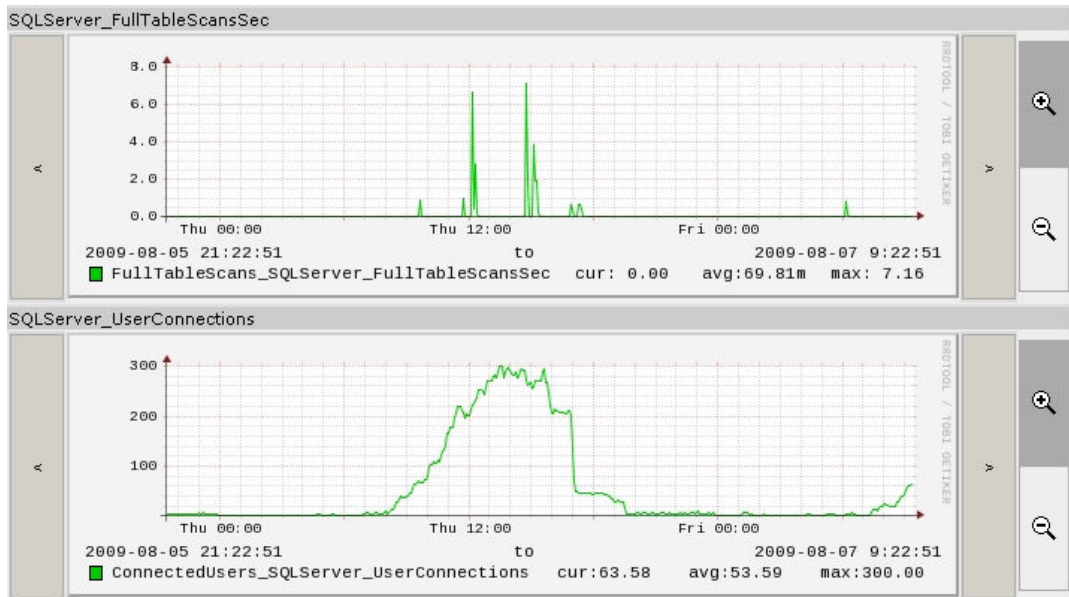


KUVIO 11. Powerware UPS -lisäosan tuottamat kuvaajat.

7.7 SQL 2000/2005 Server performance

Microsoftin SQL Serverin versioista 2000 ja 2005 tietoa WMI:n kautta keräävä lisäosa vaatii toimiakseen lisäosan nimeltä Perfmon.





KUVIO 12. SQL 2000/2005 Server Performance -lisäosan tuottamat kuvaajat.

7.7.1 Muokkaukset

SQL-lisäosa käyttää Perfmon-lisäosan perfmon.pl-skriptiä. Tämä skripti taas käyttää Zenossin mukana toimitettua Winexe-ohjelmaa. Mukana toimitettu vanhempi Wine-xen versio kuitenkin sisälsi ohjelmistovirheen, joka esti WMI-kyselyn toiminnan. Uudemmallalla 0.90-versiolla kyselyt toimivat.

Uusi Winexe-versio kopioitiin suoraan vanhemman rinnalle hakemistoon /usr/local/zenoss/common/bin nimellä winexe-static-081123. Alkuperäisen perfmon.pl-skriptin rivi

```
$output = ` \usr/local/zenoss/common/bin/winexe -U
'$username'%'$password' // $hostname 'typeperf -sc 1
"$counter" "`;
```

korvattiin seuraavasti:

```
$output = ` $ZENHOME/./common/bin/winexe-static-081123 -U
'$username'%'$password' // $hostname 'typeperf -sc 1
"$counter" "`;
```

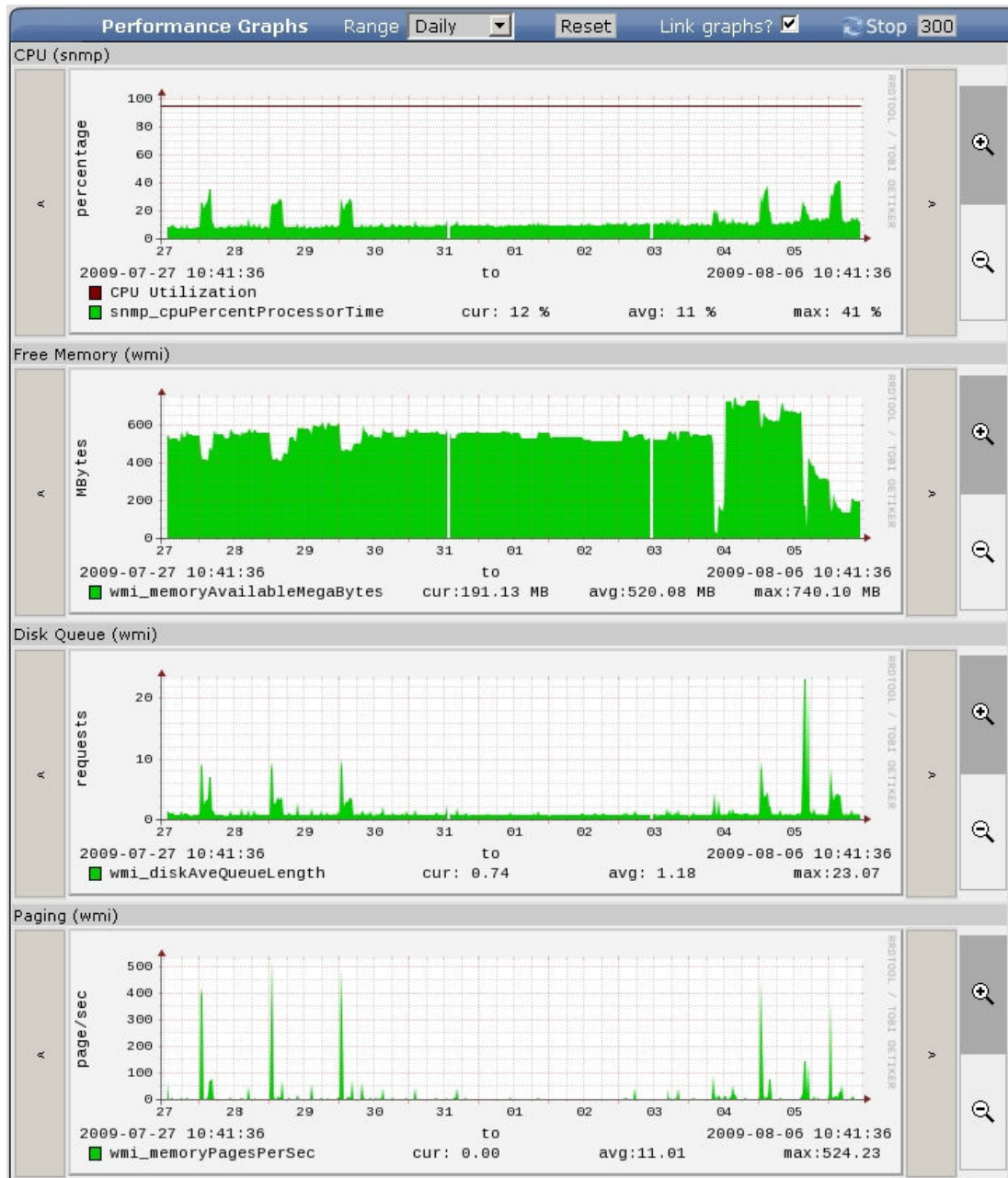
Tässä tapauksessa käytettiin \$ZENHOME-muuttujaa viittamaan oikeaan hakemistoon, mutta myös viittaus /usr/local/zenoss/common/bin/winexe-static-081123 olisi ajanut saman asian.

7.7.2 Käyttöönotto

Lisäosa otetaan käyttöön valitsemalla laiteluokan tai yksittäisen laitteen Templates-sivulta Bind templates → SQLServer sekä lisäämällä zProperties-sivulle kohtaan zSQLInstance arvo SQLSERVER.

7.8 Windows WMI device template

Tämä lisäosa kysyy suorittimen käyttöasteen SNMP:llä sekä vapaan keskusmuistin määrän, kiintolevyn jonon ja sivutuksen WMI:n kautta.



KUVIO 13. Windows WMI Device Template -lisäosan tuottamat kuvaajat.

Lisäosan käyttämä `check_snmp_cpu.pl`-skripti SNMP-kyselyyn ei tukenut SNMP:n versiota 3, joten sitä oli muokattava niin, että sama skripti toimisi kaikissa SNMP:n versioissa. Alkuperäisen skriptin rivit

```
# check_snmp_cpu.pl IP COMMUNITY
```

```

if ( @ARGV[0] eq "" || @ARGV[1] eq "" ) {
    print "check_snmp_cpu.pl IP COMMUNITY\n";
    exit 0;
}

$results = `snmpwalk -v 1 -c '@ARGV[1]' '@ARGV[0]'
1.3.6.1.2.1.25.3.3.1.2`;

```

korvattiin seuraavasti:

```

# check_snmp_cpu.pl IP COMMUNITY SECURITYNAME AUTHPASSWORD
PRIVPASSWORD PORT VERSION AUTHTYPE PRIVTYPE

if ( @ARGV[6] eq "v3" ) {
    $results = `snmpwalk - '@ARGV[6]' -u '@ARGV[2]' -l
authPriv -a '@ARGV[7]' -A '@ARGV[3]' -x '@ARGV[8]' -X
 '@ARGV[4]' '@ARGV[0]': '@ARGV[5]' 1.3.6.1.2.1.25.3.3.1.2`;
}

else {
    $results = `snmpwalk - '@ARGV[6]' -c '@ARGV[1]'
 '@ARGV[0]': '@ARGV[5]' 1.3.6.1.2.1.25.3.3.1.2`;
}

```

Uusi if-lauseke kysyy laitekohtaista SNMP-versiota, minkä perusteella se valitsee kummalla versiolla Snmpwalk-kysely tehdään. Skriptin alusta poistettiin SNMP:n versioille 1 ja 2 tarkoitettu tarkistus.

Lisäksi oli lisättävä Zenossin graafisen käyttöliittymän /Devices /Server /Windows /Templates /Device_WMI_SNMP_v2 /cpu_snmp -sivulla Command template -kohdan rivin

```

$$ZENHOME/Products/WindowsWMIDeviceTemplateV2/libexec/che
k_snmp_cpu.pl "${dev/manageIp}" "${dev/zSnmpCommunity}"

```

perään lisää tietoja hakevat argumentit

```

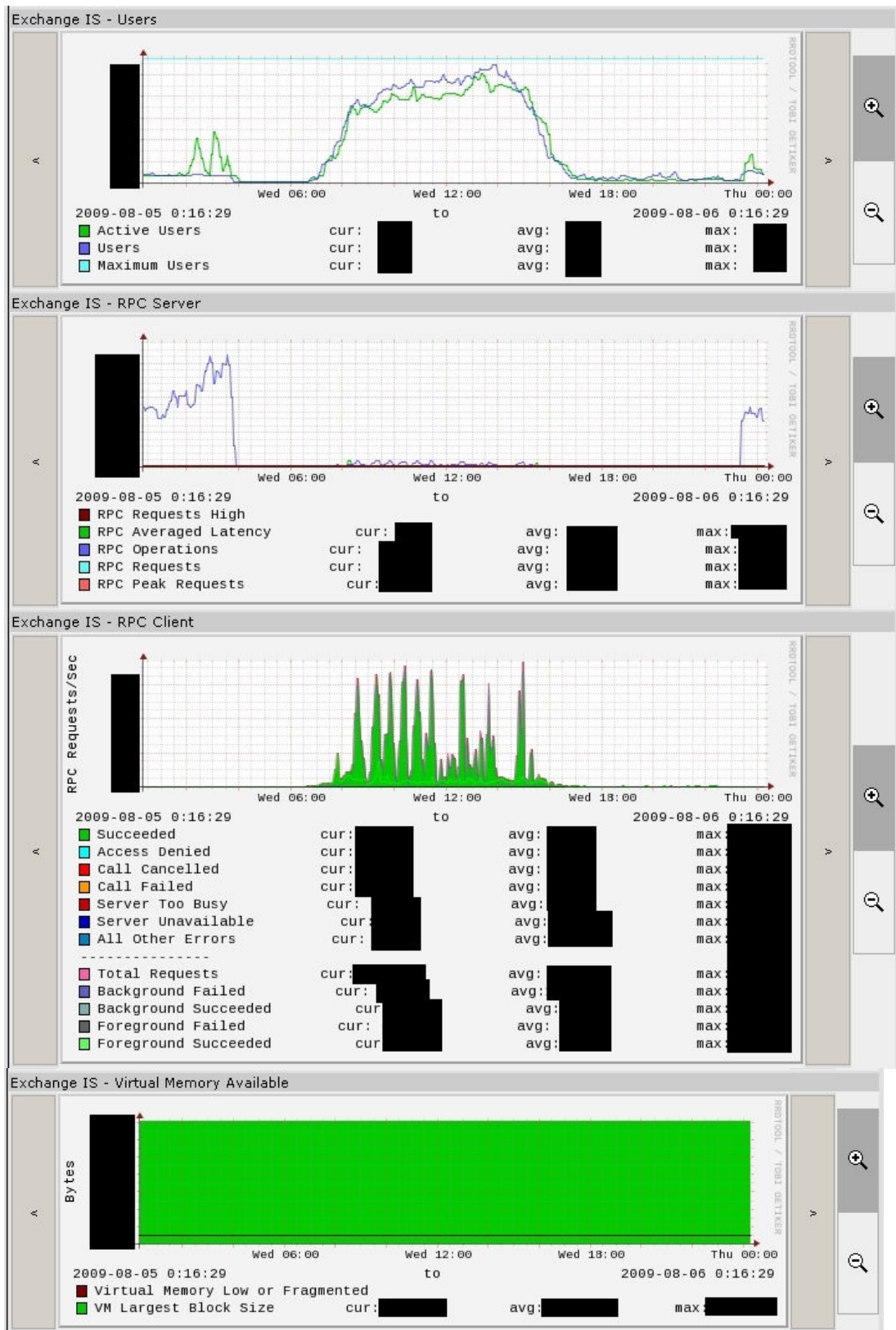
"${dev/zSnmpSecurityName}" "${dev/zSnmpAuthPassword}"
"${dev/zSnmpPrivPassword}" "${dev/zSnmpPort}"
"${dev/zSnmpVer}" "${dev/zSnmpAuthType}"
"${dev/zSnmpPrivType}"

```

Nämä arvot haetaan suoraan kunkin laitteen zProperties-asetussivulta. Skriptissä @ARGV[0] siis viittaa laitteen zProperties-sivun zSnmpSecurityName-kohtaan, @ARGV[1] zSnmpAuthPassword-kohtaan, @ARGV[2] zSnmpPrivPassword-kohtaan ja niin edelleen.

7.9 WMI Exchange monitor

Tämä lisäosa mahdollistaa Microsoft Exchange -sähköpostipalvelimen tarkan seurannan WMI:n kautta. Se haettiin erään Zenoss-käyttäjän (Dastrup 2008a) blogista.



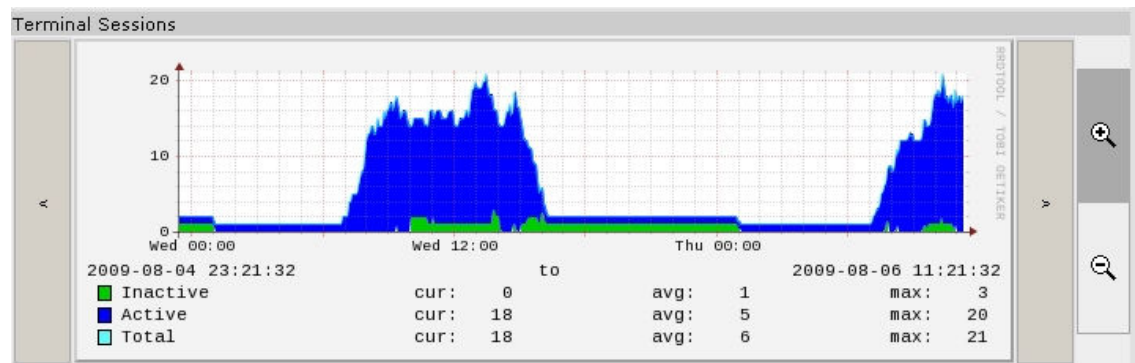
KUVIO 14. WMI Exchange Monitor -lisäosan tuottamat kuvaajat.

Kuten WMI Performance Monitor -lisäosassa, myös tässä lisäosan vastaavaa wmi_exch_stats.pl-nimistä skriptiä oli muokattava, sillä se haki Wmic-ohjelmaa vää-

rästä paikasta. Toimenpide oli sama kuin lisäosassa WMI Performance Monitor. Lisäosa sisälsi myös Intelligent Message Filtering (IMF) -suodatusseurannan, joka ei ole käytössä kuvion 12 palvelimella. Se poistettiin kokonaan käytöstä kopioimalla asetuspohja paikalliseksi postipalvelimelle, minkä jälkeen asetuspohjasta poistettiin IMF:n tilastojen piirtoon tarkoitetut kuvaajat sekä poistettiin käytöstä IMF-niminen tietolähde. IMF-seurannan saa tarvittaessa takaisin käyttöön poistamalla paikallisen asetuspohjan postipalvelimen asetuspohjasivulta kohdasta Remove local copy.

7.10 WMI performance monitor

Toimintaongelmien vuoksi lisäosasta käyttöön jätettiin ainoastaan osa, joka seuraa palvelimeen muodostettuja yhteyksiä. Lisäosa haettiin samasta blogista kuin WMI Exchange monitor (Dastrup 2008b).



KUVIO 15. WMI performance monitor -lisäosan tuottama kuvaaja palvelimeen muodostetuista yhteyksistä.

Lisäosan wmi_stats.pl-skriptiä oli muokattava, sillä se haki Wmic-ohjelmaa väärästä paikasta. Rivi

```
$cmd = $ENV{"ZENHOME"} . "/bin/wmic -U
'@ARGV[3]%'@ARGV[4]' //@ARGV[2] ";
```

Muutettiin muotoon

```
$cmd = "/usr/local/zenoss/common/bin/wmic -U
'@ARGV[3]%'@ARGV[4]' //@ARGV[2] ";
```

Lisäpaketin hallinnasta poistettiin kaikki osat lukuunottamatta Terminal Sessions -toimintoon liittyviä. Asetuspohjan nimeä muutettiin hieman, muotoon WMI Performance Monitors - Terminal Sessions.

7.11 Muut lisäosat

- **Advanced device details** -lisäosan vaativat asennetut HP ProLiant ZenPack- ja Dell monitor -lisäosat.
- **HP ProLiant MIBs** sisältää kaikki HP:n ProLiant-palvelimien käyttämät hallintatietokannat.
- **HPUX**-lisäosa hakee perustietoja HP-UX-käyttöjärjestelmää käyttävästä palvelimesta. Tärkeimpiä sen hakemia tietoja ovat levyosoiden käyttö sekä suorittimen ja muistin käyttöasteet.
- **MIB browser** -lisäosan asennuksen jälkeen sen tuomat lisäominaisuudet näkyvät päävalikon MIBs-sivulla. Jokaisen MIB:n vieressä sijaitseva suurennuslasi avaa MIB-selaimeen kyseisen hallintatietokannan.

8 ASETUSPOHJAT (TEMPLATES)

8.1 Asetuspohjan luonti

Asetuspohjan luonti aloitetaan ottamalla selvää seurattavan laitteen SNMP-ominaisuuksista. Tarvitaan tiedot laitteen käyttämästä hallintatietokannasta eli MIB:stä ja sen välittämistä tiedoista.

8.1.1 Laitteen MIB:tä ei tiedetä

Jos laitteesta ei löydy tietoa, hyvä tapa tarkistaa kaikki laitteen SNMP:n kautta antama tieto on ajaa Zenoss-palvelimen komentoriviltä Snmpwalk-ohjelma. Esimerkkinä käytetään UPS-laitetta, joka käyttää SNMP:n versiota 2c.

```
snmpwalk -v2c -c<SNMP-yhteisönimi> <laitteen IP-osoite>
1.3
```

SNMP:n versiota 3 käytävässä laitteessa käsky annettaisiin muodossa

```
snmpwalk -v3 -u<SNMPv3-käyttäjänimi> -l authPriv -x MD5 -X
<MD5-salasana> -a DES -A <DES-salasana> <laitteen IP-
osoite>:<SNMPv3-portti> 1.3
```

Edellinen käsky palauttaa monta riviä tietoa ja niitä tutkimalla voi yleensä päätellä mistä hyödyllinen tieto löytyy. Snmpwalk käy järjestyksessä läpi MIB-puuta. Tässä esimerkissä kiinnostavimpia ovat muodossa SNMPv2-SMI::mib-2 alkavat rivit. Käs-

kyn lopussa oleva 1.3 määrittää, että laite palauttaa koko MIB-puunsa, eli kaiken jakamansa tiedon. Tässä muutama käskyn palauttama rivi:

```
SNMPv2-SMI::mib-2.33.1.2.7.0 = INTEGER: 25
SNMPv2-SMI::mib-2.33.1.3.1.0 = Counter32: 0
SNMPv2-SMI::mib-2.33.1.3.2.0 = INTEGER: 3
```

Kuviossa 16 on esitetty Mib-2-olion paikka MIB-puussa.

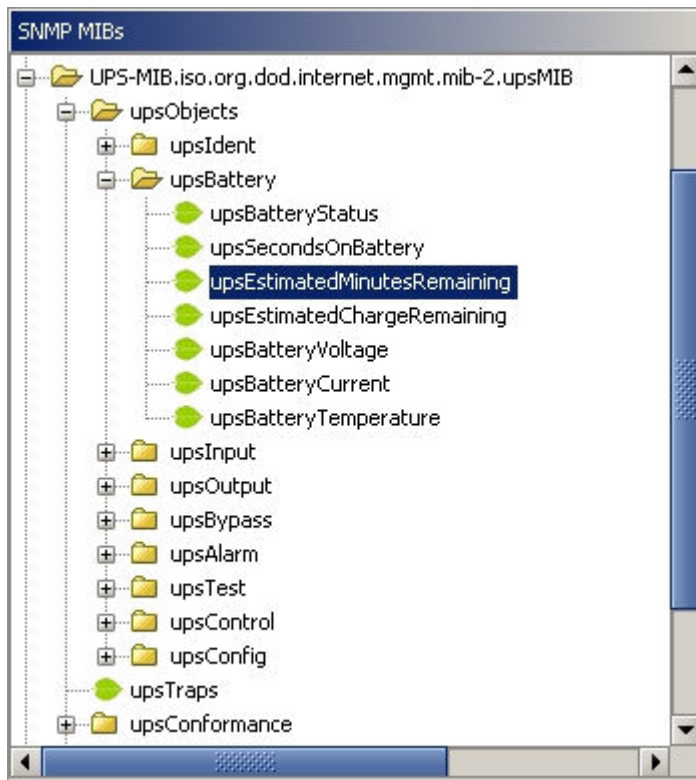
Object Name	Object Identifier
iso	1
iso	1
org	1.3
org	1.3
dod	1.3.6
dod	1.3.6
internet	1.3.6.1
internet	1.3.6.1
directory	1.3.6.1.1
directory	1.3.6.1.1
mgmt	1.3.6.1.2
mgmt	1.3.6.1.2
mib-2	1.3.6.1.2.1

KUVIO 16. Mib-2-olion sijainti MIB-puussa.

Olion sanallinen kuvaus iso.org.dod.internet.mgmt.mib-2 ja olion tunnus (OID) 1.3.6.1.2.1 viittaavat samaan paikkaan. Snmpwalk-ohjelmalla voi hakea tietoja myös olion sanallisella kuvauksella. SNMPv2-SMI::mib-2-alun jälkeen rivien seuraava numero on 33. Kun haetaan tietoja OID:sta 1.3.6.1.2.1.33, selviää, että kyseessä on RFC-dokumentissa 1628 määritelty UPS-MIB.

8.1.2 Laitteen MIB tiedetään

Jos laitteen käyttämä MIB on suoraan tiedossa, voi haluttuja tietoja kysyä laitteelta suoraan. Esimerkiksi kun tiedetään että UPS-laite käyttää RFC 1628:n mukaista UPS-MIB:tä, ei välivaiheita tarvitse käydä läpi. Tutkimalla UPS-MIB:tä erillisessä MIB-selaimessa voidaan sieltä löytyvien tietojen pohjalta tehdä asetus pohja suoraan. Hallintatietokantoja on ladattavissa MIB-tiedostoina useasta eri paikasta ilmaiseksi.



Name	upsEstimatedMinutesRemaining
OID	.1.3.6.1.2.1.33.1.2.3
MIB	UPS-MIB
Syntax	INTEGER (1..2147483647)
Access	read-only
Status	mandatory
DefVal	
Indexes	
Descr	An estimate of the time to battery charge depletion under the present load conditions if the utility power is off and remains off, or if it were to be lost and remain off.

KUVIO 17. iReasoningin MIB-selain.

MIB-selaimella voidaan katsoa MIB:n sisältöä. Kaikista olioista löytyy myös sanallinen selitys. Kuvion 17 olio 1.3.6.1.2.1.33.1.2.3 ilmoittaa UPS:n arvioidun jäljellä olevan kestoajan minuuteissa. Käsky

```
snmpwalk -v2c -c<SNMP-yhteisönimi> <laitteen IP-osoite>
1.3.6.1.2.1.33.1.2.3
```

palauttaa ainoastaan yhden rivin:

```
SNMPv2-SMI::mib-2.33.1.2.3.0 = INTEGER: 117
```

Tässä on huomattava, että OID:n viimeinen numero on 0. OID, jota on käytettävä Zennossin asetuspohjassa on siis kokonaisuudessaan 1.3.6.1.2.1.33.1.2.3.0. **Ilman viimeistä numeroa, tässä tapauksessa nolaa, kuvaajien piirto ei toimi.**

8.1.3 Uusi asetuspohja

Tässä esimerkissä lisätään asetuspohjaan yksi tietolähde ja määritellään sille kynnyksisarvo. Tietolähde ja kynnyksisarvo lisätään tämän jälkeen kuvaajaan. Uusi asetuspohja luodaan Zenossin web-käyttöliittymässä seuraavasti:

1. Mennään halutun laiteluokan tai yksittäisen laitteen sivulle. Esimerkissä käytetään luokkaa /Devices /Power /UPS.
2. Valitaan Templates-sivulta ▾ → Add template ja nimetään se asetuspohjaa kuvaavalla tavalla.

The screenshot shows the 'Performance Template' configuration page in Zenoss. The form contains the following fields:

- Name:** RFC 1628 -UPS
- Target Class:** Products.ZenModel.Device
- Description:** (empty)

Below the form is a 'Save' button. The page also features three expandable sections:

- Data Sources:** A table with columns: Name, Source, Source Type, Enabled.
- Thresholds:** A table with columns: Name, Type, Data Points, Severity, Enabled.
- Graph Definitions:** A table with columns: Seq, Name, Graph Points, Units, Height, Width.

KUVIO 18. Uusi tyhjä asetuspohja.

Kuvion 18 Data sources -kohdassa määritellään laitteesta haettavat tiedot, Thresholds-kohdassa määritellään kynnyksisarvot haetuille tiedoille ja Graph definitions -kohdassa määritellään mitä kuvaajia piirretään haettujen tietojen pohjalta.

3. Määritellään ensimmäinen haettava tieto valitsemalla Data sources -kohdassa ▾ → Add data sources. Tietolähde voidaan nimetä esimerkiksi suoraan MIB:stä löytyvällä nimellä, upsEstimatedMinutesRemaining. Tietolähteen tyyppiä jätetään oletuksena oleva SNMP.

Data Source

State at time: 2009/08/12 14:48:24

Name: upsEstimatedMinutesRemaining

Source Type: SNMP

Enabled: True

OID: 1.3.6.1.2.1.33.1.2.3.0

Type: GAUGE

RRD Min:

RRD Max:

Create Cmd:

Aliases:

Save

Test Against Device: Test

KUVIO 19. SNMP-tietolähde.

4. Ks. kuvio 19. OID-kohtaan syötetään kysyttävän tiedon täydellinen tunnus ja tallennetaan muutos painamalla Save. Tietolähteen toiminnan voi vielä tarkistaa kohdassa Test against device.

5. Kynnysarvo määritellään valitsemalla Thresholds-kohdassa ▾ → Add threshold. Kynnysarvo voidaan nimetä samoin kuin tietolähde tai muuten järkevällä tavalla.

Min/Max Threshold

State at time: 2009/08/12 15:20:30

Name: Estimated Minutes Remaining

Data Points: upsEstimatedMinutesRemaining_upsEstimatedMinutesRemaining

Min Value: 10

Max Value:

Event Class: /Perf/Snmp

Severity: Critical

Escalate Count: 0

Enabled: True

Save

KUVIO 20. Kynnysarvon asetus.

6. Ks. kuvio 20. Data points -kohdassa valitaan mitä tietolähdettä kynnsarvo koskee. Min value -kohta määrittää hyväksyttävän minimiarvon, jonka alittuessa tapahtuma syntyy, ts. hälytys laukeaa. Max value taas määrittää hyväksyttävän maksimiarvon. Jos arvon on pysyttävä tiettyjen rajojen sisällä, voidaan määrittää sekä minimiarvo että maksimiarvo. Tässä tapauksessa kynns alittuisi arvon alittaessa 10 minuuttia. Event class määrittää mihin luokkaan kyseinen tapahtuma sijoittuu ja Severity-kohdassa määritellään tapahtuman vakavuusaste. Escalate count voidaan määrittää mikäli halutaan nostaa tapahtuman vakavuusastetta pykälällä sen toistuessa useamman kerran.

7. Kuvaaja luodaan valitsemalla Graph definitions -kohdassa $\nabla \rightarrow$ Add graph. Kuvaajalle annetaan kuvaava nimi.

8. Tietolähde lisätään juuri luotuun kuvaajaan ruksaamalla haluttu tietolähde ja valitsemalla $\nabla \rightarrow$ Add to graphs. Avautuvasta valikosta valitaan juuri luotu kuvaaja. Nyt tietolähde on liitetty kuvaajaan.

9. Myös kynnsarvon voi liittää kuvaajaan. Se tapahtuu samalla tavalla kuin tietolähteen lisääminen kuvaajaan. Kynnsarvo näkyy kuvaajassa oletuksena punaisena viivana.

Seq	Name	Type	Description
0	<input type="checkbox"/> Estimated Minutes Remaining	Threshold	Estimated Minutes Remaining
1	<input type="checkbox"/> upsEstimatedMinutesRemaining	DataPoint	upsEstimatedMinutesRemaining_upsEstimatedMinutesRemaining

State at time: 2009/08/12 15:44:00

Name	UPS Time Remaining
Height	100
Width	500
Units	
Logarithmic Scale	False
Base 1024	False
Min Y	-1
Max Y	-1
Has Summary	True

Save

KUVIO 21. Kuvaajan sivu.

Kuvion 21 kuvaajan sivulta näkyy siihen liitetyt tietolähteet ja kynnsarvot. Kuvaajan kokoa voi muokata kohdista Height ja Width. Units-kohtaan voi määrittää mittauksessa käytetyn yksikön, esim. minuutit. Oletuksena Min Y- ja Max Y -kohdissa olevat arvot -1 tarkoittavat, että kuvaaja yrittää sovittaa y-akselin itse sopivaksi. Esimerkiksi prosentteja ilmaisevissa kuvaajissa Min Y:n arvoksi kannattaa laittaa 0 ja Max Y:n arvoksi 100.

10. Valitsemalla kuvaajan valikossa tietolähde, esimerkissä upsEstimatedMinutesRemaining, päästään säätämään tarkemmin kuvaajan asetuksia.

State at time: 2009/08/12 15:57:06	
Name	upsEstimatedMinutesRemaining
Type	DataPoint
DataPoint	upsEstimatedMinutesRemaining upsEstimatedMinutesRemaining
Consolidation	AVERAGE
RPN	
Limit	-1
Line Type	Line
Line Width	1
Stacked	False
Color (Hex value RRGGBB)	
Format	%5.2lf%s
Legend	\${graphPoint/id}
Available RRD Variables	None

KUVIO 22. Kuvaajan tarkemmat asetukset.

Kuvion 22 sivulta voidaan säätää tarkemmin kuvaajan piirtoasetuksia, kuten käyrän paksuutta, väriä ja tyyliä. RPN-kohta on tärkeä, sillä siinä voidaan määrittää tiedon muokkaukseen liittyvät parametrit. Yleensä laite ilmoittaa arvot kokonaislukuina. Jos laite mittaa arvoa yhden desimaalin tarkkuudella, kokonaislukuun tähän tarkkuuteen päästäkseen sen on ilmoitettava arvo kertomalla kymmenellä. Luku voidaan ennen kuvaajaan piirtoa jakaa kymmenellä komennolla 10,/.

8.1.4 Valmis asetuspohja

Data Sources

Select: [All](#) [None](#)

Name	Source	Source Type	Enabled
<input type="checkbox"/> upsBatteryStatus	1.3.6.1.2.1.33.1.2.1.0	SNMP	True
<input type="checkbox"/> upsBatteryTemperature	1.3.6.1.2.1.33.1.2.7.0	SNMP	True
<input type="checkbox"/> upsBatteryVoltage	1.3.6.1.2.1.33.1.2.5.0	SNMP	True
<input type="checkbox"/> upsEstimatedChargeRemaining	1.3.6.1.2.1.33.1.2.4.0	SNMP	True
<input type="checkbox"/> upsEstimatedMinutesRemaining	1.3.6.1.2.1.33.1.2.3.0	SNMP	True
<input type="checkbox"/> upsInputVoltage	1.3.6.1.2.1.33.1.3.3.1.3.1	SNMP	True
<input type="checkbox"/> upsOutputPercentLoad	1.3.6.1.2.1.33.1.4.4.1.5.1	SNMP	True
<input type="checkbox"/> upsOutputVoltage	1.3.6.1.2.1.33.1.4.4.1.2.1	SNMP	True
<input type="checkbox"/> upsSecondsOnBattery	1.3.6.1.2.1.33.1.2.2.0	SNMP	True
<input type="checkbox"/> upsStatus	/usr/local/zenoss/common/libexec/check_snmp -H \${here/manageIp} -C \${here/zSnmpCommunity} -r 2 -w 2 -c 3 -o 1.3.6.1.2.1.33.1.2.1.0	COMMAND	True

1 of 10 < < upsBatteryStatus > > show all Page Size 40 ok

Thresholds

Select: [All](#) [None](#)

Name	Type	Data Points	Severity	Enabled
<input type="checkbox"/> UPS Load	MinMaxThreshold	upsOutputPercentLoad_loadPercentage	Warning	True
<input type="checkbox"/> UPS Temperature	MinMaxThreshold	upsBatteryTemperature_upsBatteryTemperature	Warning	True

Graph Definitions

Select: [All](#) [None](#)

Seq	Name	Graph Points	Units	Height	Width
0	<input type="checkbox"/> UPS Charge Remaining	UPS Charge Remaining, Estimated Percent Remaining, Estimated Minutes Remaining	percent / minutes	100	500
1	<input type="checkbox"/> UPS Voltages	Input Voltage, Output Voltage, Battery Voltage	voltes	100	500
2	<input type="checkbox"/> UPS Temperature	UPS Temperature, Battery Temperature	celsius	100	500
3	<input type="checkbox"/> UPS Status	Battery (1_Unknown 2_Normal 3_Low 4_Depleted)		100	500
4	<input type="checkbox"/> UPS Load	UPS Load, Load Percentage	percent	100	500
5	<input type="checkbox"/> UPS Seconds Running on Battery	Seconds on Battery	seconds	100	500

KUVIO 23. RFC 1628:ssa määriteltyä UPS-MIB:tä käyttävän UPS-laitteen valmis asetuspohja.

Kuviossa 23 normaalien SNMP-tietolähteiden lisäksi tietolähteeksi on lisätty myös COMMAND-muotoinen check_snmp-lisäohjelmaa käyttävä lähde. Check_snmp on alunperin tehty Nagios-ohjelmalle, mutta se tulee myös Zenossin mukana.

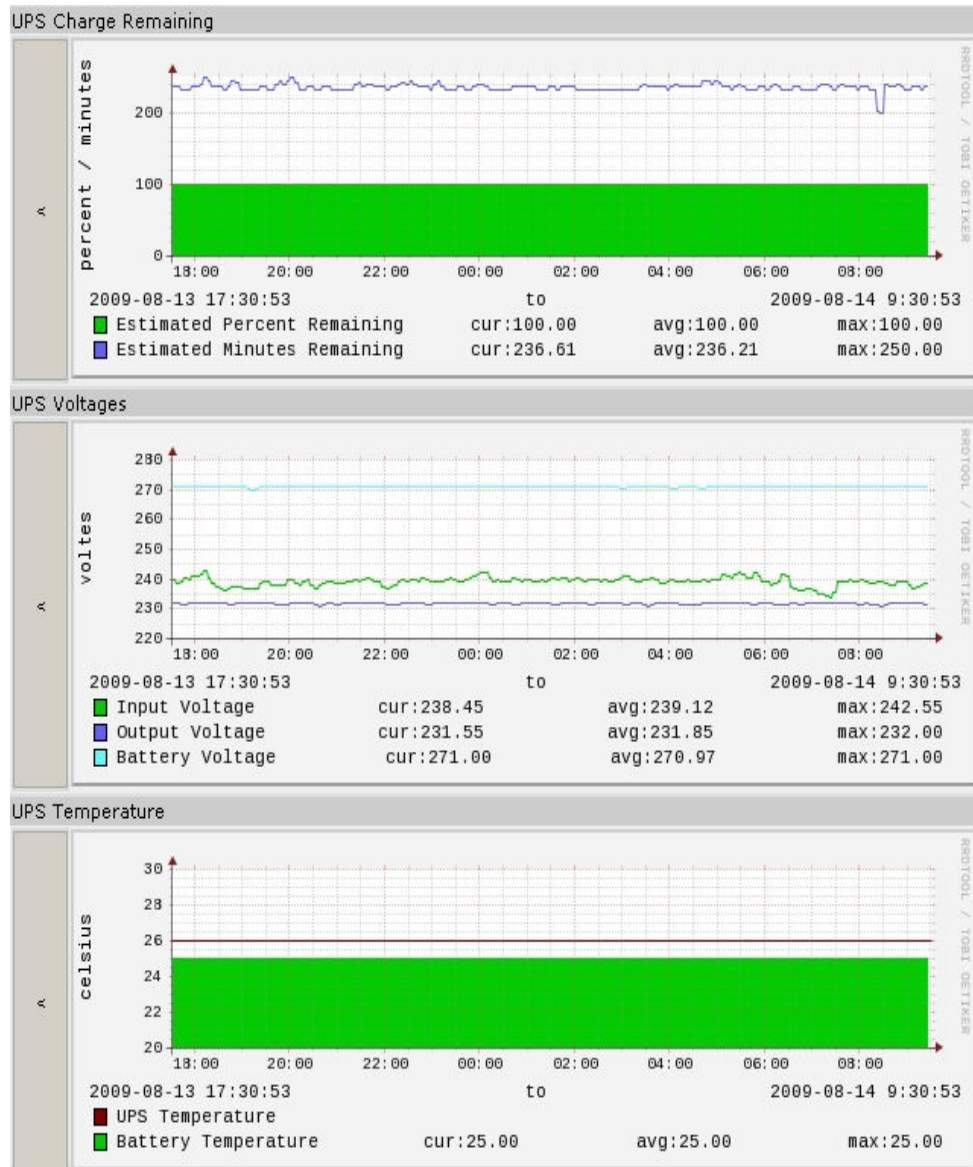
```
/usr/local/zenoss/common/libexec/check_snmp -H ${here/manageIp} -C ${here/zSnmpCommunity} -r 2 -w 2 -c 3 -o 1.3.6.1.2.1.33.1.2.1.0
```

Tässä on käytetty seuraavia asetuksia, joista

- -H määrittelee mihin laitteeseen otetaan yhteyttä (IP-osoite)
- -C määrittelee laitteen SNMP-yhteisönimen
- -r määrittelee arvon jonka laitteen odotetaan palauttavan (normaali toiminta)
- -w määrittelee arvon, jonka ylityttyä luodaan varoitusasteinen tapahtuma

- -c määrittelee arvon, jonka ylityttyä luodaan kriittinen tapahtuma
- -o määrittelee OID:n jolla arvoa kysytään.

Tämä asetusohja piirtää keräämänsä tiedot kuuteen eri kuvaajaan. Kuviossa 24 on niistä kolme ensimmäistä.



KUVIO 24. Valmiin UPS-asetusohjan luomia kuvaajia.

8.2 DHCP-palvelimen seuranta

8.2.1 Windows

Windows-palvelin ilmoittaa käytössä olevien osoitteiden määrän OID:lla 1.3.6.1.4.1.311.1.3.2.1.1.2.<verkon IP-osoite> ja vapaana olevien osoitteiden määrän OID:lla 1.3.6.1.4.1.311.1.3.2.1.1.3.<verkon IP-osoite>. Esimerkiksi yleisöverkossa verkon IP-osoitteena on 10.200.50.0. Näiden kahden tietolähteen pohjalta luotiin osoitteiden käyttöasteen kuvaaja (ks. kuvio 25).

8.2.2 Linux

Koska Linuxin Net-SNMP:n kautta ei näitä tietoja saa suoraan SNMP-kyselyllä, oli käytettävä paikallista skriptiä, joka seuraa DHCP:n käyttöä ja luo paikalliselle koneelle samantyyppiset tiedot kuin Windows-palvelimilla. Nämä tiedot voi Zenoss kysyä normaalisti SNMP:n avulla. Käytetty skripti oli nimeltään Dhcpd-snmp ja seuraavaksi kuvataan sen asennusvaiheet. Ohje perustuu ohjelman omaan Readme-tiedostoon. Ensin on haettava skriptin sisältävä paketti, minkä jälkeen se voidaan asentaa seuraavasti:

```
tar xzvf dhcpd-snmp-0.2.tar.gz
cd dhcpd-snmp-0.2
./configure
make
make install
```

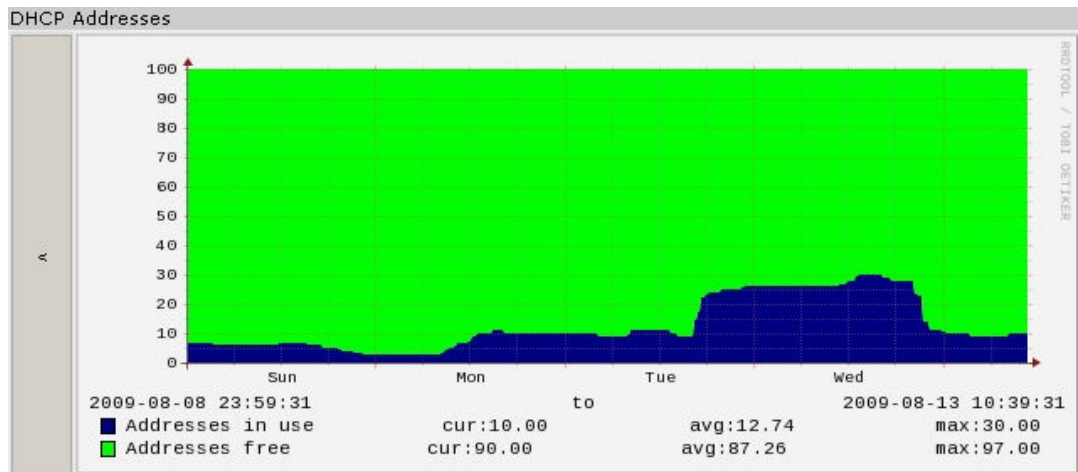
Tämän jälkeen luodaan tiedosto dhcpd-snmp.conf hakemistoon /usr/local/src/dhcpd-snmp. Tiedostossa on oltava seuraavat kaksi riviä, joista leases määrittelee dhcpd.leases-tiedoston sijainnin ja pool seurattavan DHCP-poolin ominaisuudet järjestyksessä <poolin numero>, <kuvaus>, <jaossa olevat IP-osoitteet>:

```
leases: /var/lib/dhcp3/dhcpd.leases
pool: <poolin numero>, <kuvaus>, <ensimmäinen jaettu IP-osoite>-<viimeinen jaettu IP-osoite>
```

Hakemistosta /usr/share/snmp yleensä löytyvään konfiguroitavaan snmpd.conf-tiedostoon lisätään rivi

```
pass_persist .1.3.6.1.4.1.21695.1.2 /usr/local/sbin/dhcpd-snmp /usr/local/src/dhcpd-snmp/dhcpd-snmp.conf
```

Asennushakemiston dhcp-snmp-0.2 ja ladatun paketin voi poistaa. Skripti käynnistetään komennolla dhcpd-snmp. Muutosten jälkeen snmpd-palvelu on käynnistettävä uudelleen. Skriptin voi myös lisätä automaattisesti käynnistyvien ohjelmien joukkoon. Dhcp-snmpd-skripti laajentaa Net-SNMP-ohjelmaa niin, että DHCP:stä saadaan suoralla kyselyllä tarvittavat tiedot. Käytössä olevia osoitteita voidaan nyt kysyä Zenossissa OID:lla 1.3.6.1.4.1.21695.1.2.2.4.<poolin numero> ja vapaiden osoitteiden määrää OID:lla 1.3.6.1.4.1.21695.1.2.2.6.<poolin numero>, ks. kuvio 26.



KUVIO 25. DHCP-osoitteiden käyttöä osoittava kuvaaja.

Data Sources			
Name	Source	Source Type	Enabled
<input type="checkbox"/> active leases	1.3.6.1.4.1.21695.1.2.2.4.1	SNMP	True
<input type="checkbox"/> available addresses	1.3.6.1.4.1.21695.1.2.2.6.1	SNMP	True

KUVIO 26. Asetuspohjan tietolähteiksi lisätyt Linux-palvelimen DHCP-tiedot.

8.3 Comet Systems P8510 -lämpömittarit

Lämpömittareita varten luotiin uusi laiteluokka, /Devices /Lampomittari, johon luotiin uusi asetuspohja Comet Systems P8510 -mittareita varten. Kuvion 27 asetuspohja hakee ainoastaan kaksi arvoa, lämpötilan ch1IntVal ja hälytyksen tilan, ch1Alarm.

/Devices /Lämpömittari /Templates /Comet Systems P8510 Zenoss server time: 9:46:40

Performance Template

State at time: 2009/08/17 09:42:12

Name: Comet Systems P8510
 Target Class: Products.ZenModel.Device
 Description: P8510-lämpömittarille säädetty template. Data Source ch1Alarm hakee hälytyksen tilan, joka voi olla 0 (ei hälytystä), 1 (pieni hälytys), 2 (iso hälytys). Kynnysarvoja

Save

Data Sources

Select: All None

Name	Source	Source Type	Enabled
<input type="checkbox"/> ch1Alarm	1.3.6.1.4.1.22626.1.5.2.1.4.0	SNMP	True
<input type="checkbox"/> ch1IntVal	1.3.6.1.4.1.22626.1.5.2.1.3.0	SNMP	True

Thresholds

Name	Type	Data Points	Severity	Enabled
------	------	-------------	----------	---------

Graph Definitions

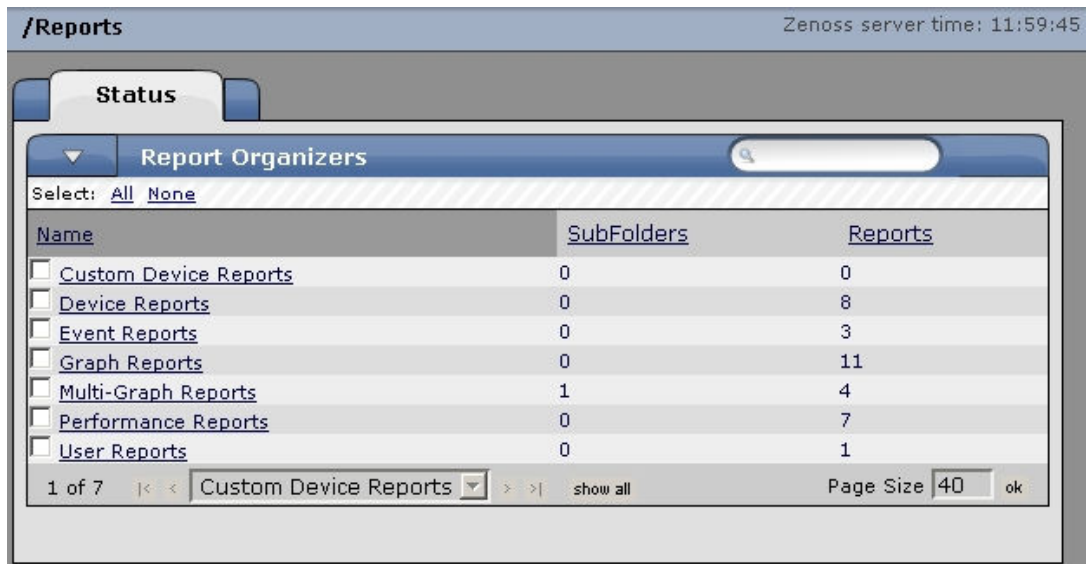
Select: All None

Seq	Name	Graph Points	Units	Height	Width
0	<input type="checkbox"/> Temperature	ch1IntVal	celsius	100	500
1	<input type="checkbox"/> Alarm	0_No Alarm 1_Alarm Hi 2_Alarm Lo		100	500

KUVIO 27. Lämpömittarin asetus pohja.

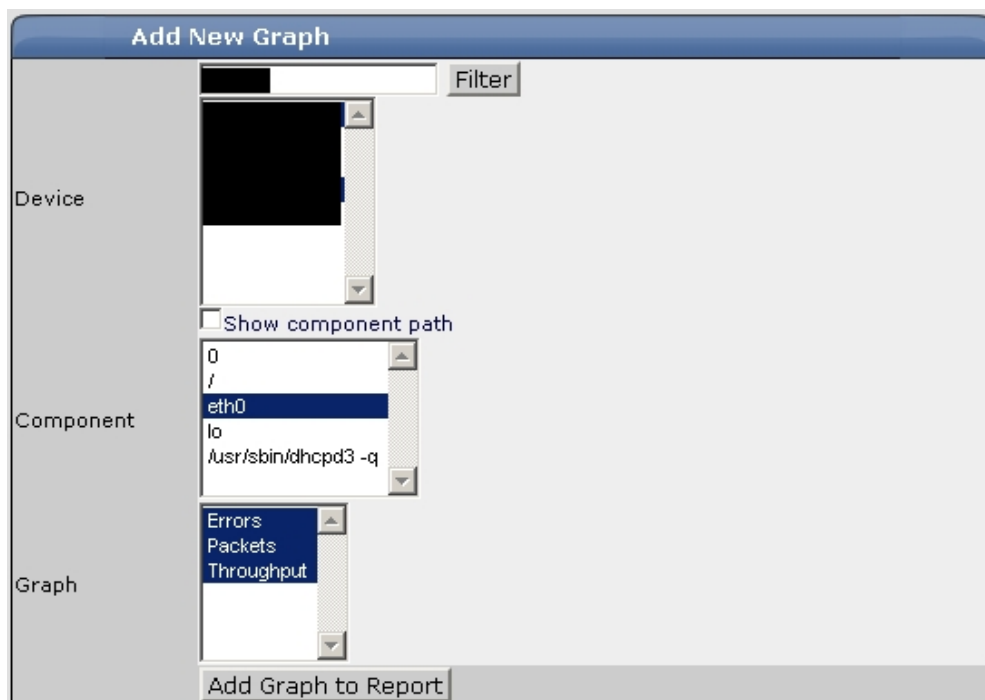
9 RAPORTIT (REPORTS)

Raportteja katsotaan ja luodaan päävalikon Reports-osion alta (ks. kuvio 28). Ohjelmassa on joitakin raportteja valmiina ja osa on tullut asennettujen lisäosien mukana. Esimerkiksi Device reports -osion alla on raportti, josta näkee kaikkien laitteiden tilan kootusti yhdellä sivulla.



KUVIO 28. Raporttien pääsivu.

Käyttökelpoisimpiin raporttilajeihin kuuluvat kuvaajia käyttävät raportit, jotka löytyvät Graph reports -osion alta. Uusi raportti luodaan valitsemalla esim. Graph reports -sivun Reports-kohdasta ▾ → Add graph report, jolloin päästään raportinluontisivulle (kuvio 29).



KUVIO 29. Kuvaajaraportin luonti.

Kuvion 29 Add new graph -osiossa määritellään näytettävät tiedot.

- Device-kohdassa valitaan laitteet josta kuvaajat haetaan. Näppäimistön Control-nappia pohjassa pitämällä voidaan valita useampi laite.
- Component-kohdassa valitaan mistä osasta halutaan tietoja. Tässä kohdassa näkyvät mm. kiintolevyt, verkkokortit ja lämpötila-anturit. Valinnan jälkeen Graph-kohtaan ilmestyvät osan seurattavat ominaisuudet, esim. kiintolevyn valinnan jälkeen Utilization (käyttöaste).
- Jos Component-kohta jätetään tyhjäksi, Graph-kohdasta ovat valittavissa kuvaajat, jotka normaalisti näkyvät laitteen Perf-sivulla.

10 HÄLYTYKSET (ALERTING RULES)

Sähköpostiin tulevia hälytyksiä varten Zenossin sähköpostiasetusten tulee olla kunnossa. Zenossin käyttämä sähköpostipalvelin määritellään Settings-asetussivulla. Sen toiminnan voi varmistaa lähettämällä testisähköpostin käyttäjän Preferences-asetussivulla. Tapahtuman vakavuusaste (Severity) on tärkeässä osassa hälytysten asettamisessa. Esimerkiksi jos laite ei vastaa Ping-viestiin, järjestelmä generoi oletuksena kriittisen vakavuusasteen tapahtuman. Hälytykset ovat käyttäjäkohtaisia. Uusi hälytyssääntö luodaan käyttäjän Preferences-asetussivulla valitsemalla Alerting rules, minkä jälkeen valitaan $\nabla \rightarrow$ Add alerting rule. Sivulle syntyy uusi sääntö, jota painamalla päästään muokkaamaan hälytyksen asetuksia (ks. kuvio 30).

KUVIO 30. Uuden hälytyksen asetusten muokkaus.

Kuvion 30 hälytyksen ehtoja voidaan muokata monipuolisesti.

- **Delay (secs)** määrittää viiveen sekunneissa ennen hälytyksen lähettämistä.
- **Enabled**-kohdasta hälytys otetaan käyttöön valitsemalla True.
- **Address (optional)** -kohtaan voi määrittellä sähköpostiosoitteen, jos hälytyksen haluaa jollekin toiselle.
- **Send clear messages**, jos päällä, lähetetään viesti kun tilanne palaa normaaliksi.

Suodattimilla määritellään ehdot hälytyksen täyttymiselle. Oletuksena hälytyksessä on kolme suodatinta, joista minkä tahansa voi tarvittaessa poistaa oikeanpuoleisesta “-“ -painikkeesta. Suodattimet käyttävät loogisia operaattoreita $<$, \leq , $=$, \geq ja $>$, joilla määritetään miten ehdon tulee täsmätä. Suodattimia voi myös lisätä, ja niistä käyttökelpoisimpia lienevät laitteen nimeä ja laiteluokkia koskevat suodattimet.

Seuraavassa esimerkissä hälytyssäntö on luotu niin, että sijainniksi (Location) on määritelty Mehtälä ja vakavuusaste (Severity) on kriittinen (Critical). Kun Zenoss havaitsi yhteyden menetyksen, se lähetti seuraavan sähköpostin otsikolla ”[zenoss] mehtalan_palvelin ip 10.100.34.34 is down”:

```
Device: mehtalan_palvelin
Component:
Severity: Critical
Time: 2009/08/20 08:34:24.000
Message:
ip 10.100.34.34 is down
```

Koska hälytyksen oli käsketty myös lähettää ilmoitus kun tilanne on ohi (Send clear messages -kohta), tuli yhteyden palaututtua seuraava viesti otsikolla ”[zenoss] CLEAR: mehtalan_palvelin ip 10.100.34.34 is up”:

```
Event: 'ip 10.100.34.34 is down'
Cleared by: 'ip 10.100.34.34 is up'
At: 2009/08/20 18:18:17.000
Device: mehtalan_palvelin
Component:
Severity: Critical
Message:
ip 10.100.34.34 is down
```

11 OHJELMAN OMAT LOKIT

Zenossin daemonien luomia lokitiedostoja voidaan tarkastella sivulta Settings → Daemons, jossa jokaisen daemonin kohdalla on oma Näytä loki -painikkeensa. Nämä lokit näyttävät vain uusimmat tapahtumat. Vanhemmat lokit löytyvät hakemistosta /usr/local/zenoss/zenoss/log. Vanhempien lokien tiedostonimet päättyvät log.1, log.2 tai log.3, joista .3-päätteiset ovat vanhimpia.

12 VARMUUSKOPIOINTI JA PÄIVITYS

Zenossin tietokantojen varmuuskopiointiin on oma ohjelmansa, Zenbackup. Sen voi ajaa joko web-käyttöliittymän kautta sivulta Settings → Backups tai komentoriviltä zenoss-käyttäjänä komennolla zenbackup. Tehdyt varmuuskopiot luodaan oletuksena pakattuina tgz-tiedostoina hakemistoon /usr/local/zenoss/zenoss/backups ja nimitään zenbackup_<päivämäärä>.tgz. Näin tehty varmuuskopio sisältää

- **Zopen tietokannan** eli järjestelmään lisätyt laitteet, käyttäjät ja niiden asetukset
- **MySQL-tapahtumatietokannan**
- **\$ZENHOME/etc-hakemiston**, joka sisältää Zenossin daemoneiden asetukset
- **\$ZENHOME/perf-hakemiston**, joka sisältää suorituskykykuvaajat RRD-tiedostoina.

Seuraavassa esimerkissä varmuuskopiointi on suoritettu komentoriviltä:

```
zenoss@zenoss:~$ zenbackup
INFO:zenbackup:Getting MySQL dbname, user, password from ZODB.
INFO:zenbackup:Backing up events database.
INFO:zenbackup:Backup of events database completed in 11 minutes.
INFO:zenbackup:Backing up the ZODB.
INFO:zenbackup:Backup of ZODB database completed in 32 seconds.
INFO:zenbackup:Backing up config files.
INFO:zenbackup:Backup of config files completed.
INFO:zenbackup:Backing up performance data (RRDs).
INFO:zenbackup:Backup of performance data completed in 29 seconds.
INFO:zenbackup:Packaging backup file.
INFO:zenbackup:Backup written to
/usr/local/zenoss/zenoss/backups/zenbackup_20090731.tgz
INFO:zenbackup:Cleaning up staging directory /tmp/tmpgiAfPG
INFO:zenbackup:Backup completed successfully in 13 minutes.
zenoss@zenoss:~$
```

Varmuuskopio palautetaan komennolla `zenrestore - file=<varmuuskopiotiedosto>`. Ennen komennon ajamista Zenossin daemoneiden on oltava pysäytettyinä.

Zenoss-ohjelmasta ei tullut uutta päivitystä toteutusvaiheen aikana, joten ohjelman päivitystä ei suoritettu tässä asennuksessa. Se kuitenkin onnistuu muiden Debianin ohjelmien tavoin Apt-ohjelmalla ja on periaatteessa hyvin yksinkertaista. Komentoriviltä ajetaan root-käyttäjänä komennot `apt-get update` ja `apt-get upgrade`. Ensimmäinen komento hakee tiedot saatavilla olevista päivityksistä ja toinen lataa sekä asentaa kaikki mahdolliset päivitykset. Ennen Zenossin päivittämistä on kuitenkin hyvä tutustua uutta versiota koskevaan Release notes -osioon ohjelman dokumentaationsivulla (*Zenoss documentation 2009*). Päivityksissä on yleensä rajattu versiot, joista voi suoraan päivittää uusimpaan versioon.