TAMPEREEN
AMMATTIKORKEAKOULU

N-CENTRAL-VALVONNAN KEHITTÄMINEN

Minttu Järvi

Opinnäytetyö
Kesäkuu 2016
Tietojenkäsittely
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut

JÄRVI, MINTTU:
N-Central-valvonnan kehittäminen

Opinnäytetyö 31 sivua, joista liitteitä 1 sivua
Toukokuu 2016

Opinnäytetyön tavoitteena oli tapaustutkimuksena selvittää Triuvare Oy:lle miten N-Centralin palvelinvalvontaa voisi kehittää ja ottaa valvonnan käyttöön SNMP-protokollan avulla myös muille verkkolaitteille. Tarkoituksena oli saada valvonta toimimaan tehokkaasti niin, että asiakkaille voitaisiin tarjota parempaa ja nopeampaa palvelua ongelmatilanteissa. Samalla hyödyttäisiin N-Centralista enemmän ja vähennettäisiin manuaalisen valvontatyön määrää. Valvontaa oli tarkoitus kehittää niin automaattiseksi kuin mahdollista, jotta resursseja säästyy muihin töihin.

Palvelinvalvontaa kehitettiin muuttamalla hälytysten raja-arvoja sekä tutkimalla N-Centralin toimintaa valvonnassa. Näin saatiin vähennettyä hälytysten määrää. Sen lisäksi valvontaa helpotettiin luomalla asiakkaiden ylläpidossa olevista palvelimista N-Centraliin helposti käytettävä lista. Siitä nähdään suoraan yleiskuva asiakkaiden palvelinten tilasta. Verkkolaitteiden valvonta saatiin pitkälti otettua käyttöön. Valvontaprosessia saatiin myös vietyä eteenpäin kehittämällä toimintatapaa hälytysten käsittelyyn.

Toimivan valvonnan merkitys on erittäin tärkeä. Sen avulla voidaan proaktiivisesti ehkäistä ongelmatilanteita. Tehokas valvonta myös vähentää sekä Triuvaren että asiakasyritysten kustannuksia. Triuvarella valvontaan ei kulu niin paljon resursseja kuin aikaisemmin, ja asiakkaat joutuvat harvemmin keskeyttämään töitään laiterikkojen vuoksi. Tulevaisuudessa valvonnan voisi ottaa käyttöön N-Centralin kautta myös sellaisille laitteille, joissa on oma erillinen valvonta, kuten Ciscon Merakit. Valvontaprosessia voisi entisestään kehittää tehokkaammaksi ja valvottavien kytkin- ja palomuurityyppien määrää kasvattaa.

Asiasanat: valvonta, monitorointi, N-Central, SNMP

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Network Services

JÄRVI, MINTTU:
Developing of N-Central Monitoring

Bachelor's thesis 31 pages, appendices 1 page
May 2016

The objective of this thesis was to study how to develop server monitoring and implement SNMP-monitoring on other network devices using N-Central. This case study was made on request by the author's employee Triuvare Ltd. The purpose of the thesis was to get monitoring working effectively so that the company could offer faster and better monitoring services for its customers. The goal was also to increase the use of N-Central, reduce the amount of manual monitoring and automate monitoring as well as possible so that the resources can be allocated to other tasks.

Server monitoring was improved by adjusting thresholds and by examining monitoring services of N-Central. As a result, the amount of monitoring notifications was reduced. In addition, monitoring was enhanced by creating a convenient dashboard that shows the general status of all monitored servers. Monitoring of network devices was implemented for the most part and the process was improved.

The presence of functional monitoring is important. Monitoring allows solving problems proactively on customers' devices. Monitoring saves both Triuvare's and our customers' resources. The future plan for monitoring is to extend monitoring to include more devices. Also the monitoring process could be even more effective.

Key words: monitoring, N-Central, SNMP

SISÄLLYS

LYHENTEET JA TERMIT

AES	Advanced Encryption Standard, salausmenetelmä
DES	Data Encryption Standard, salausmenetelmä
ICMP	Internet Control Message Protocol, TCP/IP-pinon protokolla
MD5	Message-Digest Algorithm, salausalgoritmi
MIB	Management Information Base, hallintatietokanta
NMS	Network Management Station, hallinta-asema
OID	Object Identifier, objektitunniste
SHA	Secure Hash Algoritm, kryptograafinen tiivistefunktio
SMI	Structure of Management Information, hallintatiedon rakenne
SNMP	Simple Network Management Protocol, yksinkertainen verkkohallintaprotokolla
TCP/IP	Transmission Control Protocol /Internet Protocol, tietoliikennöinnissä käytettävä protokollaperhe
UDP	User Datagram Protocol, yhteydetön kuljetuskerroksen tietoverkkoprotokolla
USM	User-based Security Model, käyttäjäperustainen tunnistautumismalli
VACM	View-based Access Control Model, näkymäperustainen pääsynhallintamalli
VPN	Virtual Private Network, virtuaalinen erillisverkko
WMI	Windows Management Instrumentation, Windowsin hallintainstrumentointi

1 JOHDANTO

Nykyaikana liiketoiminta on riippuvaista tietoliikenteen toiminnasta mm. viestinnän, rahaliikenteen ja usein myös tuotannon osalta. Siksi häiriöt tai viat palvelimissa ja verkkolaitteissa voivat aiheuttaa toimialasta riippumatta suuria ongelmia päivittäisen työn suorittamisessa ja isommassa mittakaavassa jopa vaikuttaa yritysten tuloksiin. Vastoinkäymisten välttämiseksi laitteita valvotaan, jolloin saadaan tietoa niiden tilasta ja voidaan mahdollisimman nopeasti reagoida ongelmiin tai jopa ennaltaehkäistä niitä.

Yritysten näkökulmasta IT-alaan liittyvät kustannukset tuntuvat usein suurilta. Kulut kuitenkin ovat välttämättömiä tietoliikenteen hallitessa jokaisella alalla. IT-ympäristön käyttöönoton jälkeinen laitteiden valvonta ja ylläpito myös todennäköisemmin pitävät laitteet toimintakuntoisena. Näin pyritään välttämään kalliiksi käyvät katkokset, jotka voivat näkyä suurinakin menoerinä. Valvonnan avulla on mahdollistaa säästää IT-kuluissa.

Opinnäytetyön tarkoituksena on selvittää ICT-asiantuntijapalveluyritykselle Triuvare Oy:lle miten voidaan monitoroida asiakkaiden verkkolaitteita sekä hienosäätää tällä hetkellä käytössä olevaa palvelinten valvontaa. Valvonnan työkaluna käytetään N-Centralia. Muiden alustojen käytön pohtimiselle ei ollut tarvetta, sillä valvonta haluttiin keskittää jo muussakin käytössä olevaan, maksulliseen työkaluun, jonka käyttöön saamme asiakkaana myös tukea helposti. Selvitystyön lisäksi valvonta otetaan käyttöön ja luodaan käytäntö sen ylläpitämiseen ja käyttöönottamiseen uusilla laitteilla. Hälytysten raja-arvoja säädetään hälytyksiä varten mahdollisimman hyödyllisiksi.

Tavoitteena on turvata asiakkaiden IT-ympäristöjen toiminta mahdollisimman hyvin automaattisten hälytysten ansiosta poikkeus -ja vikatilanteissa. Automatisoidun valvonnan ja hälytysten tavoitteena on myös helpottaa ICT-asiantuntijoiden työntekoa sekä säästää aikaa ja samalla myös rahaa. Valvonta osana palomuuri- ja kytkin palveluna-tuotteita saattaa myös tukea tuotteiden myyntiä.

Triuvare Oy on Tamperelainen yritys, jonka perustivat veljekset Toni ja Timi Rantanen vuonna 2005. Tällä hetkellä työntekijöitä on kaikkiaan 17. Triuvaren toimipiste on Tampereella, mutta suunnilleen 160 asiakasta ovat ympäri Suomea. Asiakkaita löytyy pienistä suuriin ja todella monelta toimialalta, esimerkiksi suurimmat kaupan ja logistiikan aloilta.

Pienimmällä asiakkaalla on yksi työasema, kun taas suurimmalla niitä on suunnilleen 250 kappaletta. Yleisin työasemamäärä asiakkailla on 5-50.

Valvontaympäristö tällä asiakasmäärällä on melko suuri, joten toimiva valvonta on merkittävässä asemassa. Valvottavia palomuureja on 101 kappaletta ja valvonnassa olevia palvelimia on 100. Valvontatyöt jakautuvat yhdentoista henkilön tekniselle ryhmälle kohtalaisen tasaisesti. Verkkolaitteiden ja palvelinten ylläpidosta päävastuuta kantavat kolmen henkilön tiimit.

2 LAITTEIDEN VALVONTA

Tietoverkkojen monimutkaisuus yhdistettynä laajaan laitekirjoon asettaa yritysten IT:stä vastaaville tahoille monenlaisia haasteita. Muutaman yksittäisen laitteen tilan satunnainen tarkastelu ei vie paljon resursseja, mutta puhuttaessa useista kymmenistä tai sadoista laitteista manuaalinen valvonta ei tule kysymykseen. Valvonnalla tähdätään siihen, että verkon ja sen laitteiden suorituskyky on parhaimmillaan ja keskeytysaika on niin vähäistä kuin mahdollista (Mauro & Schmidt 2005, 199.)

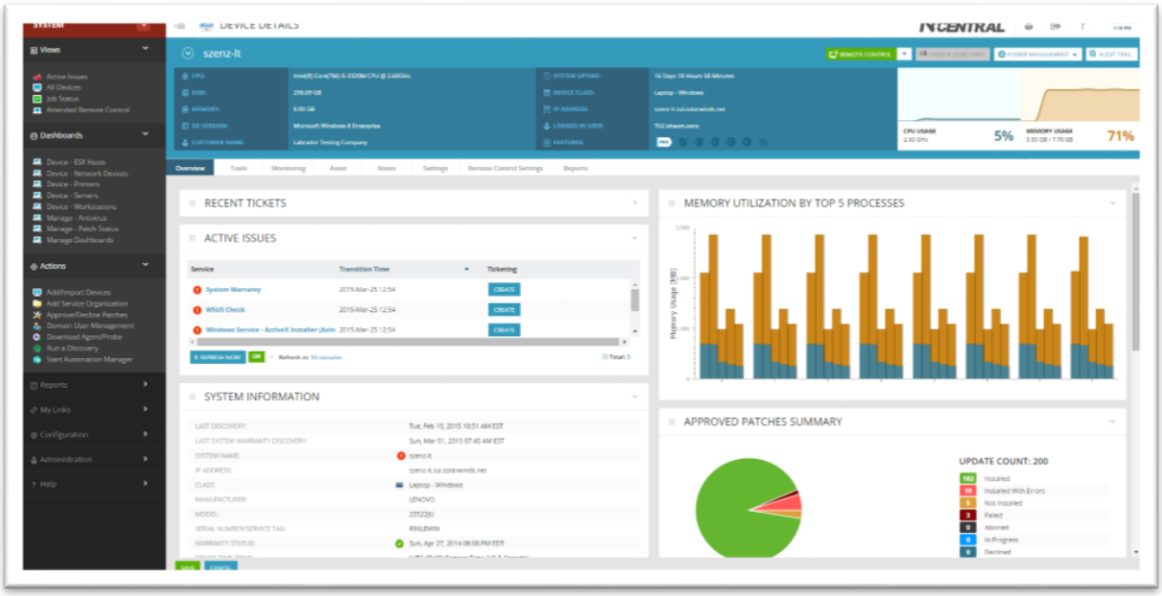
2.1 Mihin valvontaa tarvitaan?

Osa liiketoiminnasta ei juurikaan kestä ongelmia verkkolaitteiden tai palvelimien toiminnassa. Tällöin on tärkeää seurata niiden tilaa ja ennaltaehkäistä mahdolliset ongelmat. Valvonnan avulla saadaan myös arvokasta tietoa laitteiden normaalista toiminnasta. Tämä mahdollistaa muutosten sattuessa nopean reagoinnin asiakkaiden tarpeisiin. Esimerkiksi palomuurin liitäntöjen kaistankulutuksen kasvusta voidaan päätellä, että asiakkaan internetliittymän nopeutta on tarvetta kasvattaa tai verkossa on sinne kuulumatonta liikennettä. Laitteen normaalin toiminnan seuraaminen mahdollistaa myös valvontahälytysten säätämisen tehokkaaksi.

Asiakkaan kannalta laitteiden valvonta parantaa IT-ympäristön luotettavuutta ja lisää tehokkuutta vähentämällä keskeytyksiä työn tekemisessä. Valvonnan avulla usein suuriakin investointeja vaatineita palvelimia, palomuureja ja muita laitteita voidaan ylläpitää ja korjata ongelmantilanteissa lyhyellä varoitusajalla pelkkien perusylläpitotöiden lisäksi. Näin voidaan parhaassa tapauksessa myös pidentää laitteiden käyttöikää ja saada ne toimimaan parhaalla mahdollisella tavalla. Myös valvontaa myyvän yrityksen näkökulmasta valvonta tuo selkeitä etuja. Ylläpitäjien työ helpottuu ja nopeutuu sekä käsin tehtävän työn ja vianmäärityksen tarpeen väheneminen takaa virheettömämmän ja luotettavamman valvonnan. Aiemmin enemmän aikaa vievän valvonnan väheneminen näkyy säästönä, kun työntekijöiden aikaa säästyy muihin tehtäviin.

2.2 Valvontatyökalut

Cloudstats.me:n blogin mukaan (2015) valvontaa varten on olemassa monenlaisia avoimen lähdekoodin työkaluja, joita voi käyttää ilmaiseksi. Niistä käytetyimpiä ovat Nagios, Cacti ja Zabbix. Kuten johdannossakin mainittiin, tässä työssä muiden hallinta-asemien käytölle ei ole tarvetta, koska toimeksiantajan toiveen mukaan käytetään samaa työkalua kuin esimerkiksi päivitysten hallintaan. Huomiona voidaan kuitenkin mainita, että näiden alustojen toiminta ei poikkea suuresti toisistaan. Erot ovat lähinnä työkalujen monipuolisuudessa sekä graafisessa ulkoasussa. Niitä yhdistää valvonnan seuraaminen selainkäyttöliittymän kautta. Käyttöliittymä tarjoaa graafisen näkymän laitteiden tilasta (kuva 1). Graafisessa ulkoasussa on työkalujen välillä eroja. Esimerkiksi N-Central ja Nagios tarjoavat käytettävyydeltään selkeämmät grafiikat kuin Cacti. Hallinta-asemien ja valvonnan toiminnasta kerrotaan kappaleessa SNMP.



KUVA 1. Työaseman tila N-Centralissa (SolarWinds N-Able)

N-Central on SolarWinds N-Ablen:n tuote, joka on tarkoitettu IT-ympäristöjen valvontaa, hallintaa ja ylläpitoa tarjoavien palveluntarjoajien käyttöön. N-Central-palvelin on mahdollista ottaa käyttöön joko paikallisena tai hostattuna. N-Centralissa on mahdollista valvoa sekä hallita palvelimia, työasemia, verkkolaitteita sekä mobiililaitteita ja sen avulla on myöskin mahdollista automatisoida ylläpitotoimia kuten työasemien levyjen eheyttämistä sekä suorittaa keskitettyä päivitystenhallintaa työasemille. Työkalun avulla saadaan myös etäyhteydet palvelimiin ja työasemiin tarvittaessa.

Tähän asti N-Centralin käyttö on keskittynyt asiakkaiden työasemien ja palvelimien ennalta sovittuihin ylläpitotehtäviin sekä IT-tuen puitteissa akuuttien ongelmien vianmääritykseen ja korjaamiseen etäyhteyden avulla. Hälytyksiä palvelinten vikatiloista on tullut, mutta liian ympäripyöreiden oletusraja-arvojen takia niiden määrä on ollut todella suuri. N-Centralin raportointiominaisuuksia on myös käytetty hyödyksi asiakkaiden informoinnista heidän laitteidensa tilasta.

3 VALVONNASSA KÄYTETTÄVIÄ PROTOKOLLIA

N-Centralin palveluissa käytetään useita protokollia valvontainformaation hankintaan. Verkkolaitteiden osalta merkittävimpiä ovat ICMP ja SNMP. Windows-palvelimien valvontaan tehdyissä palveluissa käytössä on useimmiten WMI. ICMP-protokollaa käytetään niidenkin kohdalla hallittavan laitteen ja hallinta-aseman välisen yhteyden tarkistamiseen.

Opinnäytetyön toteutusta varten eniten selvitystä vaatii SNMP-protokolla, koska ilman sitä valvontaa ei saa otettua käyttöön palomuureille ja kytkimille. Tästä syystä toteutuksen osalta opinnäytetyö on painottunut verkkolaitteiden valvonnan kehitykseen ja SNMP-protokollaan tutustumiseen.

3.1 SNMP

3.1.1 Arkkitehtuuri

SNMP-arkkitehtuurin toiminta perustuu hallinta-asemiin, hallinta-agentteihin sekä hallittaviin laitteisiin. Hallinta-asemat valvovat ja hallinnoivat laitteita, joiden hallinta-agentit ottavat viestejä vastaan. Esimerkkejä tällaisista laitteista ovat työasemat, palomuurit, palvelimet ja kytkimet. SNMP-protokolla kuljettaa informaatiota hallinta-aseman ja agentin välillä.

IETF (Internet Engineering Task Force) vastaa internet-protokollien standardoinnista ja julkaisee RFC-dokumentteja, jotka kuvaavat internet-käytäntöjä, järjestelmiä ja protokollia. Case, Fedor, Schoffstall ja Davin (1990) määrittelevät SNMP-arkkitehtuurin tarkoituksen seuraavasti:

SNMP aiemmista protokollista poiketen vähentää itse hallinta-agentilla käsiteltävien hallintafunktioiden määrää. Siitä syystä hallinta-agentti ei tarvitse kalliita sovelluksia SNMP:n käsittelemiseen. SNMP:n yksinkertaistetut toimenpiteet tekevät hallinnan myös helpommaksi niin, että valvonta on helpommin ymmärrettävissä ja otettavissa käyttöön (Case, Fedor, Schoffstall ja Davin, 1990.)

Vaikka SNMP on jo vanha protokolla, ja sen määrittely on tapahtunut jo vuosikymmeniä sitten, se on laitteiden valvonnassa ja hallinnassa edelleen merkittävässä asemassa. Protokollan käytön yksinkertaisuus ja monipuolisuus sekä tietoturvaa parantava kolmas versio tukevat protokollan käyttöä ja kehitystä jatkossakin.

3.1.2 Kehitys ja versiot

Tarve valvontaprotokollan kehitykselle ilmeni 1980-luvulla, kun internetin kehitys oli nopeaa ja laitteiden määrä alkoi kasvaa eksponentiaalisesti. Useita protokollia uusien tarpeiden täyttämiseksi kehitettiin. SNMP:n lisäksi kehiteltiin protokollia kuten HEMS (High-level Entity-Management System) ja CMOT (CMIP over TCP/IP). 1988 IAB (Internet Activities Board) valitsi CMOT-protokollan pääasialliseksi protokollaksi verkkolaitteiden ja verkon valvontaan ja päätti SNMP:n olevan lyhytaikainen ratkaisu. CMOT olisi pääasiallinen protokolla sitten kun 1980-luvun ajatusten mukaisesti OSI-protokollat syrjäyttäisivät TCP/IP-protokollat. SNMP:n kehitys oli nopeaa ja suosion kasvaessa sekä laitevalmistajien tuen myötä siitä kehittyikin täysi internetstandardi vuonna 1990.

SNMP:n edeltäjä SGMP (Simple Gateway Management Protocol) oli tarkoitettu internetreitittimien hallintaan. Tästä syystä SNMP:kin usein yhdistetään samaan tehtävään. Reitittimien lisäksi SNMP:n avulla voidaan valvoa ja hallinnoida myös Unix ja Windows-järjestelmiä, tulostimia, kytkimiä ja reitittimiä tai mitä tahansa laitetta, jolla on ohjelma, joka voi käyttää SNMP-protokollaa informaation lähettämiseen ja vastaanottamiseen. SNMP ei myöskään rajoitu pelkästään fyysisten laitteiden hallinnointiin vaan sitä voidaan käyttää esimerkiksi ohjelmien ja tietokantojen valvontaan (Mauro & Schmidt 2005, 1.)

Mauron ja Schmidtin (2005) mukaan **SNMPv1** on protokollan alkuperäinen versio. Se määriteltiin RFC 1157-dokumentissa ja lukeutuu historiallisiin IETF-standardeihin. SNMPv1:n turvallisuus perustuu yhteisötunnuksiin (community name). Niitä on kolmea eri tyyppiä *read-only*, *read-write* ja *trap*. Nimensä mukaan *read-only* mahdollistaa tietojen lukemisen, muttei muokkaamista. *Read-write* antaa oikeuden tehdä myös muutoksia ja *trap* mahdollistaa epäsymmetrisen viestinnän eli laitteen lähettämien trap-viestin vastaanottamisen. Yhteisötunnukset ovat salaamattomia tekstimuotoisia merkkijonoja, jotka sallivat minkä tahansa merkkijonon tietävän SNMP-pohjaisen sovelluksen pääsyn lait-

teen hallintatietoihin. Vaikka SNMPv1 lukeutuu historiallisiin standardeihin, laitevalmistajat käyttävät sitä edelleen laitteidensa oletus-SNMP-versiona (Mauro & Schmidt 2005, 2.)

SNMP-protokollan tietoturvariskit tiedostettiin jo varhaisessa vaiheessa. Jo vuonna 1992 tehtiin ehdotus SNMP:n tietoturvaominaisuuksien parantamisesta. Tältä pohjalta alettiin kehittää SMP-protokollaa (Simple Management Protocol), josta tuli edeltäjäänsä tehokkaampi ja turvallisempi. Siitä alettiin käyttää nimeä SNMPv2.

SNMPv2:sta on useampi versio, joista yleisesti käyttöön jäi SNMPv2c, joka käyttää samaa yhteisötunnuskäytäntöä kuin SNMPv1 ja toi mukanaan muutamia uusia ominaisuuksia, kuten mahdollisuuden iteratiivisiin kyselyihin (GetBulkRequest). Muut versiot olivat SNMPv2u (User-Based Security Model) ja SNMPv2p (Party-Based Security Model), jotka olivat yhteisötunnuksia käyttävää versiota turvallisempia. SNMPv2p:n toiminta perustui ryhmään, joka määritettiin kommunikoimaan käyttäen määriteltyä todennusta (authentication) ja valtuutusta (authorization). SNMPv2u:n toiminnan perusperiaatteena oli siirtyä käyttäjäperustaiseen tietoturvaan aiemmasta laitesidonnaisesta tavasta, jolloin oikeudet olisivat laitteen käyttäjällä laitteen sijaan. SNMPv2u ja SNMPv2p eivät saavuttaneet suosiota monimutkaisuutensa takia. SNMPv2u:n pohjalta alettiin kehittää turvallisempaa SNMPv3-protokollaversiota.

SNMPv3 on protokollan uusin versio. Se kehitettiin pääasiassa lisäämään verkon valvonnan ja hallinnan tietoturvaa, joka on ollut alusta asti SNMP-protokollan heikkous. Kolmas versio toi mukanaan näkymäperustaisen pääsynhallinnan (VACM). Näkymät mahdollistavat käyttäjien näkemien MIB-objektien rajaamisen käyttäjäkohtaisesti eli niiden avulla eritasoiset käyttäjät saavat luku tai luku- ja kirjoitusoikeuden vain haluttuun osaan informaatiosta. SNMPv3-protokolla mahdollistaa myös vahvan todennuksen ja yksityisen tiedon kulkemisen SNMP-osapuolten välillä. Versiosta tehtiin täysi standardi jo vuonna 2002, mutta silti laitevalmistajat ovat hitaasti lisänneet versiolle tukea. Jotkin suuret laitevalmistajat kuten Cisco ovat tukeneet SNMPv3-protokollaversiota jo useita vuosia.

3.1.3 Tietoturva

SNMP:n versioissa yksi ja kaksi todennus tehdään yhteisötunnuksilla (community string). SNMPv3:n todennustapa on USM eli käyttäjäperustainen todennus. Käyttäjien todentamisessa algoritmeinä ovat käytössä MD5 ja SHA. Näin salasanat eivät valvonnassa liiku salaamattomana verkon yli kuten yhteisötunnuksia käytettäessä. SNMP-viestien salaaminen tapahtuu DES- ja AES-algoritmeilla. Uutta SNMPv3:ssa on myös VACM, jonka avulla on mahdollista antaa käyttäjille tiettyjä näkymiä, jolloin kaikille ei tarvitse antaa pääsyä jokaiseen objekteihin. On myös mahdollista määrittää samalle käyttäjälle joihinkin objekteihin kirjoitusoikeus ja osaan vain lukuoikeus. Taulukossa 1 on kuvattuna SNMP:n versioiden tietoturvan tasot.

Tietoturvan merkitys SNMP:n käytössä on suuri, sillä sen hallintaominaisuudet mahdollistavat pääsyn esimerkiksi sulkemaan laitteiden portteja tai muutamaan reititysasetuksia. Salaamattomana verkon yli kulkevat yhteisötunnukset ovat osaavalle tekijälle helposti selvitettävissä. Tästä syystä suositellaan SNMPv3:n käyttöä aina kun mahdollista. Jos laitteiden puuttuvasta SNMPv3-tuesta johtuen on pakko käyttää vanhempaa versiota, tulisi tietoturva huomioida käyttämällä VPN-yhteyttä tai käyttäen selainkäyttöliittymää SSL:n kera. Aina yhteisötunnuksia käyttäessä myös olisi suositeltavaa vaihtaa niitä tiuhaan tahtiin. Edelleenkin suurin osa SNMP-valvonnasta tehdään vanhoilla versioilla ja oletustunnuksilla public ja private (Mauro & Schmidt 2005, 116.)

TAULUKKO 1. SNMP:n tietoturvan tasot

Versio	Taso	Todennus	Salaus
v1	noAuthNoPriv	yhteisötunnus	Ei salausta
v2c	noAuthNoPriv	yhteisötunnus	Ei salausta
v3	noAuthNoPriv	käyttäjänimi	Ei salausta
v3	authNoPriv	MD5 tai SHA	Ei salausta
v3	authPriv	MD5 tai SHA	DES tai AES

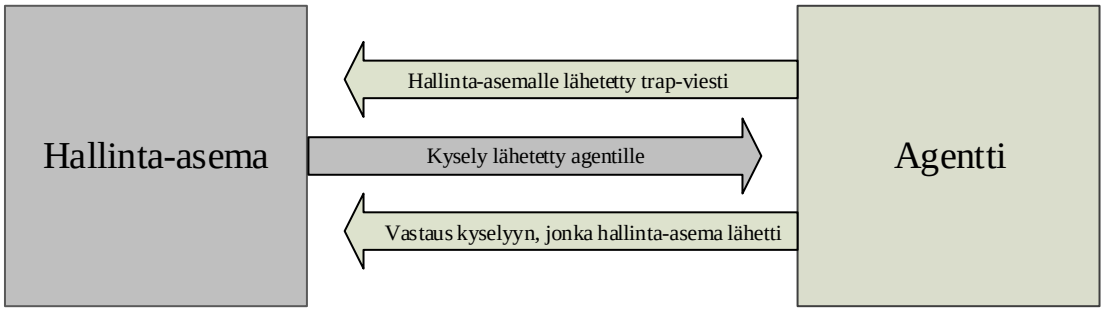
3.1.4 Toiminta

SNMP-valvontaan tarvitaan kolme osapuolta, jotka ovat hallinta-asema, agentti ja hallittava laite. Triuvarelle tekemässäni valvonnassa esimerkkinä näistä kolmesta osasesta valvonnan kokonaisuudessa ovat hallinta-asema N-Central, hallittava laite Ciscon palomuuri ja agentti, joka on sisäänrakennettuna ohjelmallisena moduulina Ciscon laitteissa.

Hallittava laite on laite, jolla on SNMP-agentti ja jota hallitaan hallinta-aseman kautta (kuvio 1). Esimerkkejä tällaisista laitteista ovat esimerkiksi reitittimet, palvelimet, kytkimet, tulostimet ja työasemat. Erilaisilta laitteilta on mahdollista valvoa erilaisia asioita. Reitittimeltä halutaan valvoa laitteen lämpötilaa sekä porttien toimintaa ja liikennemääriä. Tulostimelta sen sijaan voidaan haluta tiedustella esimerkiksi tulostimen tilaa ja tulostusjonon pituutta.

Agentti on ohjelmallinen moduuli, joka voi olla hallittavalla laitteella joko sisäänrakennettuna (Ciscon laitteet) tai erillinen asennettava ohjelma. Sen tehtävänä on lähettää vastauksia hallinta-aseman pyyntöihin sekä lähettää trap-viestejä ongelmatilanteista.

Hallinta-asemalla on ohjelmisto, jonka avulla verkon laitteita voidaan valvoa ja hallita. Hakalan ja Vainio painottavat, että hallinta-asemat tarjoavat suurimman osan prosessointia ja muistia varten vaadittavista resursseista. Verkonhallinnassa yhtä verkkoa kohden tarvitaan yksi hallinta-asema (Hakala & Vainio 2002, 270).



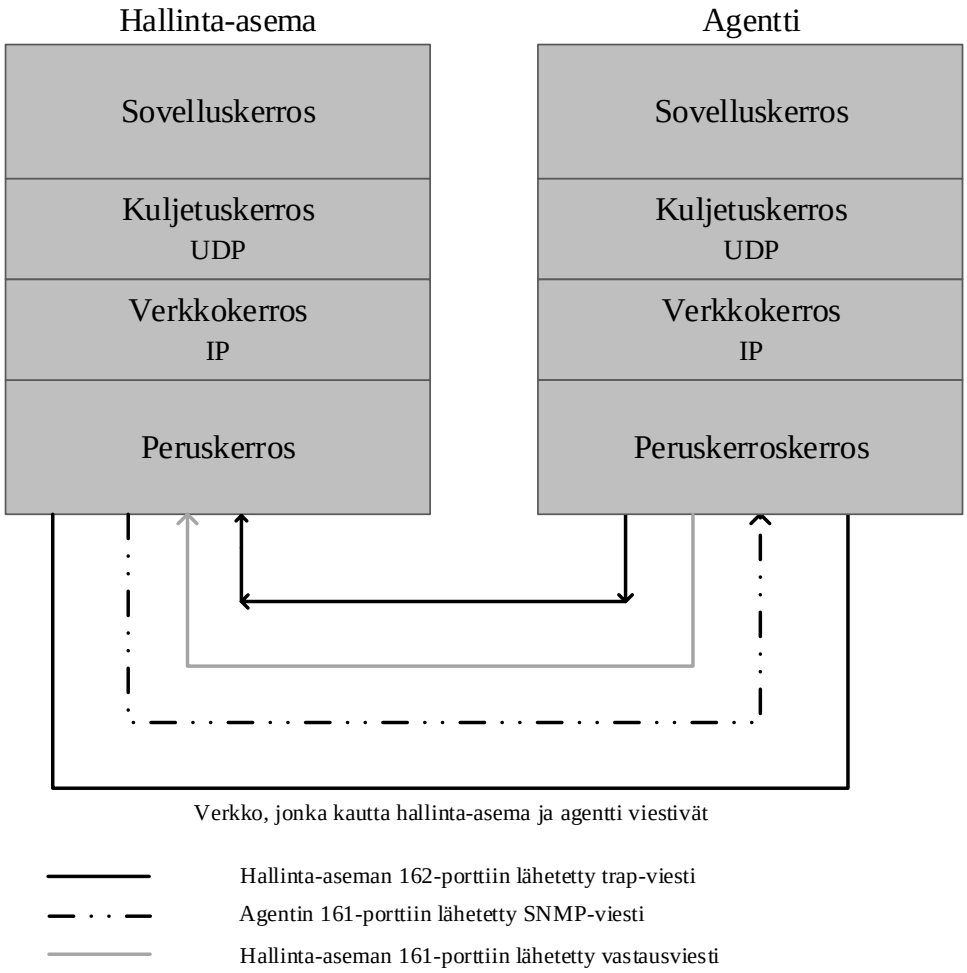
KUVIO 1. Hallinta-aseman ja agentin suhde

SNMP on TCP/IP-mallin sovellustason protokolla (kuvio 2). Sen toiminnan perusta ovat operaatiot, jotka mahdollistavat SNMP-yhteensopivien laitteiden välisen hallintainformaation kuljettamisen valvonta-alustan ja hallittavan laitteen välillä. Hallinta tarkoittaa

komentojen antamista laitteille protokollan välityksellä joko manuaalisesti tai automaattisesti. SNMP käyttää UDP-portteja 161 ja 162. 161-porttia käytetään SNMP-pyyntöjen lähettämiseen ja vastaanottamiseen ja porttia 162 käytetään trap-viestien vastaanottamiseen hallittavilta laitteilta.

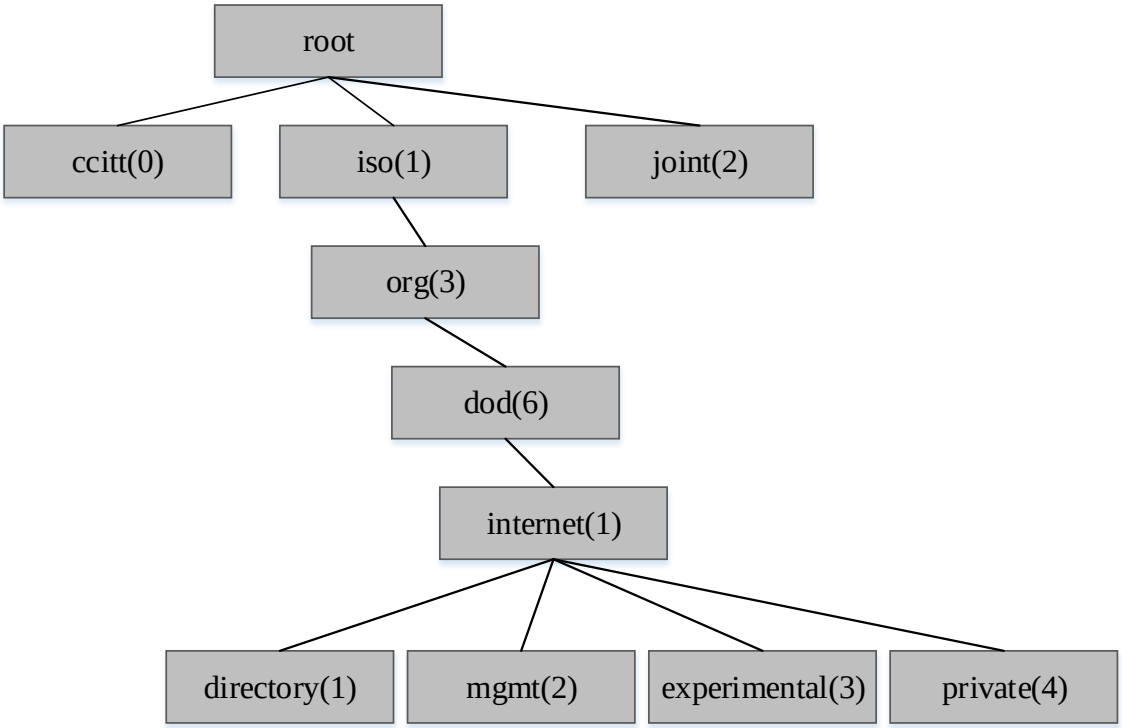
SNMP-protokolla toimii UDP:n päällä. Sen välityksellä SNMP-viestit kulkevat hallinta-asemien ja agenttien välillä. UDP valittiin TCP:n sijaan siksi, ettei verkko kuormitu liikaa TCP:n kolmivaiheisen kättelyn suuresta viestimäärästä. UDP tekee viestinnästä TCP-liikennöintiä epävakaampaa, mutta valvonnan luonteen takia yhteydettömyys ei ole suuri ongelma, koska hallinta-alustalle voi asettaa aikakatkaisun (timeout). Ellei agentilta kuulu vastausta sovitun ajan puitteissa, lähettää hallinta-asema viestin uudelleen. Aikakatkaisun keston sekä uudelleenlähetettävien pakettien määrän voi asettaa itse.

Hallinta-asemalta lähtevien viestin kohdalla UDP ei ole suurikaan ongelma, mutta agenteilta lähtevien trap-viestien tilanne on vaikeampi. Jos agentti lähettää viestin, joka ei saavu hallinta-asemalle, ei hallinta-asemalla ole keinoa tietää viestin lähetyksen epäonnistumisesta. Myöskään agentti ei tiedä saapuiko viesti perille, koska hallinta-asemalta ei ole vaadittu kuittausta trap-viestin saapumisesta perille (Mauro & Schmidt 2005, 19.)



KUVIO 2. TCP/IP kommunikointimalli ja SNMP

Simoneaun mukaan (1999) mukaan hallintatietokanta (MIB) on tietokanta, jonka tehtävänä on yksilöidä ja tunnistaa jokainen objekti sen ominaisuuksien kuten nimen, saatavuuden ja objektitunnuksen perusteella. Hakalan ja Vainion (2002) määritelmän mukaan tietokanta pitää sisällään kaikkien laitteiden tietotyypit ja muuttujat. Sen puumainen rakenne (kuvio 3) pitää sisällään ryhmitellyt objektit. Hallinta-asema lähettää tiedustelut hallittaville laitteille sen oman hallintatietokantansa mukaan. Jos laitteen agentilla on tietokannassaan kysytty objekti, se lähettää vastauksen hallinta-asemalle. Muussa tapauksessa hallinta-asemalla ilmenee virheilmoitus. Sen takia hallinta-asemalla ja agentilla täytyy olla käytössä sama hallintatietokanta. Hallintatietokannan rakenne (SMI) määrittelee tietokannan rakenteen. SMI pitää kannan rakenteen yksinkertaisena ja skaalautuvana. Sen ja hallintatietokannan kuvaamisessa käytetään ASN-formaattia, joka on ISO:n standardoima yleinen kieli.



KUVIO 3. Hallintatietokannan rakenteen objektipuu

Objektit on järjestetty puumaiseen hierarkiaan. Rakenne määrittää SNMP-objektien nimeämiskäytännön. Objektitunniste (OID) luodaan pisteillä erotetuista kokonaisluvuista, jotka määräytyvät niiden rakenteessa olevan sijainnin mukaan. Jokaisella numeerisella tunnisteella on myös helpommin luettava nimi. Mauron ja Schmidtin mukaan (2005) Private-haarassa on alahaara, joka on laitteisto- ja ohjelmistovalmistajille varattu alue. Esimerkkinä tästä on alahaara *iso.org.dod.internet.private.enterprises.cisco* eli 1.3.6.1.4.1.9, jonka alta löytyy Ciscon laitteilla olevat objektitunnisteet.

3.2 WMI

WMI on verkkopohjainen, Windows-spesifinen protokolla. N-Centralin luotaimet ja agentit käyttävät sitä valvontatiedon hankintaan Windows-käyttöjärjestelmällä varustetuilta laitteilta. Sen välityksellä kulkee esimerkiksi tieto laitteiden sarjanumeroista, päivityksistä, ja Windows-palvelimien ja työasemien suorituskyvystä ja tilasta. WMI:n avulla hallinta-aseman kautta voidaan valvotuilta laitteilta ajaa myös komentosarjoja ja sovelluksia (N-able recource center, 2016.)

4 VALVOTTAVAT LAITTEET

Tässä kappaleessa esitellään pääpiirteittäin laitteita, joita Triuvaren asiakkailta halutaan valvoa ja joiden valvontaa halutaan kehittää. Opinnäytetyön puitteissa voidaan ottaa valvonta käyttöön sellaisille laitteille, joita on paljon ja joiden valvonta helpottaa tuntuvasti Triuvaren työntekijöiden työtä.

Valvonnan käyttöönoton jälkeen on mahdollista kehittää sitä eteenpäin yrityksen ja asiakkaiden tarpeiden mukaan. Tällaisia tulevaisuudessa valvonnan piiriin tulevia laitteita ovat esimerkiksi Ciscon langattoman verkon laitteet kuten Merakit. Valvontaan liittyvät asetukset eivät suoraan sovi laitetyypiltä ja laitevalmistajalta toiselle, mutta SNMP:n toimintaperiaatteen ja N-Centralin toimintojen monistaminen on pienillä muutoksilla kohtalaisen helppoa uusillekin SNMP-valvontaa tarvitseville laitteille.

4.1 Palomuuri

Palomuurit ovat verkon tietoturvan kannalta tärkeitä laitteita, joita käytetään laajasti yrityksissä ja instituutioissa suojaamaan sisäverkkoa. Palomuuri on ulko- ja sisäverkon rajalla oleva laite, jonka läpi kaikki sisään ja ulos kulkevat paketit menevät (Liu 2011, 1.)

Opinnäytetyössä tutkitaan kolmen palomuurimallin objektitunnisteita (kuva 2). Näitä palomuureja myydään palomuuripalvelun kera asiakkaille. Jokaista Ciscon ASA-tuoteperheeseen kuuluvaa mallia varten tarvitaan siis oma valvontamalli, joka pitää sisällään sekä valmiita valvontapalveluita sekä mallikohtaisia, räätälöityjä valvottavia ominaisuuksia.

ASA5505 on pian myynnistä poistuva malli, jota kuitenkin tällä hetkellä on eniten käytössä Triuvaren asiakkailla. ASA5506 korvaa edeltäjänsä ASA5505:n tuoden muutamia uusia ominaisuuksia poistaen kuitenkin laitteesta kytkimen ominaisuuksia. Uusi malli pakottaa hankkimaan sekä palomuurin että kytkimen riippumatta siitä onko asiakkaan ympäristössä muuta tarvetta kytkimelle. Tästä syystä myös hallittavien kytkinten valvontaan täytyy kiinnittää huomiota. Edellä mainitut mallit sopivat pieniin ja keskisuuriin ympäristöihin, mutta ASA5512-X sopii myös vaativampaan käyttöön suuressa ympäristössä.

KUVA 2. Valvottavat palomuurimallit

Joillakin asiakkailla on käytössä Juniperin ja Zyxelin palomuureja, joille saatetaan kehittää jatkossa myös valvontaa. Tähän päätökseen vaikuttaa laitteiden ja erilaisten mallien määrä. Erityisen hyödyllisenä voidaan pitää sellaisten mallien valvonnan käyttöönottoa, jotka tuottavat jatkuvasti ongelmia, mutta joita asiakkaat eivät syystä tai toisesta halua vaihtaa toiseen. Valvonnan avulla voidaan näyttää helpommin konkreettisia tuloksia laitteen toiminnan häiriöistä ja tukea laitteiden ja palvelun myyntiä.

4.2 Kytkin

Kytkimiä käytetään yhdistämään useita laitteita samaan verkkoon. Esimerkkinä yrityksen verkko, jossa tietokoneet, tulostimet ja palvelimet ovat kaikki samassa verkossa. Kytkimiä on hallittavia ja ei-hallittavia. Ei-hallittava kytkin toimii suoraan ilman erityisempiä asetuksia. Tämän tyyppiset kytkimet ovat yleensä tarkoitettuja kotiverkkokäyttöön. Hallittujen kytkinten asetukset voidaan määrittää tarpeen mukaan. Niiden hallinta ja valvonta onnistuvat niin paikallisesti kuin etänäkin (Cisco Networking Basics 2011.)

Kytkinten etävalvonta onnistuu, mutta se on haastavampaa kuin palomuurien, sillä niille ei aseteta julkista IP-osoitetta. Siksi niihin ei voida suoraan muodostaa yhteyttä N-Centralin kautta kuten palomuureihin. Tästä syystä kytkinten valvonta voidaan ottaa käyttöön

vain laitteille, jotka ovat tarkoin määritellyssä ympäristössä. Sen vaatimuksena on vähintään yksi palvelin, jolle on asetettu N-Centralin luotain, jonka kautta data kulkee hallintaasemalle. Tällaisia ympäristöjä ei löydy kuin muutamalta Triuvaren asiakkaalta.

Yleisellä tasolla asiakkailla olevien kytkinmallien kirjo on laajempi kuin vaikkapa palomuurien. Tästäkin syystä kytkinvalvonta on aiheena laajempi. Opinnäytetyön puitteissa selvitetään valvontamallit sellaisille hallittaville kytkimille, joita myydään palveluna asiakkaille (kuva 3). Niitä on Ciscon SG300-sarjan kytkimet 10, 28 ja 52-porttisina. Niistä kahta pienempää myydään myös PoE-malleina (Power over Ethernet). Tulevaisuudessa kehitetään tarvittaessa valvontaa myös joillakin asiakkailla käytössä oleville HP:n 1810, 1910 ja 1920-malleille.

KUVA 3. Ciscon hallittavia kytkimiä

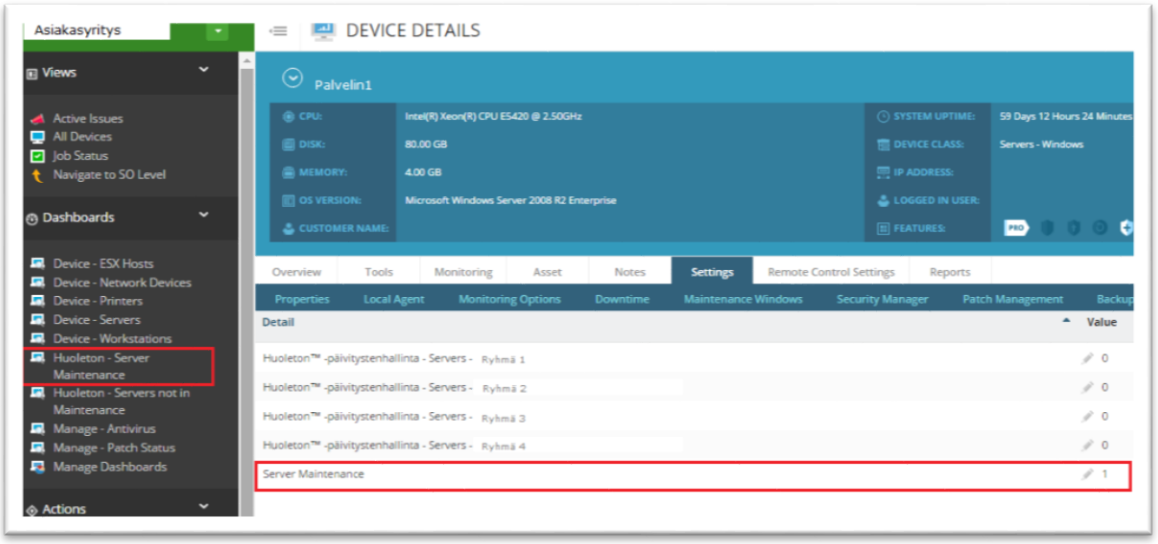
4.3 Palvelin

Palvelin on laite, joka tarjoaa toimintoja ja palveluja ohjelmille ja muille laitteille. Palvelinten toiminta on yritysten kannalta usein erittäin kriittistä, sillä pienikin vika palvelimessa saattaa estää koko yrityksen henkilöstön työnteon, häiritä kassajärjestelmien toimintaa, häiritä sähköpostien kulkemasta tai estää laitteiden pääsyn verkkoon. Palvelinongelmien vaikutus yrityksen toimintaan riippuukin paljon siitä minkälaisesta yrityksestä ja ympäristöstä on kysymys.

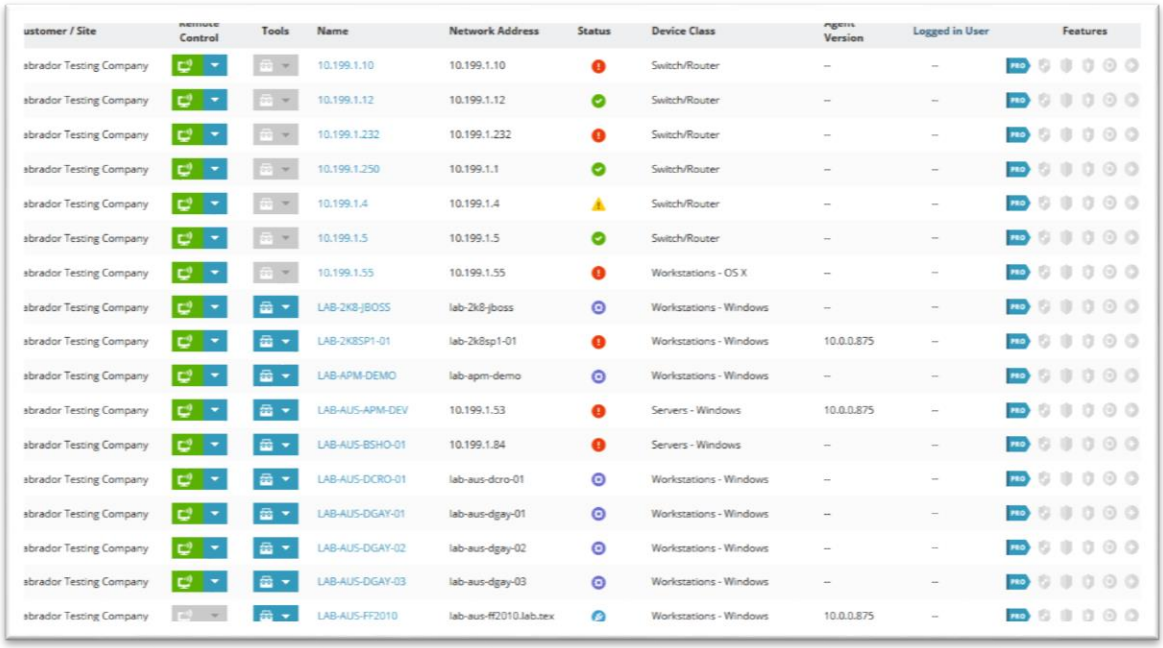
Palvelinten osalta N-Centralissa valvonta on jo hyvin pitkällä verrattuna verkkolaitteisiin. Palvelinten valvonnan osuus opinnäytetyössä on lähinnä tarkastella erilaisten hälytysten

esiintyvyyttä ja mahdollisesti rajoittaa turhien ilmoitusten määrää sekä miettiä prosessia valvontahälytyksiin reagoimiseen. Hälytyksiä taulukoidaan, jotta saadaan käsitys pidemmältä ajalta niiden esiintyvyydestä.

Palvelimilla on N-Centralin luotaimet valmiiksi Triuvaren työntekijöiden toimesta asennettuna. Suurin osa palvelimista on Windows-palvelimia, joiden valvonta onnistuu hyvin helposti WMI-protokollalla ja N-Centralin valmiilla valvontamalleilla. Valvontatyötä helpottamaan luodaan N-Centralissa suodatin, jonka kautta päästään helposti näkemään listassa kaikkien asiakkaiden meillä ylläpidossa olevat palvelimet (kuvat 4 ja 5). Suodatusta varten palvelinylläpitopalvelimille asetetaan arvo, jonka perusteella ne saadaan listanäkymään helposti (kuva 4).



KUVA 4. Linkki valvottavien palvelinten listaan ja muokattava arvo suodatusta varten



KUVA 5. Valvottavien laitteiden lista N-Centralissa (N-Central New Look and Feel, Tilner 2015)

5 VALVONTA

Tarve opinnäytetyölle tuli suoraan Triuvaren tarpeista kehittää laitteiden valvontaa. Alkutilanteessa kaikki asiakkaiden palvelimet olivat N-Centralissa ja valvonnan piirissä. Asiakkaiden palvelimilla oli asennettuna luotain, joka mahdollistaa palvelimien ja N-Central-palvelimen välisen tiedon kulkemisen. Valvonnassa on tähän asti käytetty palvelujen oletusarvoja, jonka takia turhia hälytyksiä on tullut liikaa. Niiden seasta on hidasta ja vaikeaa löytää olennaisia hälytyksiä. Verkkolaitteet eivät olleet valvonnan piirissä.

Selvitettävänä on verkkolaitteiden tuonti N-Centraliin ja SNMP-asetusten selvittäminen sekä N-Centralissa että valvottavilla laitteilla. Sen lisäksi raja-arvoja säädetään ja järkeistetään sekä mietitään kenelle hälytysten pitäisi mennä.

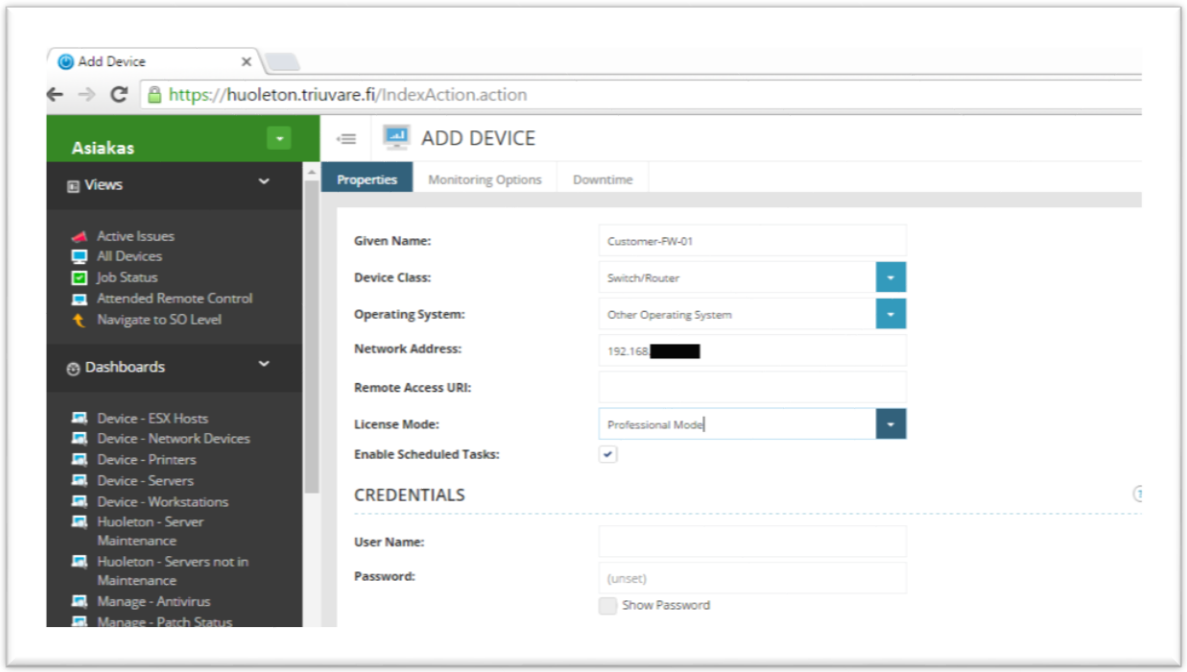
5.1 Mitä valvotaan?

Eri laitetyypeiltä valvotaan erilaisia asioita, mutta laitetyyppien kesken valvonnan kohteet ovat hyvin samanlaisia. Yleisimpiä palvelimilta valvottavia ominaisuuksia ovat yhteys N-Central-palvelimeen, suorittimen kuormitus, muistin käyttö, levyjen, aktiivihakemiston, varmuuskopioiden ja DNS:n tilat. Lista useimmiten valvottavista ominaisuuksista on liitteissä (liite 1).

Palomuureilta ja kytkimiltä valvottavat ominaisuudet ovat pitkälti samoja kuin palvelimiltakin valvottavat perusasiat. Niitä ovat mm. yhteys N-Central-palvelimeen ja suorittimen ja muistin käyttö. Näiden lisäksi palomuureilta valvotaan päälläoloaikaa, ASDM:n ja ohjelmiston versioita, aktiivisten VPN-tunnelien määrää sekä VPN-käyttäjien määrää. Kytkimeltä ja palomuurilta valvotaan myös porttien tilaa sekä pakettien hävikkiä.

5.2 Miten valvonta toteutetaan?

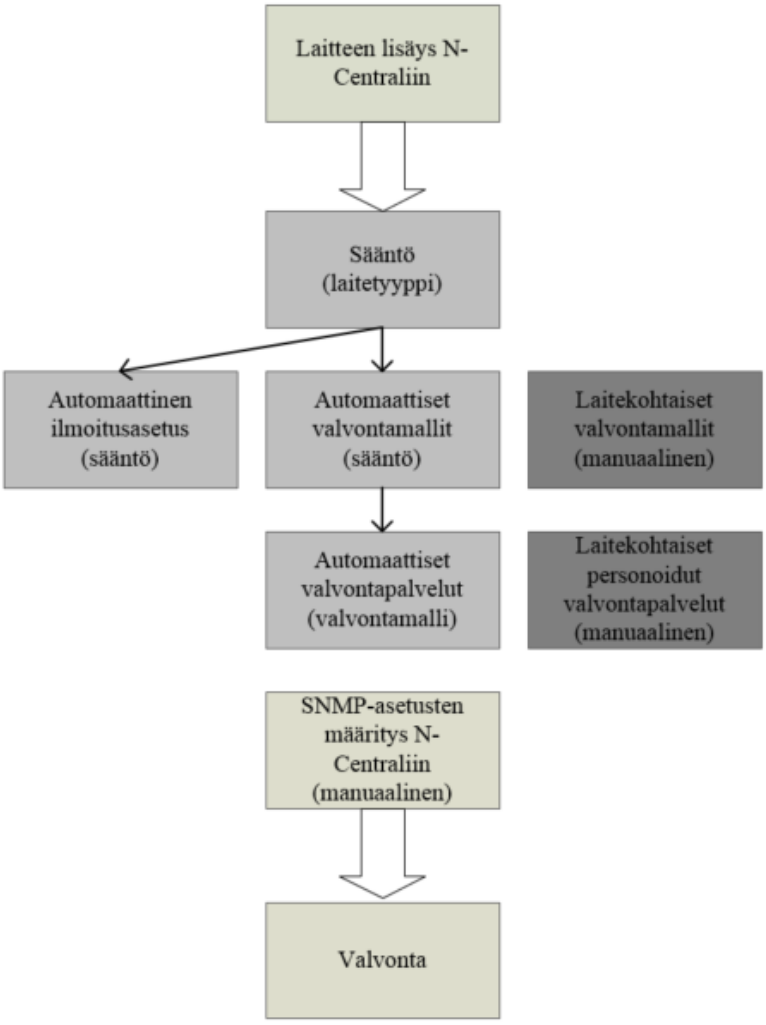
Valvonnan käyttöönotto N-Centralissa tapahtuu osin manuaalisesti ja osin automaattisesti. Valvonnan toteutus aloitetaan lisäämällä laite N-Centraliin. Palvelimen tapauksessa asennetaan luotain, joka on yhteydessä N-Central-palvelimeen. Verkkolaite tuodaan N-Centraliin käyttäen laitteen IP-osoitetta (kuva 6).



KUVA 6. Verkkolaitteen lisäys N-Centraliin

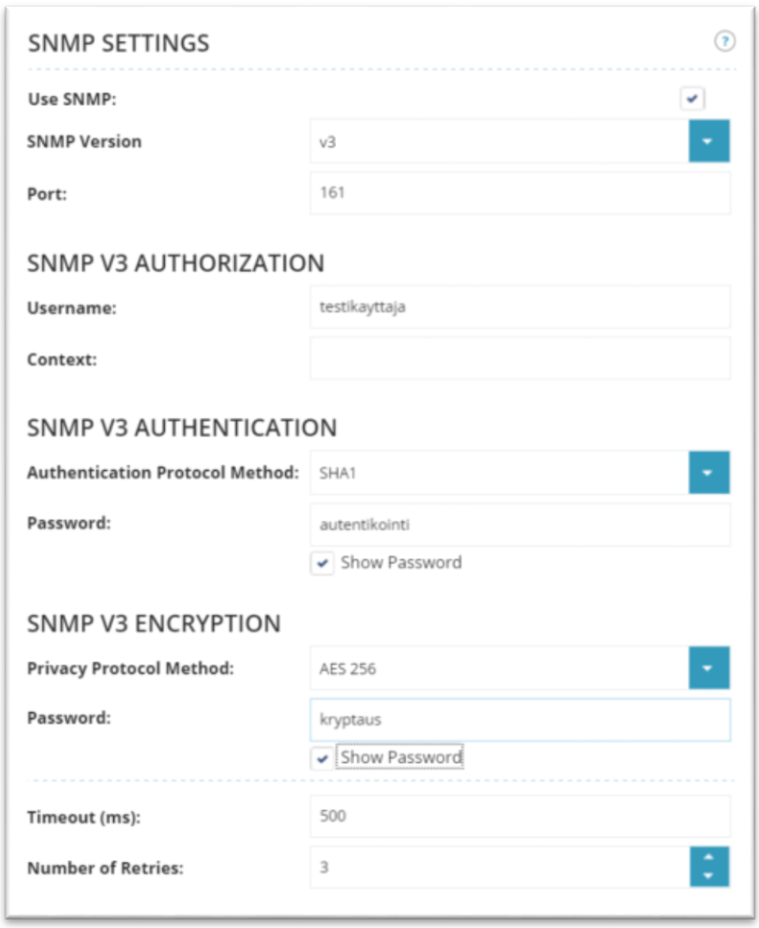
Laitteen lisäyksen jälkeen N-Central asettaa säännön laitteelle sen laitetyypin perusteella. Laitetyyppi voidaan myös asettaa manuaalisesti. Sääntö määrää minkälaisia valvontamalleja laitteelle asetetaan. Valvontamalli pitää sisällään useita valvontapalveluita. Esimerkkinä on valvontamalli Cisco hardware status, joka pitää sisällään suorittimen, tuulettimen, muistin ja virtalähteen valvontapalvelut. Hälytysasetuksia voidaan muuttaa valvontaan sopivaksi ja ne otetaan käyttöön sääntöjen kautta. Valvonnan käyttöönottoprosessi on alla myös kuvana (kuvio 4).

Hälytysasetuksissa määritetään kenelle ilmoitukset menevät ja kuinka usein. Opinnäytetyön toteuttamisen aikana hälytykset lähetetään kolmihenkiselle valvontatiimille, jonka jäsenet reagoivat hälytyksiin ja delegoivat tapauksia eteenpäin muille työntekijöille. Kun valvontainformaatiota on saatu riittävän pitkältä ajalta, voidaan raja-arvoja entisestään tiukentaa, jonka jälkeen hälytykset voidaan ohjata suoraan Triuvaren it-tuen sähköpostiin. Valvontailmoituksen analysointi vähentää turhien hälytysten määrää, joten it-tuki ei rasitu liikaa hälytyksistä.



KUVIO 4. Valvonnan käyttöönottoprosessi

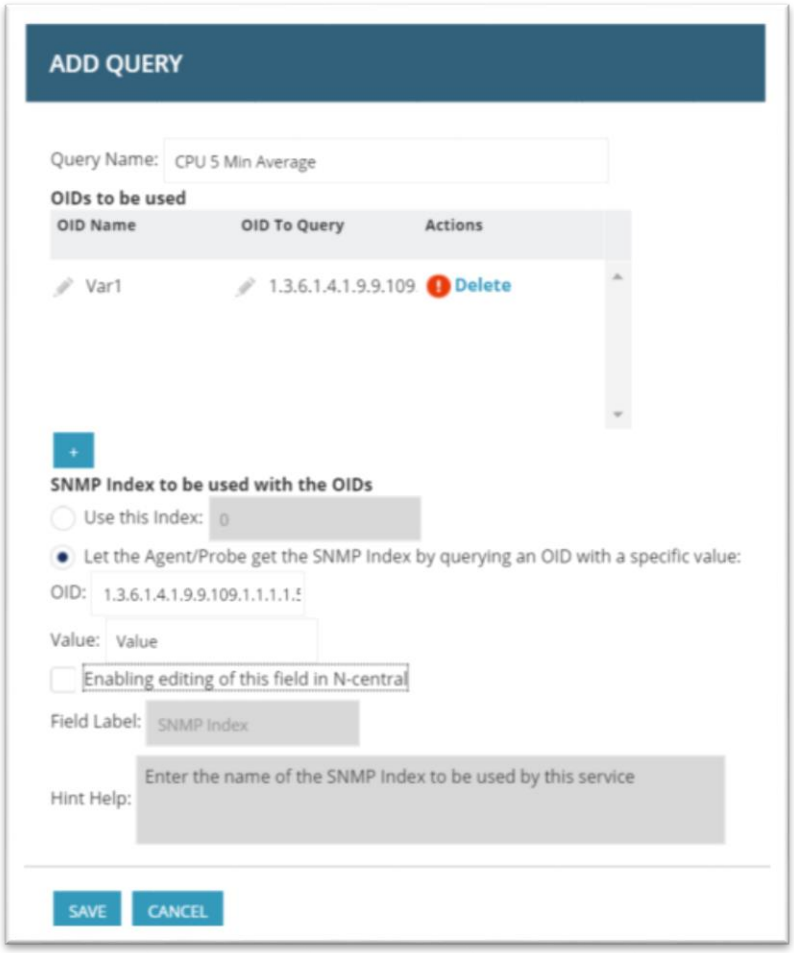
SNMP-valvonta vaatii laitteelta ja N-Centralilta toisiaan vastaavat asetukset (kuva 7). Niissä määritetään SNMP:n versio ja portti, joka on oletuksena UDP-portti 161. Valtuutusta varten tehdään käyttäjä. Todennusta varten valitaan protokolla, joita N-Centralissa on valittavissa kaksi: MD5 ja AES1. Sen lisäksi valitaan salausprotokollaksi joko DES tai AES. Verkkolaitteille asetetaan identtiset asetukset.



Kuva 7. N-Centralin SNMP-asetusten määritys

Suurin osa valvontainformaatiosta saadaan N-Centralin monipuolisten valmiiden valvontamallien perusteella. Palvelinten kohdalla ei ole käytössä kustomoituja valvontamalleja tai palveluita. Liite 1 sisältää yleisimmin käytössä olevat valvontamallit.

Verkkolaiteita varten luodaan valvontamalli jokaista valvottavaa laitetyyppiä kohden. Verkkolaitteiden valvontamallien valvontapalvelut ovat N-Centralin kehittämiä. Jatkokehityksenä aiotaan luoda laitteille kustomoituja valvontapalveluita, joiden avulla saadaan edistyneemmiltä laitteilta enemmän tietoa (kuva 8). Esimerkiksi Ciscon ASA 5512-X:n lämpötilaa ja tuulettimien tilaa on mahdollista valvoa.



KUVA 8. Kustomoidun valvontapalvelun luonti N-Centralissa

Kustomoitujen valvontapalveluiden tekemisen tueksi täytyy hankkia SNMP-selainohjelma, jonka avulla laitteilta voidaan hankkia objektitunnisteet, joiden perusteella kustomoidut palvelut tehdään. Toisena vaihtoehtona on käyttää Linux-palvelinta SNMP-informaation keräämiseen.

6 POHDINTA

Opinnäytetyön tavoitteen mukaisesti selvitettiin Triuvare Oy:lle miten N-Centralissa voidaan ottaa käyttöön SNMP-valvonta asiakkaiden verkkolaitteille ja miten palvelinten valvontaa voisi hienosäätää. Saatiin tehtyä valvonta, jonka avulla voidaan tarjota asiakkaille parempaa palvelua sekä säästää Triuvaren ja asiakkaan kustannuksissa.

Opinnäyteyön puitteissa verkkolaitevalvonta saatiin toimintaan höydyntämällä N-Centralin omia valvontamalleja ja palveluita. Laitevalvonta helpottaa Triuvaren työntekijöiden työtä, sekä säästää aikaa ja vähentää kustannuksia. Asiakkaiden laitteiden toiminta on turvattu aiempaa paremmin.

Sekä teorian, että toteutuksen osalta opinnäytetyö oli tekijälle haastava. Protokollan pitkän historian ja suhteellisen vähäisen kehityksen vuoksi iso osa dokumenteista ovat vanhoja, jo 1990-luvulta. Ne keskittyvät pääsääntöisesti varhaisten versioiden toimintaan. Yleisellä tasolla SNMPv3-protokollaa ei ole maailmalla otettu niin laajasti käyttöön kuin kannattaisi, joka on tietoturvan kannalta huolestuttavaa. Osasyynä sen käyttöönoton hitauteen on varmasti ollut dokumentaation vähyys. N-Centralin ei maksullisuutensa takia hallinta-asemana ole kovin tunnettu. Tiedonhaku N-Centralista verrattuna esimerkiksi Cactiin ja Nagiokseen on huomattavasti haastavampaa. Tiedon vähyyden vuoksi toteutus tapahtuikin pitkälti yrityksen ja erehdyksen kautta.

Jatkokehityksenä valvontaan voisi ottaa lisää laitteita, kuten verkkoasemia, Ciscon Merakeita ja enemmän erilaisia kytkimiä ja palomuureja. Valvontaprosessista kannattaisi myös tehdä selkeä ohjeistus, jotta muutkin työntekijät osaavat ottaa valvonnan laitteilla käyttöön. Suuren laitemäärän vuoksi voidaan todeta, että asiakkaiden kaikkien eri laitetyyppien valvonnan käyttöönottaminen opinnäytetyön puitteissa olisi ollut liian iso kokonaisuus. Valvontaan tällä erää valittujen laitteiden osalta opinnäytetyön toteutus sujui hyvin.

LÄHTEET

Case, J., Fedor, M., Schoffstall, M. & Davin, J. 1990. RFC-dokumentti. Cambridge: Massachusettsin teknillinen korkeakoulu. Luettu 2.1.2016. https://www.ietf.org/rfc/rfc1157.txt

Cisco Networking Basics: What You Need To Know. 2011. Blogi. Luettu 4.4.2016. http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/networking_basics/index.html

Hakala, M. & Vainio M. 2002. Tietoverkon rakentaminen. Porvoo: WS Bookwell.

Liu, A. 2011. Firewall Design and Analysis. Computer and Network Security - Vol. 4. River Edge, New Jersey: World Scientific Publishing Co.

Mauro, D. & Schmidt, K. 2005. Essential SNMP. Kalifornia: O'Reilly Media Oy.

N-Central is software for better IT service. 2016. N-Central N-Ablen esittely. Kanada: N-Central N-Able. Luettu 9.3.2016. http://www.n-able.com/products/n-central

Open Source Server Monitoring Tools– Cacti, Zabbix, Nagios. 2012. Blogi. Iso-Britannia: CloudStats.me. Luettu 20.1.2016. https://cloudstats.me/2015/08/08/open-source-server-monitoring-tools-cacti-zabbix-nagios/

Simoneau, P. 1999. SNMP network management. New York: McGraw-Hill.

Tilner, J. N-Central New Look and Feel. 2015. Blogi. Kanada: N-Central N-Able. Luettu 9.3.2016. http://blog.n-able.com/n-central-new-look-and-feel/

LIITTEET

Liite 1. Valvottavat ominaisuudet laitetyypeittäin

Valvottavan laitteen tyyppi	**Valvottava ominaisuus**
Palvelin	Aktiivihakemiston tila
Palvelin	DHCP:n tila
Palvelin	DNS:n tila
Palvelin	Levy
Palvelin	Muisti
Palvelin	Päivitysten tila
Palvelin	SQL:n toiminta
Palvelin	Suoritin
Palvelin	Tuuletinten tila
Palvelin	Varmistusten tila
Palvelin	Virtalähteen tila
Palvelin	Virustorjunnan tila
Palvelin	Yhteys N-Central-palvelimeen
Palomuuri/Kytkin	Muisti
Palomuuri/Kytkin	Virtalähde
Palomuuri/Kytkin	Yhteys N-Central-palvelimeen
Palomuuri	ASDM:n versio
Palomuuri	Käytettävyysaika
Palomuuri/Kytkin	Ohjelmistoversio
Palomuuri	Pakettien hävikki
Palomuuri	Porttien tila
Palomuuri/Kytkin	Suoritin
Palomuuri/Kytkin	VPN-putkien määrä