Hewlett-Packard Intelligent Management Center verkonhallintajärjestelmän käyttöönotto ja testaaminen

Petri Toropainen

Opinnäytetyö
Marraskuu 2012

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) TOROPAINEN, Petri	Julkaisun laji Opinnäytetyö	Päivämäärä 12.11.2012
	Sivumäärä 69	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty (X)

Työn nimi
Hewlett-Packard Intelligent Management Center verkonvalvontajärjestelmän käyttöönotto ja testaaminen

Koulutusohjelma
Tietotekniikan (Tietoverkkotekniikan) koulutusohjelma

Työn ohjaaja(t)
NARIKKA, Jorma

Toimeksiantaja(t)
Puolustusvoimien Johtamisjärjestelmäkeskus.
ALANKO, Jukka

Tiivistelmä

Opinnäytetyön tarkoituksena oli käyttöönottaa Hewlett-Packardin Intelligent Management Center verkonhallintajärjestelmä ja testata sen perusominaisuuksia. Työ toteutettiin Jyväskylän Ammattikorkeakoulun SpiderNet-tietoverkkotekniikanlaboratoriossa. Työn toimeksiantajana oli Puolustusvoimien Johtamisjärjestelmäkeskus.

HP IMC järjestelmä asennettiin VMware ESXi -virtuaalipalvelimelle, jonka käyttöjärjestelmänä oli Windows Server 2008 R2. Kyseinen palvelin liitettiin SpiderNet-laboratorioverkon laitteisiin.

Työssä testattiin HP IMC -järjestelmän ominaisuuksista eri Auto Discovery -haku tavat, laitteiden hallinta SNMPv3- ja SSH-protokollien avulla, laitteiden asetusten hallinta, laitteiden ohjelmiston hallinta ja VLAN-verkkojen hallinta. Kyseisiä ominaisuuksia testattiin Cisco Systems, Extreme Networks, Hewlett-Packard ja Juniper Networks -laitteilla.

Suoritettujen testauksien perusteella osassa IMC-järjestelmän ominaisuuksien toiminnasta löytyi virheitä, jotka estävät kyseisten ominaisuuksien käyttämisen osalla laitteista. Cisco Systems, Hewlett-Packard ja Juniper Networks -laitteet olivat hyvin tuettuja, kun IMC-järjestelmän tuki Extreme Networks -laitteille rajoittui pelkkiin valvonta ominaisuuksiin.

Työssä saatiin käyttöönotettua toimiva IMC-verkonhallintajärjestelmä ja suoritettujen testausten tulosten perusteella voi työn toimeksiantaja jatkaa järjestelmän käyttöönottoa omassa ympäristössään.

Avainsanat (asiasanat)
Verkonvalvonta, SNMP, MIB, Intelligent Management Center, IMC, SpiderNet, ITIL

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
TOROPAINEN, Petri	Bachelor´s / Master's Thesis	12.11.2012
	Pages 69	Language Finnish
		Permission for web publication (X)

Title
Hewlett-Packard Intelligent Management Center deployment and testing

Degree Programme
Data Network Technology

Tutor(s)
NARIKKA, Jorma

Assigned by
Finnish Defence Forces C4 Agency.
ALANKO, Jukka

Abstract

The purpose of this thesis was to deploy Hewlett-Packard Intelligent Management Center network management system and test its basic features. This thesis was assigned by Finnish Defense Forces C4 Agency and it was implemented at JAMK University of Applied Sciences and the SpiderNet datanetwork laboratory there.

HP IMC system was installed on VMware ESXi virtual server, running Windows Server 2008 R2 operating system. This server was attached to SpiderNet laboratory network.

The tested HP IMC features were Auto Discovery search, device management using SNMPv3- and SSH-protocols, device configuration management, device software library and VLAN network management. These features were tested using two Cisco Systems switches and one Cisco router, one Extreme Networks switch, one Hewlett-Packard switch and five Juniper Networks routers.

Based on the testing, some problems were found in IMC features, which prevent using those features with some devices. Cisco Systems, Hewlett-Packard and Juniper Networks devices were well supported.

Fully working network management systems was achieved in this thesis and based on outcome of this study, the assigner can continue their work deploying IMC.

Keywords
Networkmonitoring, SNMP, MIB, Intelligent Management Center, IMC, SpiderNet, ITIL

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

ACL	Access List
ARP	Address Resolution Protocol
CCTA	Central Computing and Telecommunications Agency
CMDB	Configuration Management Database
CMS	Configuration Management System
FTP	File Transfer Protocol
HP	Hewlett-Packard
IETF	Internet Engineering Task Force
IMC	Intelligent Management Center
IP	Internet Protocol
ISO	International Organization For Standardization
ITIL	Information Technology Infrastructure Library
MIB	Management Information Base
NMS	Network Management Station
OID	Object Identifier
PVJJK	Puolustusvoimien Johtamisjärjestelmäkeskus
RFC	Request for Comments
SCP	Secure Copy Protocol
SFTP	SSH File Transfer Protocol
SGMP	Simple Gateway Management Protocol
SMI	Structure of Management Information

SNMP	Simple Network Management Protocol
SOM	Service Operation Module
SP	Service Pack
SQL	Structured Query Language
SSH	Secure Shell
TCL	Tool Command Language
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
XML	Extensible Markup language

1 TYÖN KUVAUS

1.1 Työn tavoite

Opinnäytetyön tavoitteena oli ottaa käyttöön Hewlett-Packardin älykäs hallintakeskus (Intelligent Management Center, IMC) verkonhallintaohjelmisto SpiderNet-laboratorio ympäristössä, testata ohjelmiston yhteensopivuutta eri laitevalmistajien laitteiden kanssa ja ohjeistaa sen käyttöönotossa huomioon otettavista asioista. Toimeksiantaja opinnäytetyössä oli Puolustusvoimien Johtamisjärjestelmäkeskus (PVJJK) ja tarkoituksena oli tuottaa PVJJK:n henkilökunnalle käyttöönotto-opas HP IMC verkonhallintajärjestelmästä.

Tässä työssä tarkoituksena oli myös perehtyä ITIL palveluiden hallintaan ja minkälaisia vaatimuksia se asettaa verkonhallinnan toteuttamiselle.

1.2 Puolustusvoimien Johtamisjärjestelmäkeskus

Puolustusvoimien Johtamisjärjestelmäkeskus (PVJJK) on pääesikunnan alainen laitos. Sen toiminta on käynnistynyt 1.1.2007. Puolustusvoimien Internet-sivuilla PVJJK:n tehtävä on kuvattu seuraavasti:

> *Sen tehtävänä on luoda puolustushaaroille ja aselajeille niiden tarvitsemat johtamisedellytykset valmiuden eri vaiheissa. PVJJK kehittää ja ylläpitää puolustusvoimien integroitua tiedustelu-, valvonta- ja johtamisympäristöä sekä tuottaa hallinnolliset tietopalvelut koko puolustushallinnolle, sekä soveltuvin osin myös muulle valtionhallinnolle. (puolustusvoimien johtamisjärjestelmäkeskus 2008.)*

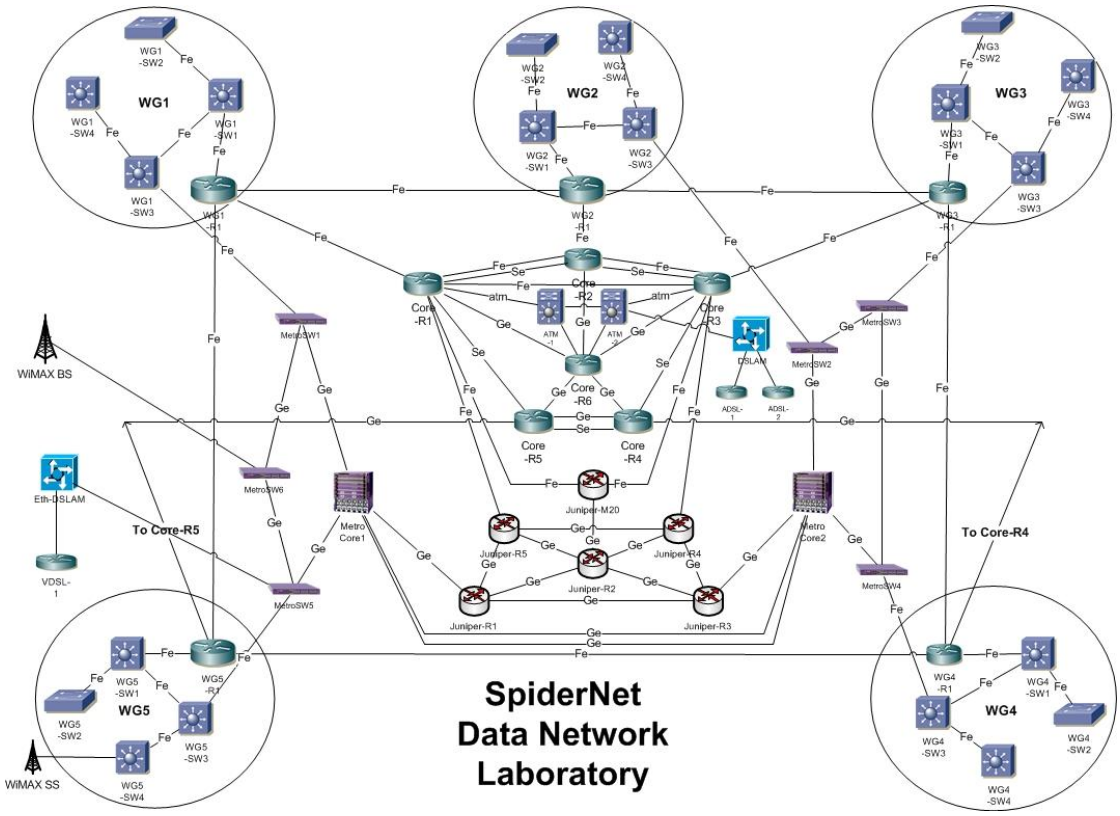
Puolustusvoimien johtamisjärjestelmäkeskuksessa työskentelee noin 750 työntekijää, joista osa on sotilaita ja osa siviilihenkilöitä. Se toimii 22 paikkakunnalla. PVJJK:n organisaatio muodostuu esikunnasta, palveluyksiköstä, hankeyksiköstä, verkostopuolustuksen kehittämiskeskuksesta ja verkkoyksiköstä, joka jakautuu kolmeen alueelliseen johtamisjärjestelmäkeskukseen. Verkkoyksikkö on suurin PVJJK:n yksikkö, ja

siellä työskentelee n. 400 henkilöä ympäri Suomen. (puolustusvoimien johtamisjärjestelmäkeskus 2008.)

1.3 Työn suorittaminen SpiderNet-laboratorioympäristössä

Tietoturvasyistä opinnäytetyössä toteutettava HP Intelligent Management Center verkonhallintajärjestelmä asennettiin ja testattiin Jyväskylän ammattikorkeakoulun SpiderNet-tietoverkkotekniikan laboratoriossa.

SpiderNet on Jyväskylän ammattikorkeakoulun tietoverkkotekniikan laboratorioympäristö. SpiderNetiä on kehitetty yli kymmenen vuotta ja sitä kehitetään edelleen sisältämään uusimpia operaattoreiden ja palveluiden tarjoajien käyttämiä tekniikoita. Kuviossa 1 on SpiderNet-laboratorioverkon topologiakuva. SpiderNet-laboratorioverkko koostuu Cisco Systems, Juniper Networksin, Extreme Networksin ja Zhonesin kytkimistä ja reitittimistä. (SpiderNet 2009.)



KUVIO 1. SpiderNet-laboratorioverkon topologia (SpiderNet 2009)

2 ITIL JA VERKONHALLINTA

2.1 Yleistä

Yritysten ja organisaatioiden eri toiminnot tukeutuvat vahvasti tietoverkkoihin ja käyttävät tietoverkkojen tarjoamia palveluita päivittäisessä toiminnassaan. Tämän vuoksi niillä on suuri merkitys yritysten ja organisaatioiden toimintaan.

Verkonhallinnalla on tärkeä rooli siinä, että nämä tietoverkkojen tarjoamat palvelut toimivat suunnitellulla tavalla, ongelmat verkossa havaitaan ja havaittuihin ongelmiin pystytään reagoimaan siten, että vaikutukset tietoverkkojen tarjoamiin palveluihin ovat mahdollisimman pienet.

Information Technology Infrastructure Library, eli ITIL on kokoelma parhaita käytäntöjä IT-palveluiden hallintaan ja se sisältää ohjeita ja käytäntöjä, jotka on hyvä ottaa huomioon verkonhallinnan toteuttamisessa.

2.2 ITIL

ITIL on osa Best Practices -julkaisuja. Se ei ole standardi, jota on noudatettava, vaan jokainen organisaatio voi soveltaa näitä käytäntöjä organisaation erityispiirteet huomioonottaen. ITIL toimii hyvänä lähtökohtana ja apuna organisaatioille, jotka haluavat saavuttaa ISO/IEC 20000 standardin mukaisen sertifioinnin. (ITIL Service Operation 2011, 3.)

ITILin uusin versio on julkaistu vuonna 2011, se koostuu viidestä (5) ydinjulkaisusta. Ydinjulkaisujen lisäksi on täydentäviä julkaisuja, joissa on yksittäisille toimialoille tai tietyn tyyppisille organisaatioille suunnattua ohjeistusta. (ITIL Service Operation 2011, 3.)

2.3 ITILin historia

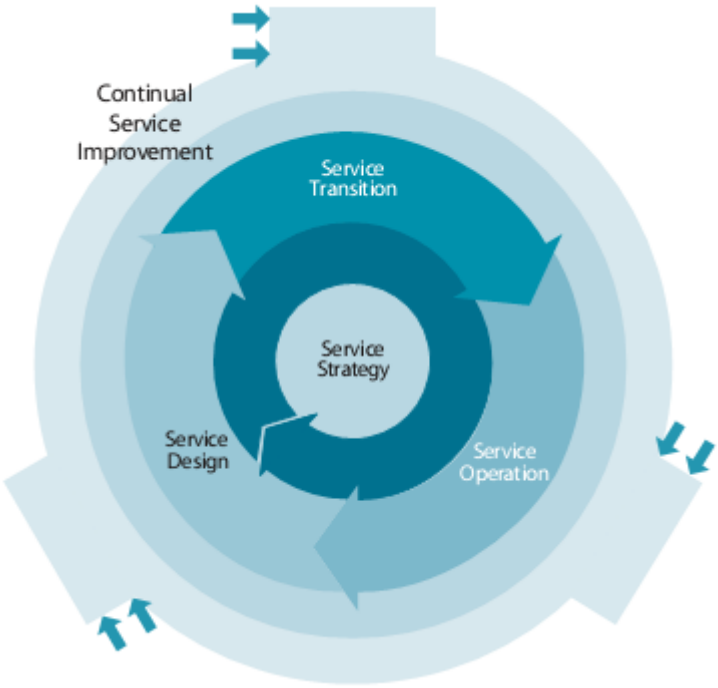
ITILin kehitys on aloitettu 1980-luvun lopulla, sen on kehittänyt Ison-Britannian hallituksen virasto nimeltään CCTA (Central Computing and Telecommunications Agency). ITIL kehitettiin, koska Iso-Britannian hallituksen IT-palveluiden taso ei ollut riittävä, joten tarvittiin keino, jolla saavutettiin parempi palveluiden laatu ja pienemmät kustannukset. (History of ITIL n.d.)

Aluksi ITIL koostui kirjojen kokoelmasta, joista jokainen opasti tietyn IT-palveluidenhallinta osa-alueen toteuttamisessa. Tämä alkuperäinen kirjasto kasvoi kattamaan yli 40 kirjaa. ITILin versio 2 julkaistiin vuonna 2001, se koostui yhdeksästä (9) kirjasta ollen kohdistetumpi tuote. ITILin versio 3 julkaistiin vuonna 2007. Versiossa 3 prosesseihin perustuvaa lähestymistapaa laajennettiin IT-palveluiden elinkaarimallilla kattamaan mm. ulkoistuksesta ja pilvipalveluista johtuvat lisääntyneet palveluiden hal-

linnan haasteet. Versio 3 sisältää myös viisi (5) ydinjulkaisua, kuten uusin vuonna 2011 julkaistu versio. (The Official Introduction to the ITIL Service Lifecycle 2007, 3.)

2.4 ITILin kehysrakenne

ITILin kehysrakenne perustuu IT-palvelun elinkaaren viiteen (5) vaiheeseen. Nämä vaiheet ovat palvelustrategia (Service Strategy), palvelun suunnittelu (Service Design), palvelutransitio (Service Transition), palvelutuotanto (Service Operation) ja jatkuva palvelun kehittäminen (Continual Service Improvement). Kuviossa 2 on kuvattu ITILin kehysrakenne. (ITIL Service Operation 2011, 3.)



KUVIO 2. ITILin kehysrakenne (ITIL Service Operation 2011, 3)

Jokainen ITILin ydinjulkaisu tarjoaa ohjeistusta kyseisen vaiheen toteuttamisessa tarvittavista periaatteista ja prosesseista. ITIL kehysrakenteessa palvelustrategia on keskellä ja palvelun toteuttaminen, palvelun suunnittelu ja palvelutransitio elinkaarenvaiheet kiertävät keskustaa. Jatkuva palvelun kehittäminen ympäröi näitä kaikkia ja tukee jokaista palvelun elinkaaren vaihetta. (ITIL Service Operation 2011, 3.)

Palvelustrategia (Service Strategy)

Palvelustrategia-julkaisussa opastetaan palveluiden hallinnan suunnittelussa. Kaikki alkaa organisaation tavoitteiden ja asiakkaan tarpeiden ymmärtämisellä. Käsiteltäviä aiheita ovat mm. markkinoiden kehittyminen, palvelukokonaisuuksienhallinta ja strategiset riskit. (ITIL Service Operation 2011, 6.)

Tässä palvelun elinkaaren vaiheessa yritys tekee suuria suuntalinjauksia siitä, minkälaisia palveluita tuotetaan, ketkä ovat mahdollisia asiakkaita ja mikä on palvelun ansaintamalli.

Palvelusuunnittelu (Service Design)

Palvelusuunnitteluvaiheessa opastetaan palveluiden ja niiden hallinnan käytäntöjen suunnittelemisessa ja kehittämisessä. Se kattaa suunnitteluperiaatteet ja käytännöt, joilla saadaan muunnettua strategiset tavoitteet palvelukokonaisuuksiksi. Tässä palvelun elinkaarenvaiheessa suunnitellaan toteutettava palvelu ja sovitaan asiakkaan kanssa palvelun tasosta. (ITIL Service Operation 2011, 6-7.)

Palvelutransitio (Service Transition)

Palvelutransitio-julkaisussa opastetaan, kuinka palveluiden tuotantokäyttöönottaminen voidaan suorittaa hallitusti ja riskit huomioon ottaen. Lisäksi julkaisussa opastetaan palveluiden hallinnan siirtämisessä asiakkaalta palvelun tarjoajalle. (ITIL Service Operation 2011, 7.)

Verkonhallinnan kannalta tässä palvelun elinkaarenvaiheessa käynnistetään palveluita, joita tullaan valvomaan ja mahdollisesti siirrytään, jostain vanhasta tekniikasta uuteen suunnitellusti ja hallitusti. (ITIL Service Operation 2011, 7.)

Palvelutuotanto (Service Operation)

Palvelutuotanto julkaisussa keskitytään palveluiden jokapäiväisen toiminnan hallintaan. Tässä palvelun elinkaarenvaiheessa pyritään pitämään palvelu toiminnassa sovitun palvelutason mukaisesti ja kustannustehokkaasti. (ITIL Service Operation 2011, 7.)

Tämä vaihe on verkonhallinnan henkilöstön päivittäistä toimintaam, ja ITIL palvelutuotanto opastaa verkonvalvojia ja operaattoreita mm. palvelun saatavuuteen, kapasiteetin optimointiin ja ongelmien ratkaisuun liittyvien päätösten tekemisessä. (ITIL Service Operation 2011, 7.)

Jatkuva palvelun parantaminen (Continual Service Improvement)

Tässä ITIL-julkaisussa kuvataan parhaita käytäntöjä palvelun kehittämiseen. Siinä yhdistetään laadunhallinnan, muutoksenhallinnan ja kapasiteetin lisäämisen käytäntöjä, periaatteita ja menetelmiä. Jatkuva palvelun parantaminen tukee kaikkia palvelun elinkaaren vaiheita, ja palautetta jokaisesta palvelun elinkaaren vaiheesta tulisi käyttää palvelun hallinnan parantamiseksi. (ITIL Service Operation 2011, 7.)

2.5 ITIL verkonhallinnan näkökulmasta

Verkonhallinta on tärkeässä roolissa IT palveluiden tuottamisessa, koska palvelut ovat riippuvaisia tietoliikenneyhteyksien toiminnasta ja verkonhallinnan vastuulla on näiden tietoliikenneyhteyksiä tuottavien laitteiden valvonta ja hallinta. ITIL-palvelutuotanto julkaisussa esitellään prosesseja, jotka ovat sovellettavissa verkonhallinnan käyttöön. Nämä prosessit ohjaavat toimintaa mm. tapahtumien ja ongelmien hallinnassa. (ITIL Service Operation 2011, 36-37.)

Verkonhallinnan tehtäviä ovat myös muutoksen- ja konfiguraationhallinta. Nämä prosessit ovat kuvattu ITIL-palvelutransitio-julkaisussa. Näiden prosessien yhteydessä esitellään konfiguraationhallintajärjestelmä (Configuration Management System,

CMS) ja konfiguraationhallintatietokanta (Configuration Management Database, CMDB), jotka sisältävät tietoja verkossa olevista laitteista ja palveluiden riippuvuuksista näihin laitteisiin. (ITIL Service Transition 2007, 65-69).

Verkonhallinnan henkilökunnan tulee osallistua myös jatkuvaan palveluiden kehittämiseen ja palvelusuunnitteluun, koska heillä on näkemystä palveluiden tuottamisesta käytännön kannalta.

3 SNMP

3.1 Yleistä

Yksinkertainen verkonhallintaprotokolla (Simple Network Management Protocol, SNMP) on protokolla, jolla voidaan valvoa ja hallita mm. reitittimien, kytkinten, Windows- ja Unix-palvelimien, virtalähteiden yms. toimintaa. Myös ohjelmistojen, kuten www-palvelimien ja tietokantojen toimintaa on mahdollista valvoa SNMP:llä. (Mauro & Schmidt 2005, 1-2.)

Ensimmäinen versio SNMP:stä on julkaistu vuonna 1988. Se kehitettiin täyttämään kasvava tarve standardoidulle tavalle hallita tietoverkkojen laitteita. Sen edeltäjä on Simple Gateway Management Protocol (SGMP), joka on tarkoitettu internetin reitittimien hallintaan. (Mts. 1-2.)

SNMP-standardit on määritelty The Internet Engineering Task Force (IETF) organisaation toimesta, Request For Comments (RFC) -dokumenteissa. SNMP versio 1 on määritelty RFC 1157 dokumentissa ja se on IETF:n historiallinen standardi. Nykyinen voimassa oleva SNMPv3 standardi on määritelty RFC 3410 - RFC 3418 -dokumenteissä. (Mts. 2.)

Vaikka SNMP:n versio 3 on julkaistu jo vuonna 2002, on SNMP:n edelliset versiot (versio 1 ja 2c) vielä yleisesti käytössä niiden turvallisuuspuutteista huolimatta.

3.2 SNMP-arkkitehtuuri ja tiedonsiirto

SNMP-arkkitehtuurissa on kahdenlaisia laitteita, joko verkonhallinta-asemia (NMS, Network Management Station) tai verkkoelementtejä. Verkonhallinta-asema suorittaa hallintasovellusta, joka valvoo ja hallitsee verkkoelementtejä. Verkkoelementti on valvottava tietoverkonlaite, kuten tietokone, reititin tai kytkin. Verkkoelementti sisältää ohjelmiston, joka suorittaa verkonhallinta-aseman pyytämiä toimintoja. Tätä verkkoelementissä sijaitsevaa ohjelmistoa kutsutaan agentiksi. Verkonhallinta-aseman ja verkkoelementin välillä tiedon siirrossa käytetään SNMP-protokollan mukaista liikennettä. (RFC 1157 1990.)

Verkonhallinta-asema on vastuussa tietojen kyselystä, asettamisesta ja trap-viestien vastaanottamisesta agenteilta. Kyselyssä verkonhallinta-asema lähettää kyselyviestin agentille pyytäen tältä jotain tietoa. Trap-viesti on tapa, jolla agentti voi kertoa verkonhallinta asemalla, että jotain on tapahtunut, esimerkiksi jonkin rajapinnan tila on vaihtunut. Verkonhallinta-asema vastaanottaa trap-viestin ja viestin sisältämien tietojen perusteella päättää tarvitaanko jatkotoimenpiteitä esimerkiksi hälytyksen tekeminen ja sähköpostin lähettäminen verkonylläpitäjälle. (Mauro & Schmidt 2005, 3-4.)

Verkkoelementin sisältämä agentti vastaa verkonhallinta-aseman lähettämiin kyselyihin ja lähettää trap-viestejä. Verkonhallinta-asema voi myös ohjata verkkoelementin tilaa lähettämällä sille set-viestejä. (Mts. 3-4.)

SNMP käyttää tiedonsiirrossa UDP-protokollaa (User Datagram Protocol). UDP on yhteydetön tiedonsiirtoprotokolla, ja se ei huolehdi pakettien perille pääsystä kuittauksien avulla kuten TCP-protokolla (Transmission Control Protocol). Tämä tekee UDP:stä epäluotettavamman, joten SNMP:n täytyy itse huolehtia tietojen perille-pääsystä ja uudelleen lähettämisestä, mikäli se on tarpeen. Yleensä SNMP:ssä tämä on hoidettu käyttämällä aikakatkaisua: jos SNMP-laite ei ole vastannut kyselyyn määräajassa, lähetetään kysely uudestaan. (Mts. 19–20.)

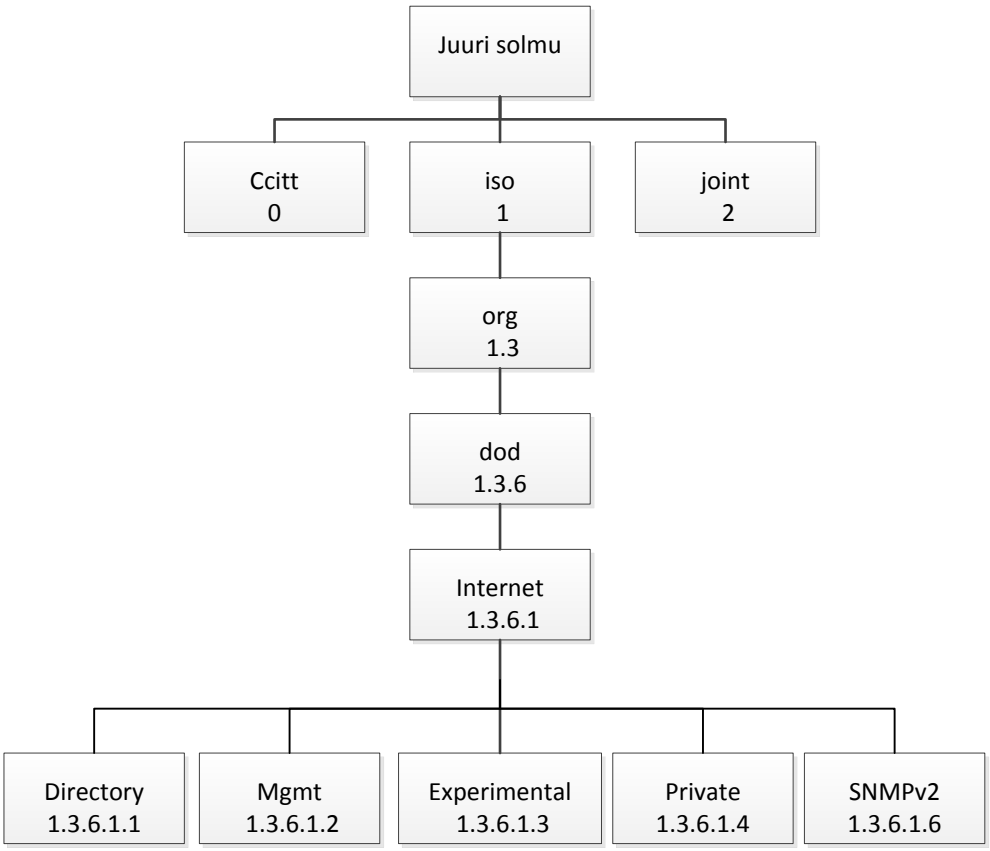
SNMP-protokolla käyttää UDP porttia numero 161 kysely-viestien lähettämiseen ja vastaanottamiseen, sekä porttia numero 162 trap-viestien lähettämiseen ja vastaanottamiseen. Kaikkien SNMP-protokollaa käyttävien laitteiden täytyy tukea näitä portteja, vaikka jotkin laitevalmistajat sallivat porttien vaihtamisen ylläpitäjän haluamiksi. (Mts. 20.)

3.3 Hallintatietojen rakenne

SNMP:ssä jokainen agentti sisältää useita tietoja kyseisestä verkkoelementistä. Yhtä tietoa kutsutaan hallituksi objektiksi. Management Information Base (MIB) on tietokanta, joka sisältää agentin tukemat hallittavat objektit. Näiden hallittujen objektien rakenteen määrittelee Structure of Management Information (SMI). Se määrittelee kuinka hallitutobjektit on nimetty ja minkälaisia datatyyppejä ne sisältävät. (Mauro & Schmidt 2005, 4 & 23.)

SMI:n versio 1 on määritelty RFC 1155 dokumentissa ja SMI:n versio 2 on määritelty RFC 2578 dokumentissa. SMI:n versio 2 määrittelee mm. uusia datatyyppejä ja kirjallisia merkintätapoja. (Mts. 23.)

Hallitut objektit tunnistetaan nimien avulla. Nämä nimet noudattavat hierarkkista Object Identifier (OID) nimeämistapaa. OID on sarja pisteellä eroteltuja lukuja, jotka pohjautuvat puun solmuihin. Tämän puun juurisolmu on nimeämätön ja sillä on kolme (3) lapsisolmua. Nämä lapsisolmut ovat ccitt, iso ja joint-iso-ccitt. Kuviossa 3 on esitetty tämän puun ylimmät tasot, kuviosta on poistettu SNMP:n kannalta tarpeettomat haarat. (RFC 1155.)



KUVIO 3. Hallintatietojen OID-puurakenne (Mauro & Schmidt 2005, 36)

SNMP hallitut objektit löytyvät alipuun 1.3.6.1, eli Internet solmun alta. OID-nimet voidaan myös ilmaista tekstimuodossa, jolloin 1.3.6.1 on toisin ilmaistuna iso.org.dod.internet. (Mauro & Schmidt 2005, 24.)

Internet-alipuun Mgmt-lapsisolmun (OID 1.3.6.1.2) alla on standardit hallitut objektit, kuten MIB-II. Private-solmun alla on laite- ja ohjelmistovalmistajien mahdollista varata oma alipuu, jonne he voivat toteuttaa laitekohtaisia hallittuja objekteja. Esimerkiksi Cisco Systemsin yksityinen alipuu on OID 1.3.6.1.4.1.9, ja sama ilmaistuna tekstimuodossa on iso.org.dod.internet.private.enterprise.cisco. (Mts. 24–25.)

MIB-II

MIB-II on tärkeä hallittujen objektien ryhmä, koska kaikkien SNMP:tä tukevien laitteiden on tuettava MIB-II hallittuja objekteja. Sen OID on 1.3.6.1.2.1 tai sanallisesti

ilmaistuna iso.org.dod.internet.mgmt.mib-2. Taulukossa 1. on lueteltu MIB-II alipuut, niiden OID:t ja lyhyt selostus alipuun tarkoituksesta. . (Mts. 35-37.)

TAULUKKO 1. MIB-II hallintaobjektien alipuut. (Mauro & Schmidt 2005, 36-37.)

Alipuun nimi	**OID**	**Kuvaus**
system	1.3.6.1.2.1.1	Määrittelee listan objekteja liittyen järjestelmän toimintaan, kuten järjestelmän nimi ja yhteyshenkilö.
interfaces	1.3.6.1.2.1.2	Ylläpitää tilatietoa jokaisen portin tilasta ja statistiikasta.
at	1.3.6.1.2.1.3	Osoitteenmuunnos-ryhmä on vanhentunut ja mukana vain yhteensopivuuden takaamiseksi.
ip	1.3.6.1.2.1.4	Ylläpitää tietoja monista IP-protokollaan liittyvistä asioista.
icmp	1.3.6.1.2.1.5	Ylläpitää tietoja ICMP:n virheistä, hylkäyksistä yms.
tcp	1.3.6.1.2.1.6	Ylläpitää tietoja TCP-yhteyksistä.
udp	1.3.6.1.2.1.7	Ylläpitää tietoja UDP:stä, mm. lähetetyt ja vastaanotetut datagrammit.
egp	1.3.6.1.2.1.8	Ylläpitää tietoja ulkoisista reititys protokollista.
transmission	1.3.6.1.2.1.10	Ei objekteja tällä hetkellä, muut media riippuvaiset MIB-tietokannat käyttävät tätä alipuuta.
snmp	1.3.6.1.2.1.11	Mittaa SNMP toteutuksen suorituskykyä, kuten lähetetyt ja vastaanotetut SNMP-paketit.

3.4 SNMP:n versiot ja niiden ominaisuudet

3.4.1 SNMP, versio 1 ja 2

SNMP:n ensimmäinen versio on määritelty RFC 1157 dokumentissä ja se on historiallinen standardi. SNMP:n versio 2 on julkaistu vuonna 1993. Se on määritelty RFC 3416–3418 dokumenteissa (Mauro & Schmidt 2005, 2-3.)

SNMP versioissa 1 ja 2 verkonhallinta-asema ja agentti tunnistavat luvallisen käytön käyttämällä yhteisö-nimiä (community). Nämä nimet toimivat salasanan tavoin, ja

jokainen SNMP viesti sisältää jonkin yhteisön kirjainyhdistelmän. Näillä yhteisönimillä rajoitetaan tietoihin pääsyä. Erilaisia yhteisö-nimiä on tietojen lukemiseen (read community), tietojen lukemiseen ja kirjoittamiseen (read-write community), sekä trap-viesteihin. Yhteisö-nimet siirretään verkossa selväkielisenä. Ne on siis mahdollista lukea helposti kaapatusta liikenteestä. (Mts. 21–23.)

3.4.2 SNMP, versio 3

SNMP:n versio 3 on voimassa oleva standardi ja sen mukanaan tuomat merkittävimmät uudistukset liittyvät tietoturvaan. Lisäksi SNMP versio 3 tuo mukanaan uusia termejä, joilla kuvataan SNMP:n toimintaa. Nämä termit poikkeavat melko paljon aiemmista versioista. (Mts. 73.)

SNMP versiossa 3 ei käytetä enää termejä verkonhallinta-asema ja agentti, vaan molempia kutsutaan SNMP-kokonaisuuksiksi (entity). Jokainen SNMP-kokonaisuus koostuu SNMP-moottorista (engine) ja yhdestä tai useammasta SNMP-sovelluksesta (application). (Mts. 74.)

SNMP:n version 3 tietoturvaa on parannettu mahdollisuudella käyttäjäkohtaiseen autentikointiin (user-based authentication) ja yksityisyyteen (privacy). Käyttäjäkohtainen autentikointi tarkoittaa sitä, että käytetään MD5 tai SHA -algoritmia käyttäjän autentikointiin, eikä salasanaa lähetetä selväkielisenä verkon yli. Yksityisyydellä tarkoitetaan mahdollisuutta salata SNMP-viesti käyttäen esimerkiksi DES-salausta. On siis mahdollista käyttää autentikointia ilman yksityisyyttä (authNoPriv), mutta ei yksityisyyttä ilman autentikointia (authPriv). Näitä tekniikoita käyttäen ei kaapatusta SNMP-paketista pystytä lukemaan mitään arkaluontoista, eikä varsinkaan salasanoja. On myös mahdollista käyttää SNMP:n versiota 3 ilman autentikointia ja yksityisyyttä (noAuthNoPriv). (Mts. 83–84.)

3.5 SNMP, trap-viesti

SNMP hallinta-aseman ja agenttien välinen tiedon siirto tapahtuu erilaisia operaatioita käyttäen. Verkonhallinnassa yksi tärkeimmistä operaatioista on trap-viesti. Se on agentin tapa kertoa verkonhallinta-asemalle, että jotain on tapahtunut. Trap-viestin lähde on agentti ja kohteena on agentille määritelty trap-kohde, yleensä verkonhallinta-asema. Verkonhallinta-asema ei kuittaa trap-viestin vastaanottamista agentille, joten agentti ei voi tietää onko verkonhallinta-asema vastaanottanut viestin. Mahdollisia syitä trap-viestin lähettämiseen ovat esimerkiksi laitteen portin tilan vaihtuminen tai reitittimen tuulettimen on rikkoutuminen. (Mauro & Schmidt 2005, 63.)

SNMP:n versio 2 tuo mukanaan Inform-toiminnan. Tämä Inform-viesti vastaa sisällöltään trap-viestiä, mutta Inform-viestin vastaanottaja lähettää kuittaus-viestin lähettäjälle. Tätä ominaisuutta voidaan käyttää kahden verkonhallinta-aseman välisessä viestinnässä. (Mts. 69.)

4 HP INTELLIGENT MANAGEMENT CENTER

4.1 Yleistä

Intelligent Management Center (IMC) on Hewlett-Packardin uusi verkonhallintajärjestelmä. Sillä voidaan valvoa ja hallita HP:n ja muiden valmistajien laitteita. IMC on suunniteltu palvelu orientoituneen-arkkitehtuurin (Service-Oriented Architecture) pohjalta. Se on modulaarinen ohjelmisto, johon voidaan lisätä uusia ominaisuuksia moduuleja asentamalla. (HP Intelligent Management Center 2012.)

Jokaisella verkkolaitevalmistajalla on omia verkonhallintajärjestelmiä, jotka on tarkoitettu heidän omien laitteiden hallitsemiseksi. Valmistajien omissa järjestelmissä on yleensä ongelmana puuttuva tuki muiden valmistajien laitteille. Lisäksi on saatavilla pelkkiä verkonvalvontaohjelmistoja, joilla vastaanotetaan laitteiden lähettämät hälytykset ja valvotaan niiden toimintaa. Verkonvalvonta ohjelmistolla ei pystytä teke-

mään muutoksia laitteiden asetuksiin, vaan muutokset vaativat jonkin muun ohjelmiston tai komentorivipohjaisen käyttöliittymän käyttämisen asetusmuutoksien tekemiseksi. HP IMC -järjestelmän tuki muiden laitevalmistajien laitteille, mahdollistaa muutoksien suorittamisen useiden eri valmistajien laitteille yhtä järjestelmää käyttäen.

4.2 Ominaisuudet

HP IMC yhdistää verkon tapahtumien- ja -hälytystenhallinnan, laitteiden asetusten hallintaan.

HP IMC -järjestelmästä on olemassa kaksi (2) eri versiota. Nämä versiot ovat Enterprise ja Standard. Standard-versiossa on mahdollista käyttää tietokantapalvelimena asennuspaketin mukana olevaa SQL-palvelinohjelmistoa, kun Enterprise-versiossa on käytettävä erillistä tietokantaa. Standard-versiossa on lisäksi rajoituksia sen käyttämisessä hierarkkisena verkonvalvonta-asemana. (HP Intelligent Management Center Installation Guide 2012, 3.)

HP IMC Standard versiossa vakiona olevia ominaisuuksia ovat muun muassa:

- Tuki laitteiden hallitsemiseksi SSH:lla, Telnetillä ja SNMP:llä
- Laitteiden asetusten ja ohjelmistojen hallinta
- Reaaliaikainen tapahtumien ja hälytysten hallinta
- Verkon ja laitteiden suorituskyvyn monitorointi ja raportointi
- Laitteiden pääsylistojen hallinta
- Turvallisuusuhkien hallinta
- Virtuaaliverkkojenhallinta
- Raportointi. (Mts. 1-9.)

Lisäksi IMC-järjestelmään on saatavilla lisämoduuleja, jotka tuovat lisäominaisuuksia laitteiden ja palveluidenhallintaan. Tällä hetkellä on saatavilla seuraavanlaisia lisämoduuleja:

- Palvelutuotannonhallinta (Service Operation Management)
- Langattomien-palveluidenhallinta (Wireless Service Manager)
- Puhe-palveluidenhallinta (Voice Service Manager)
- Käyttäjien pääsynhallinta (User Access Manager)
- Päätelaitteiden sisäänpääsynpuolustus (Endpoint Admission Defense)
- Käyttäjien käyttäytymisen auditointi (User Behavior Auditor)
- Palvelun laadunhallinta (QoS Manager)
- Verkonliikenteen analysaattori (Network Traffic Analyzer)
- MPLS VPN -hallinta (MPLS VPN Manager)
- Palveluiden terveydenhallinta (Service Health Manager). (Mts. 1-9.)

4.3 Laitteisto- ja ohjelmistovaatimukset

Laitteistovaatimukset

HP IMC-laitteistovaatimukset vaihtelevat halittavien laitteiden lukumäärän, kerättävien tietojen ja yhtäaikaisten käyttäjien määrän suhteen. Minimi vaatimuksena on 2.5Ghz kellotaajuudella toimiva 2-ydin prosessori tai kaksi 2.5Ghz kello taajuudella toimivaa prosessoria, 4Gb keskusmuistia ja 30Gb kiintolevy tilaa. Tällöin hallittavia laitteita voi olla enimmillään 200 kpl. (HP Intelligent Management Center Installation Guide 2012, 4-5.)

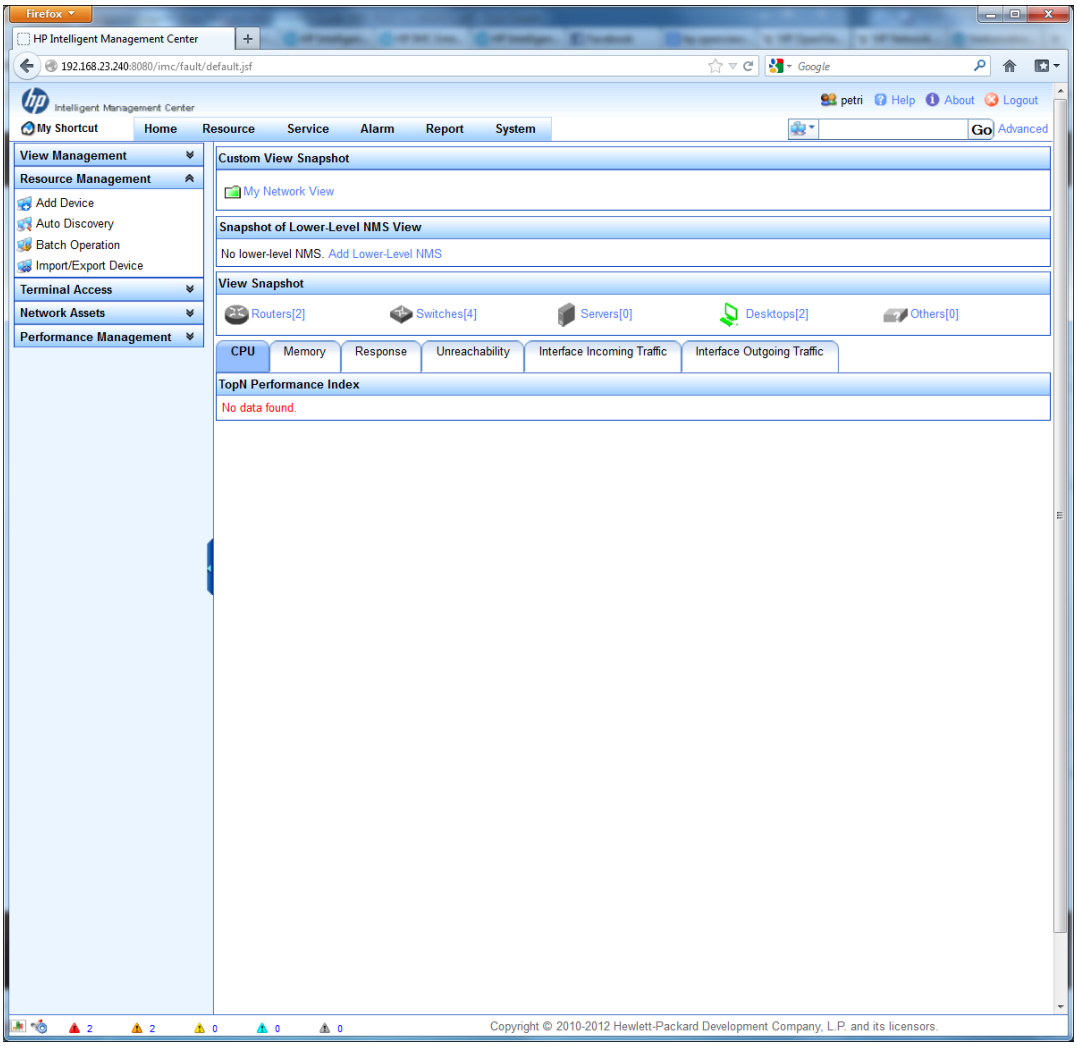
Ohjelmistovaatimukset

HP IMC-järjestelmä voidaan asentaa palvelimelle, jonka käyttöjärjestelmänä on Windows tai Linux. Tuetut Windows-käyttöjärjestelmät ovat Windows Server 2003, 2008 ja 2008 R2. Linux-käyttöjärjestelmistä tuettuina on ainoastaan Red Hat Enterprise Linux Server versiot 5 – 6.1. On suositeltua käyttää 64-bittistä käyttöjärjestelmää. (Mts. 6-7)

Lisäksi vaaditaan tietokanta, johon HP IMC-järjestelmä tallentaa tietonsa. Windows-alustalla voidaan käyttää SQL- tai MySQL-tietokantaa. Vastaavasti Linux-alustalla voidaan käyttää Oracle- tai MySQL-tietokantaa. HP IMC Standard -versio tukee sisäänrakennettua tietokantaa, joka voidaan asentaa IMC järjestelmän asennuksen yhteydessä. Tällöin asennetaan Microsoft SQL Server 2008 R2 Express tietokantapalvelinohjelmisto. (Mts. 25.)

4.4 Käyttöliittymä

HP IMC:n kaikkia ominaisuuksia käytetään web-pohjaisen käyttöliittymän kautta. Tuettuja selaimia ovat Mozilla Firefox ja Internet Explorer. HP IMC:n käyttöliittymä koostuu yläreunassa olevasta päävalikosta ja vasemmassa reunassa olevasta valikosta, sekä niiden alla ja vieressä olevasta tilasta, jossa näkyy tietoja halutusta asiasta. Kuviossa 4 on kuvankaappaus HP IMC Resource -näkymästä. IMC käyttöliittymä on samanlainen jokaisen ominaisuuden osalta, lukuun ottamatta kotisivua. Kotisivu on muokattavissa jokaisen käyttäjän tarpeiden mukaan ja siihen on mahdollista saada näkyviin käyttäjän useimmin tarvitsemia tietoja laitteista ja palveluiden tilasta.



KUVIO 4. HP IMC -käyttöliittymä

Sivun alareunassa olevat eriväriset kolmiot ilmaisevat eri vakavuusluokan aktiivisia hälytyksiä tai ilmoituksia. Niitä klikkaamalla pääsee selaamaan kyseisiä hälytyksiä.

HP IMC -järjestelmään on myös olemassa Android- ja Iphone-sovellukset, joilla pääsee käsiksi järjestelmän tietoihin älypuhelimella.

4.5 HP IMC -järjestelmän vaatimat portit

HP IMC -järjestelmän eri ominaisuudet käyttävät taulukossa 2 listattuja kuljetuskerroksen (Transport Layer) protokollia ja portteja. Liikennöinti näitä protokollia ja port-

teja käyttäen täytyy olla sallittu palomuureissa ja laitteiden pääsylistoissa (Access List, Acl).

TAULUKKO 2. IMC käyttämät TCP- ja UDP-portit

protokolla	**portti**	**käyttö**	**sijainti**
UDP	161	Laitteiden lisääminen IMC:hen. SNMP kyselyt.	Hallittava laite
TCP	22	SSH-hallinta	Hallittava laite
TCP	23	Telnet-hallinta	Hallittava laite
UDP	514, 515	Syslog	IMC-palvelin
UDP	162	SNMP trap	IMC-palvelin
TCP	8080	IMC HTTP web-sivu (vaihdettavissa)	IMC-palvelin
TCP	80443	IMC HTTPS web-sivu (vaihdettavissa)	IMC-palvelin
UDP	69	Asetusten ja ohjelmistojen hallinta TFTP	IMC-palvelin
TCP	20, 21	Asetusten ja ohjelmistojen hallinta FTP	IMC-palvelin

4.6 IMC:n tuki kolmannen osapuolen laitteille

HP ei ole julkistanut listaa mitkä IMC ohjelmiston ominaisuudet ovat tuettuja eri laitevalmistajien malleilla. Tästä syystä laitekohtainen tuki on kokeiltava erikseen jokaiselle laiteryhmälle. IMC järjestelmää on kuitenkin mahdollista laajentaa tukemaan lisää laitteita tekemällä itse omia komentotiedostoja (script).

Laitteiden hallitsemiseen HP IMC:n käyttämät komentotiedostot löytyvät palvelimelta hakemistosta:

“C:\Program Files\iMC\server\conf\adapters\”

Tämä hakemisto sisältää XML-, TCL- ja Perl-komentotiedostoja, joiden avulla IMC suorittaa toimintoja laitteilla. Kyseiset XML-tiedostot kuvailevat hakemistorakennetta, sekä TCL- ja Perl-komentotiedostojen sisältöä. TCL-komentotiedostot sisältävät

komennot, jonka avulla toimintoja suoritetaan laitteilla ja Perl-komentotiedostot suodattavat pois ylimääräiset merkit laitteiden palauttamasta tekstistä.

5 HP IMC:n KÄYTTÖÖNOTTO JA TESTIYMPÄRISTÖ

Tässä työssä tarkoituksena oli asentaa HP IMC-verkonvalvontajärjestelmä ja testata sen ominaisuuksia eri laitevalmistajien laitteilla. Testaaminen tapahtui asentamalla IMC-palvelinohjelmisto ja määrittelemällä sen asetukset, liittämällä IMC-palvelin testitopologiaan ja määrittelemällä laitteiden asetukset siten, että jokaisella testattavalla laitteella oli yhteys IMC-palvelimeen.

5.1 HP IMC -järjestelmän asennus

IMC ohjelmiston asennettiin Windows käyttöjärjestelmää käyttävälle palvelimelle, sisäänrakennetun SQL-tietokantapalvelinohjelmiston takia. Palvelimena käytössä oli SpiderNetin VMWare ESXi -virtuaalipalvelin, jossa oli käyttöjärjestelmänä Windows Server 2008 R2. Tämä virtuaalinen palvelin liitettiin SpiderNet-laboratorioverkkoon haluttuun laitteeseen ja topologiaan.

HP IMC:n toimintaa testattiin sen sisältämällä 60 päivän testilisenssillä. Tähän lisenssiin jouduttiin pyytämään jatkoaikaa HP:ltä, kun kaikkia ominaisuuksia ei ehtinyt testaamaan 60 päivässä. Uuden jatkolisenssin aktivoiminen onnistui ohjeiden mukaan ilman ongelmia.

Ennen IMC-järjestelmän asennusta tutustuttiin asennusohjekirjaan (HP IMC Installation Guide), jossa on kerrottu hyvin kattavasti asennuksen eri vaiheet. Tämän jälkeen asennettiin HP IMC 5.1 Standard versio, jossa käytettiin tietokantaohjelmistona asennuspaketin mukana tulevaa Microsoft SQL Server 2008 R2 Express SP1 -ohjelmistoa.

IMC:n asennuksessa valitaan asennettavat komponentit, asennuspolku ja asetetaan tietokannan tiedot tai asennetaan mukana tuleva tietokanta. Tässä tapauksessa asennettiin kaikki IMC-asennuspaketissa mukana tulevat komponentit.

Asennuksen lopussa käynnistetään käyttöönoton monitorointi agentti sovellus (Deployment Monitoring Agent), jolla hallitaan ja otetaan käyttöön asennettuja ominaisuuksia. Asennuksen jälkeen saadaan IMC päälle kyseisestä sovelluksesta. Tämä sovellus myös kertoo IMC-järjestelmän muisti- ja prosessori-resurssien kulutuksen sekä tietokannan koon.

5.2 IMC:n asetuksien määrittely asennuksen jälkeen

Kun IMC:n asennus on valmis ja sen prosessit on käynnistetty, kirjaudutaan web-sivun kautta järjestelmään. IMC-web-sivun osoite on muotoa http://192.168.1.1:8080, jossa 192.168.1.1 on palvelimen IP-osoite ja 8080 asennuksen aikana asetettu portti. Ensimmäistä kertaa sisään kirjauduttaessa käyttäjätunnuksena on admin ja salasana on myös admin. Ensimmäisen kirjautumiskerran jälkeen kyseinen salasana täytyy vaihtaa.

Käyttäjä ja käyttäjäryhmä asetukset

Asennuksen jälkeen alkoi käyttäjäryhmien ja käyttäjien määrittely. IMC:n käyttäjäryhmillä on mahdollista rajata käyttäjien pääsy haluttuihin toimintoihin. Esimerkiksi jollekin käyttäjäryhmälle voidaan antaa pääsy tekemään muutoksia VLAN-asetuksiin, kun taas toiselle ryhmälle voidaan antaa oikeudet pääsylistojen muokkaamiseen. Käyttäjäryhmät luodaan valikosta:

System → Operator Management → Operator Group.

Käyttäjien oikeuksia voidaan myös rajoittaa laiteryhmäkohtaisesti, näitä laiteryhmiä voidaan luoda valikosta:

System → Group Management → Device Group.

Ensin luodaan uusi laiteryhmä ja tämän jälkeen lisätään ryhmään kuuluvat laitteet. Uudet laitteet voidaan myös määrittää kuulumaan automaattisesti johonkin laiteryhmään. Tämän jälkeen voidaan luoda uusia käyttäjiä kyseisiin käyttäjäryhmiin. Uudelle käyttäjälle määritellään, mihin käyttäjäryhmään käyttäjä kuuluu, mihin laiteryhmään ja mihin verkkotopologianäkymään käyttäjällä on käyttöoikeudet.

IMC-ominaisuuksien testaamista varten luotiin uusi käyttäjä, joka liitettiin olemassa olevaan ylläpitäjä (Administrator group) käyttäjäryhmään. Kyseisen käyttäjän oikeuksia ei rajattu laiteryhmiä käyttäen. Ylläpitäjä käyttäjä ryhmää käytettiin, koska ei haluttu rajoittaa eri ominaisuuksiin pääsyä.

Laitteiden oletuksena monitoroitavat tiedot

Ennen kuin järjestelmään lisätään hallittavia ja valvottavia laitteita, on hyvä määritellä, mitä tietoja laitteen toiminnasta oletuksena haetaan, ettei niitä tarvitse määritellä jälkikäteen jokaiselle laitteelle erikseen. Oletuksena jokaiselle laitteelta haettavat tiedot määritellään valikosta:

System → System Configuration → Default Monitoring Indexes.

Oletuksena laitteilta haettaviksi tiedoiksi asetettiin prosessorin käyttöaste, muistin käyttö ja laitteen lämpötila.

Telnet-, SSH- ja SNMP-asetuspohjat

HP IMC mahdollistaa valmiiden asetuspohjien käyttämisen Telnet-, SSH- ja SNMP-asetuksien kanssa. Tämä helpottaa laitteiden liittämistä hallintaan ja muutosten tekemistä, kun laiteryhmillä on käytössä samat asetukset. SSH- ja SNMP-asetuspohjat

tehtiin erikseen Ciscon, Juniperin, HP:n ja Extremen laitteille. Asetuspohjat löytyvät valikosta:

IMC *System* → *Resource Management*.

5.3 Testattavat laitteet ja testitopologiat

HP IMC ohjelmiston ominaisuuksia ja yhteensopivuutta testattiin taulukon 3 laitteita käyttäen.

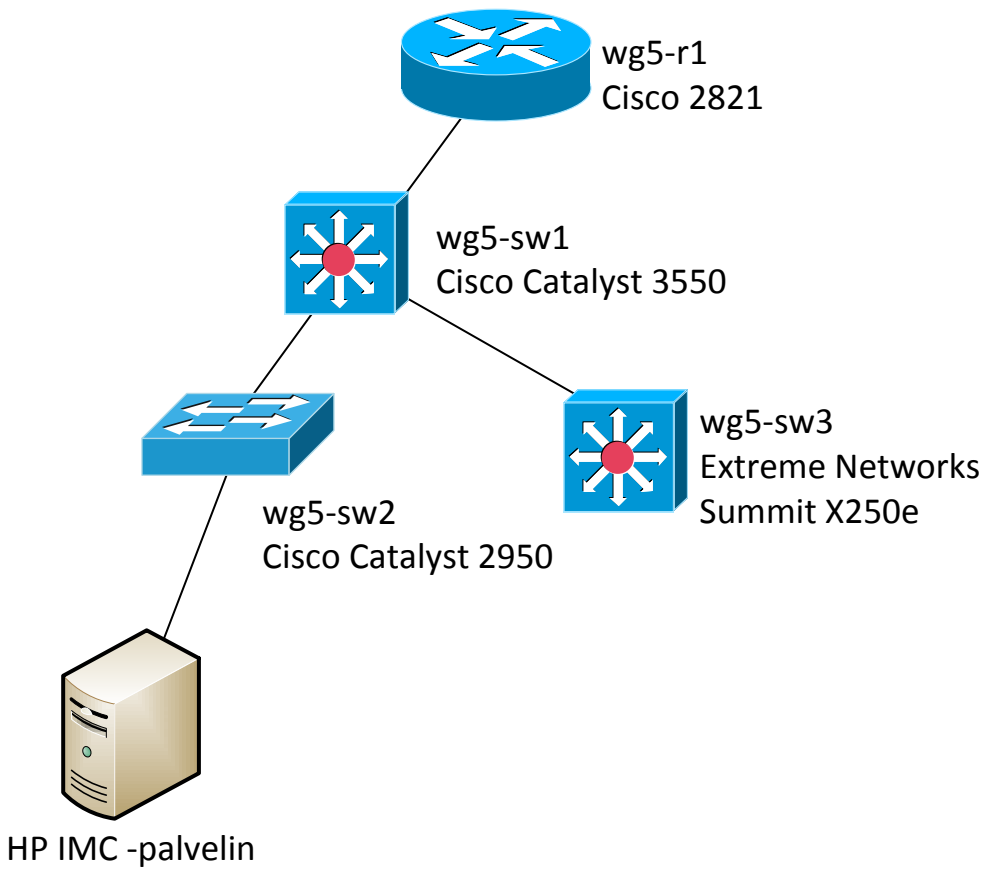
SpiderNetin laitteita pääsee konfiguroimaan laboratorioverkosta muodostamalla Telnet-yhteys laitteen konsoliosoitteeseen. Taulukossa 3 on listattu myös käytettyjen laitteiden konsoliosoitteet.

TAULUKKO 3. Käytetyt SpiderNet laitteet ja niiden konsoliosoitteet

Laite	**Malli**	**Konsoli osoite**
wg5-r1	Cisco Systems 2821	192.168.41.51
wg5-sw1	Cisco Systems Catalyst 3550	192.168.41.52
wg5-sw2	Cisco Systems Catalyst 2950	192.168.41.53
wg5-sw3	Extreme Networks Summit X250e	192.168.41.54
juniper-r1	Juniper Networks J2320	192.168.41.91
juniper-r2	Juniper Networks J2320	192.168.41.92
juniper-r3	Juniper Networks J2320	192.168.41.93
juniper-r4	Juniper Networks J2320	192.168.41.94
juniper-r5	Juniper Networks J2320	192.168.41.95
hp-sw1	Hewlett-Packard Procurve 2650	192.168.41.69

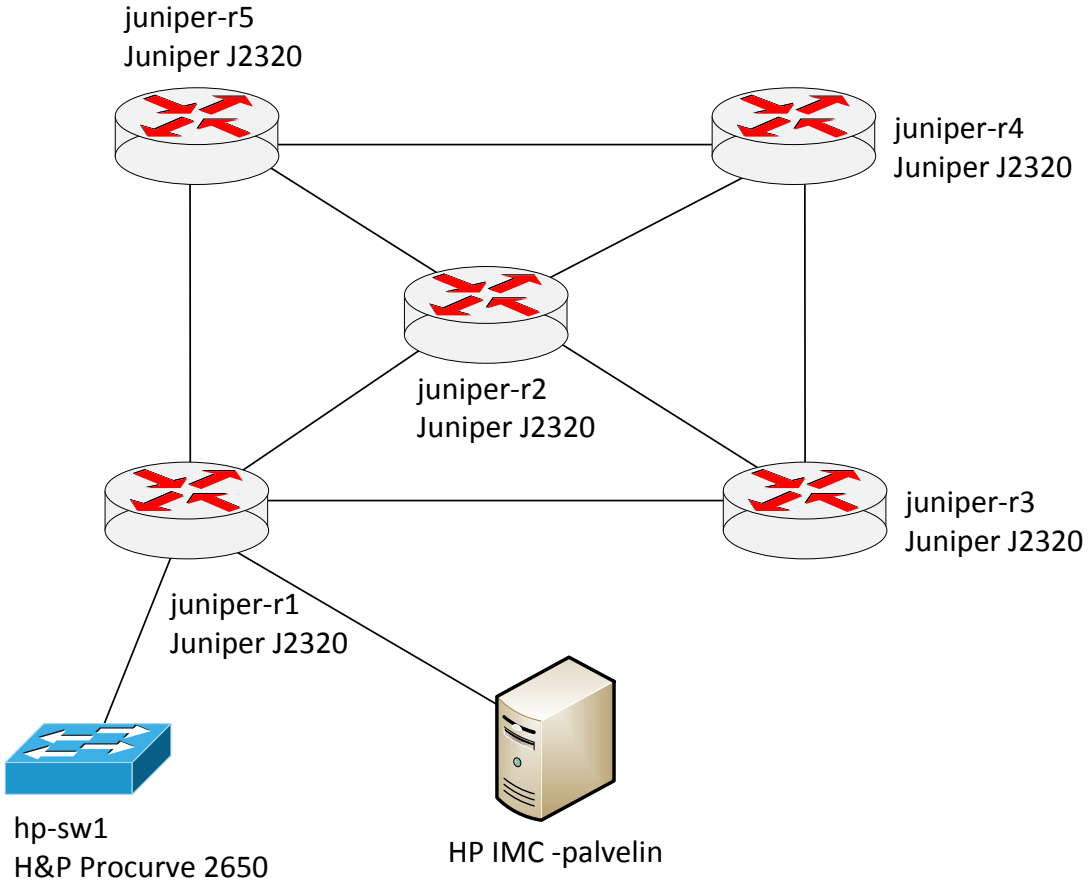
Testattujen laitteiden ohjelmistoversiot löytyvät liitteestä 1.

Testaukset toteuttiin käyttäen kahta erilaista testitopologiaa. Ensimmäisessä topologiassa IMC-palvelin ja laitteet olivat liitettyinä kuvion 5 mukaisesti. Käytössä oli SpiderNetin työryhmä 5 (wg5) laitteet. Topologian kaikkien laitteiden hallinta IP-osoitteet olivat samasta aliverkosta ja laitteisiin oli määritelty yhteinen VLAN-verkko hallintaa varten.



KUVIO 5. Ensimmäinen (1.) testitopologia

Toisessa testitopologiassa IMC-palvelin oli liitetty kuvion 6 topologian mukaisesti. HP IMC -palvelimelta oli IP-yhteys kaikkiin testattaviin laitteisiin. HP Procurve 2650 -kytkin lisättiin SpiderNet-laboratorioverkkoon tilapäisesti tämän opinnäytetyön testauksien suorittamista varten. Laitteiden IP-osoitteet eivät olleet samassa aliverkossa, ja juniper-r1 reititti liikennettä eri aliverkkojen välillä.



KUVIO 6. Toinen (2.) testitopologia

Testitopologioiden tarkoituksena oli olla mahdollisimman yksinkertaisia ja mahdollistaa liikennöinti IMC palvelimen ja hallittavien laitteiden välillä.

Taulukossa 4 on testitopologioissa käytetyt laitteiden hallintaosoitteet.

TAULUKKO 4. Laitteiden hallinta IP-osoitteet

Laite	**Hallinta IP-osoite**
HP IMC palvelin	10.10.10.1
wg5-r1	10.10.10.5
wg5-sw1	10.10.10.3
wg5-sw2	10.10.10.2
wg5-sw3	10.10.10.4
juniper-r1	10.10.1.51
juniper-r2	10.10.12.2
juniper-r3	10.10.12.3
juniper-r4	10.10.12.4
juniper-r5	10.10.12.5
hp-sw1	10.10.11.2

5.4 HP IMC 5.1 SP1 päivitys

HP julkaisi huoltopaketti 1 (Service Pack 1, SP1) ohjelmistopäivityksen IMC-järjestelmään sen jälkeen, kun ohjelmisto oli asennettu ja ominaisuuksien testaaminen aloitettu. Päivityksen asentaminen suoritettiin käyttäen IMC Deployment Monitoring Agent -sovellusta. Päivityksen asentamisessa ei ollut ongelmia. Päivitys toi mukanaan mahdollisuuden käyttää SCP-protokollaa tiedostojensiirrossa.

5.5 HP IMC Palvelutuotanto lisäosa

IMC-järjestelmän palvelutuotanto lisäosa (Service Operation Module, SOM) asennettiin tutkittaessa, kuinka IMC-järjestelmän avulla voidaan toteuttaa ITIL-vaatimuksia. IMC SOM -lisäosa asennettiin käyttäen IMC Deployment Monitoring Agent -sovel-

lusta. Asennuksen jälkeen SOM-lisäosan mukanaan tuomien ominaisuuksien käyttäminen vaatii SOM-lisäosan käyttäjäasetuksien määrittelemisen.

SOM-lisäosa tuo mukanaan palvelutiski (Service Desk) toiminnon, jonka avulla voidaan toteuttaa eri ITIL prosesseja, kuten muutoksen- ja ongelmienhallinta prosesseja. Lisäksi SOM-lisäosa sisältää konfiguraationhallintatietokannan (CMDB).

6 OMINAISUUKSIEN TESTAUS JA TULOKSET

6.1 Testattavaksi valitut ominaisuudet

Työssä testattavaksi valittiin osa IMC-järjestelmän keskeisistä ominaisuuksista, jotka ovat tärkeitä järjestelmän päivittäisessä käytössä verkonhallinnassa. Työn toimeksiantajan kanssa testattavaksi valittiin seuraavat ominaisuudet, laitteiden liittäminen IMC järjestelmään käyttäen Auto Discovery ominaisuutta, laitteiden hallinta SSH- (Secure Shell) ja SNMPv3-protokollia käyttäen, laitteiden asetustenhallinta, laitteiden ohjelmistonhallinta ja virtuaalilähiverkkojenhallinta (VLAN). Näitä ominaisuuksia testattiin Hewlett-Packard, Cisco Systems, Juniper Networks ja Extreme Networks laitevalmistajien laitteilla. (Alanko 2012.)

6.2 Laitteiden hallinta SSH- ja SNMPv3-protokollien avulla

6.2.1 Testattavat ominaisuudet

Testattavana oli HP IMC ohjelmiston tuki eri laitevalmistajien laitteille SSH- ja SNMP-hallintaprotokollia käyttäen.

IMC käyttää SNMP-protokollaa tietojen hakemiseen laitteilta ja laitteiden asetusten muuttamiseen, esimerkiksi VLAN-verkkojen hallitsemiseen. SSH-protokollaa IMC käyttää komentojen suorittamiseen laitteilla, esimerkiksi asetusten varmuuskopioinnissa.

Laitteen hallittavaksi lisäämisen jälkeen, HP IMC ohjelmiston tulisi tunnistaa laitteen tyyppi, ohjelmistoversio, rajapintojen määrä ja muut laitteen tiedot. Nämä tiedot IMC-järjestelmän tulisi hakea laitteelta SNMPv3-protokollaan käyttäen. SSH-protokollan toimivuus saadaan testattua, käyttämällä IMC-järjestelmän yhteysasetusten kokeilu (Check Access Settings) ominaisuutta.

Testattaviksi yhteystavoiksi valittiin SSH- ja SNMP:n versio 3 -protokollat niiden tietoturvaominaisuuksien vuoksi. SSH- ja SNMPv3-protokollia käyttämällä kaikki tiedot on mahdollista siirtää salattuna, joten liikennettä kaappaamalla ei ole mahdollista lukea verkonhallinta protokollien välittämiä tietoja. SNMP-protokollasta valitsin käyttöön SNMP version 3 ja suojaustasoksi autentikointi ja yksityisyys (authpriv), eli käytössä on Md5-autentikointi ja liikenne salataan käyttäen DES-salausta. IMC tukee myös SNMPv3-protokollan AES-salausta ja SHA-autentikointia. Vaihtoehtona valituille tavoille olisi olleet Telnet- ja SNMP versio 2-protokollat, joissa ei ole mahdollisuutta käyttää salattua tiedonsiirtoa.

6.2.2 Testaus

SSH- ja SNMPv3-hallinnan testaus toteutettiin käyttäen molempia testitopologioita ja laitteina käytettiin wg5-sw1, wg5-sw2, wg5-r1, wg5-sw3, juniper-r1 ja hp-sw laitteita. Kaikilta laitteilta oli yhteys IMC-palvelimeen. Laitteille määriteltiin käyttäjätunnus SSH-kirjautumista varten ja SNMPv3 vaatimat asetukset.

SSH- ja SNMP-protokollien vaatimat asetukset määriteltiin Cisco-laitteille alla olevilla komennoilla.

```
#ip domain-name spidernet.labranet.jamk.fi
#crypto key generate rsa modulus 512
#username cisco password 0 cisco
#enable password cisco
#line vty 0 4
#login local
#transport input ssh
#snmp-server view kirjoitus internet include
#snmp-server group rkirjoitus v3 priv write kirjoitus
```

#snmp-server user imck rkirjoitus v3 auth md5 testi priv des56 testi

Juniper-laitteille määriteltiin seuraavat SSH- ja SNMP-protokollien vaatimat asetukset.

#set system login user imcssh class super-user authentication plain-text-password
#set system services ssh root-login allow
#set system services ssh protocol-version v2
#set snmp engine-id use-mac-address
#commit
#set snmp v3 usm local-engine user imcj authentication-md5 authentication-password asdf1234
#set snmp v3 usm local-engine user imcj privacy-des privacy-password asdf1234
#set snmp v3 vacm security-to-group security-model usm security-name imcj group imcj
#set snmp v3 vacm access group imcj default-context-prefix security-model usm security-level privacy read-view imcj write-view imcj notify-view imcj

HP Procurve -kytkimelle määriteltiin seuraavat SSH- ja SNMP-protokollien vaatimat asetukset.

#ip ssh
#ip ssh version 2
#crypto key generate ssh
#aaa authentication ssh login local
#aaa authentication ssh enable local
#password operator user-name hpssh
#password manager user-name hpssh
#snmpv3 enable
#snmpv3 only
#snmpv3 restricted-access
#snmpv3 user "imchp"
#snmpv3 group ManagerPriv user "imchp" sec-model ver3

Wg5-sw3 Extreme Networks Summit x250e -kytkin ei tukenut SSH-protokollaa, joten sen sijaan käytettiin Telnet-protokollaa hallintayhteyden muodostamiseksi.

Tarvittavat Telnet- ja SNMPv3 -protokollien asetukset wg5-sw3 laitteelle määriteltiin seuraavasti.

#enable snmp access snmpv3
#configure snmpv3 add user imce authentication md5 testi123 privacy des testi123
#configure snmpv3 add access kirjoitus sec-model usm sec-level priv read-view internet write-view internet
#configure snmpv3 add mib-view internet subtree 1.3.6.1 type include
#configure snmpv3 add group kirjoitus user imce

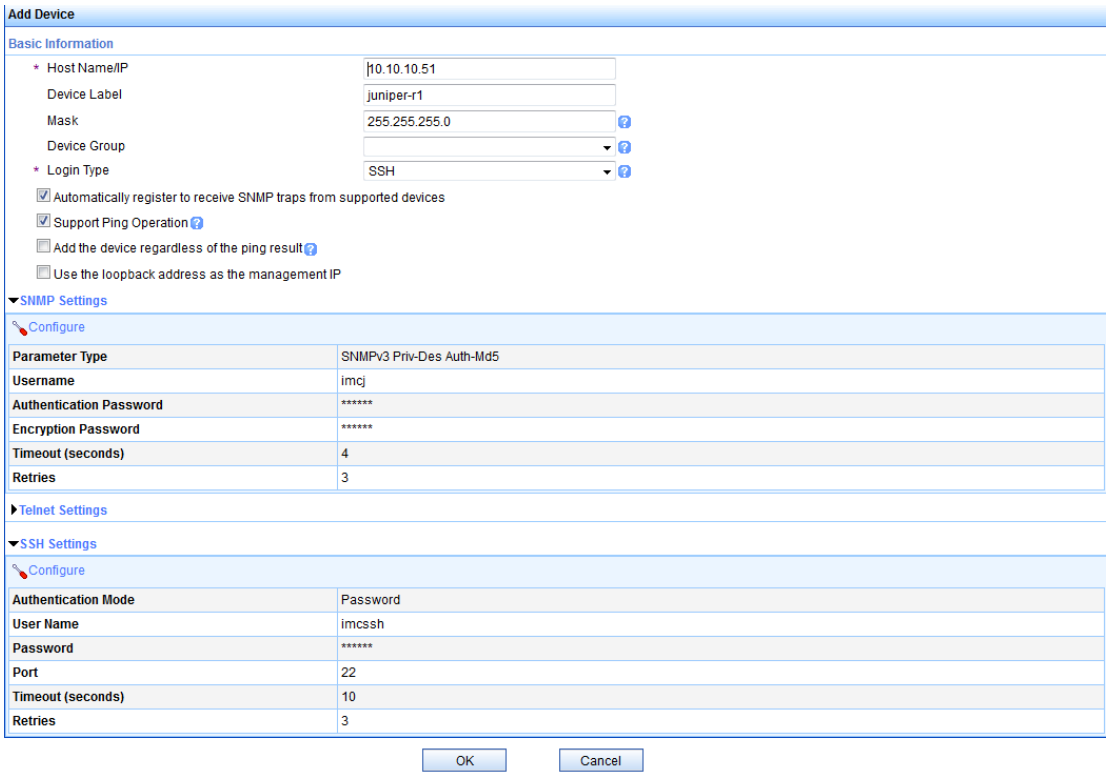
Kun laitteiden asetukset olivat konfiguroitu, lisättiin laitteet manuaalisesti hallittaviksi IMC-järjestelmään. Laite lisätään manuaalisesti hallittavaksi valikosta:

Resource → Add Device.

Laitteen hallintaan lisäämiseksi tarvitaan seuraavat tiedot:

- Laitteen IP-osoite
- Laitteen nimi
- Aliverkonpeite
- Laiteryhmä, johon laite lisätään
- Käytettävä kirjautumistapa, Telnet tai SSH
- SNMP asetukset
- Käytettävät Telnet- tai SSH -asetukset.

Kuviossa 7 on kuvaruutu kaappaus juniper-r1 laitteen hallintaan lisäämisessä käytetyistä IMC:n asetuksista.



KUVIO 7. Asetukset Juniper-r1-laitteen lisäämiseksi hallittavaksi IMC-järjestelmään

Ciscon IOS -laitteiden ja HP Procurve -kytkinten enable-tilan salasanan määritellään IMC SSH -asetuksissa valitsemalla autentikointi tavaksi ”salasana ja super-salasana” (Password + Super Password), jolloin salasanaksi asetetaan SSH-käyttäjän salasana ja super-salasanaksi enable-tilan salasana.

SSH toiminnan todennusta varten laitteille suoritettiin yhteysasetusten kokeilu (Check Access Settings). Tämä testi löytyy valikosta:

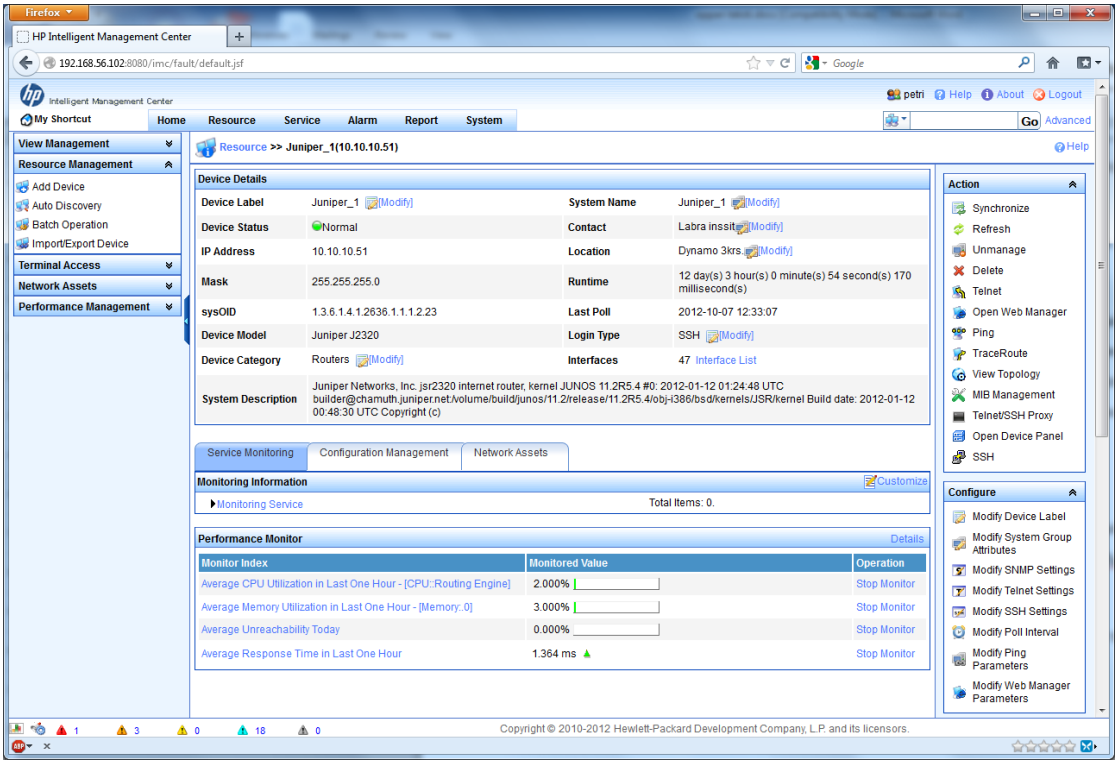
Resource → Batch Operation → Check Access Settings

Tällä testillä voidaan myös tarkastaa SNMP- tai Telnet -yhteysasetuksien toiminta.

6.2.3 Testauksen tulokset

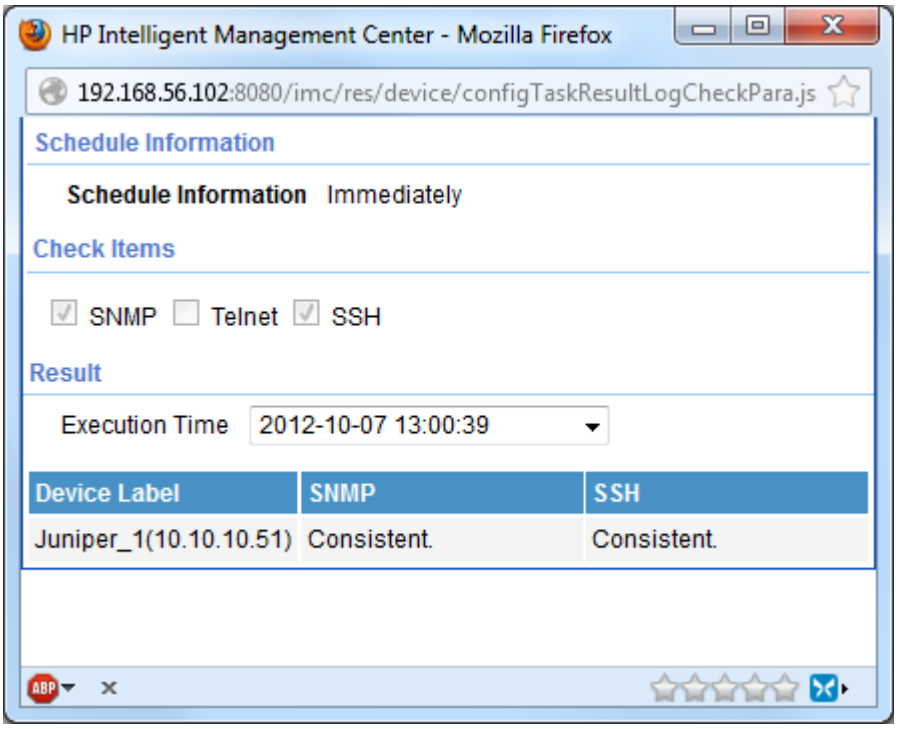
Juniper Networks J2320

Kuviossa 8 on kuvankaappaus Juniper-r1 laitteen IMC Resource -näkymästä, kun laite on lisätty hallintaan. Kuviosta nähdään kuinka IMC oli hakenut tiedot laitteelta, tunnistanut laitteen mallin ja lisännyt sen reititin-laitekategoriaan.



KUVIO 8. Juniper-r1-laitteen resource-näkymä

Kuviossa 9 on kuvankaappaus IMC-järjestelmän Juniper-r1-laitteelle suorittamasta hallintayhteyden kokeilun tuloksesta. Kuviossa nähdään SSH-asetuksien olevan ”Consistent”, eli yhteneväinen ja yhteys laitteeseen oli onnistunut.



KUVIO 9. Juniper-r1-laitteen SSH-yhteyden tarkastus

Cisco Systems -laitteet

HP IMC haki Cisco-laitteilta tietoja käyttäen SNMPv3-protokollaa, ja tämän ominaisuuden toiminnassa ei havaittu ongelmia.

SSH-yhteys ei aluksi toiminut Cisco-laitteilla. IMC-palvelimen lokien sisällön perusteella Ciscon IOS -ohjelmiston enable-tilaan siirtyttäessä annettava salasana olisi väärin. Ciscon-laitteisiin pääsi kuitenkin kirjautumaan SSH-asiakasohjelmalla ilman ongelmia, samoja salasanoja käyttäen. Nämä loki tiedostot sijaitsevat kansiossa *”C:\Program File\iMC\server\conf\log\”.*

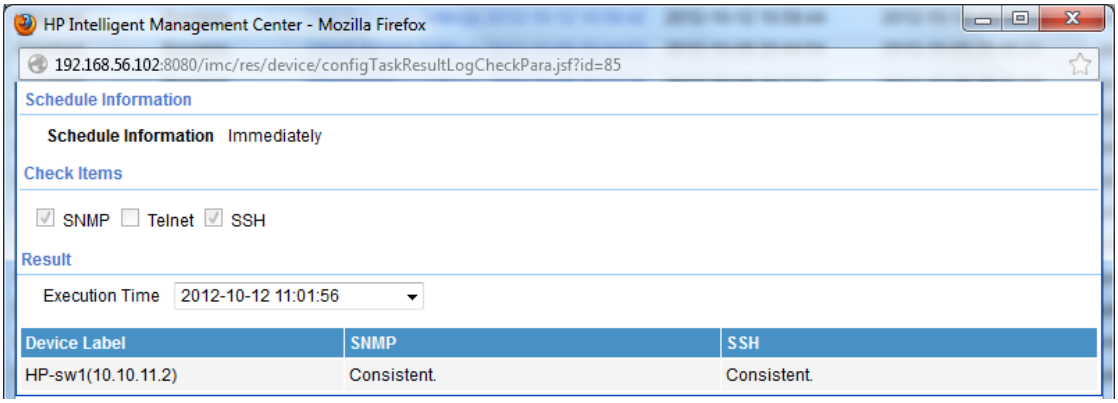
Tämä ongelma saatiin kierrettyä määrittelemällä Cisco-laitteille käyttäjätunnuksen käyttöoikeustasoksi 15 (privilege level 15), tällöin SSH:llä kirjauduttaessa siirrytään suoraan enable-tilaan, eikä IMC:n tarvitse antaa enable-tilan salasanaa. Cisco-laitteille käyttäjätunnuksen käyttöoikeustaso määriteltiin seuraavalla komennolla.

#username cisco privilege 15 password 0 cisco

Myös IMC-järjestelmän asetuksista vaihdettiin SSH-protokollan autentikointi tavaksi pelkkä salasana. Tämän jälkeen hallintayhteyden kokeilun tulokseksi saatiin ”Consistent”, eli SSH-yhteys oli onnistunut.

HP Procurve 2650

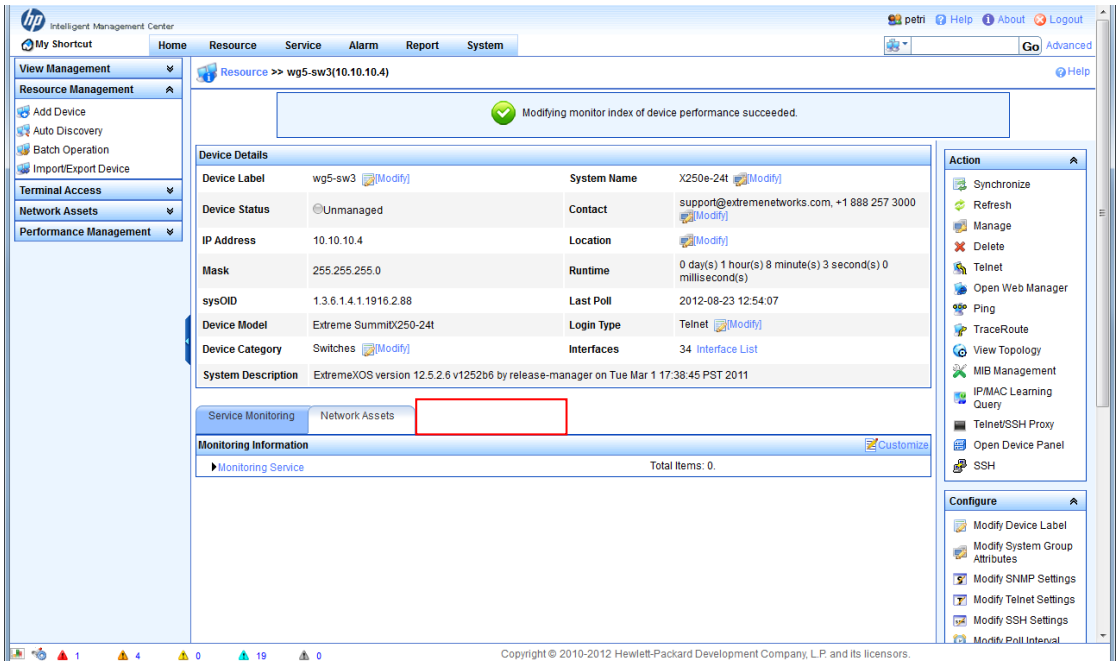
HP Procurve -kytkimeltä (hp-sw1) IMC osasi hakea laitteen tiedot SNMP-protokollaa käyttäen ja se tunnisti laitteen kuuluvan kytkin-laitekategoriaan. Kuviossa 10 olevasta kuvankaappauksessa, nähdään SSH-hallintayhteyden kokeilun olleen onnistunut.



KUVIO 10. HP procurve 2650 -kytkimen SSH-yhteyden tarkastus

Extreme Networks Summit X250e

Kuviossa 11 on kuvakaappaus wg5-sw3 Summit X250e -kytkimen IMC Resource -näkymästä. Tästä nähdään että IMC on osannut hakea laitteen tiedot SNMP:llä. Lisäksi kuviosta nähdään, että ”Configuration Management” -osio puuttuu laitteen tietojen alta, toisin kuin kuviossa 8 on juniper-r1 laitteen tapauksessa. Myös VLAN-hallinta ominasuus ei ole käytettävissä Extremen laitteen kanssa. IMC-järjestelmän (versio 5.1 SP1) tuki Extreme Networks laitteille on puutteellinen sisältäen vain hälytysten vastaanoton (SNMP trap) ja palveluiden valvonnan (Service Monitoring).



KUVIO 11. Summit X250e Resource näkymä

Extremen kytkimen kanssa käytettiin Telnet-hallintayhteyttä ja sille suoritettu hallintayhteyden kokeilu oli onnistunut.

6.3 Auto Discovery

6.3.1 Testattavat ominaisuudet

Automaattinen laitteiden haku (Auto Discovery) -ominaisuuden avulla IMC-järjestelmä hakee verkosta uusia laitteita ja lisää löydetyt laitteet hallittavaksi IMC-järjestelmään. Auto Discovery -ominaisuuden käyttäminen säästää aikaa ja pienentää virheiden mahdollisuutta, lisätessä uusia laitteita hallintaan ja kun käytössä on paljon laitteita. Tarkoituksena oli testata eri Auto Discovery -tapojen toiminta. Näitä eri tapoja ovat reititystauluun pohjautuva (Routing-Based), ARP-tauluun pohjautuva (ARP-Based), IPsec VPN yhteyksiin pohjautuva (IPsec VPN-Based), Verkkosegmenttiin pohjautuva (Network Segment-Based) ja Point-to-Point-protokollaan pohjautuva (PPP-Based).

Testattaviksi Auto Discovery -ominaisuuksiksi valittiin verkkosegmenttiin, reititystauluun ja ARP-tauluun pohjautuvat tavat. Kyseiset ominaisuudet valittiin testattavaksi, koska ne ovat yleisimmin käytetyt tavat ja sopivat käytettäviksi useimpiin verkkotopologioihin.

Verkkosegmenttiin pohjautuva Auto Discovery

Verkkosegmenttiin perustuvassa tavassa annetaan IP-osoitealue, josta etsitään uusia laitteita. Lisäksi määritellään laitteiden hallinta-asetukset (SNMP ja SSH tai Telnet). IMC-järjestelmän tulisi löytää kaikki uudet laitteet, joiden IP-osoite on tällä alueella ja hallinta-asetukset ovat oikeat.

Verkkosegmenttiin pohjautuva Auto Discovery -haku suunniteltiin testattavan ensimmäistä testitopologiaa käyttäen ja haettavaksi IP-osoitealueeksi 10.10.10.2 – 10.10.10.10. Tällöin IMC ohjelmiston tulisi löytää laitteet wg5-sw1, wg5-sw2, wg5-sw3 ja wg5-r1.

Reititystauluun pohjautuva Auto Discovery

Reititystauluun pohjautuvassa tavassa annetaan ns. siemen-osoite, hyppyjen lukumäärä (hop count) ja kirjautumisasetukset. Reititystauluun pohjautuvassa tavassa IMC-järjestelmä kirjautuu laitteeseen, jonka IP-osoite on määritetty siemen-osoitteeksi, lisää kyseisen laitteen hallintaan, lukee sen reititystaulun ja toistaa samat toiminnot reititystaulusta löytyville osoitteille. Hyppyjen lukumäärällä rajoitetaan kuinka pitkälle tätä etenemistä jatketaan.

Reititystauluun pohjautuvaa Auto Discovery -haku suunniteltiin testattavan käyttäen toista (2.) testitopologiaa, siemen IP-osoitteena juniper-r1 hallintaosoitetta (10.10.10.51) ja hyppyjen lukumääränä kahta (2). Tällöin pitäisi löytyä kaikki Juniper-laitteet ja hp-sw1-kytkin.

ARP-tauluun pohjautuva Auto Discovery

ARP-tauluun pohjautuvassa tavassa määritellään siemen IP-osoite, hyppyjen lukumäärä ja kirjautumisasetukset. ARP-tauluun pohjautuvassa tavassa IMC-järjestelmä kirjautuu laitteeseen, jonka IP-osoite on määritetty siemen-osoitteeksi, lisää kyseisen laitteen hallittavaksi, lukee sen ARP-taulun ja yrittää kirjautua ARP-taulussa oleviin osoitteisiin, suorittaen näille laitteille samat toiminnot kuin ensimmäiselle laitteelle.

ARP-tauluun pohjautuva Auto Discovery -hakua suunniteltiin testattavan ensimmäistä (1.) testitopologiaa käyttäen ja siemen-osoitteena wg5-sw1 hallintaosoitetta (10.10.10.3) ja hyppyjen lukumääränä yhtä (1). Tällöin IMC:n pitäisi löytää ja lisätä hallintaan laitteet wg5-sw1, wg5-sw2, wg5-sw3 ja wg5-r1.

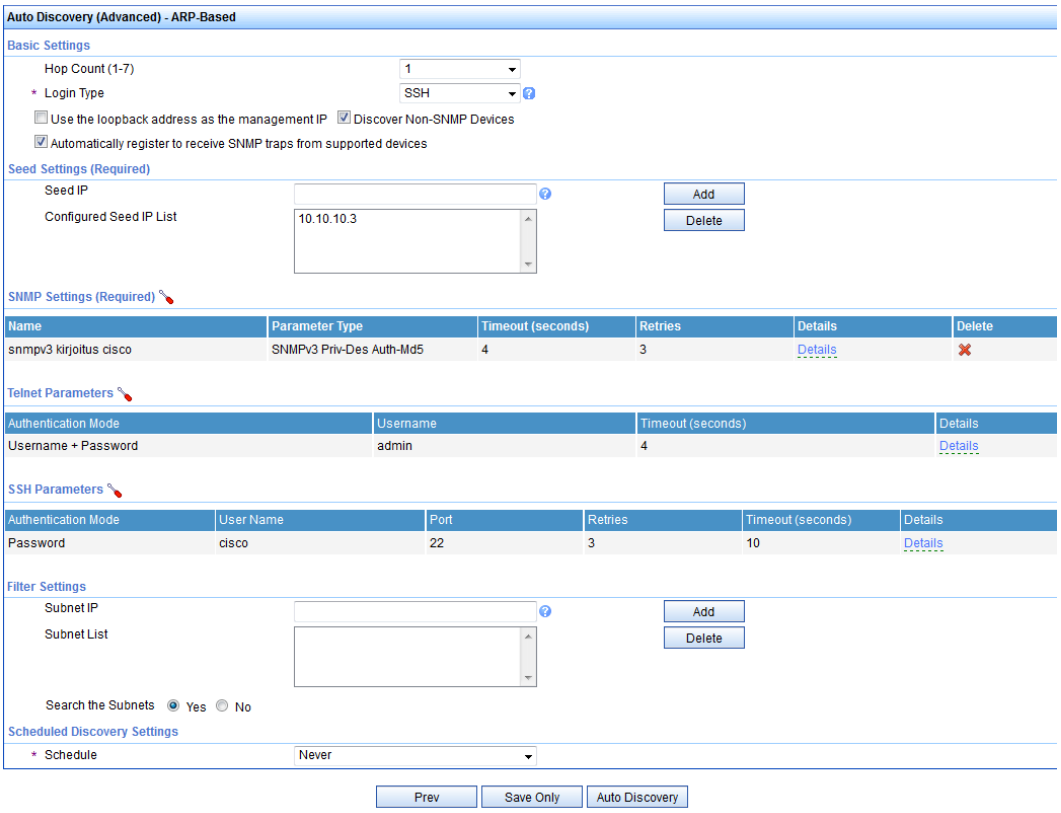
6.3.2 Testaus

Testauksessa käytetyille laitteille oli konfiguroitu SNMPv3- ja SSH -asetukset, kuten aiemmin ja kaikilta testatuilta laitteilta oli IP-yhteys IMC-palvelimeen.

Auto Discovery -ominaisuus löytyy IMC ohjelmistosta valikosta:

Resource → Auto Discovery → Go to Advanced.

Ennen jokaista testausta poistettiin IMC-järjestelmästä kaikki hallittavaksi lisätyt laitteet. Jokaisen Auto Discovery -haun asetuksissa määriteltiin oikeat laitteiden kirjautumisasetukset. Kuviossa 12 nähdään ARP-pohjaisen Auto Discovery -haun tapauksessa määritellyt asetukset.

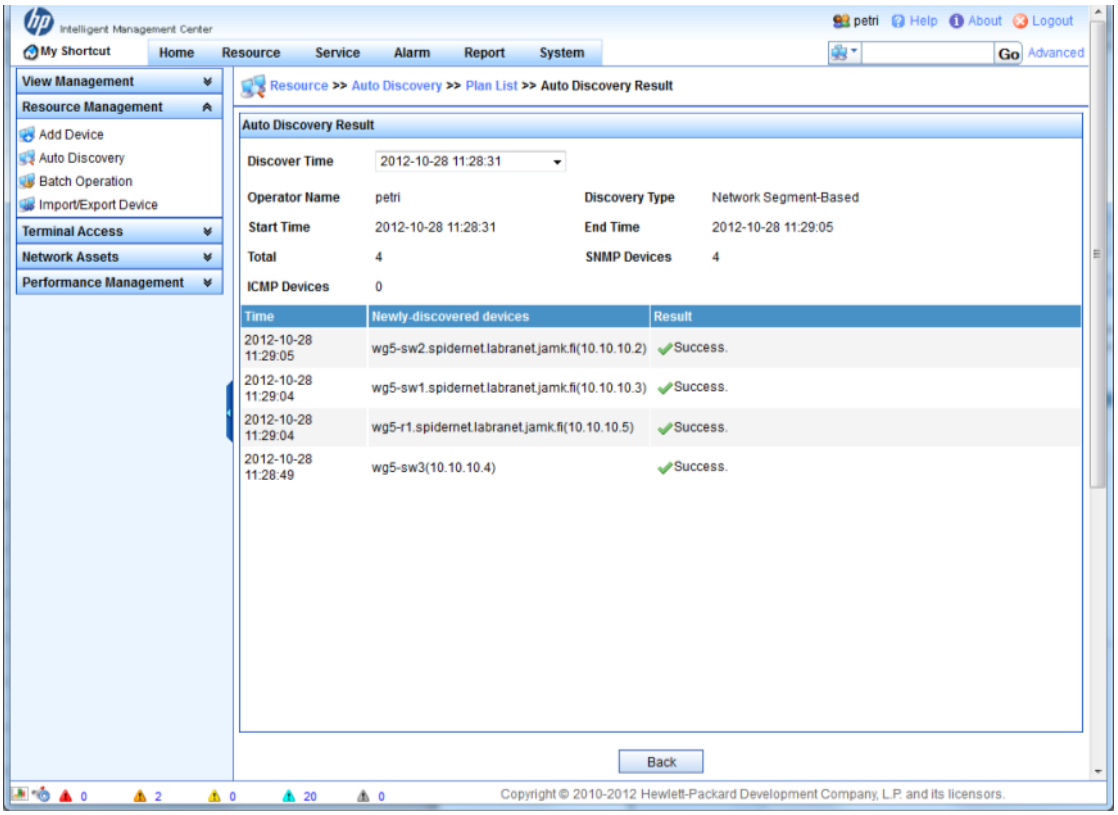


KUVIO 12. ARP-taulu pohjaisen Auto Discovery -haun asetukset

6.3.3 Testauksen tulokset

Verkkosegmenttiin pohjautuva Auto Discovery

Verkkosegmenttiin pohjautuva Auto Discovery haku löysi kaikki halutut laitteet, kuten nähdään kuviosta 13.

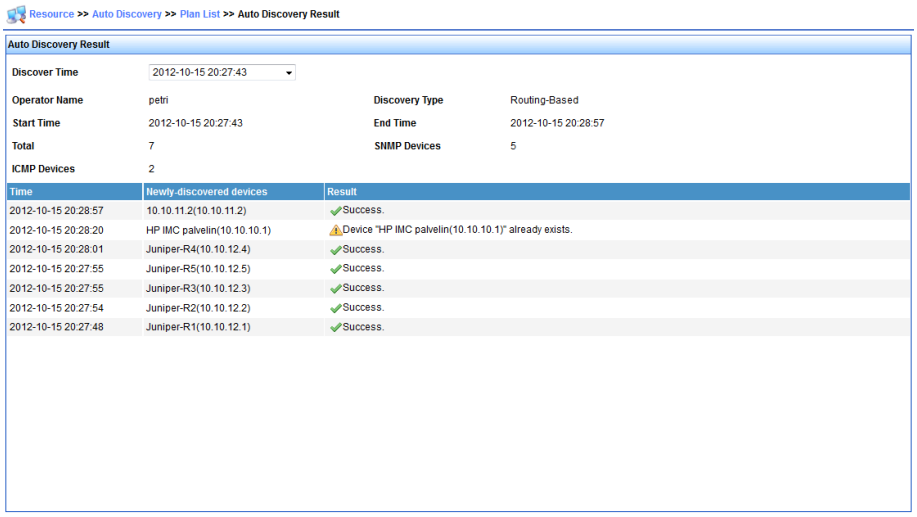


KUVIO 13. Verkkosegmenttiin pohjautuvan Auto Discovery -haun tulokset

Haun asetuksiin määriteltiin Ciscon ja Extremen -laitteiden SNMPv3-asetukset ja IMC löysi toimivat asetukset jokaiselle laitteelle. Haun asetuksissa määriteltiin laitteiden yhteystavaksi SSH-protokolla, joka täytyi jälkikäteen muuttaa wg5-sw3-laitteen osalta, koska kyseinen laite ei tukenut SSH-protokollaa.

Reititystauluun pohjautuva Auto Discovery

Reititystauluun pohjautuva Auto Discovery -haku onnistui ja IMC löysi kaikki toisen testi topologian laitteet. Kuviossa 14 on kuvankaappaus Auto Discovery -haun tuloksista. IMC lisäsi hp-sw1 laitteen ilman SNMP-hallintaa, koska haun asetuksissa oli määritelty vain Juniper-laitteiden SNMP-asetukset.



KUVIO 14. Reititystauluun pohjautuvan Auto Discovery -haun tulokset

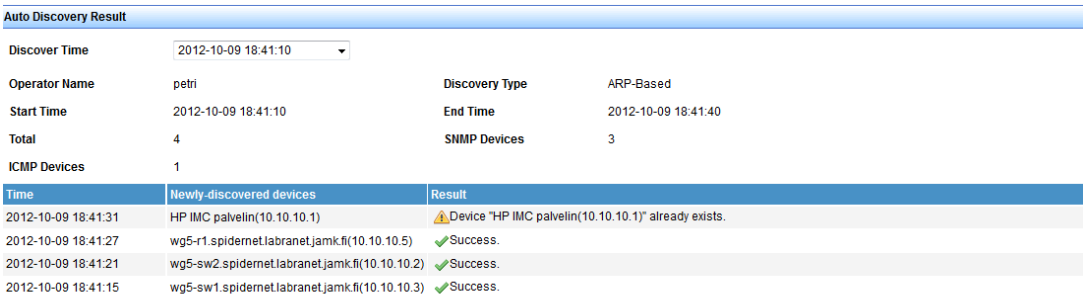
ARP-tauluun pohjautuva Auto Discovery

Kuviossa 15 on ARP-tauluun pohjautuvan Auto Discovery -haun tulos, josta nähdään että IMC löysi laitteet wg5-sw1, wg5-sw2 ja wg5-r1 ja lisäsi ne hallittaviksi. IMC ei löytänyt laitetta wg5-sw3, jonka vuoksi tarkastettiin wg5-sw1-laitteen ARP-taulu.

wg5-sw1#show arp

Protocol	*Address*	*Age (min)*	*Hardware Addr*	*Type*	*Interface*
Internet	*10.10.10.2*	*0*	*0007.857a.ecc0*	*ARPA*	*Vlan50*
Internet	*10.10.10.3*	*0*	*00c.cebf.9980*	*ARPA*	*Vlan50*
Internet	*10.10.10.5*	*0*	*001a.2f78.2221*	*ARPA*	*Vlan50*
Internet	*10.10.10.1*	*0*	*000c.29dc.e8e1*	*ARPA*	*Vlan50*

Wg5-sw1 ARP-taulusta huomattiin, että se ei sisältänyt laitteen wg5-sw3 IP- ja MAC -osoitteita, joten tästä syystä IMC ei löytänyt kyseistä laitetta.



KUVIO 15. ARP-tauluun pohjautuvan Auto Discovery -haun löytämät laitteet

6.4 Laitteiden asetusten hallinta

6.4.1 Testattavat ominaisuudet

Laitteiden asetusten hallinta on tärkeä ominaisuus, koska laitteen vikaantuessa tai epäonnistuneen asetus muutoksen jälkeen on helppoa palauttaa laite toimintaan. Työssä oli tarkoituksena testata onnistuuko IMC-järjestelmällä eri valmistajien laitteiden asetusten varmuuskopiointi ja asetusten palauttaminen laitteeseen.

6.4.2 Testaus

Asetusten hallinnan toimivuutta testattiin varmuuskopioimalla laitteiden asetukset IMC-järjestelmään, tekemällä muutos laitteiden asetuksiin ja palauttamalla asetukset alkuperäisiksi IMC-järjestelmän avulla. Asetusten hallinta ominaisuutta testattiin wg5-r1, juniper-r2 ja hp-sw -laitteilla.

IMC-järjestelmässä laitteen asetuksien hallinta löytyy valikosta:

Service → Configuration Center → Configuration Center

Laitteen asetuksien varmuuskopiointi suoritetaan valitsemalla ”Backup Configuration” ja asetukset voidaan palauttaa valitsemalla ”Restore” alasvetovalikosta ”Restore Device Configuration”.

Ennen laitteiden asetusten kopioimista täytyy asettaa IMC-järjestelmän käyttämä tiedonsiirtotapa, jolla asetustiedostot siirretään laitteesta. Tämä tapahtuu valikosta:

Service → Configuration Center → Options

Asetusten varmuuskopioinnissa voidaan käyttää tiedonsiirrossa TFTP, FTP, SFTP- ja SCP -protokollia. Kun halutaan käyttää tiedonsiirrossa SFTP- ja SCP -protokollia, täytyy laitteelle olla määritelty yhteystavaksi SSH-protokolla. Aluksi kaikille laitteille asetettiin käytettäväksi SFTP-protokolla. Muita yhteystapoja kokeiltiin, jos varmuuskopiointi ei onnistunut käyttäen SFTP-protokollaa.

SCP-tiedonsiirtoprotokollan käyttäminen wg5-r1-laitteella edellyttää seuraavien asetusten määrittelemisen laitteeseen.

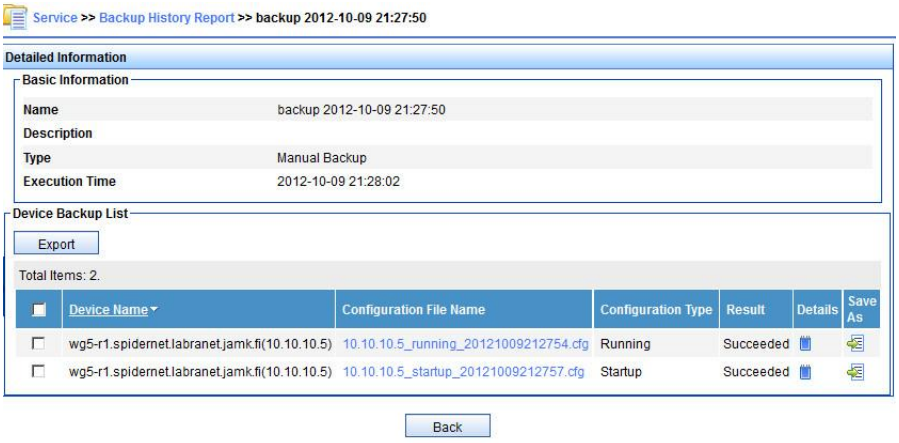
```
#aaa new-model
#aaa authentication login default local
#aaa authorization exec default local
#username cisco privilege 15 password 0 cisco
#ip scp server enable
```

Näillä komennoilla määritellään reititin käyttämään AAA-mallia (auktorisointi, autentikointi ja kirjanpito) ja käynnistetään SCP-palvelin.

6.4.3 Testauksen tulokset

Cisco-reitittimen asetusten hallinta

Asetusten varmuuskopiointi wg5-r1 laitteelta onnistui, kuten nähdään kuviossa 16 olevasta kuvankaappauksesta. IMC-järjestelmä osasi kopioida sekä ajonaikaisenasetukset (runnning-config) että käynnistysasetukset (startup-config). Varmuuskopioitujen asetustiedostojen sisältö oli sama kuin laitteelta katsottaessa.



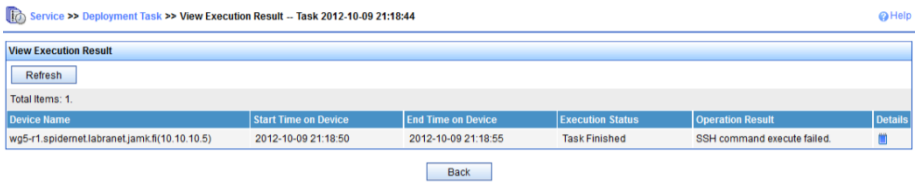
KUVIO 16. Laitteen wg5-r1 asetusten varmuuskopioinnin tulos

IMC-järjestelmän lokitiedostoista ilmeni että IMC yrittää kopioida asetukset ensin käyttäen SFTP:tä ja tämän epäonnistuttua käyttäen SSH-protokollaa. Ciscon-reitittimen tapauksessa IMC kopioi asetukset SSH-protokollaa käyttäen suorittamalla ”show running-configuration” -komennon laitteella ja kopioimalla laitteen palauttamat tiedot. IMC-järjestelmän asetusten varmuuskopiointiin liittyvä lokitiedosto löytyy palvelimelta seuraavasta tiedostosta.

”C:\Program Files\iMC\server\conf\log\imccfgbakdm.txt”.

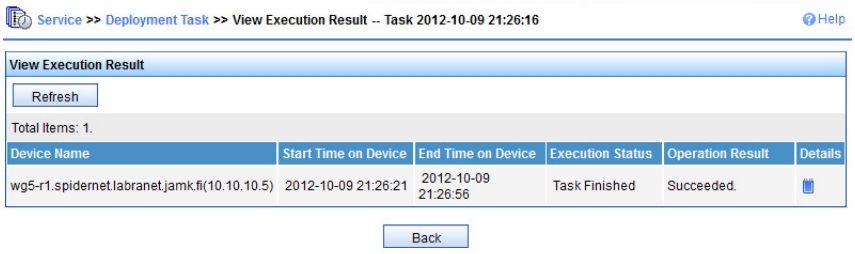
Asetusten palauttamisen toiminnan varmistamiseksi tehtiin muutos wg5-r1-laitteen asetuksiin sulkemalla yksi sen porteista, tämän jälkeen palautettiin laitteen asetukset ja tarkastettiin oliko kyseisen portin asetus palautunut avattu tilaan.

Wg5-r1-laitteen asetusten palauttamista kokeiltiin käyttäen SFTP-, SCP- ja TFTP -tiedonsiirtotapoja. Kuviossa 17 on kuvankaappaus wg5-r1-laitteen ajonaikaisten asetusten palautuksesta käyttäen SFTP-tiedonsiirtoa. Tästä kuviosta nähdään IMC-järjestelmän ilmoittavan virheestä komennon suorittamisessa ja asetusten palauttamisen epäonnistumisesta. Asetusten palauttaminen epäonnistui myös kun käytössä oli SCP-tiedonsiirtotapa, vaikka Ciscon-reitittimen pitäisi tukea kyseistä tiedonsiirtotapaa. SCP-tiedonsiirtoprotokollaa ei saatu toimimaan wg5-r1-reitittimen ja palvelimen välillä edes erillistä SCP-sovellusta käyttäen.



KUVIO 17. Asetusten palautus wg5-r1 laitteelle

Seuraavaksi käyttöön asetettiin TFTP-tiedonsiirtoprotokolla, jolloin laitteen ajonaikaistenasetuksien palautus onnistui, kuten nähdään kuvion 18 kuvankaappauksesta. Laitteelle tehty muutos oli myös palautunut ennalleen. Myös laitteen käynnistysasetuksien palautus onnistui käyttäen TFTP-tiedonsiirtoprotokollaa.



KUVIO 18. wg5-r1-laitteen käynnistysasetusten palautuksen tulos

Wg5-r1-laite ei tue SFTP-tiedonsiirtoprotokollaa ja tästä syystä asetusten varmuuskopiointi ja niiden palauttaminen ei onnistunut kyseistä protokollaa käyttäen. IMC kuitenkin osasi käyttää SSH-yhteyttä varmuuskopion tekemiseen, mutta asetusten palauttaminen onnistui vain TFTP-protokollaa käyttäen.

Juniper -reitittimen asetuksien hallinta

Juniper-r2-laitteen asetusten hallinnan testaaminen aloitettiin varmuuskopioimalla laitteen asetukset IMC-palvelimelle. IMC-järjestelmä ilmoitti ajonaikaistenasetusten varmuuskopioinnin onnistuneen, mutta varmuuskopioitu asetustiedosto sisälsi vain seuraavanlaisen tekstin:

display
^
unknown command.
imcjunos@j1> display current-configuration
^
unknown command.

Tästä voidaan päätellä IMC-järjestelmän yrittävän varmuuskopioida ajonaikaisia-asetuksia käyttäen väärää komentoa.

Myöskään käynnistysasetusten kopiointi ei onnistunut ja IMC-järjestelmän lokitiedoston perusteella ongelmana oli SSH-protokollan isäntäavaimen (Host Key) puuttuminen IMC-palvelimen rekisteristä. Kyseinen asia tulee vastaan kun kirjaudutaan laitteelle ensimmäistä kertaa SSH-protokollaa käyttäen, tällöin SSH-asiakasohjelma kysyy lisätäänkö isäntäavain tietokoneen rekisteriin.

Seuraavaksi muokattiin IMC-järjestelmän komentosarjaa, joka suorittaa laitteelle kirjautumisen SSH-protokollalla Juniper-laitteiden käynnistysasetusten varmuuskopioinnissa. Kyseinen komentosarja löytyy IMC-palvelimelta hakemistosta:

“C:\Program Files\iMC\server\conf\adapters\ICC\Juniper Network\Juniper Generic\enter_exec.tcl”

Kyseiseen tiedostoon lisättiin ”while”-silmukan sisään seuraavat rivit:

```
while {$loop == "true"} {
expect {
 "Store key in cache? (y/n)" {
        send "y\r"
}
}
```

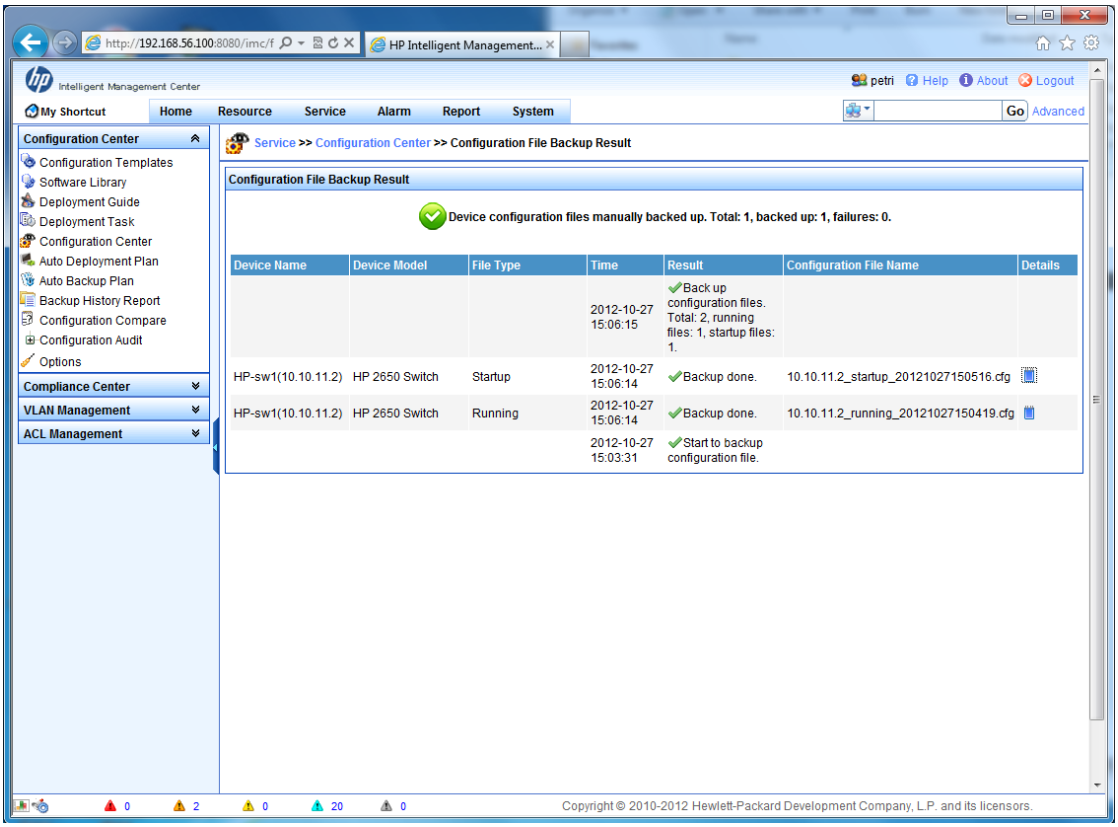
Tämä koodin avulla IMC osaa vastata kyllä, kysymykseen lisätäänkö SSH-isäntäavain palvelimen rekisteriin. Kyseinen ”enter_exec.tcl” tiedosto on kokonaisuudessaan liitteessä 2. Tämän muutoksen jälkeen IMC osasi varmuuskopioida juniper-r2-laitteen käynnistysasetukset ja ne olivat samat kuin laitteella.

Juniper Junos -käyttöjärjestelmää käyttävät laitteet eivät sisällä erillistä käynnistys- ja ajonaikaista-asetustiedostoa, kuten IOS -käyttöjärjestelmää käyttävät Cisco Systems -laitteet. IMC-järjestelmässä ei ole huomioitu tätä eroavaisuutta ja IMC yrittää kopioida käynnistys- ja ajonaikaisenasetustiedoston, myös Juniperin-laitteista. Juniperin -laitteiden tapauksessa siis riittää, että saadaan varmuuskopioitua yksi asetustiedosto.

Seuraavaksi muutettiin Juniper-r2-laitteen aika vyöhykkeeksi ”Europe/Riga”, kun se aiemmin oli ”Europe/Helsinki” ja tämän jälkeen suoritettiin asetusten palautus juniper-r2-laitteelle, käyttäen SFTP-tiedonsiirto tapaa. IMC näytti asetusten palauttamisen onnistuneen, mutta laitteelta katsottuna asetukset eivät olleet palautuneet ennalleen. Tutkittaessa juniper-r2-laitteen tiedostojärjestelmän sisältöä huomattiin, että IMC-järjestelmä oli onnistunut siirtämään kyseisen asetustiedoston laitteelle, mutta jostain syystä asetusten palauttaminen ei ollut onnistunut.

HP-kytkimen asetusten hallinta

Hp-sw1-laitteen asetusten hallinnan testaus aloitettiin suorittamalla asetusten varmuuskopiointi. Tiedonsiirto tavaksi oli asetettu SFTP-protokolla. Kuviosta 19 nähdään asetusten varmuuskopioinnin onnistuneen. Asetustiedostojen sisältö oli sama IMC:n tekemässä varmuuskopiossa ja laitteella.



KUVIO 19. Hp-sw1-laitteen asetusten varmuuskopioinnin tulos

Hp-sw1-laitteen asetusten palauttamista kokeiltiin käyttäen SFTP-, SCP- ja TFTP -tiedonsiirtotapoja. Hp-sw1-laitteen käynnistys- ja ajonaikaistenasetusten palautus ei onnistunut millään näistä tavoista. SFTP- ja TFTP -tiedonsiirtotavoilla virheilmoituksena oli, ettei laite tue kyseistä ominaisuutta (”The device does not support the features”). SCP-tiedonsiirtotavalla virheilmoitus oli, ettei tiedonsiirtoprotokolla ole tuettu (”Transmission protocol not supported”).

6.5 Laitteiden ohjelmiston hallinta

6.5.1 Testattavat ominaisuudet

Laitteiden ohjelmiston hallinta ominaisuus helpottaa ohjelmistojen päivittämistä laitteisiin ja yhtenäisten laiteohjelmistojen versioiden ylläpitämistä, kun käytössä on suuri määrä laitteita.

IMC-ohjelmistokirjasto (Software Library) löytyy valikosta:

Service → Configuration Center → Software Library

IMC osaa ladata laiteohjelmiston laitteelta tai se voidaan lisätä IMC-ohjelmistokirjastoon tiedostosta.

IMC-järjestelmän avulla pystyy varmuuskopioimaan laitteen ohjelmiston, päivittämään laitteen ohjelmiston ja palauttamaan käyttöön laitteen edellinen ohjelmistoversio.

6.5.2 Testaus

Laitteiden ohjelmistojen hallinta ominaisuutta testattiin lataamalla laitteiden ohjelmistot IMC-ohjelmistokirjastoon. Laitteiden ohjelmiston palauttamista ei ehtinyt testaamaan ajanpuutteen vuoksi.

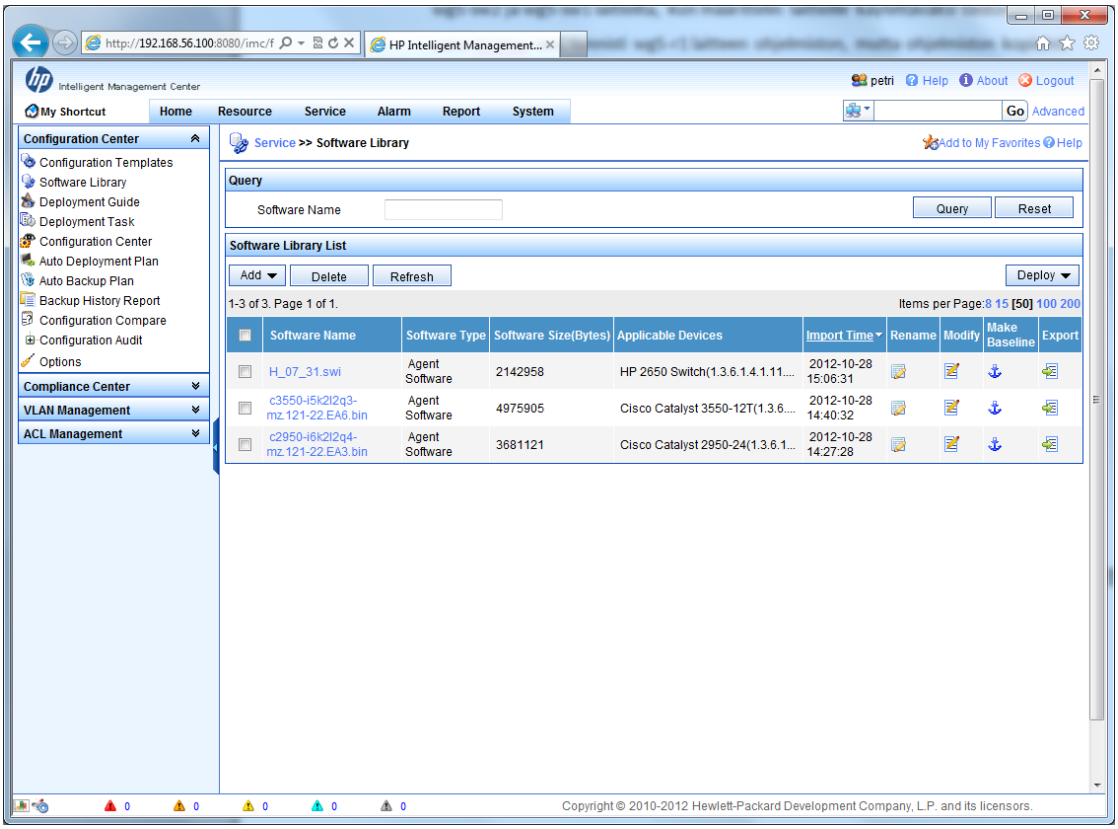
6.5.3 Testauksen tulokset

Ciscon-laitteista ohjelmiston kopioiminen IMC-ohjelmistokirjastoon onnistui wg5-sw2 ja wg5-sw1 -laitteilta, kun määriteltiin käytettäväksi tiedonsiirtotavaksi TFTP-protokolla. IMC tunnisti wg5-r1-laitteen ohjelmiston, mutta ohjelmiston kopiointi IMC-ohjelmistokirjastoon ei onnistunut TFTP:tä käyttäen, johtuen sen 32 megatavun tiedosto koon rajoituksesta. Laitteen ohjelmiston kopioimista FTP-protokollaan käyttäen ei kokeiltu, koska FTP-tiedonsiirtotavan käyttäminen olisi vaatinut FTP-palvelinohjelmiston asentamisen ja sen asetusten määrittelemisen IMC-järjestelmään.

Hp-sw1-kytkimen ohjelmiston kopioiminen IMC-ohjelmistokirjastoon onnistui kun määritteltiin IMC:n käyttämäksi tiedonsiirtotavaksi TFTP-protokolla ja määriteltiin Telnet-yhteysasetukset laitteeseen ja IMC-järjestelmään.

IMC-järjestelmä ei tunnistanut Juniper Networks ja Extremen Networks -laitteiden käyttämiä ohjelmistoversioita, jolloin ohjelmistoa ei voinut lisätä IMC-ohjelmistokirjastoon.

Kuviossa 20 on IMC-ohjelmistokirjasto näkymä, kun laitteiden ohjelmistot ovat kopioitu onnistuneesti.



KUVIO 20. IMC-ohjelmistokirjaston sisältö

6.6 Virtuaalisten lähiverkkojen hallinta

6.6.1 Testattavat ominaisuudet

HP IMC -järjestelmällä on mahdollista hallita virtuaalisia lähiverkkoja (VLAN), tämän ominaisuuden avulla voidaan luoda ja poistaa VLAN-verkkoja ja hallita niihin liitettyjä portteja. Tätä ominaisuutta testattiin Ciscon ja HP:n -kytkimillä.

IMC ohjelmistosta VLAN-verkkojen hallinta löytyy valikosta:

Services → VLAN Management.

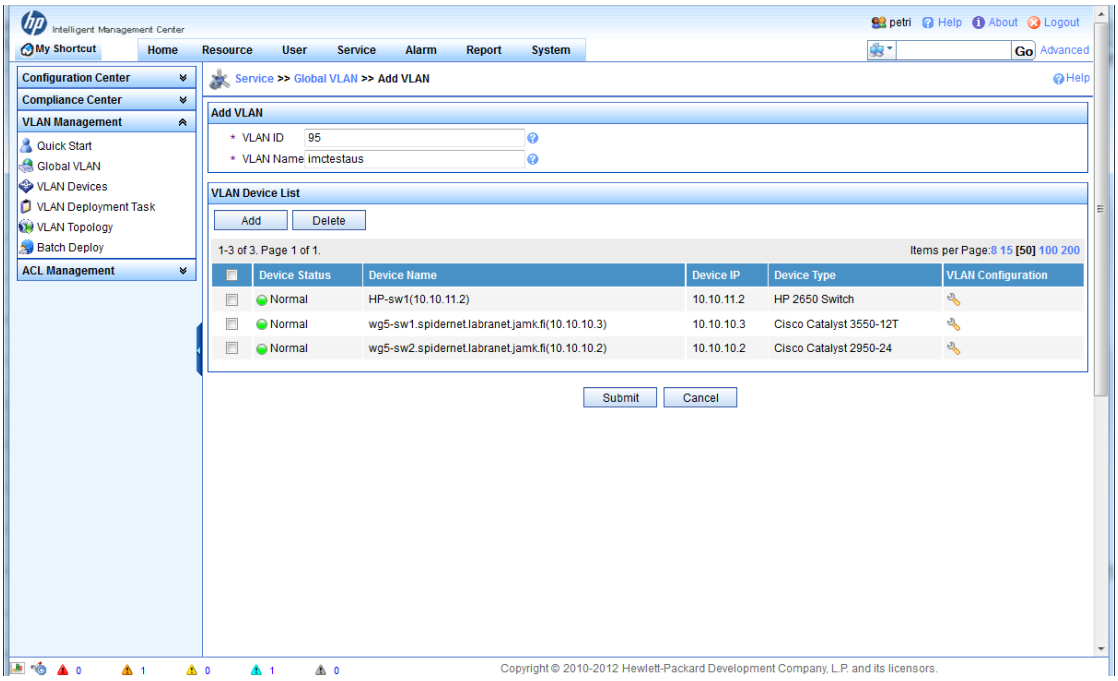
6.6.2 Testaus ja tulokset

VLAN-verkkojen hallinnan toimintaa testattiin luomalla jokaiselle laitteelle uusi VLAN-verkko, liittämällä portteja tähän VLAN-verkkoon ja poistamalla kyseinen VLAN-verkko. Jokaisen IMC-järjestelmässä tehdyn muutoksen jälkeen varmistettiin laitteelta muutoksen onnistumisen. Tämän ominaisuuden testauksessa käytettiin wg5-sw1, wg5-sw2 ja hp-sw1 -laitteita.

VLAN-verkkojen hallinnan testaaminen aloitettiin luomalla laitteille VLAN-verkko käyttäen IMC-järjestelmän yleistä VLAN (Global VLAN) -ominaisuutta käyttäen.

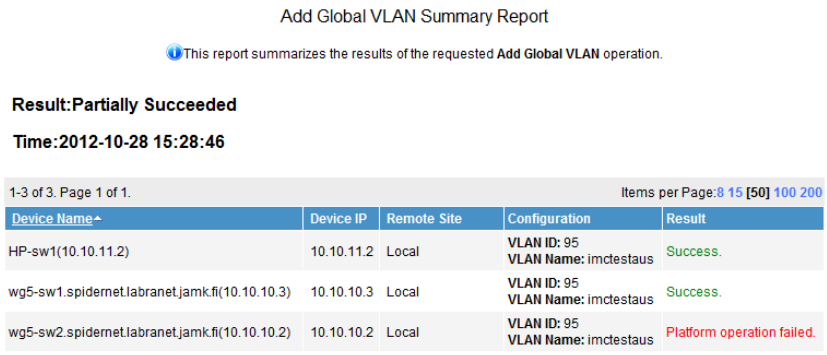
Service → Vlan Management → Global VLAN

Tällä ominaisuudella voi luoda tai poistaa VLAN-verkkoja halutuista laitteista yhdellä kertaa. Kuviossa 21 on asetukset, joilla määriteltiin uusi VLAN-verkko wg5-sw1, wg5-sw2 ja hp-sw1 -laitteille. Kyseisen verkon nimeksi määriteltiin ”imctestaus” ja VLAN-verkon tunnisteeksi numero 95.



KUVIO 21. Asetukset VLAN-verkon luomiseksi laitteille

Kuten nähdään kuviosta 22, IMC ohjelmisto ilmoitti VLAN-verkon luonnin onnistuneen wg5-sw1 ja hp-sw1 -laitteille, mutta epäonnistuneen wg5-sw2-laitteelle.



Add Global VLAN Summary Report

This report summarizes the results of the requested **Add Global VLAN** operation.

Result:Partially Succeeded

Time:2012-10-28 15:28:46

1-3 of 3. Page 1 of 1. Items per Page:8 15 **[50]** 100 200

Device Name	Device IP	Remote Site	Configuration	Result
HP-sw1(10.10.11.2)	10.10.11.2	Local	**VLAN ID:** 95 **VLAN Name:** imctestaus	Success.
wg5-sw1.spidernet.labranet.jamk.fi(10.10.10.3)	10.10.10.3	Local	**VLAN ID:** 95 **VLAN Name:** imctestaus	Success.
wg5-sw2.spidernet.labranet.jamk.fi(10.10.10.2)	10.10.10.2	Local	**VLAN ID:** 95 **VLAN Name:** imctestaus	Platform operation failed.

KUVIO 22. Uuden VLAN-verkon luonnin tulos

Seuraavaksi asetettiin jokaiselta laitteelta yksi portti Access-tilaan (untagged port) ja yksi portti Trunk-tilaan (tagged port). Tämän jälkeen tarkastettiin VLAN-verkkojen asetukset laitteilta.

Wg5-sw2-laitteelta VLAN-verkkojen asetukset tarkastettiin komennolla ”show vlan”, sekä Trunk-portin asetukset komennolla ”show interfaces fa0/2 switchport”.

```
wg5-sw2#show vlan
VLAN  Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23
50   imc_hallinta                     active    Fa0/24
95   imctestaus                       active    Fa0/11
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

wg5-sw2#show interfaces fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 30 (Inactive)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 95
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

Komennon ulostulosta nähdään VLAN-verkon luonnin onnistuneen ja portti ”Fa0/11” on liitetty kyseiseen VLAN-verkkoon, vaikka IMC ohjelmisto ilmoitti virheestä kyseisen operaation suorittamisessa. Laitteen portti ”Fa0/2” on myös määritetty onnistuneesti Trunk-tilaan.

Myös laitteelta wg5-sw1 tiedot VLAN-verkoista nähdään samalla komennolla. Lisäksi nähdään portin ”Gi0/11”-asetukset vastaavalla komennolla kuin aiemmin.

wg5-sw1#show vlan

VLAN	*Name*	*Status*	*Ports*
1	*default*	*active*	*Gi0/4, Gi0/5, Gi0/7, Gi0/8*
			Gi0/9, Gi0/10, Gi0/12
50	*imc_hallinta*	*active*	
95	*imctestaus*	*active*	*Gi0/6*
1002	*fddi-default*	*act/unsup*	

1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

wg5-sw1#show interfaces gi0/11 switchport
Name: Gi0/11
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 30 (Inactive)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 95
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Komennon ulostulosta nähdään että VLAN-verkon luonti oli onnistunut ja portti ”Gi0/6” on liitetty kyseiseen VLAN-verkkoon, sekä portti ”Gi0/11” oli määritelty onnistuneesti Trunk-tilaan.

Hp-sw1-laitteelta kyseisen VLAN-verkon asetukset nähdään ”show vlans 95”-komennolla.

HP-sw1# show vlans 95

Status and Counters - VLAN Information - Ports - VLAN 95

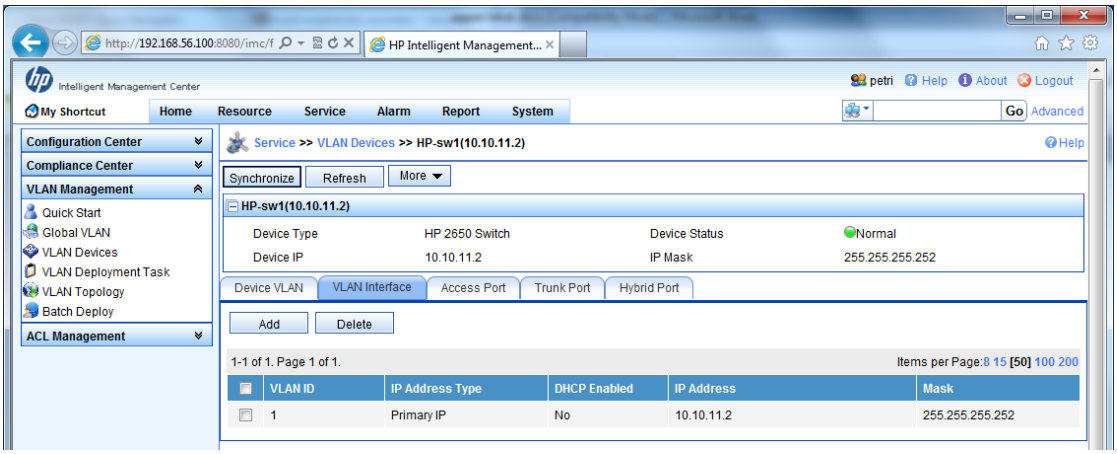
802.1Q VLAN ID : 95

Name : imctestaus
Status : Static

Port Information Mode Unknown VLAN Status
--------------- -------- ------------ ----------
3 Tagged Learn Down
5 Untagged Learn Down

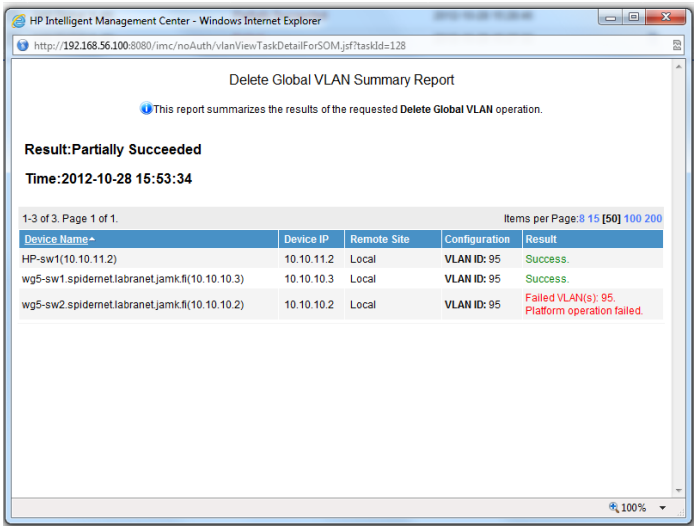
Komennon ulostulosta nähdään, että VLAN-verkko oli luotu onnistuneesti ja portti 3 on liitetty Trunk-portiksi ja portti 5 Access-portiksi.

IMC-järjestelmällä on myös mahdollista hallita hp-sw1 kytkimen virtuaalisia verkkoliityntojä (Virtual Interfaces), kuten nähdään kuviosta 23.



KUVIO 23. Hp-sw1-laitteen Virtual Interface -hallinta

VLAN-verkon poistaminen suoritettiin ”Global VLAN”-valikosta. Kuvion 24 IMC-operaation raportista nähdään VLAN-verkon poisto -operaation onnistuneen wg5-sw1 ja hp-sw1 -laitteilla, mutta epäonnistuneen wg-sw2-laitteella.



KUVIO 24. VLAN-verkon poistaminen

Laitteilta tarkastettaessa oli kyseinen VLAN-verkko poistunut wg5-sw1 ja hp-sw1 -laitteista, kuten myös wg5-sw2-laitteelta.

7 YHTEENVETO

7.1 Työn toteutus

Työn toteutus alkoi IMC-järjestelmän asentamisella virtuaali-palvelimelle ja palvelimen liittämisellä SpiderNet-laboratorioverkkoon. Tämän jälkeen aloitin IMC-järjestelmän ominaisuuksiin tutustumisen, sen asetuksien määrittelemisen ja kokeilin liittää SpiderNet-laboratorioverkon-laitteita hallittavaksi. IMC-järjestelmän asentamisessa en törmännyt ongelmiin ja IMC-asennusohje oli kattava. Kun IMC-testiympäristö oli todettu toimivaksi, aloitin testi-topologioiden ja testauksien suunnittelun. Tämän jälkeen suoritin kappaleessa 6 kuvatut testaukset.

Testauksia suorittaessa ongelmia aiheutti SSH-yhteyden toimimattomuus Ciscon-laitteiden ja IMC:n välillä, sekä laitteiden asetusten palauttamisen toimimattomuus Juniperin ja HP:n -laitteilla.

Tässä työssä sain käyttöönotettua toimivan verkonvalvontajärjestelmän SpiderNet-laboratoriossa ja toteutettua suunnitellut testaukset. Tekemieni testien perusteella IMC-järjestelmän Auto Discovery -ominaisuus toimii, kuten sen kuuluukin ja sen avulla löysi halutut laitteet. Myös VLAN-hallinta ominaisuus oli toimiva ja hyödyllinen ominaisuus, koska se mahdollistaa VLAN-verkkojen hallitsemisen yhden käyttöliittymän kautta monen eri valmistajan laitteilla. IMC-järjestelmän laitteiden asetusten hallinta ei toiminut kaikilla laitteilla täysin asetusten palautuksen osalta, tästä huolimatta asetusten hallinta ominaisuus on käyttökelpoinen, koska sillä saatiin laitteiden asetukset varmuuskopioitua ja kyseinen varmuuskopiointi toiminto on mahdollista automatisoida. Testauksien ja käyttökokemuksieni perusteella osa IMC-järjestelmän ominaisuuksista on vielä keskeneräisiä ja vaativat korjaamista.

Testauksien valmistuttua pidin koulutustilaisuuden muutamalle PVJJK:n Verkkoyksikön työntekijälle, jossa esittelin heille IMC:n ominaisuudet, suoritetut testit ja testeissä ilmenneet ongelmat.

Työssäni saamia tuloksien pohjalta voi PVJJK:n henkilökunta jatkaa IMC-järjestelmän käyttöönottoa heidän omassa ympäristössään ja opinnäytetyössä löydettyjen ongelmien perusteella heidän on mahdollista arvioida IMC:n ominaisuuksien käytettävyyttä heidän omassa organisaatiossa.

Opinnäytetyön aikataulu venyi hiukan työssä tekemieni testien suhteen, mutta kokonaisuudessaan sain työn valmiiksi alussa tehdyn aikataulun mukaisesti.

IMC:n vastaavuus ITILin vaatimuksiin

Mielestäni HP IMC-järjestelmä saadaan vastaamaan ITILin vaatimuksia kun siihen asennetaan palvelutuotanto-moduuli (Service Operation Module, SOM). Tämän moduulin avulla voidaan helposti toteuttaa ITILin eri prosesseja, kuten muutoksenhallinta ja viankorjaus -prosessit. Lisäksi kyseinen moduuli tuo mukanaan konfiguraationhallintatietokannan (CMDB), johon saadaan tallennettua verkonhallinnan kannalta arvokasta tietoa laitteista ja palveluiden riippuvuuksista laitteisiin. Kun tarvittavat

prosessit on muokattu organisaatiolle sopiviksi ja viety IMC-järjestelmään ei tarvita erillistä ohjelmistoa ITILin-prosessien toteuttamiseen.

7.2 Jatkokehitys

Seuraavana PVJJK:n tulisi testata heidän tärkeimmiksi katsomiaan IMC:n ominaisuuksia, heidän käytössä olevilla laitteilla ja ohjelmistoversioilla. Lisäksi tulisi tutkia IMC-järjestelmän hierarkkista toteutusta, jossa on useampia IMC palvelimia. Tämän pitäisi parantaa verkonhallinnan vikasietoisuutta, kun palvelimet hajautetaan maantieteellisesti eri kohteisiin. Lisäksi SOM-lisäosan prosessit täytyy muokata organisaatiolle sopiviksi.

IMC-järjestelmään on saatavilla suuri määrä laajennus moduuleita, joiden avulla on mahdollista toteuttaa monipuolista laitteiden ja verkkojen hallintaa. Näistä moduuleista mielestäni mielenkiintoisimpia testattavia olisivat QoS- ja MPLS VPN -hallinta -moduulit.

JAMK tietoverkkotekniikan koulutuksessa IMC-järjestelmää voisi hyödyntää esimerkiksi verkonhallinta tekniikoiden (SNMP, SSH) opetuksessa. Lisäksi mahdollinen tutkimuksen kohde on IMC Langattomien palveluiden hallinta -moduulin toiminta (Wireless Services Manager) LabraNetin WLAN-tukiasemien kanssa ja verrata sen toimintaa Ciscon vastaavan tuotteeseen.

LÄHTEET

Alanko, J. 2012. ATK-erikoissuunnittelija. Puolustusvoimien Johtamisjärjestelmäkeskus. Haastattelu 3.5.2012

HP Intelligent Management Center. N.d. Viitattu 8.9.2012. http://www.hp.com haku: imc standard → HP Intelligent Management Center Standard Software Platform.

HP Intelligent Management Center Installation Guide. 2012. Viitattu 19.6.2012. http://www.hp.com.

HP Intelligent Management Center Base Platform Administrator Guide. 2012. Viitattu 19.6.2012. http://www.hp.com.

History of ITIL. N.d. Viitattu 8.9.2012. http://wiki.en.it-processmaps.com/index.php/History_of_ITIL.

ITIL Service Operation. 2011. The Stationary Office.

ITIL Service Transition 2007. The Stationary Office.

Mauro, D. & Schmidt, K. 2005. Essential SNMP. 2. uud. p. Sebastopol, CA: O'Reilly.

Puolustusvoimien Johtamisjärjestelmäkeskus. 2008. Puolustusvoimien verkkosivut. Viitattu 25.6.2012. http://www.puolustusvoimat.fi/ → Laitokset → Puolustusvoimien johtamisjärjestelmäkeskus.

RFC 1157. 1990. A Simple Network Management Protocol (SNMP). http://www.ietf.org/rfc/rfc1157.

SpiderNet. 2009. SpiderNet-laboratorioverkon esittely. Viitattu 11.6.2012. http://student.labranet.jamk.fi/SpiderNet/.

The Official Introduction to the ITIL Service Lifecycle. 2007. The Stationery Office.

LIITTEET

LIITE 1. Testeissä käytettyjen laitteiden mallit ja ohjelmistoversiot.

Laite	Malli	Ohjelmistoversio
wg5-r1	Cisco Systems 2821	C2800NM-ADVIPSERVICESK9-M, Version 12.4(24)T2
wg5-sw1	Cisco Systems Catalyst 3550	C3550-I5K2L2Q3-M, Version 12.1(22)EA6
wg5-sw2	Cisco Systems Catalyst 2950	C2950-I6K2L2Q4-M, Version 12.1(22)EA3
wg5-sw3	Extreme Networks Summit aX250e	ExtremeXOS version 12.5.2.6 v1252b6
juniper-r1	Juniper J2320	JUNOS Software Release [11.2R5.4]
juniper-r2	Juniper J2320	JUNOS Software Release [11.2R5.4]
juniper-r3	Juniper J2320	JUNOS Software Release [11.2R5.4]
juniper-r4	Juniper J2320	JUNOS Software Release [11.2R5.4]
juniper-r5	Juniper J2320	JUNOS Software Release [11.2R5.4]
hp-sw1	Hewlett-Packard Procurve 2650	H.07.31

LIITE 2. Muokattu Enter_exec.tcl tiedosto.

```
#*****************************************************************
******
# Identification:enter_exec
# Purpose:      enter the "exec" mode on the device
#*****************************************************************
******

set IGNORE_DELAY true
if {$banner_skip_repeat != "0"} {
        expect -re "$banner_skip"
        expect "*"
}

set loop true
while {$loop == "true"} {
        expect {
                "Last login:" {
                        expect $exec_prompt
                        send "\r"
                        expect $exec_prompt
                        set loop false
                } -re $password_prompt {
                        if {$password == "\x24password" || $password == ""} {
                                set ERROR_MESSAGE "Missing password"
                                set ERROR_RESULT true
                                return
                        } else {
                                send "$password\r"
                                set sent_password "true"
                        }
                } -re $next_passcode_prompt {
                        if { $use_securid != "exec" && $use_securid != "enable" } {
                                set ERROR_MESSAGE "Device not configured for Se-
curID."
                                set ERROR_LOGIN true
                                cleanup
                                return
                        }
                        send "$next_passcode\r"
                } $username_prompt {
                        if { $use_securid != "\x24use_securid" && $sent_password ==
"true" } {
```

```
                        set ERROR_MESSAGE "SecurID authentication failed."
                        set ERROR_LOGIN true
                        cleanup
                        return
                    } else {

                        if {$username == "\x24username" || $username == ""} {
                            set ERROR_MESSAGE "Missing username"
                            set ERROR_RESULT true
                            return
                        } else {
                            send "$username\r"
                            set sent_password "false"
                        }
                    }
                } "new tokencode:" {
                    send "$next_passcode\r"
                } "Enter a new PIN" {
                    set ERROR_MESSAGE "Could not login. A new pin needs to be
created for this Secure ID user."
                    set ERROR_RESULT true
                    return
                } "error: Unable to authenticate" {
                    set ERROR_MESSAGE "Super-user account is required for device
management."
                    set ERROR_RESULT true
                    return
                } $exec_prompt {
                    send "\r"
                    expect $exec_prompt
                    set loop false
                } "Authentication failed" {
                    set ERROR_MESSAGE "Authentication failed"
                    set ERROR_RESULT true
                    return
                } "Login incorrect" {
                    set ERROR_MESSAGE "Login incorrect"
                    set ERROR_RESULT true
                    return
                } "Store key in cache? (y/n)" {
                    send "y\r"
                }
            }
        }
```

```
if {$useTruePrompt != "false" } {
        send "\r"
        expect -re "(.*?$exec_prompt)"
        set exec_prompt $expect_out(1,string)
}
if {$resetMorePrompting != "false"} {
        send "set cli screen-length 0\r"
        expect $exec_prompt
}
set IGNORE_DELAY false
```