Janne Hakkarainen

L212SN

LINUX-PALVELIMIEN MONITOROINTI JA HÄLYTYKSET

Opinnäytetyö
Tietojenkäsittelyn. ko.

Marraskuu 2014

MAMK
University of Applied Sciences

KUVAILULEHTI

MAMK University of Applied Sciences	**Opinnäytetyön päivämäärä** 28.11.2014
Tekijä(t) Janne Hakkarainen	**Koulutusohjelma ja suuntautuminen** Tietojenkäsittelyn ko.
Nimeke Linux-palvelimien monitorointi ja hälytykset	

Tiivistelmä

Monitorointi on laaja termi, joka tulee esille monessa eri kontekstissa. Musiikin harrastajat tietävät monitoroinnin merkityksen ja samaan aikaan tehdasvalvomoissa työskentelevät tietävät mitä termillä tarkoitetaan erilaisten tuotantoprosessien valvonnassa. Tietotekniikkaan perehtyneet tietävät, mitä monitorointi tässä yhteydessä merkitsee.

Tässä opinnäytetyössä perehdytään monitorointiin nimenomaan tietotekniikan näkökulmasta kohdennettuna erityisesti palvelinympäristöön. Työn idea lähti omasta harrastuneisuudesta Linux-maailmaan ja ennen kaikkea myös muuhun alaan liittyvään, kuin koodaamiseen.

Työssä kerrotaan yleisesti monitoroinnista kattaen esimerkiksi mitä se terminä tarkoittaa ja mitä kaikkea se pitää sisällään. Esiin tulee myös, millaisia monitorointiohjelmia on olemassa Windows- ja Linux-käyttöjärjestelmissä valmiiksi asennettuna ja mitä tietoa ne käyttäjälle kertovat. Samalla käydään läpi myös hieman yleisemmän tason asioita Linux- ja Windows-maailmasta. Monitorointijärjestelmän lisäksi perehdytään myös hälytysjärjestelmiin, jotka voivat olla joko sisäänrakennettuina yritystason ohjelmiin tai saatavana omana lisäosanaan.

Toinen iso kokonaisuus on itse työ, jossa asennetaan monitorointijärjestelmä ensin simuloituun, mutta täysin oikeaa palvelinympäristöä vastaavaan kokonaisuuteen ja tämän jälkeen tuotantopalvelimille. Työssä käydään komento komennolta läpi sekä monitorointipalvelimen asentaminen, että etämonitoroitavan laitteen tarvittavat asetukset kattaen myös sähköpostikonfiguraatiot.

Asiasanat (avainsanat)

Linux, Nagios, monitorointi

Sivumäärä 34	**Kieli** Suomi
Huomautus (huomautukset liitteistä)	
Ohjaavan opettajan nimi Janne Turunen	**Opinnäytetyön toimeksiantaja** Smart Time Oy

DESCRIPTION

MAMK University of Applied Sciences	**Date of the bachelor's thesis** 28 November 2014
Author(s) Janne Hakkarainen	**Degree programme and option** Business Information Technology
Name of the bachelor's thesis Linux server monitoring and alerts	

Abstract

As a term, monitoring is fairly extensive and has many meanings depending on the context: active music enthusiasts are familiar with the term different and factory employees know what the term means in monitoring different production processes.

This thesis focused on monitoring from the IT perspective and studied what it was all about and why. The thesis introduced monitoring in general including Windows and Linux operating systems. Both operating systems have a lot of different kinds of monitoring systems integrated that normal users do not even know to exist. The thesis also explained some general terms relating to monitoring and its general usage. In addition the thesis clarified out what the other topic alerts meant and how it appeared in monitoring systems.

The practical part of the thesis was installing the monitoring system first to a simulated environment and in the end to real production servers. The thesis introduced step by step how to install a specific monitoring system to Linux servers including the main monitoring server and also a remote host.

Subject headings, (keywords) Linux, Nagios, monitoring	
Pages 34	**Language** Finnish
Remarks, notes on appendices	
Tutor Janne Turunen	**Bachelor's thesis assigned by** Smart Time Oy

SISÄLTÖ

1 JOHDANTO

Monitorointi on käsitteenä varmasti monelle erittäin tuttu monissa erilaisissa yhteyksissä, mutta mitä se tietotekniikan maailmassa tarkoittaa? Muun muassa juuri tähän kysymykseen on tarkoitus tässä opinnäytetyössä vastata. Monitorointi on tärkeä osa-alue monilla eri aloilla, joista tietotekniikka on varmasti yksi kärkipäästä. Monitorointi tulee tiedostaa ja ottaa huomioon aina, mikäli ollaan tekemässä jotain sellaista järjestelmää, jonka katkeamaton toiminta on elintärkeää tai vähintäänkin virhetilanteista toipumisen tulisi olla mahdollisimman nopeaa suurempien vahinkojen välttämiseksi. Aina se ei välttämättä ole yrityksen tai muun toiminnan kannalta välttämätöntä, mutta todennäköisesti hyvin suuressa osassa erilaisten tehtaiden tai IT-alan yritysten kannalta erilaisten prosessien tai palvelimien tiloista on pakko olla ajan tasalla koko ajan. Ennen kaikkea silloin, kun ihmisiä ei ole niitä valvomassa.

Luvussa 2 käydään läpi tarkemmin, mitä monitorointi oikeasti tarkoittaa ja miksi sitä hyödynnetään. Samassa luvussa käsitellään myös millaisia monitorointiohjelmia on olemassa ja mitä eroja niillä on. Samalla on syytä mennä myös hieman perusasioihin liittyen esimerkiksi Linux-koneiden etäkäyttöön ja mahdollisesti tarvittavaan tiedostonsiirtoon, jotka molemmat ovat vähintäänkin syytä saattaa kaikkien tietoisuuteen. Viimeisenä asiana luvussa 2 kerrotaan laajemmin siitä, mitä hälytysjärjestelmä tarkoittaa ja pitää sisällään.

Luvussa 3 esitellään toimeksiantajaa yrityksenä sekä selvitetään minkä monitotijärjestelmän valitsimme asennettavaksi yrityksen tuotantopalvelimille. Samalla kerrotaan myös, miten etämonitorointipalvelin asennetaan ja konfiguroidaan keskustelemaan monitorointipalvelimen kanssa. Viimeisenä luvussa 3 kerrotaan, miten hälytysjärjestelmän konfigurointi valittuun monitorointijärjestelmään onnistuu. Työn lopussa kerrotaan millaisia ongelmia kohdattiin sekä miten niistä päästiin yli. Viimeisestä luvusta löytyy myös mietelmät työn kulusta ja sen onnistumisesta kokonaisuudessaan.

2 MONITOROINTI YLEISESTI

Monitoroinnista tulee varmasti monelle mieleen jonkin asian seuranta tai valvonta. Termi tuleekin yleisimmin vastaan esimerkiksi rakennusten kosteusprosentteja ja lämpötiloja seuratessa tai vastaavissa asiayhteyksissä. Musiikin harrastajat ovat myös varmasti tuttuja termin kanssa hieman toisessa tarkoituksessa. Monitorointi on tavallista toimintojen tarkkailua ja tallentamista projektista tai ohjelmasta. Se on prosessi rutiinimaisesti tiedon keräämiseen kaikista osa-alueista projektissa. (Bartle 2011.) Mielikuva tehtaiden isoista valvomohuoneista kymmenine näyttöineen kuvastaa itse asiassa melko hyvin, mistä tässä on nimenomaan tietotekniikan näkökulmasta katsottuna kyse. Oma aiheeni liittyy nimenomaan palvelimien, eikä suinkaan tehtaiden tuotantoprosessien valvontaan. Samaisen esimerkin voisikin ajatella esimerkiksi siten, että kuvitellaan tehtaan olevan yksi iso palvelin, jonka eri ominaisuuksia (prosesseja) monitoroidaan valvomohuoneessa eli vaikkapa yrityksen toimistossa, joka voi hyvin sijaita toisella puolella kaupunkia tai jopa maailmaa. Tietenkin voisimme työllistää yhden ihmisen seuraamaan kyseistä prosessia paikan päälle, mutta onko se enää järkevää, kun prosessien määrä kasvaa moninkertaiseksi?

Juuri tässä ollaankin itse asian ytimessä. Palvelinta voidaan valvoa käytännöstä mistä vain esimerkiksi selainpohjaisen käyttöliittymän kautta. Tällä tavalla kuluja saadaan pienemmäksi ja fyysisesti eri paikassa sijaitsevia palvelimia voidaan valvoa helposti ja kätevästi yhdestä paikasta sen sijaan, että jokaisessa paikassa olisi henkilö palkattu tätä työtä varten. Palvelimet ovat usein virtualisoituja pilvipalvelimia, jotka eivät välttämättä edes sijaitse samassa maassa kuin niitä käyttävä yritys. Nykymaailma on vahvasti menossa siihen suuntaan, että juuri esimerkiksi palvelinlaitteet ovat yksinkertaisesti fiksua ”vuokrata” pilvestä. Internetissä on tarjolla monia erilaisia palveluita tähän tarkoitukseen, josta esimerkkinä voidaan mainita UpCloud. Kyseistä palvelua nimitetään niin sanotuksi IaaS (Infrastructure as a Service)-pilvipalveluksi, joka tarkoitta käytännössä sitä, että kokonainen palvelinsali kaikkine ominaisuuksineen on siirretty pilveen, kattaen tallennustilat, palvelimet ja niiden ylläpidon. Eli siis kokonainen infrastruktuuri nimensä veroisesti. Tällaisten palveluiden hyvinä puolina verrattuna erillisiin yritysten omiin konesaleihin ovat esimerkiksi kustannustehokkuus ja helppo hallinta. UpCloud lupaa tyypillisen Linux-palvelimen 30 sekunnissa tilauksesta, joka antaa melko hyvän kuvan koko järjestelmästä. Omista tarpeista riippuen UpCloud avaa sinulle oman tilin, jossa voit helposti hallinta palvelimia ja kaikkea niihin liittyvää web-käyttöliittymän

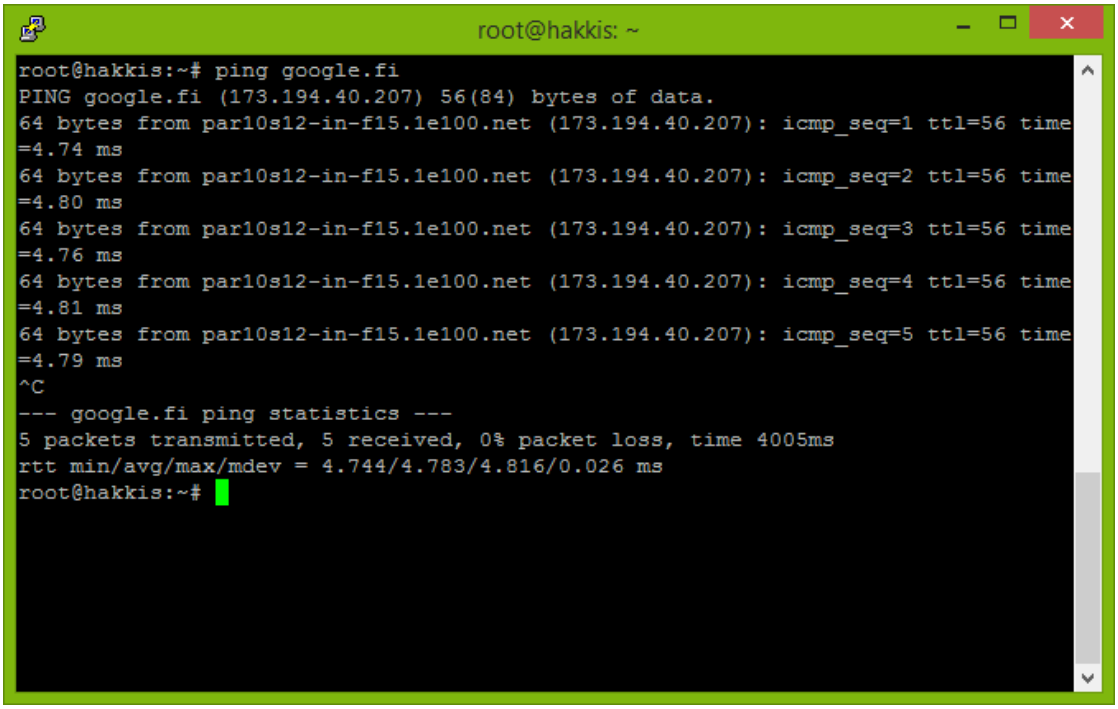
kautta. Tilauksen yhteydessä voit määritellä, minkä tehoisen palvelimen haluat, mutta hinta tietysti nousee tämän mukaan myös. Vaikka palvelin onkin virtuaalinen, se käyttää kuitenkin laitteen resursseja sen mukaan, miten tehokkaaksi se asetetaan. Voit lisätä uusia palvelimia helposti selaimella käytettävän hallintapaneelin kautta ja vaikkapa kloonata napin painalluksella kyseisen palvelimesi toiseksi samanlaiseksi, jolloin sinulla on parissa minuutissa kaks identtistä palvelinta. Saman työn tekeminen fyysisesti veisi paljon kauemmin ja olisi paljon kalliimpaa.

Koko järjestelmä perustuu siis virtualisointiin, joka tarkoittaa sitä, että samassa fyysisessä palvelinkoneessa voi pyöriä useampi näennäinen palvelin. On sanomattakin selvää, että tämä tekniikka vie paljon enemmän resursseja itse pääpalvelimelta, kuin normaalisti yhden käyttöjärjestelmän ajaminen samalla laitteella., sillä monen virtuaalikoneen pyörittäminen on melko raskasta. Tehokkailla palvelinlaitteilla tämä kuitenkin onnistuu vaivatta ja hyödyn määrä on silti suurempi kuin kulujen. Asiaa voi helposti miettiä siltä kantilta, jos yrityksen tarve olisi esimerkiksi 4 erilaista, eri käyttöön tulevaa palvelinta. Laitteet tulisi ensin tilata joltakin toimittajalta, asentaa käyttökuntoon ja viedä konesaliin valmiiksi. Virtualisoinnilla voidaan parissa minuutissa avata käyttöön 4 eri tehoista palvelinta käytöstä riippuen, tarvittaessa kloonata samanlaisia ja asentaa käyttöjärjestelmät ja tarvittavat ohjelmistot. Jälkimmäisessä tapauksessa kaiken tämän voi hoitaa kotoa käsin, pelkästään etäyhteyksiä sekä palveluntarjoajan tarjoamia työkaluja käyttäen. Kuten sanottu, hinta riippuu koneiden määrästä ja tehokkuudesta, mutta on joka tapauksessa kustannustehokkaampaa ja ennen kaikkea paljon vaivattomampaa. Myös tulevaisuutta ajatellen se voi olla paljon fiksumpi ratkaisu, mikäli yhtäkkiä olisikin tarve uudelle palvelimelle. Palveluiden selainpohjainen hallinta tarjoaa yleensä yksinkertaisen monitoroinninkin ilman lisämaksuja.

Monitorointi on erittäin tärkeää yritykselle varsinkin silloin, kun palvelimien kaatumisesta seuraisi paljon harmia yrityksen toiminnan kannalta. Toisaalta ”kolauksen” ei tarvitse olla välttämättä isokaan, kun siitä jo aiheutuu yritykselle vähänkin päänvaivaa. Tässä kohtaa lienee syytä nostaa esiin asia, joka kannattaa ja on hyvä tiedostaa kaikessa yksinkertaisuudessaan. Tämä voi jäädä helposti myös huomaamatta, jos asiaa ei mieti loppuun asti. Monitorointi- ja hälytysjärjestelmän tulisi sijaita itsenäisellä palvelimella sen takia, että itse monitorointipalvelimen toiminta olisi turvattu. Mikäli monitoroitavat palvelimet ja itse monitorointipalvelin sijaitsevat fyysisesti eri konesaleissa, riski kaik-

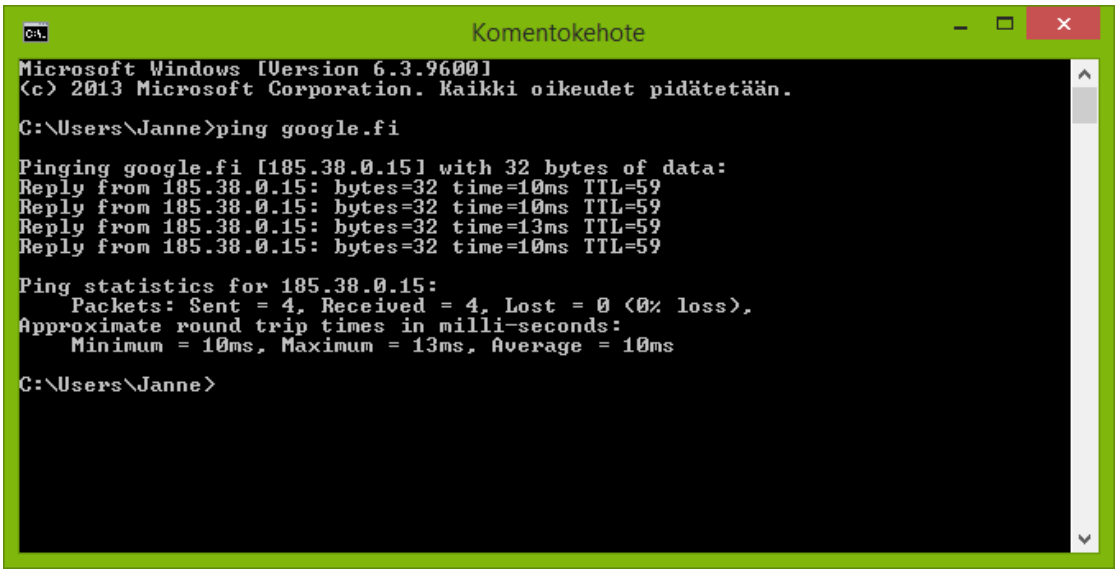
kien yhtäaikaiseen toimimattomuuteen on melko pieni. Virtuaalikoneissa sen tulisi vastaavasti sijaita omana virtuaalisena palvelimenaan, vaikka se teoriassa fyysisesti samassa paikassa olisikin. Kunnon palveluntarjoajilla kaikkien virtuaalipalvelimienkin toiminta on kahdennettu, joten syytä huoleen ei todellakaan ole. Pahimmassa tapauksessa tilanne on se, ettei tietoa ongelmallisesta palvelimesta saada, jos itse monitorointipalvelinkin on saman verkon alaisena ja fyysisesti samalla palvelimella. Sama verkko voi itse asiassa olla jopa hyvä asia, jolloin monitoroinnin ei tarvitse tapahtua internetin yli. Tällainen ratkaisu voi tietenkin olla joskus pakko toteuttaa, mutta lähiverkossa sijaitseva monitorointikokonaisuus on tässä mielessä turvallisempi. Palomuureihin ei tarvita niin isoja muutoksia ja koko järjestelmä on ikään kuin suljettu ulkopuolisilta. Joka tapauksessa etämonitorointi lähiverkossa toimii jouhevammin, eikä turhia viiveitä pääse syntymään.

Millaisia asioita voidaan monitoroida ja millaisia olisi hyödyllistä monitoroida? Tällaisia asioita on esimerkiksi kiintolevytilan sekä RAM-muistin määrä, prosessorin käyttökuorma, erilaiset lämpötilat ja web-palvelimien toiminta kattaen esimerkiksi tietokanta- ja http-palvelimet. Yksi tärkeä ominaisuus on myös liikenteen seuranta ja tieto siitä, että palvelin vastaa ping-pyyntöihin. Pingaus tarkoittaa, että pingattavalle etäkoneelle lähetetään testipaketti, johon etäkoneen on vastattava (Sonera.fi 2014).



KUVA 1. Ping-komento suoritettuna Linux-käyttöjärjestelmän komentorivillä

Kuvassa 1 on suoritettu ping-komento Linux-käyttöjärjestelmän komentorivillä. Ping-komennon jälkeen syötetään haluttu IP-osoite tai domain, johon testipaketteja halutaan lähettää, eli tässä tapauksessa google.fi.

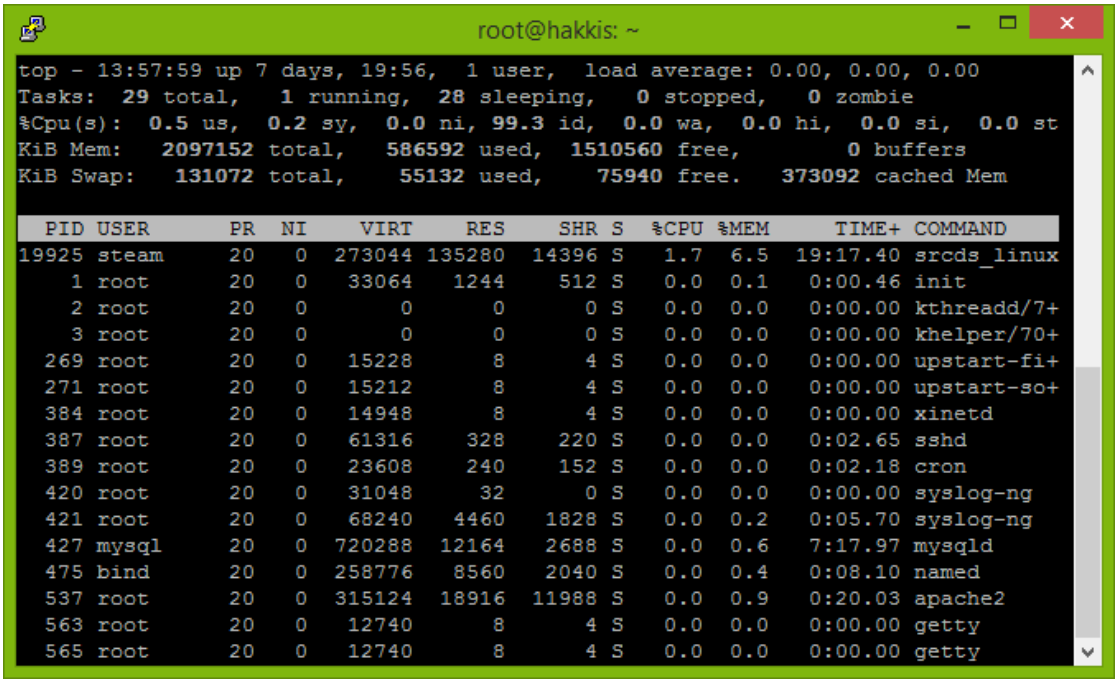


KUVA 2. Ping-komento suoritettuna Windows-käyttöjärjestelmän komentorivillä

Kuvassa 2 on suoritettu sama komento kuin kuvassa 1, mutta Windows-käyttöjärjestelmän komentorivillä. Tästä nähdään myös se, miten samanlainen kyseinen komento on käyttöjärjestelmästä riippumatta. Näinkin yksinkertainen esimerkkikomento kertoo palvelimen tilasta jo erittäin paljon. Ensinnäkin saadaan tieto siitä, että palvelin on ylipäätään käynnissä ja se vastaa pyyntöihin. Toinen hyödyllinen tieto on viive, joka ilmoitetaan tietotekniikassa yleensä millisekunteina. Mikäli viive palvelimen vastaukseen on erittäin suuri, saattaa jokin rasittaa verkkoyhteyttä liikaa. Tärkeä tieto on myös se, ettei yhtään pakettia häviä matkalle. Vaikka viive olisi pieni, mutta esimerkiksi yksi viidestä paketista ei menisi ollenkaan perille, niin sekin voi aiheuttaa paljon harmia monissa eri järjestelmässä. Monitorointijärjestelmä voi automaattisesti aika ajoin suorittaa näitä komentoja ja ilmoittaa, mikäli verkkoyhteydessä on jotakin vialla. Tällöin tilanteeseen voidaan heti puuttua, jolloin vahingot saadaan minimoitua ja yrityksen toiminta ei kärsi. Tarvittaessa tarkastuksia voidaan tehdä myös käsin, mutta suurena etuna järjestelmä osaa itse tarkastaa, että yhteys on varmasti kunnossa.

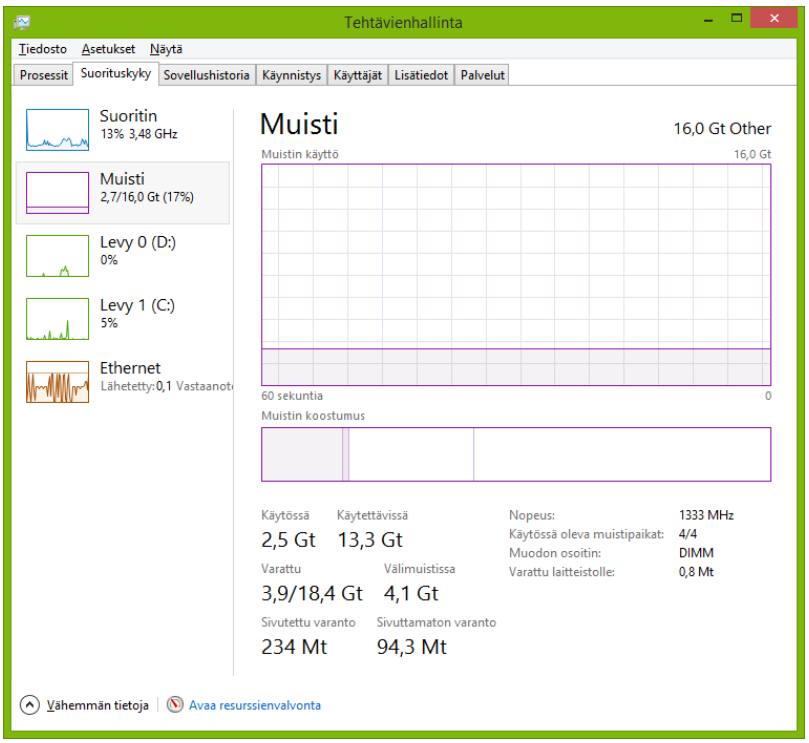
2.1 Monitorointiohjelmat

Monitorointiohjelmia on olemassa monia erilaisia hieman eri käyttötarkoituksiin. Linuxeista löytyy valmiiksi asennettuinakin joitakin yksinkertaisia monitorointiohjelmia. Linux Top-komento on suorituskyvyn monitorointiohjelma, jota käyttää monet järjestelmävalvojat valvoakseen Linuxin suorituskykyä ja se on tarjolla monille Linux/Unix -tyyppisille käyttöjärjestelmille (Saive 2014).



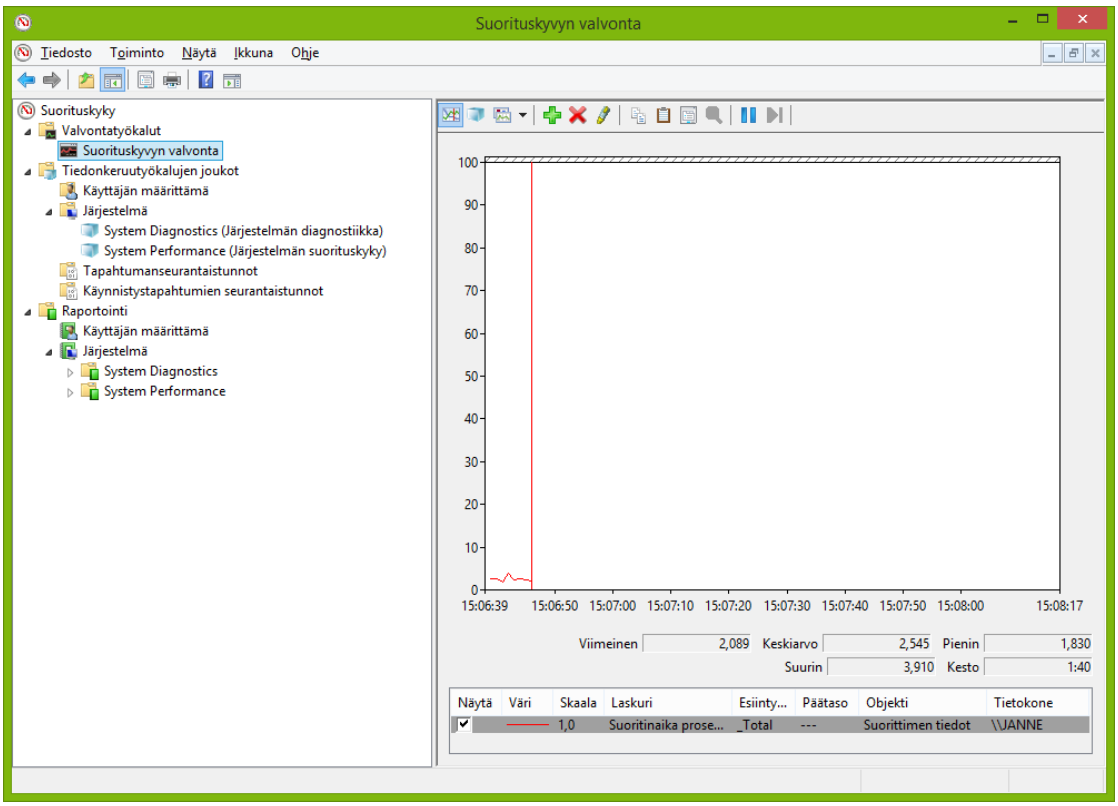
KUVA 3. Top-tehtävänhallintaohjelma Linuxissa

Kuvasta 3 näkyy hyvin mitä kaikkea infoa käyttäjälle Windowsin tehtävienhallinnan kaltainen Top-ohjelma näyttää. Siitä käy ilmi esimerkiksi prosessien määrä, prosessorin käyttöprosentteja sekä erilaisia muistitietoja. Monitorointi yksinkertaisimmillaan voi olla juuri tämän kaltaisten ohjelmien käyttöä, jolla saadaan hyödyllistä tietoa palvelimen tai miksei tavallisen työasemankin toiminnasta. Erilaisilla skriptauksilla tämän kaltaisten ohjelmien avulla voidaan tehdä toimivia monitorointijärjestelmiä pienempiin kokonaisuuksiin, mutta monessa tapauksessa on silti parempi turvautua oikeaan laajempaan monitorointiohjelmaan, joka yleensä tarjoaa paljon ominaisuuksia sisäänrakennettuna.



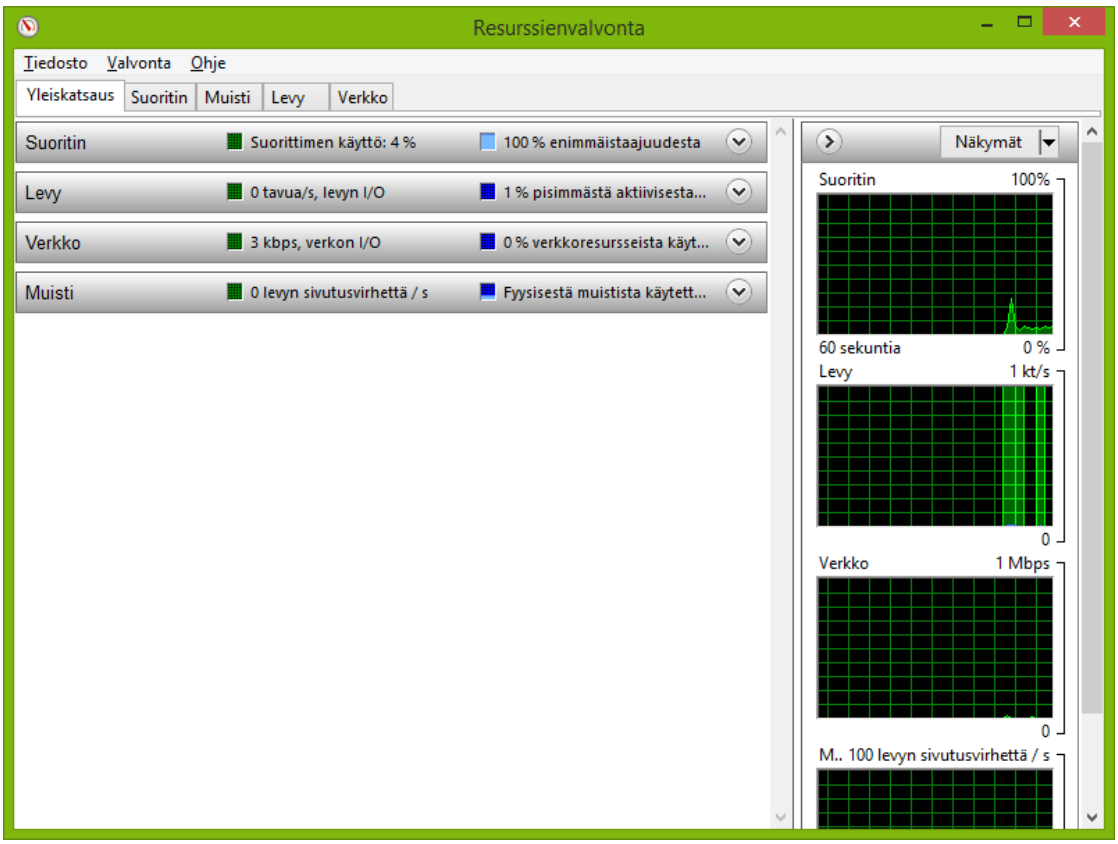
KUVA 4. Windows 8.1-käyttöjärjestelmän tehtävienhallinta.

Kuvassa 4 on esitetty Windows 8.1-käyttöjärjestelmän tehtävienhallinta. Windows 7:ään verrattuna uusi tehtävienhallinta tarjoaa paljon enemmän ja tarkempaa tietoa. Myös ulkoasu on saanut paljon ehostusta. Yksinkertaisimmillaan monitorointi voi olla tätä myös Windows-laitteissa. On siis tärkeää tiedostaa, että monitorointi ei ole todellakaan pelkästään Linux-maailman juttu, vaan samanlaisia ohjelmia on myös Windows-käyttöjärjestelmissä valmiiksi asennettunakin. Windowsille löytyy erilaisia avoimen lähdekoodin monitorointiohjelmia siinä missä Linuxillekin, mutta työssäni keskitytään nimenomaan Linux-käyttöjärjestelmään.



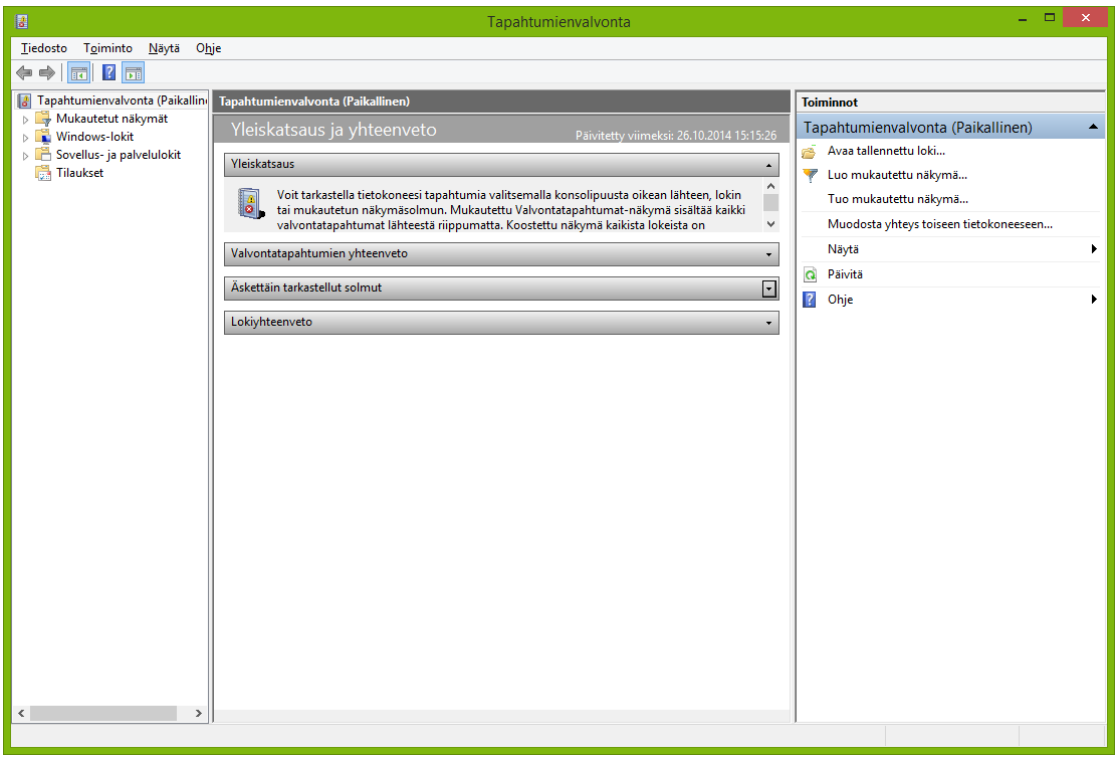
Kuva 5. Windows 8.1-käyttöjärjestelmän suorituskyvyn valvonta.

Kuten sanottu, myös Windows tarjoaa erittäin laajoja ohjelmia valmiiksi asennettuna. Windowsin ohjauspaneelista pääse valvontatyökaluihin, josta löytyy suorituskyvyn valvontaohjelma. Kuvassa 5 on ohjelman itse valvontanäkymä, jossa tällä hetkellä näkyy muun muassa prosessorin käyttö reaaliajassa käyräksi piirrettynä. Vasemmalta valikosta löytyy paljon erilaisia valintoja, josta näkee paljon kaikenlaista laitteen toimivuuteen liittyen. Kyseisen ohjelman perusnäkymästä voi seurata esimerkiksi kiintolevyn käyttöä prosentteina, RAM-muistin käyttöä siinä missä suorittimen erilaisia tietoja. Kyseessä voisi sanoa olevan siis perusominaisuuksia, joita yleensäkin monitoroidaan. Suorituskyvyn valvonnasta löytyy myös raportointiominaisuus, jota käyttäjä voi halutessaan säätää mieleisekseen. Normaaliin tehtävienhallintaan verrattuna suorituskyvyn valvonta on laajempi, mutta tarjoaa toisaalta hyvin samanlaista infoa tietokoneen tilasta.



Kuva 6. Windows 8.1-käyttöjärjestelmän resurssienvalvonta.

Kuvassa 6 on esitelty perusnäkymä Windowsin resurssienvalvonnasta. Tämä vastaa melko hyvin normaalia tehtävienhallintaa ja toisaalta myös edellä mainittua suorituskyvyn valvontaa. Resurssienvalvonnasta näkee paljon selkeämmin ja tarkemmin kaikkien eri prosessien tietoja tehtävienhallintaan verrattuna. Resurssienvalvonta kertoo erittäin tarkasti esimerkiksi laitteen kiintolevyn käyttöä ohjelmakohtaisesti sekä esimerkiksi verkon toimintaa niin lähiverkossa, kuin internetiin lähtevässä liikenteessä. Suorituskyvyn valvontaan verrattuna resurssienvalvonta näyttää jo yleiskatsauksessa graafista dataa tietokoneen tilasta, josta käyttäjä saa välittömästi paljon yleistä tietoa. Yleiskatsauksen lisäksi omilta välilehdiltä voi tarkastella vielä tarkemmin tietoa liittyen suorittimeen, muistiin, levyyn ja verkkoon.



Kuva 7. Windows 8.1-käyttöjärjestelmän tapahtumienvalvonta.

Kuvassa 7 on perusnäkymä Windowsin tapahtumienvalvonnasta. Tämä ohjelma kerää paljon erilaisia lokitiedostoja tietokoneen tapahtumista. Tapahtumienvalvonnasta löytyy joka ikinen asia, mitä tietokone on sinulta esimerkiksi kysynyt tai tehnyt. Esimerkinä mainittakoon vaikka Word-tiedoston tallentaminen. Mikäli olet sulkenut ohjelman ”ruksista” tallentamatta, niin ohjelma kysyy haluatko sulkea ohjelman tallentamatta vai haluatko tallentaa muutokset. Tapahtumienvalvonnasta löytyvät kaikki tämän tyyliset asiat lokeihin kirjoitettuna ja niitä pääsee lukemaan suoraan vasemmalta löytyvästä valikosta. Kansioita on hieman jaoteltu sen mukaan, mihin kategoriaan lokit kuuluvat. Sieltä löytyy esimerkiksi erikseen Windowsin sisäiset lokitiedostot ja ulkopuolisten ohjelmien lokit, kuten Officen. Olkoonkin tosin, että Office on osa Microsoftin tuoteperhettä, joten niiden lokit keräytyvät myös samaan sijaintiin. Kaikkien asennettujen ohjelmien lokitiedostoja ei siis suinkaan täältä löydy.

Tarkoitukseni ei ole pelotella kaikenlaisilla erilaisilla ohjelmilla, joita moni ei varmasti tiennyt omassa tietokoneessaan edes olevan, vaan nimenomaan esitellä, että niitä on valmiiksi asennettunakin erittäin monia erilaisia. Vaikka aiheeni liittyykin nimenomaan Linux-käyttöjärjestelmään, on mielestäni erittäin hyödyllistä esitellä myös Windowsin

ominaisuuksia, joita löytyy paljon. Tehtävienhallinta, tapahtumien valvonta, resurssienvalvonta sekä suorituskyvyn valvonta ovat vain esimerkkejä kaikista mahdollisista sisäänrakennetuista ohjelmista. Windowsista löytyy paljon muutakin erilaista diagnostiikkaa. Top-ohjelma Linuxissakin on kaikkea muuta kuin ainoa mahdollinen tehtävienhallinnan kaltainen ohjelma, joka löytyy valmiiksi asennettuna, mutta kaikki nämä ovat loistavia esimerkkejä siitä, millaista monitorointi voi olla. Kaikki edellä mainitut ovatkin tarkoitettuja melko lailla pelkästään kyseisen laitteen valvontaan. Etävalvonta kyseisillä tuotteilla voi olla melko hankalaa, ellei mahdotonta, joten tämän takia yritystason ulkopuolisia ratkaisuja on tehty täyttämään tarpeita.

Kaikki edellä mainitut ovat siis käytännössä eri käyttöjärjestelmien valmiiksi tarjoamia yksinkertaisia järjestelmien monitorointiin tarkoitettuja ohjelmia. Tavalliselle kotikäyttäjälle oman tietokoneen valvonta onnistuukin kyseisillä ohjelmilla varsin hyvin ja Windowsin tai Linuxin tehtävienhallinta hoitaa hommansa erinomaisesti. Palvelinkapasiteetin noustessa jo muutamaan, saati kymmeniin tai satoihin eri paikoissa sijaitseviin laitteisiin, on sanomattakin selvää, että pelkästä yksinkertaisesta tehtävienhallinnasta ei hirveästi hyötyä ole. Tarvitaan paljon laajempi kokonaisuus, jonne on mahdollista yhteen järjestelmään keskittää kaikki monitoroitavat laitteet loogiseen ja helppolukuiseen järjestykseen. Nyt esiin astuvat erilaiset yritystason monitorointijärjestelmät, jotka edellä mainittuun tehtävään kykenevät. Markkinoilla on tarjolla useita ohjelmia erilaisia käyttötarpeita varten. Jo tässä vaiheessa nostan esiin kaksi kirkkaimmin esille nousevaa nimeä, joihin törmää väkisinkin aiheeseen tutustuessa. Nagios ja Cacti ovat tiivis pari saatavilla tällä hetkellä, joista molemmat tarjoavat hieman erilaisia ominaisuuksia.

Nagios on voimakas monitorointijärjestelmä, joka auttaa yritystä löytämään ja ratkaisemaan IT-infrastruktuuriin liittyvät ongelmat ennen kuin ne vaikuttavat yrityksen toimintaan (Nagios overview 2014). Nagios tarjoaa web-käyttöliittymän kautta hallittavan järjestelmän ja sen avulla pystytään etämonitoroimaan sekä Windows-, että Linux-palvelimia, mutta itse Nagios on saatavilla vain Linuxille. Nagiokseen kuuluu myös täysi valmius käyttää jotain Linuxin sähköpostin lähetysohjelmaa suoraan hälytyksiä varten. Nagios on myös melko kevyt ja jaksaa pyöriä hieman heikkotehoisemmallakin palvelimella hyvin. Nagioksen perusversio on ilmainen, joten tämänkin takia Nagios on yksi potentiaalisesti ohjelmisto asennettavaksi yksityiseen käyttöönkin ja suurien kulujen välttämiseksi yrityksillekin, joissa tarve tällaiselle voi olla elintärkeä.

Cacti on avoimen lähdekoodin web-pohjainen tietokoneverkon monitorointi- ja kaaviointityökalu, joka on suunniteltu front-end–sovellukseksi avoimen lähdekoodin, yritysluokan tiedonkeruuohjelmalle, RDRtool:lle. Cacti sallii käyttäjän tarkkailla palveluita tietyin väliajoin ja kaavioida saadun datan. (About Cacti 2014.) Cactia siis käytetään samaan tarkoitukseen kuin Nagiostakin, mutta Cacti on erikoistunut ennen kaikkea datan saattamiseen graafiseen muotoon. Nagioksessa data esitetään enemmänkin vain lukuina. Cacti vaatii toimiakseen Apachen, PHP:n ja MySQL:n, kun Nagios ei puolestaan ei tarvitse tietokantapalvelinta itse ollenkaan. Tietokantapalvelimen toimintaa sillä voidaan kuitenkin valvoa. Cacti ei Nagioksen tapaan tarjoa tukea hälytysjärestelmälle suoraan, vaan se pitää asentaa ohjelmaan erikseen lisäosana.

Lyhyenä yhteenvetona omalta osalta Nagios vaikutti näistä kahdesta selkeämmältä ja parempiin tarpeisiin sopivalta. Cacti on nimenomaan erikoistunut graafiseen informaation, joka ei välttämättä ollut tässä skenaariossa tarpeellista. Toisenlaiseen projektiin puolestaan Cacti olisi voinut listan kärjessä. Etämonitoroinnissa Cacti hyödyntää SNMP-protokollaa, jota tulee sanoista Simple Network Management Protocol. Nagiokselle sama hoituu omalla etäpalvelimella, joka asennetaan etämonitoroitavaan laitteeseen ja Nagios osaa tämän kautta lukea tietoa kyseiseltä palvelimelta. Nagioksen ratkaisu vaikutti tässäkin melko hyvälle, vaikka Cactikin hoitaa asian toimivasti. Itse en ole Cactiin tutustunut asennuksen merkeissä, joten asennusprosessista vaikea sanoa eroja. Ohjeita löytyy molempiin hyvin, joten asennus varmasti onnistuisin, valittaisiin sitten kumpi tahansa.

2.2 Etäkäyttö ja tiedostonsiirto

Yksi oleellinen kysymys on varmasti se, että mitä hyötyä on Top-ohjelman kaltaisesta sovelluksesta, jos sitä on mahdollista käyttää vain itse palvelimen/tietokoneen komentoriviltä. Tässä kohtaa suureen osaan astuu tekniikka nimeltä SSH. SSH (Secure Shell) on tarkoitettu korvaamaan rlogin ja telnet-ohjelma. SSH käyttää turvallisempaa yhteydenottomuotoa palvelimelle kuin esimerkiksi telnet ja rlogin, Turvallisuus perustuu siihen,
että SSH muuttaa käyttäjätunnuksen ja salasanan salakirjoitukseksi, jonka vain etäpalvelimella oleva SSH-palvelinohjelma kykenee avaamaan. Se edellyttää kuitenkin, että etäpalvelin käyttää tiedostonsiirtoon SSH-protokollaa. (Peltomäki & Linjama 1999,

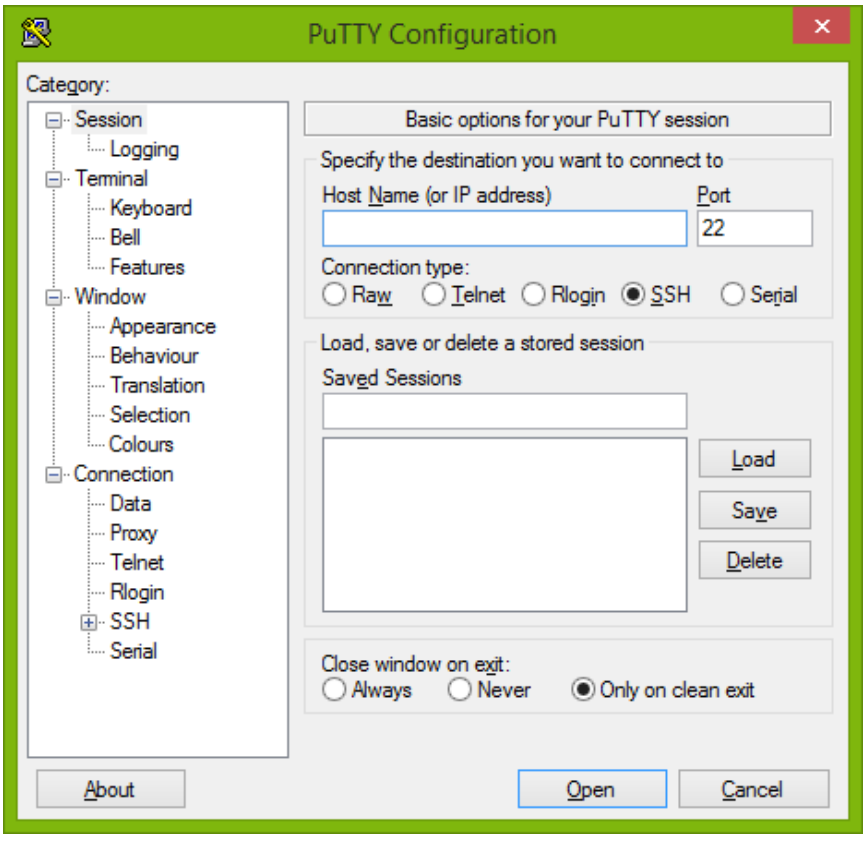
380.) SSH-palvelin asentuu usein Linux-käyttöjärjestelmän mukana, mutta tarvittaessa sen voi asentaa helposti seuraavalla komennolla:

```
sudo apt-get install openssh-server
```

Tämä tekniikka sallii sen, että palvelinkoneen komentorivi saadaan käyttöön mistä vain ja palvelinta voidaan käyttää, konfiguroida ja monitoroida aivan samalla tavalla, kuin paikan päällä. Palvelinkoneissa harvoin käytetäänkin graafista käyttöliittymää eli toisin sanoen perus työpöytää, sillä se vie resursseja aivan turhaan. Etäyhteys SSH-tekniikkaa käyttäen onnistuu Linux-koneesta toiseen Linux koneeseen kirjoittamalla komentoriville ”ssh <yhteyttä otettavan koneen haluttu käyttäjänimi, jolle kirjaudutaan>@<palvelimen osoite>”, esimerkiksi seuraavasti:

```
ssh kayttaja@palvelin.fi
```

Windows-koneesta Linux-koneeseen yhteyttä käytettäessä tarvitsee asentaa jokin SSH-asiakasohjelma, joista yksi suosituimmista on ohjelma nimeltä PuTTY.



KUVA 8. PuTTy-ohjelman perusnäkymä

Kuvassa 8 on PuTTy:n perusnäkymä. Host Name -kenttään voidaan syöttää yhdistettävän palvelimen/tietokoneen IP-osoite tai domain. Open-näppäintä painamalla saadaan auki ikkuna, josta voidaan kirjautua laitteeseen halutuilla tunnuksilla. Oikeat tunnukset syöttämällä päästään Linuxin komentorivin perustilaan. Palvelinkoneen käyttäminen etänä SSH:n avulla ei kuitenkaan ole välttämättä se fiksuin tai paras tapa, sillä on olemassa paljon laajempia ja enemmän toiminnallisuuksia sisältäviä ohjelmiakin. SSH-tekniikka onkin täten miltei ainoastaan keino asentaa palvelinkoneeseen jokin toinen, laajempi ohjelmisto ja ylläpitää itse palvelinta. SSH:n kautta monitorointi on siis vain yksi tapa muiden joukossa ja se voi hoitaa tehtävänsä pienissä järjestelmissä, jossa laajaa ja monipuolista ohjelmistoa ei välttämättä tarvita. Myös esimerkiksi tarvittavien tietojen saattaminen hienoon graafiseen muotoon selainpohjaiseen käyttöliittymään ei välttämättä jokaiselta ohjelmoijalta onnistu niin helposti, eikä sellaista ole todellakaan järkevää alkaa tekemään. Tätä varten niitä löytyy avoimen lähdekoodin ohjelmina valmiina.

FTP (File Transfer Protocol) on tiedostonsiirtoprotokolla, joka siirtää tiedostoja kahden järjestelmän välillä. FTP-protokollan keskeisiä ominaisuuksia ovat mm. tiedostojen välitön siirto pyynnön jälkeen, suurien tiedostojen tehokas siirto ja yhden palvelimen mahdollisuus hoitaa useita asiakkaita. (Peltomäki & Linjama 1999, 195.) FTP:tä ei tässä tapauksessa välttämättä tarvita, mutta se on syytä tässä yhteydessä kuitenkin mainita. Sen avulla on kätevä siirtää isojakin tiedostoja tietokoneiden välillä ja sitä käytetäänkin erittäin paljon esimerkiksi web-kehityksessä, jotta saadaan paikallisesti kehitetyt websovellukset siirrettyä verkkoon kaikkien käytettäväksi. Esimerkiksi erilaiset konfiguraatiotiedostot voivat olla nopeampi ja helpompi muokata muulla kuin komentorivipohjaisella tekstieditorilla. Kokeneempi Linuxin käyttäjä kuitenkin omaksuu komentorivipohjaisen käytön ja tulee toimeen sen kanssa ilman ongelmia. Linuxista löytyy komento, jolla voi ladata tiedoston sisältävästä internet-osoitteesta suoraan palvelimelle. Tiedoston lataus onnistuu helposti Wget-komennolla. GNU Wget on ilmainen ohjelmistopaketti tiedostojen noutoon HTTP, HTTPS ja FTP–protokollia käyttäen (GNU Wget 2012).

2.3 Hälytysjärjestelmät

Palvelimien monitorointi on erittäin tärkeä osa toimivaa kokonaisuutta, mutta miten käy, jos silmäparia ei olekaan aina käytettävissä palvelimien valvontaan? Tätä on syytä miettiä varsinkin sellaisen yrityksen sisällä, jossa ei ole öisin minkäänlaista valvontaa. Tällöin palvelimet ovat niin sanotusti oman onnensa nojassa ja vika saatetaan huomata vasta liian myöhään. Tätä varten monitoroinnin lisäksi on hyvä olla olemassa jonkinlainen hälytysjärjestelmä. Hälytysjärjestelmällä tarkoitetaan siis sitä, että mikäli palvelimella on jotain ongelmia, niin hälytysjärjestelmä osaa ilmoittaa tästä esimerkiksi sähköpostitse tai tekstiviestillä. Tällöin tilanteeseen voidaan heti suhtautua siihen tarvittavalla tavalla sen sijaan, että tieto palvelimen toimimattomuudesta tulisi itse asiakkailta, kun palvelua ei enää voida käyttää. Yrityksen jouhevan toiminnan kannalta pelkkä monitorointi ei siis välttämättä ole riittävä, vaan havainnon viasta tulisi tulla järjestelmältä ihmiselle päin, eikä toisinpäin.

Hälytysjärjestelmä on integroituna useaan monitorointijärjestelmään valmiiksi, mikä helpottaa asennus- ja konfiguraatioprosessia huomattavasti. Nagios on hyvä esimerkki tällaisesta ohjelmasta. Nagiokseen on sisäänrakennettu oma hälytysjärjestelmä, joka osaa lähettää tarvittaessa sähköpostia. Itse lähetykseen Nagios tarvitsee oman ohjelman, esimerkiksi Linuxin mail-ohjelman. Linuxin mail-ohjelmaa pystyy itsekin käyttämään sähköpostin lukemiseen tai lähettämiseen suoraan komentoriviltä. Nagiokselle tarvitsee ainoastaan kertoa käytettävä ohjelma ja ilmoittaa haluttu osoite. Periaatteessa Nagios ei siis tarjoa itse lähetysohjelmaa sisäänrakennettuna, mutta tarjoaa kaikki mahdolliset tarvittavat konfiguraatiot, jotta se osaa käyttää sille määrättyä ohjelmaa hyödykseen kätevästi. Hälytysjärjestelmä voi olla myös saatavana omana lisäosanaan, kuten esimerkiksi Cactissa. Jälkimmäisessä tapauksessa ohjelmaan tarvitsee asentaa erillinen lisäosa eli ”plugin”, jolla saadaan ohjelman perusversioon lisättyä tarvittava ominaisuus.

3 MONITOROINTI-/HÄLYTYSJÄRJESTELMÄN ASENTAMINEN JA KONFIGUROINTI

Tämän työn tarkoituksena on automatisoida Smart Time Oy:n Linux-palvelimien valvonta sekä saada tieto virhetilanteista välittömästi. Tarkoitus on myös kertoa yleistä tietoa monitoroinnista ja sen mahdollisuuksista. Smart Time Oy on ohjelmistoratkaisujen myyntiin, konsultointiin ja tuotekehitykseen erikoistunut yritys, jonka Mikkelin toimipiste sijaitsee Mikpoli-rakennuksessa Kasarmin kampuksella. Toinen toimipiste sijaitsee Helsingissä. Yksi yrityksen päätuotteista on Aika24-ajanvarauspalvelu, jonka yritykset voivat ottaa kätevästi käyttöön, jolloin heidän ei tarvitse kehittää omaa ja toiminta onnistuu helposti netin kautta. Työn ideana on siis selvittää, millaisia monitorointimahdollisuuksia on tarjolla ja minkälainen olisi paras Aika24:n palvelimien valvontaan. Tarvittavia ominaisuuksia on helppokäyttöinen web-käyttöliittymä, mahdollisuus helposti lisätä uusia laitteita valvottavaksi helposti ja mahdollisuus saada ilmoitukset ongelmista esimerkiksi sähköpostitse. Ohjelman tulisi olla tarpeeksi helppokäyttöinen ja laaja, mutta toisaalta ainoastaan yrityksen tarpeet täyttävä.

Valitsimme käytettäväksi ohjelmistoksi edelläkin mainitun Nagioksen. Nagios tarjoaa hyvin tarvitsemiamme ominaisuuksia, jolloin asennuksesta saadaan vaivattomampi. Asennusprosessin ollessa edes jossain määrin suoraviivainen, nii todennäköisesti ohjelman päivitys ja tarvittava konfigurointi on jatkossakin helppoa. Niin sanotut ”viritykset” saavat ohjelmasta äkkiä hauraan ja hankalan ylläpitää, joten Nagioksen tarjoamien valmiiden ominaisuuksien takia se oli meidän valintamme. Kilpailussa oli mukana myös niin ikään edellä mainittu Cacti. Cactista löytyi myös hyvin ominaisuuksia, mutta esimerkiksi valmiin integroidun hälytysjärjestelmän puuttuminen vaikutti päätökseen. Kaiken lisäksi Nagios oli minulle ennalta tuttu sen verran, että olin harjoittelussa ollessani jo hieman kerennyt tutustumaan siihen muun muassa erittäin nopean koeasennuksen myötä. Keskustellessamme käytettävästä ohjelmasta nämä kaksi tulivat ensiksi mieleen, joten emme sen enempää edes tutustuneet muihin vaihtoehtoihin, vaikka niitä on olemassa varmasti kymmeniä erilaisia ilmaisinakin.

Nagioksesta on olemassa lukuisia eri versioita, joista osa on maksullisia ja osa ei. Nagioksen ”lippulaiva” Nagios XI tarjoaa paljon ominaisuuksia, mutta onkin täten melko hintava. Nagios XI ilman mitään lisäpalveluita maksaa yksinään noin 2000 dollaria,

mutta hinta nousee helposti kymmeneen tuhanteen jo muutamalla hyödyllisellä lisäpalvelulla. Nagios Core tarjoaa kuitenkin monia tässä skenaariossa tarpeellisia ominaisuuksia ja riittää Smart Timen tarpeisiin erittäin hyvin. Core on avoimen lähdekoodin versio, jonka versio 3.5.1 on ladattavissa suoraan Ubuntun sovellusvalikoimasta komennolla:

```
sudo apt-get install nagios3
```

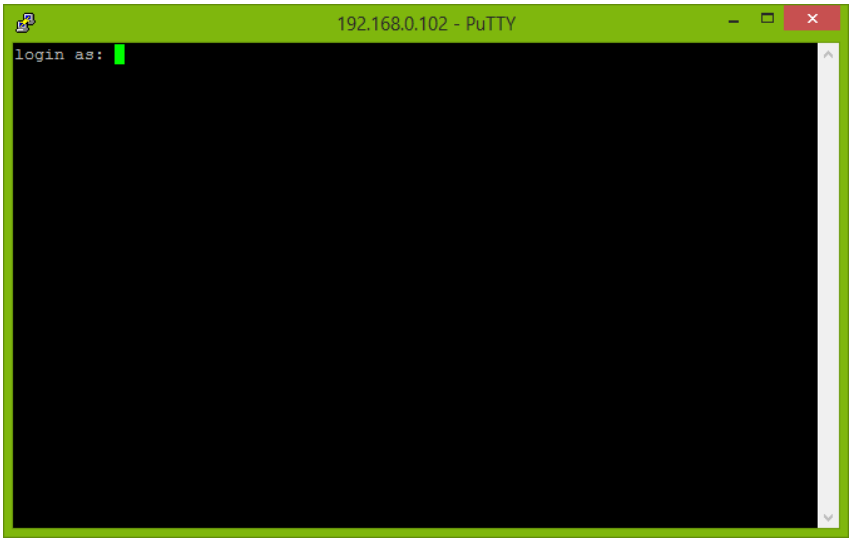
Apt-get:n avulla ohjelmien asentaminen on erittäin helppoa ja nopeaa. Yleensä ohjelmien asentaminen tämän avulla onkin varsin toimiva ratkaisu ja erittäin monen sovelluksen kohdalla se toimii loistavasti. Nagios Coren tapauksessa tässä piilee kuitenkin sellainen ongelma, että tämän version päivittäminen uudempaan on melko lailla mahdotonta. Valikoima ei tarjoa uusinta versiota Nagioksesta, jolloin se pitäisi tehdä käsin. Käsin asennettaessa tiedostorakenne on erilainen, mikä tekee päivittämisen erittäin hankalaksi. Tästä syystä tein asennuksen käsin, jolloin uusimpaan versioon siirtyminen onnistuu helposti.

3.1 Nagioksen asentaminen

Simuloin asennusprosessin kolmella eri tietokoneella lähiverkossa sen takia, ettei Smart Time Oy:n IP-osoitteita tai muita tärkeitä tietoja pääse vahingossakaan kaikkien nähtäväksi. Asennusprosessi SSH:n kautta lähiverkossa vastaa täysin sitä, jos ohjelmat asennettaisiin oikealle palvelinkoneelle internetin yli. Käytännössä IP-osoitteet/domainnimet ovat ainoat tekijät, jotka muuttuvat asennettaessa järjestelmä oikeaan palvelinympäristöön. Niin pitkään, kun tässä käytettävät kannettavat tietokoneet ovat päällä ja yhteydessä lähiverkkoon esimerkiksi WLAN:n kautta, niin kaiken tässä tarvittavan asentamisen ja konfiguroinnin voi suorittaa pöytätietokoneelta käsin. Pöytätietokoneessa käytössä on Windows 8.1 Professional–käyttöjärjestelmä ja se on niin ikään yhteydessä samaan lähiverkkoon muiden laitteiden kanssa. Palvelin, jonne monitorointiohjelmisto asennettaisiin, on simuloitu tässä skenaariossa kannettavalla tietokoneella, jonka käyttöjärjestelmänä toimii Kubuntu 14.04 Linux-jakelu. Ubuntu on vapaista ohjelmistoista (avoimesta lähdekoodista) koostuva Linux-käyttöjärjestelmä, joka rakentuu Debian-projektin tekemälle työlle (Ubuntu Suomi 2014). K-kirjain edessä tarkoittaa KDE-työpöytäympäristöä, mikä on hieman erilainen kuin normaalissa Ubuntussa. KDE perustuu vedä- ja pudota –tekniikkaan ja tiedostojen täysin graafiseen hallintaan. Kaikki

tiedostot esitetään ikkunassa kuvakkeina, joita napsauttamalla ne avautuvat niitä muokkaavaan ohjelmaan. (Peltomäki & Linjama 1999, 380.) KDE-työpöytäympäristö on erittäin samanlainen kuin vanhemmissa Windows-versioissa. Työpöytäympäristöllä ei kuitenkaan tässä tapauksessa ole mitään merkitystä, sillä käytän SSH-etäyhteyttä kannettavaan tietokoneeseen, jolloin se on täysin komentorivipohjainen ja simuloi hyvin oikeaa palvelinta, joissa ei yleensä ole käytössä työpöytäympäristöä ollenkaan. Linux-jakeluita on paljon muitakin, mutta Ubuntu on itselleni kaikista tutuin, joten oli luontevaa valita se tähän projektiin käyttöjärjestelmäksi. Etämonitoroitavaa palvelinta simuloi tässä tapauksessa toinen kannettava tietokone, jossa on käytössä myös Ubuntu-käyttöjärjestelmä kevyemmällä Xfce4-työpöytäympäristöllä. Tätä Ubuntu-jakelua kutsutaan Xubuntuksi.

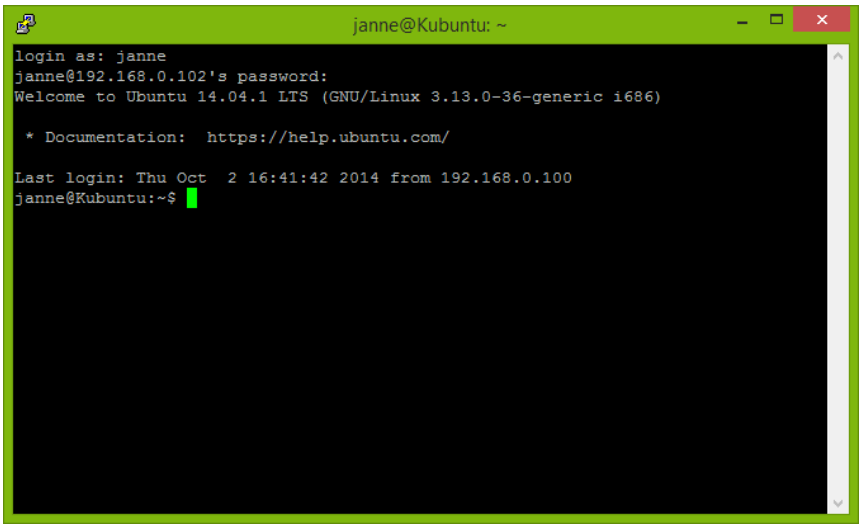
Asennus lähtee käyntiin muodostamalla SSH-yhteys palvelinkoneeseen. PuTTy:n IP-kenttään syötetään palvelimen osoite, eli tässä tapauksessa ”192.168.0.102”, joka on kannettavan tietokoneen lähiverkon IP-osoite. Oikeassa skenaariossa tämä olisi internetissä olevan palvelimen IP-osoite tai domain-nimi. Portti-kenttä saa olla tyhjä, sillä PuTTy käyttää oletuksena oikeaa porttia, kun alapuolelta on SSH valittuna.



KUVA 9. Kirjautumisikkuna Linux-palvelimelle

Open-painikkeesta päästään kuvan 9 kaltaiseen näkymään. Mikäli SSH-yhteys muodostetaan tässä kohtaa ensimmäisen kerran, palvelin kysyy pop-up –ikkunassa niin sanottua sormenjälkeä, jonka hyväksymällä saa oikeuden yhdistää palvelimelle. Sama pätee myös Linux-laitteesta toiseen Linux-laitteeseen yhdistettäessä, jolloin komentoriviltä

tulee hyväksyä se samaan tapaan. Seuraavalla kerralla samasta koneesta palvelimelle kirjauduttaessa palvelin muistaa sinut, joten sitä ei tarvitse enää hyväksyä uudestaan. Kirjautumisikkunaan syötetään oikeat tunnukset, jonka jälkeen päästääkin Linuxin komentorivin perusnäkymään.



KUVA 10. Ubuntu-käyttöjärjestelmän komentorivin perusnäkymä SSH-yhteyden kautta

Kuvassa 10 on perusnäkymä, joka vastaa täysin sitä, jos komentorivi olisi avattu itse palvelinkoneessa. Tähän voi syöttää kaikki samat komennot ja Linuxia voi käyttää aivan kuten näppäimistöllä tai hiirelläkin, mutta vain komentorivin kautta. Mikäli et aluksi kirjautunut niin sanotusti roottina eli pääkäyttäjän tunnuksilla, niin se on syytä tehdä viimeistään nyt komennolla:

```
sudo –i
```

Tämän jälkeen ladataan tarvittavat paketit apt-get –komennolla. Näihin kuuluu mm. Apache2 web-palvelin graafista selainpohjaista käyttöliittymää varten, PHP, edellä mainittu wget sekä joitakin muita tarvittavia. Paketit asentuvat kätevästi ketjutetulla komennolla, jolloin ei tarvitse asentaa jokaista yksitellen:

```
sudo apt-get install wget build-essential apache2 php5-gd
libgd2-xpm libgd2-xpm-dev libapache2-mod-php5
```

Seuraavaksi siirrytään Linuxin tmp eli tilapäiskansioon komennolla ”cd /tmp”, jonne voidaan ladata tarvittavat tiedostot Nagioksen asentamista varten. Käytännössä sillä ei ole väliä, vaikka tiedostot ladattaisiin suoraan juurikansioon. Tilapäiskansiossa mahdollisuus siihen, että poistaa vahingossa joitain tärkeitä tiedostoja on pienempi ja tiedostot pysyvät muutenkin paremmin järjestyksessä. Seuraavaksi haetaan wget-komennolla internetistä uusin Nagios Coren versio, sekä siihen lisäosapaketti. Tämä siis nimenomaan sen takia, että saadaan uusin versio, joka ei apt-get-komennolla onnistunut.

```
wget http://sourceforge.net/projects/nagios/files/nagios-
4.x/nagios-4.0.8/nagios-4.0.8.tar.gz
```

```
wget http://nagios-plugins.org/download/nagios-plugins-
2.0.3.tar.gz
```

Seuraavaksi tehdään uusi käyttäjä ja käyttäjäryhmä, johon käyttäjä lisätään sekä liitetään käyttäjä tekemäämme käyttäjäryhmään. Tämä onnistuu seuraavilla komennoilla:

```
useradd nagios
groupadd nagcmd
usermod –a –G nagcmd nagios
```

Tämän jälkeen päästää keskittymään itse asennukseen. Wgetillä ladattujen tiedostojen pääte on .tar.gz. Tätä vastaa melko suoraan Windows-maailmasta tuttu .zip. Kyse on siis pakkausformaatista, joita voidaan tehdä gzip-nimisellä ohjelmalla. Purkaminen onnistuu komentoriviltä helposti tar (tape archiver) työkalua käyttäen seuraavasti:

```
tar zxvf nagios-4.0.8.tar.gz
tar zxvf nagios-plugins-2.0.3.tar.gz
```

Tar-komennon perään voidaan laittaa useita eri parametreja, kuten tässä esimerkissä ”zxvf”. Näillä parametreilla voidaan määritellä, mitä käsiteltävälle paketille halutaan tehdä. Tässä tapauksessa tiedostot halutaan purkaa ja tulostaa tiedostonimet näytölle.

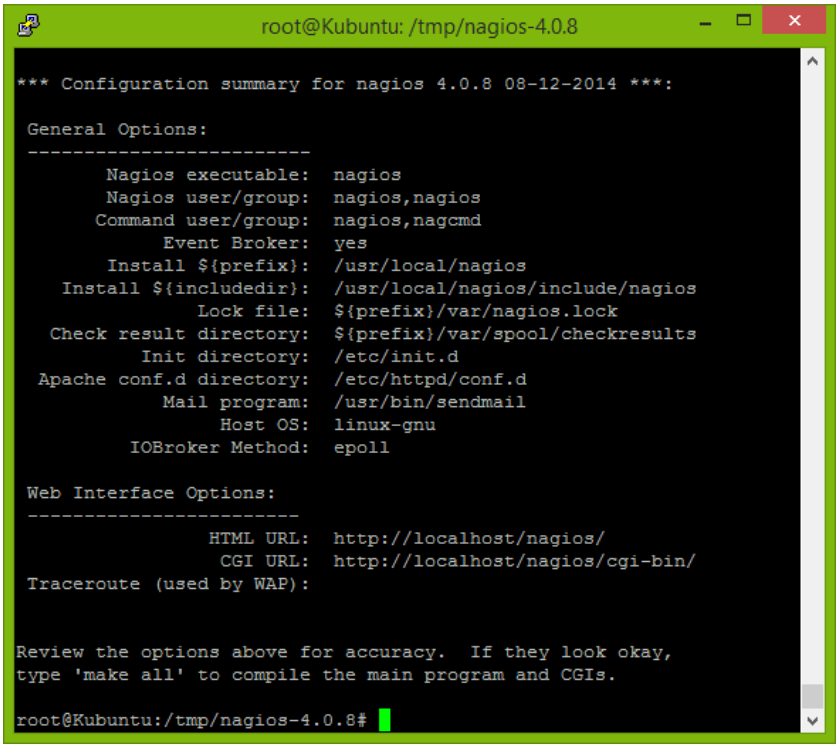
Seuraavaksi siirrytään juuri purettuun nagios-4-0-8 –kansioon cd-komennolla seuraavasti:

```
cd nagios-4.0.8
```

Tämän jälkeen voidaan aloittaa ohjelman asennus. Nagios-kansiosta löytyy configure-niminen tiedosto, joka on tyypillinen komentoriviltä suoritettava asennustiedosto. Sen käyttäminen tapahtuu kirjoittamalla ”./” configure-tiedoston nimen eteen. Asennus vaatii lisäksi muutaman parametrin, joissa määritellään käytettävät ryhmät sekä sähköpostin lähetysohjelma. Komennosta syntyy melko monimutkainen kokonaisuus, mutta tämä onnistuu joka tapauksessa seuraavasti:

```
./configure --with-nagios-group=nagios --with-command-
group=nagcmd --with-mail=/usr/bin/sendmail
```

Tämän jälkeen tilanteen pitäisi näyttää joltain tämän kaltaiselta:



KUVA 11. Nagios-ohjelman perusvalinnat asennuksen yhteydessä.

Kuvasta 11 nähdään polut, mitkä asennusohjelma lisää oletuksena. Ongelmaksi tässä kohtaa ilmenee selkeästi Apache-palvelimen konfiguraatiotiedoston polku. Omassa tapauksessa kyseistä kansiota ei ole olemassakaan, vaan Apachen konfiguraatiot löytyvät nykyään polusta /etc/apache2/conf-enabled/. Tästä syystä configure-komento tarvitsee lisäparametrin, jossa kerrotaan asennusohjelmalle oikea polku. Tässä tapauksessa komento on seuraava:

```
./configure --with-nagios-group=nagios --with-command-
group=nagcmd --with-mail=/usr/bin/sendmail --with-httpd-
conf=/etc/apache2/conf-enabled/
```

Nyt katsottaessa kohtaa ”Apache conf.d directory” polku näyttää oikean, olemassa olevan polun. Seuraavaksi käytetään Linuxin ”make”-komentoa, jonka tehtävä on koota ohjelma. Kokoaminen onnistuu helposti seuraavalla komennolla:

```
make all
```

Tämän jälkeen tarvitsee asentaa tarvittavat osat, esimerkiksi konfiguraatiotiedostot sekä web-käyttöliittymä. Tämä kaikki onnistuu muutamalla komennolla, joita asennusohjelma itsekin opastaa käyttäjää tekemään sekä kertoo mitä mikäkin eri komento tekee. Ohessa komennot, joiden avulla saa kaiken tarvittavan asennettua:

```
make install
make install-init
make install-config
make install-commandmode
make install-webconf
```

Asennuksen onnistuttua, voidaan kopioida puretusta nagios-4.0.8-kansion contrib-alikansiosta tapahtumankäsittelijät Nagioksen asennuskansioon, joka sijaitsee polussa /usr/local/nagios. Tämä onnistuu kätevästi seuraavalla komennolla:

```
cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/
```

Seuraavaksi tarvitsee vaihtaa tiedostojen ”omistajia”, jonka voi Linuxissa tehdä ”chown” komennolla. Komento rakentuu siten, että komennon perään voidaan kirjoittaa

lisäparametrinä ”-R”, joka ottaa alihakemistot mukaan rekursiivisesti. Sitten lisätään käyttäjänimi sekä ryhmä kaksoispisteellä eroteltuna, jonka jälkeen lisätään vielä tiedostopolku, mihin kyseistä operaatiota ollaan tekemässä, eli tässä tapauksessa ”eventhandlers”-kansio.

```
chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers
```

Tässä kohtaa on syytä vielä tarkistaa, ettei mitään suurempia virheitä ole päässyt syntymään. Tämä onnistuu seuraavalla komennolla:

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/na-
gios.cfg
```

Mikäli varoituksia tai virheitä ei ole, seuraava vaihe onkin käynnistää Nagios. Virheiden sattuessa ohjelma ilmoittaa hyvin virheiden sijainnin, jolloin se on helppo korjata. Nagioksen käynnistys onnistuu muidenkin ohjelmien tapaan ”init.d”-kansiosta seuraavasti:

```
/etc/init.d/nagios start
```

Komentorivi ilmoittaa, mikä Nagioksen käynnistäminen onnistui. Tarvittaessa samaan tapaan voi käynnistää uudelleen ohjelmia tai pysäyttää niitä ”restart” tai ”stop” –komennoilla. Tämä ei siis koske pelkästään Nagiosta, vaan esimerkiksi yhtä lailla Apachea tai SSH:ta. Kaikkien käynnistäminen, pysäyttäminen tai uudelleenkäynnistäminen onnistuu tätä samaa kautta. Apt-get:n kautta asennetuille ohjelmille samoja asioita voidaan tehdä seuraavallakin komennolla:

```
sudo service <ohjelman nimi> start/stop/restart
```

Nagioksen asennus on enää web-käyttöliitymän käyttäjän tekemistä sekä lisäosien asennusta vaille valmis. Tehdään ensin järjestelmävalvojan tasoinen käyttäjä, jonka nimen voi erikseen määrittää Nagioksen konfiguraatiotiedostostakin käsin. Oletuksena se on ”nagiosadmin”, joten tehdään sen niminen käyttäjä. Samalla annetaan käyttäjälle salasana. Myöhemmin voidaan samalla komennolla tehdä uusia käyttäjiä, joilla voi olla eri oikeuksia tehdä asioita käyttöliitymässä. Uutta käyttäjää lisätessä pitää muistaa ottaa ”-c” lisäparametri pois, sillä se tarkoittaa uuden htpasswd.users-tiedoston tekemistä, jota

ei tässä tapauksessa enää haluta. Järjstelmävalvojan tunnuksien tekeminen onnistuu seuraavalla komennolla:

```
htpasswd –c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

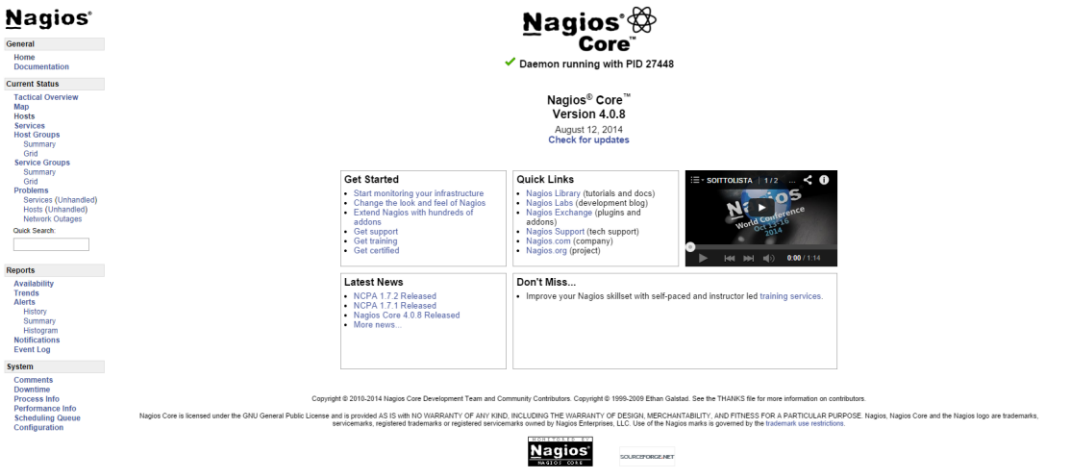
Lisäosien asennusprosessi on samantapainen, kuin itse Nagioksen, mutta paljon helpompi ja suoraviivaisempi. Aluksi navigoidaan tmp-kansioon purkamaamme nagios-plugins-2.0.3-kansioon seuraavasti:

```
cd /tmp/nagios-plugins-2.0.3
```

Kansioon siirryttyä, voidaan käyttää configure-tiedostoa samaan tapaan kuin Nagioksen kanssa. Määrityksiin käytetään sen sijaan nagios-käyttäjää ja käyttäjäryhmää. Tämän jälkeen suoritetaan ”make” ja ”make install” –komennot.

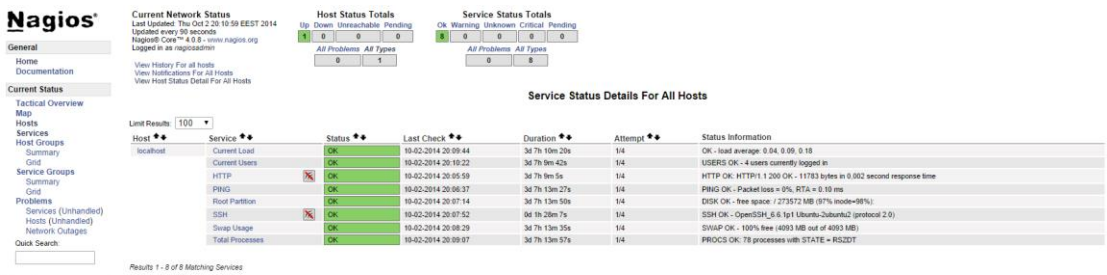
```
./configure --with-nagios-user=nagios --with-nagios-
group=nagios
make
make install
```

Nagios voi olla hyvä vielä käynnistää uudelleen tämän jälkeen, mutta nyt web-käyttöliittymään pitäisi päästä käsiksi kirjoittamalla selaimen osoiteriville ”http://palvelimen_ip/nagios/”, eli tässä simulointitapauksessa http://192.168.0.102/nagios/. Sivulle mentäessä palvelimen pitäisi kysyä käyttäjätunnusta ja salasanaa. Tähän syötetään aiemmin tehty ”nagiosadmin” tunnukseksi ja salasanaksi samassa yhteydessä laittama salasana. Mikäli erilaisia käyttäjätunnuksia on jo tehty, voidaan millä tahansa niistä kirjautua sisään. Ohessa kuva Nagios Core 4.0.5:n etusivusta:



KUVA 12. Nagios Core:n etusivunäkymä

Kuvassa 12 näkyy Nagioksen etusivu sisäänkirjautumisen jälkeen. Vasemmassa reunasta olevasta navigoinnista pääsee liikkumaan eri sivujen välillä, joista näkee erinäistä tietoa monitrointipalvelimen toiminnasta. Keskeltä ylhäältä löytyy Nagioksen nykyinen asennettu versio, joka on tässä tapauksessa 4.0.8. Mikäli uudempia versioita on saatavilla, Nagios ilmoittaa siitä ”check for updates” -tekstin kohdalla.



KUVA 13. Nagioksen Services-sivun näkymä

Kuvasta 13 pääsemme jo näkemään, mitä tietoa monitorointi meille tarjoaa. Kuvassa 13 on Nagioksen Services-sivun näkymä, jossa on listattuna kaikki monitoroitavat tietokoneet/palvelimet. Tällä hetkellä kuvassa 13 näkyy vain itse monitorointipalvelin,

sillä muita ei ole vielä lisätty. Nagios tarjoaa helposti luettavaa tietoa suoraan esimerkiksi ping-pyyntöön vastaamisesta sekä palvelimen kuormituksesta. Kaikkien ”statuksen” ollessa vihreitä, näkee suoraan, että palvelin toimii oikein.

Map-sivu näyttää palvelimet karttana, josta näkee helposti miten palvelimet ovat yhteydessä toisiinsa ja rakenne on täten helppo havaita. Muilta sivuilta löytyy tarkemmin tietoa tietystä palvelimesta, mikäli lisää infoa kaivataan. Hosts-sivu näyttää vain palvelimien tilan ja pienen statuksen sekä milloin sen tiedot on viimeiseksi päivitetty.

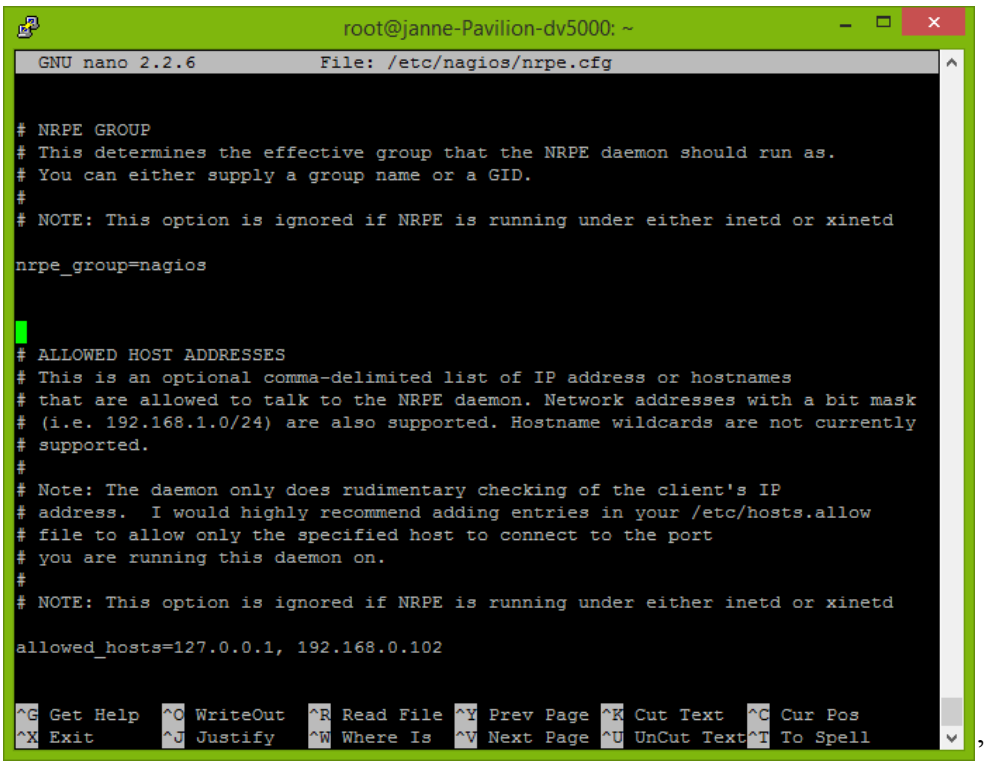
3.2 Nagios NRPE-palvelimen asentaminen ja konfigurointi

Jotta Nagioksesta saadaan enemmän irti ja päästään haluttuun lopputulokseen itse työn kannalta, niin tarvitsemme tuen etämonitoroinnille. Nagios toimii itsessään hyvin ja kertoo paljon palvelimen tilasta, mutta mitä pitää toimia, jos haluammekin Nagioksen monitoroivan itsensä lisäksi monia muita palvelimia, jotka sitten listautuisivat kaikki samaan paikkaan. Tässä kohtaa esiin astuu NRPE (Nagios Remote Plugin Executor). NRPE sallii Nagioksen lisäosien suorittamisen etänä muilla Linux/Unix laitteilla. Tämä sallii laitteiden etämonitoroinnin (levyn käytön, prosessikuorman yms.). NRPE pystyy myös kommunikoimaan joidenkin Windows laitteiden lisäosien kanssa, joten voit suorittaa scriptejä ja seurata myös Windows laitteiden tilaa. (NRPE 2013.)

NRPE-lisäosa tulee aiemmin asennetun ”Nagios plugins” paketin mukana, mutta on kuitenkin syytä tiedostaa, mistä on kyse. Lisäosa pitää siis olla asennettuna siinä palvelimessa, jossa itse monitorointiohjelmisto toimii. Tämän lisäksi etämonitoroitavaan laitteeseen tarvitaan pieni NRPE-palvelin, joka osaa kommunikoida monitorointipalvelimen kanssa. Palvelimen asentaminen onnistuu erittäin helposti komennolla:

```
sudo apt-get install nagios-nrpe-server
```

Seuraavaksi tarvitsee tehdä pieni konfiguraation, jotta laitteiden välinen kommunikaatio toimii, kuten pitää ja monitorointitieto saadaan välitettyä. Laitteelle, jonne NRPE-palvelin asennettiin, tarvitsee määrittää sitä kuuntelevan palvelimen IP-osoite. Tiedosto, jota pitää muokata, löytyy polusta /etc/nagios/nrpe.cfg.



KUVA 14. NRPE-palvelimen konfiguraatiotiedosto

Kuvassa 14 on kyseinen nrpe.cfg –tiedosto avattuna Nano-nimisellä yksinkertaisella tekstieditorilla. Avaaminen onnistuu komennolla:

```
sudo nano /etc/nagios/nrpe.cfg
```

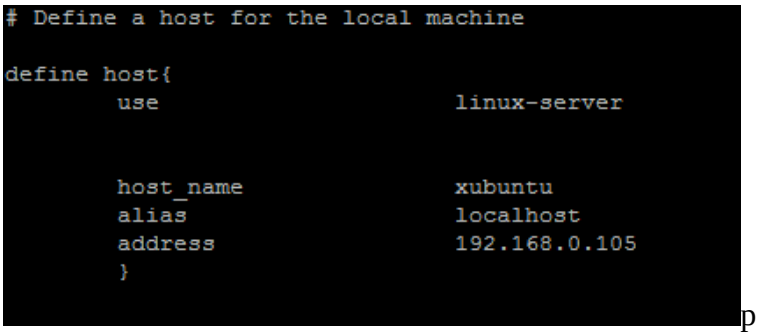
Tiedostosta löytyy Allowed host addresses -kohta, jonka alapuolelta löytyy IP-osoitteet, joilta sallitaan pääsy NRPE-palvelimeen. Kuvassa 14 olen lisännyt paikallisen IP:n perään monitorointipalvelimen IP-osoitteen pilkulla eroteltuna, jotta monitorointipalvelimen saa oikeuden tarkastella NRPE-palvelinta. Muita konfiguraatioita peruskäyttöön ei tässä tapauksessa tarvitse tehdä NRPE-palvelimen sisältävään laitteeseen.

Monitorointipalvelimeen pitääkin tehdä hieman enemmän konfigurointeja. Polusta /usr/local/nagios/etc/objects löytyy localhost.cfg –niminen tiedosto. Tätä voi käyttää pohjana tehdessämme NRPE-laitteelle oma cfg-tiedosto. Tiedoston kopiointi ja uudelleennimeäminen onnistuu helposti seuraavalla komennolla olettaen, että olemme navigoineet jo edellä mainittuun polkuun:

```
cp localhost.cfg xubuntu.cfg
```

Tiedostonimellä ei ole väliä, mutta on syytä tehdä niistä sellaisia, jotta varmasti tiedetään mikä vastaa mitäkin monitoroitavaa laitetta. Tässä tapauksessa, kun NRPE-palvelimen omaavassa tietokoneessani on Xubuntu-käyttöjärjestelmä, niin tiedän heti, että on kyse tästä laitteesta. Oikeasti nimen olisi syytä olla hieman kuvaavampi. Tämän jälkeen tiedosto voidaan avata tuttuun tapaan komennolla:

```
sudo nano xubuntu.cfg
```



p

KUVA 15. Konfiguraatiotiedosto etämonitoroitavalle laitteelle

Kuvasta 15 löytyy olennaisin kohta xubuntu.cfg tiedostosta. Use-kohta kertoo mitä ryhmää käytetään. Tämä on aikaisemmin määritetty localhost.cfg-tiedostossa. Laitteita voidaan jakaa nimen perusteella erilaisiin ryhmiin, mikä helpottaa lukemista web-käyttöliittymästä. Nämä voisivat olla esimerkiksi ”www-palvelimet, tietokantapalvelimet yms.”, jolloin tiedetään heti mitä tietty ryhmä sisältää. Host_name kertoo yksinkertaisesti monitoroitavan palvelimen isäntänimen, joka pitää olla sama, kuin tiedostonimi. Aliaksella voidaan muuttaa nimi helpommin luettavaan muotoon, mikäli host_name on pitkä ja hankala. Aliaksella ei kuitenkaan voi määritellä tarvittavia ominaisuuksia alempana, vaan näihin pitää viitata laitteen oikealla isäntänimellä eli host namella. Alias on vain web-käyttöliittymää varten, jolloin eri palvelimet voidaan helposti erottaa toisistaan. Address-kohtaan syötettään etämonitoroitavan palvelimen IP-osoite.

Alempaa löytyy Host group-kohdan määrittäminen, jotka tulee vaihtaa, mikäli ryhmän nimi on jotain muuta kuin normaali ”Linux server”. Tämä aiheuttaa muuten ristiriitaa localhost.cfg-tiedoston kanssa, mikä johtaa siihen, ettei apache/nagios suostu edes käynnistymään. Tiedoston loppuosa on erilaisten palveluiden määrittämistä varten, joiden halutaan näkyvän web-käyttöliittymässä ja joita halutaan ylipäätään monitoroida.

Seuraavaksi tulee vielä avata polusta /usr/local/nagios/etc löytyvä nagios.cfg-tiedosto. Tiedostosta löytyy määrityksen useille eri tiedostoille ja näiden polut. Nagiokselle pitää kertoa uudesta lisäämästämme etämonitoroitavasta koneesta yksinkertaisesti lisäämällä muiden tapaan seuraava rivi:

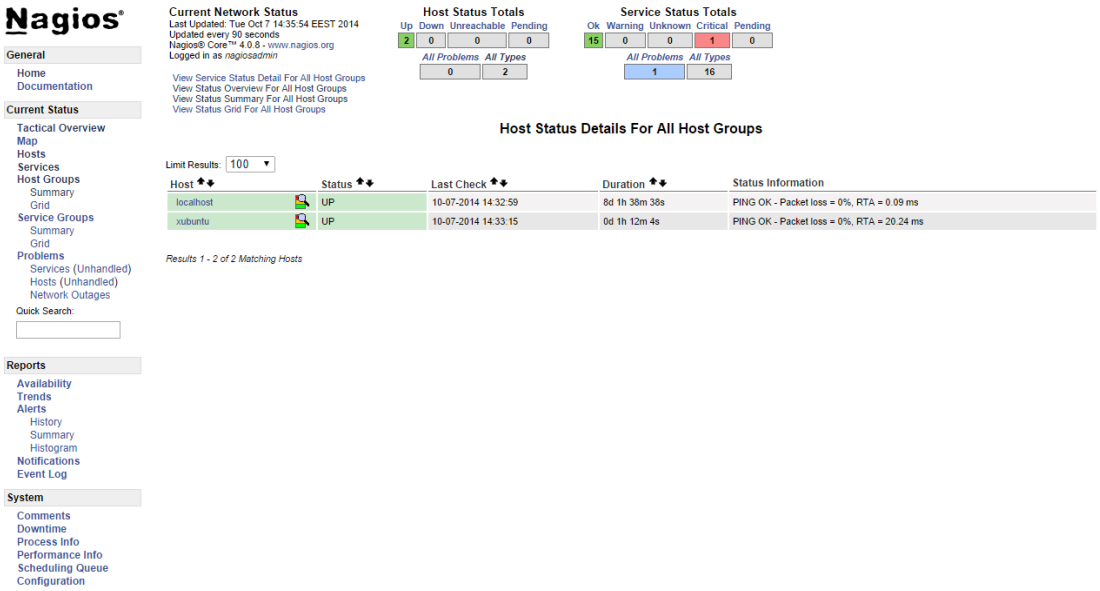
```
cfg_file=/usr/local/nagios/etc/objects/xubuntu.cfg
```

Nyt Nagios osaa ottaa huomioon myös vasta lisäämämme laitteen ja hyödyntää sen konfiguraatiotiedostoa. Mikäli järjestelmään lisätään uusi palvelin, edellinen rivi voidaan kopioida suoraan ja tiedoston nimeksi vaihdetaan vain uuden lisätyn palvelimen nimi. Tämän jälkeen on syytä vielä käynnistää uudelleen sekä NRPE-palvelin, että Nagios. Nagioksen uudelleenkäynnistys onnistui komennolla:

```
sudo /etc/init.c/nagios restart
```

NRPE-palvelin voidaan käynnistää service-komentoa käyttäen, sillä NRPE-palvelin on asennettu apt-get:n avulla.

```
sudo service nagios-nrpe-server restart
```



KUVA 16. Nagioksen Hosts-sivun näkymä etämonitoroitavan laitteen lisäyksen jälkeen

Kuten kuvasta 16 nähdään, nyt listauksessa on mukana myös vasta asentamamme etämonitoroitava laite. Tästä laitteesta saadaan samat tiedot, kuin monitorointipalvelimestakin vain asentamalla tarvittava palvelin. Lisää laitteita voidaan lisätä samalla periaatteella helposti ja nopeasti niin paljon kuin tarvitaan. Muiden palvelimien lisäyksen jälkeen tähän listaan tulevat kaikki asennetut palvelimet.

3.3 Sähköpostikonfiguraatiot

Opinnäytetyöni toinen kokonaisuus on hälytykset. Ilmoitukset ongelmista esimerkiksi sähköpostitse on erittäin tärkeä osa koko monitorointikokonaisuutta, joten seuraavaksi on syytä konfiguroida kuntoon myös tämä osa-alue. Nagioksen tarjoamien hyvien ominaisuuksien ansiosta hälytysjärjestelmän toiminta on erittäin helppoa asentaa. Erillisiä lisäosia ei tarvita. Riittää, kun kerromme mitä Linuxin sähköpostinlähetysohjelmaa halutaan käyttää. Asennusvaiheessa voidaan määrittää käytettävän sähköpostiohjelman hakemisto samalla tavalla, kuin määriteltiin Apachen konfiguraatiotiedoston polku. Komentomme oli seuraava:

```
./configure --with-nagios-group=nagios --with-command-
group=nagcmd --with-mail=/usr/bin/sendmail –with-httpd-
conf=/etc/apache2/conf-enabled/
```

Tässä tapauksessa sendmail-ohjelman polku on myös väärin, joka tuottikin asennusvaihessa ogelmia, miksi hälytykset eivät tahtoneet toimia. Yksinkertainen muutos oli käyttää Linuxin mail-ohjelmaa ja vaihtaa polku seuraavaksi:

```
--with-mail=/usr/bin/mail
```

Nyt mail-ohjelman polku on oikein ja Nagios osaa käyttää sitä notifikaatioihin. Polusta ”/usr/local/nagios/etc/objects” löytyy contacts.cfg niminen tiedosto, jonne määritetään haluttu sähköposti. Tämän jälkeen Nagios tulee käynnistää uudelleen, jotta muutokset astuvat voimaan tutulla komennolla:

```
/etc/init.d/nagios restart
```

Polku on mahdollista vaihtaa myöhemmin myös Nagioksen konfiguraatiotiedostosta käsin, mutta tämän tiedostaessa helpoin tapa on vaihtaa se heti asennuksen yhteydessä, sillä se pitää joka tapauksessa määrittää asennuksessa.

4 PÄÄTÄNTÖ

Työ onnistui kokonaisuudessaan hyvin. Minulla oli hyvin aikaa testata ja opiskella järjestelmää kotona ja kerätä internetistä paljon tietoa. Tässäkään ei tosin ongelmilta vältytty, sillä juuri sellaista ohjetta ei mistään löytynyt, jonka avulla Nagioksen asentaminen olisi suoraan onnistunut. Oli siis pakko kerätä tietoa useasta eri lähteestä ja yhdistää niistä yksi toimiva tapa asennukseen. Tämä oli tietysti vain mielenkiintoista, eikä lievältä turhautumiseltakaan vältytty. Onnistuin kuitenkin keräämään tarpeeksi tietoa, jotta sain ymmärryksen koko järjestelmästä ja se auttoi minua ratkaisemaan ongelmat. Loppujen lopuksi asennusprosessi ei ole vaikea, kun sen vain oppi. Linuxin jouheva käyttö komentoriviltä ja aikaisempi kokemus olivatkin avainasemassa asennuksessa. Koko järjestelmää pystyy ymmärtämään paljon paremmin, kun perusasiat ovat hallussa.

Suuri haitta Nagioksessa nimenomaan ainakin tällä hetkellä on se, että sen asentaminen ei suoraan onnistu ”apt-get”-komennolla. Tai onnistuu, mutta uusinta versiota ei ole tarjolla ja ikävä kyllä käsin päivittäminen jälkikäteen on erittäin haastavaa. Tämän takia Nagios oli syytä asentaa suoraan lähteestä, joka on monin tavoin aluksi vaikeampaa, mutta samalla myös erittäin toimivaa. Tällä tavoin uuden version ilmestyessä päivittäminen onnistuu helposti ja nopeasti. Päivityksessä koko asennusprosessia ei tarvitse alusta loppuun, vaan ainoastaan osa sitä, jossa itse asennus tapahtuu ja vanha versio korvautuu uudemmalla.

Ongelmia matkalle mahtui joitakin. Epämääräisistä ohjeista johtuen olin aluksi sellaisessa uskossa, ettei NRPE-tukea ollut suoraan uusimmalle Nagios-versiolle. Tämä tuntuikin liian oudolle ollakseen totta, sillä koko järjestelmän idea on nimenomaan etämonitorointi. Hieman lisää infoa etsittyäni löysin tavan, jolla sen sai toimimaan myös uusimmalla versiolla, jonka jälkeen järjestelmä olikin jo mahdollista asentaa oikeille tuotantopalvelimille. Ohjeistin Smart Timella asennuksen kanssa itse sen selvitettyäni ja teimme samalla muistioon ohjeet jatkoa ajatellen, miten Nagios NRPE-tuen kanssa asennetaan, jotta koko asiaa ei tarvitse miettiä uudestaan, mikäli sitä ei pitkään aikaan tarvitse tehdä. Ohjeet etämonitoroinnin asennukseen ovat sen sijaan vielä tärkeämmät tulevaisuutta varten, sillä uusia palvelimia pitää lisätä vielä useita, joten nyt se onnistuu työntekijöidenkin puolesta. Asennus tuotantopalvelimille onnistui melko helposti muutama ongelmaa lukuunottamatta pientä säätöä sähköpostikonfiguraation kanssa. Vasta

tässä vaiheessa huomasin, että hälytysjärjestelmä toimii parhaiten luvussa 3.3 mainitulla mail-ohjelmalla. Tämän yhteyttä sendmailiin en oikein edes tiedä, mutta vakiopolulla notifikaatiot eivät toimineet. Mikäli sähköpostiohjelman polkua ei itse asennusvaiheessa vaihdettu, sen voi myöhemmin vaihtaa käsin myöhemmin Nagioksen konfiguraatiotiedostosta. Itse Nagioksen asennus sujui ongelmitta.

Hieman ongelmia liittyi myös oletuspolkuihin asennusprosessissa. Nagios yrittää tarjota Apachen konfiguraatiotiedoston oletuspolkua ”httpd”-kansioon, joka on uusimman Apache-version myötä vaihtanut paikkaa. Tämä koitui ongelmaksi siinä kohtaa, kun konfiguraatiotiedostoa ei löytynyt, jolloin huomasin, että polku on väärin. Pienellä lisäparametrilla polun pystyi muuttamaan, jolloin tiedosto löytyy oikeasta paikasta.

Työ kokonaisuudessaan onnistui hyvin ja aikataulu pysyi hyvin kiinni. Sain työtä jatkuvasti hyvin eteenpäin, vaikka ongelmia matkalle mahtuikin. Toisaalta, jos asennus olisi onnistunut noin vain, se olisi varmasti ollut liian helppo prosessi ja mielenkiinto olisi voinut laantua. Ongelmia on siis suotavaakin mahtua matkalle ja niiden kautta oppiminen on erittäin tehokasta ja mukavaakin. Aineistoa internetistä löytyy aiheeseen liittyen paljon, mutta kriittinen lukutaito on valttia myös tässä. Jos jokin tekniikka näytti vaikeasti selitetyltä tai toisaalta niin sanotulta purkkapatentilta, kannatti suosiolla yrittää toisella hakusanalla ja/tai katsoa eri lähteestä omasta mielestä parempaa ohjetta. Yleensä asiat voi tehdä joko helposti tai vaikeasti, joista molemmat todennäköisesti saattavat toimia yhtä hyvin, mutta asennusvaiheessa ero on merkittävä. Monista eri lähteistä tiedon koostaminen auttoi pääsemään haluttuun lopputulokseen. Niin monitorointipalvelimen, kuin etämonitoroitavankin asennus onnistui sekä simuloiden, että Smart Timella tuotantopalvelimille asennettaessa, joten lopputulokseen voi olla erittäin tyytyväinen niin itse, kuin yrityksenkin päässä.

LÄHTEET

Bartle, Phil 2011. Artikkeli. http://www.businessdictionary.com/definition/monitoring.html. Päivitetty 30.9.2011. Luettu 17.9.2014.

Nagios overview. 2014. WWW-dokumentti. http://www.nagios.org/about/overview. Ei päivitystietoa. Luettu 18.9.2014.

About Cacti. 2013. WWW-dokumentti. http://www.cacti.net/. Ei päivitystietoa. Luettu 28.10.2014.

Ubuntu Suomi. Esittely. WWW-dokumentti. http://wiki.ubuntu-fi.org/Esittely. Ei päivitystietoa. Luettu 2.10.2014.

Peltomäki, Juha & Linjama, Tero 1999. Linux-käyttäjän peruskirja. Porvoo: WSOY.

Sonera.fi. Vasteajan mittaus. 2014. WWW-dokumentti. http://www5.sonera.fi/ohjeet/Vasteajan_mittaus. Ei päivitystietoa. Luettu 18.9.2014.

Saive, Ravi 2014. Artikkeli. http://www.tecmint.com/command-line-tools-to-monitor-linux-performance/. Päivitetty 27.4.2014. Luettu 18.9.2014.

GNU Wget 2012. WWW-dokumentti. http://www.gnu.org/software/wget/. Päivitetty 2.9.2012. Luettu 1.10.2014.

NRPE - Nagios Remote Plugin Executor 2013. WWW-dokumentti. http://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE--2D-Nagios-Remote-Plugin-Executor/details. Päivitetty 6.9.2014. Luettu 7.10.2014.