LAUREA

Palvelinkeskusvalvomon toiminnan kehittäminen keskitetyssä valvontaympäristössä

Ramirez, Sebastian

2010 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Palvelinkeskusvalvomon toiminnan kehittäminen keskitetyssä valvontaympäristössä

Sebastian Ramirez
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Huhtikuu, 2010

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Yritysten tietoverkot

Sebastian Ramirez

Palvelinkeskusvalvomon toiminnan kehittäminen keskitetyssä valvontaympäristössä

Vuosi 2010 Sivumäärä 34

Tutkimuksen kohteena olevan yrityksen palvelinkeskuksen valvomo valvoo yrityksen asiakkaiden palvelimia sopimuksen mukaan 24 tuntia vuorokaudessa seitsemänä päivänä viikossa. Keskitetyssä valvonnassa on noin 8500 palvelinta. Hälytykset tulevat keskitetysti valvontaoperaattorin valvontamonitorille. Hälytyksen tullessa valvontaan valvontaoperaattori ryhtyy sovittujen ohjeiden mukaisiin toimenpiteisiin ja tarvittaessa reitittää ongelman selvityksen palvelinkeskuksen valvomossa toimivalle ongelmanratkaisuryhmälle. Keskitetty valvontajärjestelmä on toteutettu kaupallisella BMC PATROL –ohjelmistolla.

Tutkimuskohteena olivat valvontaan tulevat lukuisat aiheettomat hälytykset, jotka eivät vaadi käytännössä mitään toimenpiteitä valvontaoperaattorilta tai ongelmanratkaisuryhmän järjestelmäasiantuntijoilta. Keskitettyyn valvontajärjestelmään liittyvistä ongelmista vastaa normaalisti yrityksessä oma asiantuntijaryhmä. Valvontaongelmien selvittäminen voi kestää kauan, koska selvitystä siirretään usein asiantuntijaryhmältä toiselle. Opinnäytetyön tavoitteena oli selvittää, millaisia ovat yleisimmät aiheettomat hälytykset, ja tuottaa palvelinkeskuksen valvomon ongelmanselvitysryhmälle työohjeistus, jonka avulla ongelmanratkaisuryhmä voi poistaa aiheettomasti hälyttäviä parametreja valvonnasta.

Opinnäytetyössä on käytetty konstruktiivista otetta. Työ on luonteeltaan toimintatutkimus. Tutkimuksessa kuvattiin palvelinkeskuksen valvomon näkökulmasta keskitetyn valvontajärjestelmän toimintaa ja sitä, kuinka ongelmanselvitysprosessi toimii valvontahälytyksissä. Työssä käytiin läpi kahdenlaisia aiheettomia hälytyksiä ja selvitettiin, mistä kyseiset aiheettomat hälytykset johtuivat sekä vastattiin siihen, kuinka ne saadaan korjattua. Lopputuloksena tehtiin toimiva ohjeistus, jolla voidaan poistaa tietynlaisia aiheettomia hälytyksiä sekä poistaa mikä tahansa parametri valvonnasta yksittäiseltä valvonta-agentilta.

Työn lopputulokset ottavat kuitenkin kantaa vain yhden valvonta-agentin toimintaan. Palvelimia, joilta aiheettomia hälytyksiä tulee, on tuhansia, ja yksi palvelin saattaa aiheuttaa monta erilaista aiheetonta hälytystä. Näin ollen tämä työ ei tuonut ratkaisua varsinaiseen valvontaongelmaan, mutta toi lisää keinoja palvelinkeskuksen ongelmanratkaisuryhmälle valvonnan parantamiseksi.

Asiasanat valvonta, palvelin, palvelinkeskus

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Information Technology Programme
Business Information Networks

Sebastian Ramirez

Developing operations of a data centre in a centralized monitoring environment

Year 2010 Pages 34

The monitoring room of Company X's data centre monitors its customers' servers 24 hours a day on every day of the year. There are over 8500 servers in centralized monitoring. All alarms are managed in the monitoring operator's centralized alarm-monitor. When a server is alarming, the monitoring operator reacts to the alarm as agreed with the customer and escalates the problem to the problem solving team of the data centre if necessary. The centralized monitoring system has been implemented with BMC PATROL.

The research problem of this thesis is the fact that there are false alarms coming to the centralized monitoring which require no actions from the monitoring operators or the system specialists of the problem solving team. The centralized monitoring system is administrated by its own team of specialists in the company. Solving monitoring problems can take a long time because problem solving is usually transferred several times between different specialist teams. The main purpose of this research was to produce a work instruction to the problem solving team of the data centre that would offer the methods to independently remove the most common false alarms from the centralized monitoring.

A constructive method of research is used in this thesis. The research is characterized as action research. This thesis introduced the centralized monitoring system from the monitoring room's point of view and described how the problem solving process is executed when an alarm is triggered to the alarm monitor. Two types of the most common false alarms are introduced: how to remove them from monitoring and what causes the false alarms. As a result of the research, a work instruction was produced which gives the methods to remove certain types of false alarms from the monitoring including a universal method to remove any parameter from the centralized monitoring.

The produced work instruction applies only to a single monitoring agent. There are thousands of servers that produce false alarms and there can be several different parameters in one server that are producing them. Consequently, this thesis does not remove the essential monitoring problem but offers new methods to the problem solving team to improve the centralized monitoring.

Key words monitoring, server, data centre

Sisällys

1 Johdanto

Tutkimuksen kohteena olevan yrityksen palvelinkeskuksen valvomo valvoo yrityksen asiakkaiden palvelimia sopimuksen mukaan 24 tuntia vuorokaudessa seitsemänä päivänä viikossa. Palvelimia on yhteensä yli 8000 kappaletta ja niitä valvotaan keskitetysti kaupallisella ohjelmistolla. Suurinta osaa palvelimista valvotaan BMC PATROL –ohjelmistolla, mutta myös muiden valmistajien valvontaohjelmistoja on käytössä. Hälytykset tulevat keskitetysti valvontaoperaattorin valvontamonitorille. Hälytyksen tullessa valvontaan valvontaoperaattori ryhtyy sovittujen ohjeiden mukaisiin toimenpiteisiin ja tarvittaessa reitittää ongelman selvityksen palvelinkeskuksen valvomossa toimivalle ongelmanratkaisuryhmälle. Kaikista hälytyksistä avataan kirjaus yrityksen käyttämään kirjausjärjestelmään, johon kirjataan tehdyt toimenpiteet.

Valvontaan tulee paljon aiheettomia hälytyksiä, jotka eivät vaadi käytännössä mitään toimenpiteitä valvontaoperaattorilta tai ongelmanratkaisuryhmän järjestelmäasiantuntijoilta. Tämä ongelma on ollut tiedossa kohdeyrityksessä jo pidemmän aikaa, mutta muun muassa palvelimien runsauden vuoksi ei kaikkea ole saatu vielä korjattua. Ongelma tuottaa valvomossa jatkuvasti turhaa työtä. Opinnäytetyön tavoitteena oli tuottaa palvelinkeskuksen valvomossa toimivalle ongelmanratkaisuryhmälle työohjeistus, jonka avulla voidaan poistaa aiheettomasti hälyttäviä kohteita valvonnasta.

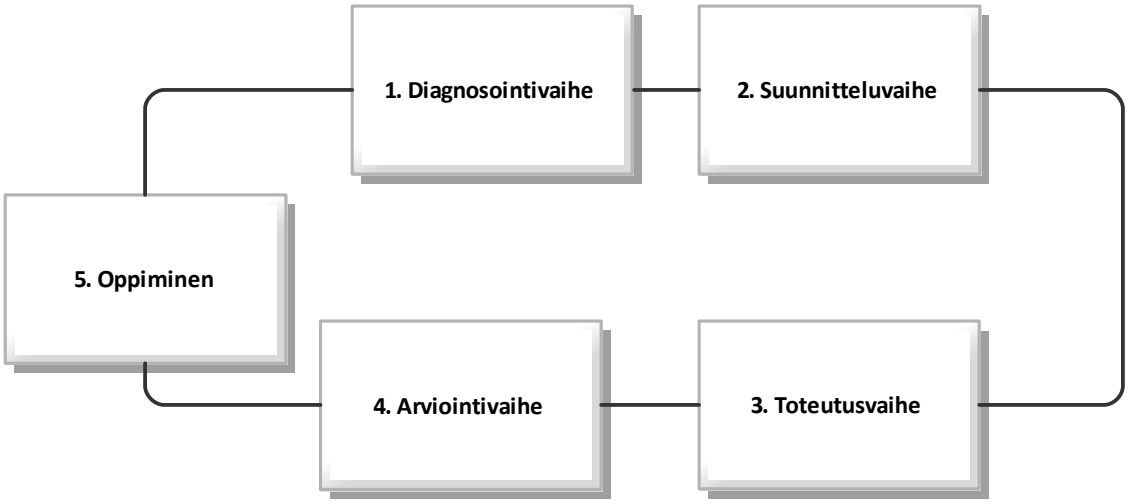
Alustavasti työn tarkoitus oli löytää korjaavat toimenpiteet aiheettomien hälytyksien poistamiselle, mutta työn edetessä tavoitteet tarkentuivat siten, että työ keskittyy valvomon näkökulmasta aiheettomien valvontahälytysten vähentämiseen. Tavoitteeksi asetettiin selvittää, millaisia ovat yleisimmät aiheettomat hälytykset ja tuottaa valvomossa toimivalle ongelmanratkaisuryhmälle työohjeistus, jonka avulla ryhmä voi tarvittaessa itsenäisesti poistaa aiheettomia hälytyksiä aiheuttavat parametrit. Työ rajattiin koskemaan ainoastaan palvelimen käyttöjärjestelmästä tai laitteistosta aiheutuneita turhia hälytyksiä. Lopputuloksena saatiin toimiva ohje, jonka avulla palvelinkeskuksen valvomo pystyy itsenäisesti poistamaan aiheettomasti hälyttäviä valvontakohteita.

Kirjoittaja työskentelee itse palvelinkeskuksen valvomon ongelmanratkaisuryhmässä ja työn toimeksianto on tullut palvelinkeskuksen valvomon ryhmäpäälliköltä. Työn toimeksiantaja toimii myös työn lopputuloksen arvioijana kohdeyrityksen puolelta.

2 Tutkimusmenetelmä

Opinnäytetyössä on käytetty suunnittelutieteellistä eli konstruktiivista otetta. ”Suunnittelutieteen tarkoitus on joko luoda tietämystä suunnittelua ja toteutusta varten, siis konstruktio-ongelmien ratkaisemista varten, tai parantaa nykyisten systeemien suorituskykyä, siis ratkaista parantamisongelmia” (Järvinen & Järvinen 2004, 103). Konstruktiivisessa tutkimuksessa tutkija voi ratkaista käytännön ongelmaa yhteisön johtajan tai käyttäjän kanssa, jolloin ollaan tekemässä toimintatutkimusta (Järvinen & Järvinen 2004, 126).

Työ on luonteeltaan toimintatutkimus, jossa on keskitytty erityisesti toteutusvaiheeseen sekä tuloksien arviointiin. Toimintatutkimuksessa tutkija toimii tutkittavassa kohteessa niin sanottuna muutosagenttina eli osallistuu tutkittavan kohteen toimintaan konsultin roolissa (Järvinen & Järvinen 2004, 128). Keskeisimpiä asioita toimintatutkimuksessa on juuri se, että tutkija toimii ongelmaa koskevien toimijoiden kanssa läheisessä yhteistyössä (Järvinen & Järvinen 2004, 129). Toimintatutkimus voidaan jakaa viiteen eri vaiheeseen, jota toteutetaan tarvittavan monta kertaa syklisenä prosessina (Järvinen & Järvinen 2004, 128). Vaiheet jakautuvat seuraavanlaisesti ja vaiheet suoritetaan alla olevassa järjestyksessä:



Kuvio 1: Toimintatutkimuksen viisi vaihetta (Järvinen & Järvinen 2004, 129)

Diagnosointivaiheessa on tarkoitus tunnistaa ja määrittää tutkittava ongelma. Suunnitteluvaiheessa tarkastellaan eri vaihtoehtoja ongelman ratkaisemiseksi. Toteutusvaiheessa valitaan jokin edellisessä vaiheessa tarkastelluista vaihtoehdoista ja toteutetaan se. Arviointivaiheessa on tarkoitus tutkia toteutuksen seurauksia. Oppimisvaiheessa tarkastellaan yleisiä löydöksiä ja opitaan neljän ensimmäisen vaiheen tuottamista tuloksista. (Järvinen & Järvinen 2004, 129.)

Työn sisältö voidaan jakaa otsikoittain toimintatutkimuksen vaiheisiin seuraavanlaisesti:

1. Diagnosointi
    - Keskitetty valvontajärjestelmä
    - BMC PATROL
    - Ongelmanselvitysprosessi valvomossa
    - Hälytysmäärät
2. Suunnittelu
    - Tutkimusongelma
    - Laitteistovalvonnan sisäiset viestit
    - Sisäisten viestien määrä valvonnassa
    - Windows-palvelut
3. Toteutusvaihe
    - Työohjeistus palvelinkeskuksen valvomon ongelmanselvitysryhmälle
    - Testaus
4. Arviointi- ja oppimisvaihe
    - Yhteenveto

Diagnosointivaiheessa käydään läpi ympäristöä, jossa työskennellään ja kartoitetaan sitä, miten keskitetty valvontajärjestelmä toimii ja kuinka paljon hälytyksiä tulee valvontaan. Suunnitteluvaiheessa lukijalle avataan varsinainen tutkimusongelma: selvitetään mitä ja millaisia aiheettomat hälytykset ovat ja käydään läpi, miten paljon aiheettomia hälytyksiä tulee valvontaan. Toteutusvaiheessa suoritetaan varsinaiset korjaavat toimenpiteet siten, että poistetaan esimerkkipalvelimen valvonnasta aiheettomia hälytyksiä lähettävä parametri ja tuotetaan yleispätevä ohjeistus palvelinkeskuksen valvomoa varten. Arviointi- ja oppimisvaiheessa tarkastellaan lopputuloksia ja käydään läpi tilastoa esimerkkipalvelimen aiheuttamista valvontahälytyksistä korjaavien toimenpiteiden jälkeen. Tässä vaiheessa myös arvioidaan tuotetun ohjeistuksen toimivuus.

3 Tutkimusongelma

Alustavasti työn tarkoitus oli tutkia keskitettyyn valvontajärjestelmään saapuvia aiheettomia hälytyksiä ja löytää korjaavat toimenpiteet niiden poistamiselle. Työ keskittyi ainoastaan Windows-palvelimen käyttöjärjestelmän ja laitteiston valvontaan. Tutkimuksen edetessä huomattiin kuitenkin aiheettomia hälytyksiä aiheuttavia kohteita olevan niin paljon ja niin monella eri palvelimella, että päätimme työn tilaajan kanssa keskittyä vain runsaimmin hälyttäneisiin kohteisiin ja tuottaa yleispätevä ohjeistus palvelinkeskuksen valvomolle näiden hälytysten poistamiseksi valvonnasta. Valvontaan liittyvistä ongelmista vastaavat normaalisti asiantuntijat, jotka vastaavat myös valvontajärjestelmän kehityksestä ja ylläpidosta.

Palvelinkeskuksen valvomossa toimivalle ongelmanratkaisuryhmälle saapuvissa toimeksiannoissa tulee usein vastaan sellaisia tilanteita, joissa huomataan keskitetystä valvontajärjestelmästä tulevan hälytyksen olevan aiheeton. Tällaiset tilanteet aiheuttavat monesti turhaa työtä sekä valvontaoperaattoreille, että ongelmanratkaisuryhmälle. Kun ongelmanratkaisuryhmä todentaa valvontahälytyksen olevan aiheeton ja kyseessä on valvonnallinen ongelma, siirretään valvontaongelman selvitys kyseisen palvelimen tai järjestelmän vastaavalle henkilölle. Hyvin usein kyseessä olevasta palvelimesta tai järjestelmästä vastaava henkilö reitittää ongelman vielä valvontajärjestelmästä vastaavalle asiantuntijaryhmälle, jossa valvontaongelma viimeistään korjataan. Haasteena tässä kuviossa on se, että ongelmanselvityksen reititys eri asiantuntijaryhmältä toiselle hidastaa varsinaisen ongelman ratkaisua. Pahimmassa tapauksessa se merkitsee sitä, että valvontaongelma häiritsee toistuvasti keskitettyä valvontaa, ja aiheuttaa näin jatkuvasti turhaa työtä palvelinkeskuksen valvomossa.

Tutkimusongelmana tässä työssä ovat keskitettyyn valvontajärjestelmään tulevat sellaiset aiheettomat hälytykset, jotka ovat palvelimien toiminnan kannalta epäoleellisia eivätkä aiheuta minkäänlaisia korjaavia toimenpiteitä palvelinkeskuksen valvomossa. Työn tutkimuskysymykset voidaan jaotella seuraavanlaisesti:

Päätutkimuskysymys:

- Onko mahdollista tuottaa valvomolle yleispätevä työohjeistus, jolla voidaan poistaa turhaan hälyttäviä kohteita valvonnasta?

Tukikysymyksiä ovat:

- Minkä tyyppisiä aiheettomat hälytykset ovat?
- Mistä aiheettomat hälytykset johtuvat?
- Miksi ne ovat aiheettomia?

Työn edetessä huomattiin työn toimeksiantajan kanssa, että aiheettomia hälytyksiä oli niin runsaasti ja erilaisia, että päädyimme keskittymään ainoastaan tietynlaisiin aiheettomiin hälytyksiin. Työ on rajattu koskemaan ainoastaan niitä hälytyksiä, jotka ovat Windows-palvelimien käyttöjärjestelmästä tai laitteiston valvonnasta tulleita. Aiheettomien hälytysten tyypit vaihtelevat paljon, sillä palvelimien roolit vaihtelevat niiden käyttötarkoitusten mukaan ja näin ollen myös palvelimelta valvottavat kohteet vaihtelevat. Tästä huolimatta on olemassa tiettyjä asioita, joita on turha valvoa riippumatta palvelimen käyttötarkoituksesta. Tämä työ ottaa kantaa juuri tämänlaisiin aiheettomiin hälytyksiin. Työn tilaaja halusi painottaa erityisesti sitä, että palvelinkeskuksen valvomolle saataisiin tuotettua työohjeistus, jolla voidaan jatkossa poistaa tarvittaessa aiheettomia hälytyksiä, ja joka kasvattaisi samalla ongelmaratkaisuryhmän osaamistasoa valvonta-asioissa.

Työn tilaajan kanssa päätettiin keskittyä kahdenlaisiin hälytystyyppeihin: laitteistovalvonnasta tulleisiin sisäisiin viesteihin sekä Windows-palveluista aiheutuneisiin hälytyksiin. Nämä kaksi tyyppiä valittiin siksi, koska ne aiheuttavat runsaasti aiheettomia hälytyksiä. Tarkoituksena oli siis tutkia, miten nämä hälytykset saadaan poistettua ja dokumentoida siitä työohjeistus. Tämän lisäksi työn tilaaja halusi saada mukaan työohjeistukseen yleispätevän keinon, jolla palvelinkeskuksen valvomo voi tarvittaessa poistaa valvottavia parametreja valvonnasta.

3.1 Laitteistovalvonnan sisäiset viestit

Palvelimien laitteistoa valvotaan PATROL-agenttiin liitettävällä Hardware Sentry –moduulilla, joka kytkeytyy palvelimella olevaan valmistajan omaan laitteistovalvonta-agenttiin ja kerää siltä olennaista tietoa palvelimen laitteiston tilasta. Laitteistovalvonnan toiminta on kuvattu tarkemmin luvussa 4.3. Keskitettyyn valvontajärjestelmään tulee runsaasti hälytyksiä palvelimen laitteistovalvonnasta. Ne käynnistävät joka kerralla luvussa 5. kuvatun ongelmanselvitysprosessin hälytyksen todentamiseksi ja mahdollisien korjaavien toimenpiteiden suorittamiseksi. Esimerkkitilanteessa tällaisen hälytyksen tullessa valvontamonitorille, valvontaoperaattori avaisi siitä kirjauksen yrityksen kirjausjärjestelmään ja mahdollisesti tiedottaisi asiakasta saapuneesta valvontahälytyksestä. Seuraavaksi valvontaoperaattori siirtäisi kirjauksen ongelmanselvitysryhmälle tutkittavaksi. Ongelmanselvitysryhmä todentaisi hälytyksen laitteistovalmistajan omalta valvontakonsolilta ja toimisi tilanteen vaatimalla tavalla. Tämä voisi tarkoittaa esimerkiksi huollon tilaamista paikalle. Mahdollisen huollon jälkeen, kun palvelin on jälleen kunnossa, asiakasta tiedotettaisiin ja hälytyksestä avattu kirjaus suljettaisiin yrityksen kirjausjärjestelmässä.

Yhdenlainen hälytystyyppi laitteistovalvonnasta tulleesta hälytyksestä ovat laitteistovalvontamoduulin sisäiset viestit (Hardware Sentry Internal Message). Nämä viestit näkyvät valvojan valvontamonitorilla hälytyksinä. Viesti sisältää tietoa moduulin tekemistä sisäisistä tehtävistä ja toiminnoista (Sentry Software 2008, 60). Viestit näkyvät valvojan valvontamonitorilla seuraavanlaisessa muodossa:

”<palvelimen nimi> : Hardware Sentry Internal Message: <viesti>”

Viestit ovat ainoastaan tarkoitettu informatiivisiksi viesteiksi tukemaan muuta mahdollista ongelmanselvitystä eivätkä liity varsinaisesti laitteiston ongelmiin (Sentry Software 2008, 60). Moduulin sisäiset viestit näkyvät keskitetyssä valvontajärjestelmässä hälytyksinä siksi, koska moduulin oletusasetuksissa on määritelty, että kaikki moduulin sisäiset viestit rekisteröidään PATROL Event –tapahtumina (Sentry Software 2008, 60). Tämä aiheuttaa sen, että nämä viestit näkyvät hälytyksinä PATROL Event Managerissa, eli keskitetyssä valvontakonsolissa. Mikäli aikaisemmin tässä luvussa mainitussa esimerkkitilanteessa olisi kyse tällaisesta

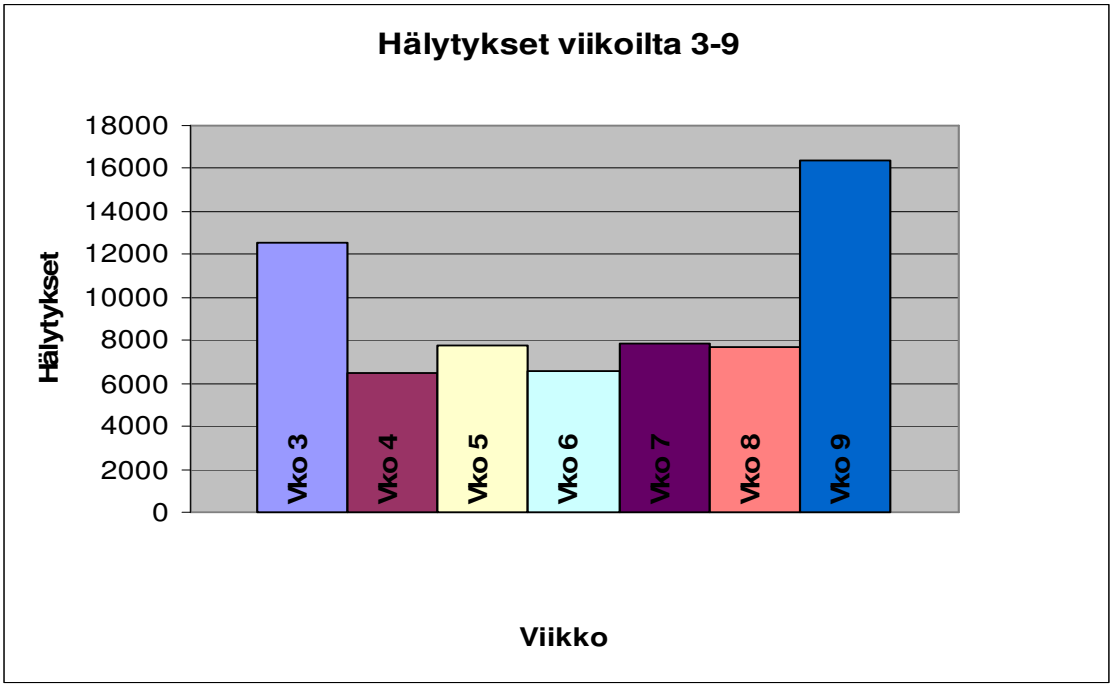
hälytyksestä, joka on laitteistovalvontamoduulin sisäinen viesti, ongelmanselvitysryhmä toteaisi hälytyksen olevan aiheeton, ja hälytyksestä avattu kirjaus suljettaisiin asiakkaalle tiedottamisen jälkeen. Kuitenkin tällainen hälytys käynnistäisi tämän tapahtumaketjun, joka on tällaisessa tilanteessa täysin turhaa työtä.

3.2 Sisäisten viestien määrä valvonnassa

Viestit tulevat hälytyksinä keskitettyyn valvontajärjestelmään ja aiheuttavat näin ollen turhaa työtä valvontaoperaattorille ja ongelmanratkaisuryhmälle. Kuvioissa 2, 3 ja 4 käytetyt luvut käsittelevät ainoastaan kokonaishälytysmääriä sekä laitteistovalvonnan sisäisten viestien osuutta siitä. Kokonaishälytysmäärässä on muitakin hälytystyyppejä, jotka ovat myös aiheettomia, mutta niitä ei ole tämän luvun kuvioissa otettu huomioon.

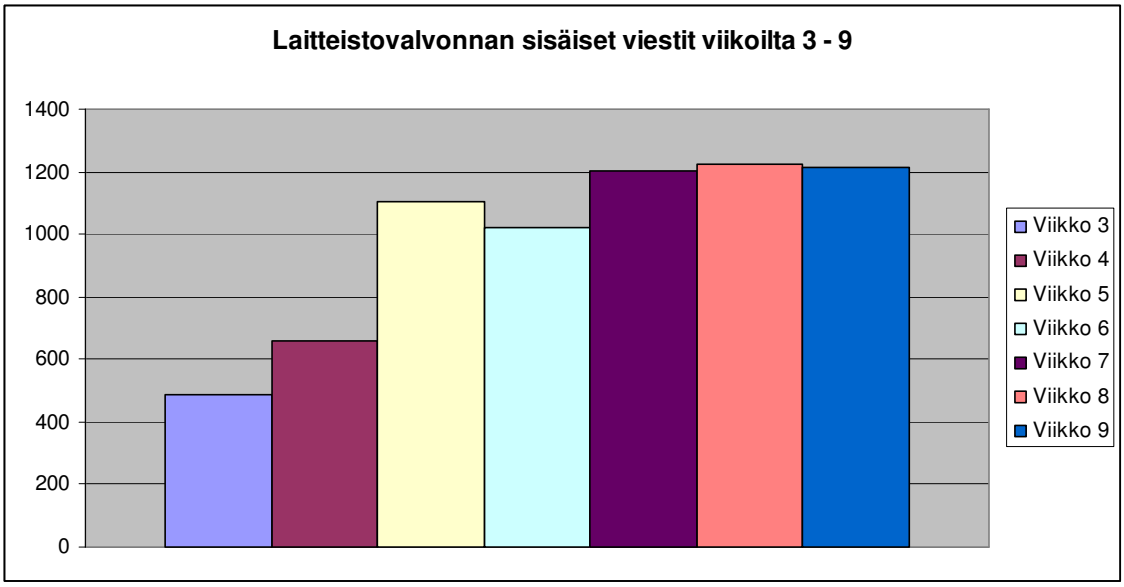
Seurasimme vuoden 2010 alusta lähtien viikkoina 3 – 9 laitteistovalvontamoduulin sisäisten viestien lukumäärää ja vertasimme sitä kokonaishälytysmäärään. Kuvioista voidaan todeta, että laitteistovalvonnan sisäisten viestien määrä voi olla todella suuri kokonaishälytysmäärään nähden. Kuvioon on otettu vähintään 14 minuuttia hälyttäneitä hälytyksiä. Tilastoissa mitataan myös sitä, kuinka monta kertaa sama hälytys on toistunut. Jos sama hälytys toistuu uudestaan, ilman että hälytys kuittaantuu kunnossa olevaksi siinä välissä, kasvattaa se ainoastaan laskurin lukuarvoa, joka osoittaa kuinka monta kertaa kyseinen hälytys on toistunut. Se ei siis näy uutena hälytyksenä valvontamonitorilla, vaan ainoastaan lukumäärä laskurissa kasvaa. Jokaisella hälytyksellä on tätä varten oma kenttä (”Occurrences”) valvontamonitorilla, kun hälytys siihen saapuu. Tämän laskurin lukuarvo näkyy myös kerätyissä tilastoissa, mutta lukuja ei lasketa kokonaishälytysmäärään, koska ne näkyvät valvontamonitorilla vain yhtenä hälytyksenä. Kuitenkin tämä tarkoittaa sitä, että kyseinen hälytys on toistunut niin monta kertaa, kun kyseinen laskuri näyttää.

Hälytyksiä oli yhteensä hieman yli 65000 kappaletta viikoilta 3 – 9. Hälytyksiä tuli eniten viikolla yhdeksän ja vähiten viikolla neljä. Hälytysmäärät olivat viikoilla 4 – 8 tasaisempia, kun taas viikoilla kolme ja yhdeksän olivat lukumäärällisesti suurimmat piikit. Seuraavasta kuviosta (Kuvio 2) voidaan helposti nähdä mitkä viikot olivat kaikista kiireisimpiä hälytysten osalta, ja mitkä rauhallisempia.



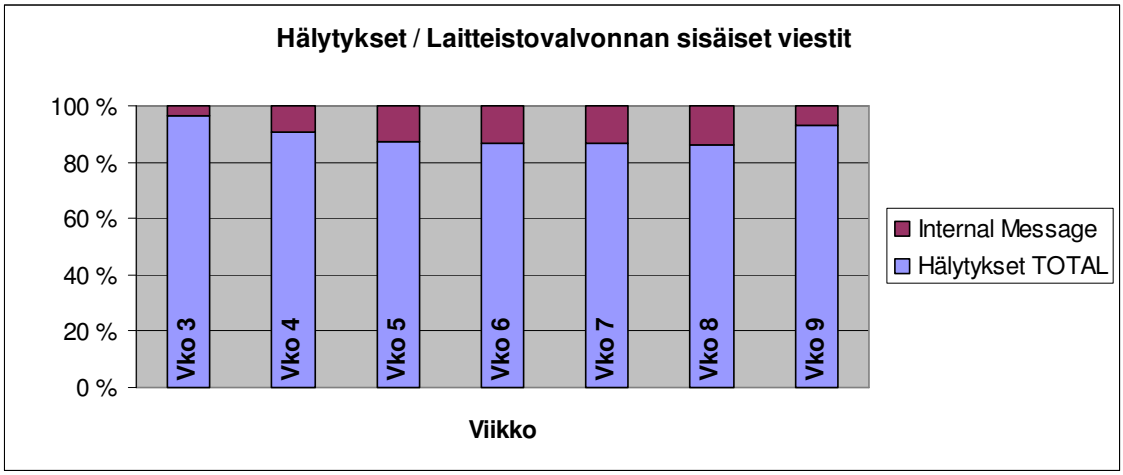
Kuvio 2: Viikkojen 3 – 9 hälytykset

Laitteistovalvonnan sisäisiä viestejä tuli viikoilta 3 – 9 yhteensä noin 6900 kappaletta. Viestit jakaantuivat viikoille tasaisesti, paitsi viikolle kolme ja neljä, jolloin viestejä tuli lukumäärällisesti huomattavasti vähemmän kuin muilla viikoilla. Alla olevasta havainnollistavasta kuviosta voidaan nähdä sisäisten viestien jakautumisen eri viikoille.



Kuvio 3: Viikkojen 3 – 9 aikana hälytyksinä tulleet laitteistovalvonnan sisäiset viestit

Kokonaisuudessaan kaikista hälytyksistä viikoilta 3 – 9 laitteistovalvonnan sisäisten viestien osuus oli noin 10,6 %. Korkeimmillaan sisäisiä viestejä suhteessa viikon kokonaishälytyksiin oli yli 16 %. Alla oleva kuvio havainnollistaa laitteistovalvonnan sisäisten viestien osuuden suhteessa kokonaishälytysmäärään.



Kuvio 4: Otannan hälytykset verrattuna laitteistovalvonnan sisäisiin viesteihin

3.3 Windows-palvelut

Windows-palvelut ovat käyttöjärjestelmässä olevia taustaprosesseja, jotka mahdollistavat sovellusten ajamisen omina istuntoinaan Windowsissa. Palvelut suorittavat itsenäisesti niille määriteltyjä tehtäviä, jotka eivät tarvitse käyttäjän toimia. Palvelut voidaan määrittää käynnistymään automaattisesti koneen käynnistyessä, niitä voidaan pysäyttää ja käynnistää uudelleen eikä palveluilla ole varsinaista käyttöliittymää, kuten perinteisillä ohjelmilla. Palvelu voidaan myös asettaa käynnistymään manuaalisesti, jolloin se käynnistyy silloin, kun sitä tarvitaan. Nämä ominaisuudet mahdollistavat esimerkiksi palvelimella tietyn palvelun pitkäaikaisen toimivuuden ilman käyttäjän toimia. Palveluita voidaan hallinnoida Windows-käyttöjärjestelmässä sisäänrakennetulla työkalulla, jolla voidaan käynnistää ja sammuttaa palveluita, sekä määrittää palvelun käynnistyminen. Yhtenä esimerkkinä palvelusta voidaan mainita Windows Firewall – palvelu, joka on käyttöjärjestelmässä oleva palomuuri. Yksinkertaistettuna palvelun käynnistyessä palomuuri on päällä, ja mikäli palvelu sammutetaan, palomuuri ei ole enää käytössä. (Microsoft 2010a;Wikipedia 2010.)

Windows-palveluita on oleellista valvoa palvelimen toiminnan kannalta. Mikäli jokin kriittinen palvelu sammuu, voi palvelin lopettaa toimintansa ja se ei enää ole käytettävissä. Kaikki kriittiset palvelut palvelimen käytettävyyden kannalta ovat määritelty käynnistymään automaattisesti palvelimen käynnistyessä. Esimerkiksi jos Windows Server 2003 käyttöjärjestelmässä palvelu Terminal Services sammuu, palvelin ei ole enää käytettävissä

Remote Desktop Connection – etäyhteystyökalulla (Microsoft 2008). Tämä voi pahimmassa tapauksessa tarkoittaa sitä, että tekninen asiantuntija saattaa joutua ajamaan satoja kilometrejä tarkistamaan palvelimen tilan.

3.3.1 Windows-palveluiden valvonta

Windows-palveluita valvotaan keskitetysti BMC PATROL – valvontaohjelmistolla. Palveluita varten on oma valvontamoduulinsa (Services), jossa on listattuna kaikki valvottavat palvelut. Valvonta-agentti kerää käyttöjärjestelmältä tietoa palveluiden tilasta ja aiheuttaa hälytyksen, mikäli asetetut raja-arvot ylittyvät. Palveluita valvotaan sillä periaatteella, että kaikki palvelimen ja asiakkaan kannalta olennaiset palvelut, joita pitää valvoa, on määritelty käynnistymään automaattisesti. Mikäli jokin näistä palveluista sammuu, siitä aiheutuu valvontahälytys ja palvelinkeskuksen valvomo reagoi hälytykseen luvussa 5. kerrotulla tavalla.

3.3.2 Windows-palveluiden hälytykset

Windows-palveluista aiheutuvat hälytykset ovat suuri osa keskitettyyn valvontaan tulevista hälytyksistä. Useimmiten Windows-palveluista johtuvat valvontahälytykset ovat täysin aiheellisia, mutta tietyissä tapauksissa valvonnassa hälyttää sellainen Windows-palvelu, jota ei tarvitsisi valvoa. Tämän vuoksi työhön otettiin mukaan myös Windows-palveluiden valvonta, ja työohjeistukseen tuotettiin myös ohjeet siihen, kuinka PATROL valvonnasta saadaan poistettua Windows–palvelu.

Windows-palveluista aiheutuneet hälytykset näkyvät valvontamonitorilla seuraavanlaisina: ”<palvelimen nimi> : ServiceStatus triggered on NT_SERVICES.SERVICE_<palvelun nimi>”. Kyseisessä esimerkkihälytyksessä on ”ServiceStatus” – parametrin raja-arvot ylittyneet, ja se on laukaissut valvonta-agentille määritetyn tehtävän, eli hälytyksen muodostamisen. Esimerkiksi jos palvelimen nimi olisi ”testipalvelin” ja palvelun nimi, joka hälyttäisi, olisi SNMP – palvelu, näyttäisi hälytys seuraavanlaiselta:

”testipalvelin : ServiceStatus triggered on NT_SERVICES.SERVICE_SNMP”

Yksi palvelimen käytettävyyden kannalta epäolennainen Windows-palvelu on Performance logs and Alerts – palvelu. Kyseisellä palvelulla voidaan kerätä tietoa palvelimen toiminnasta ja sillä voidaan kerätä myös tietoa jonkin toisen palvelimen toiminnasta etäisesti. Tälle palvelulle määritetään ajat ja tilanteet, joiden mukaan se rupeaa keräämään tietoa palvelimen toiminnasta johonkin tiettyyn, sille määrättyyn lokitiedostoon. Tämä palvelu käynnistyy siis ainoastaan silloin, jos sitä tarvitaan. (Microsoft 2010b.) Palvelu käynnistyy palvelimen käynnistyessä automaattisesti, ja sammuu, kun sitä ei tarvita. Palvelu on tämän vuoksi suurimman osan ajasta sammuksissa eikä vaikuta palvelimen varsinaiseen toimintaan millään

tavalla. Tämän vuoksi palvelusta aiheutuu usein hälytyksiä, koska palvelimilta valvotaan kaikkia automaattisesti käynnistyviä palveluita.

Toinen esimerkki palvelimen käytettävyyden kannalta epäolennaisesta palvelusta on Common Language Runtime (CLR) Optimization – palvelu. Kyseinen palvelu suorittaa .NET Framework – ohjelmistokomponenttikirjastoon liittyviä tehtäviä, ja kun kyseiset tehtävät on suoritettu, palvelu sammuu (Microsoft 2005;Microsoft 2010c). Palvelu käynnistyy palvelimen käynnistyessä oletuksena automaattisesti, joten tämän vuoksi aiheettomia hälytyksiä tulee keskitettyyn valvontaan, koska palvelu sammuu suoritettuaan tehtävänsä.

Muun muassa edellä mainittujen esimerkkien vuoksi tulimme työn tilaajan kanssa siihen tulokseen, että lisäämme työohjeistukseen kohdan, jossa ohjeistetaan palveluiden poistaminen PATROL valvonnasta, jotta palvelinkeskuksen valvomo voi tarvittaessa omatoimisesti poistaa palveluita valvonnasta.

4 Keskitetty valvontajärjestelmä

Keskitetyssä valvonnassa on noin 8500 palvelinta ja verkkolaitetta. Palvelimista n. 6500 on Windows-palvelimia ja noin 2000 Unix, Solaris-, HP-UX-, Linux-, OpenVMS-, Novell-, AS/400-palvelimia. Noin puolet kaikista palvelimista sijaitsee kohdeyrityksen konesaleissa. Keskitettyä valvontaa valvotaan palvelinkeskuksen valvomossa vuorokauden ympäri, seitsemänä päivänä viikossa ja 365 päivänä vuodessa. Valvontaan tulee hälytyksiä viikossa n. 8000 – 12000 kappaletta, päivätasolla se tekee noin 1000 – 2000 hälytystä. Palvelimien valvonta on toteutettu pääasiassa BMC PATROL – ohjelmistolla.

4.1 Valvonnan periaatteet

Palvelimia valvotaan sillä periaatteella, että palvelimilla pyörivät palvelut ovat käytettävissä sovittuna aikana. Valvonta on tarkoitettu sellaiseksi, että sen avulla voidaan ennaltaehkäistä vakavia, tuotantoon vaikuttavia tai sen estäviä ongelmia. Yksi tällainen ongelma voi olla esimerkiksi palvelimen kovalevytilan täyttyminen. Ongelmatilanteessa valvontaohjelmisto lähettää hälytyksen valvontaoperaattorin valvontamonitorille, jolloin valvontaoperaattori reagoi hälytykseen ohjeistetulla tavalla. Tilanteen vaatiessa valvomossa suoritetaan korjaavat toimenpiteet, joita voi olla esimerkiksi kovalevyn siivoaminen niin, että palvelin pysyy käytettävissä. Jatkotoimenpiteenä tällaisessa tilanteessa voisi olla asiakkaan ja palvelimesta vastaavan henkilön tiedottaminen.

Palvelimissa valvotaan tyypillisesti käyttöjärjestelmän palveluita, prosesseja, prosessorin kuormitusta, muistin käyttöä, levytilojen täyttöastetta sekä tarvittaessa käyttöjärjestelmän tapahtumalokiin tulevia virheitä ja varoituksia. Näiden lisäksi valvotaan myös palvelimen

laitteistoa. Palvelimilla voidaan valvoa myös monia muita asioita, kuten esimerkiksi tietokantoja ja varmistuksia (varmuuskopiointia).

Valvonta toimii niin, että valvottavalle palvelimelle on asennettu ohjelma, jota kutsutaan agentiksi. Agentti valvoo palvelimen resursseja ja sille on määritelty jokaiselle resurssille (parametrille) omat raja-arvot. Mikäli jokin näistä raja-arvoista ylittyy, agentti lähettää siitä viestin hallintapalvelimelle. Lähetetty viesti voi olla hälytys tai varoitus.

4.2 BMC PATROL

Tässä kappaleessa käydään läpi kohdeyrityksen käyttämän BMC PATROL – ohjelmiston eri osat ja tehdään yleiskatselmus siihen, miten valvonta toimii. Ympäristön laajuuden vuoksi työssä on tarkoitus selvittää vain palvelinkeskuksen valvomon näkökulmasta oleellisimmat asiat siitä, miten valvonta toimii.

Kohdeyrityksessä valvonta on toteutettu pääasiassa BMC:n toimittamalla PATROL -ohjelmistolla. Myös muiden valmistajien valvontaohjelmistoja on käytössä, mutta tämä työ ottaa kantaa ainoastaan PATROL – ohjelmistolla suoritettuun valvontaan. Yksinkertaistettuna valvonta toimii siten, että palvelimelle asennettu PATROL-agentti kerää hyödyllistä tietoa palvelimen tilasta ja lähettää hälytyksistä ja varoituksista viestin PATROL Event Manager -konsolille. Agentteja pystytään hallinnoimaan ja valvontatietoa voidaan analysoida PATROL Central Operator -työkalulla, joka on konsolipalvelimen kautta yhteydessä agentteihin.

4.2.1 PATROL Agentti

PATROL-agentti on palvelimella pyörivä yksittäinen prosessi, joka on asennettu kaikkiin palvelimiin, jotka ovat PATROL-valvonnassa. PATROL-agentti valvoo palvelimen resursseja ja tarvittaessa myös palvelimella olevia sovelluksia, ja se toimii itsenäisesti. Kaikki agentin tarvitsemat kokoonpanotiedot, parametrit, raja-arvot, ja tapahtumat ovat tallennettu binääritiedostoon, joka sijaitsee palvelimella PATROL-agentin kansiossa. (BMC software 2003, 2.)

4.2.2 PATROL Knowledge Module (KM)

PATROL-agentilla voidaan valvoa erilaisia kohteita palvelimella. Agentiin voidaan liittää moduuleja, jotka sisältävät tietoa järjestelmästä tai sovelluksesta, jota agentti valvoo ja hallitsee. Tällainen moduuli on eräänlainen kirjasto (Knowledge Module), joka liittää

esimerkiksi laitteiston valvonnan PATROL-agenttiin yhdeksi valvottavaksi kohteeksi ja tarjoaa sille käyttöliittymän, josta voidaan seurata valvottavan kohteen tilaa. Yksittäiset tehtävät moduulin sisällä on tyypillisesti sovellukseen liittyviä rutiineja, käyttöjärjestelmän komentoja ja PATROL:n oman skriptikielen PATROL Scripting Language (PSL) skriptejä.
Agentti kerää jatkuvasti tietoa ja tilastoja moduuleista, ja raja-arvojen ylittyessä suorittaa sille mahdollisesti määrätyt toimenpiteet, kuten esimerkiksi käynnistää palvelun. (BMC Software 2003, 2.)

4.2.3 PATROL Explorer, PATROL Event Manager (PEM)

Palvelinkeskuksen valvomossa työskentelevä valvontaoperaattori käyttää PATROL Explorer -työkalua palvelimien keskitettyyn valvomiseen. Hälytykset näkyvät valvontamonitorilla, josta valvontaoperaattori voi tarvittaessa avata kirjauksen yrityksen käyttämään kirjausjärjestelmään. PATROL Explorer – työkalulla seurataan PATROL Event Manager (PEM) -konsolille saapuvia hälytyksiä ja varoituksia. PEM – konsoli sijaitsee omalla palvelimella, johon PATROL Explorer ottaa yhteyden. PATROL Explorer – työkalu toimii Windows-käyttöjärjestelmässä. PEM – konsoli toimii Solaris-käyttöjärjestelmässä.

Agentit lähettävät viestejä PATROL Event Manageriin, joka kerää tietoa kaikilta valvonnassa olevien palvelimien agenteilta. Mikäli yhteys agenttiin katkeaa, tästä tulee myös viesti (hälytys) PEM - konsolille. Konsolille tulee käytännössä lista agenttien lähettämistä viesteistä, joiden perusteella valvontaoperaattori analysoi tilannetta ja tekee tarvittavat toimenpiteet. PATROL Explorer – työkalulla voidaan poistaa ja sulkea viestejä (varoituksia ja hälytyksiä) ja suorittaa erilaisia toimintoja (BMC Software 2004, 39). Suurinta osaa toiminnoista ei kuitenkaan käytetä valvonnan yksinkertaistamisen vuoksi ja tärkeimmät käytetyt toiminnot valvontaoperaattorille ovat juuri kirjauksen avaaminen hälytyksestä, hälytyksen sulkeminen ja sen poistaminen. Hälytyksen sulkeminen tarkoittaa sitä, että hälytys tai viesti jää valvontamonitorilla näkyviin, mutta merkitään suljetuksi. Poistamisella tarkoitetaan sitä, että viesti tai hälytys poistetaan kokonaan valvontanäkymästä. Jos hälytyksestä tai viestistä avataan kirjaus kirjausjärjestelmään, hälytys merkitään muuten suljetuksi, mutta hälytyksen tiedoista näkee kirjausjärjestelmän tikettinumeron.

4.2.4 PATROL Central Operator

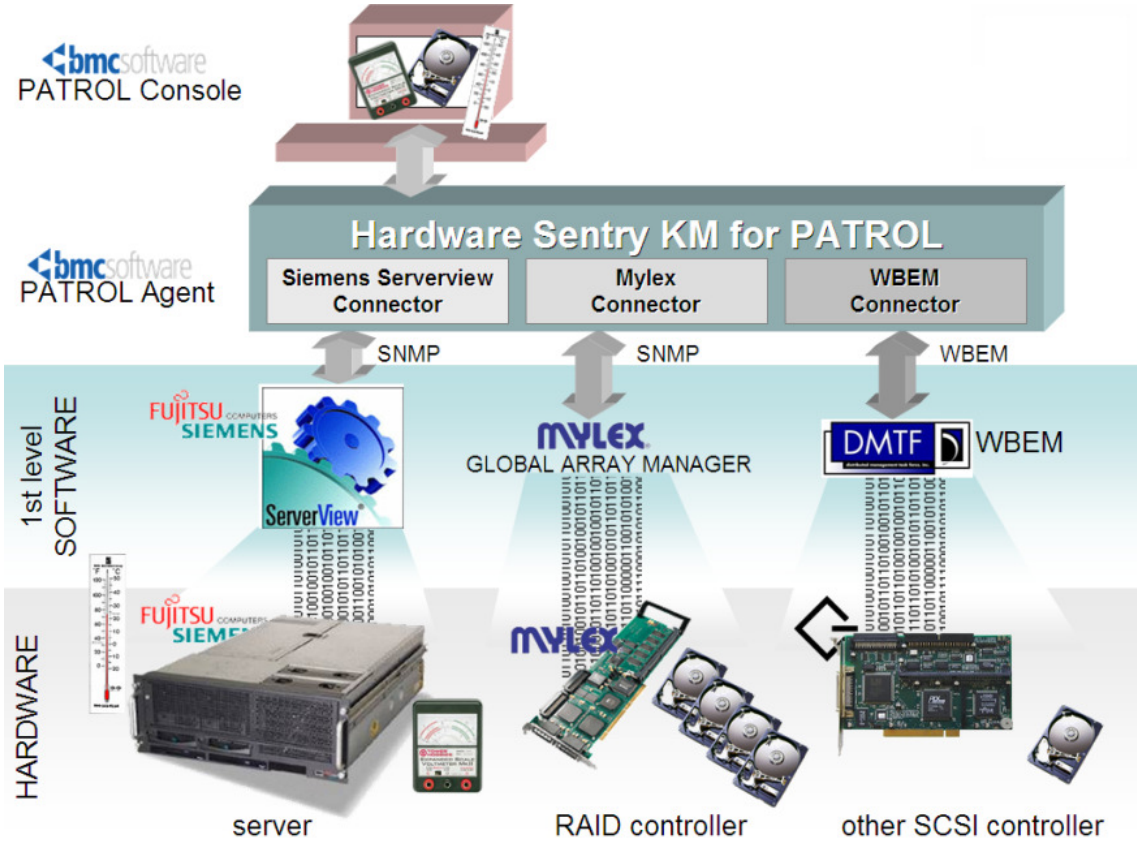
PATROL Central Operatorilla tarkoitetaan konsolia, jolla voidaan hallinnoida valvottavien palvelimien agentteja. Se on graafinen käyttöliittymä, josta näkee graafisessa muodossa valvottavat kohteet. Kaikki tilastot ja tiedot, joita agentti kerää, voidaan nähdä konsolilla

hälytysten, kuvaajien ja raporttien muodossa. Konsolilta käsin voidaan myös hallinnoida agentin raja-arvoja sekä suorittaa komentoja palvelimella.

PATROL Central Operator -konsoli ottaa yhteyden valvottavaan agenttiin siten, että konsoli on yhteydessä RealTimeServer (RTserver)– pilven (RT-pilvi) kautta konsolipalvelimeen, joka keskustelee PATROL-agenttien kanssa edelleen RT-pilven kautta. RT-pilven muodostaa joukko RTserver-palvelimia, jotka puskuroivat agenttien tilatietoja ja keskittävät liikennettä. Esimerkiksi jos PATROL Central Operator – konsoli pyytää tietoja valvottavalta agentilta, pyyntö välittyy RT-pilven kautta konsolipalvelimelle. Jos konsolipalvelimella on pyydetty tieto hallussaan, se lähettää pyydetyn tiedon takaisin PATROL Central Operator – konsolille. Jos konsolipalvelimella ei ole kysyttyä tietoa, pyyntö välitetään jälleen RT-pilven kautta valvottavalle agentille, joka lähettää pyydetyn tiedon takaisin jälleen RT-pilven kautta konsolipalvelimelle ja sieltä takaisin PATROL Central Operator – konsolille. (BMC Software 2004, 30.)

4.3 Laitteiston valvonta

Palvelimien laitteistojen keskitetty valvonta on myös toteutettu PATROL - ohjelmistolla. Agenttiin on liitetty laitteistoa varten Hardware Sentry Knowledge Module –moduuli, joka kerää tietoa laitteiston tilasta. Se on eräänlainen kirjasto, joka kerää tietoa laitteistosta erilaisista lähteistä. Näitä ovat esimerkiksi toimittajakohtaiset agenttiohjelmat palvelimilla, jotka valvovat laitteistoa käyttäen esimerkiksi Simple Network Management Protocol (SNMP) –hallintaprotokollaa (Kuva 1) (Sentry Software 2008a, 9). SNMP-protokolla on sovelluskerroksen verkonhallintaprotokolla, jonka avulla voidaan vaihtaa tilatietoja verkossa olevien laitteiden kanssa. SNMP-trap viestiä käytetään muuttuneen tilan raportointiin hallinta-koneelle (Cisco Systems 2010.) Alla olevasta kuvasta (Kuva 1) voidaan nähdä Hardware Sentryn toimintaperiaate. Esimerkissä olevassa kokoonpanossa Server View – agentti näyttää lämpötilat, tuulettimien tilan, virtalähteet sekä jännitteet palvelimella hyödyntäen SNMP-protokollaa. Levyohjaimen ohjelmisto (Mylex) näyttää fyysisten ja loogisten RAID (Redundant Array of Independent Disks)-levyjen tilan myös SNMP-protokollaa hyödyntäen. Windowsin WMI (Windows Management Instrumentation) näyttää SCSI - ohjaimeen kytkettyjen levyjen tilan WBEM:n (Web-based Enterprise Management) kautta. Hardware Sentry –moduuli kytkeytyy kaikkiin näihin tietolähteisiin. (Sentry Software 2008a, 9.).



Kuva 1: Hardware Sentry -moduulin toimintaperiaate (Sentry Software 2008a, 9)

Hardware Sentry tukee useita eri laitevalmistajia ja malleja. Palvelimilta valvotaan tyypillisesti (Kuva 2):

Kriittisistä laitteista:

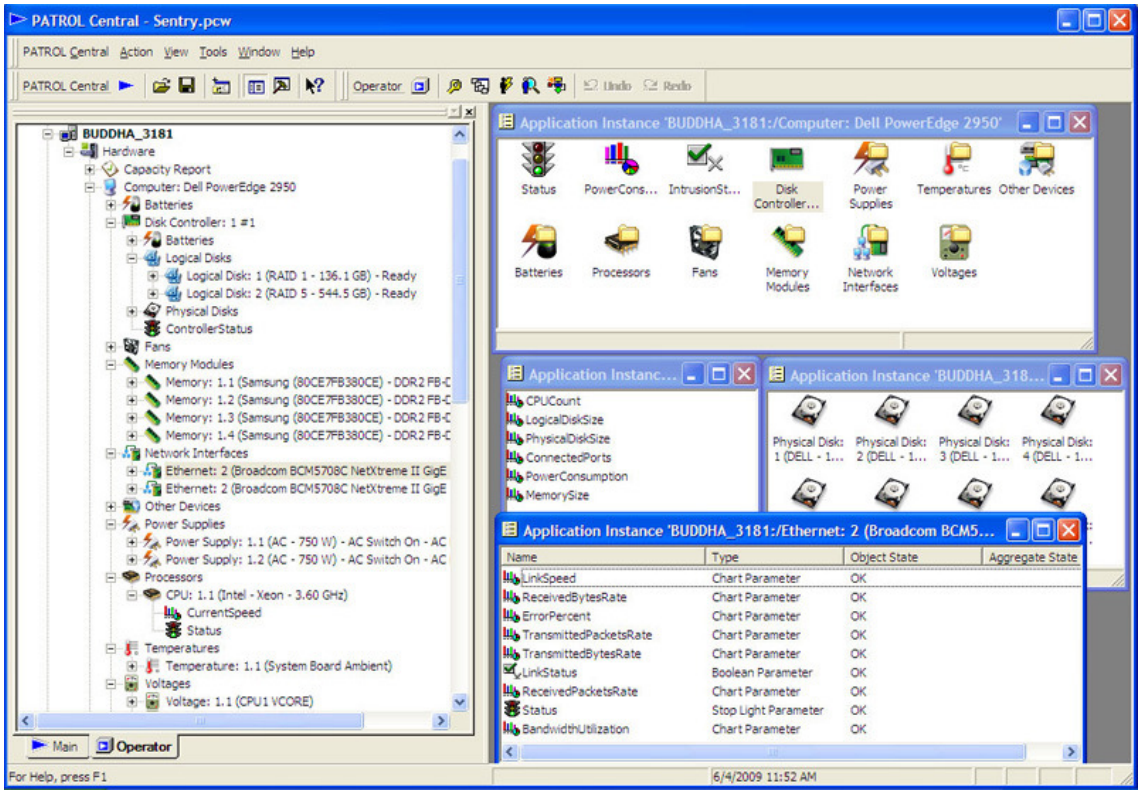
- Prosessoreita
- Muistimoduuleja
- Verkkokortteja
- Virtalähteitä

Sensoreista:

- Jännitteitä
- Lämpötiloja
- Tuulettimia

Tallennusmedioista:

- Levyjä
- RAID
- SCSI-ohjaimia
- ATA/IDE - ohjaimia



Kuva 2: Agentin Hardware Sentry näkymä PATROL konsolilla (Sentry Software 2008b)

Käynnistyessään Hardware Sentry suorittaa kolme vaihetta. Ensimmäisenä Hardware Sentry testaa jokaisen liitännän (Connector) selvittääkseen, mitä tietolähteitä on saatavilla. Tätä vaihetta kutsutaan kytkentävaiheeksi (Detection process). Kytkentävaiheen jälkeen Hardware Sentry yrittää hahmottaa laitteistoympäristöä lähettämällä kyselyitä näihin löydettyihin tietolähteisiin. Tätä vaihetta kutsutaan löytövaiheeksi (Discovery process). Lopuksi, kun kytkentävaihe ja löytövaihe on suoritettu, Hardware Sentry alkaa kerätä tietoa löydetystä laitteistoympäristöstä, kuten esimerkiksi laitteiston tila, lämpötila, jännitteet jne. Tätä vaihetta kutsutaan keräysvaiheeksi (Collection Process). Tämän jälkeen Hardware Sentry on kokonaan ladattu ja se jatkaa tietojen keräystä tietyin väliajoin. (Sentry Software 2008a, 16.)

4.3.1 Liitännät

Jokainen liitäntä (connector) on ”.hdf” – tiedosto PATROL-kansiossa palvelimella, joka on osoitettu tietylle laitteistotietolähteelle. Jokaisen hdf-tiedoston tarkoitus on kertoa Hardware Sentrylle, kuinka sen on tarkoitus ottaa yhteys kyseiseen tietolähteeseen ja mitkä tiedot ovat saatavilla kyseisestä lähteestä. Esimerkiksi ”MS_HW_Director41NT.hdf” – tiedosto ”neuvoo” Hardware Sentryä kuinka saada tietoa IBM Director 4.1 agentilta ja miten valvoa IBM:n xSeries –sarjan palvelimen laitteistoa. (Sentry Software 2008a, 17.)

4.3.2 Laitteistovalvonnan hälytykset

Laitteiston valvontahälytyksiin reagoidaan siten, että hälytyksen tullessa keskitettyyn valvontaan (PEM-konsoli), hälytykset tulee vielä todentaa ennen kuin ruvetaan varsinaisiin korjaaviin toimenpiteisiin. Tämä todentaminen tapahtuu usein tarkistamalla hälytys kohdepalvelimen laitteistovalvonnan konsolilta joko menemällä fyysisesti paikalle tai etäyhteyksien avulla. Mikäli asiakkaan ympäristössä on keskitetty laitteistovalvontakonsoli, voidaan todentaminen tehdä sitä kautta. Lähes kaikissa tapauksissa keskitettyä laitteistovalvontakonsolia ei ole, vaan hälytykset pitää todentaa kohdepalvelimelta erikseen (Kuva 3). Varsinainen ongelmanselvitysprosessi palvelinkeskuksen valvomossa käydään läpi myöhemmin tässä työssä. Alla olevasta kuvasta (Kuva 3) nähdään palvelimen oma web-pohjainen laitteistovalvontanäkymä, palvelimen valmistajana Dell.

Kuva 3: Web-pohjainen valvontakonsoli palvelimella (Dell 2009)

5 Ongelmanselvitysprosessi palvelinkeskuksen valvomossa

Tässä kappaleessa kerrotaan pääasiat palvelinkeskuksen valvomosta, sen yleisestä toiminnasta ja kuinka ongelmanselvitysprosessi toimii valvomon sisällä hälytyksen tullessa valvontamonitorille.

5.1 Taustaa

Palvelinkeskuksen valvomossa työskentelee 40 henkilöä, joista kymmenen henkilöä työskentelee valvontaoperaattoreina ja kymmenen henkilöä ongelmanselvityksessä. Valvomossa työskentelee myös 20 muuta ihmistä, jotka tekevät operointia ja ottavat vastaan toimeksiantoja arkipäivisin.

Asiakkaita palvelun piirissä on noin 500 ja palvelimia yli 8500 kappaletta. Valvonnassa on myös tietoliikenneverkkoja, jotka näkyvät keskitetyssä valvonnassa. Toimeksiantoja valvomoon tulee noin 15 000 kappaletta kuukaudessa eri kanavia pitkin.

Valvomossa tehdään katkeamatonta kolmivuorotyötä 24 tuntia vuorokaudessa 365 päivänä vuodessa. Valvonnassa ja ongelmanselvityksessä työskentelee samanaikaisesti neljä ihmistä: kaksi valvontaoperaattoria ja kaksi järjestelmäasiantuntijaa.

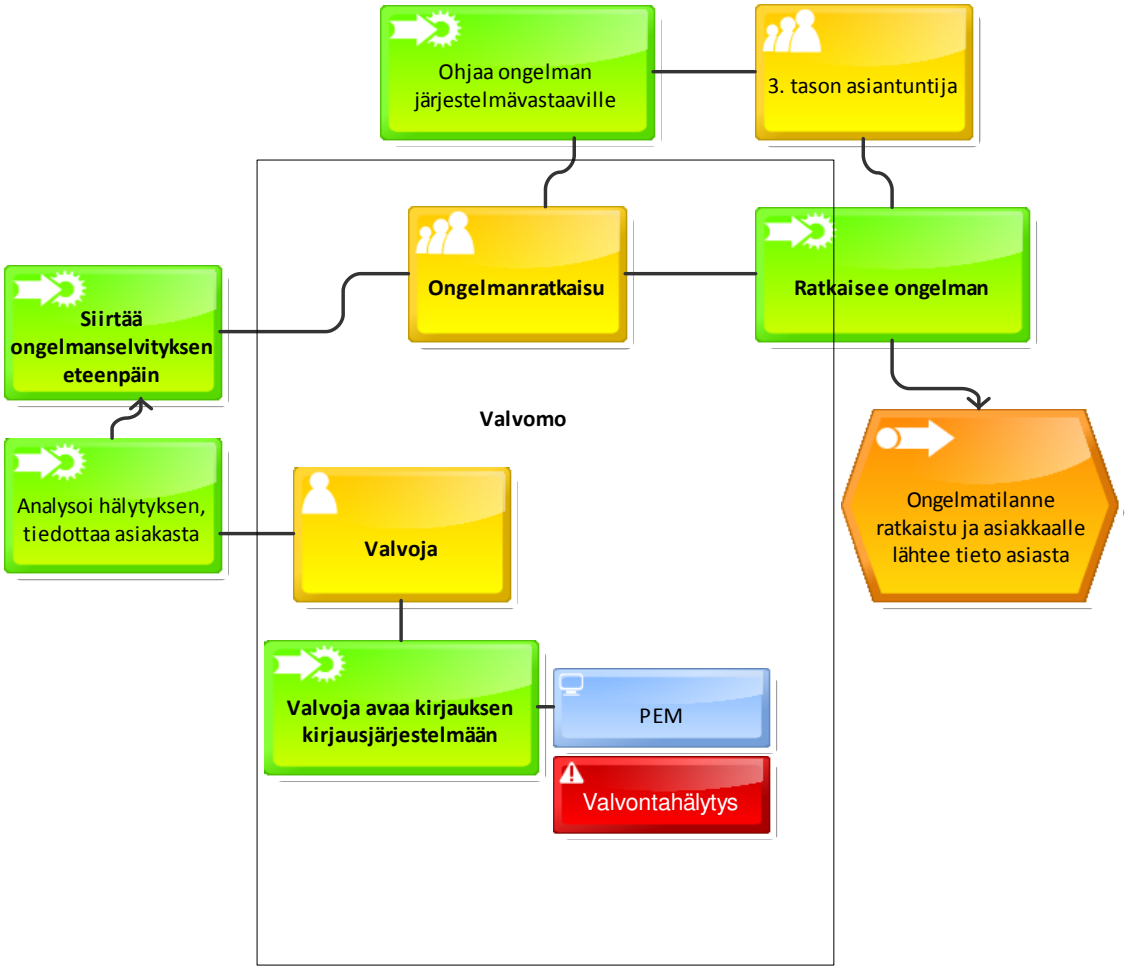
Valvomon toiminta perustuu olemassa oleviin ohjeisiin, joita varten kohdeyrityksellä on järjestelmätietokanta. Tietokannasta löytyy jokaisen tuotannossa olevan palvelimen tiedot ja siihen liittyvät erityiset työohjeet, joita tulee noudattaa mahdollisissa ongelmatilanteissa. Tietokannasta löytyy myös asiakkaan kanssa sovitut tiedotuskäytännöt, joiden mukaisesti valvomo tiedottaa asiakkaalle ongelmatilanteista.

5.2 Ongelmanselvitysprosessi

Ongelmanselvitysprosessi alkaa käytännössä siitä, kun valvontahälytys saapuu keskitettyyn valvontakonsoliin. Valvontaoperaattori analysoi hälytyksen perusteella hälytyksen kriittisyyden ja reagoi siihen sovitussa vasteajassa. Ensimmäinen toimenpide, jonka valvontaoperaattori tekee, on kirjauksen avaaminen hälytyksestä yrityksen kirjausjärjestelmään. Tähän kirjaukseen kirjataan kaikki toimenpiteet, mitä on tehty ongelmatilanteen selvittämiseksi.

Valvontaoperaattorin seuraava askel ongelmanselvityksessä on asiakkaan mahdollinen tiedottaminen valvontaan tulleesta hälytyksestä ja hälytyksestä riippuen siirtää ongelmanselvitys valvomossa toimivalle ongelmanratkaisuryhmälle. Tämä tapahtuu siten, että valvontaoperaattori siirtää kirjausjärjestelmässä olevan kirjauksen ongelmanselvitysryhmän työjonoon, jota ryhmä lukee reaaliajassa.

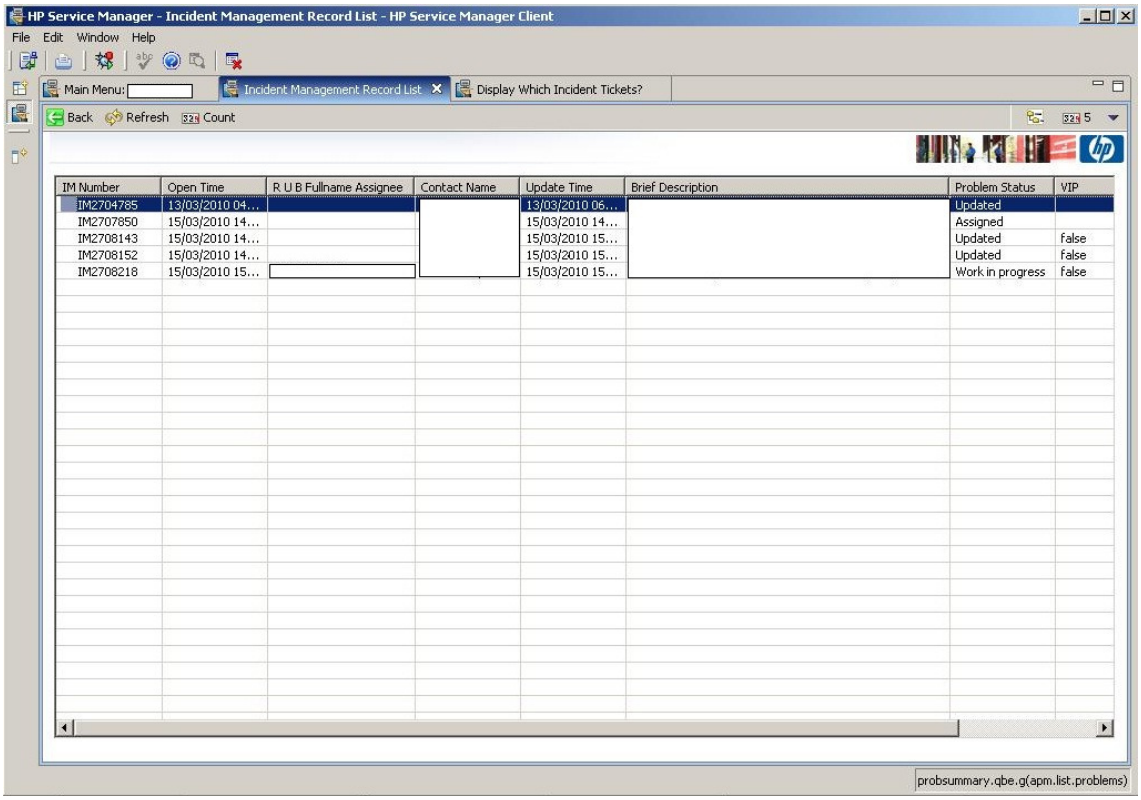
Ongelmanratkaisuryhmä tutkii ja analysoi ongelman ja tekee järjestelmätietokannassa olevien ohjeiden mukaiset toimenpiteet, jos niitä palvelimen työohjeissa on. Mikäli ongelmanratkaisuryhmä ratkaisee ongelmatilanteen, siitä lähetetään asiakkaalle lopputiedote ja hälytyksestä avattu kirjaus suljetaan kirjausjärjestelmässä.
Mikäli ongelma ei selviä ongelmanratkaisuryhmässä, ongelmatilanne voidaan siirtää kyseisen palvelimen tai ongelmakohteena olevan järjestelmän vastaavalle henkilölle tai ryhmälle, jossa ongelma viimeistään selvitetään. Ongelmanratkaisuryhmä ei ota kantaa tietoliikenneongelmiin, vaan niitä varten on kohdeyrityksessä oma ryhmänsä ja asiantuntijansa.



Kuvio 5: Ongelmanselvitysprosessin kulku palvelinkeskuksen valvomossa

5.3 Kirjausjärjestelmä

Kohdeyrityksessä käytetään Hewlett Packardin valmistamaa Service Manager 7 -kirjausjärjestelmää. Järjestelmään kirjataan kaikki toimeksiannot, mitä palvelinkeskuksen valvomossa tehdään asiakkaille. Kirjausjärjestelmä toimii samalla tietynlaisena ratkaisutietokantana, josta voidaan etsiä vanhoja kirjauksia ja niiden ratkaisuja. Palvelinkeskuksen valvomossa toimivilla eri ryhmillä on jokaisella omat työjononsa, jota kukin ryhmä lukee sovitun mukaisesti. Suljetuista kirjauksista lähtee asiakkaalle kohtaamiskysely, jossa asiakas voi arvioida palvelupyynnön suorituksen. Alla olevasta kuvasta nähdään ongelmanratkaisuryhmän työjonon näkymä.



Kuva 4: Service Manager 7 kirjausjärjestelmä

6 Hälytysmäärät

Tässä luvussa kerrotaan palvelinkeskuksen valvomon keskitettyyn valvontajärjestelmään tulevista hälytysmääristä, jotta lukija saa kuvan niiden laajuudesta. Tilastot ovat oikeita lukuja todellisista hälytysmääristä ja hälytykset on esitetty työssä kalenterivuosittain. Kohdeyrityksessä tilastot koostetaan tilikausittain. Hälytyksistä kerätään viikoittain oma tilastonsa, josta muodostuu koko vuoden tai tilikauden tilasto. Hälytysmääristä tilastoja on kerätty kunnolla vuodesta 2007 lähtien. Tähän työhön on otettu vuosien 2008 ja 2009 tilastot hälytysmääristä, jotta lukija saa vertailukelpoisen kuvan hälytysmäärien kasvusta. Tilastoissa on otettu huomioon sekä palvelimien, että verkkolaitteiden tuottamat valvontahälytykset, jotka ovat hälyttäneet vähintään 0 – 14 minuuttia.

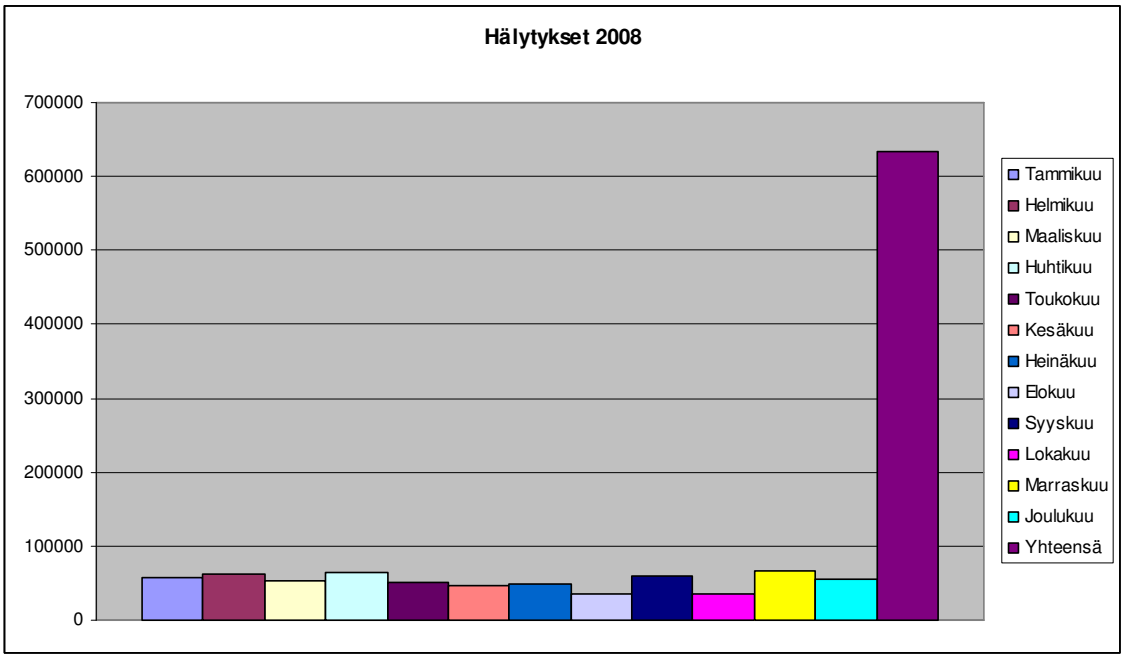
Palvelinkeskuksen keskitetyssä valvonnassa on noin 8500 palvelinta. Käytössä on useita eri käyttöjärjestelmiä: noin 6500 Windows-palvelinta ja noin 2000 Unix-, Solaris 10-, HP-UX-, Linux-, OpenVMS-, Novell-, AS/400-palvelinta. Noin puolet palvelimista sijaitsee kohdeyrityksen konesaleissa. Loput palvelimista ovat joko asiakkaan omissa tiloissa tai jonkin kolmannen osapuolen konesaleissa. Tietoliikenneverkkoja on valvonnassa noin 80 kappaletta, joissa on noin 15 000 verkon aktiivikomponenttia.

Palvelinkeskuksen valvomoon tulee toimeksiantoja keskimäärin noin 15000 kappaletta eri kanavia pitkin. Hälytyksiä keskitettyyn valvontajärjestelmään tulee vaihteleva määrä riippuen siitä, onko palvelimilla meneillään esimerkiksi huoltotöitä tai jotain muita hallittuja (tai hallitsemattomia) toimenpiteitä. Keskitettyyn valvontajärjestelmään saapuneista hälytyksistä kerätään viikoittain tilastoa, josta nähdään hälytyksien määrä, hälyttäneet palvelimet sekä hälytykset kokonaisuudessaan. Vuoden kuluessa kaikista keskitettyyn valvontajärjestelmään saapuneista hälytyksistä kootaan myös koko vuoden tilasto raportointia varten.

Hälytysmäärät ovat olleet jatkuvassa kasvussa. Myös palvelimien määrä on jatkuvassa kasvussa. Tammikuussa vuonna 2008 palvelimia oli keskitetyssä valvonnassa noin 7000. Alla olevasta taulukosta nähdään hälytysmäärät vuodelta 2008 eri kuukausilta. Havainnollistavasta kuvaajasta voidaan nähdä, että hälytysmäärät voivat vaihdella hyvin paljon eri kuukausina. Syitä vaihteluihin voi olla esimerkiksi tietoliikenneverkon huoltotyöt tai palvelimien huoltotyöt. Hälytyksiä oli vuonna 2008 yhteensä yli 600 000 kappaletta.

Taulukko 1: Valvontahälytykset eri kuukausilta vuonna 2008.

Valvontahälytykset / kuukausi	Vuosi 2008
Tammikuu	58670
Helmikuu	62250
Maaliskuu	53157
Huhtikuu	63481
Toukokuu	51216
Kesäkuu	45807
Heinäkuu	47931
Elokuu	34856
Syyskuu	59720
Lokakuu	36226
Marraskuu	65796
Joulukuu	54488
Yhteensä	633598

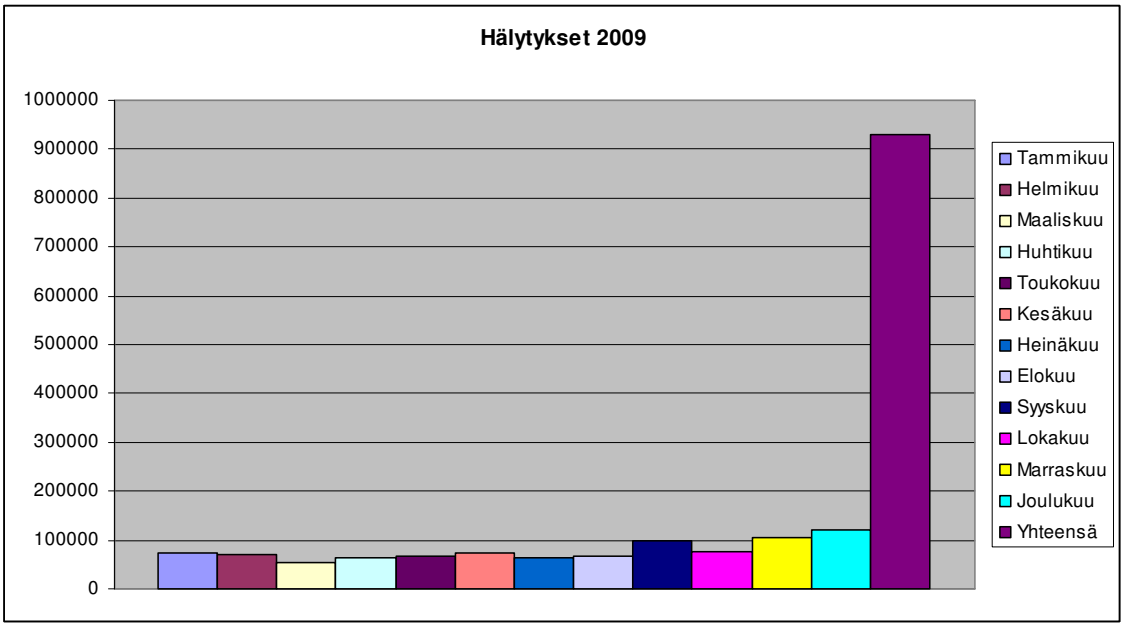


Kuvio 6: Valvontahälytykset eri kuukausilta vuonna 2008

Vuonna 2009 palvelinmäärä kasvoi noin tuhannella (Kuvio 9) palvelimella edellisvuoteen nähden, ja hälytykset kasvoivat noin 300 000 hälytyksellä. Alla olevasta taulukosta nähdään vuoden 2009 hälytykset eri kuukausilta sekä kuvaajasta voidaan havainnoida, että erot kuukausien välillä voivat olla edelleen suuria.

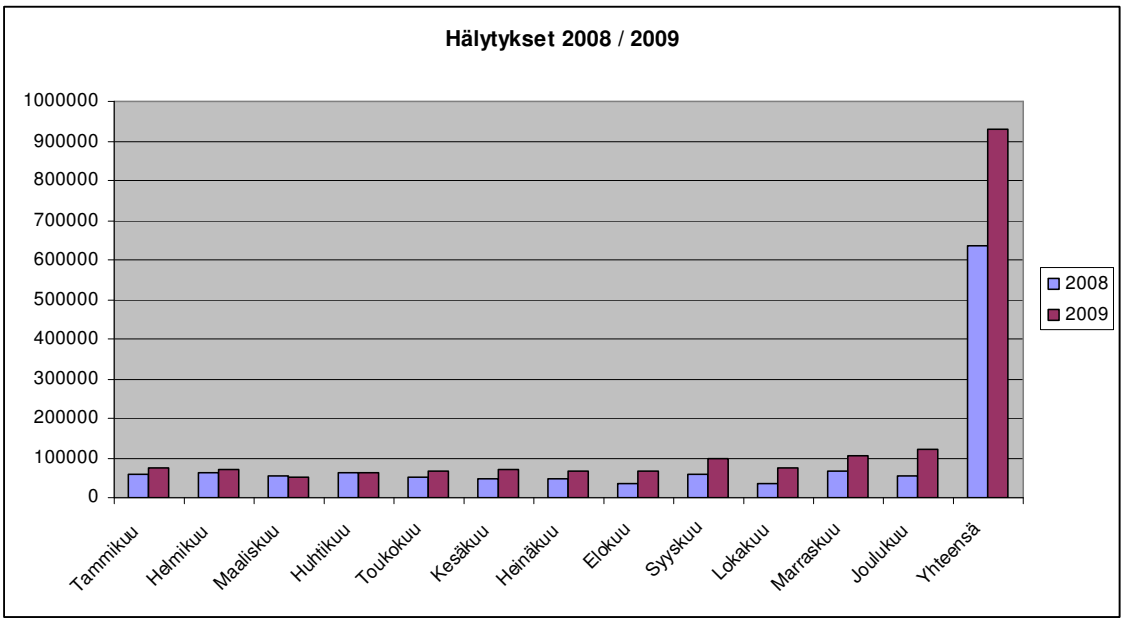
Taulukko 2: Valvontahälytykset eri kuukausilta vuonna 2009.

Tammikuu	**73499**
Helmikuu	**71045**
Maaliskuu	**52608**
Huhtikuu	**63999**
Toukokuu	**65944**
Kesäkuu	**71692**
Heinäkuu	**64781**
Elokuu	**66693**
Syyskuu	**97502**
Lokakuu	**76293**
Marraskuu	**104306**
Joulukuu	**121309**
Yhteensä	**929671**



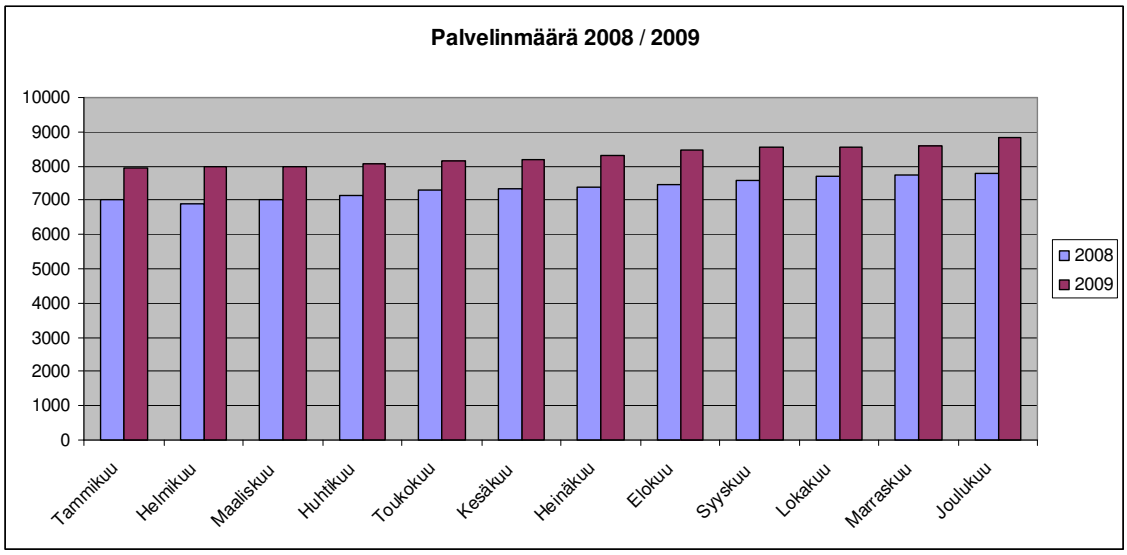
Kuvio 7: Valvontahälytykset vuonna 2009

Alla olevasta kuviosta nähdään vuosien 2008 ja 2009 hälytysmäärät, sekä se, kuinka hälytysmäärät ovat kasvaneet verrattuna edellisvuoteen.



Kuvio 8: Hälytykset eri kuukausilta vuosina 2008 & 2009

Alla olevasta kuviosta näkyy, kuinka paljon palvelimien määrä on kasvanut vuonna 2009 vuoteen 2008 nähden. Vuoden 2008 joulukuussa palvelimia oli noin 7800, kun taas vuoden 2009 joulukuussa palvelimia oli jo noin 8850.



Kuvio 9: Palvelinmäärä vuosina 2008 ja 2009

Vuosien 2008 ja 2009 isoon eroon hälytysmäärissä on voinut vaikuttaa hallittujen huoltotöiden lisäksi myös uusien palvelimien tuotantoon ottaminen, uusien valvonta-agenttien versiot ja asetukset sekä asiakkaiden haluamat yksilökohtaiset valvontaperiaatteet. Yksi esimerkki asiakkaan haluamasta asiakaskohtaisesta valvontaperiaatteesta voi olla tietynlainen lokivalvonta: jos tietynlainen viesti tulee palvelimen lokiin, asiakas haluaa siitä tiedon itselleen. Näin ollen viestistä muodostuu hälytys keskitettyyn valvontaan ja asiakkaalle lähetetään viesti asiasta. Nämä viestit voivat olla informatiivisia viestejä, eivätkä aina merkki virhetilanteesta.

7 Työohjeistus palvelinkeskuksen valvomon ongelmanratkaisuryhmälle

Kohdeyrityksen palvelinkeskuksen valvomossa toimivan ongelmanratkaisuryhmän tehtävänä on ratkaista akuutteja ongelmatilanteita, joita tuotannossa olevissa palvelimissa ja järjestelmissä esiintyy. Toimeksiantoja ongelmanratkaisuryhmälle voi tulla eri kanavia pitkin. Toimeksiantoja voi tulla esimerkiksi asiakkaalta joko käyttäjätuen kautta, tai asiakas on yhteydessä suoraan palvelinkeskuksen valvomoon sähköpostitse tai puhelimitse. Pääasiallinen työllistäjä on keskitetty valvontajärjestelmä, josta tulee eniten toimenpiteitä vaativia toimeksiantoja. Toimeksiannot tulevat ongelmanratkaisuryhmälle keskitetystä valvontajärjestelmästä luvussa 5 esitetyn prosessin mukaisesti.

7.1 Työohjeen tarkoitus

Ongelmanratkaisuryhmälle saapuvissa toimeksiannoissa tulee usein vastaan sellaisia tilanteita, joissa huomataan keskitetystä valvontajärjestelmästä tulevan hälytyksen olevan aiheeton. Tällaiset tilanteet aiheuttavat usein turhaa työtä valvontaoperaattoreille sekä ongelmanratkaisuryhmälle.

Tämän työn tuottaman ohjeistuksen tarkoituksena on kasvattaa valvomossa toimivan ongelmanratkaisuryhmän osaamista sillä tavalla, että tällaiset valvonnalliset ongelmat saataisiin korjattua jo palvelinkeskuksen valvomossa. Työohjeistuksen tarkoituksena ei ole siirtää valvontaongelmien selvitystä palvelinkeskuksen valvomoon, vaan saada tarvittavaa lisäosaamista yleisempien ongelmien ratkaisemiseksi ja näin ollen kasvattaa ryhmän ongelmanratkaisukykyä.

7.2 Työohjeen vaatimukset ja sisältö

Työn toimeksiantajan kanssa käydyissä palavereissa käytiin läpi, mitä työohjeelta halutaan. Työohje on tarkoitettu sisäiseen käyttöön palvelinkeskuksen valvomossa, joten työohjeen käyttäjän perustiedoille voitiin asettaa tiettyjä edellytyksiä. Tärkeimpinä asioina toimeksiantaja katsoi olevan laitteistovalvontaan sekä Windows-palveluihin liittyvät ohjeet. Lisäksi työohjeeseen haluttiin yleispätevä ohje, jolla voidaan poistaa ”mitä tahansa” valvonnasta. Toimeksiantajan kanssa päädyttiin listaamaan seuraavat asiat, mitä työohjeesta pitää löytyä:

- Laitteistovalvontamoduulin sisäisten viestien poistaminen valvonnasta
- Laitteen tai sensorin poistaminen laitteistovalvontamoduulista
- Laitteen tai sensorin palauttaminen laitteistovalvontamoduuliin
- Windows-palveluiden poistaminen valvonnasta
- Windows-palveluiden tuominen takaisin valvontaan
- Yleisohje, jonka avulla voidaan poistaa jokin tietty parametri valvonnasta

Ohjeen täytyi olla myös hyvin selkeä ja havainnollistava, jotta väärinkäsityksiä ja sitä kautta virheitä ei tulisi ohjeen kanssa työskennellessä. Työohjeen tarkistajana ja arvioijana toimi

työn tilaaja. Työohjetta ei ole otettu liitteeksi tähän opinnäytetyöhön salassapitoseikkojen vuoksi.

Lopputuloksena saatiin toimiva työohje, jolla voidaan poistaa eri valvontakohteita PATROL –valvonnasta. Ohje sisältää kaikki ne asiat mitä työn toimeksiantajan kanssa asetettiin vaatimuksiksi. Työohjetta testattiin esimerkkipalvelimella, josta poistettiin laitteistovalvontamoduulin sisäiset viestit valvonnasta.

7.3 Testaus

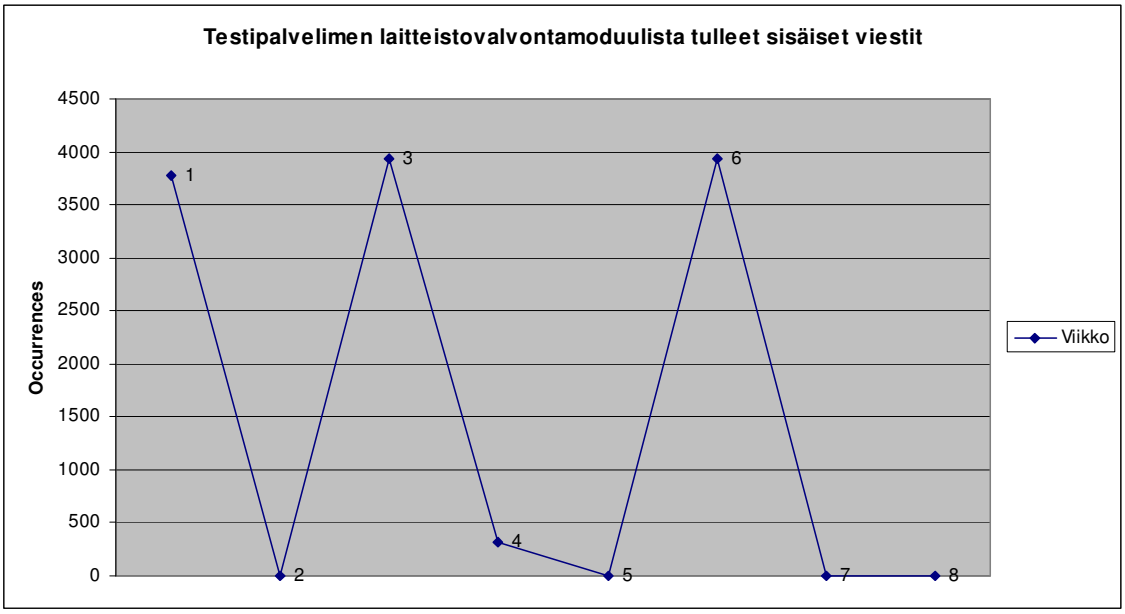
Työn toimeksiantajan kanssa käydyissä keskusteluissa sovittiin, että otetaan yksi tuotantopalvelin seurantaan, ja tarkkaillaan sen käytöstä laitteistovalvontamoduulin hälytysten osalta. Aikaisemmin tässä työssä käytiin läpi, millaisia hälytyksiä laitteistovalvontamoduulin aiheettomat hälytykset ovat ja miten paljon niitä tulee kokonaishälytysmäärään nähden. Totesimme kyseisessä luvussa laitteistovalvontamoduulin sisäisiä viestejä tulevan hälytyksinä yli 10 % kaikista niistä hälytyksistä, jotka ovat hälyttäneet vähintään 0 – 14 minuuttia. Sen vuoksi päätettiin testata työohjeistus siten, että poistetaan seurattavasta tuotantopalvelimesta laitteistovalvontamoduulin sisäiset viestit, ja tarkkaillaan, tulevatko moduulin sisäiset viestit enää hälytyksinä.

Seurasimme esimerkkipalvelimelta kahdeksan viikon ajan sieltä tulleita laitteistovalvontamoduulin sisäisiä viestejä, jotka tulivat valvontaan hälytyksinä. Keräsimme viikoittain kyseisen palvelimen tuottamat laitteistovalvontamoduulin sisäiset viestit ja teimme tilastoa niiden toistuvuudesta. Tilastoissa mitataan siis sitä, kuinka monta kertaa sama hälytys on toistunut. Mikäli sama hälytys toistuu uudestaan, ilman että valvonta-agentti on kuitannut sen olevan kunnossa, kasvattaa se laskurin lukua, joka mittaa kuinka monta kertaa kyseinen hälytys on toistunut. Kyseisiä lukuja ei siis sellaisenaan lisätä kokonaishälytysmäärään, koska toistuvuutta ei lasketa eri hälytyksiksi. Kuitenkin toistuvuus antaa kuvan siitä, kuinka usein kyseinen palvelin lähettää hälytyksen näistä viesteistä ja kuinka paljon kyseiset hälytykset kuormittavat valvontajärjestelmää turhaan.

Testattavan palvelimen tiedot:

- Merkki: Fujitsu Siemens
- Malli: Primergy RX300
- Prosessori: Intel(R) Xeon(TM) MP CPU 2.80GHz
- Käyttöjärjestelmä: Windows Server 2003 Standard Edition
- PATROL agentin versio: 3.7.40i

Testi tehtiin siten, että seurattuamme kuusi viikkoa esimerkkipalvelimelta tulleita hälytyksiä teimme muutoksia palvelimen valvonta-agentille. Muutokset tehtiin työohjeistuksen mukaisella tavalla muuttamalla laitteistovalvontamoduulin asetuksia siten, ettei kyseisen moduulin sisäisistä viesteistä tule hälytystä keskitettyyn valvontajärjestelmään. Kyseinen muutos ei vaikuta millään tavalla palvelimen varsinaiseen toimintaan, vaan vaikuttaa ainoastaan valvonta-agentin asetuksiin ja sitä kautta sen valvontaperiaatteisiin. Seurasimme muutoksien jälkeen vielä kaksi viikkoa palvelimelta tulevia laitteistovalvontamoduulin hälytyksiä, eikä kyseisiä hälytyksiä enää tullut keskitettyyn valvontajärjestelmään. Alla olevasta kuviosta voidaan todeta muutosten vaikutus palvelimelta tuleviin laitteistovalvontamoduulin sisäisiin viesteihin.



Kuvio 10: Testipalvelimelta tulleet laitteistovalvontamoduulin sisäiset viestit.

Kuviosta voidaan myös todeta, että viestejä tulee hyvin vaihteleva määrä eri viikoilta. Määriin voi vaikuttaa esimerkiksi se, onko palvelinta käynnistelty uudelleen. Viikkoina 1, 3 ja 6 viestejä tuli eniten. Muutokset tehtiin kuudennen viikon jälkeen valvonta-agentille, jonka jälkeen hälytyksiä ei enää tullut laitteistovalvontamoduulin sisäisistä viesteistä. Testiä voidaan näin ollen arvioida onnistuneeksi.

8 Yhteenveto

Työn tavoitteena oli selvittää, millaisia ovat yleisimmät aiheettomat hälytykset ja tuottaa valvomon ongelmanselvitysryhmälle työohjeistus, jonka avulla voidaan poistaa aiheettomasti hälyttävät parametrit valvonnasta. Työssä kuvattiin palvelinkeskuksen valvomon näkökulmasta keskitetyn valvontajärjestelmän toimintaa sekä sitä, kuinka

ongelmanselvitysprosessi toimii valvontahälytyksen tullessa. Työssä haettiin vastauksia seuraaviin tutkimuskysymyksiin: onko mahdollista tuottaa valvomolle yleispätevä työohjeistus, jolla voidaan poistaa turhaan hälyttäviä kohteita valvonnasta? Tukikysymyksinä olivat muun muassa: minkä tyyppisiä aiheettomat hälytykset ovat ja mistä aiheettomat hälytykset johtuvat? Miksi ne ovat aiheettomia?

Työn lopputuloksena saatiin toimiva ohjeistus, jolla voidaan poistaa tietynlaisia aiheettomia hälytyksiä sekä poistaa mikä tahansa parametri valvonnasta yksittäiseltä valvonta-agentilta. Työssä käytiin läpi kahdenlaisia aiheettomia hälytyksiä, mistä kyseiset aiheettomat hälytykset johtuivat ja vastattiin siihen, kuinka ne saadaan korjattua. Työn tavoitteisiin pääsemistä voisi näin ollen kuvata hyväksi.

Työn lopputulokset ottavat kuitenkin kantaa vain yhden valvonta-agentin toimintaan. Palvelimia, joilta aiheettomia hälytyksiä tulee, on tuhansia, ja yksi palvelin saattaa aiheuttaa monta erilaista aiheetonta hälytystä. Näin ollen tämä työ ei tuonut ratkaisua varsinaiseen valvontaongelmaan, mutta toi lisää keinoja palvelinkeskuksen ongelmanratkaisuryhmälle valvonnan parantamiseksi. Tämän työn tuottaman ohjeistuksen hyödyt tulevat esiin vasta pidemmällä aikavälillä, jos hyötyä mitataan hälytysmäärien vähenemisellä. Kaikille valvonta-agenteille tulisi ajaa sama konfiguraatio esimerkiksi laitteistovalvonnan sisäisten viestien poistamiseksi. Haasteena tässä saattaa olla se, että laitteistovalvontamoduulien eri versioissa saattaa olla eri parametrit, joilla määritetään sisäisten viestien päällä oleminen. Näitä haasteita tutkivat kuitenkin kohdeyrityksessä keskitetystä valvonnasta vastaavat asiantuntijat.

Työn tuottaman ohjeistuksen avulla palvelinkeskuksen valvomo pystyy poistamaan aiheettomia hälytyksiä valvonnasta. Jatkossa olisi hyvä ottaa käyttöön sellainen käytäntö, että ongelmanratkaisuryhmä pyrkisi poistamaan aiheettomaksi todennetun hälyttävän parametrin valvonnasta, eikä siirtäisi ongelmanratkaisua eteenpäin kuten aiemmin. Näin saataisiin tällaiset valvonnalliset ongelmat ratkaistua nopeasti, mikä helpottaisi valvontatyötä. Apuna tässä voitaisiin käyttää yrityksen järjestelmätietokantaa, johon merkittäisiin kaikki tehdyt muutokset kyseessä olevan palvelimen tietoihin. Näin palvelimesta ja sillä pyörivistä järjestelmistä vastaavat henkilöt pysyisivät ajan tasalla tehtyjen muutosten kanssa.

Jatkossa työohjetta voisi kehittää esimerkiksi siten, että työohjeeseen liitettäisiin lista tietyistä valvottavista kohteista, jotka voitaisiin poistaa valvonnasta huolimatta palvelimen käyttötarkoituksesta. Tässä työssä käsiteltiin vain muutamaa esimerkkiä, jotka voitaisiin poistaa valvonnasta. Työohjeistusta voitaisiin laajentaa myös siten, että ohjeeseen lisättäisiin parametrien raja-arvojen säätäminen.

Lähteet

Cisco Systems. 2010. Internetworking Technology Handbook. Viitattu 16.3.2010. http://www.cisco.com/en/US/docs/internetworking/technology/handbook/SNMP.html

Dell. 2009. Dell OpenManage Server Administrator Version 6.2 User's Guide. Viitattu 27.3.2010. http://support.euro.dell.com/support/edocs/software/svradmin/6.2/en/UG/HTML/index.htm

Järvinen, P & Järvinen, A. 2004. Tutkimustyön metodeista. Tampere: Tampereen yliopistopaino.

Microsoft, 2005. David Notario's web blog: What is mscorsvw.exe and why is it eating up my CPU? What is this new CLR Optimization Service? Viitattu 16.3.2010. http://blogs.msdn.com/davidnotario/archive/2005/04/27/412838.aspx

Microsoft, 2008. Terminal Services Overview. Viitattu 16.3.2010. http://technet.microsoft.com/fi-fi/library/cc755053%28en-us,WS.10%29.aspx

Microsoft, 2010a. Introduction to Windows Service Applications. Viitattu 16.3.2010. http://msdn.microsoft.com/en-us/library/d56de412%28VS.80%29.aspx

Microsoft, 2010b. Performance logs and Alerts overview. Viitattu 16.3.2010. http://technet.microsoft.com/en-us/library/cc738564%28WS.10%29.aspx

Microsoft, 2010c. .NET Framework Conceptual Overview. Viitattu 16.3.2010. http://msdn.microsoft.com/en-us/library/zw4w595w.aspx

Sentry Software. 2008b. Hardware Sentry KM for PATROL screenshot gallery. Viitattu 27.3.2010. http://www.sentrysoftware.net/Products/Hardware_Overview.asp

Wikipedia, 2010. Windows Service. Viitattu 16.3.2010. http://en.wikipedia.org/wiki/Windows_service

Julkaisemattomat lähteet

BMC Software. 2003. Monitoring and Managing a Microsoft Windows Environment 2446. Houston.

BMC Software. 2004. PATROL Agent Reference Manual. Houston.

Sentry Software. 2008a. Hardware Sentry KM for PATROL User Guide. Houston.

Kuviot ja kuvat

Taulukot