LAUREA

Nagios-verkonvalvontaohjelmiston asennus ja käyttöönotto Laurea-ammattikorkeakoulussa

. . . . . .

Gröning, Harri & Hernberg, Ilja

2009 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Nagios-verkonvalvontaohjelmiston asennus ja käyttöönotto Laurea-ammattikorkeakoulussa

Harri Gröning
Ilja Hernberg
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Lokakuu 2009

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Tiivistelmä

Harri Gröning
Ilja Hernberg

Nagios verkonvalvontaohjelmiston asennus ja käyttöönotto Laurea - ammattikorkeakoulussa

Vuosi 2009 Sivumäärä 92

Nykypäivänä yritystoiminnan kannalta ensiarvoisen tärkeää on organisaation verkkojen sekä verkon palveluiden hyvä toimivuus. Erinäiset verkon ongelmat ilmenevät verkon käyttäjille verkon hitautena tai mahdollisesti jopa verkon täytenä toimimattomuutena. Ongelmatilanteita voidaan ennaltaehkäistä sekä monissa tapauksissa kokonaan estää toimivan verkonvalvonnan avulla. Lisäksi verkonvalvontaohjelmisto mahdollistaa vikojen huomattavasti nopeamman diagnosoinnin, mikä nopeuttaa esiintyvien vikojen korjaamista merkittävästi.

Opinnäytetyön toimeksiantajana oli Laurea-ammattikorkeakoulu. Toimeksiantona oli Nagios – verkonvalvontaohjelmiston asentaminen sekä käyttöönotto Laurean Leppävaaran ja Tikkurilan toimipisteissä.

Ohjelmiston perusasennuksessa on suuria puutteita, joten toimeksiantoon kuului myös mahdollisien ominaisuuksien tarpeen kartoittaminen sekä hyödyllisten lisäominaisuuksien käyttöönotto ja testaus.

Projektin tuotoksena luotiin toimiva verkonvalvontaohjelmiston asennus monine lisäominaisuuksineen, sekä lisättiin valvottavat laitteet ohjelmistoon. Lisäksi asennus dokumentoitiin mahdollisimman kattavasti, jotta tulevat ohjelmiston ylläpitäjät pystyvät tarpeen mukaan asentamaan ohjelmiston uudelleen.

Asiasanat: Nagios, Verkonvalvonta, Linux

Laurea University of Applied Sciences
Laurea Leppävaara
Degree Programme in Business Information Systems

Abstract

Harri Gröning
Ilja Hernberg

Installation and deployment of Nagios Network Monitoring Tool in Laurea

Year 2009 Pages 92

In the business world of today it is essential to have a reliable, well thought out network. Different problems concerning corporation networks may manifest themselves as general slowness, and even complete unusability. It is possible to prevent most problems from occurring with the use of a good network monitoring tool. In addition, network monitoring makes problem diagnosis considerably faster. It also speeds up the fixing of potential problems within the corporation's networking infrastructure.

The client for this thesis is Laurea University of Applied Sciences. The client wanted the writers of this thesis to implement a working network monitoring tool called Nagios at two Laurea units; Leppävaara and Tikkurila.

The basic installation of Nagios has a lot of shortcomings concerning functionality which forced the project group to survey the special needs of Laurea. Also these additional functions had to be implemented and tested.

Nagios was installed and the monitored routers, servers and services within Leppävaara and Tikkurila were added to Nagios. The project group documented how Nagios was installed, also some manuals concerning the use of Nagios were also created. This was carried out to ease the work of administrators in Laurea in the future concerning new installations and possible upgrades to newer versions of the network monitoring tool.

Keywords: Nagios, Network Monitoring, Linux

Sisällys

1 Johdanto

Nykypäivän yritystoiminnassa tietoverkot ovat usein ratkaisevassa roolissa. Onkin suositeltavaa, että organisaation käyttämiä tietoverkkoja pystyttäisiin helposti valvomaan. Verkonvalvonta mahdollistaa erilaisten vikatilojen havainnoimisen sekä korjaamisen ennen kuin niistä koituu suurempia haittoja organisaatiolle. Ongelmana monissa verkonvalvontaohjelmistoissa on se, että ne ovat hyvinkin vahvasti sidottuja tiettyihin alustoihin tai laitevalmistajiin. Tämä koituu varsinkin isoissa organisaatioissa ongelmaksi, sillä usein organisaation sisällä on useilla eri alustoilla toimivia koneita. Yhtenä vaihtoehtona on ottaa käyttöön jokin Open Source –verkonhallintaohjelmisto.

Opinnäytetyön kirjoittajat suorittivat opintoihin kuuluvan viiden kuukauden mittaisen työharjoittelun Laurea-Ammattikorkeakoulu Oy:ssä. Laurea-Ammattikorkeakoulu on monialainen, tunnustettu kehittäjä Helsingin metropolialueella. Laurea tarjoaa alempia- ja ylempiä amk-opintoja noin 8000 opiskelijalle. Laureassa on yhteensä 16 eri koulutusohjelmaa, joista viisi on englanninkielisiä.

Toimeksianto opinnäytetyöhön saatiin Isto Haminalta, joka toimi ATK-asiantuntijana Laurean Tikkurilan toimipisteessä. Isto Hamina oli jo jonkin verran ottanut selvää Nagioksen toiminnasta sekä testannut sitä ja huomannut joitakin puutteita ohjelmistossa. Suurimpana ongelmana oli se, että Nagios ei itsessään käytä minkäänlaista tietokantaa laitteiden ja palveluiden hallinnoimiseen vaan kaikki laitteistoihin tehtävät muutokset täytyy editoida käsin erinäisiin asetustiedostoihin. Opinnäytetyön kirjoittajat saivat Isto Haminalta toimeksiannon ottaa selvää mahdollisista ratkaisuista yllä olevan ongelman korjaamiseksi. Lisäksi haluttiin saada jonkinlainen parempi graafinen käyttöliittymä Nagioksen hallinnoimiseksi sekä raporttien esiin tuomiseksi. Toimeksiantoon kuului myös Nagios–verkonvalvontaohjelmiston asennus sekä käyttöönotto Laurean kahteen toimipisteeseen (Tikkurila ja Leppävaara). Toimeksiantaja halusi saada selvyyden siitä, millaisia tarkistuksia Nagios mahdollistaa sekä mitkä tarkistukset olisi suotavia otettavaksi käyttöön Laureassa. Tässä työssä keskityttiin SNMP:n käyttämiseen mahdollisien tarkistuksien tekemiseksi. Nagios mahdollistaa näiden tarkastuksien tekemisen myös kahdella omalla protokollallaan jotka ovat: NRPE (Nagios Remote Plugin Executioner) sekä NSCA (Nagios Service Check Acceptor). Nämäkin mahdollisuudet käydään läpi tässä opinnäytetyössä.

Nagiokseen voidaan määritellä myös ominaisuus, joka mahdollistaa automaattisen sähköpostin tai tekstiviestin lähettämisen ennalta määritellyille tahoille vikatilanteiden ilmetessä. Tekstiviestinlähetystä ei otettu vielä tässä vaiheessa käyttöön Laureassa.
Suuren tutkimisen ja testauksen jälkeen ryhmä päätyi Centreon–nimiseen lisämoduuliin joka asennetaan Nagios–ytimen päälle. Centreon mahdollistaa MySQL-tietokannan käytön laitteiden

hallinnassa sekä mahdollisuuden konfigurointitiedostojen automaattiseen luontiin selkeän ja melko yksinkertaisen web-käyttöliittymän kautta. Centreoniin päädyttiin senkin takia, että se on tällä hetkellä vahvasti kehittyvä järjestelmä. Centreonia kehitetään jatkuvasti, ja uusia versioita ohjelmistosta tulee tiheään tahtiin. Lisäksi Centreonissa on kattavat dokumentoinnit, sekä aktiiviset foorumit, joiden kautta saadaan käyttötukea mahdollisissa ongelmatilanteissa. Centreonin kehittäjä on aktiivisena osana yhteisöä, hänelle pystytään suoraan laittamaan mahdollisia parannusehdotuksia sekä mahdollisia virheitä ohjelmiston toiminnassa.

1.1 Työn tarkoitus ja tausta

Tietoliikenneverkon ja sen palveluiden toiminta on tärkeä asia niitä tuottavalle organisaatiolle. Yleensä niissä ilmenevät ongelmat näkyvät esimerkiksi palvelun toimimattomuutena tai verkon hitautena loppukäyttäjille. Suurin osa ongelmatilanteista voidaan välttää tai jopa ennalta ehkäistä valvomalla verkon ja sen palveluiden toimintaa asianmukaisella tavalla.

Projektin tilaajana on Laurea-ammattikorkeakoulu. Laurea-ammattikorkeakoulun IT- järjestelmien puutteena on ollut oikeanlainen työkalu verkonvalvontaan. Laurealla on suuri tarve keskitettyyn verkonvalvontaan. Tällä hetkellä käytössä on useita eri sovelluksia, mikä johtaa valvonnan sekavuuteen sekä tehottomuuteen. Projektin lähtökohtana on saada toimiva, kustannustehokas ohjelma verkon toimintojen valvomiseen. Markkinoilla on useita maksullisia verkonvalvontatyökaluja, tässä projektissa verkonvalvontatyökaluna toimii ilmainen avoimen lähdekoodin ohjelma nimeltään Nagios. Nagios on toiminnaltaan samankaltainen kuin maksulliset kilpailijansa. Koska projekti toteutetaan opinnäytetyönä, ei maksullinen ohjelma ollut tarkoituksenmukainen. Projektilla pyritään saavuttamaan Laurea-ammattikorkeakoulun verkonvalvonta-tasoa ylemmäksi.

Nagios verkonvalvontaohjelma valvoo verkon laitteita ja niillä tuotettuja palveluita. Nagioksella pystytään myös valvomaan käyttäjien tekemiä toimintoja, mutta opinnäytetyössä ei Nagiosta käytetä kyseiseen toimintoon. Ohjelmiston olennainen tarkoitus projektissa on valvoa reitittimiä, kytkimiä, tulostimia sekä palvelimia. Palvelinten valvomiseen ei riitä se, että tiedetään niiden olevan käynnissä vaan toimivuutta on hyvä tutkia myös palveluiden tasolla.

Tällä hetkellä Laurean tiloissa olevilla laitteistoilla (reitittimet, kytkimet, tulostinpalvelimet) on olemassa useita eri verkonvalvontatyökaluja. Ongelmana onkin ollut juuri tämä työkalujen suuri määrä. Ryhmämme toimeksiantona oli selvittää minkälaisia verkonvalvontatyökaluja on tarjolla. Tärkeimpänä kuitenkin pidettiin jonkinlaisen keskitetyn verkonvalvontaohjelmiston asentaminen Laureaan.

Tämän työn keskeisimmät käsitteet liittyvät verkonvalvontaan, verkonhallintaan sekä verkkojen rakentamiseen.

1.2 Työn tavoitteet

Lyhyesti kuvattuna projektin tavoite on saada Laurea-ammattikorkeakoulun IT-palveluille toimiva verkonvalvontatyökalu. Projektin tehtävä on olla toiminnallinen opinnäytetyö. Toiminnallisella opinnäytetyöllä tarkoitetaan sitä, että työ toteutetaan käytännössä. Opinnäytetyön aiheena oleva Nagios verkonhallintajärjestelmä tullaan ottamaan käyttöön ensisijaisesti Laurea-ammattikorkeakoulun Tikkurilan toimipisteessä ja myöhemmin myös Leppävaarassa. Dokumentointi on oleellisen tärkeä osa projektia. Dokumentointi pyritään tekemään mahdollisimman kattavaksi uudelleenasennuksien, vikatilojen korjaamisen sekä mahdollisien koulutuksien tekemiseksi mahdollisimman helpoksi. Projektin dokumentoinnin tulee olla sen veroinen, että tulevat yrityksen IT- asiantuntijat pystyvät asentamaan ja ylläpitämään järjestelmää ilman suuria ongelmia.

Tavoitteet projektissa ovat selkeät. Tavoitteena on saada aikaan toimiva verkonvalvonta Laurea-ammattikorkeakoululle Laurean IT-henkilökunnan verkon ylläpitämisen helpottamiseksi. Tavoitteena on saada aikaan toimiva ratkaisu ”avaimet käteen” -periaatteella Laurea-ammattikorkeakoululle.

Opinnäytetyön tekijöiden tavoite, on kasvaa ammattiosaamisen suhteen verkonvalvonnan ammattilaisiksi. Tekijöiden oppimisen kannalta kehittyviä osaamisalueita ovat verkonvalvonnan lisäksi verkostoituminen muiden saman järjestelmän asiantuntijoiden kanssa sekä Linux-pohjaisen toimintaympäristön tunteminen.

2 Termit

Tässä osassa opinnäytetyötä käydään läpi yleisimpiä tässä työssä esiintyviä termejä sekä käsitteitä.

2.1 RPM (RedHat Package Manager)

RPM on useissa Linux–jakeluissa käytettävä paketinhallintajärjestelmä. RPM–paketti sisältää asennettavan ohjelman pakattuna, sekä siihen liittyvät metadatat (riippuvuudet, versionumerot yms.)

RPM ei osaa käsitellä verkossa olevia pakettivarastoja, joten käytännössä lähestulkoon kaikki RPM – jakelut käyttävät jotain paketinhallintaohjelmaa, joka osaa hakea aina uusimman ver-

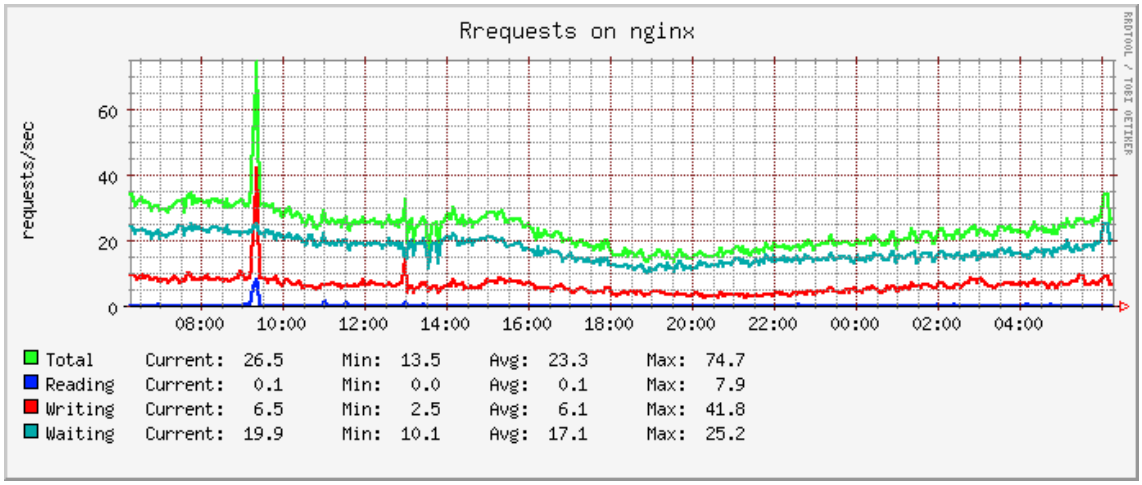
sion halutusta ohjelmasta verkossa olevasta pakettivarastosta käsin. (Foster-Johnson 2005, RedHat RPM –guide, Fedora project.)

2.2 RRDTool (Round Robin Database Tool)

RRDtool käyttää Round Robin-tietokantatyökalua. Round Robin on tekniikka, jossa tietokannan koko määritellään etukäteen tietynlaiseksi. Tämä on helpoiten selitetty käyttämällä vertauksena ympyrää, jonka reunalla on tiettyjä etukäteen määriteltyjä pisteitä. Nämä pisteet ovat paikkoja, joihin tietoa voidaan säilöä. Jos piirretään viiva ympyrän keskeltä yhteen näistä pisteistä, saadaan osoitin. Kun johonkin tiettyyn pisteeseen kirjoitetaan tietoa, tai pisteestä luetaan tietoa, osoitin siirtyy automaattisesti ympyrällä seuraavaan kohtaan. Koska olemme ympyrässä, ei informaatiolle ole erikseen määriteltyä alkua tai loppua. Kun osoitin on tehnyt täydellisen ympyrän määritellyissä tiedontallennuspaikoissa, alkaa se automaattisesti käyttää vanhoja tallennuspaikkoja uudestaan. Tämän ansiosta tietokanta ei kasva suunnattoman suureksi, eikä näin ollen vaadi niin paljon ylläpitoa. RRDtoolia käytetään varsinkin silloin, kun halutaan valvoa jotain tiettyä asiaa pitkällä aikavälillä (esimerkiksi suorittimen rasitusta, kovalevytilaa, käyttäjämääriä). RRDtoolia käytetään yleisesti graafisten käyrien toteuttamiseen verkonvalvonnassa. (Oetiker, RRDTool dokumentointi.)

RRDtool on saanut alkunsa halusta parantaa MRTG:n (Multi Router Traffic Grapher) tarjoamia ominaisuuksia. MRTG sai alkunsa pienestä skriptistä, jota käytettiin yliopistomaailmassa yliopiston Internet-yhteyden tilan graafiseen esittämiseen. MRTG:ä käytettiin myös muiden tietojen graafiseen esittämiseen (lämpötila, nopeus, volttien käyttö, printtien määrä jne). (Oetiker, RRDTool dokumentointi.)

RRDtoolia käytetään yleensä yhdessä SNMP:n kanssa. SNMP hoitaa tiedon keräämisen ja lähettämisen RRD-tietokantaan jossa sitten tiedot kerätään talteen ja luodaan halutunlaiset graafiset esitykset etukäteen määritellyistä asioista (Kuvio 1).

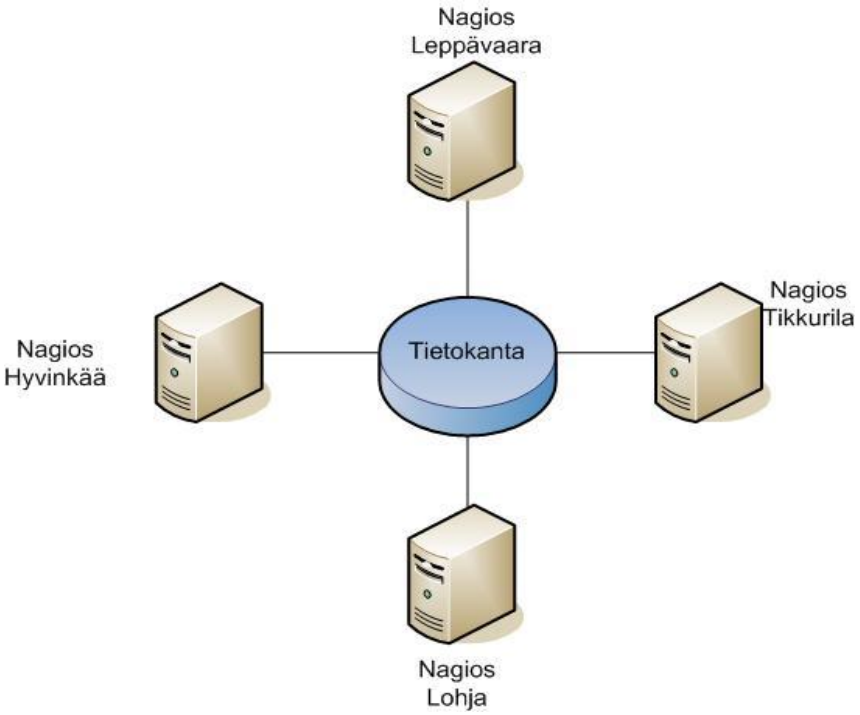


Kuvio 1. RRDTOOL graafinen käyrä

2.3 NDOutils

NDOutils on lisäominaisuus Nagiokseen, joka mahdollistaa konfiguraatiotietojen tallentamisen SQL-tietokantaan. Tällä hetkellä Nagioksessa itsessään ei ole mahdollisuutta tallentaa tietokantoihin vaan kaikki laitemääritykset täytyy tehdä käsin erillisiin konfiguraatiotiedostoihin. NDOutils onkin loistava työkalu Nagiosta käytettäessä, sillä SQL-tietokantojen käyttö mahdollistaa uusien laitteiden lisäämisen sekä vanhojen hallinnoinnin yksinkertaisen PHP-pohjaisen käyttöliittymän kautta. (Galstaad 2007, NDOUtils documentation.)

NDOutilsia tarvitaan myös RRDToolin toiminnassa. NDO tallentaa haetut tiedot RRD-tietokantaan (Kuvio 2).



Kuvio 2. Esimerkki tietokannan käytöstä

Jotta NDOutils osaa hallinnoida eri Nagios–ympäristöjen kokoonpanoja, tulee jokainen ympäristö nimetä eri lailla ja selvästi, jotta tiedetään mistä palvelimesta milloinkin on kyse. NDOutils sisältää neljä eri pääkomponenttia:

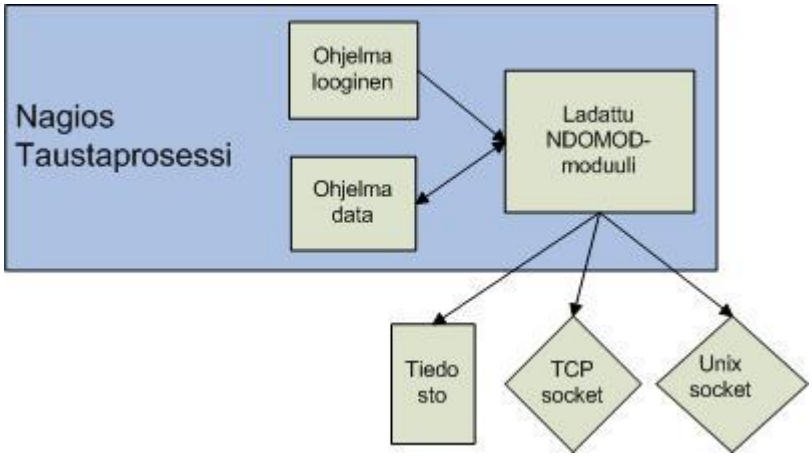
1. NDOMOD Event Broker Module
2. LOG2NDO Utility
3. File2Sock Utility
4. NDO2DB Daemon

Ndomod-moduuli noutaa dataa Nagioksen taustaprosessista. Nagios pitää konfiguroida ajamaan Ndomod-moduuli käynnistyessään. Kun moduuli on ladattu, pystyy se pääsemään käsiksi Nagioksen dataan sekä loogisiin määrityksiin. NDOutils pystyy kirjoittamaan Nagioksen dataa joko tiedostoon, TCP-socketiin tai Unix-Socketiin. (Galstaad 2007.)

LOG2NDO Utility mahdollistaa Nagioksen lokitiedostojen tuomisen NDO2DB-prosessiin. Työkalu lähettää lokitiedoston joko standarditiedostoon, Unix-socketiin tai TCP-socketiin sellaisessa muodossa, jota NDO2DB ymmärtää (Kuvio 3).

File2Sock Utility lukee standardimuotoisia tiedostoja ja lähettää näistä saadut tiedot joko TCP- tai Unix-socketiin.

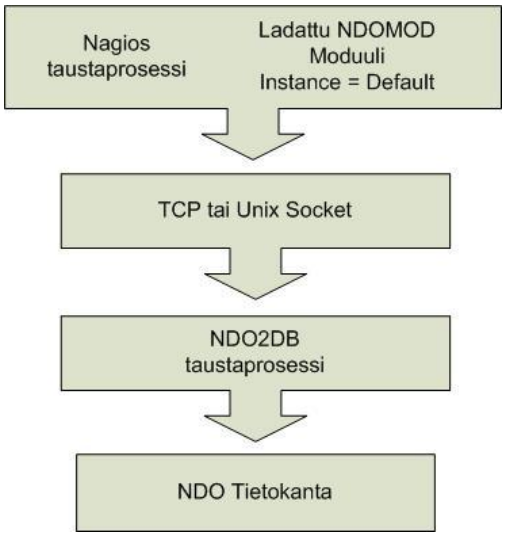
NDO2DB ottaa datan NDOMOD ja LOG2NDO komponenteista ja siirtää ne SQL-tietokantaan.



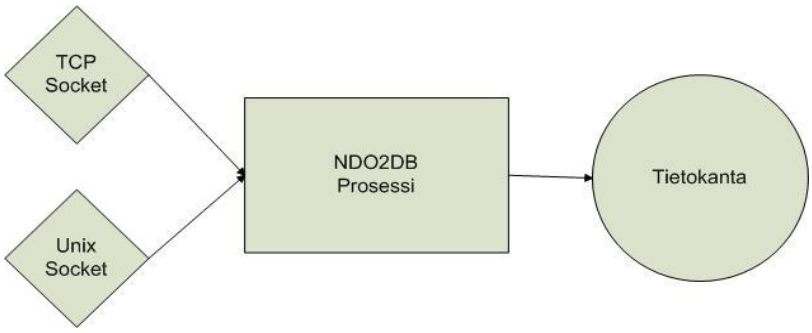
Kuvio 3. NDOutils toimintaperiaate

Alla kuvataan hieman jokaista vaihetta jonka NDOutils käy läpi toiminnassa ollessaan:

1. NDOMOD-moduuli konfiguroidaan Default-nimellä koska tässä esimerkissä ei ole käytössä kuin yksi Nagios – ympäristö.
2. Sillä aikaa kun Nagios on käynnissä valvomassa määriteltyä verkkoa NDOMOD–moduuli kerää tietoa ja lähettää kerätyn tiedon joko TCP- tai Unix-socketiin (luotu NDO2DB–taustaprosessin avulla)
3. NDO2DB–taustaprosessi lukee datan joka saapuu socketiin NDOMOD-moduulista.
4. NDO2DB–taustaprosessi suorittaa ja muuttaa datan joka on saatu NDOMOD-moduulista.
5. Prosessoitu data siirretään ja säilötään SQL-tietokantaa.(Kuviot 4 ja 5)



Kuvio 4. NDOutils toimintaperiaate 2



Kuvio 5. NDO2DB

2.4 Apache

Apache HTTP Server on WWW-palvelinohjelmisto joka on ollut avainasemassa Internetin kasvussa. Vuonna 2009 Apache oli ensimmäinen web-palvelinohjelmisto, joka ylitti 100 miljoonan nettisivun rajapyykin. Apache oli ensimmäinen varteenotettava vaihtoehto Netscape Communications Corporation web-palvelimelle.(The Apache Software Foundation 2009, Apache HTTP Server version 2.2 Documentation)

Apache perustuu avoimeen lähdekoodiin, joten sen käyttö on ilmaista. Tämä onkin oleellisesti vaikuttanut Apachen suosioon web-palvelinmarkkinoilla. Ohjelmiston ydintä voidaan laajentaa monilla erilaisilla lisämoduuleilla. Sellaisenaan palvelin ei tue muuta kuin staattisten tiedostojen jakamista HTTP-protokollan yli, mutta näiden lisämoduulien avulla Apacheen saadaan monia uusia ominaisuuksia. (The Apache Software Foundation 2009.)

2.5 MySQL (My Structured Query Language)

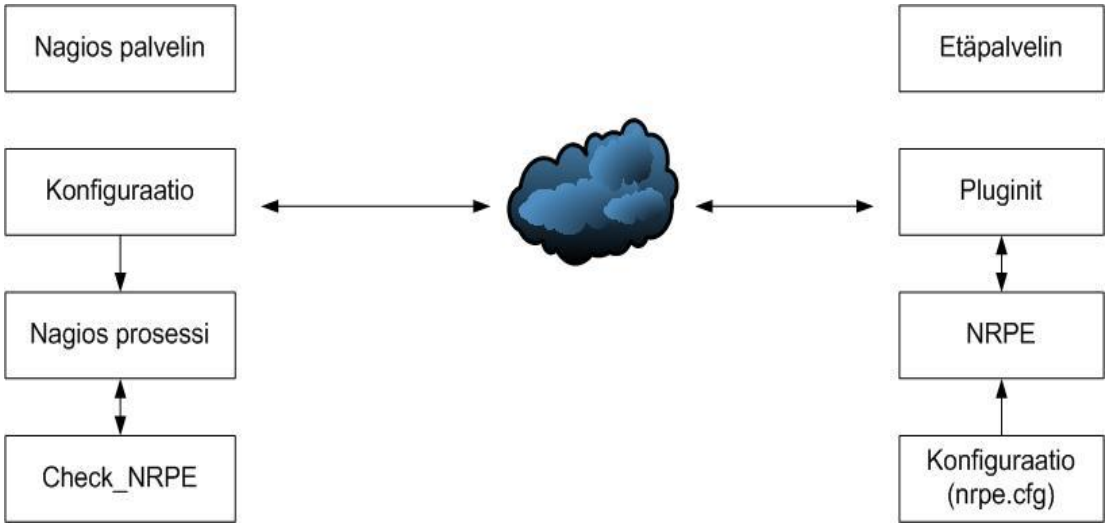
MySQL on ruotsalaisen MySQL AB:n kehittämä, vapaalla GNU GPL – lisenssillä toimiva tietokantaohjelmisto. MySQL on suosittu web-palveluiden tietokantaohjelmistona. Tietokannan päälle rakennettu ohjelmistologiikka suoritetaan yleensä PHP, Python tai Perl-kielellä, ja sivut julkaistaan Apache-palvelimella. Varsinkin PHP on ollut avainasemassa MySQL:n suosion kasvussa, sillä nämä ohjelmistot yhdistetään yleensä toisiinsa.(MySQL AB 2008, MySQL 5.4 Reference Manual.)

Oletuksena MySQL ei sisällä graafista käyttöliittymää, vaan tietokantojen hallinta tapahtuu komentoriviä hyväksi käyttäen. Graafista käyttöliittymää varten tarvitsee asentaa lisäohjelma

MySQL:n päälle. Suosittuja graafisia käyttöliittymiä ovat MySQL Administrator, MySQL Query Browser sekä phpMyAdmin. (MySQL AB 2008.)

2.6 NRPE (Nagios Remote Plugin Executor)

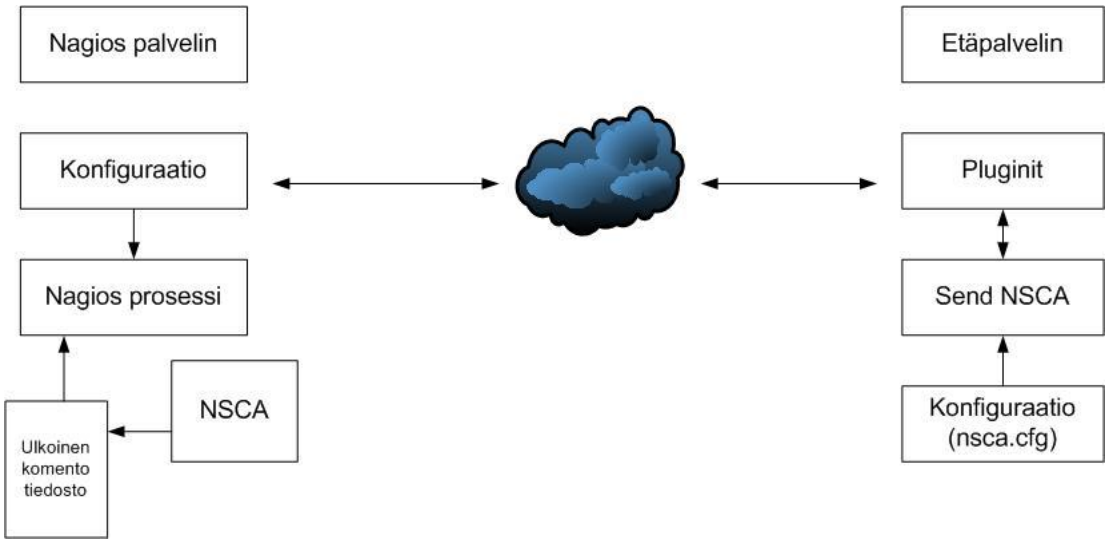
Nagios Remote Plugin Executor. Aktiivinen lisäosa joka mahdollistaa tarkistusohjelmien suorittamisen etäpalvelimella sijaitsevista kohteista. Nagios-palvelin antaa tarkastuksen suorituskäskyn ”Check_nrpe” – nimiselle lisäohjelmalle, joka lähettää tiedot verkon yli etäpalvelimelle asennetulle NRPE- prosessille. NRPE suorittaa etäpalvelimella tarkastusohjelman. Tarkastuksen tulos lähtee välittömästi samaa reittiä takaisin palvelimelle. (Kuvio 6) (Galstad 2007, NRPE documentation.)



Kuvio 6. NRPE toiminta

2.7 NSCA (Nagios Service Check Adaptor)

Nagios Service Check Adaptor. NSCA-tarkastusprosessi on passiivinen tarkastusprosessi. Etäpalvelimelle asennetaan ”send_nsca”-niminen passiivinen tarkastusprosessi, joka suorittaa etäpalvelimella tarkastuksia lisäohjelmien avulla. NSCA lähettää tarkastuksen tulokset Nagios palvelimelle. Tulokset otetaan vastaan ”NSCA” lisäosan avulla, joka kirjoittaa ne ulkoiseen komentotiedostoon. Nagios-prosessi konfiguroidaan lukemaan tätä komentotiedostoa tietyin väliajoin, näin ollen NSCA ei käytä suuria määriä palvelimen resursseja, koska se ei ole aktiivinen tarkastus. (Kuvio 7)



Kuvio 7. NSCA toiminta

3 Verkonhallinta

Jotta tietoverkot toimisivat niin kuin on tarkoitettu, mahdolliset vikatilanteet on pystyttävä kartoittamaan sekä korjaamaan mahdollisimman nopeasti. Tämä luo organisaatioissa tarpeen ainakin jonkin asteiselle verkonhallinnalle, joiden avulla verkon ylläpitäjät pystyvät ennalta-ehkäisemään vikatiloja. Hyvin toteutettu verkonhallinta mahdollistaa myös mahdollisten vikatilojen huomattavasti nopeamman diagnosoinnin, minkä ansiosta vikojen aiheuttamat ongelmat jäävät mahdollisimman lyhytaikaisiksi.

Verkonhallinnan tärkeyttä korostaa sekin, että nykypäivänä tietoverkkojen kehityksessä on havaittavissa se, että verkkojen kompleksisuus on lisääntynyt. Nykypäivän organisaatioissa verkot pitävät sisällään monien eri laitteiden sekä valmistajien yhdistelmiä. Tämä johtaa siihen, että verkossa on huomattavasti enemmän osa-alueita, jotka saattavat aiheuttaa vikoja.

Organisaation toiminnan kannalta erityisen tärkeää on myös se, että mahdolliset verkkoviat eivät näy käyttäjällä asti. Nykyisin organisaation toiminta saattaa lakata lähes kokonaan jos syystä tai toisesta organisaation tietoverkko ei olekaan käytössä.

Tietoverkon ylittäessä muutaman laitteen rajan, alkaa verkonhallinta ilman tähän tarkoitettuja työkaluja olla melko tehotonta. Verkonhallintaan on olemassa monia erilaisia automatisoituja työkaluja jotka helpottavat nykyisten verkkojen valvontaa. Varsinkin jos organisaatiossa

on usean eri valmistajan laitteita, automaattisen verkonhallinnan merkitys kasvaa huomattavasti.

3.1 Verkonhallinnan vaatimukset

Verkonhallinnalle voidaan asettaa monia eri vaatimuksia tarkastusnäkökulman mukaan. Peruskäyttäjällä on erilaiset tarpeet verkonhallinnalle kuin esimerkiksi ylläpitäjällä. ITU-T (International Telecommunication Union) X.700 dokumentoinnissa verkonhallinnan vaatimukset on jaettu viiteen eri osa-alueeseen.

3.1.1 Vikojen hallinta (Fault Management)

Verkon ylläpitäjän on pystyttävä paikallistamaan täsmällisesti mistä vian syy johtuu. Ylläpitäjän on myös hyvä nähdä vian mahdollisesti aiheuttamat muutokset verkon toimintaan sekä tarpeen vaatiessa pystyttävä eristämään vikaa aiheuttava laite muusta verkosta. Ylläpitäjän tulee saada selville verkon normaaliksi palautuminen vian korjauksen jälkeen.

Toimintatapa vikaantumisen havaitsemisen jälkeen tulisi olla seuraavanlainen:

1. Paikallistetaan vian sijainti
2. Eristetään muu verkko viasta mahdollisesti aiheutuvista ongelmista
3. Konfiguroidaan verkko siten, että saadaan minimoitua jonkun tietyn komponentin hetkellisen poissaolon aiheuttamat vaikutukset
4. Korjataan tai vaihdetaan viallinen komponentti

3.1.2 Käytön hallinta (Account Management)

Verkon ylläpitäjän on pystyttävä seuraamaan verkossa tapahtuvaa liikennettä käyttäjä sekä käyttäjäryhmäkohtaisesti. Monissa organisaatioissa verkon käyttäjiä tai osastoja laskutetaan verkon palvelujen käytöstä. Vaikka laskutusta ei organisaation sisäisesti tapahtuisikaan, on ylläpitäjän hyvä pystyä seuraamaan verkon resurssien käyttöä, koska käyttäjät voivat käyttää väärin oikeuksiaan, ja tästä johtuen kuormittaa verkkoa muiden käyttäjien kustannuksella. Lisäksi käyttäjät voivat käyttää verkkoa tehottomasti, tämän huomaaminen mahdollistaa sen, että ylläpitäjä voi opastaa heitä mahdollisessa toimintatapojen muuttamisessa. Ylläpitäjän on myös huomattavasti helpompi suunnitella mahdollisia verkon laajennuksia.

Käytön hallinnan ensisijainen etu on se, että saadaan tarkka selvyys siitä mitä verkon tarjoamia resursseja käytetään eniten, tämä mahdollistaa mahdollisten investointien tekemisen oikeille verkon osa-alueille.

3.1.3 Kokoonpanon hallinta (Configuration Management)

Kokoonpanon hallinnan ensisijainen tehtävä on mahdollistaa verkossa olevien laitteiden käynnistäminen sekä pysäyttäminen tarpeen mukaan. Toivottavaa on se, että nämä toimenpiteet pystytään tekemään ajastetusti esimerkiksi aina tiettynä päivänä tai tiettyyn kellon aikaan.

Ensisijainen etu kokoonpanon hallinnassa on se, että tämä mahdollistaa verkon loogisen rakenteen muuttamisen suhteellisen helposti. Esimerkkinä voidaan ottaa mahdollinen vikatilanne jonka aiheuttamien ongelmien minimoimiseksi tulee muuttaa laitteiden reititystä jollakin tavalla.

3.1.4 Suorituskyvyn hallinta (Performance Management)

Useimmissa verkoissa laitteet käyttävät verkosta saatuja resursseja, juuri tämä resurssien jakaminen on usein ollut syynä verkon rakentamiseen. Suorituskyvyn hallinta koostuu kahdesta eri osa-alueesta jotka ovat valvonta sekä hallinta. Valvonnalla tarkoitetaan verkon liikenteen tarkkailua ja hallinnalla tarkoitetaan sitä, että ylläpitäjällä on käytössään välineet verkon asetuksien säätämiseksi. Tämä jälkimmäinen osa-alue kulkee osittain käsi kädessä kokoonpanon hallinnan kanssa. Erona suorituskyvyn hallinnassa on se, että se on enemmänkin hienosäätöä kuin varsinainen kokoonpanon hallinta.

3.1.5 Turvallisuuden hallinta (Security Management)

Turvallisuuden hallinnalla tarkoitetaan verkkoon ja siihen liitettyihin laitteisiin pääsyn seurantaa sekä kontrollointia. Turvallisuuden hallinta on pääosin erilaisten lokitiedostojen keräämistä, tallennusta ja tutkimista.

3.2 Verkonhallinnan standardit ja protokollat

Verkonhallintaan liittyen on useita vakiintuneita standardeja. Alla olevissa luvuissa käydään hieman tarkemmin läpi niitä standardeja sekä protokollia, joita tässä opinnäytetyössä käytettiin.

3.2.1 SNMP (Simple Network Management Protocol)

SNMP (Simple Network Management Protocol) on tietoliikenneprotokolla, jota käytetään TCP/IP – verkkojen hallintaan. Protokolla toimii OSI-mallin(Open Systems Interconnection Reference Model) 7. kerroksessa (application layer). SNMP viittaa joukkoon verkonhallinta-standardeja, joita ovat itse protokolla SNMP, tietokannan rakenteen kuvaus MIB (Management Information Base), sekä joukko tieto-olioita SMI (Structure of Management Information). (Jaakohuhta & Lahtinen 1997: 494.) SNMP:n avulla voidaan kysellä verkossa olevien laitteiden tilaa tai vaihtoehtoisesti laite pystyy antamaan hälytyksiä itsenäisesti. Tällä hetkellä SNMP:tä on olemassa kolme eri versiota: SNMPv1, SNMPv2 sekä SNMPv3. Perusidea kaikessa SNMP-protokollaan perustuvassa verkonhallinnassa on se, että verkossa on joukko SNMP:llä hallinnoitavia laitteita, SNMP-agentteja, joiden tilaa voidaan tutkia ja joita voidaan konfiguroida SNMP-verkonhallinta-aseman kautta (Kimmo Kaario 2002, TCP/IP-verkot s. 270.) SNMP käyttää UDP-protokollaa (User Datagram Protocol), tämä mahdollistaa mahdollisimman pienen rasituksen SNMP:n puolesta verkkoon. SNMP:ssä käytetään kahta UDP-porttia (161 ja 162). Porttia 161 käytetään kyselyiden tekemiseen ja 162 porttia käytetään hälytyksiin. SNMP on nykyisin yleisin TCP/IP-verkkojen hallintaan tarkoitettu työkalu ja se määritellään useissa RFC-dokumenteissa (RFC3411, RFC3412, RFC3413, RFC3414, RFC3415, RFC3416, RFC3417, RFC3418)

TCP/IP – verkkojen alkuaikoina verkonhallintaan ei kiinnitetty riittävästi huomiota. Enimmäkseen vikatilojen etsintään sekä suorituskyvyn analysointiin käytettiin ICMP-protokollaa (Internet Control Message Protocol). Tätä protokollaa käytettäessä mahdollisuudet ovat hyvin rajoitetut varsinkin silloin, kun erityyppisiltä verkkolaitteilta pitäisi kerätä monenlaista tietoa syvällisempää verkonhallintaa varten. (Kaario 2002 s.271.)
TCP-IP – verkonhallintamallissa on neljä perusosaa:

1. Hallinta-asema (Management Station)
2. Hallinta-agentti (Management Agent)
3. Hallintatietokanta (Management Information Base, MIB)
4. Verkonhallinnan yhteyskäytäntö (Network-management protocol)

Hallinta-asemassa ajetaan yleensä jonkinlaista verkonhallintajärjestelmää, joka mahdollistaa tiedon analysoinnin, vikailmoitukset, vikojen korjaamisen ja niin edelleen. Tähän järjestelmään kuuluu yleensä myös jonkinlainen ohjelmisto verkon hallintaa ja valvontaa varten. Tässä projektissa juuri Nagios toimii tuona verkonhallintajärjestelmänä.

Hallinta-agentti on verkossa oleva laite (esimerkiksi palvelin, printteri, reititin) jonne on SNMP toteutettu siten, että sitä voidaan hallinnoida verkonhallintajärjestelmästä käsin.

Hallittavia resursseja kuvataan olioina. Joukkoa näitä olioita kutsutaan hallintatietokannaksi (Management Information Base).

Hallinta-asemat ja hallinta-agentit liitetään yhteen verkonhallinnan yhteyskäytännön (Network-management protocol) avulla. SNMP:llä on käytössään seuraavanlaiset perusoperaatiot:

1. Lukeminen: Haetaan agentin olioiden arvoja
2. Kirjoittaminen: Asetetaan agentin olioiden arvo
3. Ilmoitus: Ilmoittaa verkon tapahtumista hallinta-asemalle.

SNMP:n suurin puute on turvallisuus – SNMP:n käytössä piilee aina suuria tietoturva-aukkoja. SNMP:n uusin 3-versio korjaa periaatteessa suurimmat tietoturva-aukot, mutta käytännössä SNMPv2 on edelleen yleisesti käytössä ja tietoturva SNMP-verkonhallinnan yhteydessä ei ole tämän takia aina parasta mahdollista. (Kaario 2002 s.273).

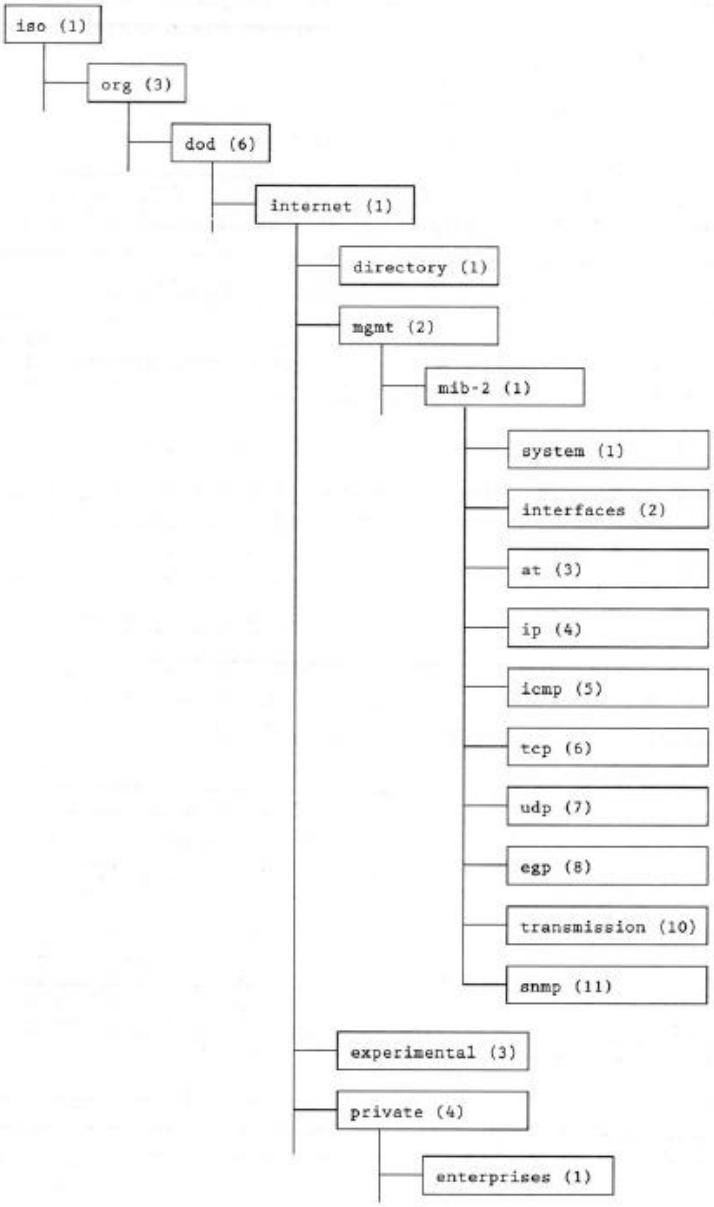
SNMP on suunniteltu ja standardisoitu vain IP-verkkojen valvontaan ja hallintaan. Vaikka suurin osa verkoista on IP-pohjaisia, on olemassa muitakin protokollia. Näiden valvomiseen SNMP ei ole ideaali.

Laajoissa tietokantahauissa SNMP aiheuttaa verkkoon suurta liikennettä, sillä SNMP:ssä tuetaan vain yksinkertaisia hakuja, joka johtaa siihen että on mahdollista palauttaa vain yksi tieto kerrallaan yhdessä kyselyssä. Otetaan esimerkiksi tietokanta jossa on 4000 riviä sisältävä taulu, ja jokainen rivi aiheuttaa 6 erilaista kyselyä saadaan esimerkiksi Get-request ja Get-response viesteillä 4x6x4000 = 96000 pakettia.

3.2.2 MIB (Management Information Base)

MIB eli Management Information Base on hallintatietokanta joukolle objekteja (olioita) jotka SNMP määrittää. MIB määrittää verkonhallinnassa käytetyt objektit puumaiseksi rakenteeksi (Kuvio 8). Tietokanta muodostuu hallintaobjekteista joilla tarkoitetaan object-id ja object-value paria. Tietokantarakenteen oikeanlaisen toiminnan kannalta on sen tuettava kahta vaatimusta:

1. Resurssia kuvaavien objektien tulisi olla samanlaisia kaikissa järjestelmissä
2. Objektien määrittelemiseksi täytyy olla yhteinen sovittu menetelmä



Kuvio 8. MIB puurakenne

Määritetyt tiedot tallennetaan MIB-kantaan josta ne sitten luetaan tietojen hyväksikäyttämisen yhteydessä. MIB määrittelee perustyypit joita SNMP:tä tukevien laitteiden on tuettava toimiakseen (McClogherie 1991.)

Perusstandardissa määritetään 10 eri hallintaobjektia:

- System: Yleisinformaatio
- Interfaces: Tiedot laitteen rajapinnoista
- AT: Osoitteenmuutostaulukkoihin liittyvä informaatio
- IP: IP -protokollan toteutus- ja suoritusaikainen informaatio
- ICMP: ICMP -protokollan toteutus- ja suoritusaikainen informaatio
- TCP: TCP -protokollan toteutus- ja suoritusaikainen informaatio
- UDP:UDP -protokollan toteutus- ja suoritusaikainen informaatio
- EGP: EGP -protokollan toteutus- ja suoritusaikainen informaatio
- DOT3: DOT3 -protokollan toteutus- ja suoritusaikainen informaatio
- SNMP: SNMP -protokollan toteutus- ja suoritusaikainen informaatio

3.2.3 RMON (Remote Network Monitoring)

RMON on kehitetty vuonna 1995 paikkaamaan SNMP:n puutteita. RMON mahdollistaa kokonaisen verkkosegmentin hallinnan, kun perustietokannoilla pystytään vain yksittäisten verkkolaitteiden tarkasteluun. Sekä SNMP, että RMON käyttävät objektien tarkastelussa erinäisiä agentteja, joita kutsutaan yleisesti nimellä tiedonkeruuyksikkö (probe). Tällä tarkoitetaan ohjelmistoa tai erillistä laitetta joka on sijoitettu johonkin verkon laitteeseen keräämään tietoa liikenteestä ja tallentamaan tämän kerätyn tiedon MIB-kantaan. RMONin voi asentaa mihin verkon laitteeseen vain, yleisimmin se asennetaan kytkimeen tai reitittimeen. RMON1:lla on kymmenen objektiryhmää joiden avulla kerätyn tiedon mukaan voidaan tehdä päätelmiä verkon tilasta (Waldbusser 2000):

1. Tilastot: Jatkuva lähiverkon statistiikka
2. Historia: Valittujen tietojen historia
3. Hälytykset: Määritykset RMON SNMP-laukaisimille
4. Koneet: Lähetetyt/Vastaanotetut kehykset
5. Yhteyksien määrä: Aktiivisten yhteyksien määrä
6. Matriisi: Eri järjestelmien välillä vastaanotettu/lähetetty liikenne
7. Suodatus: Määritellyt paketit esim. kiinnostavista MAC-osoitteista
8. Kaappaus: Kerää ja lähettää uudelleen etukäteen määriteltyjä paketteja
9. Tapahtumat: Lähettää hälytyksiä tiettyjen tapahtumien yhteydessä
10. Token Ring: Laajennukset token ring-verkkojen toimintojen määrittämiseksi.

RMON2 laajentaa kymmenen lisäryhmää hallintatietoihin:

- Protokolla hakemisto (Protocol Directory): Lista protokollista, joita probe voi monitoroida
- Protokollien levittämä liikenne (Protocol distribution): Liikennetilastot jokaisesta käytetystä protokollasta
- Osoitekartta (Address map): Kartat verkkokerroksen IP-osoitteista MAC-osoitteisiin.
- Verkkokerroksen koneet (Network-layer hosts): Verkkokerroksen liikenneanalyysi koneittain
- Verkkokerroksen matriisi (Network-layer matrix): Verkkokerroksen liikennetilastot lähde- ja kohdepareittain
- Ohjelmistokerroksen koneet (Application-layer hosts): Liikennetilastot, ohjelmistoprotokollittain konekohtaisesti
- Ohjelmistokerroksen matriisi (Application-layer matrix): Liikennetilasto ohjelmistoprotokollittain, kohde- ja lähde laitepareittain
- Käyttäjähistoria (User history): Ajoittaisia näytteitä käyttäjien luomasta liikenteestä.
- Probe:n asetukset: Laitteiden asettaminen etänä
- RMON määrittely: Vaatimukset RMON2 MIB:n noudattamiseksi (Waldbusser, 2000.)

4 Nagios

4.1 Johdanto

Nagioksen historiaa; vuonna 1999 julkaistiin sovellus nimeltä Netsaint, jonka nimi muutettiin myöhemmin tuotemerkkisyistä Nagiokseksi. Ohjelman kehitys lähti liikkeelle tarpeesta tuottaa valvontapalveluja pienelle lähiverkolle ilman suuria kustannuksia. Nagioksen alkuperäinen visionääri ja kehittäjä on henkilö nimeltä Ethan Galstad. Nagios on historiansa varrella käynyt läpi yhdeksän suurta versiomuutosta (Galstad 2009).

Nagiosta käytetään kymmenissä tuhansissa yrityksissä ja organisaatioissa ympäri maailman. Suurimmat verkot joissa käytetään Nagiosta valvontatyökaluna sisältävät tuhansia koneita.

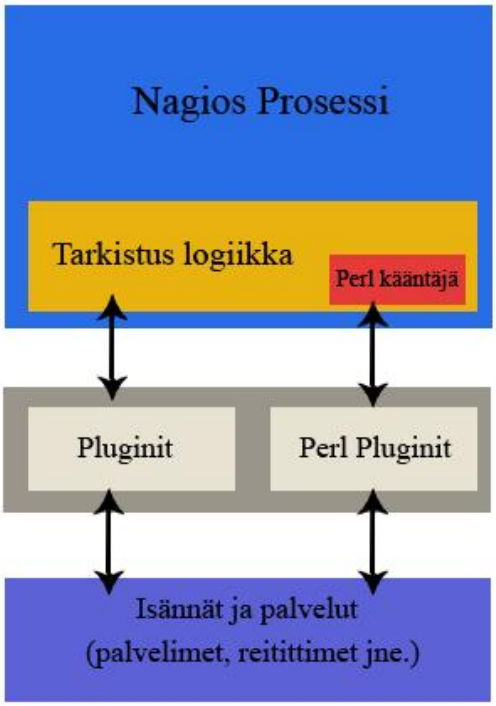
Nagioksella voidaan valvoa kaikkia lähiverkossa toimivia laitteita, joilla on jokin verkko osoite, yleensä IP- osoite. Esimerkiksi verkon aktiivilaitteet, palvelimet, tulostimet, ja työasemat pystytään valvomaan Nagioksella. Nagioksen kannalta valvottavat laitteet jaetaan kahteen ryhmään, palvelimet (host) ja palveluihin (services). Palvelimiksi lasketaan kaikki fyysiset

laitteet verkkokytkimistä työasemiin. Palveluiksi lasketaan puolestaan palvelimilla tuotettuja asioita, esim. DNS- palvelut (Domain Name Service) tai jokin palvelimen tai muun laitteen ominaisuus. Tässä vaiheessa on hyvä muistaa, että jokainen palvelu liittyy johonkin palvelimeen.

Nagiokseen voidaan määritellä myös ominaisuus joka mahdollistaa automaattisen sähköpostin tai tekstiviestin lähettämisen ennalta määritellyille tahoille vikatilanteiden ilmetessä (Galstad 2009).

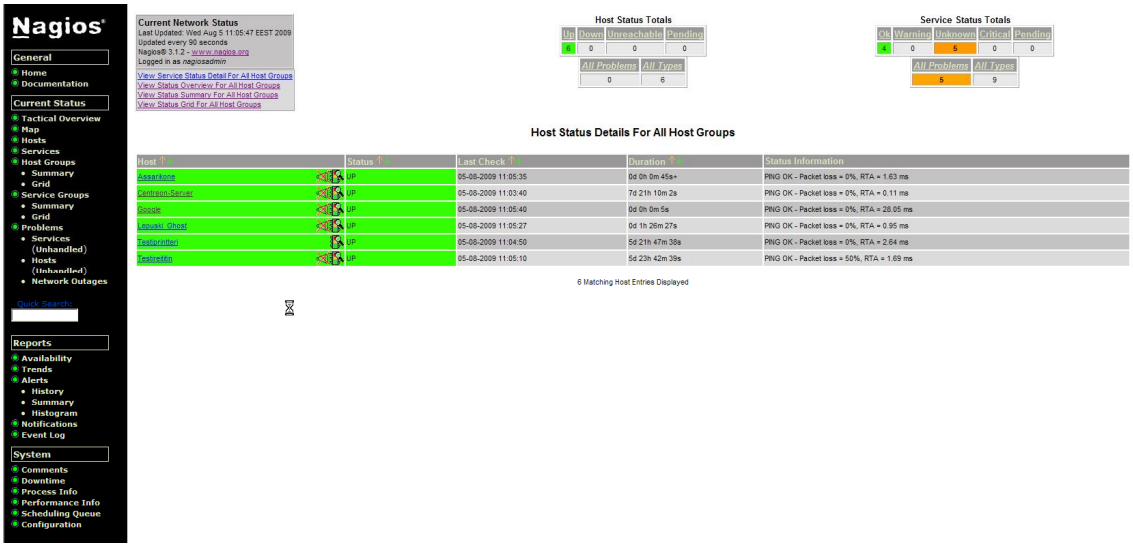
4.2 Nagioksen toimintaperiaate

Nagios on modulaarinen ohjelma. Modulaarisella ohjelmalla tarkoitetaan sitä, että Nagios koostuu pienemmistä osioista, jotka on linkitetty pääohjelmassa yhteen pakettiin. Nagios käyttää niin sanottuja plugineja, jotka ovat mahdollisia käyttäjän / ylläpitäjän itse asentamia lisäominaisuuksia ohjelmaan. Pluginit ovat ajettavia scriptejä jotka on ohjelmoitua hyväksikäyttäen Perliä. Lisäksi Nagioksesta voidaan poistaa oletuksena asennettavia ominaisuuksia joita ylläpitäjä ei näe tarpeelliseksi. Nagios -taustaprosessin tarkoituksena on koordinoida mahdolliset etukäteen määritellyt tarkastukset, prosessi pitää myös sisällään mahdolliset monitoroitavat laitteet. Mahdollisesti tehtävät tarkastukset ajetaan ulkoisia sovelluksia hyväksi käyttäen joita tämä Nagioksen prosessi kutsuu sekä hallinnoi (Kuvio 9). Nykyisissä versioissa Nagioksen oletusasennus pitää sisällään huomattavan määrän näitä tarkastusohjelmia.



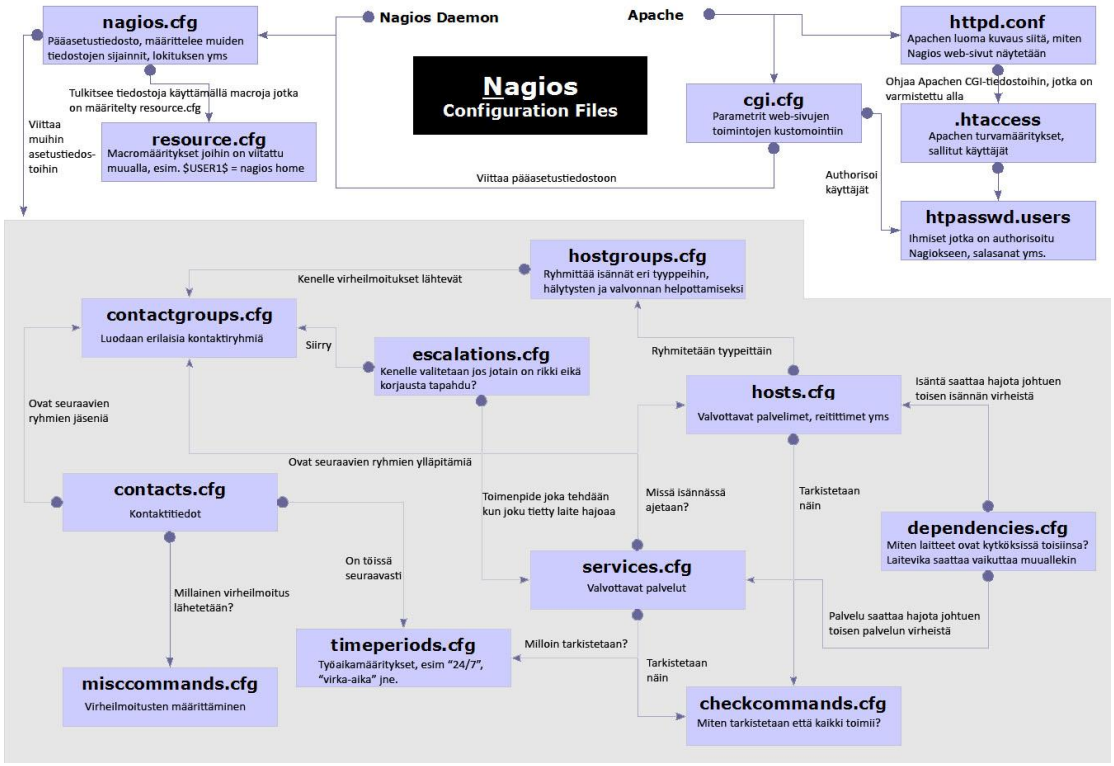
Kuvio 9. Pluginien toimintaperiaate

Tarkastussovellukset suorittavat niille määritellyt komennot, sekä tämän jälkeen lähettävät Nagiokseen tarkastustuloksen sekä mahdollisesti tähän tarkastukseen liittyvät lisätiedot. Nagiokseen syötettyjä laitteita sekä näistä kerättyjä tietoja voidaan tarkastella yksinkertaisen WWW-liittymän kautta (Kuvio 10). Mahdollisten ongelmatapauksien ilmetessä saadaan mahdollistettua automaattisten hälytysten lähettäminen ylläpitäjille joko sähköpostia, tai SMS –viestiä hyödyntäen.



Kuvio 10. Nagios WWW-käyttöliittymä

Nagioksen toiminta perustuu suurilta osin erinäisiin asetustiedostoihin sekä näiden muokkaamiseen. Centreon–asennus joka tähän projektiin otettiin käyttöön vähentää huomattavasti manuaalista asetustiedostojen editoinnin tarvetta. Tästä johtuen emme käy kovinkaan syvällisesti läpi jokaista asetustiedostoa sekä niitä muutoksia joita näihin pystytään tekemään. Alla olevassa kuvassa on selitetty miten asetustiedostot on linkitetty toisiinsa (Kuvio 11). Kuva sisältää myös lyhyet selitykset jokaisen asetustiedoston tarkoituksesta.



Kuvio 11. Nagios asetustiedostot

4.3 Makrot

Suurin syy, joka tekee Nagioksesta hyvinkin joustavan ohjelman on erilaisten makrojen käytön mahdollisuus. Makrot mahdollistavat laitetietojen käytön tarkastuskomentoja käytettäessä. Ennen kuin Nagios ajaa jonkin komennon, korvaa se mahdolliset makrot joita komennossa näkyy etukäteen määritellyillä arvoilla.

Esimerkki makron käytöstä:

Kun käytetään Host, tai Service makroja komentojen määrittelyissä, viittaavat ne automaattisesti siihen laitteeseen johon tarkastusta ajetaan.

Define host {

Host_name	*linux-kone*
Address	*192.168.2.10*
Check_command	*check_ping*

...

}

Define command {

Command name check_ping

Command_line /usr/local/nagios/libexec/chec_ping –h $HOSTADRESS -w 100.0,90% -c 200.0,60%

Lopullinen komento jonka Nagios ajaa:

/usr/local/nagios/libexec/check_ping –H 192.168.2.10 –w 100.0,90% -c 200.0,60%

Tämä mahdollistaa sen, että check_ping-komentoa voidaan ajaa mihin tahansa laitteeseen, koska laitteen IP-osoite on määritetty define_host-kohdassa. Käyttämällä $hostadress-makroa korvataan tämä kohta automaattisesti sen laitteen IP-osoitteella, jolle tarkistus halutaan suorittaa.

4.4 Nagios-tilatyypit

Nagios sisältää erilaisia tiloja valvottaville laitteille. Tarkistettavan kohteen tila muodostuu kahdesta eri asiasta, jotka ovat: tila (OK, Warning Critical ja Unknown) sekä kyseisen tilan tyyppi (Hard ja Soft). Nämä tilatyypit vaikuttavat olennaisesti Nagioksen toimintaan, koska näiden perusteella lähetetään mahdolliset ilmoitukset sekä ajetaan tapahtumien käsittelijät.

Jotta saadaan vähennettyä liiallisten vikailmoituksien lähettämistä, Nagioksessa pystytään määrittelemään, kuinka monta kertaa jokin tietty palvelu on saavuttamattomassa tilassa (esimerkiksi ping ei kulje läpi), ennen kuin katsotaan, että laite tai palvelu on viallinen. Tätä kontrolloidaan max_check_attempts-komennolla palvelumäärityksissä.

Soft – tila:

Soft tila muodostuu, kun valvottava toiminto ei anna halutunlaista lopputulosta, eikä tarkistusta ole suoritettu yhtä monta kertaa kuin se on määritelty max_check_attempts–kohdassa. Tällöin muodostuu soft-error. Kun valvottava laitteisto palautuu normaaliksi ennen kuin max_check_attempt–kohdassa määritelty tarkastuksien määrä tulee täyteen, muodostuu soft-recovery. Yllä mainitussa tilanteessa Soft–errorista muodostuu vain merkintä lokitiedostoihin joita ylläpitäjä pystyy tarkastelemaan. Tässä tilanteessa ei lähetetä virheilmoituksia tekstiviestillä tai sähköpostilla.

Soft tilassa oleviin laitteisiin pystytään määrittelemään etukäteen ns. event handlerit, jotka ajavat tietyn komennon tämän tilan tullessa ilmi (esimerkiksi käynnistävät laitteen uudestaan). Tämä mahdollistaa sen, että järjestelmä korjaa automaattisesti valvotun laitteen ennen kuin siitä lähtee ilmoitusta ylläpitäjälle.

Hard–tila:

Hard–tila muodostuu kun valvottava laite ei anna halutunlaista lopputulosta, ja max_check_attempts–kohdassa määritelty tarkistusten määrä tulee täyteen tai tila muuttuu OK–muotoisesta joko warning tai critical-muotoon. Hard–tilassa olevaan laitteeseen pystytään myös määrittelemään event handlerit, jotka yrittävät korjata vian automaattisesti. Hard–tilassa olevista laitteista lähtee ilmoitus ylläpitäjille.

Tilatyyppien toiminnasta löytyy esimerkki allaolevasta kuvasta (Kuvio 12).

Aika	Tarkistusten määrä	Tila	Tilatyyppi	Tilan muutos	Toiminto
0	1	OK	HARD	Ei	Palvelun alkuperäinen tila
1	1	CRITICAL	SOFT	KYLLÄ	Ensimmäinen havainto virheestä, event handlerit ajetaan.
2	2	WARNING	SOFT	KYLLÄ	Palvelu ei korjaannu
3	3	CRITICAL	HARD	KYLLÄ	Maksimi tarkastusten määrä saavutetaan, palvelu siirtyy HARD-tilaan. Event handlerit ajetaan ja ilmoitukset lähetetään.
4	1	WARNING	HARD	KYLLÄ	Palvelu muuttuu HARD-WARNING tilaan, ilmoitukset lähetetään.
5	1	WARNING	HARD	Ei	Palvelu pysyy HARD-WARNING tilassa. Riippuen ilmoituksien lähetysvälistä joko lähetetään uusi virheilmoitus tai ei.
6	1	OK	HARD	KYLLÄ	Palvelu palaa normaaliksi, tapahtuu HARD recovery. Palvelun palautumisesta lähetetään ilmoitus.
7	1	OK	HARD	Ei	Palvelu OK vieläkin.
8	1	UNKNOWN	SOFT	KYLLÄ	Palvelu muuttuu SOFT -NON OK tilaan (virheen laadusta ei vielä tietoa). Logeihin kirjoitus eikä lähetetä virheilmoitusta.
9	2	OK	SOFT	KYLLÄ	Palvelu palaa normaaliksi, tapahtuu SOFT recovery. Ei virheilmoitusten lähetystä.
10	1	OK	HARD	Ei	Palvelu OK.

Kuvio 12. Tilatyyppien toiminta

4.5 Laitteisto ja ohjelmistovaatimukset

Nagios on suunniteltu toimimaan Linux- ja Unix-käyttöjärjestelmissä, ja nykyään se sisältyy myös suosittuihin Linux–jakeluihin, kuten esimerkiksi Opensuseen, jota käytettiin kyseisessä projektissa. Laitteistovaatimuksiltaan Nagios ei vaadi kovin paljoa. Palvelu saadaan toimimaan vanhemmissakin koneissa ilman suurempia ongelmia. Nagios vaatii toimiakseen myös asennetun ja konfiguroidun Web-palvelimen. Suositelluin ja eniten käytetty web-palvelinohjelmisto on Apache, joka otettiin tässäkin projektissa käyttöön.

4.6 Nagioksen ja Centreonin asentaminen

Tässä kappaleessa käydään läpi Nagioksen ja Centreonin asennuksen eri vaiheet. Tarkempi dokumentaatio asennuksesta löytyy tämän opinnäytetyön liitteistä. Nagios tarvitsee useita lisäohjelmia toimiakseen. Kyseiset ohjelmat ovat: sudo, mailx, fping, iputils, dos2unix, vron, dejavu, gcc, gcc-c++, apache2, php5-mysql, apache2-mod_php5, php5-pear, php5-ldap, php5-

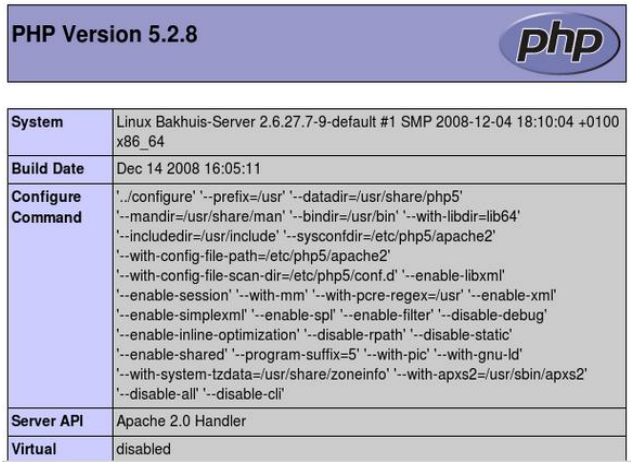
snmp, php5-gd, php5 –soap, php5-posix, php5-gettext, php5-mbstring, php5-session, php5-xml, mysql, libmysqlclient15-devel, perl-dbd-mysql, phpmyadmin, rrdtool, perl-Config-IniFiles, net-snmp, perl-Net-SNMP, perl-SNMP, gd, libjpeg-devel, libpng-devel, fontconfig-devel, freetype2-devel. Ohjelmien asennuksesta sekä käyttötarkoituksesta löytyy tarkempaa tietoa tämän opinnäytetyön liitteissä olevasta asennusohjeesta sekä opinnäytetyön termit–osiosta. Järkevää on asentaa yllä olevat ohjelmat ennen Nagioksen asennuksen aloittamista, näin vältytään monilta asennuksen aikana ilmeneviltä ongelmilta. Ennen siirtymistä asennuksen seuraavaan vaiheeseen on suositeltavaa, että tarkistetaan kriittisten apuohjelmien toimivuus. Tärkeimmät ovat Apache, PHP sekä Mysql.

Apachen toimivuuden tarkistaminen onnistuu seuraavasti: avataan selain, sekä syötetään osoite – kenttään paikallinen IP – osoite 127.0.0.1, jos Apache – palvelin on toiminnassa ilmestyy ruudulle It works! – teksti.

PHP:n toimivuuden tarkistamiseen täytyy luoda pienimuotoinen scripti. Luodaan index.php – niminen tiedosto Apachen kotikansioon. Tiedostoon syötetään seuraava teksti:

```
<?php
   phpinfo();
?>
```

Tämän jälkeen syötetään taas selaimeen IP. Jos PHP on asennettu, sekä toiminnassa ruudulle tulee alla olevan kaltainen viesti (Kuvio 13).



PHP Version 5.2.8

System	Linux Bakhuis-Server 2.6.27.7-9-default #1 SMP 2008-12-04 18:10:04 +0100 x86_64
Build Date	Dec 14 2008 16:05:11
Configure Command	'../configure' '--prefix=/usr' '--datadir=/usr/share/php5' '--mandir=/usr/share/man' '--bindir=/usr/bin' '--with-libdir=lib64' '--includedir=/usr/include' '--sysconfdir=/etc/php5/apache2' '--with-config-file-path=/etc/php5/apache2' '--with-config-file-scan-dir=/etc/php5/conf.d' '--enable-libxml' '--enable-session' '--with-mm' '--with-pcre-regex=/usr' '--enable-xml' '--enable-simplexml' '--enable-spl' '--enable-filter' '--disable-debug' '--enable-inline-optimization' '--disable-rpath' '--disable-static' '--enable-shared' '--program-suffix=5' '--with-pic' '--with-gnu-ld' '--with-system-tzdata=/usr/share/zoneinfo' '--with-apxs2=/usr/sbin/apxs2' '--disable-all' '--disable-cli'
Server API	Apache 2.0 Handler
Virtual	disabled

Kuvio 13. PHP - version tarkistus

MySQL:n sekä phpmyadminin asennuksen jälkeen tarkistetaan, että nämä toimivat. Kirjoitetaan selainkenttään http://127.0.0.1/phpmyadmin. Esiin tulee sisäänkirjautumisruutu. Syöte-

tään käyttäjäksi ”root” sekä salasanaksi asennuksen aikana syötetty salasana. Mikäli tietokantakin toimii, voidaan siirtyä itse Nagioksen asennukseen.

Nagioksen asennuksen eri vaiheet on dokumentoitu opinnäytetyön liitteissä. Seurataan asennusohjetta tarkasti. Erityisen tärkeää ovat eri käyttäjien, sekä käyttäjäryhmien luominen ja näiden tarkka dokumentointi. Järkevää on antaa ryhmille, sekä käyttäjille näiden toimintatarkoitusta vastaavat nimet, jotta loppupään konfigurointi helpoittuu. Tiivistettynä Nagioksen asennuksen vaiheet ovat seuraavat (kts. liitteet):

1. Käyttäjien luonti
2. Käyttäjäryhmien luonti
3. Käyttäjien siirto oikeisiin käyttäjäryhmiin
4. Nagios-asennuspaketin haku
5. Asennuspaketin purkaminen
6. Nagios–tiedostojen kääntäminen ja asennus erikseen määritettyjen parametrien mukaisesti
7. Nagios–pluginien asennuspaketin haku
8. Asennuspaketin purkaminen
9. Pluginien kääntäminen ja asennus erikseen määritettyjen parametrien mukaisesti
10. NDOutilsin haku
11. NDOutilsin tiedostojen kääntäminen ja asennus erikseen määritettyjen parametrien mukaisesti
12. NDOutils–asetustiedostojen kopiointi oikeisiin paikkoihin
13. Tiedosto–oikeuksien määrittäminen
14. Broker modulen käyttöönotto
15. NDO–käynnistysscriptin luominen
16. Asennettujen palveluiden asettaminen käynnistymään automaattisesti järjestelmän käynnistyksen yhteydessä

Tässä vaiheessa ei NDOutilsia ole vielä asennettu loppuun asti, jatketaan NDOutilsin loppuasennusta Centreonin asennuksen jälkeen. Centreon–asennuksen vaiheet ovat seuraavat:

1. Haetaan uusin versio Centreonista ohjelman viralliselta kotisivulta (http://www.centreon.com)
2. Puretaan asennuspaketti
3. Ajetaan export path-komento jolla määritellään minne Centreonin asetustiedostot tallentuvat
4. Ajetaan asennusohjelma. Asennusohjelmaa ajettaessa on ensiarvoisen tärkeää, että kaikki tiedot joita ohjelma kysyy syötetään oikein

5. Onnistuneen asennuksen jälkeen käynnistetään Apache2 uudestaan
6. Siirrytään Centreonin loppuasennukseen joka tapahtuu selaimena avulla osoitteessa http://localhost/centreon
7. Graafisen loppuasennuksen suorittamisen jälkeen kokeillaan Centreonin toimivuus syöttämällä uudestaan yllä oleva osoite. Tällä kertaa järjestelmä ohjautuu automaattisesti Centreonin sisäänkirjautumisruutuun. Syötetään käyttäjätunnus ja salasana ja tarkistetaan että päästään sisään Centreoniin. Tässä vaiheessa NDO–tietokanta ei vielä ole toiminnassa joten järjestelmä antaa virheilmoituksen tästä.

Seuraavaksi suoritetaan NDOutilsin asennus loppuun joka samalla luo Centreonin käyttämät tietokannat. NDOutilsin loppuasennuksen vaiheet ovat seuraavat:

1. Kirjaudutaan sisään MySQL–tietokantaan ja luodaan NDO–tietokanta valmista asennuscriptiä hyväksi käyttäen
2. Määritetään Centreonin tietokannan käyttäjä
3. Vaihdetaan tietokannan salasana
4. Päivitetään NDOutilsin asetustiedostoihin järjestelmä käyttämään TCP–sockettia UNIX–socketin sijaan. (Huomaa että kyseinen muutos täytyy tehdä useaan kohtaan kahdessa eri tiedostossa.
5. Käynnistetään NDOutils ja tarkistetaan lokitiedostosta ettei virheitä ilmennyt

Tämän jälkeen Nagios ja Centreon on asennettu palvelimelle onnistuneesti. Oletuksena osoitteet joilla päästään käsiksi graafisiin käyttöliittymiin ovat http://localhost/nagios sekä http://localhost/centreon.

Mahdollisissa virheissä ensimmäisenä kannattaa tarkistaa tietokanta–asetukset, käyttäjätietojen oikeellisuus, sekä mahdolliset virheet tiedostojen luku- ja kirjoitusoikeuksissa.

4.7 Nagios WWW-käyttöliittymä

Nagios verkonvalvontaohjelmisto toimii yksinkertaisen www-käyttöliittymän avulla. Tämän ansiosta valvontaohjelmiston käyttö on alustariippumaton ja toimii millä tahansa käyttöjärjestelmällä Internet-selainta hyväksi käyttäen.

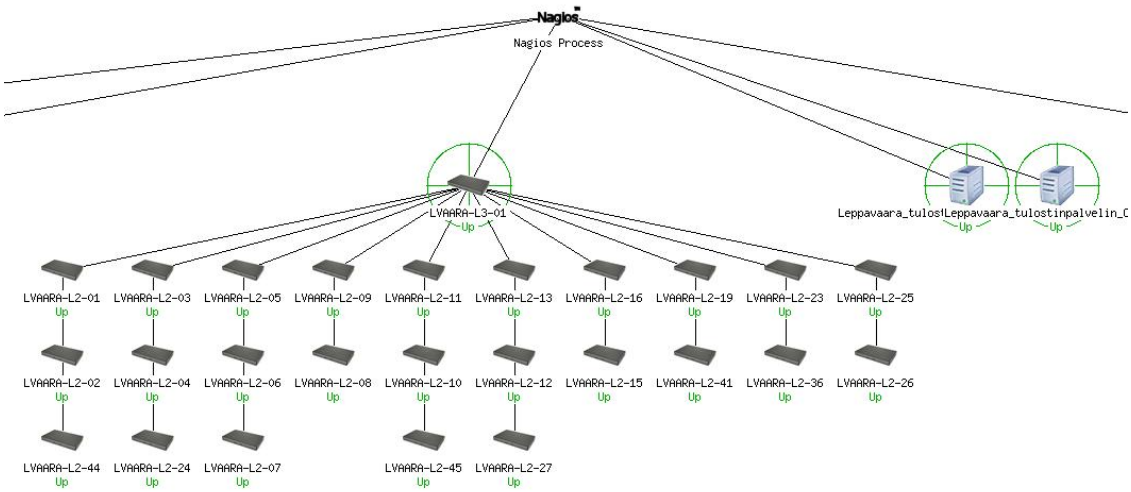
Järjestelmässä pystytään liikkumaan melko vaivattomasti valikosta toiseen vieressä olevaa päävalikkoa hyväksi käyttäen. Alla selitetään tarkemmin mitä mistäkin valikosta tapahtuu.

Home: Nagios aloitussivu, ei sisällä mitään järjestelmän toimivuuden kannalta tärkeää.
Documentation: Tätä kautta päästään käsiksi Nagioksen viralliisiin ohjedokumentteihin
*Tactical Overview:*Yleiskuva valvottavista laitteista.
Map: Automaattisesti generoitu kartta laitteista ja niiden kytkennöistä
Hosts: Asennetut hostit ja näiden tilat
Services: Asennetut palvelut ja näiden tilat
Host Groups: Hostien listaus ryhmittäin
Service Groups: Palveluiden listaus ryhmittäin
Problems: Havaitut ongelmat
Reports: (availability, trends, alerts yms.): Erinäisiä raporttityökaluja. Pystytään suorittamaan hakuja itse määritellyillä atribuuteilla.
Notifications: Lähetetyt virheilmoitukset
System: Mahdollisia ylläpidon kommentteja, mahdollisia laitteiden alhaalla oloaikoja (hallittuja alasajo- ja/uudelleenkäynnistyksiä). Asennettujen laitteiden asetuksia.

Nagioksessa on mahdollista piirtää kartta valvotuista verkkolaitteista (Kuvio 14). Ohjelmisto piirtää kartan automaattisesti sen mukaan, miten laitteet on asennettu järjestelmään.

Alla olevassa kuvassa on esimerkkinä otettu esiin Laurean Leppävaaran toimipisteen valvotut laitteistot. Kuten kuvasta näkyy, ylimmän tason laitteena on Layer 3–tason reititin. Tähän reitittimeen on kytketty Layer 2 tason kytkimiä.

Mikäli Lvaara-L3-01 laite kaatuu, lähtee kyseisestä laitteesta varoitusviestit etukäteen määritellyille ylläpitäjille, mutta järjestelmä ei lähetä virheilmoituksia laitteista jotka on kytketty kiinni L3-01-reitittimeen koska reititin on ylemmällä tasolla muihin laitteisiin nähden. Tämän avulla saadaan vähennettyä turhien virheviestien lähetystä.

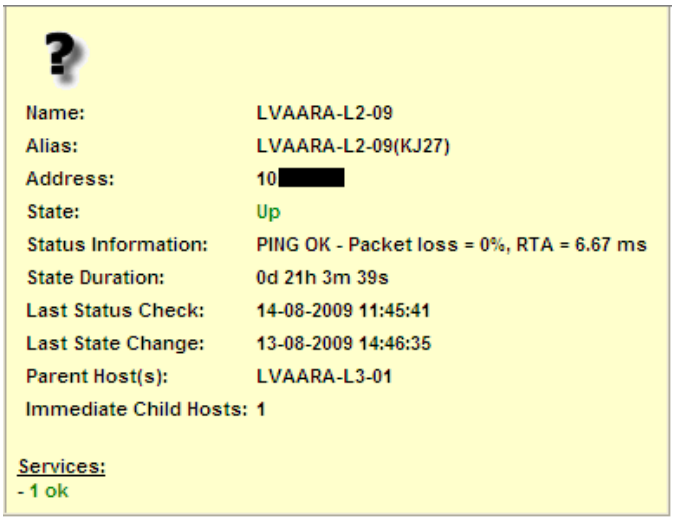


Kuvio 14. Nagios statuskartta

Erinäisiä hakuja tehdessä sivun ylälaidassa näkyy aina yhteenveto valvotuista laitteista (Kuvio 15). Klikkaamalla esimerkiksi ”Down” kohdassa olevaa tekstiä päästään käsiksi kaikkiin laitteisiin jotka eivät vastaa pyyntöihin.

Kuvio 15. Järjestelmän yhteenveto

Viemällä hiiren halutun laitteen yläpuolelle aukeaa ruutu joka sisältää lisätietoja laitteesta (Kuvio 16).

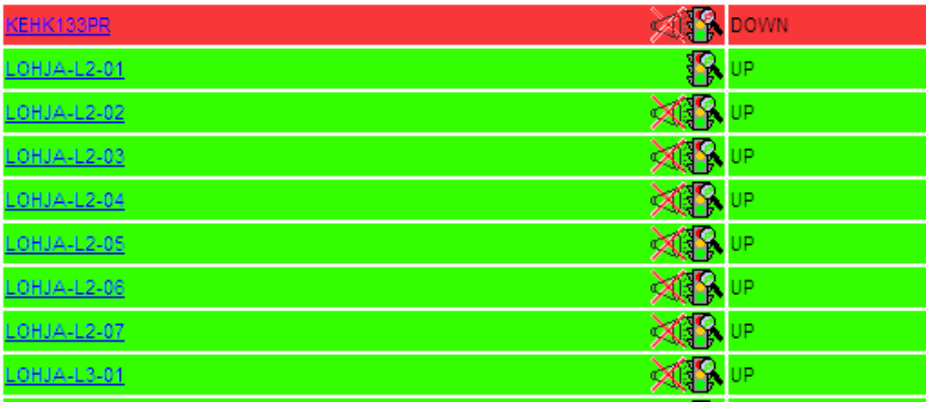


Kuvio 16. Lisätietoja laitteesta

Nagioksessa on mahdollista ottaa kartan lisäksi toisenlainen näkymä valvotuista laitteista. Kyseisessä näkymässä ei näytetä erikseen sitä, miten laitteet on kytketty toisiinsa. Kyseessä on vain tiivistetty listaus valvotuista laitteista (Kuvio 17).

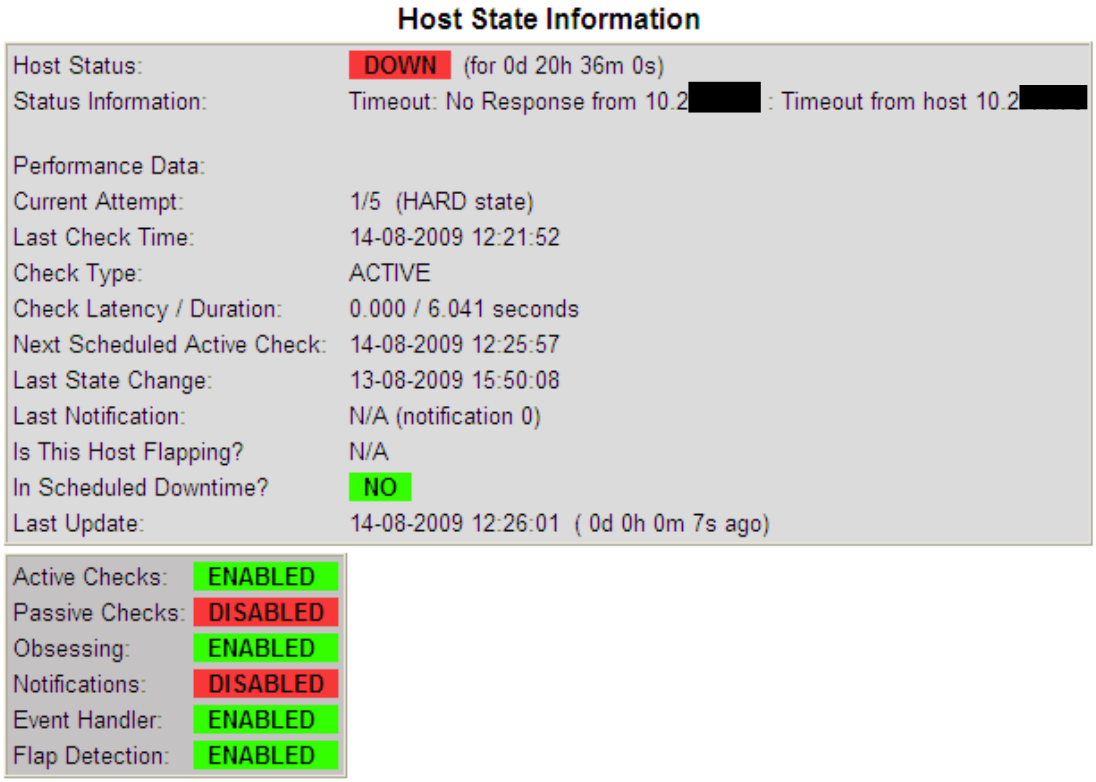
Laite joka ei vastaa näkyy punaisella pohjalla ja toimivat laitteet näkyvät vihreällä pohjalla.

Alla olevasta kuvasta nähdään että laitteella LOHJA-L2-01 ovat varoitusviestit päällä, kun taas muista laitteista ei virheilmoituksia lähetetä ylläpitäjille.



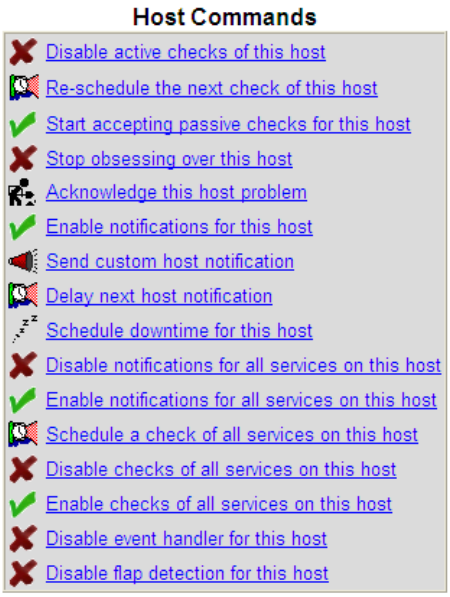
Kuvio 17. Valvotut hostit

Jos halutaan lisätietoa laitteesta, klikataan laitteen nimeä, tämä ohjaa käyttäjän alla olevalle sivulle josta nähdään lisätietoja laitteesta (Kuvio 18).



Kuvio 18. Lisätietoja laitteesta

Samalla lisätietosivulla pystytään ajamaan tiettyjä komentoja laitteeseen liittyen (Kuvio 19). Pystytään ottamaan laitteeseen liittyvät testit pois päältä, ajoittamaan mahdollisien testien ajoaikoja, lähettämään viestejä laitteeseen liittyen sähköpostin välityksellä niille henkilöille jotka on merkattu ylläpitämään kyseistä laitetta jne.



Kuvio 19. Valvottavan laitteen komennot

Ylläpitäjät pystyvät syöttämään laitteeseen kommentteja mikäli näin haluavat (Kuvio 20). Tämä helpottaa ylläpitoa huomattavasti.

Host Comments

Add a new comment | Delete all comments

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
14-08-2009 12:31:49	nagiosadmin	Vian syy: SNMP-liikenne estetty	2	Yes	User	N/A	
14-08-2009 12:30:33	nagiosadmin	Laitevikaa, syytä tutkitaan	1	Yes	User	N/A	

Kuvio 20. Ylläpidon kommentit

Nagioksessa on myös mahdollista tehdä listauksia etukäteen määritellyiden ryhmien perusteella. Kuviossa 21 on haku on rajattu tulostinpalvelimiin, sekä WLAN – tukiasemiin. Kuviossa 22 näkyy yhteenveto ryhmäkohtaisesti. Klikkaamalla Host Group – kohtaa päästään tarkistelemaan tarkemmin laitteita jotka kyseisen ryhmän alle no asennettu.

Tulostinpalvelimet (Tulostinpalvelimet)

Host	Status	Services	Actions
Leppavaara_tulostinpalvelin_Henkilokunta	UP	1 OK 4 UNKNOWN	
Leppavaara_tulostinpalvelin_Oppilas	UP	1 OK 4 UNKNOWN	
Lohja_tulostinpalvelin_Henkilokunta	UP	1 OK 4 UNKNOWN	
Lohja_tulostinpalvelin_Oppilas	UP	1 OK 4 UNKNOWN	
Tikkurila_Tulostinpalvelin	UP	3 OK 1 CRITICAL	

WLAN tukiasemat (WLAN_aps)

Host	Status	Services	Actions
TIKKURILA-WLAN-01	UP	1 OK	
TIKKURILA-WLAN-02	UP	1 OK	

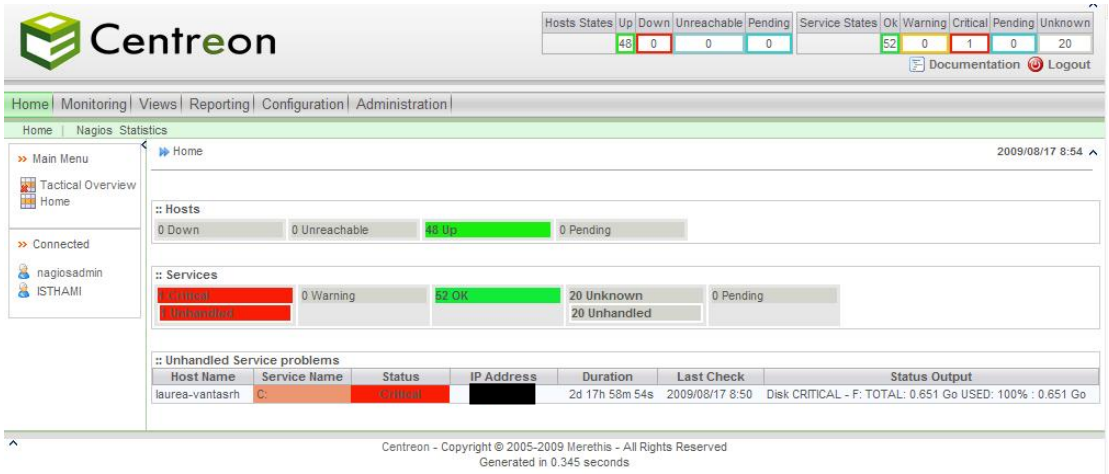
Kuvio 21. Ryhmälistaus 1

Kuvio 22. Ryhmälistaus 2

5 Centreon

Nagioksessa itsessään ei ole mahdollisuutta graafiseen laite tai käyttäjähallintaan, vaan kaikki muutokset asetuksiin joudutaan tekemään käsin erinäisiä asetustiedostoja muokkaamalla. Tämä on ylläpidon kannalta todella työlästä ja aikaa vievää sekä vaatii kattavaa tietämystä järjestelmän toiminnasta johtaen siihen, että mahdolliset ylläpitäjät jouduttaisiin kouluttamaan hyvinkin perusteellisesti ennen kuin he kykenisivät käyttämään järjestelmää jouhevasti. Tämä ongelma ratkaistiin asentamalla Nagioksen päälle Centreon–niminen lisämoduuli.

Centreon mahdollistaa saman käyttöliittymän alta laitteiden hallinnoinnin tietokantojen avulla, graafisien käyrien piirtämisen, sekä monia muita lisäominaisuuksia Nagiokseen (kuvio 23). Centreon käyttää RRDtoolia graafisten käyrien hallinnoimiseen sekä NDOutilsia tietokantojen hallintaan (Centreon Wiki).



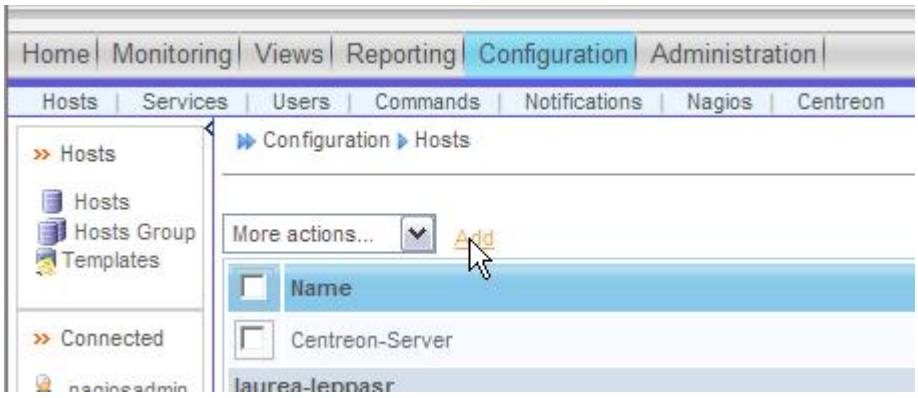
Kuvio 23. Centreon päänäkymä

Samoin kuin Nagioksessa, myös Centreonin kautta nähdään yhteenveto asennetuista laitteista ja niiden tiloista (Kuvio 24). Klikkaamalla numeroa näytetään esimerkiksi kaikki ”critical” tilassa olevat laitteet.

Kuvio 24. Centreon yhteenveto

5.1 Hostin lisääminen

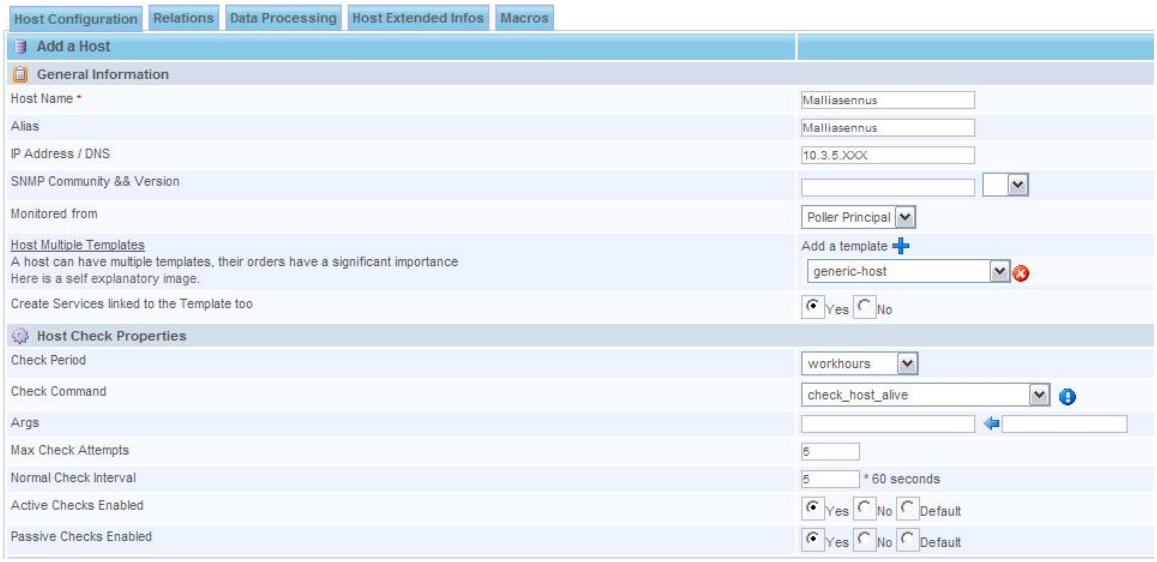
Hostien lisääminen on Centreonissa melko helppoa, alla käymme läpi kohta kohdalta miten tämä tapahtuu.
Valitaan päävalikosta Configuration -> Hosts ja klikataan Add –kohtaa (Kuvio 25).



Kuvio 25. Hostin lisääminen 1

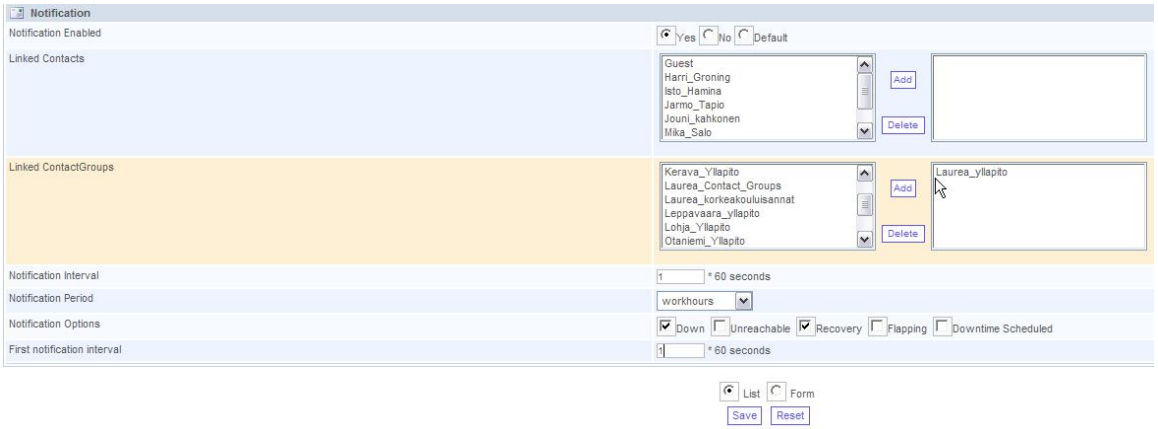
Tämän jälkeen päästään syöttämään halutun laitteen tiedot järjestelmään (Kuvio 26). Syötetään nimi, alias IP-osoite / DNS jne. Centreonissa on mahdollista luoda omia valmiita mallipohjia eli templateja, jos järjestelmään on luotu esim. printtereille oma mallipohjansa, voidaan tässä kohtaa valita se käyttöön.

Lisäksi syötetään tarkistukseen liittyvät asetukset, valitaan kuinka usein tarkistukset tehdään, mitä tarkistuksia tehdään sekä näiden tarkistusten maksimimäärät.



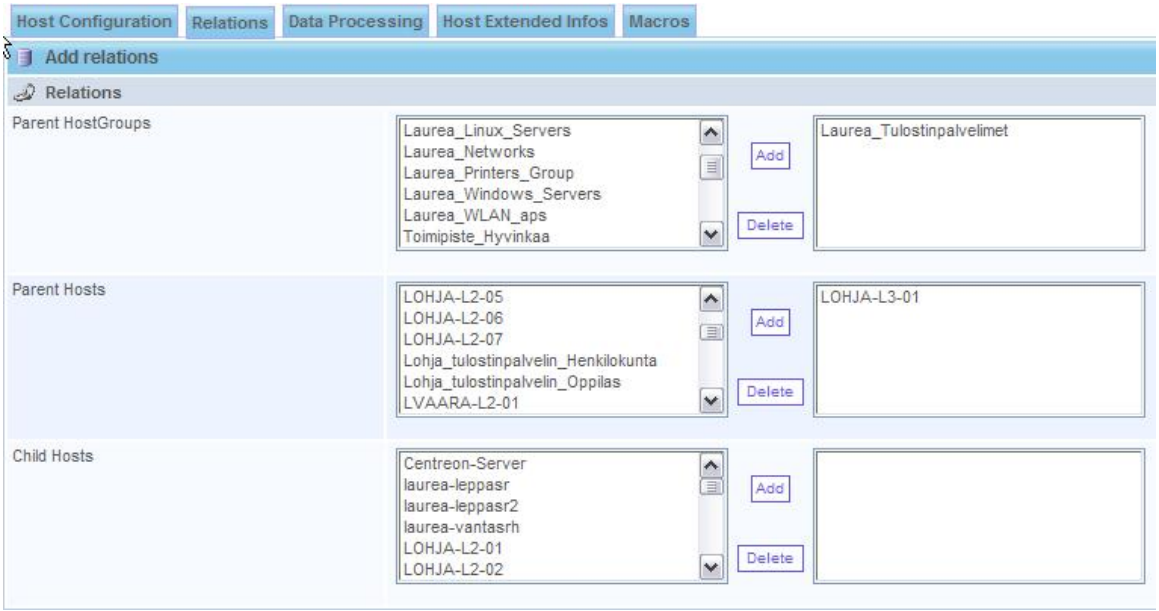
Kuvio 26. Hostin lisääminen 2

Tarkistusasetuksien syöttämisen jälkeen laitetaan vielä varoitusviestin asetukset kuntoon (Kuvio 27). Tässä kohdassa saadaan valittua jo luotujen ryhmien ja käyttäjien perusteella ne henkilöt/ryhmät joille kyseisestä laitteesta lähetetään varoitusviestit. Lisäksi pystytään määrittelemään milloin, sekä mistä tilanteista varoitusviestit lähetetään. Esimerkiksi alla olevissa asetuksissa on määritelty, että laitteesta lähetetään varoitusviestejä virka-aikana, sekä silloin kun jokin palvelu menee nurin tai alkaa toimia.



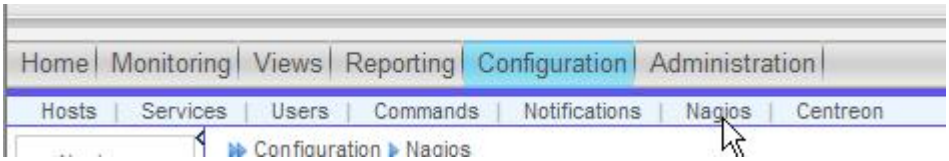
Kuvio 27. Hostin lisääminen 3

Lisäksi tässä vaiheessa on järkevää syöttää eri laitteiden väliset suhteet järjestelmään. Tämä onnistuu relations–kohdasta (Kuvio 28). Syötetään laitteen isäntäryhmä raporttien haun ja tulostamisen helpottamiseksi sekä isäntähostit. Isäntähostit mahdollistavat sen, että ylemmän tason laitteen rikkoutuessa varoitusviestejä ei lähetetä tähän kytketyistä laitteista. Tämän tavoitteena on se, että saadaan vähennettyä turhien varoitusviestien lähettämistä. Kun nämä tiedot on syötetty, voidaan painaa ”Save” nappulaa ruudun alalaidasta.



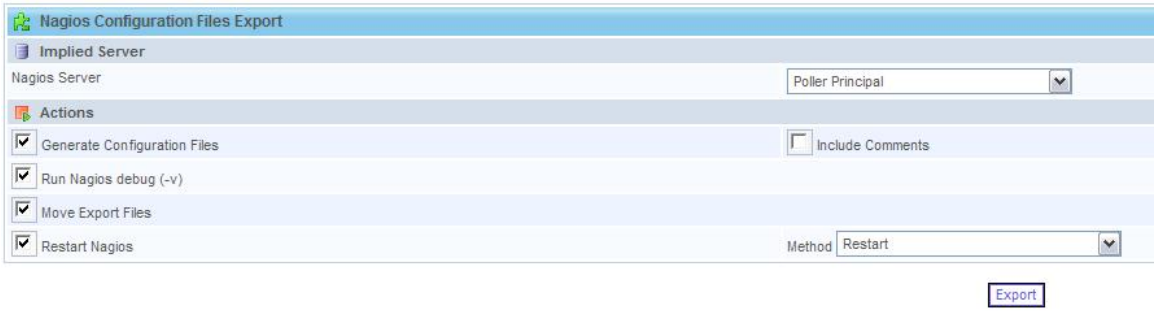
Kuvio 28. Hostin lisääminen 4

Huomaa, että tässä vaiheessa eivät tehdyt muutokset ole vielä siirtyneet Nagiokseen. Tällä hetkellä laitteet on asennettu vasta Centreonin puolelle järjestelmää. Jotta saadaan siirrettyä lisätyt laitteet Nagiokseen, täytyy vielä luoda asetustiedostot. Tämä onnistuu menemällä Configuration päävalikon alta Nagios kohtaan (Kuvio 29).



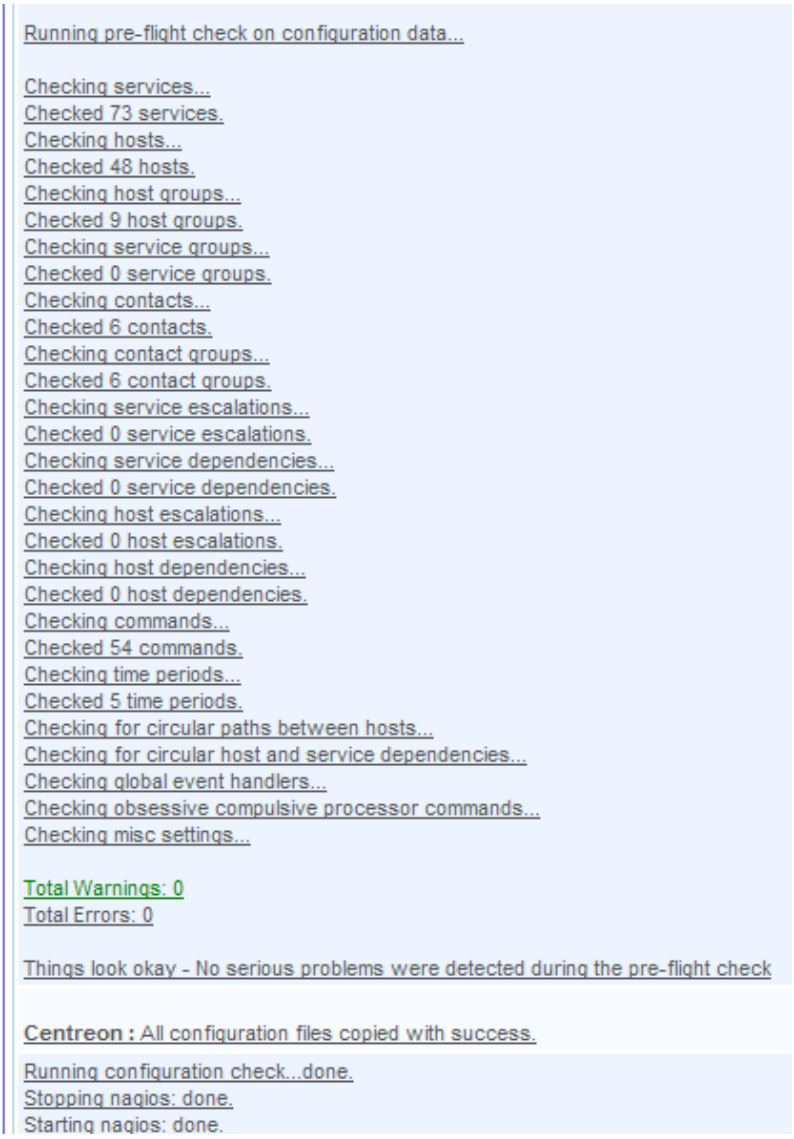
Kuvio 29. Hostin lisääminen 5

Valitaan Move Export Files ja Restart Nagios kohdat jo valittujen lisäksi sekä painetaan Export nappulaa (Kuvio 30). Tämä luo asetustiedostot, ajaa Nagioksen oman tarkistusohjelman virheiden varalta, siirtää luodut asetustiedostot Nagiokseen sekä käynnistää palvelut uudestaan. Tämä joudutaan tekemään aina tehtäessä joitain muutoksia Centreonin kautta.



Kuvio 30. Hostin lisääminen 6

Exportin jälkeen ruudulle tulostuu raportti asetuksien tarkistamisesta ja siirtämisestä (Kuvio 31). Jos virheitä ei ole löytynyt, ja asetukset on kopioitu oikein, saadaan alla olevan kaltainen tuloste. Huomaa alla Total Warnings ja Total Errors – kohdat.

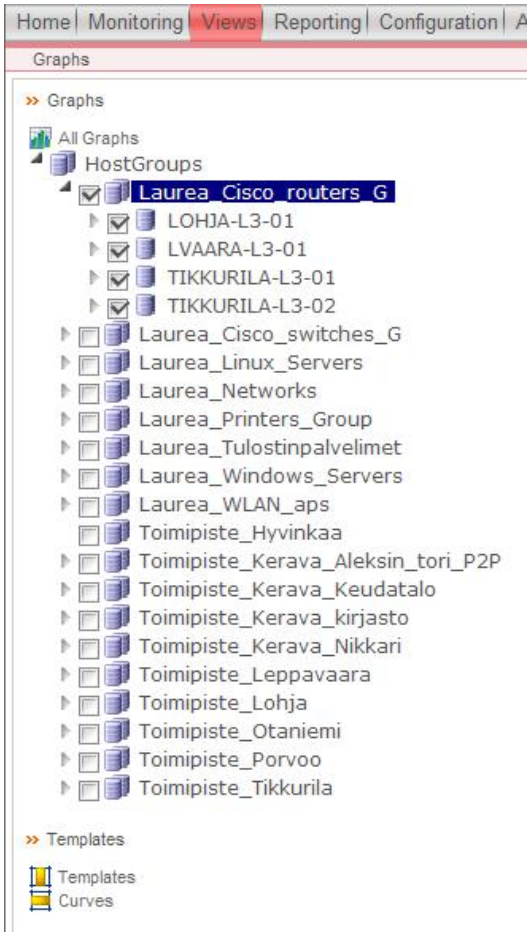


Kuvio 31. Hostin lisääminen 7

5.2 Raporttigraafien piirtäminen

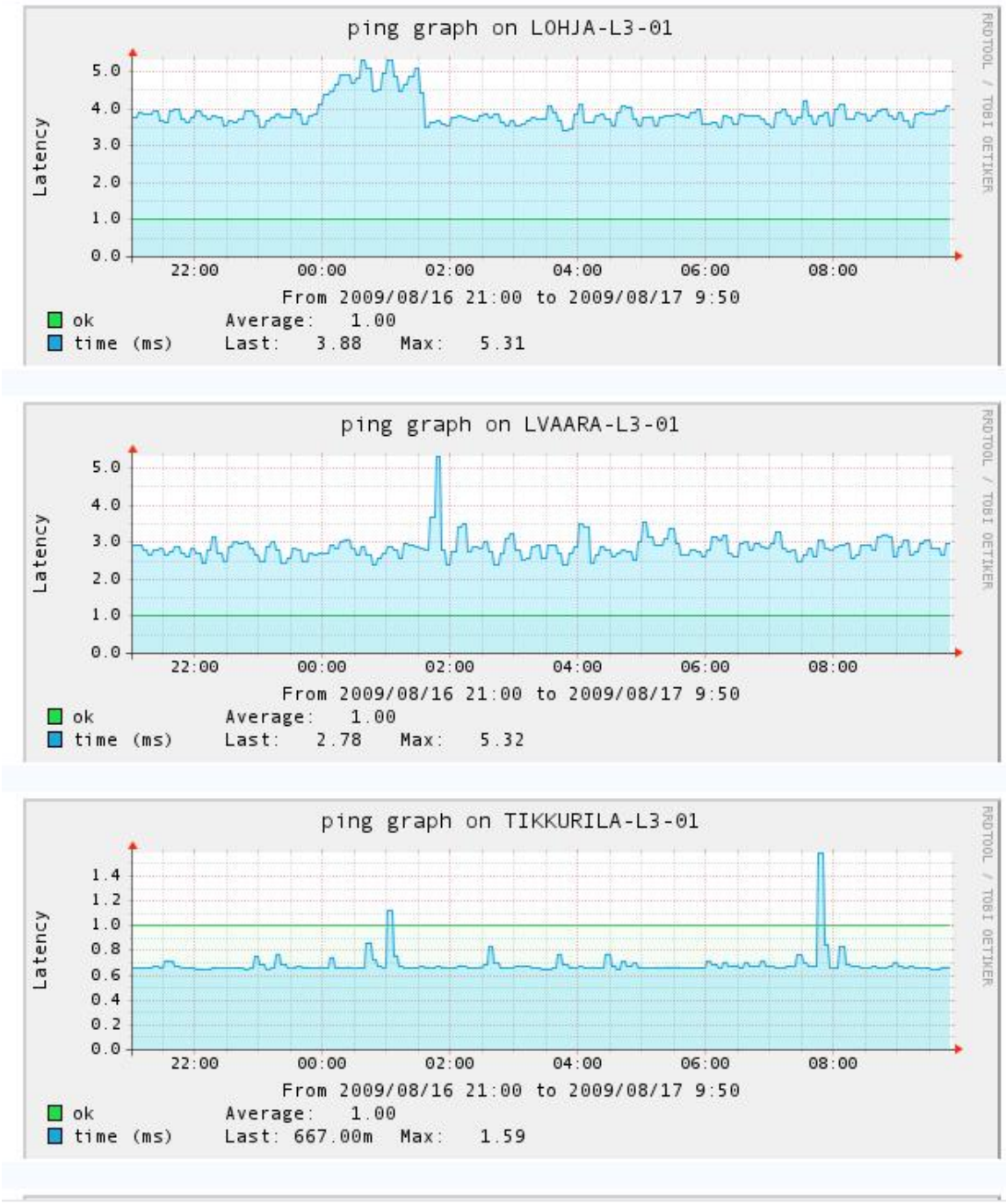
Centreon mahdollistaa NDOutilsia sekä RRDtoolia hyväksikäyttäen myös erilaisten raporttigraafien piirtämisen. Tämä ominaisuus on todella hyödyllinen ylläpidon kannalta katsottuna, sillä se helpottaa huomattavasti mahdollisien vikatilojen huomaamista jo etukäteen.

Valitaan päävalikosta Views-kohta joka avaa järjestelmään lisätyt Hostgroupit (Kuvio 32), näitä hyväksi käyttäen pystytään tekemään rajattuja hakuja tai valinnan mukaan ottamaan raportit ulos kaikista tietyn toimipisteen laitteista. Alla olevassa esimerkissä on valittu kaikki asennetut reitittimet.



Kuvio 32. Raporttigraafien piirtäminen 1

Valituilla asetuksilla saadaan alla olevanlainen listaus laitteista. Kyseisiin laitteisiin on asennettu vasteaikatarkistus ja tästä piirtyvät graafit näytölle (Kuvio 33).



Kuvio 33. Raporttigraafien piirtäminen

5.3 Centreon-käyttäjähallinta

Centreoniin voidaan luoda omia käyttäjiä sekä halutunlaisia käyttäjäryhmiä. Nämä ominaisuudet löytyvät suoraan Nagioksestakin, mutta Centreon mahdollistaa huomattavasti helpomman ja selkeämmän käyttöliittymän näiden hallinnoimiseen. Valitaan Configuration -> Users Centreonin päävalikosta jolloin saadaan alla olevan kaltainen listaus luoduista käyttäjistä (Kuvio 34). Sisäänkirjautumisen käyttäjätunnus on tästä raportista sensuroitu tietoturvallisuussyistä.

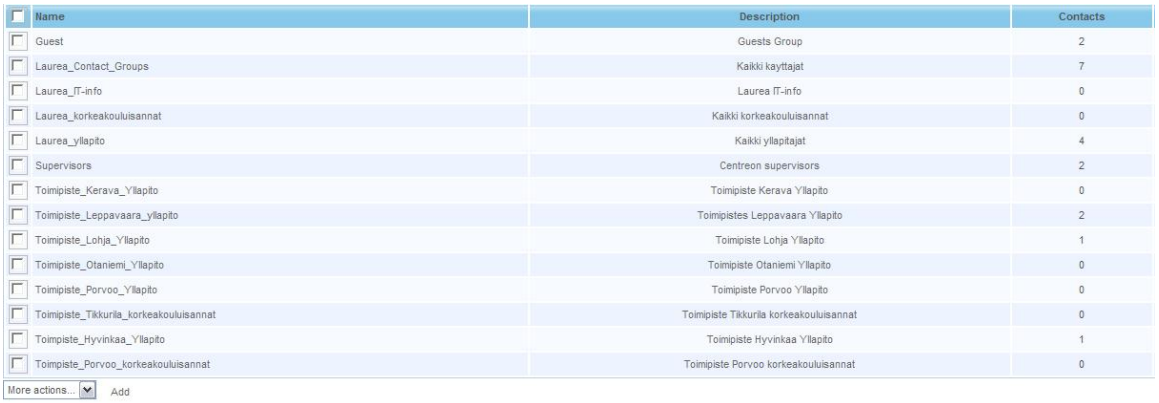
Kuvio 34. Käyttäjänhallinta 1

5.3.1 Uuden käyttäjäryhmän lisääminen

Ennen käyttäjien lisäämistä kannattaa järjestelmään luoda halutut käyttäjäryhmät ylläpidon helpottamiseksi. Valitaan päävalikosta Configuration -> Users ja vasemmasta navigointipalkista valitaan Contact Groups-kohta (Kuvio 35).

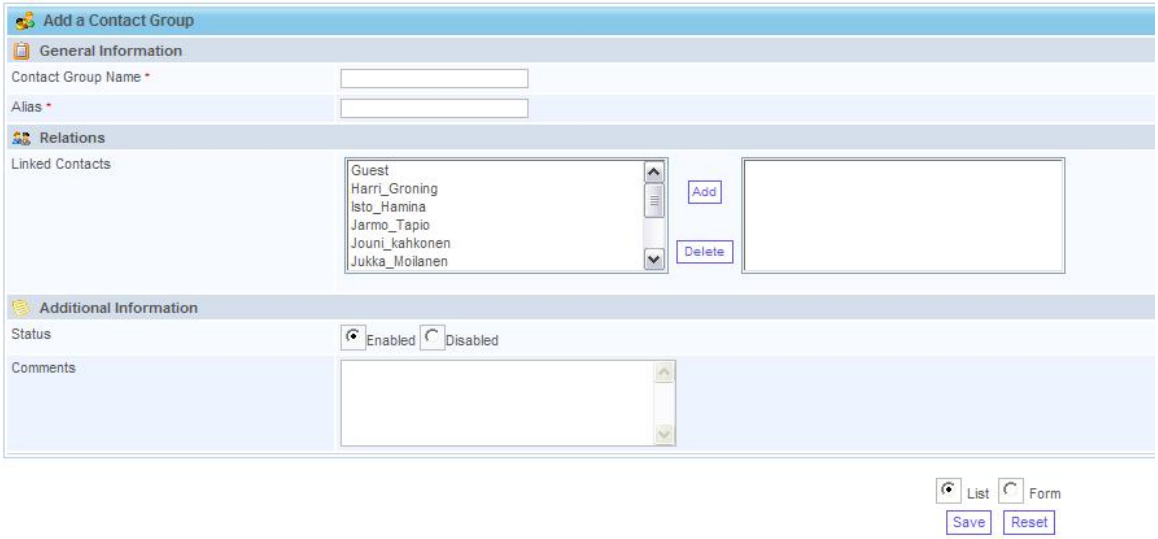
Kuvio 35. Käyttäjähallinta 2

Käyttäjäryhmien valinnan jälkeen aukeaa alla olevan kaltainen listaus jo asennetuista ryhmistä (Kuvio 36), jos halutaan luoda uusi ryhmä, painetaan Add- nappulaa.



Kuvio 36. Käyttäjähallinta 3

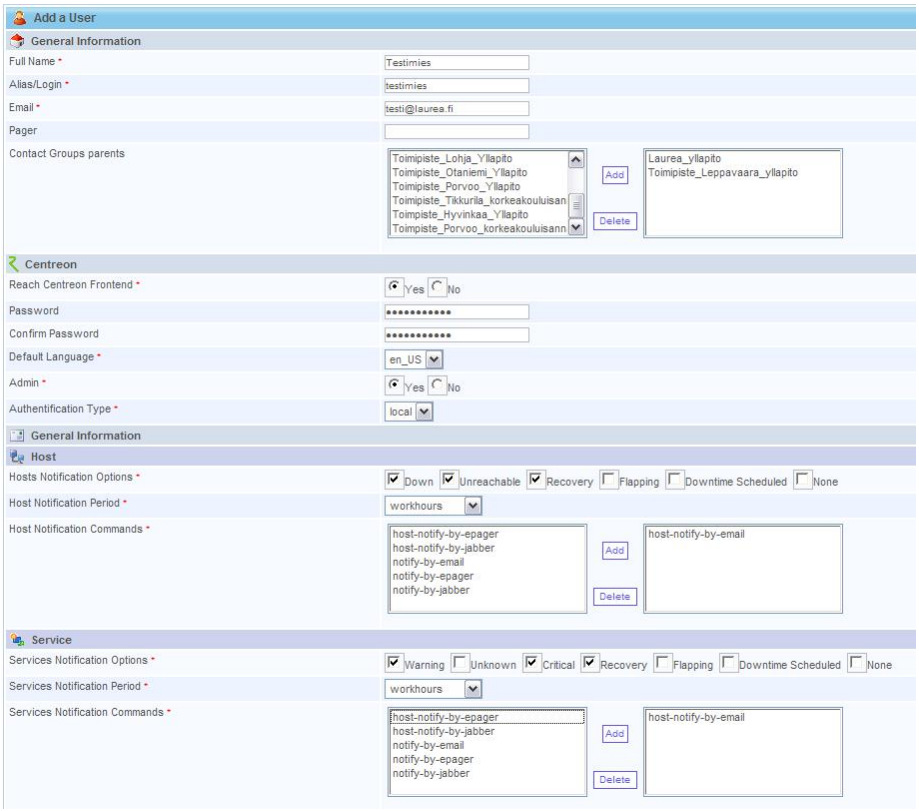
Tämän jälkeen syötetään kontaktiryhmän nimi sekä alias ja linkitetään mahdolliset jo luodut käyttäjät ryhmään (Kuvio 37). Lopuksi painetaan Save–joka tallentaa tehdyt muutokset Centreoniin.



Kuvio 37. Käyttäjähallinta 4

5.3.2 Uuden käyttäjän lisääminen

Käyttäjälistauksen esiin ottamisen jälkeen painetaan Add–nappulaa. Tämän jälkeen aukeaa alla olevan kaltainen sivusto (Kuvio 38). Syötetään halutut tiedot ja painetaan Save–nappulaa. Kontaktiryhmät kannattaa laittaa jo tässä vaiheessa kuntoon, tämän avulla saadaan hallinnoitua sitä, minkä toimipisteen varoitusviestejä luodulle käyttäjälle lähetetään.



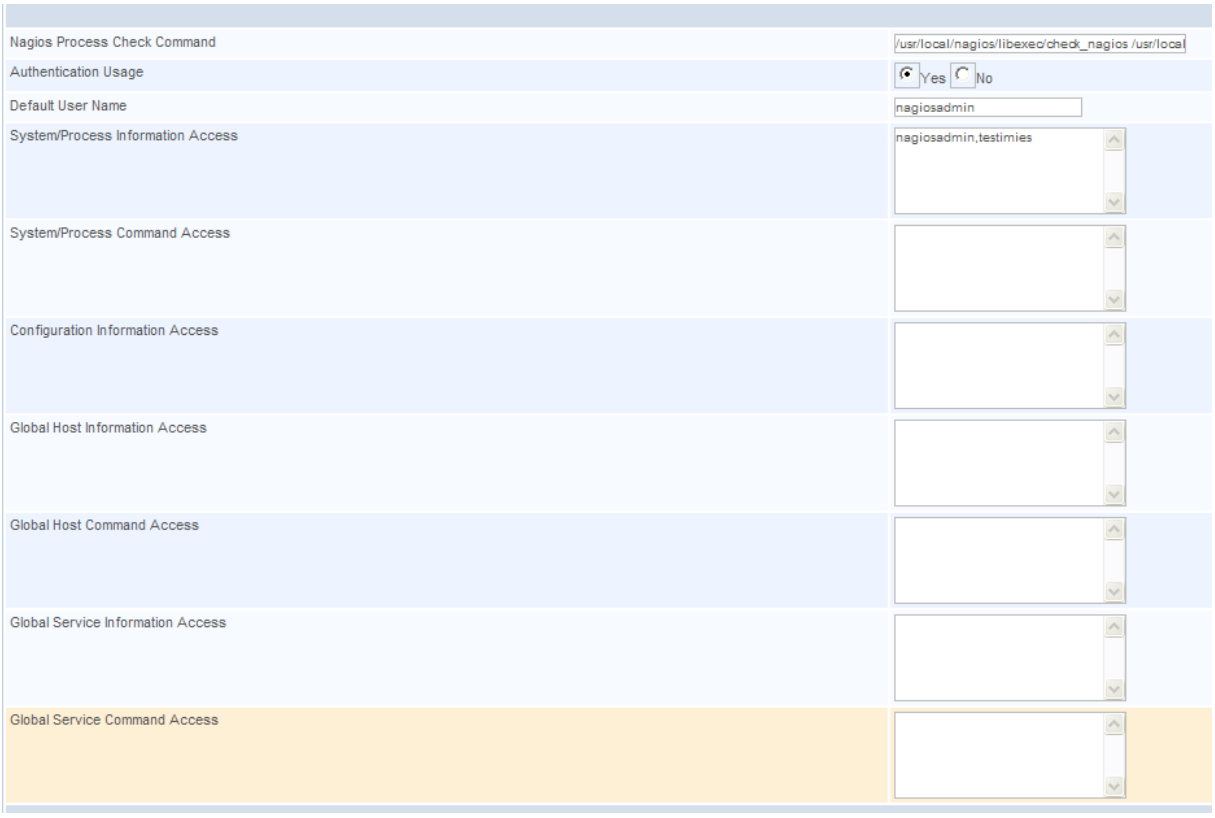
Kuvio 38. Käyttäjähallinta 5

Autentikoidaan luotu käyttäjä myös Apache – palvelimelle allaolevalla komennolla.

htpasswd2 /usr/local/nagios/etc/htpasswd.users <käyttäjänimi>

Lisäksi käyttäjälle täytyy lisätä oikeudet erinäisiin Nagioksen sisältämiin CGI – palveluihin. Tämä tehdään muokkaamalla CGI.cfg – tiedostoa. Muokkaaminen voidaan tehdä joko käsin, tai Centreonin graafista käyttöliittymää hyväksi käyttäen. Lisätään luotu käyttäjänimi kenttiin sen mukaan, mihin CGI - palveluihin annetaan käyttäjälle oikeus.

Alla oleva valikko löytyy Centreoninista Configuration-välilehden alta (Kuvio 39).



Kuvio 39. CGI-tiedoston muokkaus

6 Toimintaympäristö

Tämän kappaleen tarkoitus on valottaa lukijalle sitä millaisessa toimintaympäristössä projektin verkonvalvontatyökalua on käytetty.

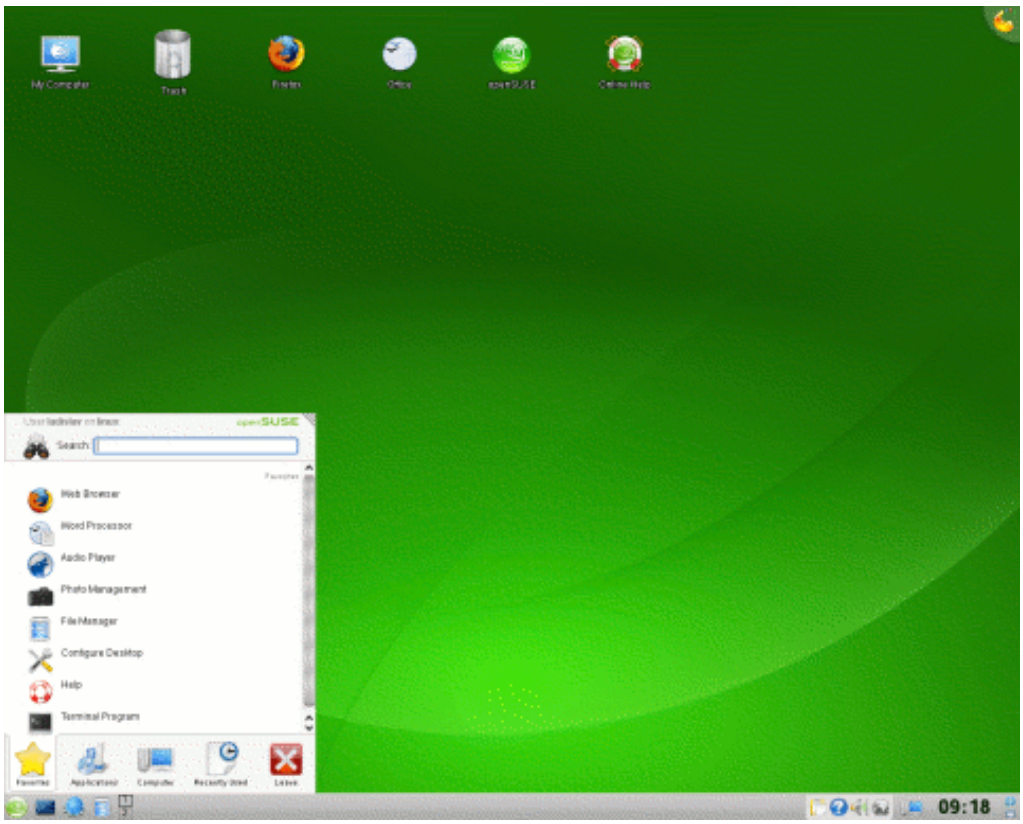
Toimintaympäristönä projektissa on Laurea-ammattikorkeakoulu, tarkemmin Tikkurilan- ja Leppävaaran toimipisteet. Laurea-ammattikorkeakoululla on useita toimipisteitä, joilla kaikilla on oma verkkonsa. Teknisenä toimintaympäristönä toimii Laurea- ammattikorkeakoulun IT-infrastruktuuri. Projektin luonteen vuoksi Laurea-ammattikorkeakouluun ei ole rakennettu erillistä testiympäristöä projektin kohteena olevaa verkonvalvontajärjestelmää varten. Testiympäristön rakentaminen projektia varten olisi ollut turhaa ja myös kallista. Verkonvalvontatyökalu voidaan ottaa käyttöön ilman testiympäristöä, koska verkonvalvontatyökalun käyttöönotto varsinaisessa yritysverkossa ei ole suuri riski. Verkonvalvontatyökalun testaaminen ei myöskään vaadi testiympäristöä vaan työkalu saadaan parhaiten käyttöön oikeassa konkreettisessa verkossa.

Laurea-ammattikorkeakoulun verkon infrastruktuurista, emme voi paljastaa teknisiä yksityiskohtia kuten palvelinten IP-osoitteita tässä projektissa, vedoten asiakkaan asettamaan vaitiolovelvollisuuteen. Projektin kannalta asiakkaan verkon teknisten osien salassapito ei kui-

tenkaan muuta itse projektin kohteena olevan järjestelmän käyttäytymistä eikä käyttöönottoa. Projektin kohteena oleva verkonvalvontatyökalu ei ole tilaajan verkosta riippuvainen, vaan sen käyttöönotto, asennus ja ylläpito tapahtuu samoin jokaisessa muussakin verkossa.

Toimintaympäristönä Laurea-ammattikorkeakoulu on erittäin hyvä työstettävässä projektissa. Verkon infrastruktuuri, laitteisto ja verkon toteutustekniikka tarjoavat hyvän alustan verkonvalvontajärjestelmän ominaisuuksien hyödyntämiselle. Useat toimipisteet ja niiden välinen tietoliikenne tuo välimatkaa verkon yli valvottavista kohteista. Kohdeyrityksen laitteiden nykyaikaisuus on hyödyllinen osa projektissa. Uusien ja laadukkaiden kytkinten, työasemien, palvelinten ja tulostimien monitorointi on huomattavasti toimintavarmempaa ja helpompaa kuin vanhojen, ei niin laadukkaiden laitteiden monitorointi.

Itse Nagios-verkonvalvontatyökalun toimintaympäristönä toimii Linux-käyttöjärjestelmä. Linuxista löytyy useita eri variaatioita, projektin käyttöjärjestelmänä toimii Linux OpenSuse (Kuvio 40). Opensuse valittiin projektiin sen takia, että se on jatkuvasti kehittyvä järjestelmä, sekä se omaa hyvän dokumentaation.



Kuvio 40 Opensuse työpöytä

7 Kehitysideoita

Tässä kappaleessa käydään läpi projektin edetessä eteen tulleita ideoita, jotka olisi hyvä toteuttaa joskus lähitulevaisuudessa. Kyseisiä ominaisuuksia ei erinäisistä syistä otettu mukaan tähän opinnäytetyöhön. Pääosin ideoiden toteuttamatta jättäminen johtui resurssien puutteesta, Nagios ja Centreon aiheena olivat jo niin laajoja, että ryhmän oli pakko karsia niitä asioita pois, jotka nähtiin vähemmän tärkeiksi. Alla on listattuna muutamia kehitysehdotuksia projektiryhmän näkemässä tärkeysjärjestyksessä.

Jossakin toisessa organisaatiossa SSL–salauksen toteuttaminen sijoitettaisiin listalla ylemmäksi. Laurean tapauksessa salauksen suorittamista ei pidetty ensiarvoisen tärkeänä johtuen siitä, että Nagios–palvelu määriteltiin toimimaan ainoastaan asiantuntijaverkosta käsin.

7.1 WWW-palveluiden lisääminen valvontaympäristöön

Palvelupuolella erityisesti eri www-palveluiden esim. sähköpostin, optiman, winhavillen ja intran lisääminen Nagioksen tarkkailun piiriin nostaisi valvonnan ennaltaehkäisevyyttä, sekä parantaisi Laurean IT-palveluiden tasoa.

Suositeltavaa olisi, että kyseiset sähköiset palvelut lisättäisiin Nagios-valvonnan piiriin. Projektiryhmä olisi halunnut toteuttaa tämän, mutta liian vähien resurssien vuoksi toteutus ei ollut mahdollista.

7.2 Kytkinten ja reitittimien porttien valvonta

Verkkopuolella kytkinten porttien muuttaminen valvottaviksi palveluiksi parantaisi ongelmien havaitsemista tuntuvasti. Tämä olisi työläs operaatio, koska se vaatisi jokaisen kytkimen portin lisäämistä käsin valvonnan piiriin. Kyseinen operaatio helpottaisi pientenkin vikojen havaitsemista pienellä vaivalla, kuten esimerkiksi irronneen tai toimimattoman verkkokaapelin huomaamisen, sekä tarkan paikantamisen. Tätä kannattaisi hyödyntää ainakin verkon toiminnalle elintärkeissä kytkimissä, kuten talojakomoissa.

7.3 SSL -salaus

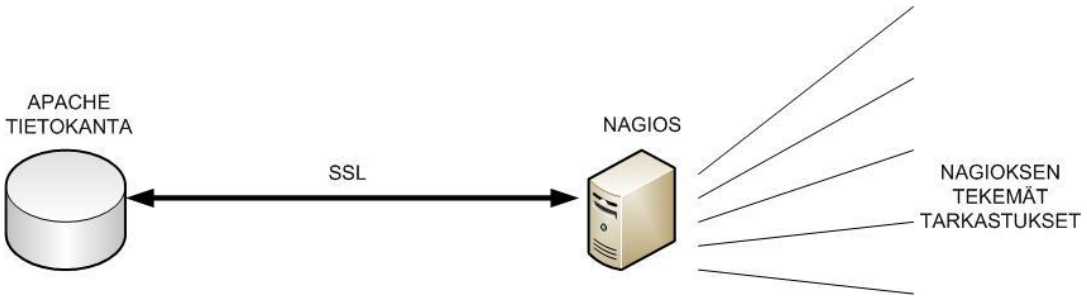
WWW-sivujen selailun suojaukseen käytetään useimmiten SSL-protokollaa (Secure Sockets Layer). SSL mahdollistaa yhteyden vahvan salaamisen käyttäjän WWW-selainohjelman ja

WWW-palvelimen välillä. Salaus suojaa tietoliikenteen siten, että ulkopuolinen tarkkailija ei yhteyttä seuraamalla pysty näkemään luottamuksellisia tietojasi.

SSL-yhteys alkaa "turvakättelyllä", jolla saadaan muodostettua suojattu yhteys asiakkaan www-selainohjelman ja www-palvelimen välille. Tässä kättelyssä asiakas-ohjelmisto ja palvelin sopivat yhteyskohtaisista ja kertakäyttöisistä salakirjoitusavaimista. Niitä käytetään istunnon ajan tiedon salaamiseen ja tulkintaan (Freier, Karlton, Kocher, 1996).

Yhteyden salaamisen lisäksi SSL-protokolla mahdollistaa palvelutarjoajan vahvan todentamisen varmenteiden avulla. Todennus tapahtuu siten, että palvelimella on oma palvelinvarmenne, jonka perusteella käyttäjä voi varmistua kommunikoivansa oikean www-palvelimen kanssa (Freier, Karlton, Kocher, 1996).

Projektin Nagios verkonvalvontatyökalun puolesta SSL:llä voitaisiin suojata tietokanta yhteys. Toisin sanoen Nagios toimii Apachen päällä ja SSL suojaisi tämän yhteysvälin (Kuvio 41).



Kuvio 41. SSL-yhteyden toiminta

7.4 SMS-hälytykset

Nagios verkonvalvontatyökalulla on myös mahdollista lähettää palvelun antamia hälytyksiä suoraan mobiililaitteeseen tai laitteisiin. Tämä helpottaisi huomattavasti ylläpitäjien työskentelyä. Ylläpitäjän ei tarvitsisi olla suoraan koko ajan kiinni verkonvalvontatyökalussa tai mikäli sähköpostihälytykset olisivat käytössä, niin koneen äärellä saadakseen tietoa verkonvalvontatyökalun antamista hälytyksistä. SMS-hälytyksien käyttöönotto voidaan perustella ylläpitäjien työajan säästämisestä johtuvista eduista. Projektissa eteen ilmestyi varsin pätevä SMS-hälytys lisäosa Nagiokseen nimeltään MMS Foxbox, jonka kustannukset pysyisivät pieninä verrattuna saavutettuun hyötyyn.

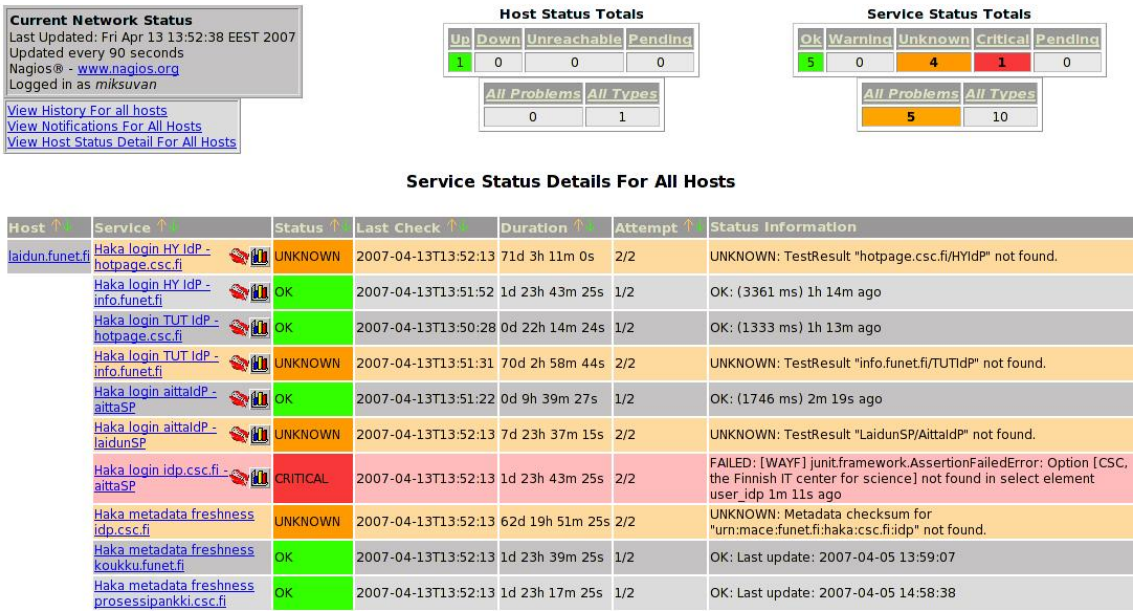
Foxboxin ominaisuudet riittävät hyvin Laurean kokoiselle organisaatiolle. Palvelu vaatii ainoastaan mobiililaitteen sekä Nagios/Linux palvelimen. Foxbox mahdollistaa 30 sms viestiä/min

kumpaankin suuntaan. Foxbox pitää sisällään oman käyttöliittymänsä mobiililaitteeseen. Palvelun kustannuksista ei projektin luonteen vuoksi puhuta sen tarkemmin.

7.5 Shibboleth Identity / Service Provider–valvonta

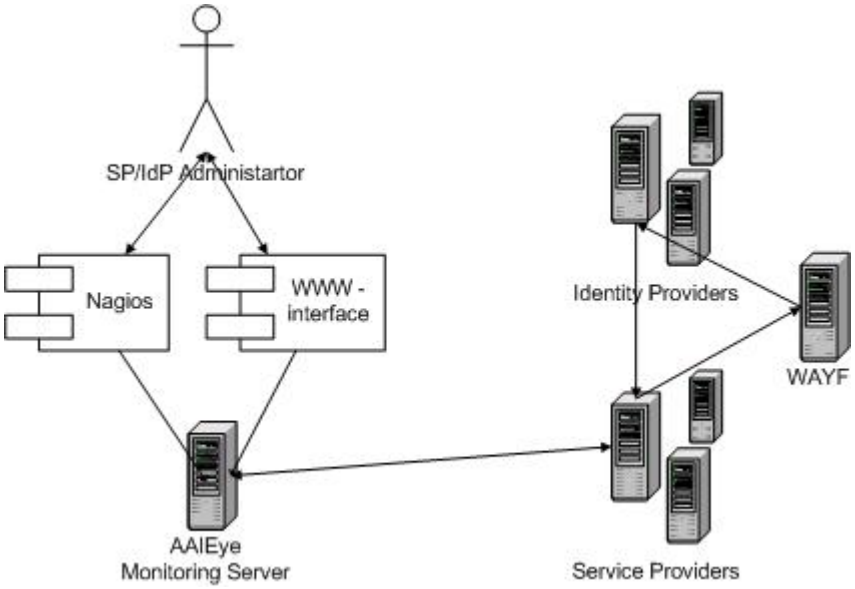
Laurea on mukana Haka–hankkeessa, joka on Suomen korkeakoulujen ja tutkimuslaitosten yhteinen käyttäjätunnistusjärjestelmä. Haka–hankkeen tarkoituksena on mahdollistaa jäsenorganisaatioiden opiskelijoiden kirjautuminen myös muiden kuin kotiorganisaationsa palveluihin omilla käyttäjätunnuksillaan. Haka vapauttaisi käyttäjät monien käyttäjätunnuksien ja salasanojen opettelusta, koska se mahdollistaisi yhden käyttäjätunnuksen käytön kaikissa tarjotuissa palveluissa.

Haka–hankkeessa käytetään pääasiassa Shibboleth–ohjelmistoa käyttäjätietojen varmistamiseen. Shibboleth–ohjelmiston toimintaa pystytään valvomaan AAIEye Probe, sekä AAIEye Server–ohjelmilla, joihin on mahdollista asentaa Nagios–ominaisuus mahdollistaen palvelun tilan seuraamisen suoraan Centreon-käyttöliittymästä (Kuvio 42).



Kuvio 42. Nagios Shibboleth tarkistukset

AAIEye Probe on Shibboleth:n yhteydessä toimiva sovellus, joka analysoi Shibboleth–palvelun luomia lokeja ja laatii näiden pohjalta yhteenvedon kirjautumisista, joka lähetetään CSC:n palvelimelle (Kuvio 43).

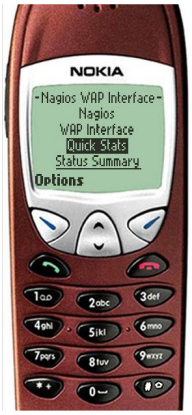


Kuvio 43. Nagioksen toiminta Yhdessä AAIEye kanssa

AAIEye Server on Shibboleth:n yhteydessä toimiva sovellus, joka huolehtii kirjautumistestien ajamisesta, sekä kirjautumistilastojen kokoamisesta. AAIEye Server vastaanottaa AAIEye probelta dataa, sekä ajaa tarvittavat monitorointitestit. AAIEye Serveriä voidaan hallinnoida suoraan Nagioksesta käsin, mikäli tämän mahdollistava lisäominaisuus on asennettu. Olisi syystä harkita Shibboleth – järjestelmän liittämistä Nagiokseen ylläpitämisen helpottamiseksi (Haka-palveluiden monitorointi).

7.6 WAP-käyttöliittymä

Nagios mahdollistaa myös WAP-käyttöliittymän mobiililaitteeseen (Kuvio 44). WAP-käyttöliittymästä ylläpitäjä pystyy näkemään kaikki oleelliset tiedot; tilannepäivitykset, hälytykset, palveluiden ongelmat ym. WAP-käyttöliittymällä ei kuitenkaan pysty tekemään säädöksiä verkonvalvontatyökaluun. WAP-käyttöliittymä palvelee ylläpitäjää samankaltaisesti kuin SMS-hälytykset.



Kuvio 44. WAP-käyttöliittymä

8 Johtopäätökset

Johtopäätöksissä on otettu huomioon asiakkaan kertomat mielipiteet ja projektin tekijöiden omat johtopäätökset työn toteutumisesta.

Projektin aiheena ollut Nagios-verkonvalvontaohjelmisto on osoittautunut päteväksi työkaluksi Laurean kokoisen organisaation käyttöön. Opinnäytetyön aiheena käyttöön otettu verkonvalvontaohjelmisto on tällä hetkellä käytössä Laureassa. Hyviin käyttökokemuksiin ei ole päästy helpolla. Nagios on osoittautunut olevan asiantuntevuutta vaativa ohjelmisto, jonka käyttöönotto on vaatinut suuria ponnisteluja niin asiakkaan asiantuntijoilta kuin projektin tekijöiltäkin. Suuri haaste oli projektin tekijöiden yhteisen ajan löytyminen. Nagios-verkonvalvontaohjelmiston käyttöönoton tekninen vaikeus on riippunut monesta eri tekijästä, kuten asiakkaan verkon rakenteesta, verkon suojauksesta ja verkon yleisistä määräyksistä sekä asetuksista. Lisäksi verkonvalvonta ohjelmiston entuudestaan jokseenkin vieras toimintaympäristö on antanut lisähaastetta toteutuksen onnistumiselle.

Projektia voidaan kuitenkin vaikeuksista huolimatta pitää onnistuneena ja jopa menestyksekkäänä. Projektille asetetut tavoitteet on saavutettu lähestulkoon kaikki. Opinnäytetyön kehittämisideoihin on lisätty projektin osat, joita ei aikataulun puolesta ole kyetty toteuttamaan. Nämä asiat kuuluivat alun perin projektisuunnitelmaan. Asiakkaan eli Laurean näkökulmasta projekti avaa uusia mahdollisuuksia tämän ohjelmiston jatkokehittämiselle. Asiakkaan antamat vaatimusmäärittelyt työlle on toteutettu, kiteytettynä ne tarkoittavat toimivaa kustannustehokasta verkonvalvonta ohjelmistoa.

Nagios-verkonvalvontaohjelmisto on osoittanut olevansa yhtä kattava, käytettävä ja luotettava kuin kalliit kilpailijansa sekä laajennettavuudeltansa jopa kilpailijoidensa edellä. Nagios suorittaa samat verkonvalvonta operaatiot samoilla protokollilla ja samankaltaisin tekniikoin kuin kilpailijansa. Erona on vain se, että Nagios on ilmainen ja avoimeen lähdekoodiin perustuva ohjelmisto. Vastaavanlaisia avoimeen lähdekoodiin perustuvia verkonvalvontaohjelmistoja on olemassa, mutta emme ole projektin aikana vertailleet kustannus syistä ja ajallisista syistä Nagiosta kilpailijoihinsa muuten kuin kilpailijoiden julkisten puheiden ja käyttökokemusten perusteella. Suurimpana erona kilpailijoihin voidaan puhua hinnan lisäksi käyttöönotosta. Käyttöönotto voisi hinnakkaan kilpailijan tuotteella olla helpompi.

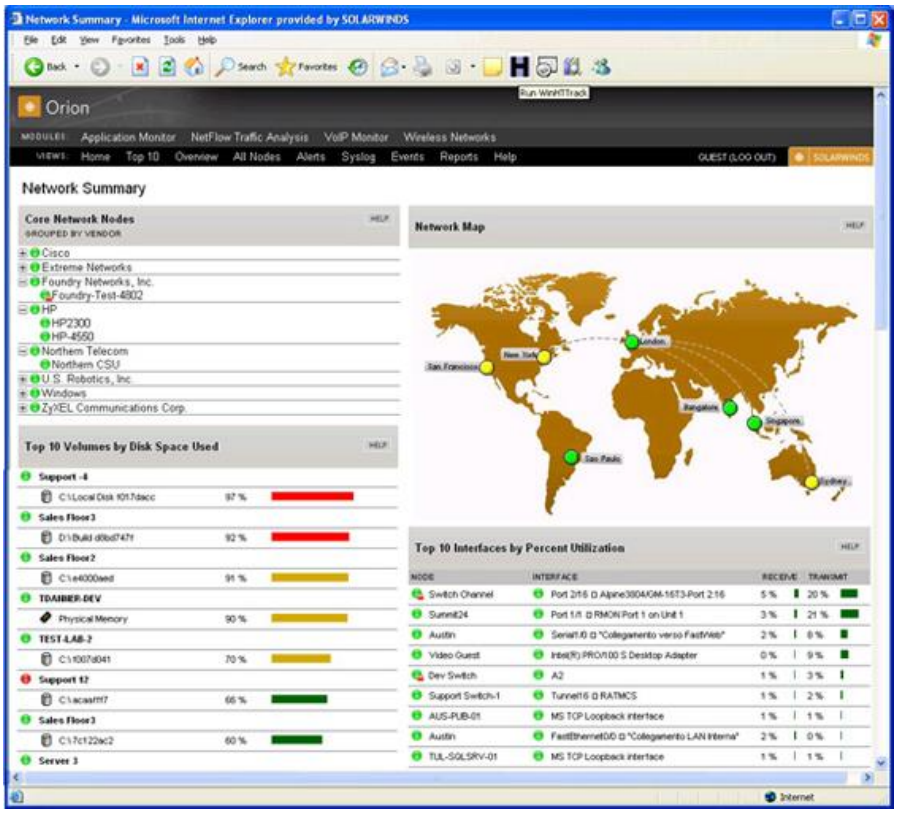
Tässä opinnäytetyössä tavoitteena oli tutkia lähinnä ilmaisia verkonvalvontaohjelmistoja, joten kovin suurta painoarvoa ei annettu maksullisten ratkaisujen tutkimiseen. Esimerkkinä maksullisesta verkonvalvontaratkaisusta voidaan ottaa Castle Rock Computing, Inc. –yrityksen tarjoamat ohjelmistot. Castle Rock Computing tarjoaa SNMPc7 Network Manager-ohjelmistoa, josta löytyy kaksi eri versiota: SNMPc Enterprise Edition ja SNMPc Workgroup Edition. Lisäksi

yritys tarjoaa erillisenä lisäohjelmana Online-mahdollisuuden ohjelmistolle. Ohjelmistopaketin hinnoittelu on seuraavanlainen:

- SNMPc 7.1 Enterprise Edition: $4,995
- Päivitykset ja tuki: $1,995 / vuosi
- SNMPc 7.1 Workgroup Edition (max 1000 laitetta, 1 käyttäjä): $1,795
- Päivitykset ja tuki: $695 / vuosi
- Online-käyttömahdollisuus (Online 2009 plugin for SNMPc enterprise): $6.995
- Online-käyttömahdollisuus + SNMPc 7.1 Enterprise Edition: $10,995

Kuten yllä olevasta hinnoittelusta nähdään on valmiin verkonvalvontaratkaisun käyttöönotto melko kallista. Laurean tapauksessa olisi siis Nagiosta vastaavan järjestelmän hinnaksi tullut $10,995 + $1,995 / vuosi (Castle Rock Computing 2009).

Ryhmä tutki muitakin kaupallisia verkonvalvontaohjemistoja. Solarwinds on ohjelmisto, joka tarjoaa suuren joukon erilaisia työkaluohjelmistoja tietoverkkojen ja palvelujen valvontaan sekä ylläpitoon. Solarwindsin tunnetuin tuote on Orion NPM verkonvalvontaohjelmisto (kuvio 45). Solarwindsin tuotteissa helppokäyttöisyys on pääosassa ja keskitytään valvontajärjestelmän ylläpitämisen sijaan itse asiaan eli verkkojen ja palvelujen valvontaan sekä raportointiin. Solarwindsin ohjelmiston lähtöhinta on 2015€ jolla saa tuen 100 valvottavalle laitteelle. Rajattoman määrän laitteita sisältävän lisenssin hinta on 17090€ (Solarwinds, 2009).



Kuvio 45. Solarwinds Orion

Nagioksen käytöstä löytyy maailmalta useita hyviä käyttökokemuksia. Alla listattuna muutaman yrityksen kokemuksia Nagioksen käyttöönotosta:

Banrisul (Banco de Estado do Rio Grande do Sul) on 12. isoin pankki Brasiliassa. Pankille on yli 460 konttoria Brasiliassa ja se palvelee yli 3 miljoonaa asiakasta. Banrisul käyttää monimutkaista IT-infrastruktuuria Brasilian pankkijärjestelmästä ja pankkijärjestelmien säännöksistä johtuen. Banrisul käytti useiden isojen yrityksien valvontaohjelmistoja (IBM, HP, CA ja BMC). Yrityksellä oli tarvetta keskitetylle verkonvalvonnalle joka mahdollistaisi koko IT-infrastruktuurin tarkastelun yhden käyttöliittymän alta. OPServices-niminen yritys räätälöi Nagios-pohjaisen verkonvalvonnan vastaamaan Banrisulin tarpeita. Nagios-järjestelmän käyttöönotton jälkeen Banrisulin verkonvalvontakustannukset tippuivat 80% (Case Banrisul, 2009).

Sunrise Communications AB on Sveitsin suurin yksityinen internet-palveluntarjoaja. Monien yritysfuusioiden ja uudelleenjärjestelyiden johdosta yrityksellä oli useita eri valvontajärjestelmiä käytössä (BMC Patrol, CA Spectrum, Big-Brother). Yrityksen tietotaito verkonvalvonnan suhteen oli myös hajautettu useisiin eri paikkoihin ja järjestelmiin. Sunrise Communications halusi yhtenäistää verkonvalvontansa yhden järjestelmän alle. Haasteena projektissa oli yrityksen haluama nopea aikataulu, laitteiden monimuotoisuus ja budjetin pienuus. Nagioksen käyttöönoton jälkeen yrityksen kustannustehokkuus parani huomattavasti, vikojen selvitykseen käytetty aika pieneni huomattavasti ja osa pidempään vaivanneista ongelmista katosi kokonaan (Case Sunrise Communications AB).

”Nagioksen avulla saimme vähennettyä usean kaupallisen valvontaohjelmiston määrän yhteen samalla vähentäen ylläpitokustannuksia” (Michael Niedermann, Tietohallintopäällikkö, Sunrise Communications AG)

Muita yrityksiä jotka käyttävät Nagiosta ovat esimerkiksi: 3Com, Amazon.com, AT&T, Domino’s Pizza, EBay, Google, HP invent, IBM, Myspace, Symantec, Twitter, Yahoo.

Kuten yllä olevissa esimerkeissä tulee ilmi, on Nagios kustannustehokas ohjelma. Lisäksi Nagiksen käyttöönotto on mahdollista todella suurissakin organisaatioissa.

Opetusarvoltaan työ on ollut antoisa. Projektin jäsenet ovat kehittyneet ammatillisesti IT-alan projektin hallinnassa, sekä järjestelmän käyttöönotossa yrityksessä. Projektin tuloksesta kuuluu suuri kiitos Laurea-ammattikorkeakoulun IT-asiantuntija Isto Haminalle. Ilman hänen panostaan sekä mielenkiintoa työtä kohtaan projekti tuskin olisi onnistunut.

Lähteet

Sähköiset lähteet:

Case Banrisul, 2009
http://www.nagios.com/supportMedia/files/casestudies/OpServices-Banrisul.pdf

Case Sunrise Communications AB, 2009
<http://www.nagios.com/supportMedia/files/casestudies/Intuit-Sunrise.pdf>

Castle Rock Computing 2009
<http://www.castlerock.com/>

Centreon Wiki
<http://en.doc.centreon.com/Main_Page>

Foster-Johnson 2005. RedHat RPM –guide, Fedora project
http://docs.fedoraproject.org/drafts/rpm-guide-en/

Galstad 2009, Nagios Core Version 3.X documentation
<http://nagios.sourceforge.net/docs/3_0/>

Galstad 2007, NDOutils documentation version 1.4
<http://nagios.sourceforge.net/docs/ndoutils/NDOUtils.pdf>

Galstad 2007, NRPE documentation
<http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf>

Freier, Karlton, Kocher 1996, The SSL Protocol Version 3.0
http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt

Haka-palveluiden monitorointi
http://www.csc.fi/hallinto/haka/tekniikka/valvonta/index_html/?searchterm=nagios

McClogherie 1991, RFC1213
<http://www.faqs.org/rfcs/rfc1213.html>

MySQL AB 2008, MySQL 5.4 Reference Manual
<http://dev.mysql.com/doc/refman/5.4/en/index.html>

The Apache Software Foundation 2009, Apache HTTP server Version 2.2 Documentation
<http://httpd.apache.org/docs/2.2/>

Oetiker, RRDTool dokumentointi
<http://oss.oetiker.ch/rrdtool/doc/rrdtool.en.html>

Waldbusser 2000, RFC2819
<http://tools.ietf.org/html/rfc2819>

Kirjalliset lähteet:

Jaakohuhta & Lahtinen 1997. Tietoliikenneverkot – Tehokäyttäjän Opas.
Jyväskylä: Gummerrus Kirjapaino Oy.

Jaakohuhta 2003. IT- Ensyklopedia
Helsinki, Edita Prima Oy.

Kaario 2002. TCP/IP-verkot
Helsinki, WSOY.

Kuvat

Liitteet

Liite 1: Nagios ja Centreon asennus

Alhaalla käydään läpi Nagios – ympäristön asennus kohta kohdalta. Mukaan ei tähän raporttiin otettu käyttöjärjestelmän asennusta, koska nämä ovat erilaisia riippuen asennettavasta julkaisusta. Opinnäytetyön Nagios – ympäristö rakennettiin Opensuse 11.1 Linux-julkaisuun. Nagios asennus seuraa pääpiirteittäin alla olevia ohjeita Linux – julkaisusta riippumatta, komentojen syntaksissa tosin saattaa olla joitain eroavaisuuksia. Asennus tapahtuu pääpiirteittäin komentoriviä hyväksi käyttäen. Alla olevassa ohjeessa komennot jotka syötetään komentoriville, on kursivoitu luettavuuden helpottamiseksi.

Nagioksen asennus tarvitsee joitakin esiasennuksia ennen varsinaisen asennuksen aloittamista. Asennetaan aluksi nämä.

\# *yast –i sudo mailx fping iputils dos2unix vron dejavu*

Yast (Yet Another Setup Tool) on RPM-pohjainen asennustyökalu openSUSEen. Asennetaan tämän avulla joitakin lisäohjelmia.

Sudo: Ohjelma joka mahdollistaa komentojen ajamisen eri käyttäjän oikeuksilla. Mahdollistaa komentojen ajamisen esimerkiksi super userina.

Mailx: Sähköpostiohjelma. Päivitetty versio openSUSEn mukana tulevaan mail ohjelmaan.

Fping: Päivitetty versio ping ohjelmaan. Mahdollistaa ICMP pakettien lähettämisen useisiin palvelimiin kerralla. Nopeuttaa suurien palvelinmäärien tarkistusta.

Dos2unix: Konvertoi ASCII – tekstitiedoston UNIX muodosta DOS – muotoon tai toisinpäin.

\# *yast –i gcc gcc-c++ make automake*

Asennetaan kääntäjä GNU Compiler Collection. Mahdollistaa C,C++, Objective-C, Fortran, Java sekä Ada – kielillä kirjoitettujen ohjelmien kääntämisen.

\# *yast –i apache2*
\# *yast –i php5 php5-mysql apache2-mod_php5 php5-pear php5-ldap php5-snmp php5-gd php5 –soap php5-posix php5-gettext php5-mbstring php5-session php5-xml*

Asennetaan apache2 nettipalvelinohjelmistoksi sekä PHP5-ohjelmisto. Ohjelmistojen käyttötarkoitus on selitetty tarkemmin opinnäytetyön termit-osiossa.

yast –i mysql libmysqlclient15-devel perl-dbd-mysql

Asennetaan MySQL – palvelin. Ohjelma on selitetty tarkemmin opinnäytetyön termit osiossa.

yast –i rrdtool

Asennetaan RRDTool. Ohjelma on selitetty tarkemmin opinnäytetyön termit-osiossa.

yast –i perl-Config-IniFiles

Asennetaan Perl. Ohjelma on selitetty tarkemmin opinnäytetyön termit-osiossa.

yast –i net-snmp perl-Net-SNMP perl-SNMP

Asennetaan SNMP. Ohjelma on selitetty tarkemmin opinnäytetyön verkonhallinnan standardit ja protokollat
.

yast –i gd libjpeg-devel libpng-devel fontconfig-devel freetype2-devel

Asennetaan GD Library. GD on avoimeen lähdekoodiin perustuva ohjelma joka mahdollistaa yleisimpien kuvaformaattien muokkaamisen.

Näiden ohjelmien asennuksen jälkeen päästään asentamaan itse Nagiosta.

```
# /usr/sbin/useradd -m nagios -p Salasana
# /usr/sbin/groupadd nagios
# /usr/sbin/usermod -G nagios nagios
# /usr/sbin/groupadd nagcmd
# /usr/sbin/usermod -A nagcmd nagios
# /usr/sbin/usermod -G nagcmd nagios
# /usr/sbin/usermod -A nagcmd wwwrun
# /usr/sbin/usermod -G nagcmd wwwrun
```

Luodaan tarvittavat käyttäjät ja ryhmät sekä siirretään käyttäjät oikeisiin ryhmiin.

cd /usr/local/src

 # wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.1.2.tar.gz

Siirrytään latauskansioon ja haetaan Nagios –paketti.

 # tar –xzf nagios-3.1.2.tar.gz
 # cd nagios-3.1.2

Puretaan haettu paketti ja siirrytään kansioon jonne Nagios purettiin.

 # ./configure --prefix=/usr/local/nagios --with-command-group=nagcmd --enable-
nanosleep --enable-event-broker
 # make all
 # make install
 # make install-init
 # make install-commandmode
 # make install-config
 # make install-webconf

Luodaan asennustiedostot halutuilla asetuksilla. Tämän jälkeen asennetaan Nagios.

 # cd /usr/local/src
 # wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins- 1.4.13.tar.gz

Nagioksen asennuksen jälkeen siirrytään asentamaan Nagioksen käyttämät pluginit. Siirrytään latauskansioon, haetaan plugin-paketti.

 # tar -xzf nagios-plugins-1.4.13.tar.gz
 # cd nagios-plugins-1.4.13

Puretaan tiedosto ja siirrytään purettuun kansioon.

 # ./configure --with-nagios-user=nagios --with-nagios-group=nagios

```
#       make
#       make install
```

Konfiguroidaan käyttämään käyttäjää nagios sekä ryhmää nagios. Tämän jälkeen asennetaan pluginit make-komennolla.

Pluginien asennuksen jälkeen siirrytään NDOutilsin asennukseen. NDOutils on tarkemmin selitetty opinnäytetyön termit-osiossa.

```
#       cd /usr/local/src
#       wget http://prdownloads.sourceforge.net/sourceforge/nagios/ndoutils-
        1.4b8.tar.gz
```

Siirrytään latauskansioon ja haetaan ndoutils paketti.

```
#       tar -xzf ndoutils-1.4b8.tar.gz
#       cd ndoutils-1.4b8
```

Puretaan haettu paketti ja siirrytään luotuun kansioon.

```
#       ./configure --prefix=/usr/local/nagios/ --enable-mysql --disable-pgsql \ --with-
        ndo2db-user=nagios --with-ndo2db-group=nagios
#       make
```

Konfiguroidaan ja asennetaan ndoutils.

```
#       cp ./src/file2sock /usr/local/nagios/bin
#       cp ./src/ndomod-3x.o /usr/local/nagios/bin/ndomod.o
#        cp ./src/ndo2db-3x /usr/local/nagios/bin/ndo2db
#        cp ./config/ndo2db.cfg /usr/local/nagios/etc/
#        cp ./config/ndomod.cfg /usr/local/nagios/etc/
```

Kopioidaan ndoutilsin määritystiedostot oikeisiin kansioihin. Kansiossa on myös ndomod-2x.o sekä ndo2db-2x nämä tiedostot on tarkoitettu Nagioksen vanhemman version kanssa käytettäväksi.

*# sudo chmod 774 /usr/local/nagios/bin/ndo**
*# sudo chown nagios:nagios /usr/local/nagios/bin/ndo**

Asetetaan tiedosto-oikeudet ndo-alkuisille tiedostoille nagios kansiossa. 774 numero määräytyy sillä millaiset tiedosto oikeudet annetaan käyttäjälle, ryhmälle ja muille käyttäjille. Ensimmäinen on käyttäjä (read, write, execute 4+2+1 = 7), toinen on ryhmä (read, write, execute) ja kolmas numero viittaa muihin käyttäjiin, joille annetaan vain lukuoikeudet (read = 4).

Chown-komennolla vaihdetaan tiedostojen omistaja ja ryhmä nagiokseksi.

Sudo komennon alussa tarkoittaa sitä, että komento ajetaan superuserina, tätä ei tarvita jos ollaan root-käyttäjänä kirjautuneena sisään.

broker_module=/usr/local/nagios/bin/ndomod.o config_file=/usr/local/nagios/etc/ndomod.cfg

Editoidaan /usr/local/nagios/etc/nagios.cfg käynnistämään NDO:n tarvitsema broker module. Tämä tehdään lisäämällä yllä oleva komento nagios.cfg – tiedoston broker module kohtaan.

On hyvä tarkistaa että nagios.cfg sisältää myös seuraavanlaisen rivin: event_broker_options=-1,tämä ottaa event brokerit käyttöön.

Seuraavaksi luodaan ndo:lle scripti joka mahdollistaa palvelun helpomman käynnistämisen ja lopettamisen. Luodaan /etc/init.d/ndo2db – tiedosto. Ja kopioidaan sinne alla oleva teksti:

#!/bin/sh
#
#
 # chkconfig: 345 99 01
 # description: Nagios to mysql
#
 # Author : Gaëtan Lucas
 # Realase : 07/02/08
 # Version : 0.1 b
 # File : ndo2db
 # Description: Starts and stops the Ndo2db daemon
 # used to provide network services status in a database.
#

```
status_ndo ()
{
        if ps -p $NdoPID > /dev/null 2>&1; then
            return 0
        else
                return 1
        fi

        return 1
}

printstatus_ndo()
{
        if status_ndo $1 $2; then
                echo "ndo (pid $NdoPID) is running..."
        else
                echo "ndo is not running"
        fi
}

killproc_ndo ()
{
        echo "kill $2 $NdoPID"
        kill $2 $NdoPID
}

pid_ndo ()
{
        if test ! -f $NdoRunFile; then
                echo "No lock file found in $NdoRunFile"
                echo -n "       checking runing process..."
                NdoPID=`ps h -C ndo2db -o pid`
                if [ -z "$NdoPID" ]; then
                        echo "    No ndo2db process found"
                        exit 1
                else
                        echo "    found process pid: $NdoPID"
                        echo -n "       reinit $NdoRunFile ..."
```

```
                                        touch $NdoRunFile
                                        chown $NdoUser:$NdoGroup $NdoRunFile
                                        echo "$NdoPID" > $NdoRunFile
                                        echo "     done"
                                fi
                        fi

                        NdoPID=`head $NdoRunFile`
}

# Source function library
# Solaris doesn't have an rc.d directory, so do a test first
if [ -f /etc/rc.d/init.d/functions ]; then
                        . /etc/rc.d/init.d/functions
elif [ -f /etc/init.d/functions ]; then
                        . /etc/init.d/functions
fi

prefix=/usr/local/nagios
exec_prefix=${prefix}
NdoBin=${exec_prefix}/bin/ndo2db
NdoCfgFile=${prefix}/etc/ndo2db.cfg
NdoRunFile=${prefix}/var/ndo2db.run
NdoLockDir=/var/lock/subsys
NdoLockFile=ndo2db.lock
NdoUser=nagios
NdoGroup=nagios

# Check that ndo exists.
if [ ! -f $NdoBin ]; then
  echo "Executable file $NdoBin not found.  Exiting."
  exit 1
fi

# Check that ndo.cfg exists.
if [ ! -f $NdoCfgFile ]; then
  echo "Configuration file $NdoCfgFile not found.  Exiting."
  exit 1
fi
```

```
# See how we were called.
case "$1" in

        start)
                echo -n "Starting ndo:"
                touch $NdoRunFile
                chown $NdoUser:$NdoGroup $NdoRunFile
                $NdoBin -c $NdoCfgFile
                if [ -d $NdoLockDir ]; then
                        touch $NdoLockDir/$NdoLockFile;
                fi
                ps h -C ndo2db -o pid > $NdoRunFile
                if [ $? -eq 0 ]; then
                        echo " done."
                        exit 0
                else
                        echo " failed."
                        $0 stop
                        exit 1
                fi
                ;;

        stop)
                echo -n "Stopping ndo: "

                pid_ndo
                killproc_ndo

                # now we have to wait for ndo to exit and remove its
                # own NdoRunFile, otherwise a following "start" could
                # happen, and then the exiting ndo will remove the
                # new NdoRunFile, allowing multiple ndo daemons
                # to (sooner or later) run
                #echo -n 'Waiting for ndo to exit .'
                for i in 1 2 3 4 5 6 7 8 9 10 ; do
                    if status_ndo > /dev/null; then
                        echo -n '.'
                        sleep 1
```

```
                else
                        break
                fi
        done
        if status_ndo > /dev/null; then
                echo
                echo 'Warning - ndo did not exit in a timely manner'
        else
                echo 'done.'
        fi

        rm -f $NdoRunFile $NdoLockDir/$NdoLockFile
        ;;

status)
        pid_ndo
        printstatus_ndo ndo
        ;;

restart)
        $0 stop
        $0 start
        ;;

*)
        echo "Usage: ndo {start|stop|restart|status}"
        exit 1
        ;;

esac

# End of this script
```

Scriptin kirjoittamisen jälkeen lisätään vielä ndo käynnistymään automaattisesti palvelimen käynnistyksen yhteydessä. Se tehdään alla olevalla komennolla.

```
#               chkconfig --add ndo2db
#               chmod +x /etc/init.d/ndo2db
```

Chkconfig – komennolla lisätään ndo2db ajettavaksi käynnistymisen yhteydessä ja chmod-komennolla annetaan tiedostolle executable – oikeudet.

NDOutils ei vielä tässä vaiheessa ole asennettu loppuun asti, Centreonin asennuksen jälkeen joudutaan vielä tekemään erinäisiä muutoksia asetustiedostoihin sekä tietokantoihin. Näistä lisää myöhemmin tässä dokumentissa.

Siirrytään asentamaan Centreonia. Haetaan Centreon viralliselta kotisivulta ja ladataan se /usr/local/src – kansioon.

```
#               cd /usr/local/src
```

Siirrytään latauskansioon.

```
#               tar –xzf centreon-2.0.2.tar.gz
#               cd centreon-2.0.2
```

Puretaan ladattu tiedosto ja siirrytään kansioon.

```
#               export PATH="$PATH:/usr/local/nagios/bin/"
```

Export path komennolla estetään tiedostojen hajautuminen useaan paikkaan (nagios, ndomod jne.). Komento aiheuttaa sen, että kaikki tiedostot kopioidaan /usr/local/nagios/bin – kansioon.

```
#               ./install.sh –i
```

Komennolla aloitetaan Centreonin asennus. Alla oleva asennusohjelma käynnistyy, määritellään oikeat polut ja käyttäjät.

```
################################################################################
#

#                   Centreon (www.centreon.com)
#                    Thanks for using Centreon
#
```

```
#                          v 2.0
#
#                      infos@oreon-project.org
#
#              Make sure you have installed and configured
#              sudo - sed - php - apache - rrdtool - mysql
#
################################################################################
--------------------------------------------------------------------
      Checking all needed binaries
--------------------------------------------------------------------
rm                                        OK
cp                                       OK
mv                                        OK
chmod                                      OK
chown                                      OK
echo                                      OK
cat                                      OK
more                                       OK
mkdir                                      OK
find                                     OK
sed                                      OK
```

Tässä kohtaa näytetään Centreonin lisenssiehdot. Ehdot tulee lukea loppuun asti, ja tämän jälkeen tulee päättää hyväksytäänkö ne, vai ei. Jos ehtoja ei hyväksytä, asennus päättyy.

```
This General Public License does not permit incorporating your program into
proprietary programs.  If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library.  If this is what you want to do, use the GNU Library General
Public License instead of this License.

Do you accept GPL license ?
[y/n], default to [n]:
> y
```

Seuraavaksi kysytään mitä osia Centreonista halutaan asentaa. Vastataan kaikkiin yes.

```
--------------------------------------------------------------------
```

Please choose what do you want to install

Do you want to install Centreon Web Front
[y/n], default to [n]:
> y

Do you want to install Centreon CentCore
[y/n], default to [n]:
> y

Do you want to install Centreon Nagios Plugins
[y/n], default to [n]:
> y

Do you want to install Centreon Snmp Traps process
[y/n], default to [n]:
> y

Tämän jälkeen asennetaan yllä valitut moduulit.

Start CentWeb Installation

Where is your Centreon directory?
default to [/usr/local/centreon]
>

Valitaan kansio jonne centreon halutaan asennettavaksi. Jos painetaan vain enter tässä kohdassa, valitaan oletusarvo. Jos kansiota ei löydy, kysyy asennusohjelma halutaanko kyseinen kansio luoda.

Do you want me to create this directory ? [/usr/local/centreon]
[y/n], default to [n]:
> y
Path /usr/local/centreon OK

Tässä määritellään minne Centreon tallentaa mahdolliset lokitiedostot.

Where is your Centreon log directory
default to [/usr/local/centreon/log/]
>

Do you want me to create this directory ? [/usr/local/centreon/log/]
[y/n], default to [n]:
> y
Path /usr/local/centreon/log/ OK

Tässä määritellään missä Centreonin asetustiedostot sijaitsevat. Tärkeää on tässä vaiheessa huomata se, että jos valitaan joku muu kansio kuin oletuskansio joudutaan tekemään muutoksia muihin asetustiedostoihin. Niinpä suositellaan käytettäväksi oletuspolkua.

Where is your Centreon etc directory
default to [/etc/centreon]
>

Do you want me to create this directory ? [/etc/centreon]
[y/n], default to [n]:
> y
Path /etc/centreon OK
Where is your Centreon generation_files directory?
default to [/usr/local/centreon/]
>
Path /usr/local/centreon/ OK

Polku jossa RRDs.pm sijaitsee. Centstorage sekä centreon pluginit käyttävät tätä.

Where is installed RRD perl modules [RRDs.pm]
default to [/usr/lib/perl5/RRDs.pm]
>/usr/lib/perl5/vendor_perl/5.10.0/i586-linux-thread-multi/RRDs.pm
Path /usr/lib/perl5 OK
/usr/bin/rrdtool OK
/usr/bin/mail OK

PEAR.php –tiedoston sijainti.

Where is PEAR [PEAR.php]

default to [/usr/share/php/PEAR.php]
>/usr/share/php5/PEAR
Path /usr/share/php OK

Selvitetään Nagioksen asennustiedostojen sijainti.

Where is installed Nagios ?
default to [/usr/local/nagios/]
>
Path /usr/local/nagios/ OK

Where is your nagios config file
default to [/usr/local/nagios/etc//nagios.cfg]
>
Path /usr/local/nagios/etc OK

Where is your Nagios var directory ?
default to [/usr/local/nagios/var/]
>
Path /usr/local/nagios/var/ OK

Where is your Nagios plugins (libexec) directory ?
default to [/usr/local/nagios/libexec/]
>
Path /usr/local/nagios/libexec/ OK

Where is your nagios binary ?
default to [/usr/local/nagios/bin/nagios]
>
/usr/local/nagios/bin/nagios OK

Where is your Nagios image directory ?
default to [/usr/local/nagios/share/images/logos/]
>
Path /usr/local/nagios/share/images/logos/ OK

Where is your nagiostats binany ?
default to [/usr/local/nagios/bin/nagiostats]
>

/usr/local/nagios/bin/nagiostats OK
p1_file : /usr/local/nagios/bin/p1.pl OK
/usr/bin/php OK
Finding Apache group : www-data
Finding Apache user : www-data
Finding Nagios user : nagios
Finding nagios user nagios in /etc/passwd OK
Finding Nagios group : nagios
Finding nagios group 'nagios' in /etc/group OK

Seuraavaksi scripti kysyy halutaanko käyttää NDO:ta. Tähän vastataan yes, jotta saadaan kaikki halutut lisäominaisuudet käyttöön.

Do you want use NDO ?
[y/n], default to [n]:
> y

Scripti kysyy NDO moduulien sijaintia.

Where is your NDO ndomod binary ?
default to [/usr/sbin/ndomod.o]
> /usr/local/nagios/bin/ndomod.o
/usr/local/nagios/bin/ndomod.o OK

Konfiguroidaan sudo antamaan Centreonille tarvittavat oikeudet mahdollisten muutoksien tekemiseksi (esimerkiksi Nagioksen uudelleenkäynnistys).

Configure Sudo

Where is sudo configuration file
default to [/etc/sudoers]
>
/etc/sudoers OK
Nagios init script OK
Your sudo is not configure

Do you want I configure your sudo ? (WARNING)
[y/n], default to [n]:
> y
Configuring Sudo OK

Seuraavaksi kysytään joitain tietoja Apache – palvelimeen liittyen.

Configure Apache server

Do you want write Apache configuration file ?
[y/n], default to [n]:
> y
Create '/etc/apache2/conf.d/centreon.conf' OK
Configuring Apache OK

Do you want reload your Apache ?
[y/n], default to [n]:
> n
Preparing Centreon temporary files

Seuraavaksi scripti tarkistaa ja asentaa Centreonin vaatimat php – tiedostot.

Start Centreon Web Front Installation

In process

Change macros for php file
Change macros for php file OK
Copy CentWeb in system directory
CentWeb file installation OK
Install Centreon cron OK

Osa PEAR – kirjastoista puuttuu tässä vaiheessa, mutta ne haetaan ja päivitetään automaattisesti jos asennuskoneessa on yhteys Internetiin.

Pear Modules
Check PEAR modules
PEAR 1.5.0 1.4.11 NOK
DB 1.7.6 NOK
DB_DataObject 1.8.4 NOK
DB_DataObject_FormBuilder 1.0.0RC4 NOK
MDB2 2.0.0 NOK
Date 1.4.6 NOK
HTML_Common 1.2.2 NOK
HTML_QuickForm 3.2.5 NOK
HTML_QuickForm_advmultiselect 1.1.0 NOK
HTML_Table 1.6.1 NOK
Archive_Tar 1.1 1.3.1 OK
Auth_SASL 1.0.1 NOK
Console_Getopt 1.2 1.2 OK
HTTP 1.2.2 NOK
Image_GraphViz 1.1.0 NOK
Net_SMTP 1.2.8 NOK
Net_Socket 1.0.1 NOK
Net_Traceroute 0.21 NOK
Net_Ping 2.4.1 NOK
Validate 0.6.2 NOK
XML_RPC 1.4.5 NOK
SOAP 0.10.1 NOK
Log 1.9.11 NOK
.

Do you want I install/upgrade your PEAR modules
[y/n], default to [y]:
> y

Upgrading PEAR modules
PEAR 1.5.0 1.4.11 1.7OK
Installing PEAR modules

DB 1.7.6 1.7.13 OK
DB_DataObject 1.8.4 1.8.8 OK
DB_DataObject_FormBuilder 1.0.0RC4 1.0.0RC7 OK
MDB2 2.0.0 2.4.1 OK
HTML_QuickForm_advmultiselect 1.1.0 1.4.1 OK
HTML_Table 1.6.1 1.8.2 OK
Auth_SASL 1.0.1 1.0.2 OK
HTTP 1.2.2 1.4.0 OK
Image_GraphViz 1.1.0 1.2.1 OK
Net_SMTP 1.2.8 1.3.0 OK
Net_Traceroute 0.21 0.21.1 OK
Net_Ping 2.4.1 2.4.3 OK
Validate 0.6.2 0.8.1 OK
XML_RPC 1.4.5 1.5.1 OK
SOAP 0.10.1 0.11.0 OK
Log 1.9.11 1.10.1 OK

Päivityksen jälkeen scripti tarkistaa vielä kerran moduulit. Jos kaikki on OK, siirrytään seuraavaan kohtaan.

Check PEAR modules
PEAR 1.5.0 1.7.1 OK
DB 1.7.6 1.7.13 OK
DB_DataObject 1.8.4 1.8.8 OK
DB_DataObject_FormBuilder 1.0.0RC4 1.0.0RC7 OK
MDB2 2.0.0 2.4.1 OK
Date 1.4.6 1.4.7 OK
HTML_Common 1.2.2 1.2.4 OK
HTML_QuickForm 3.2.5 3.2.10 OK
HTML_QuickForm_advmultiselect 1.1.0 1.4.1 OK
HTML_Table 1.6.1 1.8.2 OK
Archive_Tar 1.1 1.3.2 OK
Auth_SASL 1.0.1 1.0.2 OK
Console_Getopt 1.2 1.2.3 OK
HTTP 1.2.2 1.4.0 OK
Image_GraphViz 1.1.0 1.2.1 OK
Net_SMTP 1.2.8 1.3.0 OK
Net_Socket 1.0.1 1.0.8 OK
Net_Traceroute 0.21 0.21.1 OK

Net_Ping 2.4.1 2.4.3 OK
Validate 0.6.2 0.8.1 OK
XML_RPC 1.4.5 1.5.1 OK
SOAP 0.10.1 0.11.0 OK
Log 1.9.11 1.10.1 OK
All PEAR module OK

Centreon Post Install

Create /usr/local/centreon/www/install/install.conf.php OK
Create /etc/centreon/instCentWeb.conf OK

Seuraavaksi asennetaan CentStorage, toiselta nimeltään ODS (Oreon Data Storage). Tällä hetkellä CentStorage mahdollistaa RRD:n sekä MySQL:n käytön. Lisäksi CentStorage mahdollistaa erilaisten graafien luomisen Centreonin kautta.

Start CentStorage Installation

Where is your Centreon Run Dir directory?
default to [/var/run/centreon]
>

Do you want me to create this directory ? [/var/run/centreon]
[y/n], default to [n]:
> y
Path /var/run/centreon OK

Where is your CentStorage binary directory
default to [/usr/local/centreon/bin]
>

Do you want me to create this directory ? [/usr/local/centreon/bin]
[y/n], default to [n]:
> y
Path /usr/local/centreon/bin OK

```
Where is your CentStorage RRD directory
default to [/var/lib/centreon]
>


Do you want me to create this directory ? [/var/lib/centreon]
[y/n], default to [n]:
> y
Path /var/lib/centreon                              OK
Finding Nagios group :                              nagios
Finding nagios group 'nagios' in /etc/group         OK
Finding Nagios user :                               nagios
Finding nagios user nagios in /etc/passwd           OK
Preparing Centreon temporary files
/tmp/centreon-setup exists, it will move...
Creating Centreon Directory '/var/lib/centreon/status'    OK
Creating Centreon Directory '/var/lib/centreon/metrics'   OK
Replace Centstorage Macro                           OK
Set CentStorage properties                          OK
Replace Centstorage init script Macro               OK

Do you want I install CentStorage init script ?
[y/n], default to [n]:
> y

Do you want I install CentStorage run level ?
[y/n], default to [n]:
> y
Adding system startup for /etc/init.d/centstorage ...
  /etc/rc0.d/K30centstorage -> ../init.d/centstorage
  /etc/rc1.d/K30centstorage -> ../init.d/centstorage
  /etc/rc6.d/K30centstorage -> ../init.d/centstorage
  /etc/rc2.d/S40centstorage -> ../init.d/centstorage
  /etc/rc3.d/S40centstorage -> ../init.d/centstorage
  /etc/rc4.d/S40centstorage -> ../init.d/centstorage
  /etc/rc5.d/S40centstorage -> ../init.d/centstorage
Set logAnalyser properties                          OK
Set nagiosPerfTrace properties                      OK
```

Install CentStorage cron OK
Create /etc/centreon/instCentStorage OK

CentStorage on tämän jälkeen asennettu. Seuraavaksi siirrytään SNMP:n asennukseen.

Where is your SNMP configuration directory
default to [/etc/snmp]
>
/etc/snmp OK
Where is your SNMPTT binaries directory
default to [/opt/snmptt]
> /usr/local/src/centreon-2.0-b3/snmptt
/usr/local/src/centreon-2.0-b3/snmptt

Vastataan scriptin kysymyksiin liittyen Centreonin pluginien sijantiin.

Start CentPlugins Installation

Where is your CentPlugins lib directory
default to [/var/lib/centreon]
>
Path /var/lib/centreon OK
Finding Nagios user : nagios
Finding nagios user nagios in /etc/passwd OK
Finding Nagios group : nagios
Finding nagios group 'nagios' in /etc/group OK
Preparing Centreon temporary files
/tmp/centreon-setup exists, it will move...
CentPlugins is installed

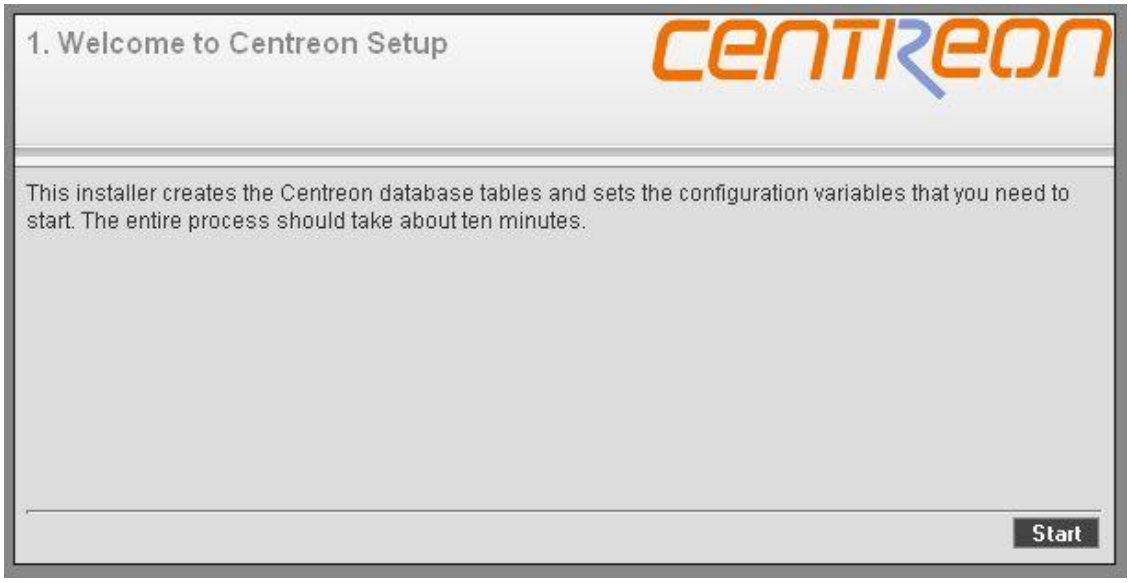
Käynnistetään Apache2 palvelin uudestaan tässä vaiheessa seuraavalla komennolla.

 # service apache2 restart

Centreon ei vielä tässä vaiheessa ole loppuun asti asennettu, vaan vaaditaan vielä selainpohjaisen loppuasennuksen suorittaminen. Jos apache –palvelin on toiminnassa otetaan yhteys

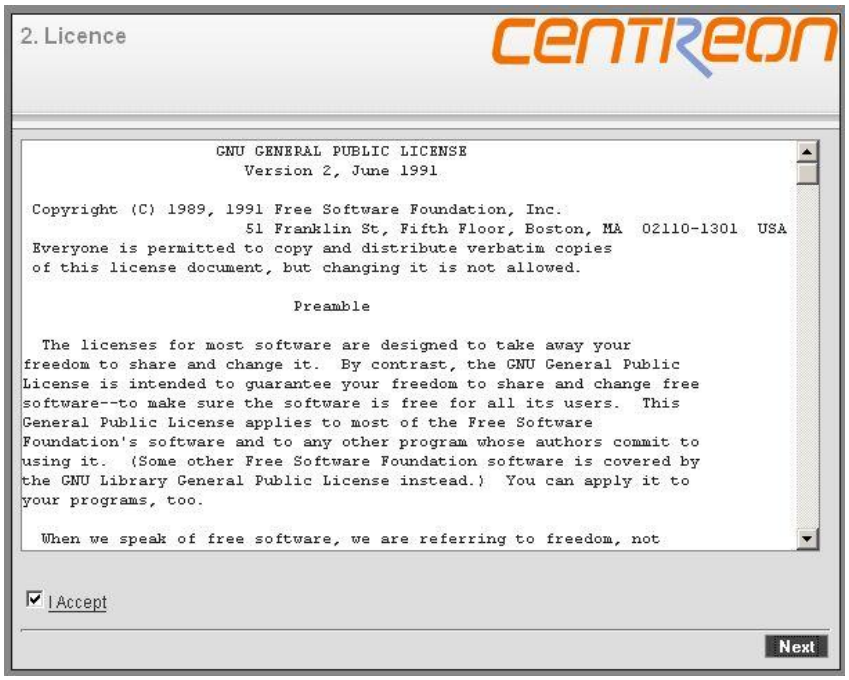
Centreoniin osoitteessa: http://localhost/centreon. Selain ohjautuu automaattisesti oikeaan paikkaan (http://localhost/centreon/install/setup.php).

Web-asennuksen alku:



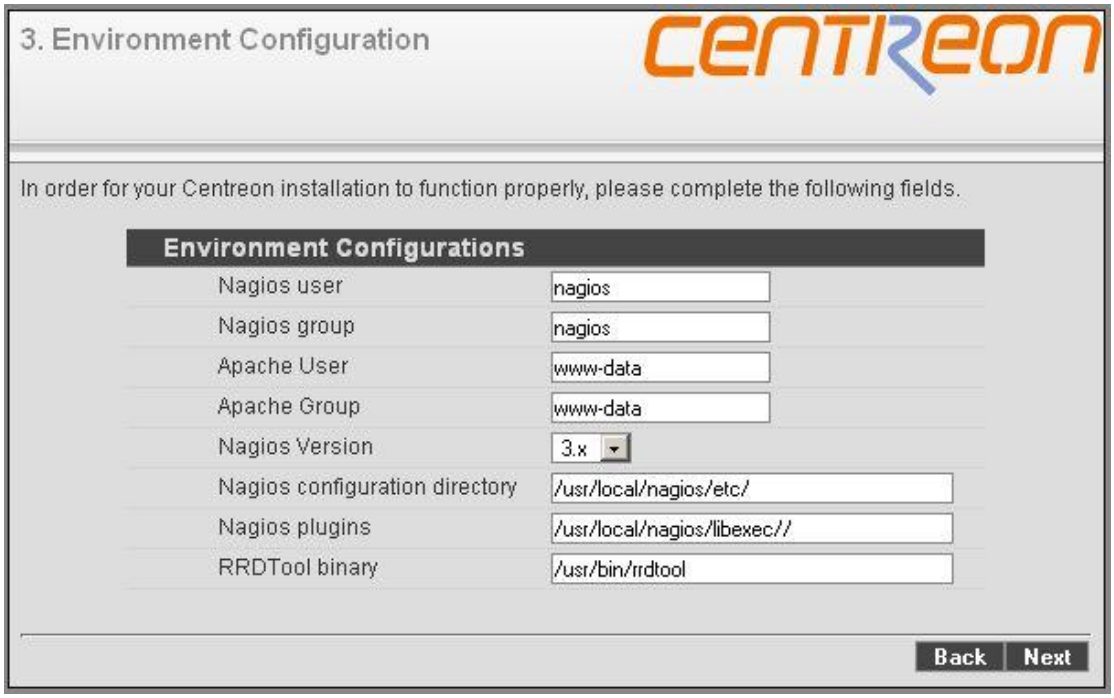
Kuvio 46. Centreon WWW-asennus 1

Luetaan ja hyväksytään käyttösäännöt.



Kuvio 47. Centreon WWW-asennus 2

Määritetään ympäristymuuttujat. Nagioksen käyttäjänimi, ryhmä jne.

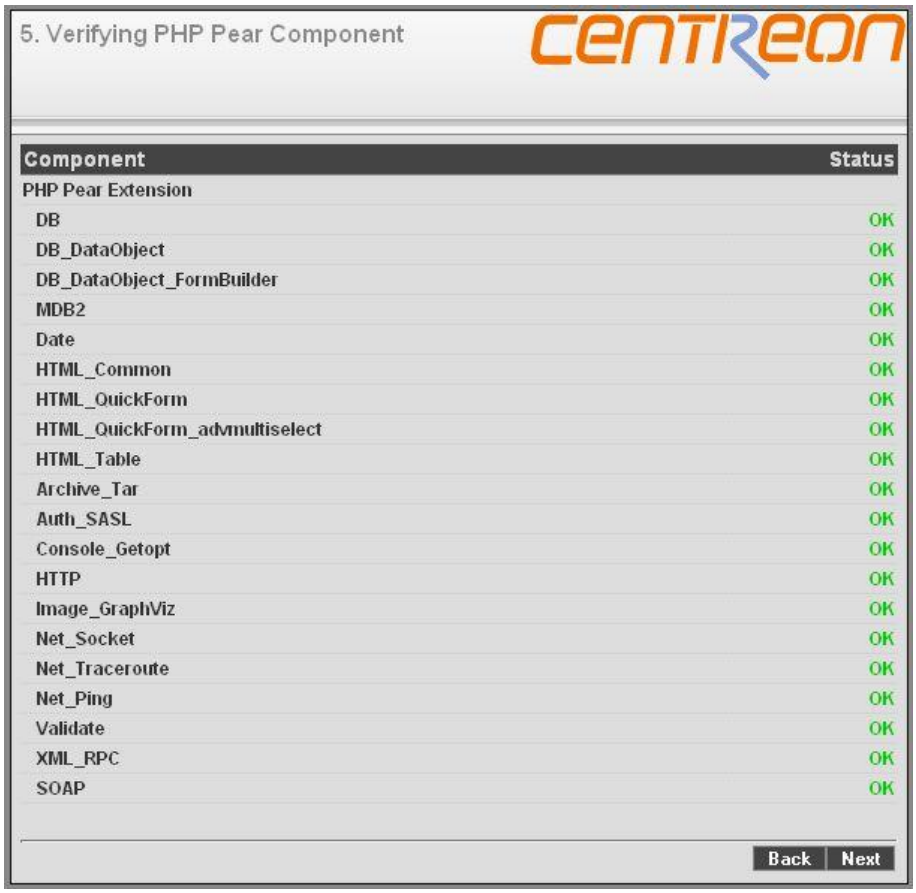


Kuvio 48. Centreon WWW-asennus 3

Asennusohjelma tarkistaa PHP-komponentit sekä käyttöoikeudet Nagiokseen asetustiedostojen kansioon.

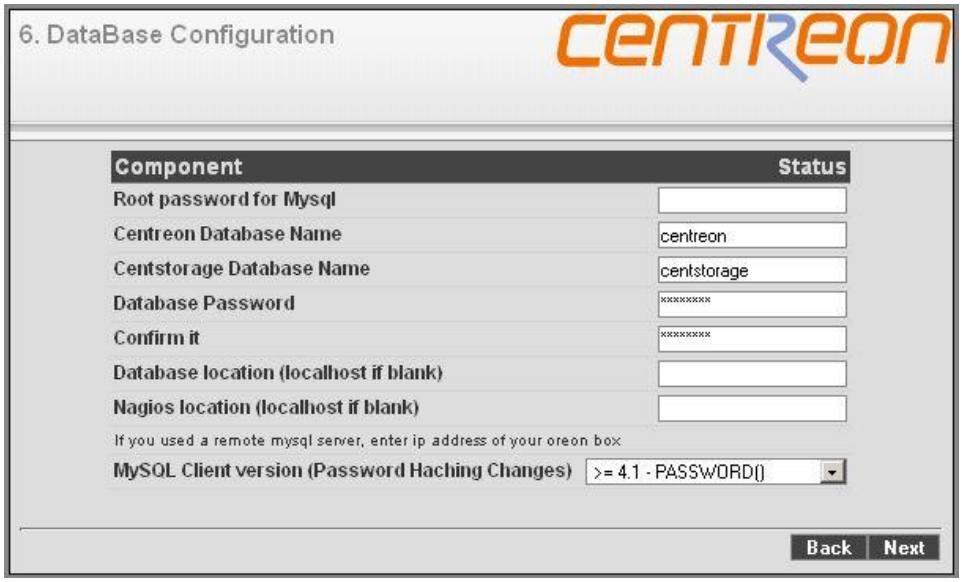
Kuvio 49. Centreon WWW-asennus 4

Tarkistetaan Pear-komponenttien toimivuus.



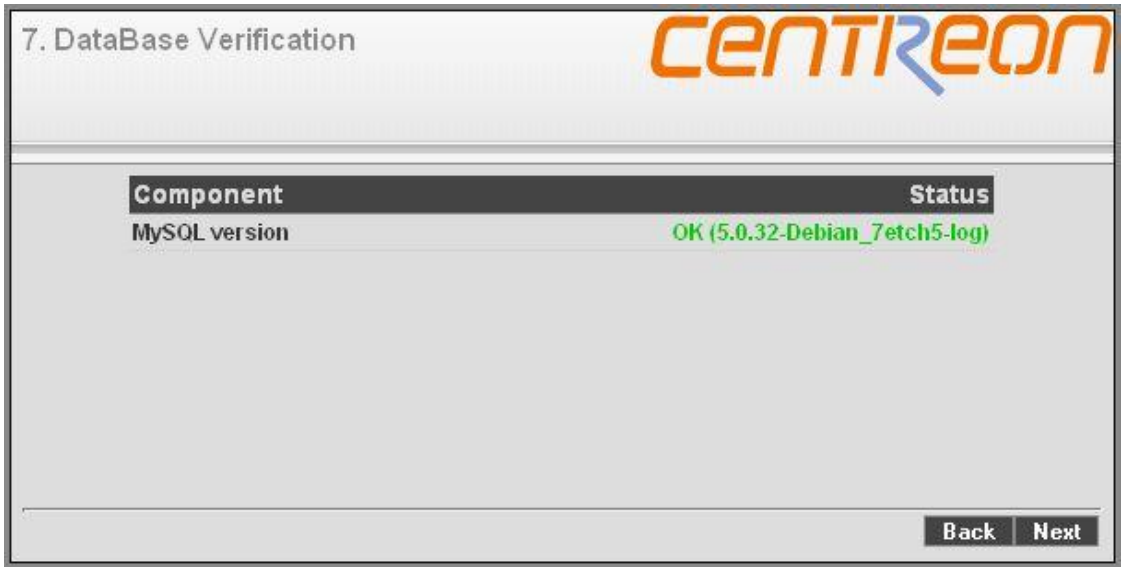
Kuvio 50. Centreon WWW-asennus 5

Määritetään tietokannan asetukset. Syötetään root-salasana ylimpään ruutuun. Tarkistetaan että tietokannan nimet sekä salasanat ovat oikein.



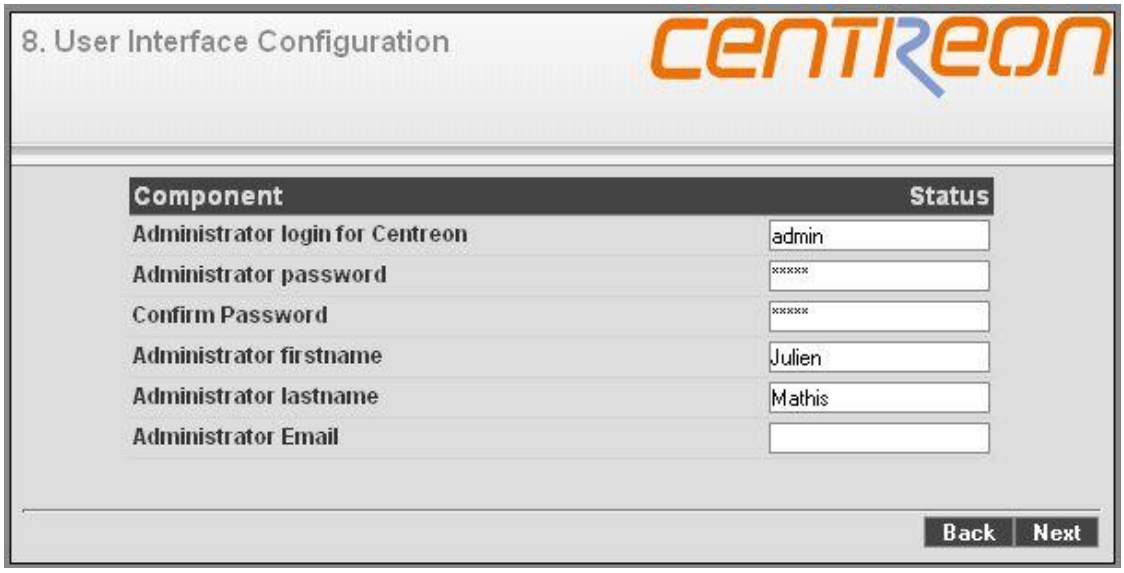
Kuvio 51. Centreon WWW-asennus 6

Ohjelma tarkistaa MySQL:n version.



Kuvio 52. Centreon WWW-asennus 7

Luodaan ylläpitäjätili Centreoniin.

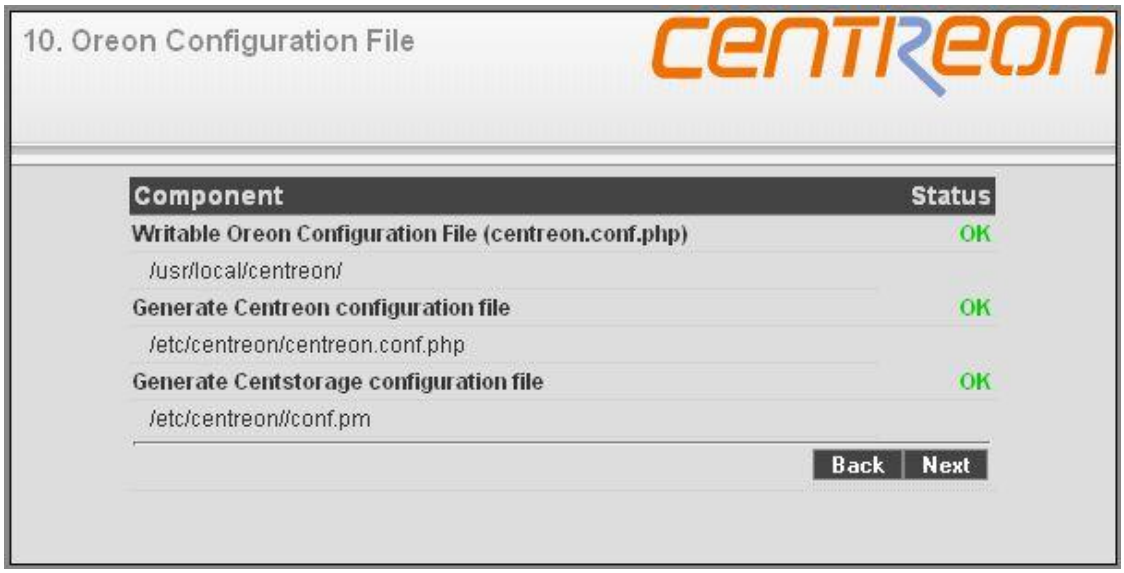


Kuvio 53. Centreon WWW-asennus 8

Otetaan LDAP – autentikointi käyttöön jos näin halutaan. Tässä asennuksessa ei otettu LDAP:a käyttöön.

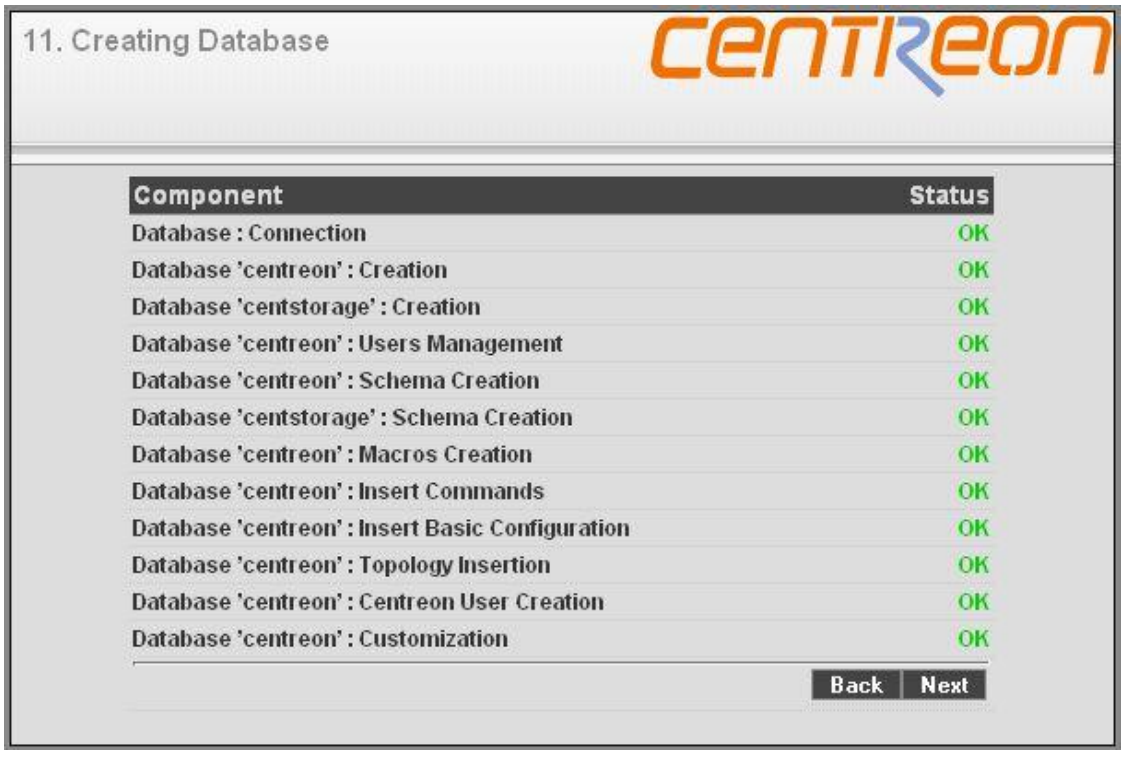
Kuvio 54. Centreon WWW-asennus 9

Tarkistetaan asetustiedostot sekä kirjoitusoikeudet. Jos järjestelmä ei anna OK – vastausta kannattaa tarkistaa, että apachen käyttäjällä on kirjoitusoikeudet Centreonin etc – kansioon.



Kuvio 55. Centreon WWW-asennus 10

Asennusohjelma luo tarvittavat tietokannat. Jos tässä tulee virheitä, ovat tietokanta-asetukset todennäköisesti väärin.



Kuvio 56. Centreon WWW-asennus 11

Asennus loppuu.

Kuvio 57. Centreon WWW-asennus 12

Kuvio 58. Centreon WWW-asennus 13

Jos syötetään sama osoite kuin aiemmin (http://localhost/centreon) järjestelmä ei enää ohjaudu asennusohjelmaan vaan esiin tulee sisäänkirjautumisruutu.

Tässä vaiheessa Centreon on asennettu. Siirrytään seuraavaksi NDO:n loppujen asetuksien laittamiseen.

Aloitetaan luomalla NDO:n käyttämä tietokanta.

Kirjaudutaan mysql – palvelimelle sisään root käyttäjänä. – p määrittää sen että järjestelmä pyytää syöttämään root-salasanan. Luodaan tietokanta alla olevien komentojen avulla. Annetaan myös tarvittavat oikeudet tietokantaan.

```
#       mysql –u root –p
        mysql> CREATE DATABASE `ndo` DEFAULT CHARACTER SET utf8
                COLLATE utf8_general_ci;
        mysql> exit
#       mysql –u root –p ndo <
        /usr/local/src/centreon2.0.2/www/install/createNDODB.sql
#       mysql –u root –p
        mysql> GRANT SELECT , INSERT , UPDATE , DELETE on `ndo` . * TO 'centreon'@'localhost';
        mysql> exit
```

Määritetään Centreonin tietokannan käyttäjä.

```
#       mysql -u root
        mysql> use centreon;
        mysql> update cfg_ndo2db set db_user = 'centreon';
        mysql> exit;
```

Vaihdetaan tietokannan salasana.

```
#       mysql -u root
        mysql> use centreon;
        mysql> update cfg_ndo2db set db_pass = 'XXXXXXX';
        mysql> exit;
```

Seuraavaksi päivitetään NDOutilsin asetustiedostot (ndo2db.cfg ja ndomod.cfg). Oletuksena käytetään unix – sockettia, centreon sen sijaan etsii oletuksena TCP sockettia. Tämä johtaa seuraavanlaiseen virheilmoitukseen: ”ndomod: Could not open data sink! I’ll keep trying, but some output may get lost...”. Muutetaan ndo2db.cfg tiedostossa järjestelmä käyttämään TCP sockettia. Tiedosto sijaitsee /usr/local/nagios/etc/ndo2db.cfg

Alla esimerkki käytössä olevasta asetustiedostosta.

```
##############################################################################
```

```
#
#                  GENERATED BY CENTREON
#
#            Developped by :
#               - Julien Mathis
#               - Romain Le Merlus
#
#                     www.centreon.com
#             For information : contact@centreon.com
##############################################################################
#
#       Last modification August 3, 2009, 1:35 pm
#       By harri_groning
#
##############################################################################

ndo2db_user=nagios
ndo2db_group=nagios
socket_type=tcp
socket_name=/var/run/ndo.sock
tcp_port=5668
db_servertype=mysql
db_host=localhost

db_name=ndo
db_port=3306
db_prefix=nagios_
db_user=centreon
db_pass=XXXXXXXXXXXX
max_timedevents_age=1440
max_systemcommands_age=1440
max_servicechecks_age=1440
max_hostchecks_age=1440
max_eventhandlers_age=1440
```

Lisäksi tehdään tarvittavat muutokset myös ndomod.cfg – tiedostoon, joka sijaitsee samassa paikassa. Muistetaan laittaa output osoitteeksi 127.0.0.1. Alla esimerkki ndomod.cfg – tiedostosta.

```
##############################################################################
#
#                  GENERATED BY CENTREON
#
#             Developped by :
#                - Julien Mathis
#                - Romain Le Merlus
#
#                     www.centreon.com
#              For information : contact@centreon.com
##############################################################################
#
#        Last modification August 3, 2009, 1:35 pm
#        By harri_groning
#
##############################################################################

instance_name=Central
output_type=tcpsocket
output=127.0.0.1
tcp_port=5668
output_buffer_items=5000
file_rotation_interval=14400
file_rotation_timeout=60
reconnect_interval=15
reconnect_warning_interval=900
data_processing_options=-1
config_output_options=3
```

Tässä kohdassa on tärkeää, että tietokannan asetukset ovat oikein.
Ajetaan NDOutils käyttämällä ndo2db.cfg tiedostoa.

```
#               /usr/local/nagios/bin/ndo2db -c /usr/local/nagios/etc/ndo2db.cfg
```

Tarkistetaan, että ndoutils käynnistyi. Tiedostossa pitäisi lukea: “ndomod: Succesfully connected to data sink.” Jos nagios.log sisältää jonkinlaisia virheilmoituksia, tarkistetaan että ndo2db.cfg, sekä ndomod.cfg sisältävät oikeanlaiset tiedot tietokantayhteyden muodostamiseen. Lisäksi on hyvä tarkistaa että määritelty käyttäjä omaa riittävät oikeudet mysql-tietokantaan (Select, insert, update sekä delete.)

```
tail -f /usr/local/nagios/var/nagios.log | grep ndomod
```