VERKONHALLINTA SOVELLUKSET

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2008
Antti Oksanen

Lahden ammattikorkeakoulu
Tietoliikennetekniikka

Antti Oksanen:

Opinnäytetyö
Verkon palveluiden hallinta

Tietoliikennetekniikan opinnäytetyö, 43 sivua, 5 liitesivua

Kevät 2008

TIIVISTELMÄ

Opinnäytetyön tavoitteena on vertailla kahta verkonvalvontaan käytettyä ohjelmistoa ja miettiä ohjelmien soveltuvuutta PK- yritysten dataverkkojen valvontaan. Ohjelmat ovat Linux -pohjainen Nagios ja Windows -pohjainen GFI:n NSM (Network Server Monitor). Ohjelmista Nagios edustaa vapaanlähdekoodin ohjelmistoa eli toisin sanoen ohjelma on peruskäytössä ilmainen. GFI:n NSM ohjelma edustaa kaupallista ohjelmistoa ja ohjelman käyttöön tulee olla maksettu lisenssi.

Nykyinen dataverkkoihin ja verkkopalveluihin luottava yritysinfrastruktuuri on haavoittuva palveluiden kaatuessa. Verkonhallinnalla pyritään tarkkailemaan verkon toimivuutta ennen palvelun kaatumista ja mahdollisesti reagoimaan ennalta tuleviin ongelmiin. Verkonhallintasovellukset pyrkivät vapauttamaan ylläpitäjiä tuottaviin tehtäviin ja automatisoimaan valvontaa.

Verkonhallinnan ”de facto” standardiprotokolla on SNMP, jonka kolme versiota SNMPv1, SNMPv2 ja SNMPv3 mahdollistavat laitteiden etävalvonnan ja -hallinnan. TCP/IP -pohjainen SNMP protokolla sisältää MIB- hallintatietokannan, jossa on tiedot valvottujen laitteiden tarkastuksista (objekteista). MIB tietokanta on hierarkkinen tietokanta, jonka sisältämät objektit on nimetty numeerisesti. Nimien numeeriset muodot periytyvät hierarkian korkeammilta tasoilta ja niiden pohjalta verkonvalvontaohjelmat saavat tietoa laitteiden tilasta.

Nagioksen ja GFI NSM- verkonvalvontaohjelmien asennukset eroavat toisistaan melkoisesti vaikka ohjelmien tarjoamat ominaisuudet ovat hyvin samankaltaiset. Ohjelmista GFI NSM on mielekkäämpi käyttää ja erottuu edukseen graafisen hallintansa ansiosta.

PK- yritysten erilaiset vaatimukset huomioon ottaen on molemmilla ohjelmilla hyviä puolia. Yritysten vaatimukset rajoittuvat kuitenkin perusohjelmalliseen puoleen, joten molemmilla vertailun ohjelmilla saadaan tarkastukset muokattua vaatimuksiin sopiviksi.

Avainsanat: verkonvalvonta, Nagios, GFI, NSM, SNMP

Lahti University of Applied Science
Faculty of Technology

Oksanen, Antti : Monitoring of Network Services

Bachelor´s thesis in telecommunications technology, 43 pages, 5 appendices

Spring 2008

ABSTRACT

The objective of the thesis is to compare two network monitoring programs and consider the suitability of those programs to monitor a company's network appliances. These two programs are Linux–based Nagios and Windows–based GFI NSM. Nagios represents license free program´s, it is under generic public license. GFI NSM is a licensed program that requires the user to pay for a license.

Nowadays the infrastructure of companies relies on data and network appliances. If the network fails, the productivity of the company drops. Network monitoring aims to inform the network administrator if there is a problem in the network. By doing that it tries to minimize losses and offer automatic monitoring to prevent basic problems.

Network monitoring relies on the SNMP protocol which is the standard of network monitoring. SNMP offers distance monitoring of network appliances. The SNMP protocol includes a MIB database of objects used to monitor network equipment. MIB is a hierarchic database.

The installation procedures of Nagios and GFI NSM differ from each other quite a lot. There are many similarities in features offered by the programs but GFI NSM is simpler to administrate.

Considering the needs of companies, both programs are able to provide basic checks. For special requirements the checks can be customised to meet the needs.

Keywords: Network Monitoring, Nagios, GFI, NSM, SNMP

SISÄLLYS

LYHENTEET

AD	Active Directory
	Aktiivihakemisto järjestelmä
CMIP	Common Management Information Protocol
	Yleinen hallinta tieto protokolla
CMOT	CMIP over TCP/IP
	CMIP TCP/IP:n päällä toteutettuna
DNS	Dynamic Name Server
	Nimien selvitys palvelu
FTP	File Transfer Protocol
	Tiedoston siirtoon käytetty protokolla
GPL	General Public License
	Vapaa ohjelmisto lisenssi
HTTP	Hypertext Transfer Protocol
	Hypertekstin siirtoon käytetty protokolla
HTTPS	HTTP Secure
	Tietoturvallinen versio HTTP protokollasta
IAB	Internet Architecture board
	Internet arkkitehtuurista vastaava lautakunta
ICMP	Internet Control Message Protocol
	Internet hallinta viesti protokolla
IMAP	Internet Message Access Protocol
	Internet viestien käsittely protokolla
IP	Internet Protocol
	Internet protokolla, vastaa pakettien siirrosta
ISP	Internet Service Provider
	Internet palveluntarjoaja

ITU-T	International Telecommunication Union – Telecommunication Telealan standardeja kansainvälisesti koordinoiva järjestö
MIB	Management Information Base Hallintotietokanta SNMP protokollan palveluille. tietokannan olioita voidaan käsitellä verkonhallinnan protokollilla.
MIB-II	Management Information Base II Hallintotietokanta 2 uudistettu versio
MS	Microsoft Microsoft – yritys
MSDE	Microsoft Desktop Engine Microsoftin työpöytä moottori tietokannalle
NRPE	Nagios Remote Plugin Executor Nagioksen tiedonhakuun käyttämä lisäosa
NSCA	Nagios Service Check Acceptor Nagioksen palvelu tarkastus vastaanotto lisäosa
NSM	Network Server Monitor GFI:n valmistama ohjelma verkon palveluiden valvontaan
NTP	Network Time Protocol Ajanhallinta protokolla
OSI	Open Systems Interconnection Tiedonsiirtoprotokollien kuvaus seitsemässä kerroksessa
ODBS	Open Database Connectivity Microsoftin määrittelemä rajapinta API tietokannoille
PDU	Protocol Data Unit Protokolla tieto yksikkö. Sisältää yhteyskäytännön hallinta ja käyttäjä tietoja
RFC	Request For Comments Internet standardeja määritteleviä dokumentteja
POP	Post Office Protocol Postin kuljetus protokolla

POP3	Post Office Protocol version 3 Postin kuljetus protokolla versio 3
SMI	structure of management information MIB tietokannan olioiden järjestyksen rakenteen määritykset
SMP	Simple Management Protocol Yksinkertainen hallinta protokolla josta piti tulla SNMP:n seuraaja
SMTP	Simple Mail Transfer Protocol Yksinkertainen sähköpostin kuljetus protokolla
SNMP	Simple Network Management Protocol Yksinkertainen verkonhallinta protokolla
SQL	Structured Query Language Standardoitu kyselykieli relaatiotietokannalle
SSH	Secure Shell Tietoturvallinen tiedon käsittely protokolla
SSL	Secure Sockets Layer Turvallisen yhteyden salausprotokolla
TCP	Transmission Control Protocol Tiedonsiirron hallinta protokolla
TELNET	TELecommunication NETwork Yhteys protokolla pääteyhteyksille
UDP	User Datagram Protocol UDP – tiedonsiirto protokolla
VBS	Visual Basic Scripting Visual Basic ohjelmointikieli

1 JOHDANTO

Työn tavoitteena on perehtyä verkonvalvontaan ja tarkastella kahden verkonvalvontaohjelmiston käyttöä ja tarkastuksia. Ohjelmistojen tarkastelussa otetaan huomioon soveltuvuus PK -yritysten tietoverkkojen ja verkkopalveluiden valvontaan. Työssä perehdytään myös verkonvalvontaan ja SNMP –protokollan toimintaan. Työ on toimeksianto Systematic Oy:ltä. Opinnäytetyön teoriaosuudessa perehdytään verkonvalvontaan ja SNMP protokollaan. Verkonvalvonta ja –hallinta on syntynyt tarpeesta automatisoida verkon toimintojen valvontaa. Yrityksien kasvavien tietoverkkojen valvonta, ylläpitäjien toimesta, ilman keskitettyä hallintaa olisi hankalaa tai mahdotonta. Automatisoinnilla pyritään kontrolloimaan ongelmia ja siihen, että ongelmatilanteessa ongelman syy olisi jo valmiiksi tiedossa.

Systematic Oy on yritys, joka tarjoaa tietoteknisiä palveluita, pääsääntöisesti PK- (pienille ja keskisuurille) yrityksille Lahden seudulla. Yritykselle tuli tarve vertailla ja pohtia kahden verkonvalvontaan käytettävän ohjelman eroja ja soveltuvuutta markkinakäyttöön. Markkinakohteina olisivat yritykset, joiden tietotekniseen laitteistoon kuuluisi vähintään yksi palvelimen lailla palveleva työasema tai varsinainen palvelin. Ohjelmat eroavat toisistaan merkittävästi, sillä ohjelmista Nagios on ilmainen ja toimii Linux -käyttöjärjestelmän päällä. Toinen ohjelma, kaupallinen GFI NSM (Network Server Monitor), on maksullinen ja Windows käyttöjärjestelmän päällä toimiva kokonaisuus.

Opinnäytetyö jakautuu neljään osaan, ensimmäisen käsitellessä verkonvalvontaa ja SNMP (Simple Network Management Protocol) -protokollaa teoriatasolla. Toinen osa sisältää ohjelmien asentamisen ja asetusten tarkistamisen. Kolmas osa on ohjelmien ominaisuuksien vertailua ja viimeinen, neljäs osa, keskittyy johtopäätökseen.

2 VERKONVALVONTA JA HALLINTA

2.1 Tausta verkonvalvonnalle

Tietotekniikka on vahvasti kasvava ala ja eritoten laajenevat yritysten sisäiset verkot asettavat uusia vaatimuksia järjestelmien ylläpitäjille. Palvelut monipuolistuvat ja niiden toimintavarmuutta on kasvatettu hajauttamalla niitä eri palvelimiin. Palvelut vaativat valvonnalta uusia ominaisuuksia, joihin ei perinteisellä ylläpitämisellä päästä. Monikansallisissa yrityksissä on palveluiden toiminnan varmistamiseksi lähdetty jopa sijoittamaan kahdennettu palvelin eri maahan. Yritysten tuoton ja toimivuuden riippuessa yhä enemmän tietoteknisistä palveluista tulee niiden välittömään korjaamiseen kiinnittää enemmän huomiota. Jatkuva valvonta taas tarkoittaa valvonnan automatisointia. Automatisoinnilla pyritään vapauttamaan ylläpitäjiä tehtäviin, jotka tähtäävät enemmän verkon kehitykseen kuin valvontaan. (Feldman. 1999.)

Toimiva automaattinen valvonta edellyttää toimiakseen standardoituja työkaluja, jotka soveltuvat myös verkon aktiivilaitteiden valvontaan. Toiminnan kannalta on ehdottoman tärkeää hallintaprotokollan luotettava ja nopea toiminta. Tällä hetkellä verkonhallinnan de facto standardi on SNMP, jonka suosiota edesauttoi hyvä yhteensopivuus TCP/IP (Transmission Control Protocol / Internet Protocol)-protokollan kanssa. SNMP ei suikaan ole ainoa verkonhallintaan käytetty protokolla vaan sillä on aikoinaan ollut kilpaileva protokolla CMIP (Common Management Information Protocol). CMIP:stä kehitettiin, TCP/IP:n yleistyessä, CMOT (CMIP over TCP/IP), joka oli TCP:IP:n kanssa yhteensopiva. CMOT ei kuitenkaan ollut niin nopea kuin SNMP, joten CMOT -protokolla ei yleistynyt yleiseen käyttöön. CMOT oli kuitenkin huomattavasti monipuolisempi verrattuna SNMP -protokollaan mutta samalla CMOT kulutti enemmän resursseja ja toimi hitaammin. (Hautaniemi. 1994.)

Verkon valvonnan perinteinen käsite on ainoastaan tilanteen seuranta, kunnes havaitaan vika. Kun vika on havaittu, alkaa vian laajuuden hahmotusprosessi, joka käytännössä perustuu suulliseen tietoon käyttäjiltä. Seuraavassa vaiheessa vikaa tutkitaan ja syyn löydyttyä suoritetaan korjaavia toimenpiteitä. Tässä vaiheessa on normaali työrutiini pysähtynyt ja suoritetaan vain niitä toimenpiteitä joihin ei vikaantunut verkon osaa vaikuta. Pienikin vika voi aiheuttaa mittavan seisauksen vian osuessa kriittiseen paikkaan. Ylläpitäjillä vian hahmottamiseen käytettävä tieto saattaa tällaisessa tilanteessa perustua käyttäjien antamaan käsitykseen. Väärä informaatio saattaa aiheuttaa luotettavaksi tulkittuna runsaasti aikaa vieviä lisätöitä. (Hautaniemi. 1994.)

2.2 Verkonhallinta

Verkonhallinta jakautuu käsitteenä kahteen osaan, verkonvalvontaan ja verkonhallintaan. ITU-T (International Telecommunication Union- Telecommunication) on asettanut omat suosituksensa verkonhallintaan X 700 -suosituksessa. X 700 -suositukset jakautuvat viiteen kategoriaan:

1. Fault management (Vikojen hallinta)
2. Accounting management (Käytön hallinta)
3. Configuration management (Kokoonpanon hallinta)
4. Performance management (Suorituskyvyn hallinta)
5. Security management (Turvallisuuden hallinta). (ITU- T 2008.)

Vikojen hallinnalla pyritään vian täsmälliseen paikantamiseen. Lisäksi vikojen hallinta pyrkii korjaamaan havaitun vian. Tietoa viasta ja verkon kunnosta saadaan hälytyksistä, virhelokeista, laitteista ja diagnostiikkatesteistä. Perusdiagnostiikaksi voidaan lukea esimerkiksi vastauspyynnön lähetys laitteelle. Vianhallinnan lyhyen tähtäimen ratkaisu on vian paikallistaminen, eristäminen ja verkon toimintaan saaminen. Loppukäyttäjän näkökulmasta verkon toimivuus on se, mikä merkitsee. Pidemmällä tähtäimellä pyritään estämään vian toistuminen. (Feldman. 1999.)

Käytön hallinta kohdistuu resurssien jakautumisen seurantaan niin käyttöoikeuksien hallinnan kuin resurssien käytön seuraamisen osalta. Käyttäjät jaetaan ryhmiin ja ryhmien kautta annetaan heille oikeudet ja tunnukset tarvittaviin resursseihin. Tarpeen vaatiessa voidaan tehdä yksilöllisiä lisäyksiä oikeuksiin. Myös käyttäjien tapahtumien seuranta esimerkiksi laskutusta varten on mahdollista. Tiedoilla voidaan vaikuttaa verkon suunnitteluun ja ohjeiden tekemiseen. Lisäksi on tehtävä päätöksiä rajoista joita käyttäjille annetaan ja mahdollisista toimista rajan ylittyessä. Lainopilliset ja tietoturvaan liittyvät seikat on syytä ottaa tarkasti huomioon, tietojen keräämisessä ja hyödyntämisessä. (Feldman. 1999.)

Kokoonpanonhallinta on keskeinen osa verkonvalvontaa, ja sen osana on hallita verkon laitteiden asetuksia ja määrityksiä. Verkkoa rakennettaessa on dokumentointi tehtävä tarkasti, jotta kokoonpanon hallintaa varten on helpompi tehdä suunnitelma. Verkon kokoonpanosta on tiedettävä laitteiden tarkat tiedot sekä verkon looginen ja fyysinen rakenne, jotta tarvittaessa saadaan esimerkiksi reititystauluja muokkaamalla tehtyä muutoksia asetuksiin. Ylläpidon puolestakin on hyötyä, jos verkkoon voidaan tehdä korjauksia kokonaisuuden kaatumatta. Laitteiden uudestaan käynnistäminen ilman ongelmia on tärkeää, jotta varmuuskopioiden ottaminen ja palauttaminen sujuvat ongelmitta. (Feldman. 1999.)

2.3 Verkonvalvonta

Suorituskyvyn hallinta on keskeinen osa verkonhallintaa. Tietoliikenneverkko on yhtä haavoittuvainen ruuhkautumiselle kuin moottoritiet ovat tieliikenteelle. Yleisen kuorman ylittäessä kriittisen pisteen verkon kapasiteetti romahtaa. Suorituskyvyn hallinnalla seurataan verkon osien kuormitusta mittaamalla eri asioita. Mitattavia asioita ovat mm. virheiden määrä, liikennemäärät sekä käyttö- ja vasteajat. Mittauksilla pyritään ennaltaehkäisemään tilannetta, jossa verkon kuorman kriittinen piste ylittyisi. Ennaltaehkäisyllä voidaan keskittyä kuormittuviin verkon osiin ja tarvittaessa uudistaa niitä kasvattaen samalla verkon kapasiteettiä. Verkonhallinta ja -valvonta järjestelmissä yksinkertaiset suorituskyvyn hallinta- ja valvonta- työkalut antavat tietoa verkon tilasta ja aktiivilaitteista. Tiedot saadaan

esiin graafisessa ja helposti luettavassa muodossa. Tietojen avulla voidaan paikallistaa verkon pullonkauloja ja eristää suorituskykyongelmat. (Feldman. 1999.)

Turvallisuudenhallinnan merkitys on lisääntynyt verkkojen kasvaessa ja erilaisten etätyöskentelytapojen lisääntyessä. Turvallisuudenhallinnan päätarkoitus on luottamuksellisen tiedon suojaaminen kontrolloimalla pääsykohtia tietoihin. Luottamuksellinen tieto voi käsittää esimerkiksi kaiken yritystä koskevan tiedon. Turvallisuudenhallinta antaa ylläpidolle mahdollisuuden suojata tietoja rajoittamalla pääsyä yrityksen verkkoon ja työasemille. Oikein toteutetulla ja ylläpidetyllä turvallisuudenhallinnalla saavutetaan turvallinen ja silti käyttökelpoinen verkko. Turvallisuudenhallinta ei suoranaisesti ota kantaa ohjelmistojen tietoturvaan eikä myöskään fyysiseen turvallisuuteen. (Feldman. 1999.)

Verkonvalvonta tarkoittaa tilan tarkkailua, tietojen keräämistä verkon rakenteesta, laitteista ja toimivuudesta. Verkon tärkein ominaisuus, suorituskyky, on kriittisessä asemassa, sillä liikaa kuormitettu verkko ei kykene välittämään viestejä perille vaan tieto katoaa matkalla. Ylläpitäjien käsityksestä verkon normaalista kuormasta saattaa vikatilanteessa olla huomattavaa hyötyä. Suurin hyöty kuormatiedolla saavutetaan kuitenkin ennaltaehkäisevässä mielessä, sillä yleisesti kuorman nouseminen ja kriittisen toimintarajan saavutus voidaan ennakoida ja eniten kuormittuvia verkonlaitteita korvata uudemmilla. Tietojen keräämisellä voidaan ennakoida ja reagoida tilanteeseen, vaikka varautumalla investointeihin. (Feldman. 1999.)

3 SNMP

3.1 SNMP -standardit

Vuonna 1988 IAB valitsi SNMP:n lyhyen tähtäimen ratkaisuna verkonhallinta standardiksi. IAB:n tarkoitus oli antaa kehitysaikaa CMIP:lle, jota oltiin edelleen kehittämässä TCP/IP:n päälle CMOT -protokollaksi. Yleinen käsitys oli että OSI (Open Systems Interconnect) -protokollat tulisivat syrjäyttämään TCP/IP:n käytöstä pian, mutta historia on osoittanut toisin. Alun perin SNMP:n ja CMOT:n kehityksessä tähdättiin samankaltaiseen tietokantaan, joka olisi helpottanut myöhempää siirtymistä CMOT:n käyttöön. (Hautaniemi. 1994.)

OSI mallin erot TCP/IP -pinoon aiheuttivat suunnittelussa kuitenkin huomattavia ongelmia, jonka takia vielä samana vuonna SNMP vapautettiin OSI -mallia koskevasta suunnittelusta, vain TCP/IP -maailmaan. Vuonna 1989 SNMP:stä tuli TCP/IP -verkkojen de facto standardi, jonka tukemiseen lähtivät myös laitevalmistajat mukaan. 1990 SNMP hyväksyttiin, MIB:n ja SMI:n ohella viralliseksi Internetstandardiksi. (Hautaniemi. 1994.)

3.2 SNMP-protokolla

SNMP on sovellustason protokolla, jota käytetään vaihtamaan hallintatietoja verkkolaitteiden välillä. SNMP on osa paljon käytettyä, TCP/IP -protokollapinoa ja toimii UDP -protokollan päällä. Protokolla mahdollistaa verkon tilan tarkkailun ja ongelmien korjaamisen, samalla mahdollistuu verkon keskitetty suunnittelu ja suorituskyvyn valvonta. SNMP on versiokehityksensä aikana ehtinyt jo versioon kolme, jota kutsutaankin SNMPv3 nimellä. SNMP on kolmas osa TCP/IP:n verkonhallintaa MIB:n ja SMI:n rinnalla. (RFC1157. 1990.)

Alkuperäisen SNMP -protokollaversio yhden (SNMPv1) piti olla vain väliaikainen verkonhallintaprotokolla, mutta hyvien kilpailijoiden puuttuessa siitä tuli pitkäaikainen ratkaisu verkonhallintaprotokollaksi. Yksinkertaisuudella oli myös kääntöpuolensa sillä SNMPv1:ssä oli erittäin puutteellinen tietoturva. Kuka tahansa verkossa olija saattoi lähettää SNMP kyselyn koska autentikoinnissa oli suuria puutteita. Autentikointi perustui ainoastaan selväkielisenä lähetettävään hallinta-alueen nimeen ja kaikki sanomat kulkivat verkossa selväkielisinä. (Puska. 2000.)

SNMP versio kaksi kehitettiin paikkaamaan versio yhdessä olleita tietoturva aukkoja. Apuna kehityksessä toimi SMP (Simple Management Protocol), jonka pohjalta lähdettiin rakentamaan uutta SNMP:tä. Uutta versiota kehitettiin kahdessa työryhmässä, joista toinen keskittyi vain tietoturvaan ja toinen kaikkeen muuhun. SNMPv2 mahdollisti hajautetun verkonhallintakonseptin, joka käytännössä mahdollistaa useamman hallinta-aseman käytön. Useamman hallinta-aseman järjestelmissä asemat päivittivät tietoja suoraan toisilleen ”Inform-Request” -viesteillä, jottei kaikkia tietoja tarvitse kysyä laitteilta. Tavoitteena on turhan toiston vähentäminen. (Orava. 2000.)

SNMPv2 korjasi myös useita SNMPv1:ssä esiintyneitä toimintavirheitä. Tärkeimpänä mainittakoon ”Get-Request”- ja ”Get-Next-Request” -operaatiot. Operaatioiden toiminta SNMPv1:ssä oli atomaarista eli yhdenkin objektin tarkistuksen epäonnistuessa koko operaatio hylättiin. SNMPv2:ssa virheellisen objektin arvo palautettiin virhekoodin kanssa. Versio kaksi saavutti standardiluonnoksen aseman syksyllä 1993. Versio yhden julkaisusta oli silloin ehtinyt kulua jo neljä vuotta. (Orava. 2000; Hautaniemi. 1994.)

Uusin versio SNMP:stä on SNMPv3 eli versio 3, joka on määritelty RFC dokumenteissa 2271 – 2275. SNMPv3:n suurin uudistus on sen salauksen käyttö, jota käytetään sekä datan salaukseen että yhteysneuvottelun salaukseen. Salauksella saadaan aikaan luotettava yhteys. SNMPv3 käyttää myös käyttäjän hallintaa, jolloin mahdollistuu tunnuksia vastaava olioiden hallinta. Käytännössä voidaan määrittää joukko olioita, joihin pääsee vain laajemmat oikeudet omaavilla tunnuksilla.

Samalla varmistetaan yksityisyys, etteivät asiattomat pääse käsiksi viesteihin. Tunnistuksen myötä myös etäkäyttö mahdollistui, jolloin autentikointi toimii varmennuksena. SNMPv3 on edellisistä versioista poiketen suunniteltu joustavammaksi protokollaksi kuin versiot 1 ja 2, jotta versio kolmen elinkaari olisi pidempi. (IETF. 2008; RFC2571. 1999.)

3.3 SNMP perusoperaatiot

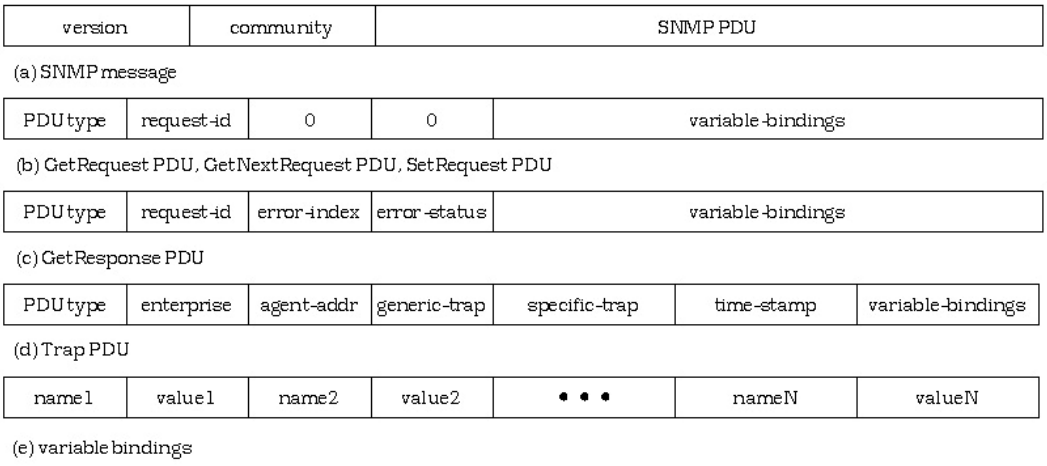
SNMP-protokolla käyttää hallinnoitujen laitteiden kontrolloimiseen neljää perus operaatiota:

- Read operatios (Lukuoperaatiot) on käytetyin operaatio, jolla valvotaan laitteiden toimintaa. Verkonhallintajärjestelmät käyttävät lukuoperaatiota lukeakseen muuttujien arvoja valvontapiirin laitteista. Esimerkkinä hallinta-asema pyytää laitteelta GetRequest -operaatiolla, jonkin olion arvoa.
- Write operations (Kirjoitusoperaatiot) on ohjauskomento. Verkonhallintajärjestelmät syöttävät arvoja valvontapiirin laitteisiin saavuttaakseen tarkoituksen mukaisen seurauksen. Esimerkkinä SetRequest, jolla voidaan asettaa arvoja olioille.
- Traversal operations (Kauttakulkuoperaatiot), puurakenteen seuraavan arvon lukemista tarkoittava operaatio.
- Traps (loukut), hallinnoidut laitteet ilmoittavat oma-aloitteisesti tärkeistä muutoksista verkkorakenteessa, hallintatyöasemalle. Toiminta perustuu ennalta-asetettuihin arvoihin ja niiden ylittyessä agentti ilmoittaa tilanteesta hallintatyöasemalle. (Happonen. 2005.)

3.4 SNMP yhteyskäytäntö

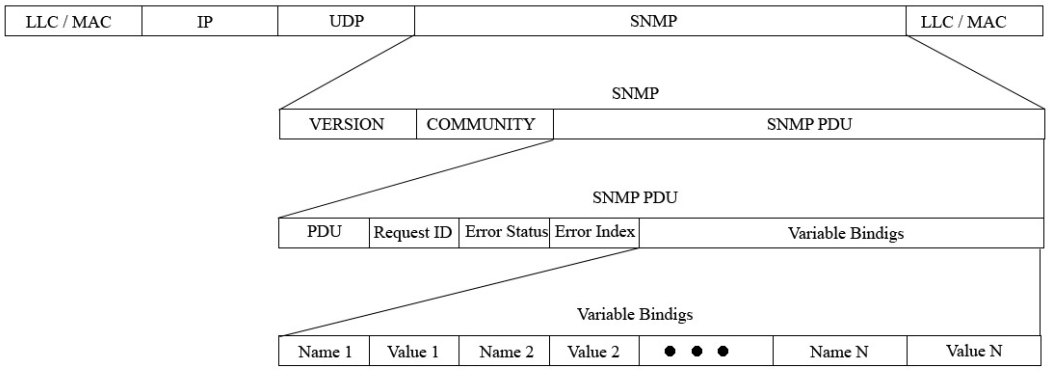
SNMP protokolla vaihtaa tietoa verkonhallintatyöaseman ja agenttien välillä SNMP viesteillä. Yhteyskäytäntö on pidetty yksinkertaisena, jotta hallittavat laitteet eivät kuormittuisi SNMP -yhteyksistä liikaa. KUVIOSSA 1 on esitelty SNMPv1:ssä käytetyt viestityypit joita on viisi. (Stallings 1996)

Kaikista viesteistä löytyy versionumero, yhteisönimi ja yksi PDU (Protocol Data Unit) -tyyppi. PDU sisältää viestin varsinaisen objekti -informaation ja määrittelee samalla viestin tyypin. Request ID määrittelee ID pyynnön tunnistavan numeron, error-status ja error-index määrittävät mahdollisen virheen tilan ja virheen lähteen. Variablebindigs määrittää varsinaisten objektien tiedot (Object-id, object-value). Trap viesti poikkeaa niin sisällöllisesti kuin käytöllisestikin muista viesteistä. Viestin sisältämä enterprise määrittää viestin laukaisseen objektin tunnisteen ja agent-addr agenttisolmun osoitteen. Gereric-trap ja specific-trap määrittävät yhdessä trap-viestin tyypin ja time-stamp kertoo ajan sidottuna verkkolaitteen viimeiseen alustushetkeen. (Happonen. 2005.)

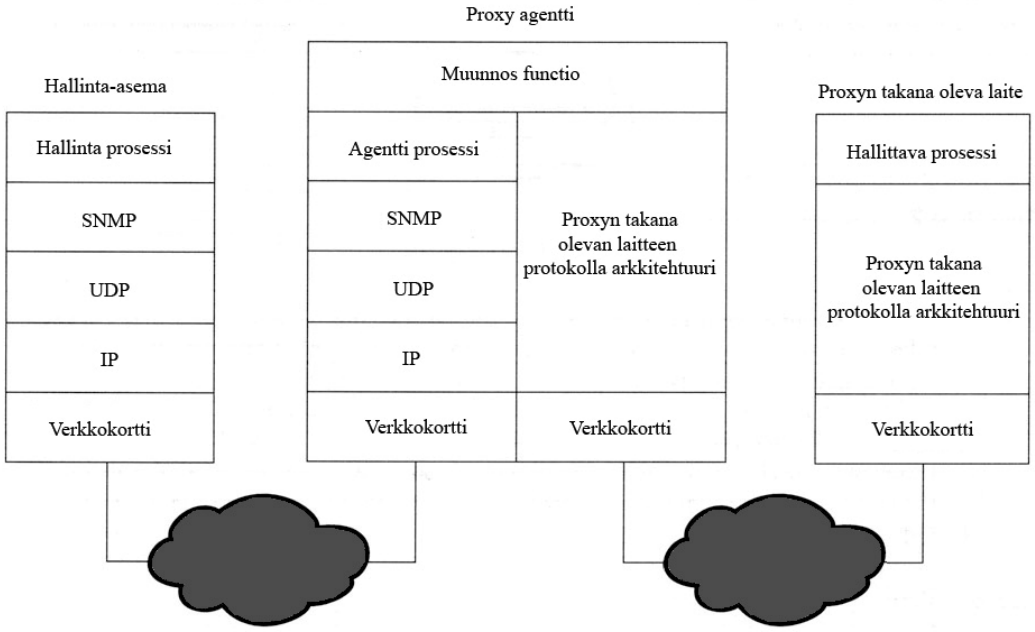


KUVIO 1. SNMP –protokollan tukemat viestityypit (Stallings, muokattu).

SNMP toimii UDP (User Datagram Protocol) -protokollan päällä ja käyttää hyväkseen IP -reititystä. KUVIO 2 selventää SNMP viestin rakennetta kerrosmaisesti ja selittää SNMP -protokollaviestin sijoittumista verkossa kulkevaan viestiin. SNMP -protokolla on suunniteltu hallinta-aseman ja agenttien väliseen keskusteluun, jolloin UDP protokollan käytöllä on haettu suorituskykyä, pakettien siirron luotettavuuden kustannuksella. Siirron luotettavuus onkin siksi toteutettu tarvittaessa ylempien protokollakerroksien avulla. Verkonvalvontasolmun tyypistä ja roolista riippuen protokollat voivat tukea myös muuta kuin UDP -protokollaa. Protokollia voivat olla tarpeen mukaan mm. FTP (File Transfer Protocol), TCP tai jokin sovelluskerroksen protokolla. (Stallings. 1996.)



KUVIO 2. SNMP -protokollan sijoitus ja rakenne (Syscom-Net, muokattu)



KUVIO 3. SNMP -protokollan proxy toiminta. (Charton, Leblanc muokattu)

KUVIOSSA 3 on esitetty proxy toiminnallisuuden toimintaperiaate eri protokollien välille. Proxy -agentin tehtävänä on tulkita eri protokollien SNMP -viestejä ja välittää niitä eteenpäin käyttäen vastaanottavan laitteen protokollaa. (Charton, Leblanc. 1999.)

3.5 SNMP-verkonhallinta

SNMP -verkonhallinnan peruskonsepti koostuu neljästä elementistä:

- hallinta-asema
- hallinta-agentti
- hallintatietokanta
- verkonhallintaprotokolla.

Hallinta-asema on laite johon verkon laitteiden hallinta on keskitetty, eli laite, jonka kautta verkkoa hallinnoidaan. Aseman tärkeimpiin ominaisuuksiin kuuluvat hallintaohjelmat, joita voi olla useita. Verkonhallintaohjelmilla valvotaan verkkoa, tehdään analyysejä sekä autetaan verkkoa toipumaan virheistä. Hallinta-asema tarvitsee myös rajapinnan, jonka avulla ylläpitäjä valvoo ja tarvittaessa ohjaa verkkoa. Kaikki verkosta kerätty informaatio tallennetaan hallinta-aseman ylläpitämään hallintatietokantaan, joka yleisesti on MIB. Hallinta-agenttia käsitellään tarkemmin kappaleessa 4.4 (Hautaniemi. 1994.)

Yhteys hallinta-asemasta agentille on toteutettu verkonhallintaprotokollalla, joka tässä tapauksessa on SNMP -protokolla. SNMP -protokolla määrää asemien tavan kommunikoida ja mahdollistaa arvojen toimittamisen verkon yli. Standardi ei määrittele kuinka montaa agenttia yksi hallinta-asema pystyy käsittelemään, mutta toimintojen pysyessä yksinkertaisina voi agenttien lukumäärä olla satoja. (Hautaniemi. 1994.)

3.6 Tietoliikenneverkkojen kehitys

Tietoliikenneverkot kehittyvät valtavaa vauhtia. IPv6 on lyömässä itseään läpi, uusi tekniikka mahdollistaa uusia tietoturva uhkia. Kiinan räjähdysmäisesti kasvava talous, osana tietoteknistä kehitystä, on valtava haaste kehittää verkon valvontaa samaa vauhtia. Tiedonmäärän valtava lisääntyminen ja uudet verkkosovellutukset pakottavat yhtiöt tarjoamaan yhä nopeampia laajakaistoja. Video- ja tv -lähetykset ovat siirtymässä tietoliikenneverkkoon (Dong. 2004.)

4 VERKONHALLINNAN OSA-ALUEET

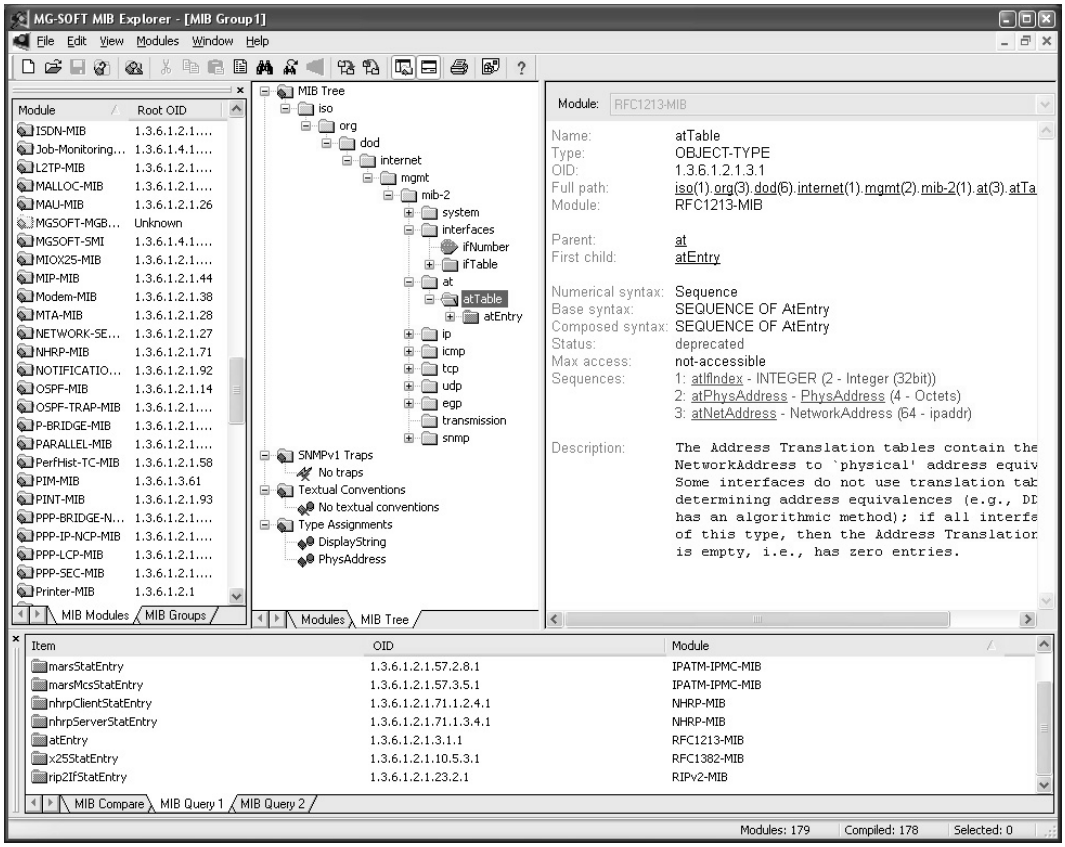
4.1 TCP/IP -verkonhallinta

TCP/IP -verkonhallinta koostuu kolmesta osasta:

- Management Information Base (MIB). MIB on tietokanta jossa määritellään mitä muuttujia verkkolaitteesta ylläpidetään. Tietokantaan voidaan kohdistaa kyselyitä ja selvittää SNMP protokollan avulla verkkolaitteen tila ja tietoja.
- Structure of Management Information (SMI). MIB tietokanta ei voi olla järjestykseltään satunnainen, jotta tietokanta olisi tehokas. SMI määritteleekin MIB- tietokannan rakenteen ja samalla ylläpitää tunnistusjärjestelmää, jota käytetään viittaamaan tietokannan muuttujiin.
- Simple Network Management Protocol (SNMP). Verkonhallinta protokolla, jolla laitteista noudetaan informaatiota valvontajärjestelmään. RFC (request For Commnets) 1157:ssä määritelty protokolla, jota käsitellään tarkemmin tämän työn kappaleessa kolme.

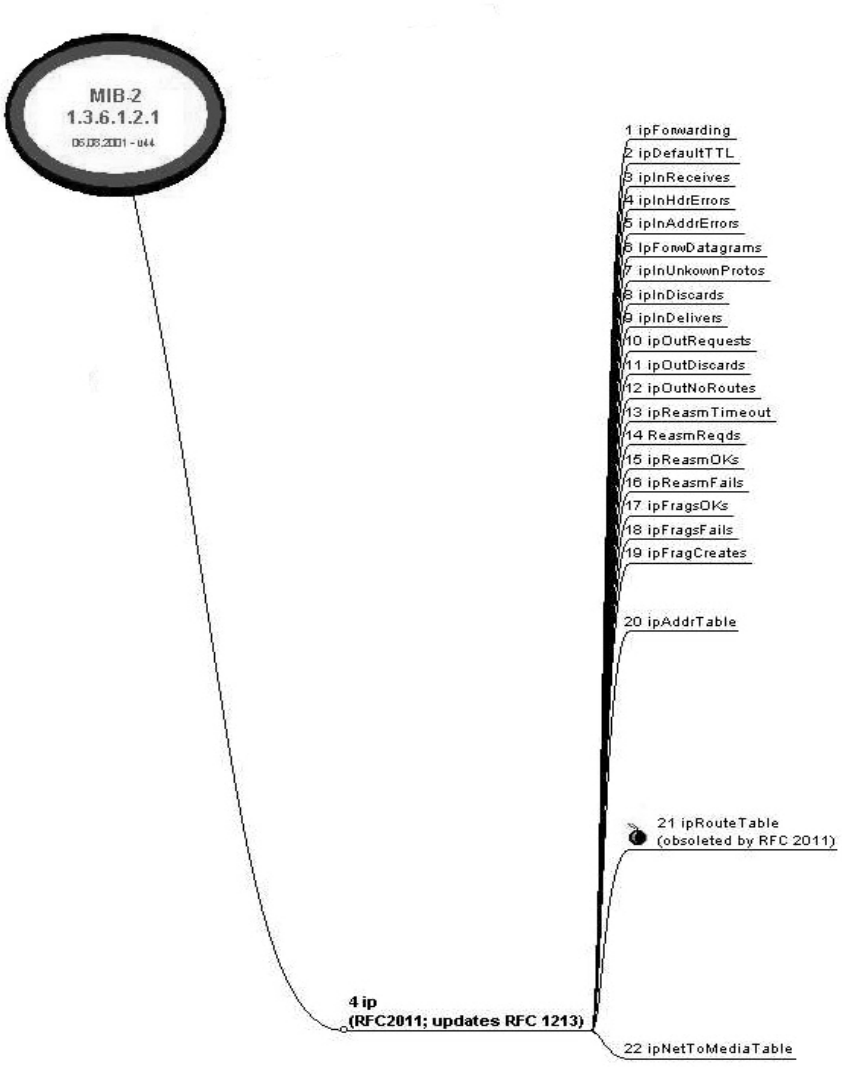
4.2 MIB

Management Information Base I on määritetty RFC -dokumentissa 1156 ja MIB II on määritetty RFC -dokumentissa 1213. MIB on puumallinen tietokanta johon tallennetaan valvottavan kohteen tietoja. Valvottavia kohteita nimitetään objekteiksi. Objektien tietoja voivat olla mm. asetukset, portti, hälytys ja protokollatilastot. MIB on rakenteeltaan standardoitu, joten tietty objekti löytyy loogisesta puurakenteesta aina samasta paikasta. Puumainen tietokanta voi olla hieman hankala luettava nimien perusteella. Tietokannan graafiseen selailuun on kehitetty muutamia ohjelmia, joiden avulla puurakenteesta saa paremman käsityksen. Yksi ohjelmista on MG-SOFTin kehittämä ”MIB Explorer”, joka on ladattavissa yrityksen kotisivuilta. KUVIOSSA 4 on esitetty näkymä ohjelmasta. (MG-SOFT. 2008.)



KUVIO 4. Näkymä MG SOFT MIB Explorer – ohjelmasta. (MG SOFT)

MIB:n sisältämät objektit, eli tieto on määritelty SMI:n standardin määritysten mukaisesti, joka samalla määrittää datatyypit joita MIB voi käyttää. MIB -rakenteen objektit ovat suurimmaksi osaksi laskureita, joilla on numeerinen arvo. Esimerkkinä voidaan mainita tcpOutSegs objekti, joka ilmaisee lähetettyjen segmenttien määrän siitä alkaen kun valvontaohjelmisto on käynnistetty. Valvontaohjelmisto pyytää ipOutRequests -tietoja agentilta MIB osoitteella .iso.org.dot.internet.mgnt.mib.ip.ipOutRequests eli käytännössä viitataan numeeriseen osoitteeseen 1.3.6.1.2.4.10. KUVIOSSA 5 on esitetty MIB-II puun IP –haara. (Doh. 2003).



KUVIO 5. MIB -II tietokannan rakenteen osa. (Doh. 2003 muokattu)

4.3 SMI

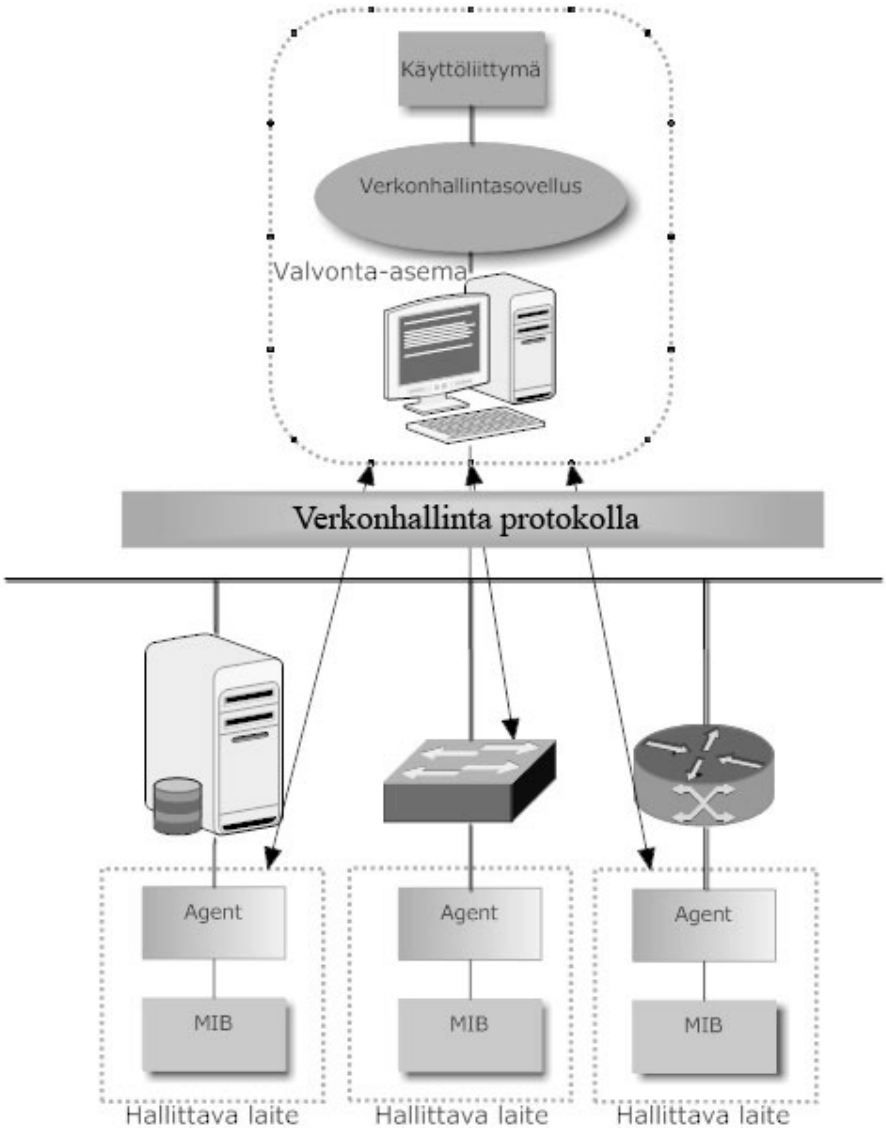
SMI on joukko määrityksiä, jotka koskevat MIB tietokannan sisältämiä olioita. Hallittavilla olioilla on oltava nimi, rakenne ja koodaus. Nimitiedon tulee määritellä kuvaavasti objektin tietoja juuressa. Objektin tyyppi, joka voi olla kokonaisluku tai merkkijono, on määritelty rakenne osassa. Koodaus määrittelee informaation muotoilun ennen verkkoon lähettämistä. (RFC1155. 1990.)

SMI on tärkeä osa MIB tietokantaa, sillä ilman määrityksiä tietokanta olisi hyödytön. SMI kertoo kuinka, jokin tietokannan osa tulee olla määritettynä MIB tietokannassa. SMI määritysten johdosta, tietokanta on kaikille sama ja tulkinnan varaa ei ole.

4.4 Agentti

Jotta verkon laitteita voidaan hallinnoida, tarvitsee myös hallittavaan laitteeseen asentaa agentti, jonka kanssa hallinta-asema keskustelee. Agentti asennetaan tavallisesti tärkeimpiin verkon laitteisiin. Agentti voidaan asentaa työasemiin, kytkimiin ja reitittimiin. Agentin merkitys verkonhallinnalle on erittäin keskeinen. Agentin tehtävä on kerätä hallintaan liittyvää tietoa verkkosegmentin alueella ja tallentaa keräämänsä tieto tietokantaan. Agentin tietokannan on taas tarkoitus palvella hallintatyöasemaa, joka suorittaa kyselyitä tietokantaan keskittäen tietoa. Agenttiin voidaan myös ohjelmoida hälytyksiä, jolloin agentti ottaa itse yhteyttä verkonhallintatyöasemaa. Verkonhallinnan hälytykset ovat ennalta määritettyjen ehtojen täyttymistä. (Happonen. 2005)

Verkon laajuuden kasvaessa voi agentti toimia myös proxy-tilassa, jonka kautta muut agentit välittävät tietojaan hallintakoneelle. Proxy-toiminnosta on hyötyä kun käytössä on monia eri standardeja joiden tulee keskustella keskenään. Proxy-tilalla voidaan myös pienentää hallintaviestien aiheuttamaa verkkokuormaa, mikäli käytössä on hitaampia verkkoyhteyksiä. (Sinkkonen. 2007)



KUVIO 6. Vuorovaikutusmalli valvonta-aseman ja laitteiden välillä (Sinkkonen. 2007 muokattu)

KUVIOSSA 6 on esitettynä verkonhallintaprotokollaa hyödyntävä verkkokokonaisuus. Valvonta-asema lukee lähettämällä lukupyyntöjä, hallittavista laitteista tietoja, jotka laitteiden agentit ovat tallentaneet MIB tietokantaan. Tietojen avulla, ylläpitäjän on mahdollista valvoa verkon laitteiden toimintaa yhdestä paikasta. (Sinkkonen. 2007.)

4.5 Verkonhallinnan toimenpiteet

Verkonhallinnan tähdätessä automaattiseen suoritukseen, ei pelkkä tiedon kerääminen riitä vaan kerätyn tiedon perusteella tulee pystyä myös toimimaan. Toimintamalleja voi olla useita riippuen viasta, ajankohdasta ja laitteesta. Vikasietoisessa verkossa esimerkiksi kytkimen uudestaan käynnistys saattaa riittää korjaamaan vikailmoituksen tietystä portista. Tosin tätä voitaneen hyödyntää ainoastaan yöaikaan koska päivällä verkon osittainen kaatuminen saattaisi aiheuttaa suurempia ongelmia. Käytännössä yleisin malli on sähköposti-ilmoitus viasta. Tärkeimmistä palveluista voidaan lähettää tekstiviesti, jolla pyritään hakemaan ylläpitäjän välitöntä huomiota. (Feldman. 1999.)

Tiedotus viasta tulee myös toistaa sopivin väliajoin. Toisto korostuu etenkin usean ylläpitäjän ympäristöissä, jossa vastuu verkosta jakaantuu monelle. Sopivalla väliajalla haetaan käyttömukavuutta ja käytännöllisyyttä. Jo muutaman tunnin viive toiseen ilmoitukseen antaa ylläpidolle aikaa keskittyä vian korjaamiseen ja toiminnan tarkastukseen. Ilmoitusten väli ei myöskään saa olla liian suuri, jottei asia pääse unohtumaan. (Feldman. 1999.)

Tärkeintä toimenpiteissä, jotka koskevat ylläpitäjää tai henkilöä, joka tarkastaa tehdyt ilmoitukset, on pitää huolta että turhia ilmoituksia tulee mahdollisimman vähän. Mitättömistä asioista tulevat ilmoitukset eivät auta ketään, vaan kasvattavat työtaakkaa. (Feldman. 1999.)

5 GFI NSM ESITTELY JA ASENNUS

5.1 GFI NSM

GFI NSM (Network Server Monitor) on Windows-pohjainen verkonvalvonta ja -hallinta ohjelmisto. Ohjelma on kehitetty huomaamaan ongelmat, ennen kuin käyttäjät ehtivät ongelmia huomata. Ohjelman avulla ylläpitäjän on mahdollista suorittaa tietyille ongelmille automatisoituja korjaustoimenpiteitä. Vaativammissa ongelmissa ohjelma lähettää hälytyksen ylläpitäjälle. Hälytyksillä pyritään minimoimaan palveluiden saatavuuden puutteesta johtuvat ongelmat ja tappiot.

NSM ohjelmassa on monia suoraan mahdollistettuja tarkastuksia joita ovat mm.

- Muutamat ohjelmistot ovat suoraan tuettuja. Ohjelmistoja ovat Exchange 2000/2003, MS SQL (Microsoft Structured Query Language), Windows järjestelmä loki, Oracle ja ODBS (Open Database Connectivity) tietokannat.

- Laitteiden resurssit kuten muistin, kovalevyn prosessorin käyttöaste sekä tiedostojen sisällön tarkastus.

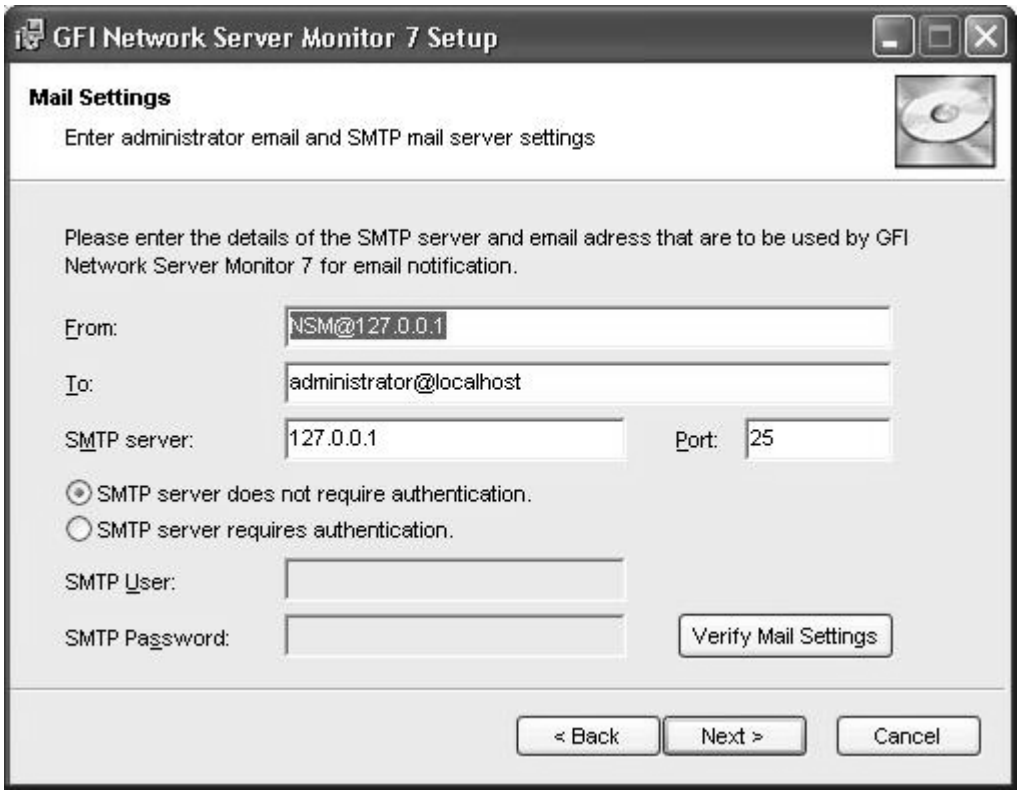
- Useat verkon palveluista ovat myös valvonnan piiriin määritettävissä suoraan. Esimerkiksi FTP, HTTP (Hypertext Transfer Protocol) ja AD (Active Directory)

Laitteistovaatimuksia ei NSM ohjelman asennukselle ole ilmoitettu. Rajoittavina tekijöinä toimivat tuetut käyttöjärjestelmät joita ovat Windows 2000 (SP4 tai uudempi), Server 2003 tai Windows XP. Lisäksi asennettuna täytyy olla .NET Framework 1.1 ja käytettävän internet selaimen täytyy tukea Windows Script Host 5.5-Script-tuki löytyy kaikista uusimmista selaimista aina IE (Internet Explorer) 6:sta lähtien. Erikseen asennettuna tuen saa myös IE 5.5 versiolle. (GFI NSM. 2008.)

5.2 GFI NSM -asennus

GFI N.S.M -ohjelman ollessa maksullinen, on työssä asennettu ohjelman evaluation (koekäyttöön tarkoitettu) versio. Versiota saa koekäyttää ilmaiseksi kymmenen päivää, jonka jälkeen vaaditaan rekisteröinti ja lisenssin hankinta, mikäli käyttöä halutaan jatkaa. Asennettu versio on uusin 7.0 (Build 20070803, tarkistettu 5.3.2008) ja on ladattavissa yrityksen kotisivuilta.

Asennus aloitetaan käynnistämällä ladattu ohjelmatiedosto. Asennus on Windows ohjelmille tyypillisen johdonmukainen, selostaen kaikki vaiheet. Johdonmukaisuuden ja ohjeiden takia asennusta voidaan pitää helppona. Asennus aloittaa suorituksen hyväksyttämällä käyttäjällä lisenssisopimusehdot. Seuraavaksi kysytäänkin jo käyttäjän nimeä, yritystä ja lisenssiavainta. Ohjelman asennuksessa voidaan suoraan valita suoritetaanko ohjelma paikallisten tunnusten alla vai järjestelmäsovelluksena (Local System Account). Tähän käytäntöön ei tässä työssä puututa, vaan jätetään kohta järjestelmä riippuvaiseksi muuttujaksi. Työn asennuksessa valittiin järjestelmäsovellus-muoto. Seuraavaksi ohjelma haluaa tietoa järjestelmän ylläpitäjän yhteyksistä, sekä SMTP (Simple Mail Transfer Protocol) palvelimen osoitteesta. Tietojen kysyntä on esitetty KUVIOSSA 8. Asetusten täyttämisen jälkeen asetukset voidaan testata ”Verify Mail Settings” painikkeella. Tämä on syytä tehdä, jotta jatkossa ilmenevät virheilmoitukset välittyvät oikein. (GFI NSM. 2008.)



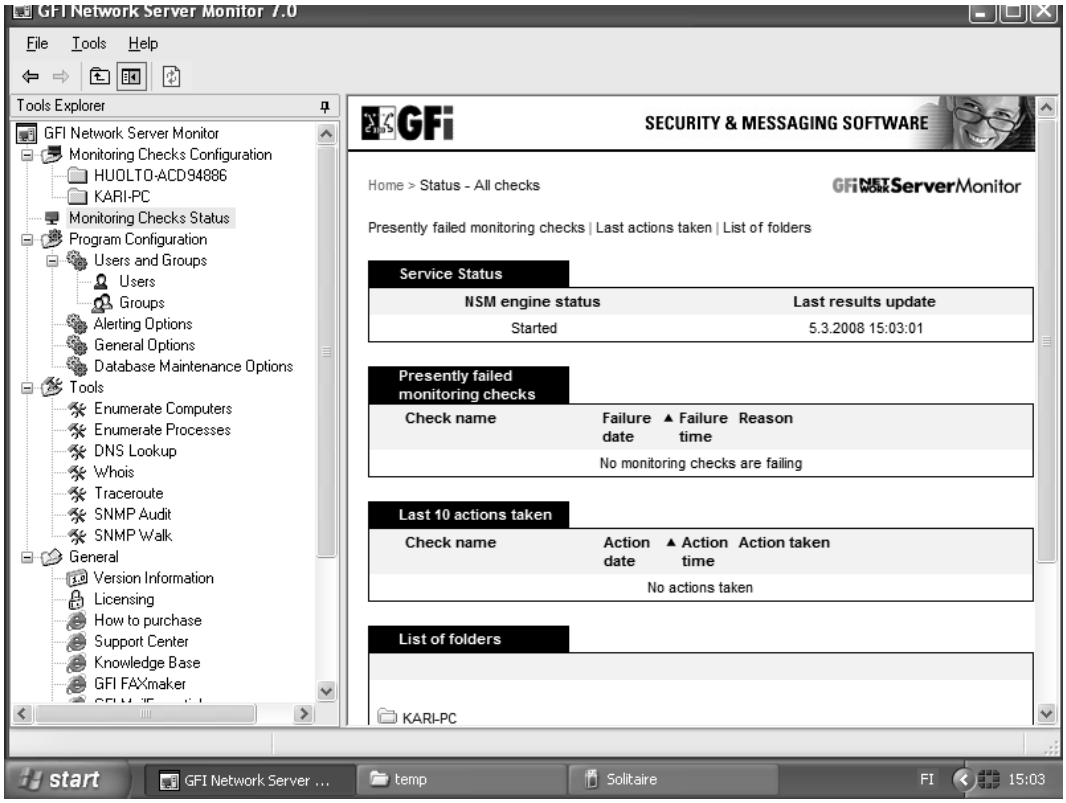
KUVIO 8 NSM ohjelman SMTP asetukset

Seuraavaksi valitaan ohjelman käyttöön tuleva tietokanta. Vaihtoehtoja ovat Microsoft Access ja Microsft SQL Server 7 tai uudempi/MSDE (Microsoft Desktop Engine). Suosituksena suuriin verkkoihin on täysiverinen SQL-tietokanta, mutta pienempiin verkkoihin Access tietokantakin riittää mainiosti. Tietokannan hyväksynnän jälkeen päästään valitsemaan ohjelman asennus kansiota, jota seuraa asennuksen tietojen hyväksyntä. Asetusten tarkistusten jälkeen annetaan hyväksyntä ja ohjelma aloittaa asennuksen. Asennus kestää alle minuutin ja päättyy ikkunaan, josta voidaan siirtyä suoraan itse ohjelmaan.

5.3 GFI NSM-asetukset

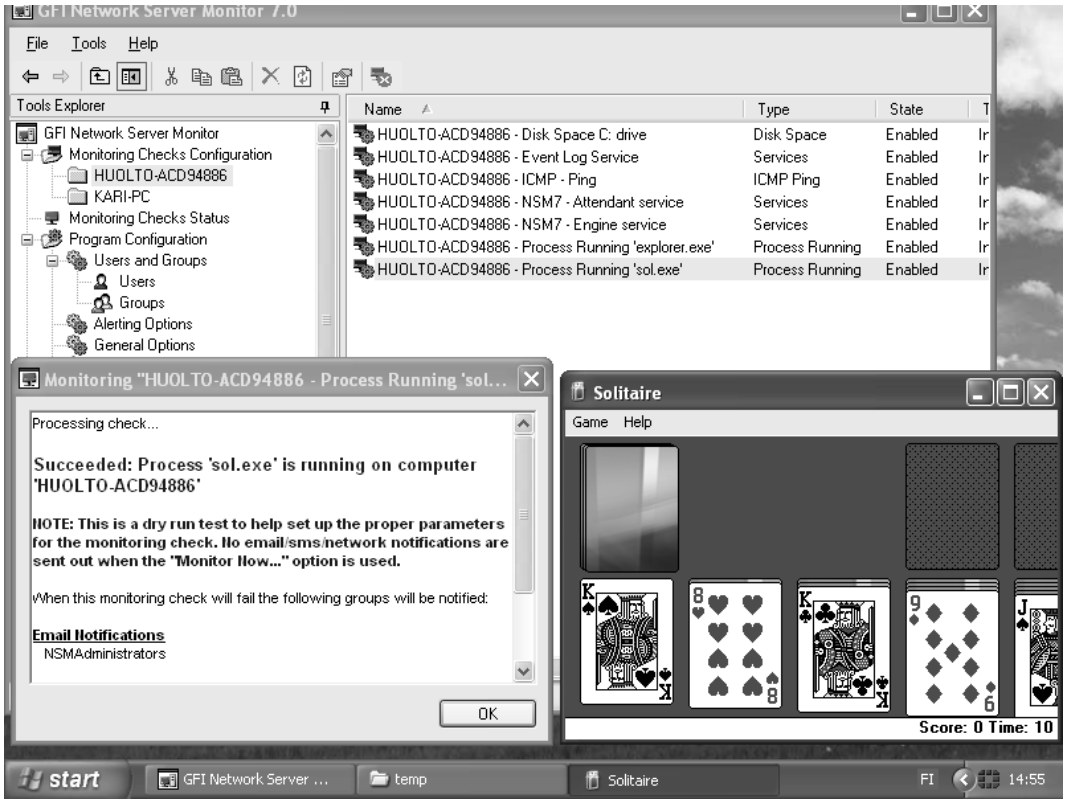
Käynnistyttyään ohjelma tarjoaa oletuksena pikaista asetusten määrittelyä asennus velhon avulla. Velhon avulla määritellään valvottavasta kohteesta perustiedot, kuten käyttöjärjestelmä, mahdolliset domain- tai verkkopalvelut ja tarjolla on muutama valmiiksi määritetty ohjelmakin. Viimeisenä osiona valitaan verkon koneista, joko selaten tai IP-osoitteen perusteella, kyseinen kone/koneet, jota ase-

tukset koskivat ja lisätään kohde tarkasteltavien koneiden listalle. Asetusten hyväksynnän jälkeen ohjelma käynnistyy KUVION 9 näköiseen käyttöliittymään.



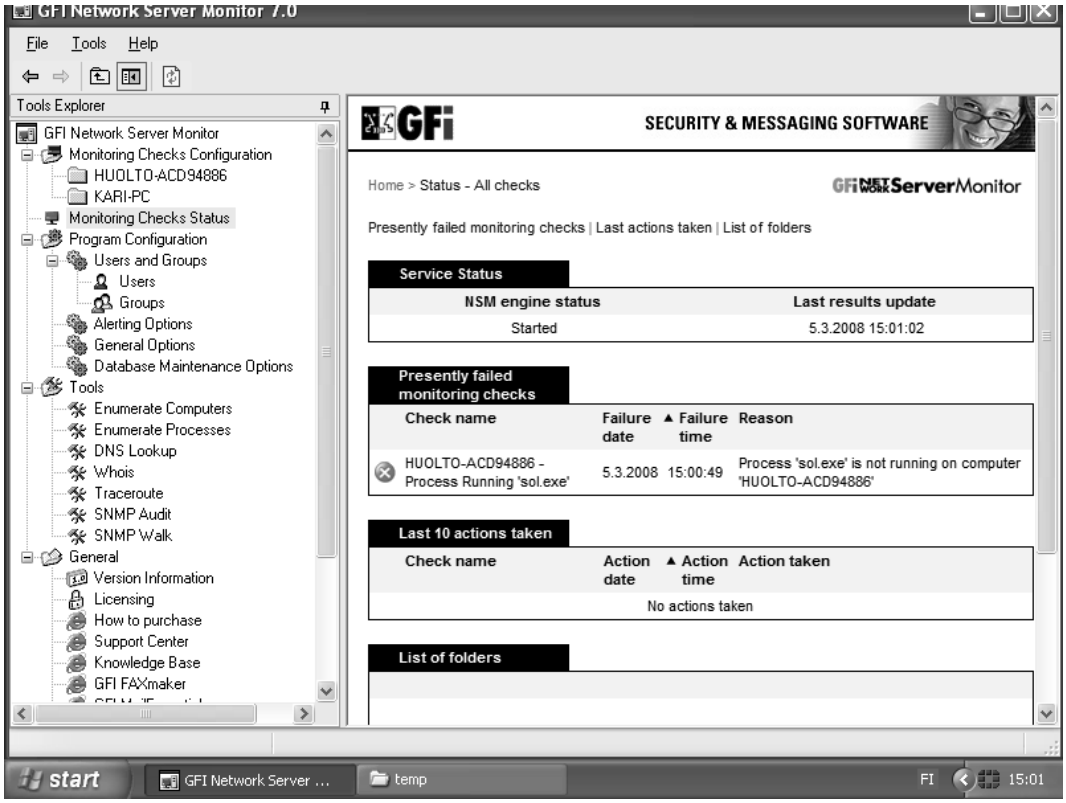
KUVIO 9. GFI NSM aloitusnäkymä

Tehtävä, jota varten GFI NSM ohjelma on suunniteltu, on tiedottaminen verkon häiriöistä. Tämä ominaisuus ei toimi, jos ohjelman asetukset, koskien ylläpitäjän tietoja tai hälytysasetukset, ovat puutteelliset. Siksi onkin erityisen tärkeää varmistaa sähköpostipalvelimen ja muiden käytettävien hälytysreittien toiminta ennen kuin ohjelman oletetaan toimivan oikein. Helpoin ja varmin tapa on luoda tarkastuskohteeksi prosessi, joka voidaan sammuttaa toiminnon aiheuttamatta ongelmia. Esimerkkitapaukseksi käynnistettiin tarkasteltavalle koneelle pasianssi eli ”sol.exe” -ohjelma. Lisäksi luotiin tarkastus, joka tarkastaa että koneella pyörii palvelu nimeltä ”sol.exe”. GFI NSM:n toiminta tarkastettiin suorittamalla manuaalinen testi, joka löysi halutun prosessin koneelta. Tämä voidaan todeta KUVIOSTA 10.



KUVIO 10. GFI löytää sol.exe prosessin

Seuraavaksi ohjelma ”sol.exe” suljettiin ja odotettiin automaattisen tarkastuksen huomaavan ohjelman puuttuvan. NSM huomasi ”sol.exe” -prosessin sulkeutuneen ja teki siitä virheraportin, joka voidaan todeta KUVIOSTA 11. Vähintään yhtä tärkeää kuin virheen havainnointi, on virheen korjautumisen huomiointi. Tämä saatettiin testata käynnistämällä ”sol.exe” -prosessi jälleen, jolloin oletusajan kuluttua (n. 2 min) ohjelma havaitsi prosessin ja poisti virheilmoituksen. Myös tilanteen korjautumisesta voidaan automatisoida ilmoitus samalla tavalla kuin virheen ilmenemisestä.



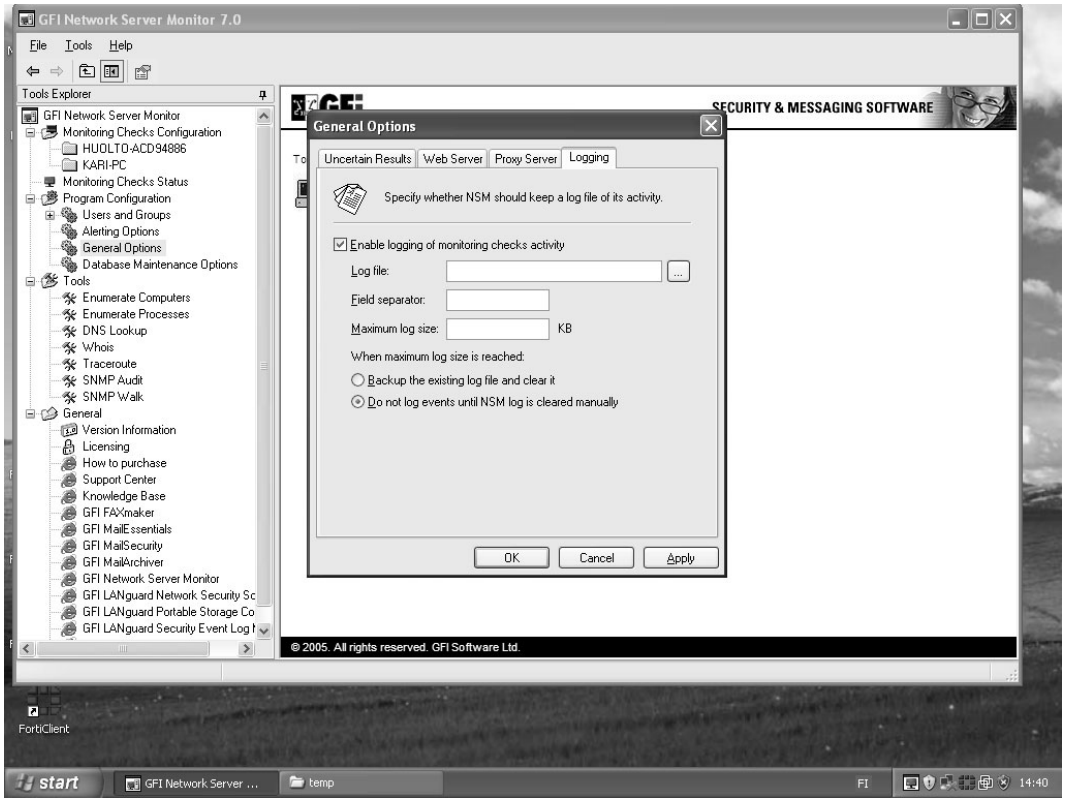
KUVIO 11. Prosessi sol.exe on suljettu ja NSM on huomannut puutteen.

Ohjelman suorittamista tarkastuksista voidaan määrittää, tiedottaako ohjelma virheestä kerran vai määrätyn ajan välein. Etenkin vähemmän akuuteissa ongelmissa, on hyvä saada aika-ajoin muistutus ongelmasta, jottei ongelma pääse unohtumaan.

5.4 GFI NSM -käyttöliittymä

Ensivaikutelma ohjelmasta on aavistuksen sekainen. Laajahko valikko on nähtävissä ruudun vasemmassa reunassa ja oikeanpuoleinen ruutu kertoo valikosta valitun kohdan tietoja. Ohjelman käyttöön tottuu kuitenkin nopeasti ja valikkokokonaisuus alkaa hahmottua selkeäksi toimintaympäristöksi. Valikon kautta on nopeasti valittavissa toimintoja, joilla voi mm. tarkistaa etäkoneella pyörivät palvelut, kartoittaa verkossa olevat koneet ja traceroute-toiminnolla jopa seurata IP-verkon reitin toisen koneen luokse. Useat graafiset yhteneväisyydet Windows-sovelluksiin, kuten Office-tuoteperheeseen, luovat käyttöliittymästä tutun ja helppokäyttöisen.

Ohjelmasta näkyy kaupallisuus selvästi. Näkyvän valikon suurimman osan täyttävät valmistajan toisten ohjelmien mainos-linkit, joiden olisi suonut olla jossain muualla. Tärkeintä on kuitenkin, ettei yleisnäkymää tilanteesta ole unohdettu. Kuten KUVIOSSA 11 näkyy, voidaan verkon yleistilannetta pitää helposti silmällä. Verkon virheistä tulee selvät ilmoitukset kootusti samaan paikkaan ohjelmaa. Tämän lisäksi voidaan mahdollistaa pitkäaikaisempi lokin luonti tarkastusten tiloista, tämä vaihtoehto on esitetty KUVIOSSA 12



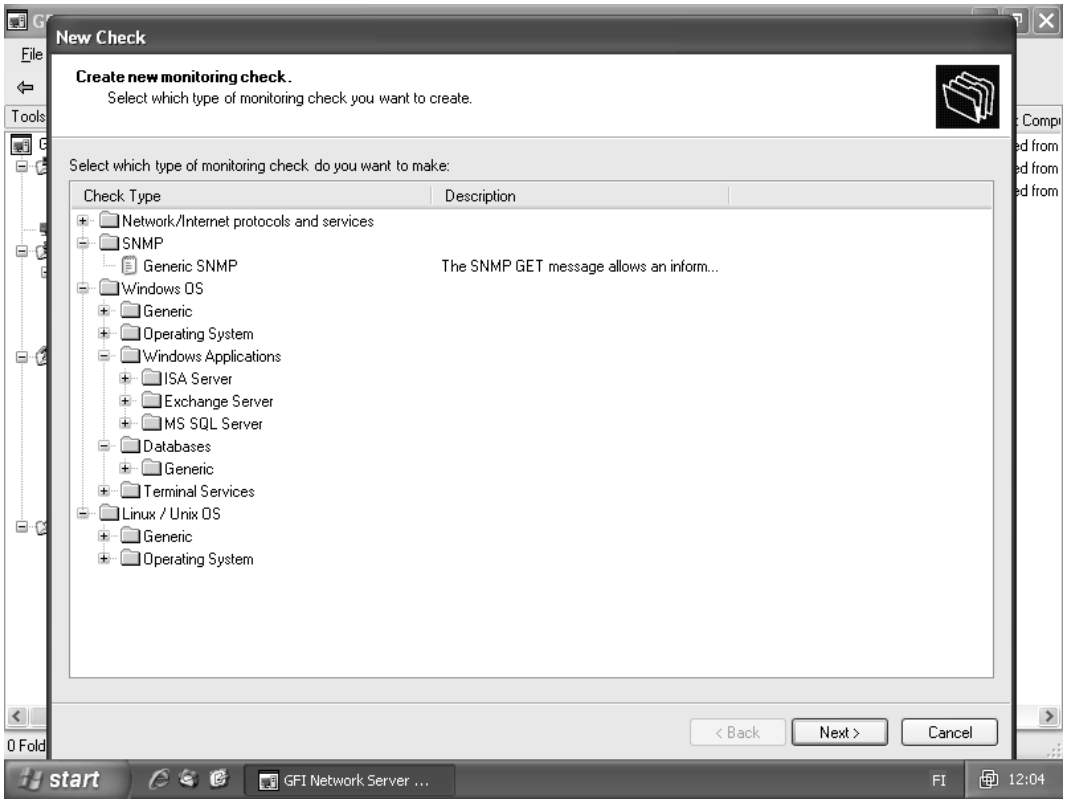
KUVIO 12. GFI NSM ohjelman tarjoama valinta tarkemman lokin asetuksista

Käyttäjien kannalta helpoin virheiden tarkastuspaikka on verkkosivu, jonka ohjelma tekee oletuksena porttiin 11695. Osoitteesta http://NSM-koneen-nimi:11695 pääsee suoraan tarkastamaan virhetietoja. GFI NSM ei tarjoa lainkaan asetuksia verkkosivujen kautta, siksi sivuille ei myöskään vaadita tunnistautumista. Koneen nimen ja porttiosoitteen tietävät henkilöt pääsevät tarkistamaan tilanteen halutessaan.

6 GFI NSM-TARKASTUKSET

6.1 GFI NSM - valmiit määritykset

GFI NSM sisältää runsaasti valmiita tarkastusmäärityksiä, jotka on jaoteltu neljään pääkategoriaan. Kategorioita ovat Network / Internet protcols and services, SNMP, Windows OS ja Linux / Unix OS. Pääkategorioiden alta paljastuu useita eri tarkastuksia, jotka voidaan helposti lisätä kohdetyöaseman tai -palvelimen tarkastuslistalle. KUVIOSTA 13 voimme todeta tarkastusten kansiorakenteen.



KUVIO 13. GFI NSM tarkastusten kansio näkymä

Network / Internet protocols and services -valikon alta löytyy mm. HTTP / HTTPS (HTTP Secure), FTP, IMAP (Internet Message Access Protocol), NTP (Network Time Protocol), POP3 (Post Office Protocol version 3) ja SMTP-tarkastuksia. Tarkastuksilla voidaan seurata mm. postipalvelimen ja aikapalvelun

toimintaa. SNMP-valikon alta löytyy valinta Generic SNMP, joka käsittää kaikki SNMP-protokollan sisältämät tarkastelu- ja hallintakohdat.

Seuraava ja laajin valikko, Windows OS, sisältää viisi alavalikkoa, jotka ovat Generic, Operating System, Windows Applications, Databases ja Terminal Services. Generic-valikko käsittää enemmän itse muokattavia tarkastuksia, joten niihin palataan seuraavassa kappaleessa. Operating System-valikko käsittää normaaleja koneen ylläpidollisia tarkastuksia kuten tiedoston olemassa oloa, levytilaa, prosessorin käyttöastetta, kansion kokoa ja active directoryn rakenne kyselyitä. Windows Applications – valikko tarjoaa tarkastukset ISA, Exchange ja MS SQL-palvelimille. Databases-valikko tarjoaa tarkastuspohjan ODBC tietokanta kyselyille. Viimeisenä kohtana oleva Terminal Services -valikko tarjoaa tarkastukset, joilla voidaan varmistaa terminaalipalvelimen käytettävyys niin portti, kuin kirjautumis- tasollakin.

Linux / Unix OS -valikko tarjoaa, nimensä mukaisesti, tarkastuksia Linux ja Unix käyttöjärjestelmille. Tarkastusten määrä on huomattavasti suppeampi, kuin Windows puolella, mutta kaikki perustarkastukset kuten mm. levytilan, suoritin kuorman, tiedostokoon ja prosessien toimimisen tarkastukset on katettu. Linux puolelle on jätetty mahdollisuus omien SSH (Secure Shell) tarkastusten suorittamiseen, joka käytännössä mahdollistaa erittäin laajojen ja monipuolisten tarkastusten tekemisen ja suorittamisen.

NSM ohjelman tarkastukset perustuvat tunnuksiin, eli valvottaville koneille ei tarvitse asentaa mitään. Palveluita päästään valvomaan käyttäjätunnuksilla, joka mahdollistaa suurien konemäärien helpon valvonnan. Tällä saavutetaan etua suurissa ympäristöissä, joissa etä–agentin asentaminen kaikille koneille olisi mahdotonta.

Tarkastusten varmuuskopiointi hoituu helposti suoraan *File* valikon alta *Export Configurations***.** Asetusten varmuuskopioinnilla on suuri merkitys kun tarkastuskohteita alkaa olla suuria määriä. Vielä muutaman koneen perus tarkistukset voidaan helposti palauttaa asettamalla tarkistukset uudestaan. Kuitenkin kun kysees-

sä on kymmenien tai satojen valvottavien koneiden asetukset, on helpompaa palauttaa kaikki asetukset yksittäisestä tiedostosta, kuin lähteä syöttämään tarkastusten tietoja uudestaan.

6.2 GFI NSM -skriptit

Vaikka GFI NSM tarjoaa valtavan määrän valmiita tarkastuksia, on valinnoissa varmasti myös puutteita. Etenkin keskisuurissa yrityksissä on käytössä monia pienehköjen ohjelmatalojen ohjelmoimia laskutus, toiminnanohjaus tai palkan hallinta järjestelmiä. Nämä ohjelmat, etenkin tuotannonohjausjärjestelmät, saattavat toimia normaaleista toimintatavoista poiketen ja vaatia niitä varten räätälöityjä tarkastuksia.

Näitä puutteita varten on ohjelmassa jätetty valittaviksi, sekä Windows että Linux puolelle, mahdollisuus käyttää omia tarkastuksia erilaisten scriptien tai muiden ohjelmoitujen tarkisteiden avulla. Windows puolella on mahdollisuus käyttää tarkastuksessa VBS (Visual Basic Scripting) -koodeja, joilla voidaan toteuttaa lähes mitä vain. VBS koodit soveltuvat tarvittaessa vaikka kokonaisen ohjelman poistamiseen ja uudestaan asentamiseen vaatimatta käyttäjän toimenpiteitä.

Linux puolella käytössä on SSH-scriptit, joiden toimintamalli on myös erittäin laaja. Omien tarkastusten ominaisuuksilla, tarjotaan ylläpitäjälle mahdollisuus valvoa kaikkea tarvittavaa poissulkematta erikoisuuksia. Sekä Windows, että Linux puolella, on toteutettavissa myös terminaalin puolella suoritettavia komentoja. Komentojono suoritteet tarjoavat pääsyn kaikkiin komentojonon tarjoamiin mahdollisuuksiin, joilla voidaan mm. verrata tiedostoja, tarkastaa IP-tietoja, formatoida levykkeitä ja tarkastaa milloin tiedostoa on muokattu.

6.3 GFI NSM -toimenpiteet

Hyväkin valvontaohjelma on hyödytön, jos ohjelman suorittamiin tarkastusraportteihin ei puututa mitenkään. Normaalioloissa epäonnistuneen tarkastuksen aiheuttamaan hälytykseen reagoi oletuksena ylläpitäjä, ennen reagointia pitää tieto tapahtuneesta saada ylläpitäjälle. GFI tarjoaa oletuksena kolme perustapaa tiedottaa ylläpitäjää, jotka ovat sähköposti, tekstiviesti ja verkkoviesti. Sähköpostiviesti vaatii luonnollisesti toimivan sähköpostipalvelimen, tarvittavine määrityksineen. Tekstiviestihälytys vaatii toimivan yhdyskäytävän, dataverkosta puhelinverkkoon. Verkkoviesti toimii palvelimen verkon alueella ja soveltuu hyvin käyttäjiä koskevien tiedotusten tai ongelmatiedotteiden välitykseen. Kun ylläpitäjää on tiedotettu ongelmasta alkaa ongelman korjauksen seuraava vaihe, syynselvitys ja korjaavat toimenpiteet.

Tiedostetuissa ja toistuvissa virheissä voidaan tukeutua ohjelman tarjoamiin työkaluihin, joilla saadaan automaattisesti suoritettua komentoja ja scriptejä kohdekoneella. Komennoilla on esimerkiksi mahdollista käynnistää uudestaan jokin kaatunut palvelu. Toimenpiteillä mahdollistetaan nopea reagointi toistuvaan ongelmaan ja tarjotaan ylläpidolle mahdollisuus selvittää ongelman todellista syytä. Jokaiseen tapaukseen ei voi luoda valmista toiminta mallia, sillä eihän ohjelma välttämättä kaadu aina samasta syystä.

GFI NSM ohjelmalla suoritettujen tarkastusten käytön ei havaittu vaikuttavan valvottujen palvelinten toimintaan. Havainnot perustuvat palvelimen prosessori- ja muistikuorman seuraamiseen valvontojen toiminnassa.

7 NAGIOS ESITTELY JA ASENNUS

7.1 Nagios

Nagios on verkonvalvontaan ja -hallintaan suunniteltu ohjelma, jonka tarkoitus on tiedottaa ylläpitäjälle verkon ongelmatilanteista. Ohjelma perustuu avoimeen lähdekoodiin ja on suunniteltu toimimaan pääsääntöisesti Linux-käyttöliittymän alla. Nagios toimii kuitenkin myös osan *NIX käyttöliittymien alla, esimerkiksi UNIX. Nagioksen vahvaksi puoleksi voidaan lukea ohjelmiston kuuluminen GPL:n (General Public License) alaisuuteen, eli kuka tahansa saa muokata ja levittää ohjelmistoa. (Nagios. 2008.)

Nagios on rakennettu modulaariseksi ohjelmistoksi, eli pääohjelmaan saa lisättyjä optioita joita kutsutaan ”Plugin” nimellä. Pluginit ovat yleensä ohjelman suorittamia tarkastuksia, mutta myös ohjelman toiminnallisia laajennuksia. Ohjelman pääkehittäjänä tunnetaan henkilö nimeltä Ethan Galstad. Ohjelman perustuessa avoimeen lähdekoodiin on kehityksessä ollut valtavana apuna käyttäjien tuki ja raportointi erilaisista ohjelman toimintahäiriöistä tai - virheistä. Ohjelman lisäoptioiden kehittäjinä mainitaan useita henkilöitä, joista mainittakoon Ton Voon ja Benoit Mortier. (About Nagios. 2008.)

Nagioksen keskeinen idea on keskittää verkkoon liitettyjen laitteiden hallinta, sekä valvoa verkon aktiivilaitteiden toimintaa yhdestä paikasta. Tietokone, jolle Nagios on asennettu, toimii niin sanottuna hallintatyöasemana ja valvottavat kohteet jakautuvat kahteen ryhmään. Ensimmäinen ryhmä on nimeltään Hosts (palvelimet), joilla käsitetään fyysiset laitteet. Toista ryhmää kutsutaan Services (palvelut)-nimellä ja ryhmä käsittää Hosts-laitteissa toimivia ohjelmallisia palveluita kuten SSL (Secure Sockets Layer). Nagios mahdollistaa myös häiriöraportin lähettämisen ylläpitäjälle tai muulle määritetylle henkilölle. Raportista löytyy virheen tiedot, jolloin ylläpitäjä voi ryhtyä tarpeellisiin toimiin. Raportti voidaan lähettää niin sähköpostin kuin tekstiviestin muodossa. (Nagios. 2008.)

Nagios mahdollistaa oletuksena niiden verkon peruspalveluiden valvonnan, jotka ovat seuraavassa listassa:

- SMTP, ICMP, HTTP, SSH, NTP, FTP, DNS, POP (Post Office Protocol), TELNET (TELecommunication NETwork)
- Valvottavista laitteista on mahdollisuus saada resurssi tietoja muistin, levyn ja suorittimen käyttöasteesta. Lisäksi voidaan seurata lokitiedostoja, käyttäjien toimia, varmistuksia, toiminnanohjausta.
- Laitteissa olevista lämpösensoreista on mahdollista lukea esimerkiksi prosessorin ja näytönohjaimen lämpötiloja. (Nagios. 2008.)

Nagioksen ollessa modulaarinen ja vapaasti kehitettävä ohjelma, ovat nuo oletuksena mahdollistetut valvontakohdat vasta alkua. Nagiokseen voidaan helposti lisätä erilaisia, omia tai muiden käyttäjien itse kehittämiä lisäosia, joilla mahdollistuu uusia valvontakohteita. Nagioksen ominaisuuksiin kuuluu myös vikatilanteisiin reagoiminen, esimerkiksi palvelun kaatuminen saadaan korjattua käynnistämällä palvelu uudestaan. (Nagios. 2008.)

Tietoturvallisuus on Nagioksessa otettu huomioon jo käyttäjien valvonnassa. Nagios toimii web-käyttöliittymän päällä ja eri käyttäjille on mahdollista asettaa oikeuksia valvoa eri palveluiden tiloja.

Laitteistovaatimuksiltaan Nagios on kevyt ohjelmisto ja toimiikin fyysisesti mietittynä melkein kaikilla alustoilla, jotka kykenevät toimimaan Ethernet-verkossa. Käyttöjärjestelmä on rajattu Linux ja *NIX puolelle ja lisäksi koneeseen tulee olla asennettuna Web -palvelin jossa suosituksena on Apache. (Nagios. 2008.)

7.2 Nagios-asennus

Tässä työssä Nagios asennetaan VMware server 1.0.4:n päällä toimivaan virtuaalikoneeseen, käyttäen alustana openSUSE käyttöjärjestelmää. Asennuksessa hyödynnetään osittain graafista käyttöliittymää. Graafisena käyttöliittymänä toimii Gnome ja käyttöjärjestelmä on versio 10.3. Käyttöjärjestelmään on ennalta asennettu apache2 ja c/c++ kehityskirjastot. Molemmat lisäykset voitiin asentaa openSUSE:n Yast ohjauskeskuksesta ohjelmistohallinnan kautta.

Asennuksen tarkemmat vaiheet on kuvailtu Liite 1:ssä. Asennus vaatii perustietämystä Linux-käyttöjärjestelmän sekä asennusoperaation kulusta. Itse operaatiosta on ohjeet Nagioksen kotisivuilla.

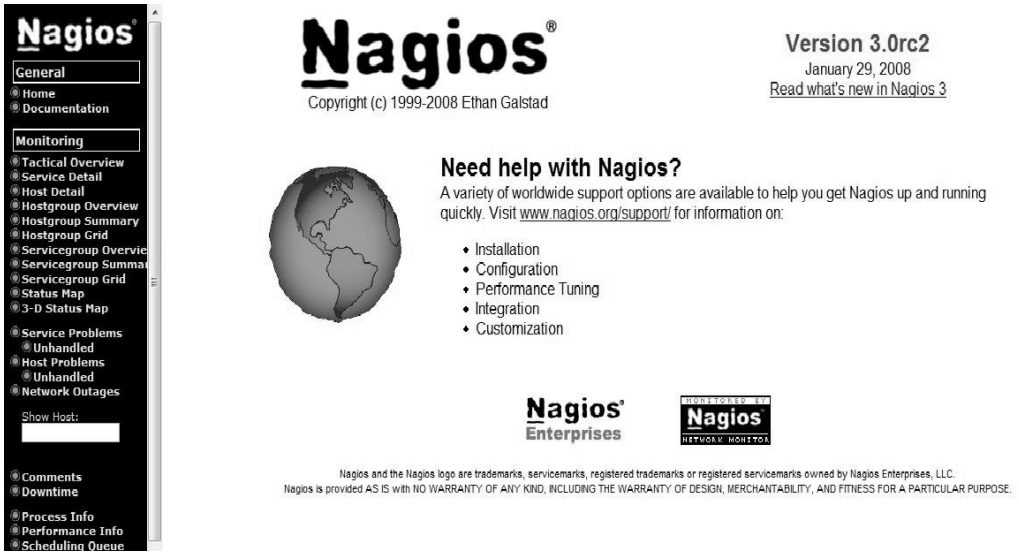
7.3 Nagios-asetukset

Nagioksen varsinaiset asetukset suoritetaan jo asennusvaiheessa. Asennuksen jälkeisiä asetuksia ovat lähinnä tarkastusten käyttöönotto ja tarvittavien agenttien asennus valvottaville kohteille. Nagios perustuu agenttitoimintaan, jolloin valvottavalle kohteelle asennetaan agentti, joka vastaa Nagioksen kyselyihin tai omatoimisesti lähettää tietoja Nagios palvelimelle.

Nagioksen tarkastusten asetukset perustuvat komentokehotteessa tehtäviin asetustiedostojen muokkauksiin. Tärkein tiedosto services.cfg, joka oletuksena asentuu */etc/nagios/* kansioon, toimii linkittävänä tekijänä tarkastusten ja koneiden nimien välillä. Nagioksen tarkastelun piiriin kuuluvien koneiden tiedot ja osoitteet on määritetty *etc/nagios/hosts.cfg* tiedostossa, jonne myös uusien koneiden tiedot tulee lisätä. Muita tärkeitä asetus tiedostoja ovat mm. */etc/nagios/contactgroups.cfg* ja */etc/nagios/contact.cfg*. Tiedostoissa ovat henkilöt ja ryhmät, joille tiedotetaan mahdollisista ongelmista tarkastuksissa.

7.4 Nagios-käyttöliittymä

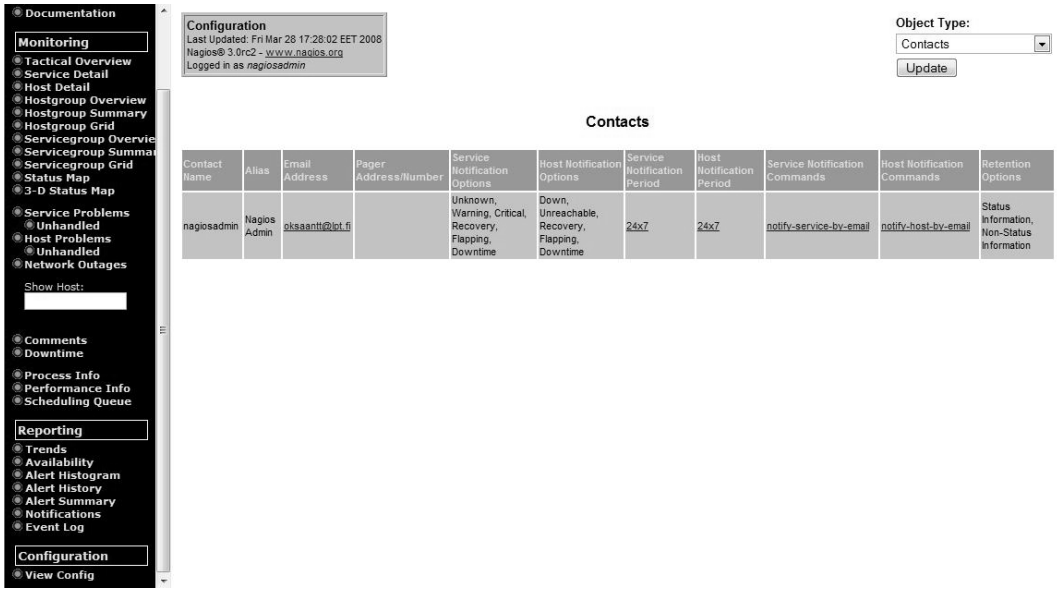
Nagioksen tarkastusten seuranta on helpoiten luettavissa Nagios-koneen verkkosivuilta, jotka toimivat osoitteesta http://nagios-kone/nagios. Sivu vaatii tunnukset joilla tarkastusten tilaa pääsee seuraamaan. Käyttäjätunnus on oletuksena nagiosadmin**,** mutta salasana annetaan Web option asennuksen yhteydessä. KUVIOSSA 14 on esitetty perusnäkymä, joka sivustolta avautuu. Sivuston vasemmassa reunassa on palkki josta voidaan valita haluttuja tarkastelun kohteita. Nagiokseen voi rakentaa myös ryhmityksiä, joiden avulla tiettyjen koneryppäiden valvonta helpottuu.



KUVIO 14. Nagioksen verkkokäyttöliittymän perusnäkymä

Yksittäisen koneen tarkastukset saadaan esille, kun valitaan koneen nimi ”*Host detail*”- välilehdeltä (liite1). Sivulla näkyy perustietoa kyseisen koneen tarkastuksista ja tarkastus tiedoista. ”*Host commands*” kohdan alla on tarjolla muutamia tarkastuksiin liittyviä komentoja kuten tarkastusten päälle ja pois päältä kytkeminen (liite 2). Koneen yksittäisiä tarkastuksia pääsee seuraamaan valitsemalla saman sivun ylälaidasta ”*View Status Detail For This Host*” (liite 3). Näkymä avaa tilannekatsauksen koneen tarkastuksiin. Yksittäisen tarkastuksen tietoihin pääsee valitsemalla kyseisen tarkastuksen nimi. Tiedoista käy ilmi mm. nykytilanne, historia, tarkastusarvojen rajat sekä seuraavan tarkastuksen ajankohta.

Yleisilmeeltään sivusto on selkeä ja informatiivinen. Kaikki on johdonmukaisesti esillä, vaikkakin selkeä kansiorakenne sivun vasemman reunan palkin paikalla olisi hyvä vaihtoehto. Sivuston etusivulla on selkeästi kerrottu mistä voi etsiä tukea ongelmatilanteissa. Nagioksen ylläpidon kannalta tärkein valikko ”*Configuration*” on sijoitettu vasemman reunan palkissa alimmaiseksi. Valikon kautta pääsee tarkastelemaan komentokehotteessa tehtyjen muutosten tuloksia graafisesta näkymästä. Kyseessä on siis asetustiedostojen tarkasteluun tarkoitettu työkalu, jolla voidaan tarkastaa tekstitilassa tehdyt muutokset. KUVIOSSA 15 on esitetty Nagiokseen määritetyn ylläpitäjän tiedot.



KUVIO 15. Nagiokseen määritetyn ylläpitäjän tiedot.

8 NAGIOS-TARKASTUKSET

8.1 Nagios-pluginit

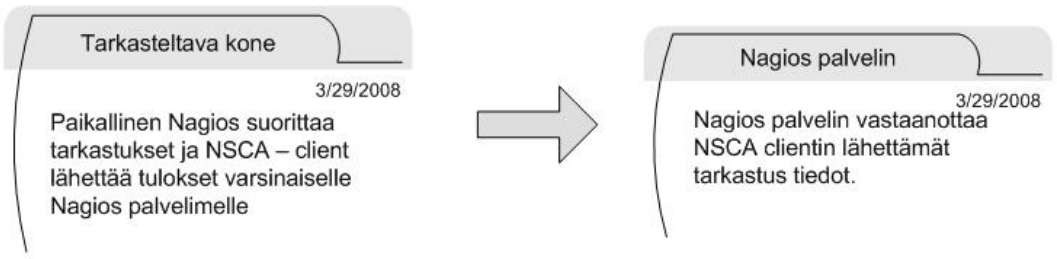
Nagios perustuu ohjelmaan asennettaviin plugin-tarkastuksiin ja on muodoltaan modulaarinen. Ohjelman peruspluginit eli tarkastukset asennettiin jo ohjelman asennuksen yhteydessä, mutta niitä voidaan lisätä myös jälkikäteen. Perus plugin -paketti tarjoaa perustarkastukset, joihin kuuluvat mm. muisti-, prosessori-, levy- ja saavutettavuustarkastukset.

Nagioksen ilmaisuus, avoimuus ja plugin tarkastusten vapaa kehitys tarjoavat puitteet ottaa käyttöön suuri määrä erikoisiakin tarkastuksia. Tarkastuksia on ladattavissa verkosta yksityisten käyttäjien sivuilta ja useimmissa on jopa mukana tarkat asennusohjeet. Plugin tarkastuksia on mahdollista kirjoittaa Perl-ohjelmointikielellä käyttäen varsin yksinkertaisia muuttujia. Lisäksi Nagios on saavuttanut itselleen suuren käyttäjäkunnan, joka käytännössä tarjoaa loputtoman käyttötuen Nagioksen keskustelupalstoilta.

Nagioksen määritysten varmuuskopiointi onnistuu kopioimalla tiedostoja. Ohjelman uudelleenasennuksen jälkeen on helppo palauttaa käytetyt asetukset kopioimalla varmuuskopioidut asetukset tuoreiden päälle. Nagios ohjelmalla suoritettujen tarkastusten, ei käytönaikana havaittu vaikuttavan valvottujen palvelinten toimintaan. Havainnot perustuvat palvelimen prosessori- ja muistikuorman seuraamiseen valvontojen toimiessa. Nagioksen verkkoon kohdistuvasta kuormasta tulee huomattavaa vasta erittäin laajoissa kokonaisuuksissa tai hitailla yhteyksillä. Esimerkiksi haarakonttoreiden välillä on suositeltavaa ylläpitää molemmissa lähiverkoissa omaa Nagios hallintapalvelinta.

8.2 Nagios-NSCA

NSCA eli Nagios Service Check Acceptor, on järjestelmä jossa Nagios-palvelin ei suorita lainkaan kyselyitä tarkasteltaville kohteille, vaan ainoastaan vastaanottaa kohteiden lähettämää tietoa. Tarkasteltaviin Linux kohteisiin asennetaan send_nsca –client, tarvittavat pluginit ja Nagios. Pluginit suorittavat tarkastukset asennetun Nagioksen avulla ja tarkastuksen jälkeen send_nsca –client lähettää tiedot varsinaiselle Nagios-palvelimelle. Windows ympäristössä toimitaan samalla periaatteella. Nagioksen Linux sidonnaisuudesta johtuen tarkastukset ovat kuitenkin enemmän suodatusta olemassa olevasta tiedosta, eikä itse ohjelmaa luonnollisesti tarvitse asentaa. KUVIOSSA 16 on esitetty NSCA prosessi.

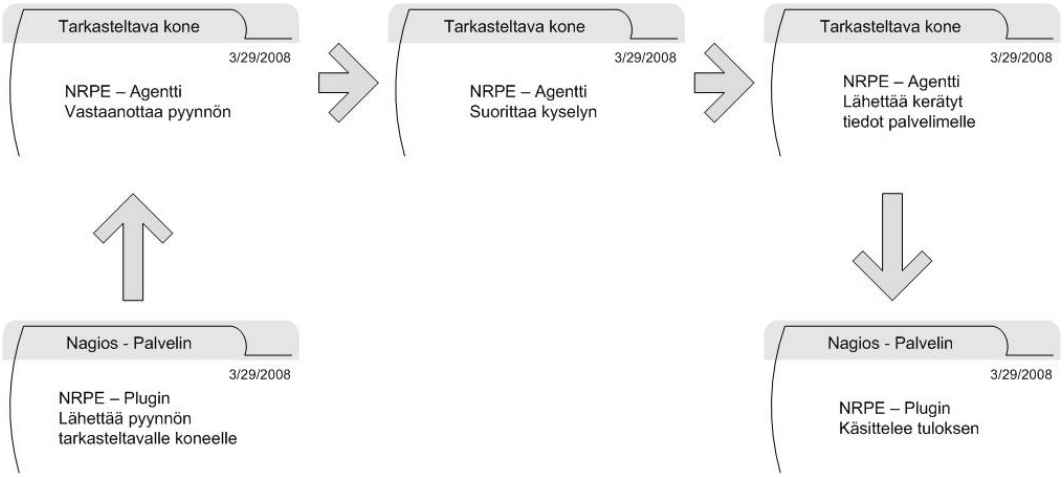


KUVIO 16. NSCA prosessista.

NSCA-järjestelmää käytetään hajauttamaan tarkastusten vaatimia resurssitarpeita. Järjestelmän avulla voidaan valvoa koneiden perustietoja, kuten prosessorin, muistin ja levyn käyttöä.

8.3 Nagios-NRPE

NRPE eli Nagios Remote Plugin Executor on Nagioksen aktiivinen lisäosa. Lisäosaa käytetään tarkastusten tietojen hakemiseen valvottavilta kohteilta. Tiedon haku perustuu server –client-keskusteluun, jossa palvelin pyytää valvottavalle kohteelle asennettua NRPE-agenttia suorittamaan kyselyn. Kysely voi olla vaikka muistin käyttöön tai prosessorikuormaan liittyvä tarkastus. Kun NRPE-agentti on saanut tarkastuksen suoritettua, agentti lähettää keräämänsä tiedot Nagios palvelimen NRPE-pluginille. Palvelin käsittelee tiedot ja tekee tulosten pohjalta mahdollisen hälytyksen. KUVIOSSA 17 on esitetty NRPE-prosessi.



KUVIO 17. NRPE-kyselyprosessi

NRPE-plugin ei kuulu Nagioksen oletus plugin pakettiin, vaan NRPE pitää ladata valvottavalle työasemalle erikseen. Nagios-palvelimelle tulee asentaa perus NRPE-plugin paketti, joka palvelin käyttää ottaessaan yhteyttä valvottavaan kohteeseen. Windows käyttöjärjestelmällä varustetuille koneille tulee asentaa NRPE_NT -paketti, joka mahdollistaa prosessorin, levytilan, lokien, muistin ja palveluiden tarkastuksen. Windows NRPE tarkastuksen toimimiseksi tulee NRPE-asetustiedostoon, *nrpe.conf*, lisätä Nagios-palvelimen IP-osoite. Tiedoston *Command definitions* kohtaan tulee lisätä tieto valvottavasta palvelusta. NRPE palvelu käynnistetään helpoiten komentokehotteen kautta, syöttämällä komento *net start nrpe_agent.* Nyt Nagios-palvelin voi suorittaa tarkastuksia valvottavalle windows koneelle.

8.4 Nagios - SNMP

SNMP on Nagioksen käytetyin tarkastusmuoto. Syynä suosioon on helposti käyttöön saatava tietoturvallinen yhteys. Toinen syy suureen suosioon on SNMP:n laaja tuki verkon aktiivilaitteiden keskuudessa. SNMP mahdollistaa lukuisten asioiden valvonnan tarkasteltavalta koneelta. SNMP palvelun käyttöä ei oletuksena ole mahdollistettu niin Linux kuin Windows-käyttöjärjestelmissäkään. SNMP on kuitenkin helposti otettavissa käyttöön ja asennuksen jälkeen on SNMP:n laaja MIB-kirjasto vapaasti tarkastelun kohteena. SNMP:tä voidaan käyttää perinteiseen tapaan tarkastusten kysely väylänä tai sitten siihenkin on mahdollista ohjel-

moida trappeja eli liipaisimia. Liipaisin on tarkasteltavalle koneelle asetettu arvo, jonka täytyttyä kone lähettää itse hälytyksen Nagios palvelimelle.

SNMP-protokollaa käytettäessä on yleistä, että tarkastuksia hajautetaan SNMP-agenttien avulla. Hajautus tarkoittaa tilannetta, jolloin verkkosegmentissä on yksi agentti, joka kerää itselleen tarkastustietoa segmenttinsä muilta koneilta. Tietyin väliajoin Nagios-palvelin kysyy kerättyjä tietoja agentin tietokannasta. Toiminnolla saavutetaan säästöä verkkokaistassa, joka on hyödyllistä etenkin hitaita verkkoyhteyksiä käytettäessä. Agentilla voidaan mahdollistaa tiedonsiirto eri standardien välillä, jolloin agentti toimii myös tulkkina.

8.5 Nagios toimenpiteet

Nagioksen heikkous on ohjelman automatisoidun korjaustoimenpiteen puute. Ohjelma osaa kyllä lähettää tiedon tarkastuksen epäonnistumisesta, mutta sille ei voi määrätä muuta automatisoitua toimenpidettä. Nagios onkin verkonvalvonnan perusosaaja, jonka ei ole määräkään kyetä hallitsemaan laitteita. Nagios tarkastelee verkon palveluita ja laitteita ilmoittaen virheistä ylläpitäjälle.

Korjausautomaation puute vaatii ylläpidolta puuttumista toistuvissakin vioissa, joka saattaa olla turhauttavaa. Turhautuminen saattaa toimia motivoivana osana ylläpidolle ja painostaa selvittämään todellista ongelmaa. Muuten ongelma saatettaisiin käsitellä tilapäisellä korjauksella, esimerkiksi palvelun käynnistyksellä manuaalisesti.

9 OHJELMIEN VERTAILU

9.1 Vaatimukset

Kasvava tietotekniikan määrä yritysten käytössä pakottaa kasvattamaan tietoteknistä valvontaa. Tuottavuuden riippuminen palveluiden ja laitteiden toiminnasta aiheuttaa painetta ylläpidolle, jonka osalle jää toiminnan varmistaminen. Tehtävää helpottamaan suunnitellut ja tehdyt ohjelmat Nagios ja GFI:n NSM tarjoavat automatisoitua valvontaa. Ohjelmien avulla ylläpidon resursseja vapautetaan tuottavampaan käyttöön, koska vian sattuessa ohjelman pyrkimys on tietää hyvinkin tarkasti vian aiheuttaja. Tällöin ylläpidolta säästyy vian etsinnän vaiva.

Vaatimuksena toimivalle ratkaisulle on helppo ja käyttäjäystävällinen ympäristö, joka toimii tarkasti. Myös tarkastusten muokattavuus ja riittävät tiedotuskanavat ovat avaintekijöitä, valittaessa tuotetta tuotantoympäristöön. Kasvava tietotekninen taito saattaa houkutella mahdollista asiakasta sillä ajatuksella, että hän voi päivittää itse tarkastus listaa. Luonnollisesti kuitenkin kaiken ratkaisee yritysmaailmassa tärkeimpänä tekijänä kustannustehokkuus. Korkea tehokkuus, luotettavuus ja matalat kustannukset ovat hyvä lähtökohta.

Hinta on usein rajoittava tekijä PK-yritysten tietoverkkohankinnoissa. Ohjelman edullisuus suhteutettuna ylläpitokustannuksiin on asia, joka kiinnostaa verkonvalvonnan toteutusta pohtivia yrityksiä. Tarkasti suunniteltu ja toimivasti tuotteistettu verkonvalvontayhdistelmä oikean hinnoittelun kera, on yhdistelmä, joka kiinnostaa yrityksiä.

9.2 Soveltuvuus vaatimuksiin

Molemmat vertailuun valituista ohjelmista täyttävät vaatimusehdot täysin. Koekäytön yhteydessä ei havaittu vakausongelmia kummassakaan ohjelmassa, joten ohjelmien perustoteutus on selvästikin laadukasta. Myös asennus- ja perustarkastusten luonti ja toiminnan toteaminen ei tuottanut ongelmia.

GFI NSM on selkeästi mielekkäämpi käyttää graafisen ja helposti hallittavan ympäristönsä johdosta. Helppo on kuitenkin suhteellinen käsite, sillä kaikki riippuu osaamisesta. Henkilö, joka on tehnyt paljon töitä komentokehotteen tai Linuxin päätteen kautta, saattaa arvostaa Nagioksen tekstipohjaista käyttämistä. Totuus kuitenkin on, että nykyisillä käyttöjärjestelmillä on graafisuus huomattavasti käytetympää, kuin tekstipohjainen hallinta. Toki komentokehote-pohjainen hallinta on edelleen graafisen puolen rinnalla ja sitä on halutessa mahdollista käyttää.

Vertailtavat ohjelmat ovat erittäin samantyyppisiä ominaisuuksiltaan ja tarkastuksiltaan. GFI NSM vie voiton valmiiden tarkastusten määrässä, mutta Nagioksen laaja käyttäjäkunta, itse tehtyine tarkastuksineen kääntää tilanteen päinvastaiseksi. Molempiin ohjelmiin voidaan tehdä lisää tarkastuksia vaihtelevilla tyyleillä ohjelman mukaan.

GFI NSM on parempi tarkastusten tulosten toiminta malleissa. Mahdolliset korjaavat komentojen suoritukset epäonnistuneen tarkastuksen jälkeen eivät ole valittavissa Nagioksessa. Tämä ei kuitenkaan ole suuri puute, sillä harvoin on tilannetta, jolle olisi helposti luotavissa valmis korjausmalli. Enemmänkin on kyse vain toiminnan seuraamisesta ja tilanteen raportoimisesta, joihon molemmat ohjelmat kykenevät täysin.

Taulukossa 1 on esitetty ohjelmien vahvuuksia ja heikkouksia.

	Nagios	GFI NSM
Vahvuudet	* Hinta * Tarkastuksia saa ladattua netistä * Vertaiskäyttäjien tuki * Linux pohjaisuus	* Graafinen hallinta * GFI:n tekninen tuki * Paljon valmiita tarkastuksia * Windows pohjaisuus * Käytön helppous
Heikkoudet	* Graafisen hallinnan puute * Linux pohjaisuus * Asetusten muokkaus * Automatisoitujen toimenpiteiden puuttuminen	* Hinta

TAULUKKO 1. Nagioksen ja GFI NSM vertailu

10 YHTEENVETO

Työssä vertailtiin kahta verkonvalvontaan tarkoitettua ohjelmaa ja pohdittiin niiden tuotteistusta PK-yritysten verkkojen valvontaan. Ohjelmat olivat Linux-pohjainen Nagios ja Windows-pohjainen GFI NSM. Työssä tutustuttiin myös verkonvalvontaan ja SNMP-verkonvalvontaprotokollaan.

Koska Nagios pohjautuu Linux-käyttöjärjestelmään, se vaatii tuntemusta käyttöjärjestelmän toiminnasta, jotta ohjelman asennus onnistuu. GFI NSM on paremmin profiloitu Windows käyttöjärjestelmään tottuneille henkilöille. Useat vastaavuudet tuttujen ohjelmien kanssa, kuten Office tuoteperhe, saavat aikaan luontevan tuntuman. Johtopäätöksenä GFI NSM-ohjelma on mielekkäämpi vaihtoehto. GFI NSM:n havainnollisen graafisen käyttöliittymän avulla on helppo selittää asiakkaalle, mikä virhe tarkoittaa mitäkin ja mitä virheen jälkeen on mahdollista tehdä.

Ohjelmien välillä ei paljastunut suuria eroja, mikä oli jo odotettavissa. GFI NSM ohjelman pienet paremmuudet ratkaisevat vertailun. Paremmuudella on kuitenkin hintansa. Koska Nagios on ilmainen ohjelma, se kykenee toteuttamaan samat perustarkistukset, mutta sen ylläpito on hankalampaa. Siksi onkin pohdittava, kumpi on yrityksen kannalta parempi vaihtoehto. Maksaa lisenssi ohjelmasta ja säästää ylläpidossa tai säästää ohjelmassa ja maksaa ylläpidossa. Kysymykseen ei ole yksiselitteistä vastausta, sillä asia riippuu paljolti yrityksen omasta tietotekniikasta vastaavan henkilön osaamisesta.

Pienten yritysten budjetti on usein rajoittava tekijä tietoverkko- ja ohjelmistopuolen hankinnoille. Nagios on ilmaisuutensa ansiosta houkutteleva vaihtoehto. Koska se on hyvin suunniteltu ja tuotteistettu ohjelman asennus toimintaan ei vie pitkää aikaa. Vastapainona saadaan tiedotusjärjestelmä, jolla ylläpito saa tiedon asiakkaan ongelmasta mahdollisesti ennen kuin asiakas tiedostaa ongelmaa. Järjestelmällä voidaan vähentää ongelmista, kuten palvelimen käyttöjärjestelmälevyn täyttymisestä aiheutuvia pulmia.

Tulevaisuus on verkonvalvonnan kannalta tuomassa lisää kysyntää hallinnalle. Hallintaa ollaan lisäämässä yrityspuolella ja siellä vaatimukset ohjelmien kyvyille ovat lisääntymässä. Nykyisellään hallittavuus tarkoittaa yksittäisten sovellusten uudestaankäynnistys mahdollisuutta. Tulevaisuuden perushallittavuudeksi vaaditaan työaseman graafinen etähallinta ja näkymän jakaminen käyttäjän kanssa. Samalla vaatimukset etenkin tietoturvan suhteen tulevat kasvamaan. Valvonta yleisesti on lisääntymässä, joka voidaan havaita Internetin sisältöä koskevan lainsäädännön lisääntyessä. Olemme kulkemassa kohti hallittuja verkkoja, joissa valvonta on osa jokapäiväistä arkea.

LÄHTEET

About Nagios 2008. About Nagios. [verkkodokumentti] Nagios [viitattu 29.3.2008] Saatavilla: http://www.nagios.org/about/

Charton E, Leblanc G. 1999. Administration réseau: SNMP, SNMPv2. [verkkodokumentti] Année universitaire [viitattu 23.1.2008] Saatavilla: http://www.linux-france.org/article/gvallee/snmp/snmp.html

Doh, C. 2003 Native MIB-2-Tree [verkkodokumentti] Carsten Familie [viitattu 17.1.2008] Saatavilla: http://carsten.familie-doh.de/mibtree/mib-2-native.html

Dong, L. 2004. IPv6 Updates in China [verkkodokumentti] IPv6 Summit in Asia Pasific [viitattu 23.1.2008] Saatavilla: http://www.ap-ipv6tf.org/events/2nd_Summit_AP/slides/Keynote_Liu_Dong.pdf

Feldman, J. 1999. Verkonhallinta. Gummerus Kirjapaino Oy, Jyväskylä.

GFI NSM. 2008. Overview [verkkodokumentti] GFI [viitattu 17.1.2008] Saatavilla: http://www.gfi.com/nsm/

Happonen, A. 2005. Verkon toiminnan seuraaminen. [verkkodokumentti] Lappeenrannan teknillinen yliopisto. [viitattu 19.1.2008] Saatavilla: www.it.lut.fi/kurssit/04-05/010626000/linux-tyot/SNMP_Raportti_Ari_Happonen.pdf

Hautaniemi, M. 1994 TKK/Atk-keskuksen verkon valvonta ja hallinta [Verkkodokumentti]. Helsinki: Teknillinen korkeakoulu [viitattu 16.1.2008]. Saatavissa: http://keskus.hut.fi/julkaisut/tyot/diplomityot/611/thesis.html

IETF 2008 The Internet Engineering Task Force [verkkodokumentti] IETF [viitattu 17.1.2008] Saatavissa: http://www.ietf.org/

ITU-T. 2008. Telecommunication Standardization Sector [verkkodokumentti] ITU-T [viitattu 17.1.2008] Saatavissa: http://www.itu.int/ITU-T/

MG-SOFT. päivitetty 2008. Network Management Software [verkkodokumentti] MG-SOFT [viitattu 17.1.2008] Saatavilla: http://www.mg-soft.si/

Nagios 2008. Table Of Contents [verkkodokumentti] Nagios [viitattu 29.3.2008] Saatavilla: http://nagios.sourceforge.net/docs/3_0/toc.html

Orava, S. 2000 SNMP:n hallintatietokantojen sisältämä palvelunlaatutieto IP- ja ATM-verkoissa. [verkkodokumentti] Lappeenrannan teknillinen korkeakoulu [viitattu 20.1.2008] Saatavilla: http://edu.lut.fi/LutPub/web/nbnfi-fe20011205.pdf

Puska, M. 2000. Lähiverkkojen tekniikka. 2, uudistettupainos. Gummerus Kirjapaino Oy, Jyväskylä.

RFC1155 1990 Rose, M Structure and Identification of Management Information for TCP/IP-based Internets [verkkodokumentti] Request for Comments 1155 [viitattu 20.1.2008] Saatavissa:

RFC1157. 1990. Case, J., Fedor, M., Schoffstall, M., DAVIN, J., "A Simple Network Management Protocol". [verkkodokumentti] Request for Comments 1157 [viitattu 20.1.2008] Saatavissa: http://www.ietf.org/rfc/rfc1157.txt

RFC1905. 1996. Case, J., McCloghrie, K., Rose, M., Waldbusser, S. [verkkodokumentti] Request for Comments 1905. [viitattu 20.1.2008] Saatavissa: http://www.freesoft.org/CIE/RFC/1905/index.htm

RFC2012. 1996. McCloghrie, K. SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2. [verkkodokumentti] Request for Comments 2012. [viitattu 20.1.2008] Saatavissa: ftp://ftp.funet.fi/pub/standards/RFC/rfc2012.txt

RFC2571 1999 D. Harrington, R.Presuhn, B.Wijnen An Acrchitecture for Describing SNMP Management Frameworks [verkkodokumentti] Request for Comments 2571. [viitattu 20.1.2008] Saatavissa: http://www.ietf.org/rfc/rfc2571.txt

Sinkkonen, A. 2007 Nagios – verkonvalvontaohjelmiston tehokas hyödyntäminen [verkkodokumentti] Savonia Ammattikorkeakoulu [viitattu 10.01.2008] Saatavilla: http://openlab.savonia-amk.fi/wiki/index.php/Nagios_IWN

SNMP. päivitetty 2008. Secure internet management and SNMP [verkkodokumentti] SNMP [viitattu 23.1.2008] Saatavilla: http://www.snmp.com/

Stallings, W. 1996.SNMP, SNMPv2, and RMON Practical Network Management, Second Edition. Addison-Wesley Publishing Company, INC, United States of America

Sundell, S. 2002. SNMP kaataa netin. [verkkodokumentti]. MikroPC 03/2002, 16. [viitattu 20.1.2008] Saatavissa: http://mikropc.net/rml/arkisto/mikropc/pdf/pc0103200216.pdf

Syscom-Net [verkkodokumentti] Syscom [viitattu 10.1.2008] Saatavissa: http://www.syscom-net.co.jp/tech/index.html

LIITTEET

Liite 1 Nagioksen asennus ohjeet.

Asennus aloitetaan kirjautumalla käyttöjärjestelmään normaaleilla käyttäjäoikeuksilla, jotka muutetaan päätteen kautta ”su –l” komennolla pääkäyttäjän eli root käyttäjän oikeuksiksi. Seuraavaksi luotiin käyttäjä ”nagios” ja asetettiin sille salasana. Käyttäjä luotiin komennolla ”**/usr/sbin/useradd nagios**” ja lisättiin salasana ”**passwd nagios**” komennolla, jonka jälkeen ohjelma kysyi nagios käyttäjälle asetettavan salasanan. Seuraavaksi luotiin käyttäjäryhmä ”nagios” komennolla ”**/usr/sbin/groupadd nagios”** ja asetettiin Nagios käyttäjä nagios ryhmään komennolla ”**/usr/sbin/usermod -G nagios nagios**”

Seuraavaksi vuorossa oli ulkoisten komentojen mahdollistaminen luomalla ”**nagcmd**” ryhmä johon lisättiin sekä nagios käyttäjä että apache käyttäjä. Ryhmä luotiin samalla tavalla kuin nagios ryhmä, eli komennolla ”**/usr/sbin/groupadd nagcmd**”. Käyttäjät lisättiin komennoilla ”**/usr/sbin/usermod -G nagcmd nagios**” ja ”**/usr/sbin/usermod -G nagcmd wwwrun**”.

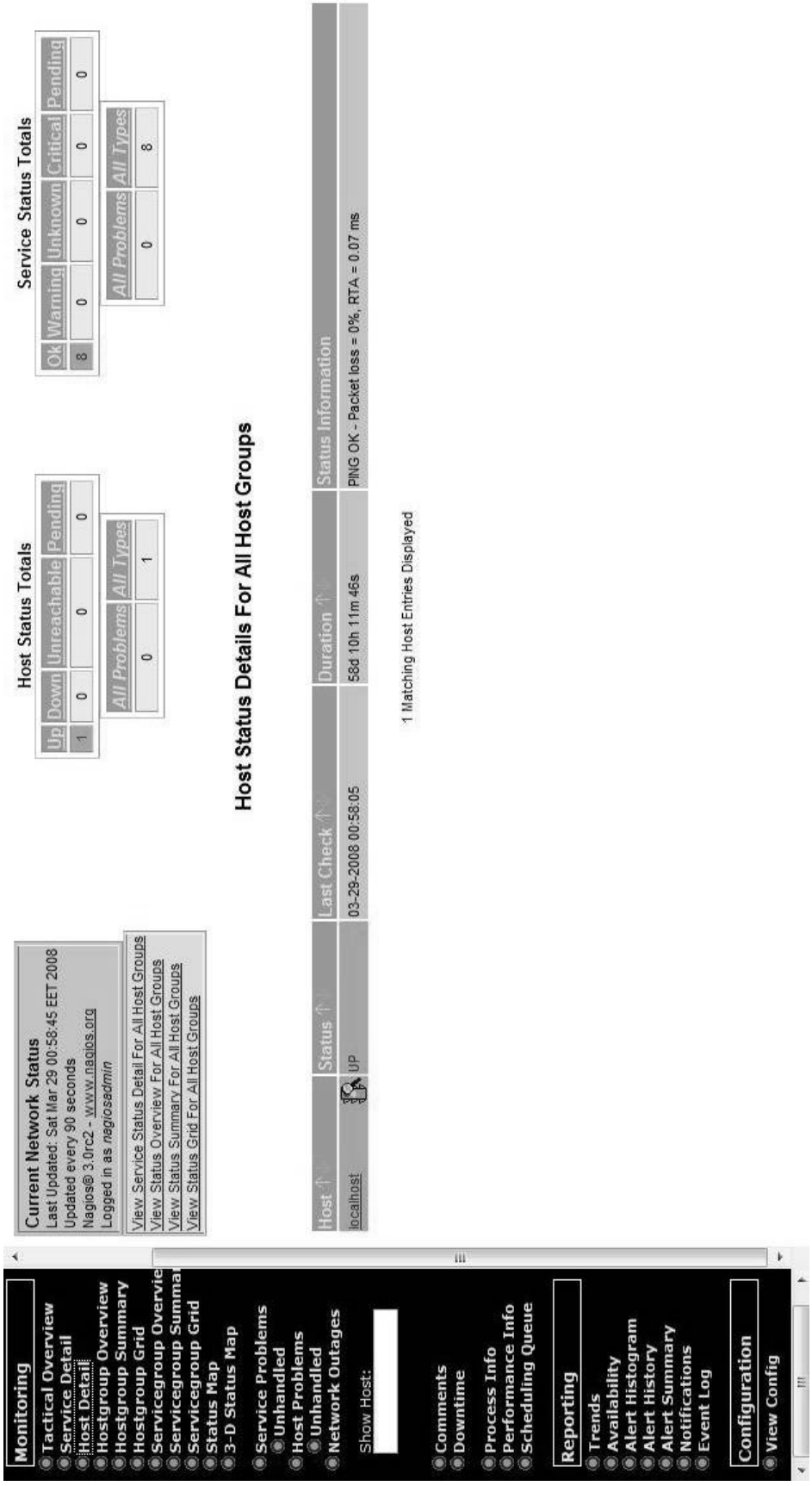
Itse asennuksen päätin toteuttaa komentopäätteen kautta, jotta asetuksissa olisi mahdollisimman suuri muokattavuus. Nagioksen viimeisin versio (30.1.2008) 3.0rc2 ladattiin komennolla ”**wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.0rc2.tar.gz**” sivustolta. Samoin ladattiin nagioksen plugin paketti ”**wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.11.tar.gz**”. Asennus aloitettiin purkamalla Nagioksen paketti komennolla ”**tar xzf nagios-3.0rc2.tar.gz**”. Seuraavaksi suoritettiin Nagioksen asennuksen aloitus käsky niin että aikaisemmin asetetut käyttäjät ja ryhmät tulevat käyttöön. Suoritettava komento on ”./**configure --with-command-group=nagcmd**” ja komento tulee suorittaa hakemistossa mihin Nagios paketti purettiin. Nagios käännetään komennolla ”**make all**” sekä asennetaan binäärit ja html-tiedostot komennolla ”**make install**”. Muodostetaan myös inid – skripti, joka toteutetaan

komennolla ”**make-inid**”. Lopuksi asetetaan oikeudet ulkoiseen komentojen suorittamiseen komennolla ”**make install-commandmode**”.

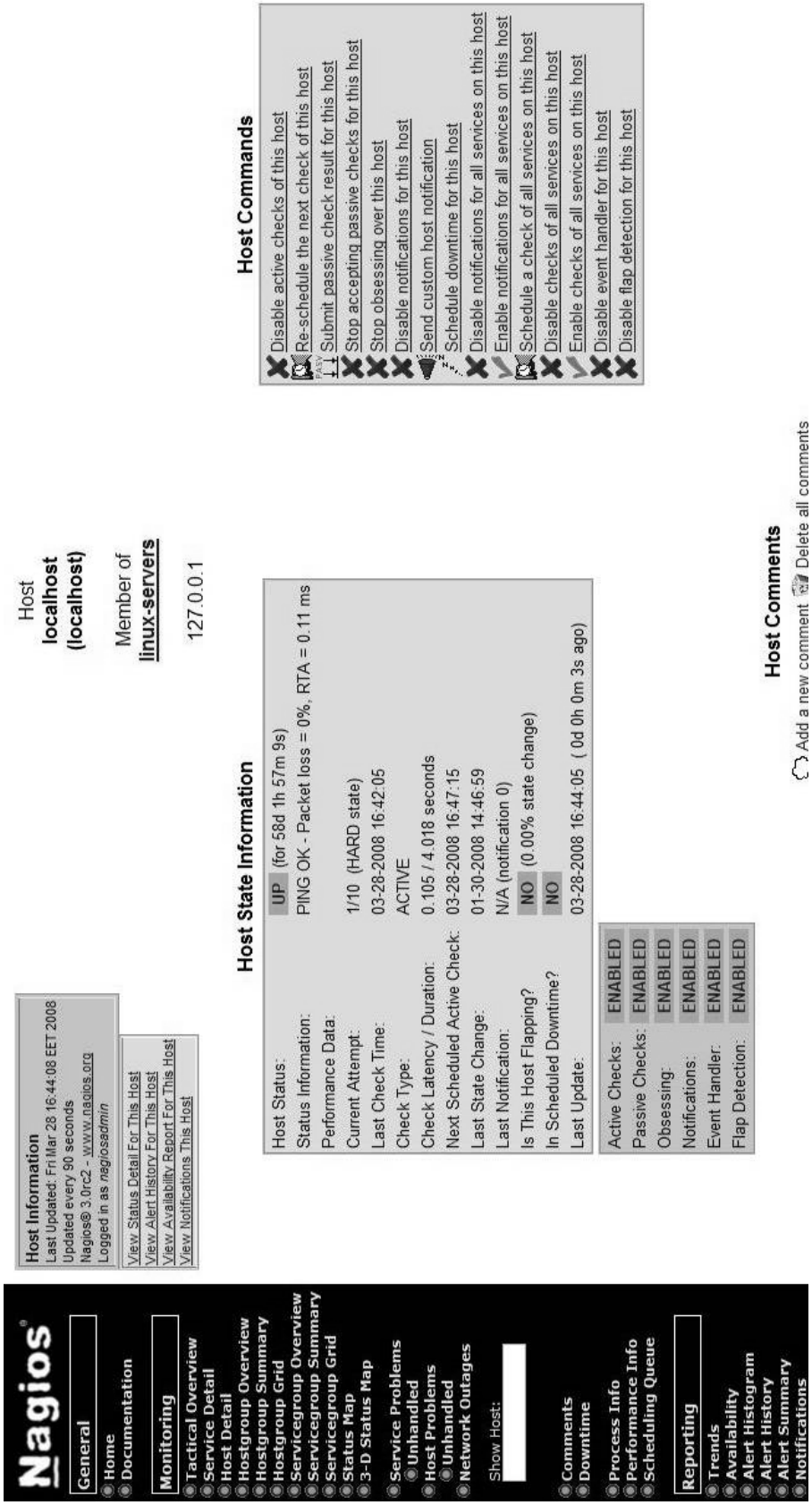
Hälytysten sähköposti tiedottamista varten tulee tehdä muokkauksia ”**contacts.cfg**” tiedostoon. Tiedoston muokkaaminen onnistuu helpoiten vi tekstieditorilla. ”**vi /usr/local/nagios/etc /objects/contacts.cfg**” komento avaa tiedoston käsittelyä varten. Tiedostossa tulee oletus sähköposti osoitteen tilalle asettaa ylläpitäjän sähköposti, jotta postit kulkeutuvat oikeaan osoitteeseen. Asennus jatkuu seuraavaksi komennolla ”**make install-webconf**”, joka asentaa nagioksen Web – käyttöliittymän tiedostot apacheen. Seuraava vaihe on luoda käyttäjä, jolla on oikeudet käyttää Nagiosta Web – käyttöliittymän kautta. Käyttäjän luonti yhdistettynä salasanan asetukseen tehdään komennolla ”**htpasswd2 -c /usr/local/nagios/etc/htpasswd .users nagiosadmin**”. Tämän jälkeen täytyy apache palvelu käynnistää uudestaan, jotta asetukset tulevat voimaan. Käynnistys toteutetaan komennolla ”**service apache2 restart**”.

Seuraavaksi siirrytään Nagioksen pluginien asennukseen, purkamalla jo ladattu paketti komennolla ”**tar xzf nagios-plugins-1.4.11.tar.gz**”. Paketin asetusten asettaminen aloitetaan komennolla ”**./configure --with-nagios-user=nagios --with-nagios-group=nagios**”. Seuraavaksi paketti käännetään komennoilla “**make**” ja “**make install**”. Seuraavaksi lisäämme Nagioksen automaattisesti käynnistettävien ohjelmien listalle komennoilla ”**chkconfig --add nagios**” ja “**chkconfig nagios on**”. Jälkimmäinen komento määrittelee missä istunnoissa nagios käynnistyy. Istunnoilla tarkoitetaan normaalia graafista tilaa, teksti tilaa sekä vikasieto ja muita asennettuja käyttöliittymä tiloja. Ennen Nagioksen käynnistystä tulee asetus tiedostot varmistaa ongelmien varalta, tämä suoritetaan komennolla ”**/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg**”. Ja mikäli virheitä ei ilmene voidaan Nagios käynnistää komennolla ”**service nagios start**”.

Liite 2 Nagioksen näkymä johon on listattu kaikki valvotut koneet.



Liite 3 Nagioksen näkymä kattaen yhden tarkasteltavan koneen tiedot



Liite 4 Nagioksen yhden tarkasteltavan koneen tarkastusten tiedot.