Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Jussi Siuro

Opinnäytetyö

Verkonvalvonta Stonesoftin testiverkkoon

Työnohjaaja: Harri Hakonen
Tilaaja: Stonesoft Oyj
Helsinki 11/2008

Tampereen ammattikorkeakoulu, tietojenkäsittelyn koulutusohjelma
Tekijä: Jussi Siuro
Työn nimi:Verkonvalvonta Stonesoftin testiverkkoon
Sivumäärä: 39
Valmistumisaika: Syksy 2008
Työnohjaaja: Harri Hakonen
Työn tilaaja: Stonesoft Oyj

TIIVISTELMÄ

Opinnäyte työn aiheena oli toteuttaa verkonvalvonta järjestelmä Stonesoftin testiverkkoon. Aluksi tuli tutkia mahdolliset vaihtoehdot verkonvalvonta ohjelmaksi. Nopean tarkastelun jälkeen päädyttiin Nagiokseen.

Teoriaosuudessa keskityttiin verkonvalvontaan yleisellä tasolla. Aluksi pyrittiin selvittämään, minkä takia on tarpeellista tukeutua nykyisissä verkoissa keskitettyyn verkonvalvontaan. Valvonta protokollista SNMP oli suurennuslasin alla, koska se on yleisin ja tehokkain verkonvalvontaan tarkoitettu työkalu. SNMP oli myös käytössä toteutetussa työssä.

Käytännön työ tehtiin Stonesoft Oyj:n toimeksiannosta. Työ toteutettiin asentamalla Nagios alustavasti testiverkkoon ja lisäämällä valvottavat kohteet. Työn määrä oli melko suuri, koska laitteita oli paljon ja vaihtuvuus suuri. Asennuksen jälkeen laitteet olivat monitoroitavissa www-käyttöliittymän kautta. Nagioksen konfigurointia käsiteltiin opinnäytetyössä verkkolaitekohtaisesti.

Tulevaisuudessa opinnäyte työtäni on mahdollista käyttää nykyisen ympäristön ylläpitämiseen ja kehittämiseen. Useimmat verkot ovat identtisiä keskenään rakenteeltaan, joten työn pohjalta voi myös rakentaa pohjan omalle verkonvalvonta järjestelmälle.

Avainsanat Nagios, SNMP, palomuuri, verkonhallinta, tietoliikenne

TAMK University of Applied Sciencies
Degree Programme in Business Information Systems
Writer: Jussi Siuro
Thesis: Implementing Network Management System in Stonesoft Testing Network
Pages: 39
Graduation time: Autumn 2008
Thesis Supervisor: Harri Hakonen
Co-operating company: Stonesoft Corporation

ABSTRACT

Topic of the thesis was to implement a network monitoring system in Stonesoft test network. At first some studying had to be done to find suitable Monitoring software. It was pretty obvious from the beginning that the product will be Nagios. Nagios is most flexible product for this purpose of use.

Theory part of the thesis was mainly focusing on Network monitoring in generally. It is important that nowadays large companies are able to optimize their networking by monitoring the status of the network. The thesis was also handling SNMP. SNMP is a protocol, which is developed to manage and monitor devices on an IP network. It is most common protocol for monitoring network devices at the moment.

The practical part of the thesis contained the steps how-to implement the Nagios and what is needed in order to monitor different Operating Systems and network devices. The Nagios was installed in test network environment and basic checks were performed on monitored devices. After the installation it was possible to monitor network devices via web-interface of Nagios.

In future this thesis is possible to use as a guide to implement or maintain Nagios network monitoring system. And this is not only for Stonesoft test network, because large scale networks are pretty identical so this is applicable for other environments as well.

Keywords Nagios, SNMP, firewall, network mangement, data communications

Sisällysluettelo

1. Johdanto **6**

1.1 Taustaa opinnäytetyöhön **6**

1.2 Opinnäytetyön tarkoitus **6**

2 Stonesoft Oyj **7**

3 Verkonhallinta **9**

3.1 Verkonhallinnan vaatimukset **9**

3.1.1 Vikojen hallinta 11

3.1.2 Käytön hallinta 11

3.1.3 Kokoonpanon hallinta 12

3.1.4 Suorituskyvyn hallinta 13

3.1.5 Turvallisuuden hallinta 13

4 SNMP Verkonhallintaprotokolla **15**

4.1 Komponentit **15**

4.1.1 Manageri 16

4.1.2 Agentti 16

4.1.3 Hallintatietokanta 17

4.2 SNMP ja UDP **17**

5 Nagioksen toteutus Stonesoftin testiverkkoon **21**

5.1 Verkonvalvontatyökalun valintaan vaikuttavat kriteerit **21**

5.2 Nagios **23**

5.2.1 Kuinka Nagios toimii? 25

5.2.2 Nagioksen konfigurointi 25

5.2.3 Nagioksen käyttöönotto Stonesoftin testiverkkoon 26

5.2.4 Valvottavat kohteet 27

5.2.4.1 Windows palvelimet 28

5.2.4.2 Verkkolaitteet 30

5.2.4.3 Linux koneet ja palomuurit 32

6 Kehitysnäkymät 35

7 Käsitteet 37

Lähteet 39

1. Johdanto

Yhteisöjen ja yritysten toimintoja siirretään jatkuvasti yhä enemmän verkkoon. Verkkojen koko kasvaa, laitteiden määrää ja luonnollisesti vikojen määrä kasvaa. Tästä johtuen tulee nopeasti olla käsillä tieto missä vika on. Parempi on, jos viat voidaan estää ennen aikaisesti. Tätä varten on kehitetty keinoja joilla voidaan monitoroida verkon laitteita ja toimintoja, sekä saada reaaliaikaista tietoa verkon tilasta. Tämä tieto voidaan tuoda vaikka suoraan kännykkään.

1.1 Taustaa opinnäytetyöhön

Olen töissä Stonesoft Oyj:ssä, joka on suomalainen ohjelmistoyritys, päätuotteenaan sillä on StoneGate tietoturvajärjestelmä. StoneGate on kokonaisuus, mihin kuuluu niin palomuuri, tunkeutumisen havainnointi kuin IPSec ja SSL VPN. Tätä kaikkea ohjataan keskitetyllä hallintajärjestelmällä, StoneGate Management Center (SMC).

Yrityksellä on useita tuotteita, jotka vaikuttavat moneen asiaan. Tätä varten on oltava toimiva testausympäristö. Tuotteen testaamista varten on rakennettu oma testiverkko, missä omien laitteiden lisäksi ovat tietenkin muut verkkolaitteet, kytkimet, reitittimet sekä useat palvelimet useine palveluineen.

Fyysisten laitteiden määrän vähentämiseksi osan palveluista tarjoaa virtuaaliympäristöön asennetut palvelimet. Yhdestä kokonaisuudesta, missä testejä tehdään, tulee jo pienen yrityksen verkko. Näitä kokonaisuuksia on useampi. Tämä sen takia, että testaaminen olisi mahdollisimman tehokasta.

1.2 Opinnäytetyön tarkoitus

Toimeksiantaja näki tarpeelliseksi, että testiverkolle tulisi rakentaa toimiva monitorointi järjestelmä. Valvonta järjestelmällä säästettäisiin huomattavasti aikaa ja voitaisiin vähentää mahdollisia itse verkosta johtuvia virheitä. Kun verkossa olevat virheet voidaan sulkea pois, niin itse tuotteen testaus muuttuu tehokkaammaksi

2 Stonesoft Oyj

Stonesoft Oyj on suomalainen, vuonna 1990 perustettu kansainvälisesti toimiva tietoturva yhtiö, jolla on pääkonttori Helsingissä ja Amerikan pääkonttori sijaitsee Atlantassa. Tällä hetkellä Stonesoft työllistää n.190 henkilöä. Stonesoft keskittyy yritysten verkkoturvallisuuteen, sekä asiakkaitten yhä enemmän verkkoon siirtyvän liiketoiminnan turvaamiseen.

Stonesoft aloitti aluksi tietoturvaratkaisujen jälleenmyyjänä, mutta pian Stonesoft aloitti oman ohjelmiston kehittelyn, joka saikin hyvän vastaanoton kansainvälisillä markkinoilla. Tämä tuote oli StoneBeat -tuoteperhe, joka julkaistiin vuonna 1996. StoneBeatin tarkoituksena oli varmistaa tietojärjestelmien ja tietoliikenteen korkea käytettävyys. Tuolloin ei vielä ollut vastaavia tuotteita markkinoilla, vaikka yritykset olivatkin siirtämässä liiketoimintaansa verkkoon. Tämän seurauksena Stonesoft katsoi, että korkea käytettävyys olisi nouseva tärkeäksi kilpailutekijäksi.

Vuonna 2001 Stonesoft toi markkinoille StoneGate-ohjelmiston, joka on VPN- ja palomuuriratkaisu, jossa käytettään StoneBeat tuoteperheen parhaita ominaisuuksia. Vuonna 2004 StoneGate -tuoteperhe laajeni entisestään, kun palomuuri sai rinnalle IPS:n, eli tunkeutumisen havainnointi- ja estämisjärjestelmän. Nykyään StoneGate käsittää edellä mainittujen lisäksi vielä SSL VPN:n. SSL VPN on etäkäyttäjille tarkoitettu etäyhteys, jota voi käyttää mistä tahansa millä laitteella tahansa. SSL VPN ei tarvitse erillistä asiakasohjelmaa, kuten Ipsec VPN. Kaikkia edellä mainittuja komponentteja hallinnoidaan keskitetysti StoneGate Management Centerin avulla.

Talous ja tulevaisuus

Stonesoft Oyj:n liikevaihto kasvoi voimakkaasti StoneBeatin lanseeraamisen jälkeen. Vuonna 1997 liikevaihto oli 6,7 miljoonaa euroa ja vuonna 2001 se oli jo 57,7 miljoonaa euroa. Vuonna 1999 yhtiö listautui pörssiin. Yhtiön strategisten muutosten takia liikevaihto alkoi pienetä ja vuonna 2003 se oli enää 23,1 miljoona euroa.

Vuoden 2007 aikana Stonesoft Oyj:n toiminta kehittyi suotuisasti. Vuoden 2007 päätavoite oli liikevaihdon kasvu ja kaiken kaikkiaan Stonesoft Oyj kasvatti liikevaihtoaan 15%:lla ja päätuotteensa, StoneGaten myyntiä 28%:lla. Vuoden 2007 liikevaihto oli 19 miljoonaa euroa. (Vuosikertomus 2007.)

Stonesoft konserniin kuului vuoden alussa 2006 Oulussa sijaitseva Embe Systems Oy. Embe on sulautettujen ohjelmistoratkaisujen asiantuntija yritys, mutta Stonesoft myi sen vuonna 2006. Syy tähän oli halu keskittyä yrityksen ydinliiketoimintaan, StoneGaten tuotekehitykseen. Tuotekehitysyksiköt ovat Helsingissä ja Sophia Antipoliksessa Ranskassa. (Vuosikertomus 2006.)

Vuosi 2008 näyttää Stonesoftin kannalta hyvältä. Isot tilaukset tämän vuoden puolella lupaavat Stonesoftille hyvää tulosta vuodelle 2008. Vuosia miinuksella ollut kassavirta saattaa kääntyä plussan puolelle.

3 Verkonhallinta

Tietoverkkojen pääasiallinen tehtävä on kuljettaa dataa. Tietoverkossa voidaan tarjota erilaisia palveluita, joiden tarjoamisen erinäiset protokollat mahdollistavat. Mutta toimiva verkko kaipaa myös protokollia ja palveluita, jotka vahtivat verkkoa ja sen laitteita. Verkon ylläpitäjänä toimiminen nykypäivänä olisi täysin mahdotonta, kun verkot eivät välttämättä rajoitu enää vaan rakennukseen, eikä valtion rajaan vaan se on levittäytynyt koko maailmaan. Organisaatiolle toimiva verkko on jo suuri investointi, joka halutaan pitää kunnossa. Globaaleista verkoista puhuttaessa ei sen hallinta ole enää yhden ihmisen käsissä, vaan itse verkkoa ja sen toimintaa organisaatiossa hoitaa oma pieni organisaatio. Organisaatiolla on verkkohallintastrategia ja tarvittavat työkalut.

Verkonhallintajärjestelmä on yleensä ohjelmisto, jolla verkkoa valvotaan. Näissä järjestelmissä eri verkon osissa sijaitsevat laitteet keskustelevat asennetun ohjelmiston kanssa, joka sitten antaa kokonaiskuvan verkon tilasta verkonvalvojalle. Verkonhallinnasta on tullut tärkeä osa yritysten liiketoimintaa, ja verkon valvontaan laitetaan rahaa varmistaakseen sen toimivuus. Tämän takia on tärkeää varmistaa, että verkonvalvontaan tehtävät investoinnit ovat jollain tavalla suhteutettu siitä saatavaan hyötyyn. (Hautaniemi 1994)

3.1 Verkonhallinnan vaatimukset

Terplan on listannut periaatteita, joilla perustellaan verkonvalvonnasta saatava etu.

- Organisaation omaisuuden kontrollointi
    - Tietoverkot ovat firmoille elintärkeitä. Ilman tehokasta kontrollia verkot eivät maksa itseänsä takaisin
- Hallinnan kompleksisuus
    - Jatkuvasti kasvavat verkot ovat uhka tarkalle verkonvalvonnalle.
- Palveluiden parantaminen
    - Palveluiden oletetaan kasvavan samassa suhteessa kun organisaation verkkoresurssit kasvavat.
- Tarpeiden tasapainottaminen

    - Eri käyttäjäryhmät tarvitsevat erilaisia palveluita ja eritavalla resursseja käyttöönsä. Verkonvalvojan täytyy ottaa huomioon ja jakaa nämä oikein.
- Katkosten vähentäminen
    - Nykyaikana tietoverkot ovat niin tärkeitä yrityksille, että vaatimukset verkossa olevien palveluiden saatavuudelle tulee olla sata prosenttia.
- Kustannusten hallinta
    - Verkon käyttäjille tulee olla tarvittavat resurssit käytössä kohtuuhintaan. Tämän takia verkon käyttöastetta tulee tarkkailla jatkuvasti.

(Stalling 1993: 3) [1]

Edellä mainitut Terplanin listaamat edut ovat käytännöllisiä, kun haetaan oikeutusta kunnollisen verkonvalvonnan rakentamiselle. Nämä eivät kuitenkaan ole riittävän käytännönläheisiä luomaan toimivaa verkonvalvonta järjestelmää. Kansainvälinen standardointi organisaatio (ISO) on kehittänyt tätä varten jaottelun, osana OSI -järjestelmänhallintaa. OSI -järjestelmänhallinta on joukko standardeja, joilla määritellään verkonhallintasovelluksia, hallintapalvelut ja käytettävät hallintaprotokollat.

- Vikojen hallinta
- Käytön hallinta
- Kokoonpanon hallinta
- Suorituskyvyn hallinta
- Turvallisuuden hallinta

Nämä jaetaan vielä kahteen ryhmään: verkonvalvontaan ja verkonhallintaan. Verkonvalvonta on verkon tilan tarkkailua ja analysointia. Verkonhallinta taas on enemmänkin verkon dokumentointia ja asetusten määrittelyä. Ensiksi mainittuun ryhmään kuuluvat vikojen, suorituskyvyn ja käytön valvonta.

[1] Alkuperäinen lähde: Terplan K. 1992. Communication Networks Management. Englewood Cliffs, NJ

3.1.1 Vikojen hallinta

Vika on epänormaali verkon tila, mikä vaati toimenpiteitä verkonylläpitäjän taholta. Esimerkiksi virheellinen verkkokaapeli, rikkoutunut kytkin tai palvelimen hajonnut kovalevy ovat vikoja, jotka edellyttävät välittömiä toimia verkon toimintakyvyn palauttamiseksi. Vika tulee erottaa verkon häiriöstä, joita esiintyy ajoittain ja joihin ei välttämättä ehdi edes reagoida, ennen kuin tilanne on palautunut ennalleen.

Vikojen hallinnassa on tärkeintä paikallistaa mahdollisimman nopeasti vian aiheuttaja. Verkkohäiriöiden paikallistamisessa verkossa apuna ovat erinäiset valvontatyökalut. Sen jälkeen kun vika on paikallistettu, tulee muu verkko eristää häiriöiltä tai muuttaa verkon asetuksia niin, että häiriö tai vioittunut komponentti aiheuttaa mahdollisimman vähän haittaa. Lopuksi tulee tietenkin vaihtaa rikkoutuneet komponentit uusiin ja palauttaa verkko tilaan, missä se oli ennen häiriötä.

Käyttäjät odottavat nopeaa ja luotettavaa vikojen hallintaa. Jos käyttäjät saavat tarpeeksi nopeasti tietoa ja selvityksen siitä mihin kaikkeen viat vaikuttavat, he sietävät yllättävän hyvin vikatilanteita. Käyttäjien tiedottaminen pätee myös ennalta päätettyjen huoltokatkoihin. Hyvin hoidetussa verkossa ilmenee ja tulee ilmetäkin huoltokatkoja. Tämänlaisia tilanteita varten verkossa tulee olla vaihtoehtoisia reittejä mitä hyödyntää. Aina ei välttämättä vika ole omassa lähiverkossa vaan operaattorien puolella, tällöin on hyvä olla useita reittejä käytössä myös ulospäin, parasta on, että vaihto sujuu käyttökatkoksitta ja automaattisesti

3.1.2 Käytön hallinta

Jossain organisaatioissa saatetaan laskuttaa yksiköitä tai projekteja verkon käytöstä. Tämä on käytännössä organisaation sisäistä varainsiirtoa, mutta sillä voidaan valvoa ja kontrolloida verkon käyttöä. Näin saadaan selville tai vahtia käyttäjiä tai käyttäjäryhmiä, jotka saattavat hyväksikäyttää verkkoa tai tietämättään kuormittaa verkkoa suotta. Asiaa tarkasteltaessa toiselta puolelta, ylläpitäjä voi opastaa käyttäjiä tehokkaampaan verkon käyttöön, mikäli hän huomaa, että verkko ei ole tarpeeksi tehokkaassa käytössä.

Tämä auttaa myös verkon edelleen kehittämisessä, kun ollaan tarkoin selvillä verkon käyttöasteesta ja resursseista

Loppukäyttäjille tulee kyetä perustelemaan mihin tietoa kerätään, mistä sitä kerätään ja minkälaisissa aikajaksoissa se kootaan. On oltava myös esittää keinot, millä tavalla tietoa analysoidaan ja millaisia mittareita siihen käytetään. Perustelut antavat syyt rajoittaa tiettyjä verkkoresurssien käyttöä, tai kiintiöiden jakamista.

3.1.3 Kokoonpanon hallinta

Modernit tietoliikenneverkot ovat nykyään koottu erinäisistä verkkolaitteista ja loogisista alijärjestelmistä. Verkossa oleva laite ei ole sidottu ainoastaan yhtä tehtävää varten vaan sille voidaan määritellä useampia tehtäviä. esimerkiksi reititin voi reitityksen lisäksi toimia DHCP -palvelimena. Sama fyysinen laite voi olla samanaikaisesti kytkin ja reititin. Kokoonpanon hallinnalla tarkoitetaan verkon alustamista ja verkon hallittua alas tuontia kokonaan tai osiltaan. Myös verkkokomponenttien tilan tarkkailu, uudelleen konfigurointi ja päivittäminen ovat osa kokoonpanon hallintaa.

Kokoonpanon hallintaa tehdään hyvin monella tasolla. Alimmalla tasolla voidaan puhua verkkolaitteiden ajureiden parametrien hallinnasta, kun taas laajimmillaan voidaan puhua, jopa kokonaisten verkkosegmenttien hallinnasta. Kokoonpanon hallinta käsittää myös toimenpiteet, jotka toistuvat usein tai tietyn ajoin, kuten esimerkiksi tiettyjen verkkolaitteiden alasajo.

Kokoonpanon hallinta käsittää myös verkon ja konfiguraatioiden dokumentoinnin sekä raportoinnin. Tähän kuuluu myös asiakkaille ja loppukäyttäjille tehtävät raportit verkon tilasta ja sen muutoksista. Asiakas saattaa haluta tietää ostamansa palvelun käyttöasteen. Tätä tietoa hyväksi käyttäen asiakas saa hyödynnettyä mahdollisimman hyvin palvelunsa tarjoamat resurssit. Esimerkkinä voidaan mainita yritykset, jotka tarjoavat asiakkailleen levytilaa verkossa tai pitävät yllä www-sivuja.

3.1.4 Suorituskyvyn hallinta

Verkossa olevat useat eri komponentin keskustelevat keskenään ja jakavat verkossa olevia resursseja. Suorituskyvyn hallinta kerää ja analysoi tietoa verkon suorituskyvystä. Tietyt resurssit vaativat verkolta, että suorituskyky on riittävällä tasolla toimiakseen. Suorituskyvyn hallinta koostuu kahdesta laajasta toiminnallisuudesta: valvonnasta ja hallinasta. Valvonta on tiedon keräämistä verkosta ja hallinnassa käytetään tätä tietoa hyväksi ja yritetään tehostaa verkon suorituskykyä. Suorituskyvyn hallinnalla on joitain samoja toimintoja kuin edellä mainitulla kokoonpanon hallinnalla, nämä ei kumminkaan sulje toisiaan pois. Tässä hallinta on enemmän verkon hienosäätämistä.

Stalling on listannut viisi kysymystä, jotka liittyvät verkon suorituskykyyn ja sen monitorointiin.

- Mikä on verkon käyttöaste?
- Onko jossain liian paljon liikennettä?
- Onko jossain verkon teho laskenut liian alhaiselle tasolle?
- Onko pullonkauloja?
- Onko vasteaika kasvanut?

Näihin kysymyksiin saa vastauksen, kun tutkii joukkoa verkkolaitteita ja resursseja. Analysoimalla tätä tietoa saadaan tietoa kuinka mikäkin osa verkosta toimii ja opitaan tunnistamaan mahdolliset ongelma-alueet.

3.1.5 Turvallisuuden hallinta

Turvallisuuden hallinta on verkon ja sen laitteiden käytön kontrollointia ja valvontaa, sekä verkonhallintaa varten kerätyn tiedon käsittelyä. Kaikki verkosta kerätty tieto ja lokit ovat osa turvallisuuden hallintaa. Sen takia on tärkeä valvoa, kenellä on pääsy näihin tietoihin. Tässä yhteydessä puhuttaessa turvallisuuden hallinnasta ei ole kyse käyttäjien ja käyttäjäryhmien oikeuksien määrittelystä eri tietojärjestelmissä. Turvallisuuden hallinta on pääsyn rajoittamista ja valvontaa verkon eri laitteisiin ja verkosta saataviin palveluihin.

Turvallisuuden hallinta varmistaa ja parantaa tietojärjestelmien turvallisuutta. Välineet, joita käytetään verkon resurssien ja käyttäjien tiedon turvaamiseen tulee olla ainoastaan pienen valikoidun ryhmän käsissä. Käyttäjien tulee tietää, mitkä ovat heidän oikeudet ja heillä tulee olla luottamus siihen, että verkon turvallisuus on varmistettu.
(Stallings 1993:2-9)

4 SNMP Verkonhallintaprotokolla

SNMP (Simple Network Mangement Protocol) on osa TCP/IP protokolla perhettä ja se on yleisin verkonhallinta protokolla. Suuri osa verkonvalvontaohjelmista käyttää SNMP:tä. SNMP:n suosio perustuu sen yksinkertaiseen rakenteeseen, ja nykyään lähes kaikki lähi- ja etäverkko laitteet tukevat sitä. SNMP on tosin muutama huomattava puute, jotka johtuvat juuri sen yksinkertaisuudesta. Yksi näistä ja varmasti merkittävin puute on turvallisuus. SNMP:ssä ei ole kunnollista autentikointi menetelmää. Tämän takia kehiteltiin työryhmä kehittelemään uutta versiota SNMP:stä, tästä syntyikin SNMPv2. SNMPv2 oli tosin yhtä kehno kuin edeltäjänsä ja tällä hetkellä onkin yleistymässä SNMPv3, jossa on kehittynyt autentikointi ja pääsynvalvonta. Kaikki SNMP versiot ovat taaksepäin yhteensopivia. (Held 2003: 531-532.)

SNMP-protokolla on tarkoitettu verkkolaitteiden hallintaan ja seurantaan. Verkon ylläpitäjä voi muuttaa hallittavan laitteen tilaa esimerkiksi sulkea reitittimestä portin ja seurata millä nopeudella portti toimii tai mikä on laitteen lämpötila. SNMP:llä voidaan hallita myös paljon muutakin kuin reitittimiä, muun muassa unix- ja Windows-koneita, tulostimia sekä virtalähteitä. Käytännössä SNMP:llä voidaan hallita laitteesta riippumatta. mitä tahansa ohjelmaa, missä ajetaan SNMP -ohjelmaa. Verkon etähallittavuuden lisäksi etäseuranta on tärkeä ominaisuus. Suuren verkon kaikkien verkkolaitteiden seuranta yhdeltä koneelta käsin säästää aikaa.
(Essential SNMP 2001:1)

4.1 Komponentit

Yleisellä tasolla verkonhallinta koostuu jokaisessa hallintaprotokollassa samoista peruskomponenteista. SNMP ei eroa näistä. SNMP perustuu palvelin-asiakasmalliin, jossa hallittavat laitteet ovat palvelimia ja hallitsija on asiakas. Palvelinta sanotaan agentiksi (agent) ja asiakasta manageriksi (manager).

4.1.1 Manageri

Manageri hallitsee verkon toimintaa ja sisältää listan hallintatehtävistä. Manageereita kutsutaan usein myös nimellä NMS (Network Management Station). NMS vastaanottaa agenteilta tulleet kyselyiden vastaukset (query) ja hälytykset (traps). NMS kyselee agenteilta heidän (laitteen) tietoja ja päättelee jälkeenpäin onko jotain toimenpiteitä vaativaa tapahtunut. Agentti voi lähettää hälytyksen (trap) NMS:lle, kun jotain muutoksia tapahtuu laitteen toiminnassa. Trap-viesti eli hälytys on agentin lähettämä viesti managerille jostain tapahtumasta. Esimerkkinä managerista voidaan mainita Nagios, johon tutustutaan lähemmin luvussa 5.

Manageri on yleensä raudan ja ohjelmiston yhdistelmä. Varsinkin isoissa verkoissa itse alusta, jolla verkonvalvonta työkalu toimii, tulee olla tarpeeksi tehokas. Erityisesti levytilan määrä ja prosessorin laskentateho ovat tärkeitä asioita ottaa huomioon. (Essential SNMP 2001: 43-44)

4.1.2 Agentti

Agenttia (agent) ajetaan hallittavassa laitteessa, joko erillisenä ohjelmana (esimerkiksi unixissa demonina), tai sulautettuna laitteen omaan käyttöjärjestelmään (Ciscon IOS) tai matalan tason käyttöjärjestelmään, joka hallitsee UPS:ia (UninterruptiblePower Supply). Todellisuudessa laitevalmistajat implementoivat agentteja moniin tuotteisiinsa helpottamaan ylläpitäjien työtä. Agentti toimittaa laitteesta monenlaista tietoa NMS:lle Esimerkiksi agentti pystyy pitämään kirjaa reitittimen porttien tilasta ja NMS pystyy kysymään agentilta yksittäisen portin tilaa. Kun agentti huomaa jotain epäilyttävää toimintaa valvottavassa kohteessa se voi lähettää NMS:lle hälytyksen (trap) ja NMS käsittelee sen. Osa laitteista lähettää ”all clear” hälytyksen (trap), kun poikkeavasta tilanteesta on palauduttu. Myös nämä hälytykset (trap) voivat osoittautua hyödyllisiksi, jos halutaan tietää milloin vika on korjattu/korjaantunut.(Essential SNMP 2001: 4)

4.1.3 Hallintatietokanta

Hallintatietokanta, Management Information Database (MIB) on tietokanta, missä agentti pitää tietoa objekteista, joita agentti valvoo. Objekti on mikä tahansa hallittava kohde, josta ollaan kiinnostuneita Kaikki tieto mikä kertoo managerille objektin tilan tai parametrin arvon on määritelty MIB:ssä. MIB on kuin sanakirja. Hallittavalle objektille tai resurssille annetaan nimi, jonka jälkeen se selittää sen tarkoituksen. Se kuinka hallintatietokanta muodostuu, on määritelty SMI standardin mukaisesti.

Structure of Management Information (SMI) on kehys, joka antaa rajat hallintatietokantojen muodostamiseen. SMI määrittelee tietotyypit joita voidaan käyttää valvottavien objektien ja resurssien kuvaamiseen. (Stalling 1993:78-79)

4.2 SNMP ja UDP

SNMP käyttää viittä eri viestityyppiä keskustellessaan agentin ja managerin välillä:

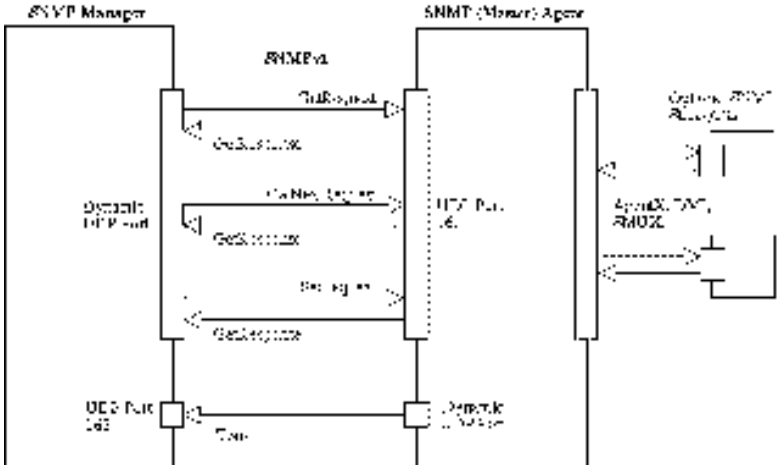
- GET
- GET-NEXT
- GET-RESPONSE
- SET
- TRAP

Manageri lähettää GET tai GET-NEXT viestin saadakseen agentilta haluamansa tiedon. Agentti vastaa GET ja GET-NEXT viesteihin GET-RESPONSE viestillä. Managerin lähettämällä SET viestillä voidaan muuttaa jotain agentin muuttujia, mihin Agentti vastaa GET-RESPONSE viestillä, onko se sallittu. TRAP-viesti eli hälytys on agentin lähettämä viesti managerille jostain tapahtumasta.(Essential SNMP: 28-42)

Tiedonkulku Managerin ja agentin välillä tapahtuu UDP (User Datagram Protocol) tiedonsiirto protokollaa käyttäen. UDP on protokolla, joka toimii kuljetuskerroksessa. Toisin kuin TCP, UDP on yhteydetön ja siitä johtuen epäluotettava protokolla. Palvelin vaan lähettää tietyllä nopeudella UDP -paketteja välittämättä siitä saako kohde pakettia. UDP:n etuna voidaan mainita, että se on palvelimelle kevyempi vaihtoehto, koska palvelimen ei tarvitse kontrolloida pakettien perille menoa. SNMP sovelluksen tehtävä on

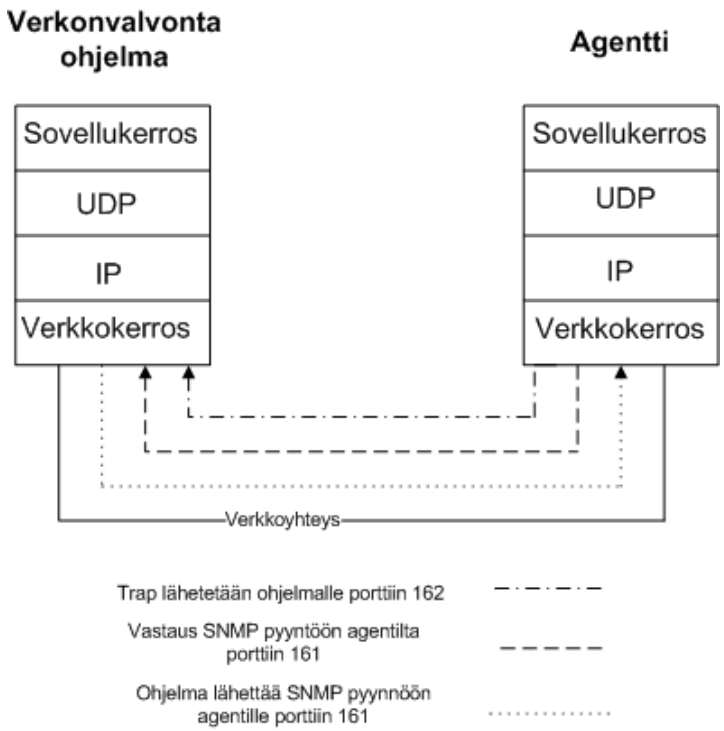
varmistaa paketin perille meno. Yleensä tämä on toteutettu yksinkertaisella aikarajoituksella(timeout). Manageri lähettää UDP pyynnön Agentille ja odottaa vastausta, mikäli vastausta ei kuulu lähettää se pyynnön uudestaan. Se kuinka suuri timeout on, määritellään SNMP konfiguraatio tiedostossa. UDP erottelee kohteet porttinumeroiden perusteella kuten TCP:kin.

SNMP käyttää udp porttia 161 pyyntöjen vastaanottamiseen ja lähettämiseen sekä porttia 162 hallittavien objektien trappien vastaanottamiseen. Hallittavien laitteiden tulee käyttää näitä oletusportteina. Joidenkin laitetoimittajien SNMP agentteja voi muokata ja vaihtaa oletusportteja. Mikäli portteja muuttaa tulee myös Managerin konfiguraatiota muuttaa niin, että se osaa kommunikoida hallittavan objektin kanssa oikeaan porttiin.(Kuvio 1.)



Kuvio 1: SNMP Managerin ja SNMP agentin tiedonvälitys **(**PROTOS Test-Suite: c06-snmpv1)

Tiedonkulku SNMP -toiminnoissa perustuu olemassa olevalle TCP/IP arkkitehtuuriin. Se on useamman tietoverkkoprotokollan yhdistelmä, missä standardisoidut protokollat mahdollistavat kommunikoinnin eri laitealustojen ja käyttöjärjestelmien välillä. Nämä protokollat voidaan kuvata kerrosmallina, missä tieto liikkuu kerrokselta toiselle ja jokaisella kerroksella on tehtävänsä. (Kuvio 2.)



Kuvio 2: Tiedonkulku eri verkkokerroksissa

Joka kerta kun suoritetaan jokin SNMP -toiminto NMS:n ja agentin välillä, kuten pyyntö tai trapin lähettäminen, sen kulku eri verkkokerroksilla on seuraava:

- Sovelluskerros
  Sovelluskerroksella toimii itse SNMP -protokolla. SNMP sovellukset kommunikoivat UDP porttien kautta. Sovelluskerros välittää tietoa myös loppukäyttäjälle valvontaohjelman käyttöliittymän kautta.

- Kuljetuskerros(UDP)
  Kuljetuskerros mahdollistaa eri komponenttien keskustelun. Se on rajapinta verkkosovelluksiin, joihin se kommunikoi porttien kautta. Portit 161 ja 162 ovat SNMP:n käytössä. Kuten aikaisemmin mainittiin, on SNMP:n käyttämä kuljetusprotokolla UDP.

- Internet-kerros(IP)
  IP protokolla on Internet kerroksen ydin. Internet-kerroksessa tietoa välittävät reitittimet, jotka reitittävät paketteja IP -osoitteen perusteella. Itse IP -protokolla

tekee päätöksen siitä lähetetäänkö paketti paikalliseen verkkoon, vai reitittimen kautta ulkoverkkoon.

- Verkkokerros(MAC)
  Viimeinen kerros on verkkokerros. Se on fyysisen verkon, kuten verkkokorttien ja ajurien, ja protokolla kerroksen välinen rajapinta. Verkkokerros tutkii mille protokollalle tiedot annetaan käsiteltäväksi.

(Essential SNMP 2001: 10-14)

5 Nagioksen toteutus Stonesoftin testiverkkoon.

Stonesoftin palomuurin ja IPS (Intrusion Prevent System) tuotteen testaamiseen on rakennettu aikaa myöten testilaboratorio, johon kuuluu useampia verkkoympäristöjä manuaali testaukseen. Testilaboratoriossa on itse palomuurilaitteiden lisäksi suuri määrä erilaisia palvelimia (DNS, DHCP, POP, AD jne.), sekä tietenkin itse verkon aktiivi laitteita, kuten kytkimiä ja reitittimiä. Myös StoneGate tuotteiden hallintaan käytettävät Management Centerit kuuluvat luonnollisena osana testiverkkoon. Manuaalisesti tapahtuvan testauksen lisäksi on olemassa myös automaatti testaukseen (ATF) varatut verkkoympäristöt. ATF ympäristöissä on vielä edellä mainittujen laitteiden lisäksi omat, itse testausta kontrolloivat serverit.

Kun lasketaan kaikki laitteet, joita kuuluu tähän ympäristöön, saadaan kokoon yli sata valvottavaa kohdetta. Näin isoa määrää laitteitta ei pysty enää järkevästi kontrolloimaan ilman valvontajärjestelmää. Tämän takia Stonesoft näki tarpeelliseksi verkonvalvonta järjestelmän kehittämisen testiverkon valvontaan.

Tavoitteena on vähentää verkon valvontaan käytettävää aikaa ja mahdollistaa verkon tehokkaampi käyttö. Valvontajärjestelmällä haluttiin myös mahdollistaa ongelmatilanteiden ennakointi ja reagointiajan antaminen ylläpidolle.

5.1 Verkonvalvontatyökalun valintaan vaikuttavat kriteerit.

Ennen toteutusta tuli valvonnalle ja valvontaa toteuttavalle työkalulle määritellä tarpeisiin sopivat kriteerit. Markkinoilta löytyy, niin Open Source kuin kaupallisiakin ratkaisuja valvonnan tarpeisiin. Tarkoitus oli löytää tuote, joka täytti niin verkonhallinnalle määritetyt vaatimukset ja työnantajan vaatimukset.

Työntilaajan kanssa määrittelimme yhdessä verkonhallinta työkalulle seuraavat kriteerit:

- Hinta
    - Tuotteen tulisi olla mahdollisimman kustannustehokas. Markkinoilla on kattavia järjestelmiä, mutta melko kalliita kun ylläpitokustannukset lasketaan mukaan. Näin ollen Open Source -tuotteet tulisi asettaa etusijalle.

- Tuetut alustat
    - Millä alustalla itse järjestelmä toimii. Tällä hetkellä kaksi mahdollista alustaa olisivat Linux tai Windows.

- Tuetut monitoroitavat alustat
    - Mitkä ovat mahdolliset monitoroitavat alustat. Testiverkosta löytyy niin Windows kuin Linux koneita, sekä niiden päällä pyöriviä erinäisiä palveluita. Ympäristöstä löytyy myös yhä kasvavassa määrin Vmware-palvelimia ja niissä käynnissä olevia virtuaalikoneita ja tietenkin verkon kytkimet ja reitittimet. Verkko infrastruktuuriin kuulu Ciscon, HP:n, Dellin ja Dlinkin laitteita, joten kirjo on hyvin laaja.

- Tarvitaanko monitoroitavalle laitteelle erillinen agentti
    - Koska valvottavien laitteiden määrä on hyvin suuri ja koostuu erilaisista alustoista, niin tulee määritellä mitä itse valvottavalta kohteelta vaaditaan, että sen voi liittää valvovan järjestelmän alle.

- Laajennettavuus ja järjestelmän jatkokehitys
    - Verkko muuttuu koko ajan. Aika ajoin tulee uusia palveluita tai havaitaan, että jotain tiettyä ominaisuutta tulee valvoa. Tällöin tulee tarpeelliseksi voida helposti liittää tämä ominaisuus osaksi valvottavia kohteita. Tämä tarkoittaa sitä, että tuote tulisi olla niin muokattavissa, että siihen pystyisi itse tarvittaessa ohjelmoimaan lisäominaisuuksia.

- Mahdolliset hälytystavat

  - Jos ongelmia ilmenee, mitkä ovat hälytyskeinot, joilla ylläpitoa varoitetaan. Eli onko se ainoastaan käyttöliittymässä näkyvä varoitus vai välitetäänkö se tekstiviestin tai sähköpostin välityksellä verkosta vastaavalle taholle.

- Järjestelmän stabiilius.
  - Jotta verkonvalvonta voitaisiin katsoa lisähyötyä tuottavaksi toiminnaksi, tulisi sen olla luotettava. Järjestelmän stabiilisuteen vaikuttaa ennen kaikkea alusta, johon valvontatyökalu on asennettu ja tietenkin valvovan ohjelman koodista.

- Käyttöönoton kynnys
  - Ohjelman ei tulisi varata mielettömiä määriä resursseja sitä toteutettaessa. Tähän lasketaan niin työtunnit kuin tarvittavat laitteet ja lisenssit.

Tuotteen valinta

Määrittelemämme kriteerit johtivat siihen, että tuote olisi Open Source -pohjainen. Painavimmat syyt tähän olivat lähinnä hinta ja laajennettavuus. Ainoa realistinen vaihtoehto markkinoilla oli Nagios. Nagiosta löytyi tarpeeksi tietoa ja sen laajennettavuus itse ohjelmoitavine plugineineen oli omiaan monimuotoiseen testiympäristöön. Plugin (Plug-in) on laajennus osa Nagioksessa, millä voidaan tuoda eri ominaisuuksia valvonnan piiriin.

Tutkin myös kahta kaupallista tuotetta, OpManageria ja Novel NetEye:tä, mutta niistä ei löytynyt mitään semmoista ominaisuutta joka olisi lisännyt tuotteesta saatavaa hyötyä, suhteessa hintaan. Myös Nagioksen referenssit antoivat vakuuttavan kuvan tuotteesta, joka toimisi testi ympäristössä ja olisi tarpeeksi vakaa.

5.2 Nagios

Nagios on verkonhallintasovellus, joka monitoroi verkkoa ja sen resursseja. Se on alun perin rakennettu toimimaan Linux-alustalla, mutta toimii hyvin useimpien UNIX va-

rianttien alla. Nagios kehitettiin vuonna 1999, jollain tuote julkaistiin nimellä NetSaint. Nimi vaihdettiin tuotemerkkisyistä kumminkin Nagiokseksi vuonna 2002. Nagios on käytössä useissa yrityksissä ja se skaalautuu isoimpienkin organisaatioiden työkaluksi. Suurimmat verkot ja järjestelmät, mitä Nagioksen on raportoitu valvovan, ovat sisältäneet tuhansia eri laitteita tai palveluita.

Nagios on avoimeen lähdekoodiin (Open Source) perustuva tuote, joka perustuu GPL -lisenssiin. Lisenssi takaa käyttäjälle oikeuden kopioida, jakaa edelleen ja muuttaa lähdekoodia. GPL takaa myös, että edellä mainitut vapaudet säilyvät myös koodin tehdyissä muutoksissa. Nagioksen luojana ja pääkehittäjänä tunnetaan Ethan Galstad. Galstadin rinnalla perus Nagios -pluginien kehittäjinä voidaan mainita Ton Voon, Benoit Mortier, Holger Wiess ja Thomas Guyot-Sionnest. Näiden lisäksi avoimen lähdekoodin luonteen vuoksi on kehitystyössä ollut paljon myös ulkopuolista työvoimaa.

Kaikki verkko infrastruktuuriin kuuluvat laitteet ovat Nagioksen valvottavissa, niin kytkimet, reitittimet, työasemat ja palvelimet. Perustasolla Nagios seuraa ICMP- viestein(Internet-Control Message Protocol) laitteen tilaa verkossa. ICMP-viestein valvonta ei kumminkaan täytä nykypäivän verkonvalvonnan vaatimuksia. Tästä syystä Nagioksessa voidaan käyttää SNMP –plugineja, joilla verkkolaitteista saadaan yksityiskohtaistakin tietoa. SNMP on tällä hetkellä tehokkain tapa, valvoa yleisimpiä markkinoilla olevia verkon aktiivilaitteita, kytkimiä ja reitittimiä.

Fyysisten laitteiden lisäksi Nagios valvoo myös verkossa olevia palveluita. Nagios jakaakin verkossa valvottavat kohteet palvelimiin (hosts) ja palveluihin (Services). Nagioksen valvomia palveluita ovat muun muassa: HTTP, SMTP, FTP, POP, SSH, DNS ja Telnet. Listaa voidaan jatkaa loputtomiin, koska Nagioksessa on täysin avoin plugin -tekniikka. Tämä sallii omien palvelu tarkastuksien luonnin ja kehityksen.

Eri palveluiden tarkastuksen lisäksi Nagios valvoo levyn ja muistin kulutusta ja prosessorin kuormaa eli palvelimien resursseja. Nagioksessa voidaan määritellä komentoja, jotka se ajaa tietyn ongelman ilmetessä, esimerkiksi käynnistää palvelun uudelleen. Vikatilojen ilmetessä voidaan määritellä, ketkä saavat ilmoituksen virheistä ja lähetetäänkö ilmoitus sähköpostina vai tekstiviestinä. Nagioksen keräämää tietoa valvottavista kohteista voidaan tutkia www- käyttöliittymän kautta. (Nagios: About nagios)

5.2.1 Kuinka Nagios toimii?

Aluksi määritellään valvonnan kohteet (hosts) eli, fyysiset laitteet. Tämän jälkeen määritellään palvelut(services), joita halutaan Nagioksen valvovan. Kun on määritelty halutut palvelut, resurssit ja laitteet, tulee näille määritellä komennot, jotka tekevät tarkastuksen. Kaikki Nagioksen tekemät tarkastukset(check) tehdään ulkoisten sovellusten, komentojen avulla, jotka sitten Nagioksen ydinprosessi kutsuu. Nagioksessa ajettavat komennot käyttävät plugineja, sovelluksia tai skriptejä, jotka sitten palauttavat laitteen tai palvelun tilan. Jos esimerkiksi valvottava kohde on palvelimen kovalevy, tarkastus palauttaa levyn vapaan tilan prosentteina. Saatua arvoa verrataan määriteltyihin rajaarvoihin ja jos arvot ylittyvät, nagios -prosessi muuttaa palvelun tilaa.

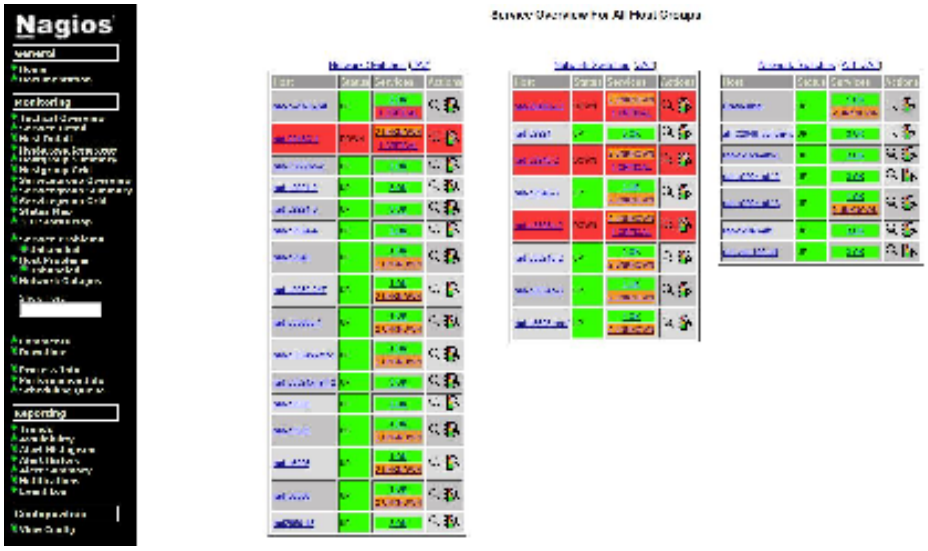
Tilan muutoksesta lähetetään tieto www-käyttöliittymään tai sitten suoraan verkonvalvojan sähköpostiin tai SMS -viestinä puhelimeen. Mikäli tilan muutos edellyttää jonkin komennon suorittamista itse valvottavassa kohteessa, esimerkiksi palvelun uudelleen käynnistämistä. Tämä voidaan toteuttaa automaattisesti myös Nagioksen avulla.

5.2.2 Nagioksen konfigurointi

Nagios serveriä, www-käyttöliittymää ja itse monitorointia ohjataan usealla tiedostolla. Tiedostot sijaisevat /usr/local/nagios/etc hakemiston alla. Konfigurointi tiedostoja on kolmea eri tyyppiä. Ensimmäisenä voidaan mainita *nagios.cfg* ja *cgi.cfg*, joilla määritellään Nagios serverin www-käyttöliittymän ominaisuuksia. Resurssi tiedostot pitävät sisällään arkaluontoista tietoa, toisin sanoen tietoa jota ei haluta näkyvän graafisessa käyttöliittymässä. Tämänlaista tietoa voi olla esimerkiksi tietokanta yhteyksien asetukset. Kolmas konfiguraatio tiedosto tyyppi on objektitiedostot, nämä ovat Nagios konfiguraation sydän. Objekteihin kuuluvat palvelimet, palvelut, työkoneet ja verkkolaitteet, eli kaikki mitä tahdotaan valvoa. Näistä yksityiskohtaisemmin kohdassa Nagioksen käyttöönotto Stonesoftin testiverkkoon. (Turnbull 29-31)

Nagioksen www-käyttöliittymä on valinnainen komponentti. Sitä ei ole pakko käyttää verkon monitoroinnissa.(Kuvio 3.) Yleistä kumminkin on, että monet yritykset käyttävät sitä esittääkseen visuaalista kuvaa verkostaan, laitteistaan ja palveluistaan. Nagiosta

voidaan käyttää myös ilman tätä www-käyttöliittymä jolloin se ainoastaan lähettää haluttuja ilmoituksia ja varotuksia halutun ilmoituskanavan kautta. (Turnbull:113)



Kuvio 3: Valvottavat kytkimet ryhmitelty konehuoneen mukaan www-käyttöliittymässä

5.2.3 Nagioksen käyttöönotto Stonesoftin testiverkkoon

Nagios asennettiin Ubuntu -alustalle, joka oli virtuaalikone ja kytkettynä testiverkon hallintaverkkoon. Asentaminen tapahtui Nagioksen oman dokumentoinnin pohjalta. Ennen Nagioksen asennusta tuli Ubuntuun asentaa Apache, GCC -kääntäjä ja GD -kirjasto. Tämän jälkeen luotiin käyttäjä Nagiokselle ja oma käyttäjäryhmän.

Ensimmäisessä vaiheessa, jota tämä työ koskee, Nagios ainoastaan asennettiin ja lisättiin valvottavat kohteet. Kohteissa käytettiin ainoastaan oletus plugineja, joten kehitys ja valvonnan optimointi jätettiin siten myöhäisempään vaiheeseen.

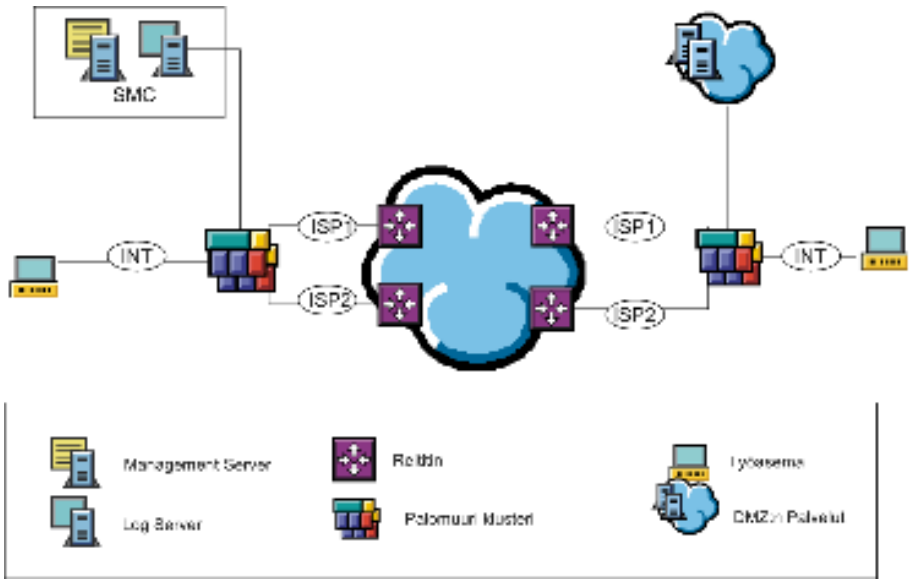
Käyttöönotossa tuli huomioida useita asioita, yksi niistä oli verkossa toimivat palomuurit. Suuriosa valvottavista laitteista olivat kytkettyinä hallintaverkon, mutta osa oli sijoitettuna eri verkkoon, jonka välissä oli palomuuri. Tämä tuli huomioida SNMP sekä muiden protokollien osalta, joita Nagios käyttää verkon valvonnassa. Toisaalta suurin osa valvottavista kohteista on palomuuri koneita, joihin ei välttämättä aina ole asennet-

tuna valvonnan sallivaa politiikkaa. Joten esimerkiksi virheilmoitukset tulisivat suunnitella siten, että tämänkaltaisista tapahtumista ei aiheutuisi turhia hälytyksiä.

5.2.4 Valvottavat kohteet

Kuten aikaisemmin mainitsin, StoneGate tuoteperhe koostuu useammasta komponentista. Yksi toimiva Yksikkö saadaan Management serveristä, missä sijaitsee myös loki serveri. Loki serveri voi olla myös oma fyysinen laitteensa. Yhdessä loki ja management serveri muodostavat StoneGate Management Centerin, SMC:n. SMC:llä hallitaan useampaa erillistä palomuuria tai palomuuri klusteria, joka koostuu useammasta palomuurilaitteesta. Yhteen klusteriin voi kuulua 2-16 yksittäistä palomuuri laitetta.

Yksi kokonaisuus testiverkosta koostuu kahdesta palomuuri klusterista ja niiden takana olevasta sisäverkosta. Klustereiden välillä on useampi verkko, joilla voidaan simuloida useampaa ISP:tä. (Kuvio 4.)



Kuvio 4: Stonesoftin testiverkon perusrakenne

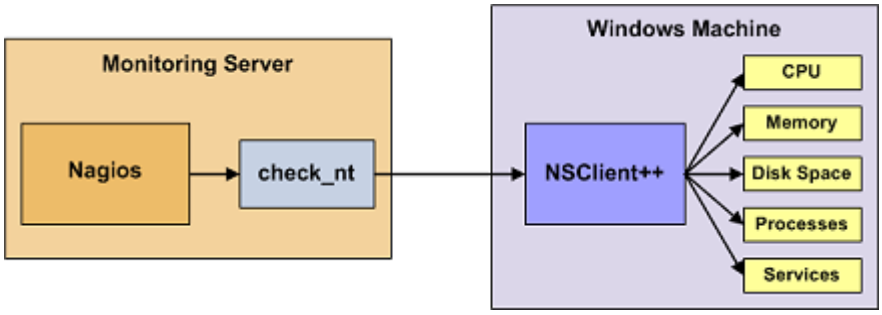
Valvottaville kohteille määriteltiin Nagioksen konfiguraatio tiedostoihin tarkennetut ryhmät (hostgroups), jotta hallinta olisi helpompaa. Ryhmiä oli kaiken kaikkiaan kahdeksan: Network switches 1,2 ja 3, DMZ, SG-managements, Firewalls, SG hosts, Windows Servers.

Network Switches ovat testilaboratorion kytkimet ja ne ovat jaoteltu eri ryhmiin vielä konehuoneiden mukaan. DMZ ryhmään kuuluu DMZ verkkosegmentissä sijaitsevat serverit, joissa on erinäisiä palveluita mm. Active Directory, autentikointipalvelimia ja tiedostopalvelimia. Palomuurien hallinta palvelimet sekä loki serverit kuuluvat ryhmään SG-managements. Palomuurit ovat oma ryhmänsä ja samalla suurin yksittäinen ryhmä, Firewalls. SG-hosts ovat palomuurien takana sijaitsevat operatiiviset työkoneet. Sekä omana viimeisenä loogisena ryhmänä ovat Windows-palvelimet.

5.2.4.1 Windows palvelimet

SMC voidaan asentaa, joko Windows tai Linux alustalle. Verkossa on myös muita palveluita jotka olivat Windows alustalla. Tärkeimpinä näistä voidaan mainita Active Directory ja DNS palvelin. Tämä tietenkin aiheuttaa myös sen, että eri alustat tulee voida liittää valvonnan piiriin. Linuxille riitti olemassa olevat lisäosat, mutta Windows vaati *check_nt* -lisäosan lisäksi vielä erillisen daemonin, NSClienti++:n.

NSClient++ on alun perin juuri Nagiosta varten kehitelty monitorointi lisäosa Windows koneisiin. Se toimii proxyn tapaan nagios *check_nt*-pluginin ja monitoroitavan Windows palvelun välillä (Kuvio 5). NSClient++ on NT palvelu, joka suorittaa tila kyselyitä käyttäen sisäänrakennettuja moduuleita suorituskyky tietojen ja palveluiden tilatiedon kokoamiseen. NsClientissä on mukana kattava valikoima moduuleja, joilla tietoa Windows järjestelmästä voidaan kerätä.



Kuvio 5: Windows resurssien valvonta NsClientin avulla (Nagios: Monitoring Windows Machines)

Jotta voitiin ottaa *check_nt* -plugin käyttöön tuli *nagios.cfg* tiedostoon lisätä rivi, mikä saa Nagioksen huomioimaan myös Windows kohteet. Tämä rivi on valmiina *nagios.cfg* tiedostossa, mutta se on kommentoituna.

cfg_file=/usr/local/nagios/etc/objects/windows.cfg

Tämän jälkeen tuli määritellä kyseiseen Windows-objekti tiedostoon, valvottavat, koneet, palvelut ja resurssit. Windows konfiguraatio tiedostossa aluksi määritellään itse valvottavat kohteet (Kuvio 6). Määritelmä sisältää nimen, IP-osoitteen ja ryhmän mihin kyseinen objekti kuuluu. Alussa oleva *use* -määritelmä kertoo, mitä valmista mallipohjaa käytetään palvelimen monitorointiin. Mallipohjassa määritellään yleiset monitorointiin liittyvät asiat: tarkistusten aikaväli, minä viikonpäivänä tarkistus tehdään ja kuinka ilmoitus viasta tapahtuu ja kenelle (Kuvio 7).

```
define host{
        use                     windows-server
        host_name               sg-win2003srv-1
        alias                   My Windows Server
        address                 192.x.x.x
        hostgroups              DMZ
        }
```

Kuvio 6: Windows-objektin määritelmä

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

Kuvio 7: Mallipohja Windows-objekteille

Lopuksi Windows koneille määriteltiin valvottavat palvelut. Kohteissa valvotaan järjestelmän käynnissä olo aikaa (UPTIME), prosessorin kuormaa (CPULOAD), muistinkäyttöä (MEMUSE), levynkäyttö (USEDDISKSPACE) ja W3SVC palvelun tilaa (SERVICESTATE W3SVC). W3SVC on Windows Servereissä oleva palvelu, jolla luodaan ja hallitaan www-sivuja ja http-palveluita (Kuvio 8).

Nagios käyttää *check_nt* lisäosaa kutsuessaan NSClientilta tila tietoja (Kuvio 5).

```
define service{
        use                     generic-service
        host_name               sg-win2003srv-1,MGMT-5,MGMT-6
        service_description     CPU Load
        check_command           check_nt!CPULOAD!-l 5,80,90
        }
```

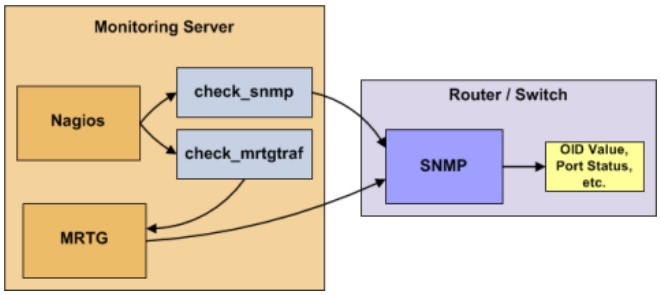
Kuvio 8: Komento valvottavalle palvelulle, jota kutsutaan *check_nt* lisäosan kautta.

5.2.4.2 Verkkolaitteet

Kytkimet ja reitittimet ovat tärkeä osa verkko infrastruktuuria niin myös Stonesoftin testilaboratoriossa. Verkkolaitteiden tilaa on hyvä tutkia, koska niiden hajoaminen aihe-

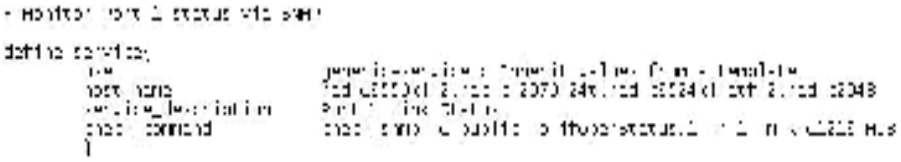
uttaa aina eniten häiriötä ja haittaa verkossa. Kaikki kytkimet, reitittimet ja hubit eivät välttämättä ole hallittavissa, koska niille ei ole hallintaliittymää. Näin ollen ei niille voi määritellä IP -osoitettakaan, jolloin ne jäävät näkymättömiksi verkonvalvonta järjestelmille.

Suurin osa isoimmista kytkimistä ja reitittimistä ovat kuitenkin hallittavissa verkon kautta ja näitä pystytään valvomaan melko yksityiskohtaisestikin, mikäli ne tukevat SNMP -protokollaa. Nagioksessa on olemassa myös MRTG -lisäosa, jolla voidaan tutkia liikennemääriä. Multi Router Traffic Grapher (MRTG) on Perl -kielellä kirjoitettu työkalu, jolla voidaan SNMP:tä hyväksi käyttäen lukea reitittimeltä statistiikka liikennemääristä. SNMP:llä hallittavassa kohteessa tuli olla asennettuna SNMP – agentti, että Nagios pystyi hallitsemaan laitetta (Kuvio 9).



Kuvio 9: Valvonta prosessi SNMP pluginin avulla (Nagios: Monitoring Routers and Switches)

Verkkolaitteita valvottaessa on käytäntö hyvin samanlainen kuin Windows koneiden kanssa. Kaikki kytkimet, joissa on verkkoliityntä ja IP-osoite, voidaan valvoa ainakin lähettämällä ICMP-viestejä (*check_ping*). Tämä kertoo onko laite ylhäällä ja tavoitettavissa. Tämä ei kuitenkaan anna tarpeeksi tarkkaa kuvaa isoista kytkimistä tietoliikenneverkon solmukohdissa. Tämän takia käytetään SNMP hyväksi jolloin voidaan saada yksityiskohtaistakin tietoa verkkolaitteista. Nagioksen *check_snmp* -pluginilla voidaan tarkastella esimerkiksi kytkimien porttien tilaa. Nagioksen konfiguraatio tiedostoon tuli määritellä *check_snmp* komento, joka hakee MIB – tietokannasta (1)portin toiminnallisen tilan (Kuvio 10).



Kuvio 10: Kytkimille tehtävä portin tilan tarkastus *check_snmp* pluginilla

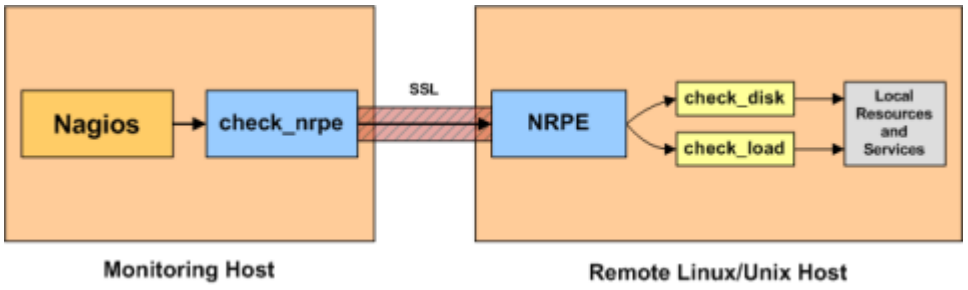
Nagioksen *check_snmp* -plugin käyttää SNMP *snmpget* operaatiota kohteen tila tarkasteluihin. Mikäli *snmpget* operaatio on onnistunut, säilyttää nagios -palvelun tai portin tilan vihreänä. Virheellinen paluuarvo tuottaa tilan muutoksen ja valvottava kohde muuttuu punaiseksi www-käyttöliittymän näkymässä.

5.2.4.3 Linux koneet ja palomuurit

Testiverkossa olevat StoneGate palomuurit, sekä työasemat ovat linux koneita. Linux palvelimien ja työasemien valvontaan käytetään sitä varten kehitettyä NRPE lisäosaa. Tätä lisäosa tarvitaan, mikäli halutaan valvoa etäkoneen sisäisiä palveluita ja resursseja. Julkisia palveluita, kuten SSH, FTP, HTTP, POP3 ja IMAP voidaan valvoa suoraan nagios -pluginien avulla. Esimerkiksi *check_http* tarkastaa etäkoneella http-palvelun tilan. StoneGate palomuureja ei tällä valvota, koska turvallisuus syistä tämän ajaminen palomuureissa olisi mahdotonta.

NRPE (Nagios Remote Plugin Executor) lisäosa koostuu kahdesta osasta. Itse koneella, missä nagios prosessi on käynnissä, on *check_nrpe* –pluginin. Ja jokaisella valvottavalla linux työasemalla on käynnissä NRPE daemon, joka suorittaa *check_nrpe* -pluginin lähettämän kyselyn etäkoneessa. NRPE daemon lähettää tämän jälkeen saadun tuloksen nagios prosessille käsiteltäväksi. Nagioksen *check_nrpe* -pluginin ja NRPE daemonin välinen yhteys voidaan suojata SSL protokollalla, jolloin kyselyt voidaan tehdä myös suojaamattoman verkon kautta (Kuvio 11).

On myös mahdollista suorittaa tarkastukset *check_by_ssh* – pluginin avulla. Tällöin tarkastukset käyttävät SSH -protokollaa, ja suorittavat komennot etänä SSH tunnelin kautta. Tämä kuitenkin vie huomattavasti paljon enemmän prosessori tehoa, sekä etäkoneella, että Nagios serverillä. Tästä aiheutuvat ongelmat tulevat hyvin ilmi kun valvottavia kohteita alkaa olla kymmeniä.



Kuvio 11: ”check_nrpe” –prosessi**,** jolla valvotaan linux koneiden paikallisia palveluita ja resurseja. (Nagios: Monitoring Linux/Unix Machines)

Testiverkon valvottaville linux koneille tuli asentaa sekä nagios -pluginit, että NRPE lisäosa. Etäkoneessa oleva NRPE lisäosa, asennettiin xinetd (Extended Internet Daemon) palvelun alle. Tämä mahdollistaa sen, että NRPE daemon kuuntelee porttia, mihin tulee nagios – pluginin lähettämiä tila kyselyjä. Xinetd on avoimeen lähdekoodiin perustuva ”superserveri”, jolla voidaan hallita verkkoyhteyksiä turvallisemmin.

Tämän lisäksi tuli vielä varmistaa, että koneessa ei olisi palomuuria, joka estäisi kyselyt TCP portiin 5666. Myös */etc/xinetd.d/nrpe* – tiedostoon tuli määritellä, että yhteydet valvovasta Nagios serveristä tuli sallia.(kuvio 12)

Nagios serverille tuli myös asentaa NRPE samalla tavoin kuin etäkoneelle. Plugineja ei tarvinnut asentaa, koska ne ovat asennettu jo aikaisemmin. Tämän lisäksi tuli tehdä *commands.cfg* tiedostoon määrittely NRPE komennoille, jotta voitaisiin käyttää *check_nrpe* – pluginia. Seuraavaksi *host.cfg* tiedostoon tehtiin määrittely, jolla valvottiin palvelua *check_nrpe* komennon kautta. (Kuvio 13)

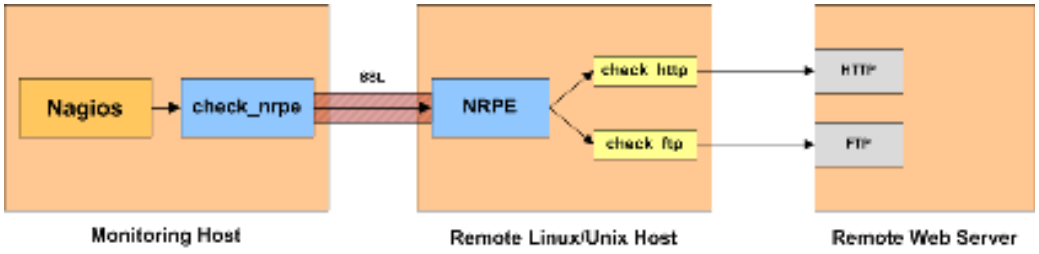
```
# 'check_nrpe' command definition
define command{
    command_name check_nrpe
    command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```

Kuvio 12: ”*Command.cfg*” tiedostoon on lisätty ”*check_nrpe*” komento Linux koneiden valvontaa varten.

```
define service{
    use generic-service
    host_name icecast
    service_description CPU Load
    check_command check_nrpe!check_load
    }
```

Kuvio 13: Palvelu joka tarkastaa etäkoneella prosessorikuorman käyttäen NRPE komentoa ”check_load”.

Perustapauksessa NRPE lisäosa valvoo paikallisesti palveluita, mutta sitä voidaan käyttää myös välillisesti. Tällä tavalla voidaan valvoa laitteitta, joilla ei ole suoraan yhteyttä Nagios serveriin (kuvio 14). Esimerkiksi jos valvottava kohde on verkossa, mihin nagios -prosessilla ei ole yhteyttä. Näin tapahtuu, jos Nagiokselle ei ole määritelty reititystä, tai sitten välissä on palomuuri, joka estää tilakyselyt. Tällöin NRPE, joka on asennettu etäkoneelle voi tehdä välillisesti tarkastuksia koneisiin, joihin sillä on yhteys. Asennettu NRPE toimii ikään kuin välityspalvelimena (proxy), Nagioksen ja tavoittamattomissa olevien koneiden välillä.(*Nagios: NRPE Documentation*)



Kuvio 14. Koneiden valvonta välillisesti NRPE lisäosan avulla.

6 Kehitysnäkymät

Verkonvalvonta järjestelmä on nyt otettu käyttöön, mutta sen resursseista on hyödynnetty vasta murto-osa. Tulevaisuudessa on tarkoitus määritellä tarkasti, mitä palveluita me halutaan valvoa kohde koneissa. Nagioksen hyvä puoli on sen laajennettavuus. Periaatteessa kaikki data mitä pystyy tarkastelemaan itse kohde koneella, pystyy myös monitoroimaan etänä. Erityisen tärkeänä näkisin omalle tuotteelle spesifistisen palveluiden monitorointi. Etenkin SMC:n Management serverin ja Loki servereiden tila. Verkkolaitteista ainoastaan isoimmat kytkimet ja reitittimet ovat tällä hetkellä valvonnan piirissä, mutta mikään ei estä konfiguroimasta myös pienempiä kytkimiä ja reitittimiä valvonnan piiriin.

Nousevana trendinä on näkynyt palvelimien virtuaalisointi. Miten Nagios soveltuu virtuaalipalvelimien valvontaan ja ylläpitoon ja kuinka paljon on mahdollista valvoa itse virtuaalipalvelimien isäntä koneita, esimerkiksi VMware ESX serveriä, joka on ihan oma käyttöjärjestelmänsä. Erityisen tärkeää olisi saada näistä suorituskyky tietoa. Virtuaalipalvelimilla on omat käyttöliittymänsä, joilla valvoa isäntä koneen ja virtuaalikoneiden resursseja. Mutta olisiko mahdollista myös Nagioksella valvoa samoja asioita keskitetysti?

Tärkeä on myös monitorointijärjestelmän ylläpito prosessien järjestäminen ja suunnittelu. Vaikka Nagios hoitaa valvonnan melko itsenäisesti ei se päivitä konfiguraatio tiedostojaan verkkoinfrastruktuuri muuttuessa. Yleensä laitteita tulee lisää ja niitä vaihdetaan uusiin. Vanha konfiguraatio tiedosto ei välttämättä ole sellaisenaan kelvollinen, jos laitevalmistaja muuttuu tai päivitetään sen käyttöjärjestelmä. Olennaisena osana tähän kuuluu myös www-käyttöliittymä, ja sen mukauttaminen sellaiseksi, että sitä on helppo käyttää ja tulkita. Suurin hyöty tästä saadaan silloin, kun viat voidaan nopeasti paikallistaa vain ja ainoastaan paria kuvaa katsomalla. Mielestäni liiallinen yksityiskohtien valvonta vesittää hyvän verkonvalvonta järjestelmän tehokkuuden. Kun vika on paikallistettu, voi sen jälkeen alkaa tutkia ongelmaa tarkemmin. Tärkeintä on, että pystyyttään reagoimaan nopeasti ja haarukoida viallinen komponentti mahdollisimman tarkasti.

Lopuksi tulisi suunnitella tarkoituksen mukainen hälytysjärjestelmä, joka ilmoittasi tietyn kriittisyys tason ylittävät ongelmat suoraan sähköpostiin tietylle ryhmälle ihmisiä. Konehuoneet ovat myös yliherkkiä lämpenemään ja ilmastointilaitteen hajoaminen saattaa olla kohtalokasta monelle koneelle. Ilmastointi laitteen hajoaminen voi tuoda mittavat tappiot, joten tämä on varmasti yksi asia, jota tulisi tutkia vastaisuuden varalle. Olisiko oma laite, joka mittaisi laitehuoneen lämpötilaa vai välillisesti laitteiden lämpötilaa.

7 Käsitteet

SNMP	SNMP (Simple Network Management Protocol) on TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla
TCP/IP	TCP/IP (Transmission Control Protocol / Internet Protocol) on usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä
NMS	(Network Management System) On laitteiston ja ohjelmiston yhdistelmä, jota käytetään verkon valvontaan
MIB	(Management Information base) on SNMP:n määrittämä hallintatietokanta joukolle objekteja.
SMI	(Structure of Management Information) sisältää tiedot kuinka määritellään ja rakennetaan MIB:t.
GPL	(General Public License) Vapaa ohjlemistolisenssi, joka takaa käyttäjälle vapauden muuttaa kopioida ja jakaa ohjelmia ja niiden lähdekoodia.
CGI	Common Gateway Interface on tärkeä Web-ympäristön tekniikka, jonka avulla selain voi välittää dataa palvelimella suoritettavalle ohjelmalle
Plugin	Nagioksen käyttämä lisäosa tarkastusten tekemiseen
NRPE	(Nagios Remote Plugin Executor) Lisäosa jolla voi suorittaa komentoja etänä Linux ja UNIX koneilla.
Xinetd	(Extended Internet Daemon) Linux koneissa ja UNIX järjestelmissä toimiva daemon, jolla hallitaan verkkoyhteyksiä
SSL	(Secure Sockets Layer), on salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli
SMC	(StoneGate Management Center) Keskitetty StoneGate tuotteiden hallinta järjestelmä
ATF	(Automated Test Framework) Automaattinen testaus järjestelmä

UDP	(User Datagram Protocol) on yhteyskäytäntö, jolla sovellus voi lähettää viestejä toiselle tietokoneelle
MAC	MAC (Media Access Control) on IEEE 802-verkoissa (esimerkiksi Ethernet) verkon varaamisen ja itse liikennöinnin hoitava osajärjestelmä
DMZ	Demilitarisoitu alue, joka tarkoittaa fyysistä tai loogista aliverkkoa, joka yhdistää organisaation oman järjestelmän turvattomampaan alueeseen,
IPsec	(IP Security Architecture) on joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia Internet-yhteyksien turvaamiseen.
VPN	(Virtual Private Network) on tapa, jolla kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.
IPS	(Intrusion Prevent System) Tunkeutumisen havainnoiti järjestelmä. Tutkii verkkoliikennettä
UPS	(Uninterruptible Power Supply) on järjestelmä tai laite, jonka tehtävä on taata tasainen virransyöttö lyhyissä katkoksissa ja syöttöjännitteen epätasaisuuksissa.
MRTG	(Multi Router Traffig Grapher) Ohjelmisto, jolla monitoroidaan ja mitataan liikennemääriä.

Lähteet

Kirjallisuuslähteet

Douglas R. Mauro & Kevin J. Schmidt 2001. Essential SNMP. O'Reilly & Associates

Held, Gilbert 2003. Ethernet Networks: design, implementation, operation, management. 4th Edition Chichster: Wiley, cop.

Turnbull James 2006. Pro Nagios 2.0. Apress

Stallings, W 1993. SNMP, SNMPv2 and CMIP: The Practical Guide to Network-Management Standards. Addison-Wesley Publishing Company Inc.

Stonesoft Oyj: Vuosikertomus 2006

Stonesoft Oyj: Vuosikertomus 2007

Internet-lähteet

Hautaniemi, Mika 1994. Diplomityö: TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta [online] [viitattu 5.9.2008]
http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/verkonhallinta.html

Nagios: About nagios [online] [viitattu 12.9.2008]
http://www.nagios.org/about/

Nagios: Monitoring Linux/Unix Machines [online] [viitattu 7.11.2008]
http://nagios.sourceforge.net/docs/3_0/monitoring-linux.html

Nagios: Monitoring Routers and Switches [online] [viitattu 7.10.2008]
http://nagios.sourceforge.net/docs/3_0/monitoring-routers.html

Nagios: Monitoring Windows Machines [online] [viitattu 7.10.2008]
http://nagios.sourceforge.net/docs/3_0/monitoring-windows.html

Nagios:NRPE Documentation [online] [viitattu 10.11.2008]
nagios.sourceforge.net/docs/nrpe/NRPE.pdf

PROTOS Test-Suite: c06-snmpv1 [online] [viitattu 10.11.2008]
http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/