jamk.fi

Keskitetyt verkonhallintajärjestelmät

Sami Suomi

Opinnäytetyö
Huhtikuu 2020
Tekniikan ala
Insinööri (AMK), Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Sami Suomi	Opinnäytetyö, AMK	4 / 2020
	Sivumäärä 48	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Keskitetyt verkonhallintajärjestelmät

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Juha Piispanen, Jarmo Viinikanoja

Toimeksiantaja(t)
Nodeon Finland Oy

Tiivistelmä

Työn toimeksiantaja toteutti asiakkaalleen selvitystyön, jossa tutkittiin keskitettyjen verkonhallintajärjestelmiä sekä niiden soveltuvuutta heidän infrastruktuuriinsa. Keskitetyt verkonhallintajärjestelmät nopeuttavat laajojen tietoliikennekokonaisuuksien ajantasaisuuden ylläpitoa monitoroimalla siihen liitettyjen tietoliikennelaitteiden tilaa sekä antamalla käyttäjilleen mahdollisuuden nopeilla toimenpiteillä toteuttaa tietoliikennelaitteiden konfiguraatiollisia muutoksia tai ohjelmistoversioiden päivityksiä.

Tutkimuksessa keskityttiin markkinoilla oleviin on-premise-ratkaisuihin, jotka pystyvät toteuttamaan tietoliikennelaitteiden monitoroinnin sekä tarvittavat muutostyöt näille laitteille. Pelkkään monitorointiin tarkoitetut ratkaisut on rajattu pois tutkimustyön alueesta. Tietoliikenneverkon päätelaitteiden, joihin voivat kuulua työkoneet, palvelimet, langattomat tukiasemat tai vastaavat laitteet, monitorointi ja hallinta rajattiin myös pois ja työssä keskityttiin paikallisten tietoliikennelaitteiden seurantaan sekä hallintaan.

Tuloksina keskitettyjen verkonhallintajärjestelmien tutkimustyössä selvitettiin järjestelmien toimintaperiaatteita sekä eroavaisuuksia niiden toiminnallisuuksissa. Monitoroinnit sekä muutostöiden teko hallintajärjestelmillä ovat kaikilla tutkituilla järjestelmillä pitkältikin samoilla protokollilla toteutettuina.

Avainsanat (asiasanat)

Keskitetty hallinta, tietoliikenne

Muut tiedot (Salassa pidettävät liitteet)
Liite 2 on salassa pidettävä, ja se on poistettu julkisesta työstä. Salassapidon perusteena on yksityisen, valtion, kunnan tai muun julkisyhteisön, yhteisön, laitoksen tai säätiön liike- tai ammattisalaisuudet (JulkL 24§, 17 ja 20).

jamk.fi

Description

Author(s)	Type of publication	Date
Suomi, Sami	Bachelor's thesis	4 / 2020
		Language of publication: Finnish
	Number of pages: 48	Permission for web publication: x

Title of publication

Centralized network management systems

Degree programme

Information and Communication Technology

Supervisor(s)

Piispanen Juha, Viinikanoja Jarmo

Assigned by

Nodeon Finland Oy

Abstract

Research on centralized networking management systems was produced by the assigner to their client. Centralized network management systems quicken the maintenance and upkeep of broad networks, by monitoring attached network devices or by giving the administrator a possibility to make quick configuration changes to multiple devices at the same time.

Research on centralized network management systems was primarily focused on on-premise solutions which were able to monitor the attached networking devices and manage their configuration files. End devices like desktops, servers, wireless APs or similar devices were not the in the scope of the research. Research heavily focuses on monitoring and managing site networking devices such as switches and routers.

As a result of the research work on the network management systems, the operating principles of the systems were clarified as well by comparing the differences in their functionalities. Monitoring and the modification tasks with different management systems were largely carried out with the same protocols and technologies.

Keywords/tags (subjects)

Centralized management, networking

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Johdanto

1.1 Tutkimuksen kuvaus

Tutkimustyö keskitetyistä verkonhallintajärjestelmistä toteutettiin tilaustyönä Nodeon Finland Oy:n asiakkaalle. Asiakkaan tarpeina oli selvittää, kuinka hallita ja ylläpitää suuren kytkin/reititin laitemäärän omaavan tietoliikenneverkkonsa, kuinka toteuttaa näiden laitteiden järjestelmätiedostoihin muutoksia sekä tarve saada kerättyä informaatio laitteisiin liitetyistä lisäosista. Markkinoilla on useita nämä tehtävät toteuttavia järjestelmiä, mutta näiden toiminnallisuuksista ei, markkinointipuheet pois lukien, tilaajalla ole kokemusta, ja tämän tiedon tiivistämiseksi toteutettiin selvitystyö verkonhallintajärjestelmistä.

1.2 Tutkimusasetelma

Tutkimustyö on toteutettu kvalitatiivisena eli laadullisena tutkimustyönä. Laadullisena tutkimuksessa voidaan käyttää monia eri tutkimusmenetelmiä, joissa tutkija osallistuu tutkimusprosessiin, ja näin ollen tutkimuksen tunnusmerkkeinä toimii narratiivinen selostus työn vaiheista, aineistolähtöinen analyysi, hypoteesittomuus sekä tutkimuksen joustava suunnittelu ja toteuttaminen. (Järvenpää, E. 2006.)

Tutkimustyön tarkoituksena oli tutkia syvällisemmin saatavilla olevien verkonhallintajärjestelmien ominaisuuksia sekä vertailla eri verkonhallintajärjestelmien käyttöönottoa, toiminnallisuuksia sekä eroavaisuuksia. Tällä pyritään saamaan päivittynyt näkymä lukijalle tämänhetkisten tarjolla olevien verkonhallintaratkaisuiden mahdollisuuksista sekä mitkä asiat ovat huomioon otettavia verkonhallintajärjestelmien kanssa.

1.3 Toimeksiantaja

Opinnäytetyö toteutettiin Nodeon Finland Oy:lle. Nodeon Finland Oy on vuonna 2013 perustettu kriittisen infrastruktuuriin erikoistunut teknologia-asiantuntija sekä kasvuhakuinen yritys, joka tarjoaa palveluita usealta eri osa-alueelta. Nodeon Finland Oy:ltä löytyy asiantuntijuutta usealta eri asiantuntija-alueelta, joita ovat automaatiosuunnittelu, sähkösuunnittelu, valaistussuunnittelu, tietoliikennesuunnittelu, tele- ja turvajärjestelmät, järjestelmäarkkitehtuuri sekä järjestelmien integraatiot. Näitä aloja yhdistämällä Nodeon Finland tarjoaa asiantuntijuutta älykkään liikenteen projekteissa, liikennevirtojen mittauksissa ja analysoinnissa, liikenteen varoitus- ja opastusjärjestelmien parissa, teollisessa internetin (Internet of Things) ratkaisuissa sekä näiden muiden monipuolisten suunnitteluprojektien parissa. (Suunnitteluosaaminen, n.d)

2 Keskitetyt verkonhallintajärjestelmät

2.1 Yleistä

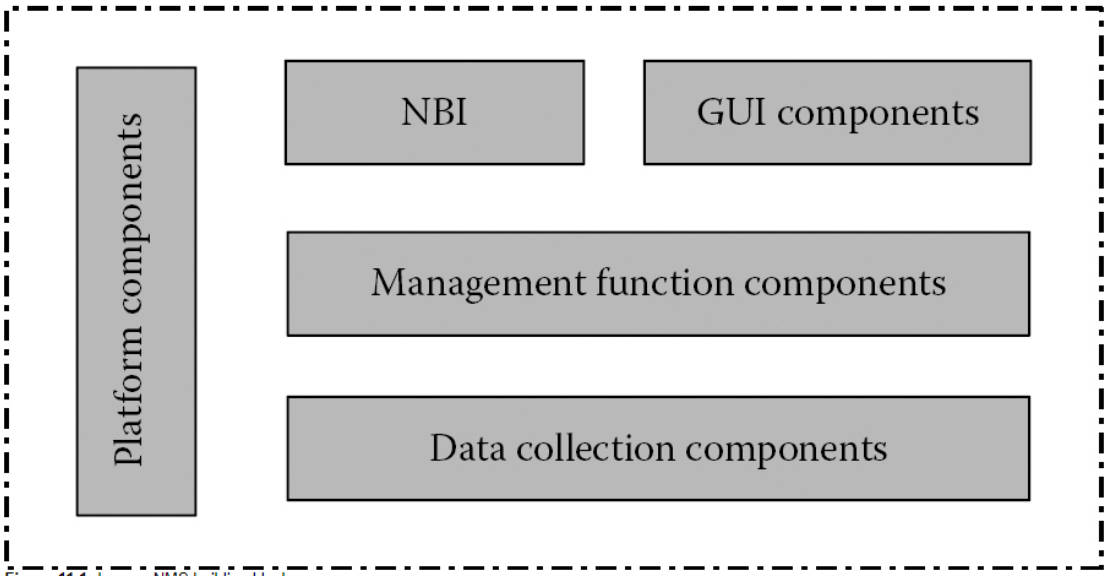
Perinteisellä tavalla toteutetut tietoliikenneverkkojen muutostyöt on toteutettu tietoliikenneasiantuntijoiden toimesta etäyhteyksien avulla laitteille ja tekemällä tarvittavat muutostyöt komentorivien kautta. Tämä kuitenkin on hidasta ja aikaa vievä prosessi, jos muutoksen teko koskee useampaa tietoliikennelaitetta tai niiden luomaa loogista kokonaisuutta. Myös ihmisen tekemät useat toistuvat konfiguraatiomuutokset tietoliikenneverkon herkille asetuksille ovat alttiita virheille ja voivat pahimmassa tapauksessa keskeyttää tuotantoympäristössä olevien palveluiden toiminnan. Tämä voi tuoda suuriakin kustannuksia tietoliikenneympäristön ylläpitäjille SLA- (Service Level Agreement) sopimusten ehtojen täyttämisessä, jotka määrittelevät palvelutasojen toiminnallisuudet palveluntarjoajan sekä asiakkaan välillä.

Alati kasvavat tietoliikennekokonaisuudet sekä niiden tuoma kompleksisuus luovat haasteen niiden ylläpidossa. Tämä luo tarpeen kustannuksien laskemiseksi ja on tavoitettavissa vain hyvin hallitulla tietoliikenneverkolla. Kompleksisuutta saadaan vähennettyä luomalla yksinkertaisempia käyttöliittymiä verkon hallintaa varten. Vaihtoehtoisena ratkaisuna on käyttää useita tietoliikenneasiantuntijoita, mutta se luo lisäkustannuksia sekä riskejä. (Sathya, J. 2016.)

Ohjelmistokehittäjät sekä tietoliikenneasiantuntijat ovatkin kehitelleet ratkaisuja, joilla saataisiin toteutettua isojakin muutostöitä verkonhallintaa varten. Keskitetyt verkonhallintajärjestelmät ovat tällainen ratkaisu. Keskitetyllä verkonhallintajärjestelmällä (Network Management Systems, Network Control Manager) tarkoitetaan ohjelmistoa tai ohjelmistoja, joilla voidaan hallita ja monitoroida suuren tietoliikenneinfrastruktuurin laitteita, joihin kuuluvat kytkimet, reitittimet, tukiasemat ja mahdollisuuksien mukaan jopa virtuaaliset palvelimet sekä konesalien laitekanta. Se toimii järjestelmäylläpitäjän tehtäviä edesauttavana työkaluna laitekantojen ja niiden kautta kulkevan datavirran monitoroinnissa, laajan määrän fyysisten laitteiden ohjelmistoversioiden päivittämisessä sekä konfiguraatiotiedostojen jakelussa tai muuttamisessa. Keskitetyt verkonhallintajärjestelmät myös tukevat vianselvitystä nopeuttavina työkaluina järjestelmien ylläpitäjille. (Rouse 2018.)

Arkkitehtuurillisesti verkonhallintajärjestelmät voidaan lajitella pienempiin komponentteihin, joista kullakin komponentilla on tehtävä täytettävänään muodostaakseen kokonaisuuden. Kuviossa 1 kuvataan verkonhallintajärjestelmän kokonaisuutta, ja siihen kuuluvia komponentteja, joita ovat:

- Platform components
- North bound interface
- GUI components
- Data collecting components
- Management function components



Kuvio 1. Verkonhallintajärjestelmän komponentit. (Sathyan, J. 2016.)

Alustakomponentit (*Platfrom components*) sisältävät verkonhallintajärjestelmän tietokantoja käyttöä varten objektien tietueet, jotta taustalla olevia SQL-tietokantoja voitaisiin hyödyntää niin verkonhallintajärjestelmässä, kuin myös mahdollisesti ulkopuolisella järjestelmällä. Tämä komponentti myös hoitaa lokien keräämisen, joista parsimalla voidaan luoda vaadittavia toimenpiteitä kuvaavat hälytykset. Kommunikaatioyhteyksien salaamista varten alustakomponentit salaavat välitetyt viestit laitteiden ja muiden järjestelmien väliltä. (Sathayan, J. 2010.)

Verkonhallintajärjestelmältä ulospäin lähtevä rikastettu data kulkee NBI:n (*North bound Interface*) kautta. Verkonhallintajärjestelmän käyttöliittymästä voidaan ohjata sille asetettujen noodien tilaa, mutta jotkin ohjelmistot toimivat verkonhallintajärjestelmän formatoidun tiedon avulla. Näitä ovat esimerkiksi Java-pohjaiset ohjelmistot sekä .NET-rajapinnat. (Sathayan, J. 2010.)

Graafisen käyttöliittymän komponentit (*GUI components*) verkonhallintajärjestelmän keräämän tiedon käyttäjäystävällisemmäksi esitystavaksi. GUI-komponentit tekevät esimerkiksi seuratuilta tietoliikennelaitteilta kerättyjen rajapintojen käyttöasteesta, vikatilanteista tai seuratun tietoliikenneverkon topologiasta käyttäjälle kuviot, jotka helpottavat käyttäjien työtä. (Sathayan, J. 2010.)

Tiedon keruuta varten verkonhallintajärjestelmillä on erilliset komponentit *(Data collecting components).* Tietoa voidaan kerätä seuratuilta tietoliikennelaitteilta tai erillisiltä järjestelmiltä useiden protokollien avulla, ja nämä protokollat yleensäkin ovat käytettävissä useiden eri valmistajien tuotteissa. Yleisimmät protokollat verkonhallintajärjestelmillä tiedonkeruussa on käytettyinä *simple network management protocol* (SNMP), *file transfer protocol* (FTP), *extensible Markup Language* (XML), tai *transaction language 1* (TL1). (Sathayan, J. 2010.)

Hallintakomponentteja (*Management function components*) on useita ja niiden tehtävä on toteuttaa muutostehtäviä järjestelmässä. Näitä tehtäviä on esimerkiksi vikatilanteista hälytyksen luominen, verkon kartoittaminen, konfiguraatiomuutokset laitteille perinteisesti komentorivin kautta, tai muutostyöt API-rajapintojen kautta. (Management (Sathayan, J. 2010.)

2.2 Vaatimukset hallintajärjestelmiltä

Tässä luvussa käsitellään vaatimukset, joiden perusteella keskitettyjä verkonhallintasovelluksia valikoitiin tarkempaa tutkimista sekä testaamista varten. Vaatimukset verkonhallintajärjestelmän ominaisuuksista on neuvoteltu Nodeon Finland Oy:n selvitystyön tilaajan kanssa, ja niiden perusteella on tehty valinnat, mitä keskitettyjä verkonhallintajärjestelmiä tutkitaan sekä testataan tässä tutkimustyössä. Vaatimukset ovat tiivistettynä tietona taulukossa 1 ja tarkemmin avattuna tässä luvussa, miksi nämä ovat vaatimuksia. Tutkimustyössä kartoitetut järjestelmät on listattu liitteessä 1, ja näistä järjestelmistä vaatimuksien perusteella on karsittu pois ne, jotka eivät täytä vaatimuksia tai täyttävät vaatimukset vain osittain.

Taulukko 1. Tiivistetty listaus vaatimuksista verkonhallintajärjestelmiltä.

- Konfiguraatioiden muutostöitä varten hallinta - Monitorointi - Inventaariotiedot - Laitekantojen ja käyttäjien ryhmittely - Laitekonfiguraatioiden oikeellisuus (Compliance Audits) - Tuki vähintään 1000 laitteen seurantaan/hallintaan - Muun tai kolmannen osapuolen järjestelmän tuottaman datan hyödyntäminen verkonhallintajärjestelmässä

Keskitetyltä verkonhallintajärjestelmältä vaaditaan pelkän verkon monitoroinnin lisäksi kykyä hallita sille asetettuja paikallisia tietoliikennejärjestelmiä. Hallinnan tulee tapahtua yhdestä käyttöliittymästä, jonka kautta käyttäjä saa näkymäänsä usean paikallisen järjestelmän tila-, hallinta- sekä inventaariotiedot. Paikallisella järjestelmällä tarkoitetaan yhtä tietoliikennekokonaisuutta, joka kattaa siihen järjestelmään kuuluvat päätelaiteet. Yleisesti eri paikalliset järjestelmät sijaitsevat maantieteellisesti erillään toisistaan. Vaatimuksiin kuuluu kyky luoda myös suuria massamuutoksia jo ennalta luotuun tietoliikennejärjestelmään tai päivittää suuren laitekannan ohjelmistoversiot uusimpaan on vaadittuna.

Verkonhallintajärjestelmälle etuna on myös seuratun tietoliikennejärjestelmän laitteiden konfiguraatiotiedostojen varmuuskopiointi sekä käytössä olevien konfiguraatiotiedostojen vertailun esimääriteltyihin arvoihin sekä ohjelmistoversioiden ajantasaisuuden tarkastaminen (Compliance Audit) tai varmuuskopioituihin tiedostoihin. Tällä voidaan tarkastaa, ettei tuotantoon ole joutunut virheellisiä konfiguraatiotiedostoja laitteille ajettavaksi.

Useat hallintajärjestelmät tarjoavat ympäristökokonaisuuksille eri kokoisia ratkaisuita palveluinaan. Näin ollen valmistajilla voi olla tarjolla sadalle laitteelle tuki ohjelmistossa tai päivitetymmässä versiossa tuki kymmenelle tuhannelle laitteelle. Näiden eri sovellusversioiden laitteistovaatimukset eroavat alustaltaan, ja rajauksena käytetään, että hallintajärjestelmäsovelluksen on tuettava 1000 laitteen hallintaa.

Keskitetyssä verkonhallintajärjestelmässä halutaan olevan mahdollisuus luoda ryhmittelyitä eri laitekantojen, niiden roolien, sijaintien tai tehtävätarkoituksen mukaisesti. Ryhmittelyä varten tulee järjestelmän kyetä kartoittamaan verkkokokonaisuudessa sijaitsevat tietoliikennelaitteet. Näiden ryhmittelytietojen lisäksi verkonhallintajärjestelmältä toivotaan kykyä kerätä seuraamaltaan verkko-osuudelta tietoliikennelaitekantojen inventaariotiedot. Näihin tietoihin sisältyvät laitteisiin kalustetut SFP-moduulit, virtalähteet sekä muut lisätarvikkeet.

Keskitetyltä verkonhallintajärjestelmältä toivotaan myös kykyä vastaanottaa muiden järjestelmien keräämää informaatiota. Käytettävissä voisi näin olla muun valmistajan luoma järjestelmä, jonka tuottamaa informaatiota voitaisiin hyödyntää hallintajärjestelmäsovelluksessa. Esimerkkinä monitorointityökalu Zabbixen keräämällä statistiikalla voitaisiin luoda yhteenvetoja tämän hallintajärjestelmän käyttöpaneelista ja tehdä tarvittavat muutostyöt automatisoidusti tai käyttäjän toimesta.

Seuraavat luvut tässä kappaleessa käsittelevät tarkemmin vaatimusmääreet täyttävät on-premise-verkonhallintaratkaisut. Tutkimustyöhön valikoitui viisi kappaletta eri valmistajien luomaa järjestelmää.

2.3 Cisco Prime Infrastructure 3.7

Cisco tarjoaa asiakkailleen Prime Infrastructure -palvelun, jonka sisällä on aikaisemmin CiscoWorks-nimikkeellä ollut paikallisten verkkojen hallintaratkaisu. Prime Infrastructuren avulla voidaan kartoittaa discovery-tehtävällä, monitoroida sekä hallinnoida Ciscon laitekantaa määritellyssä tietoliikenneverkossa. Cisco tarjoaa näin tukensa omalle laitekannallensa, joka vaihtelee Primen järjestelmäversioiden mukaisesti. Kuitenkin tuki kattaa Ciscolta yli 13000 laitemallin laitteet. (Compatibility information n.d.)

Cisco Prime Infrastructure -verkonhallintajärjestelmä on suunniteltu fyysisille ja langattomille verkkoyhteyksille. Prime Infralla voidaan hallita kampusverkon kokoisia verkkokokonaisuuksia sekä runkoverkon laitekantaa, jotka laitemääriltään voivat vaihdella 500 - 24 000 yksikön väliltä. Cisco Prime Infrastructurella halutaan tarjota

käyttäjälleen yhdestä käyttöliittymästä pääsy laitteiden hallintaan sekä monitorointiin. Palvelu pyrkii yksinkertaistamaan ja luomaan läpinäkyvyyttä muutostentekoon ja hallintaan. (Prime Infrastructure 3.x Data Sheet 2020.)

Ciscon tuottama Prime Infrastructure on pääpainotteisesti Single-Vendor-pohjainen ratkaisu, jonka suurin hyöty saadaan, kun käytetään saman valmistajan muita sovelluksia tai laitekantaa. Kuitenkin Ciscon tarjoamalla työkalulla on mahdollista monitoroida myös kolmannen osapuolen valmistamia laitteita erinäisten hallintaprotokollien ylitse. Tuki kolmannen osapuolen tietoliikennelaitteille jää geneeriseksi, eikä kaikkia mahdollisia Cisco Prime Infran ominaisuuksia voida niille hyödyntää. Esimerkiksi vaatimusmäärittelyissä nostettu konfiguraatiomuutosten sekä sovelluspäivitysten tekeminen kolmannen osapuolen laitteille ei onnistu Cisco Prime Infrastructuren tarjoamien työkalujen avulla.

Itse Prime Infra -hallintasovelluksen BASE-lisenssi ei ole tilausmaksupohjainen, ja se on kertakustannusluontoinen, mutta tälle on saatavilla erillinen tilausmaksupohjainen tuki. Lisensointi Cisco Prime Infrastructurelle on hinnoiteltuna seurattavien laitemäärien perusteella. Jokainen laitemalli, joka halutaan liittää Cisco Prime Infran hallintanäkymän alle, on hinnoiteltu erikseen.

Ominaisuuksia Prime Infrastructurelle on luotu useita. Lyhykäisyydessään taulukossa 2 on listattuna eri omaisuudet, jotka Cisco Prime Infra tarjoaa (Cisco Prime Infrastructure 3.x datasheet 2020.).

Taulukko 2. Tiivistelmä Cisco Prime Infrastructure 3.7:n ominaisuuksista

- Verkon topologian kartoittaminen L2/L3 tasolla ja sen visuaalinen esittäminen.
- Monitorointi sekä muutosten hallinta tietoliikennelaitteille.
- Päätelaitteiden liikennevuon seuranta.
- Mahdollisuus luoda omia muutospohjia (Config-template) Cisco-laitteille.
- Tietoliikennelaitekannan inventaarion hallinta.
- Näkymä laitteille kalustetuista SFP-moduuleista, verkkomoduuleista tai virtalähteistä.
- Yksittäisen tai usean laitteen ryhmittely yhteen tai useaan ryhmään.
- Ryhmittely sijainnin, järjestelmäkokonaisuuden tai laitemallin perusteella.
- Tietoliikennelaitteiden rajapintojen ryhmittely
- Salatut tiedonsiirtoprotokollat.
- Konfiguraatiotiedostojen vertailu sekä Compliance ominaisuus. (Compliance vain standard editionissa tai vastaavassa versiossa)

Ciscon Prime Infrastructure tarjoaa Compliance Audit -työkalun järjestelmällään. Tällä voidaan varmistaa verkon tietoliikennelaitteiden konfiguraatioiden noudattaminen esimääriteltyihin oletusarvoihin sekä vahvistetaan hallittujen laitteiden tietoturvallisuutta. Compliance-tehtävät määritellään käytäntöihin. Auditoinnissa järjestelmä tutkii laitteen konfiguraatiotiedoissa olevaa tekstiriviä, show-komennolla saatua ulostuloa tai laitteen tilatietoa. Ulostulon vertailuun voidaan käyttää säännöllistä lauseketta. Tehtävälle voidaan tämän lisäksi määritellä toiminta-askel, jonka se toteuttaa määriteltyjen ehtojen tullessa voimaan. Luodut tehtävät voivat voimaan tullessaan luoda ilmoituksen järjestelmävalvojalle, kertoa sen kriittisyydestä tai jopa antaa valmiin korjausehdotuksen, jonka voi suoraan ajaa kohdelaitteelleen, jos sellainen korjausehdotus on luotuna. (Auditing device configurations for compliance 2020.)

Palvelualustana Prime Infrastructure tarjoaa firmware/softwaretiedostoille säilytyspaikan, jonka kautta voidaan jakaa määritellyt päivitysversiot laitteille. Säilytyspaikkaan voidaan siirtää imaget lataamalla ne verkkolaitteelta, lataamalla suoraan Ciscon sivustolta, URL:in kautta, FTP-protokollan ylitse tai suoraan paikalliselta asemalta Web-käyttöliittymän avulla.

Sovellusversioiden päivitykset voidaan jakaa paikallisen levyjakopalvelimen (Cisco Primen oma repositorio) kautta tai *config*-muutospohjien kautta tulee määritellä erillinen FTP/TFTP/SFTP-palvelin, jota käytetään ohjelmistojen päivitysversioiden jakamisessa tietoliikennelaitteille.

Järjestelmävaatimukset Cisco Prime Infrastructurelle

Prime Infrastructuresta on seitsemän eri versiota tarjolla. Ominaisuuksiltaan versiot ovat samanlaisia, mutta alustavaatimukset kasvavat seurattujen objektien määrän kasvaessa. Virtuaaliympäristössä käytettävät versiot ovat Express, Express-Plus, Standard sekä Professional. Puhtaasti fyysisellä alustalla toimivat versiot ovat Hardware Appliance Gen 2/3 sekä DNAC Appliance. Compliance Audit on käytettävissä Standard, Professional, Hardware Appliance Gen 2/3 sekä DNAC Appliance versioissa. (Cisco PI 3.7 Quick Start guide 2019)

Cisco Prime Infrastructure voidaan asentaa paikallisesti Ciscon tarjoamalle paikalliselle palvelimelle. Vähimmäisvaatimukset paikallisen palvelun käyttämiselle on listattu taulukossa 3.

Taulukko 3. Cisco Prime Physical Appliance system requirements. (Cisco PI 3.7 Quick Start guide 2019)

CPU	10 ydintä / 20 threads
Keskusmuisti	64 GB
Kiintolevytila	3600 GB (4x900GB) RAID 10
Kiintolevyjen I/O nopeus	320 MBps

Virtuaalisessa ympäristössä käytettynä Cisco Prime Infrastucture vaatii käytettäväkseen VMware ESXi version 6.0, 6.5 tai 6.7. Cisco tarjoaa valmiin OVA-imagen, jonka voi tuoda suoraan VMwaren alustalle. Standard edition:issa, joka kattaa vaatimuksissa olevat halutut määreet ovat taulukon 4 mukaiset vähimmäisvaatimukset. Järjestelmän Snapshot-kuvia varten on kiintolevytilavaatimus korkea. (Cisco PI 3.7 Quick Start guide, 2019)

Taulukko 4. Cisco Prime Virtual Appliance system requirements. (Cisco PI 3.7 Quick Start guide 2019)

vCPU	16 ydintä
Keskusmuisti	64 GB
Kiintolevytila	600 GB
Kiintolevyjen I/O nopeus	200 MBps

2.4 SolarWinds

SolarWinds on Yhdysvaltalainen IT-alan yritys, joka tarjoaa verkkoinfrastruktuurin seurantaan ratkaisuja, jotka ovat jaoteltuina pienempiin kokonaisuuksiin. SolarWindsin tuotekategoriaan kuuluu verkonhallinta, järjestelmien hallinta, tietoturvallisuus, tietokantojen hallinta sekä sovellusten hallinta. (Solarwinds, n.d.) Tämän kokonaisuuden SolarWinds yhdistää yhdellä alustalla, jota kutsutaan SolarWinds Orioniksi. (How can IT be easier for you? n.d.)

SolarWinds on vuosien mittaan tehnyt useita yritysostoja, kuten Kiwi Enterprisesin (Morrison, C. 2009) sekä Rhinosoftin (Hay, R. 2012), ja implementoinut näiden kautta ostettujen yritysten luomia järjestelmiä omaan tuotekategoriaansa. Näin ollen SolarWindsillä on laaja kirjo useita eri työkaluja tarjolla kategoriassaan, ja ne ovat hinnoiteltuina erikseen. Käyttäjä voi täten räätälöidä tarpeidensa mukaisesti halutut työkalut SolarWinds Orion alustaan. Taulukkoon 5 on listattuna verkonhallinnan sekä monitoroinnin osalta SolarWindsin tarjoamat työkalut, jotka ovat oleellisimmat tutkimustyössä. Näiden Network Management-työkalujen lisäksi Solarwinds tarjoaa tietoturvaan, tietokannoille, ohjelmistoille sekä tukipalveluille omia ratkaistuita.

Taulukko 5. SolarWindsin verkonhallintaan ja -monitorointiin tarkoitetut työkalut (Network Management Licensed Products. n.d.)

SolarWinds työkalut	Selite
Network Perfomance Monitor	Verkon tilan sekä häiriöiden havaitseminen.
Network Configuration Manager	Tietoliikennelaiteiden konfiguraatiomuutosten luonti sekä luotujen tehtävien automatisointi.
Network Topology Mapper	Tietoliikenneverkon kartoitus sekä laitteiden havaitseminen.
ipMonitor	Verkko- sekä päätelaitteiden IP-monitorointi sekä näiden raportointi.
IP Address Manager	Aliverkkojen skannaus sekä DHCP, DNS ja IP-osoitteiden hallinta.
Log Analyzer	Lokitiedostojen parsiminen sekä määriteltyjen avainkohtien havaitseminen.
User Device Tracker	Kytkinten, kytkinporttien, päätelaitteiden sekä luvattomien käyttäjien monitorointi sekä hallinta.
NetfFlow Traffic Analyzer	Tietoliikennekaistan monitorointi ja analysointi. Applikaatioiden seuranta.
VoIP & QoS Manager	Voice over Internet Protocol- sekä Quality of Service-laadunvalvonta.
Engineer's Toolset	Erillinen työkalu Orion perheestä. Tukee monitoroinnin, hallinnan sekä Stress-testaukset. (Yksinkertaistettu käyttöliittymä)
Kiwi CatTools Kiwi Syslog Server	Erilliset työkalut SolarWinds-perheestä. Työkalu konfiguraatioiden massamuutoksille. (Yksinkertaistettu käyttöliittymä) Syslog server, keskistetty lokipiste.

Alustavaatimukset SolarWindsille

SolarWinds Orion voidaan ottaa käyttöön pilvipalveluissa, tai paikallisesti On-Premise pohjaisena ratkaisuna. SolarWinds Orion ilmoittaa vähimmäisvaatimukseksi yhdelle käyttöönotettavalle työkalulle taulukossa 6 olevat arvot. Kuitenkin jokaista lisättyä työkalua varten tulisi laitteistovaatimusten nousta CPU n+1 core sekä RAM n+2GB. Taulukkoon 6 on myös laskettuna hardwarevaatimukset Network Configuration Managerille, IP Address Managerille sekä Network Topology Mapperille, jotka täyttävät luvussa 2.2 listatut vaatimukset sekä tuen jopa 2000 laitteen monitorointia ja hallintaa varten. (Multi-module system guidelines, n.d.)

Orion platform vaatii käytettäväksi käyttöjärjestelmäkseen Windows Server 2008 R2, 2012/R2, tai Windows Server 2016. Valmista Open Virtualization Format (OVF) pohjaa ei ole saatavilla SolarWindsistä, ja palvelu toimii ainoastaan Microsoftin Windows Server pohjaisesti. Virtuaaliympäristöä hyödyntääkseen, tulee Windows Serveristä luoda erillinen virtuaalinen instanssi.

Taulukko 6. SolarWinds Orionin järjestelmävaatimukset(SolarWinds Orion Requirements, 2019)

	Vähimmäisvaatimukset	**Tarvittavilla työkaluilla olevat vaatimukset** -Network Configuration Manager -Network Topology Mapper -IP Address Manager
CPU	4 Corea	6 Corea
Keskusmuisti	8 GB	14 GB
Kiintolevytilaa	150 GB	150 GB
Verkkoliitäntä	Suositeltu 1 Gbps	Suositeltu 1 Gbps
Käyttöjärjestelmä	Windows Server 2016 (64-bit) Windows Server 2019 (64-bit)	Windows Server 2016 (64-bit) Windows Server 2019 (64-bit)

2.5 ManageEngine OpManager

ManageEngine OpManager on intialaisen vuonna 1996 perustetun Zoho Corporationin tytäryhtiö ManageEnginen luoma tietoliikenneverkon monitorointi- sekä hallintajärjestelmä. ManageEngine OpManager tarjoaa pienestä suureen skaalatun tietoliikenneverkon ylläpitämiseen hallintajärjestelmän. Hallintajärjestelmä kykenee seuraamaan tietoliikenneverkkojen lisäksi myös palvelimien, virtuaalisten palvelimien sekä muun palvelin infrastruktuuriin liittyvät komponentit. (Corporation Fact Sheet, n.d.)

OpManager on jaoteltuna eri sovellusjakeluihin, jotka pohjautuvat seurattavien noodien lukumäärien sekä haluttujen työkalujen sisältöön. Näitä erinäisiä jakeluita ovat Standard-, Professional- ja Enterprise-versiot. Näihin versioihin voidaan myös lisätä erillisiä työkaluja (Add-on) tarpeen mukaan. (Editions and Pricing, n.d.)

Testiympäristössä käytössä ollut versio ManageEngine OpManagerista on Standard, ja tästä versiosta puuttuivat työkalut verkkolaitteiden konfiguraatiomuutosten teolle sekä firmware/software-päivitysten ajamiselle. Nämä työtehtävät mahdollistava työkalu on lisäosana saatava Network Configuration Manager. OpManagerin Network Configuration Manager kuitenkin järjestelmän valmistajan dokumenttien mukaan täyttää vaatimuksissa olevat avainkohdat.

Alustavaatimukset ManageEngine OpManagerille

Alustavaatimuksiltaan ManageEngine OpManager ei vaadi suuria määriä resursseja alustaltaan, jolle se asetetaan toimintaan. Palvelinalustanaan ManageEngine OpManager evaluation -versio voi käyttää Windows 7 tai uudempaa tai Linux-jakeluista Ubuntua, Susea, RedHat Enterprisea, Fedorea tai Mandrakea. Tuotantoympäristöön tarkoitettu versio ManageEngine OpManagerista tukee kahta eri palvelinalustaa. Alustana voidaan siis käyttää isommassa ympäristössä joko Windows Server 2008 tai uudempaa tai RedHatin Enterprise 64-bit versiota. Järjestelmän alustavaatimukset tuotantopalvelimelle ovat taulukossa 7.

Taulukko 7. ManageEngine OpManagerin järjestelmävaatimukset (ManageEngine System Requirements n.d.)

	Vähimmäisvaatimukset
CPU	4 Core / 8 Threads
Keskusmuisti	16 GB
Kiintolevytilaa	100 GB
Verkkoliitäntä	Suositeltu 1 Gbps
Käyttöjärjestelmä	Windows Server 2008 / 2012 /2012 R2 / 2016 / 2019 (64-bit) Ubuntu / Suse / Red Hat Enterprise Linux (upto version 8) / Fedora / Mandriva (Mandrake Linux)

2.6 What's Up Gold

What's Up Gold on yhdysvaltalaisen Progress Softwaren kehittämä verkonhallintatyökalu. Hallinta-työkalu on lisenssipohjainen, joka korkeimmalla kultalisenssillä tarjoaa käyttäjälleen myös verkonhallintaan tarvittavat työkalut. Alhaisemmat lisenssimallit tarjoavat ainoastaan monitorointiin tarkoitetun version, joista puuttuu tämä vaatimuksissa mainittu verkonhallintaominaisuus.

What’s up Gold on vahvasti järjestelmien monitorointiin tarkoitettu sovellus, joka kattaa seurannan tietoliikenteen, palvelimien, pilvissä sijaitsevien palvelimien, konesalien ja päätelaitteiden osalta. Hallintajärjestelmällä pystytään kartoittamaan OSI-mallin L2- ja L3-tasolla verkkolaitteita sekä hallintasovellus kykenee yhdistämään muiden monitorointijärjestelmien tarjoaman informaation REST API -rajapintojen kautta. Mahdollisuus luoda automatisoituja tehtäviä, kuten uusien laitteiden lisääminen, tai tarvittavien muutostöiden teko on myös mahdollista tällä hallintasovelluksella. Listauksena taulukossa 8 What’s Up Goldin oletusominaisuuksista sekä erilisinä työkaluina tarjotut lisäosat. (Network Monitoring Software n.d.)

Taulukko 8. What's Up Goldin listaus ominaisuuksista

What’s Up Gold	Oletusominaisuudet	Lisäosien tuomat edut (Add-ons)
	- Verkon kartoittaminen OSI-mallin tasoilla L2 & L3 - Reaaliaikaiset hälytykset verkon objekteista - Sovellusten suorituskyvyn monitorointi - Pilvipalveluiden resurssien seuranta, ja raportointi - Verkon suorituskyvyn monitorointi - Virtualisoitujen alustojen monitorointi	- Verkon käytön analysointi - Palvelinsovellusten monitorointi - Konfiguraatioiden hallinta & muutostyöt - Virtualisoitujen ympäristöjen monitorointi

2.7 NetBrain

NetBrain Technologies Inc. on yhdysvaltalainen ohjelmistoyritys. Suomessa NetBrainin edustajana/jälleenmyyjänä toimii 5FeetNetworks. NetBrainin Technologies Incorporatedin eräänä tuotteena on tietoliikenneverkkojen automatisointiin suuntautunut NetBrain-ratkaisu, jonka avulla järjestelmän käyttäjä voi säästää vianselvitykseen menevästä ajasta, ja automatisoida muutoksentekoa. Ohjelmistolla kyetään luomaan Discover-ominaisuuksilla dynaamisia topologioita suoraan Microsoft-visiolle, Worddille sekä Excelille ja näin ollen avustaa avustamaan dokumenttien ajantasaisuuden ylläpitoa. (Dynamic Map n.d.)

NetBrainilla on käytössään patentoitu tietoliikennepolkujen kartoitustyökalu, joka hyödyntää verkon kartoittamisessa komentorivipohjaista sekä API-rajapintojen avulla tehtyä paikannuksia. Valmiiden NetBrainin tai NetBrainin yhteisön tekemien Runbookien avulla voidaan automatisoida tiettyjä tehtäviä eri osa-alueilla verkossa tai vianselvityksessä ajaa valmiita Runbookeja vian selvittämiksesi/korjaamiseksi. (Rokka, H. 2020)

NetBrain tarjoaa myös tuen virtuaaliympäristöjen seurannalle ja ohjaamiselle. Tällä kyetään seuraamaan konesaleissa olevien palvelimien tiloja sekä saamaan visuaalinen tuki virtualisoitujen laitteiden verkkoteknisen topologian rakentumisesta. (NetBrain features, 2020)

NetBrainin yhtenä tärkeänä ominaisuutena on kyky luoda digitaalinen kaksonen (Digital Twin) seuratusta tietoliikennekokonaisuudesta. Samanlaista digitaalista kaksosta hyödynnetään yleensä teollisuuden koneiden kunnossapidossa sekä tuotekehityksessä. Digitaalinen kaksonen rakentuu yleisestikin toteutetulla Discover-prosessilla, mutta NetBrainin etuna informaatiota kerätään noodeilta huomattavasti enemmän NetBrainin patentoidun tekniikan avulla. Kaikki komennot, joita tietoliikennelaitteen CLI- sekä API-rajapinnoista haetaan, tallennetaan tietokantaan, ja näiden kerättyjen tietojen perusteella NetBrain luo verkkotopologian sekä digitaalisen kaksosen järjestelmästä. (Rokka, H. 2020.)

Tämän patentoidun kartoittamistyökalun avulla NetBrain kykenee luomaan tarkemman kuvan tietoverkon rakenteesta ja sen tilasta verraten perinteisiin SNMP/ICMP-pollauksiin perustuviin tiedonkeruisiin. Digitaalisen kaksosen avulla voidaan nopeammin etsiä esimerkiksi End-To-End-ongelmatilanteita ilman, että tarvitsisi selvittää koko tietoliikennereitin varrella olevien laitteiden konfiguraatiotiedostoista eri rajapintojen ACL-, QoS-, tai PBR-konfiguraatioita. (Rokka, H. 2020)

NetBrain tukee usean eri laitevalmistajan reitittimiä, kytkimiä, palomuureja, ja palvelimia. Yhteensä vuoden 2020 alussa NetBrainilta tuettuna olevia laitemalleja on melkein 300 kappaletta. NetBrainille on valmistaja taulukoinut tukemiensa valmistajien laitteet sekä minkä tasoisesta seurannasta on kyse kullekin laitemallille. NetBrain

myös pyrkii lisäämään tarpeen tullen muiden valmistajien laitekantaa heidän tukemalleen listalle. (Multi-Vendor Support List, n.d.)

3 Järjestelmien tietoturva ja tulevaisuuden tuki

3.1 Tietoturva

Tietoturvan näkökulmasta keskitetty verkonhallintajärjestelmä tuo käyttäjälleen mahdollisuuden tehdä laajoja ja nopeita muutoksia nykyiseen tietoliikenneinfrastruktuuriinsa. Tietoliikennelaitteiden sovellusversioiden päivittämisen ja jakelun yksinkertaistaminen sekä nopeuttaminen edesauttaa tietoturva-aukkojen paikkaamista nopealla toiminnalla. Nopean toiminnan etuna on myös kustannusten laskeminen, kun muutokset saadaan tehtyä huomattavasti nopeammin verraten manuaaliseen työhön.

Hyödyntämällä nopean toiminnan mahdollisuutta laitteiden konfiguraatiomuutoksissa, voitaisiin luoda verkonhallintajärjestelmällä esimerkiksi kuukausittainen työtehtävä/tehtävät, joka muuttaisi eri järjestelmien tietoliikennelaitteiden paikallisten tunnusten salasanat. Tämä tehtävä tosin tuo lisäaskeleen uusien salasanojen jakelulle huoltotoimijoille.

Hallintaoikeuksien laajuus sekä hallinnoitavien paikallisten järjestelmien määrän ollessa suuri, luo tämä kysymyksen, kuinka paljon ”valtaa” keskitetyllä verkonhallintajärjestelmällä tulisi olla. Kun verkonhallintajärjestelmällä kyetään tekemään monia muutoksia, joilla pystytään mahdollisesti tuottamaan vahinkoa verkolle, voidaan tulkita, ettei verkonhallintajärjestelmän kautta tehtävien muutoksien ei tulisi olla pelkästään yhden käyttäjän hyväksyttävissä.

Tämän estämiseksi Cisco Prime Infra, Solarwinds ja NetBrain on mahdollistanut työtehtävien luomisen, jotka tulee hyväksyttää järjestelmävalvojan kautta. Näin yksittäi-

nen käyttäjä ei saa luotua tarkoituksellisesti tai vahingossa vääriä toimenpiteitä keskitetyllä verkonhallintajärjestelmällä. Hallintajärjestelmillä ei ole käytettävissään keinoa, jolla voitaisiin peruuttaa tehdyt muutostyöt. Jos mahdollisesti vääränlainen konfiguraatiomääritys ajetaan laitteille ja tämän myötä tietoliikenneyhteydet katkeavat, ei ole muuta keinoa kuin paikallisesti käydä palauttamassa verkkolaitteet entisille asetuksilleen.

Tarkastellessa Cisco Security Advisories tietokannan Prime Infran ilmoitettuja tietoturvahaavoittuvuuksia voidaan havaita, että vanhempiin Prime Infra versioihin on löydetty haavoittuvuuspinta-alaa erinäisten hyökkäystekniikoiden avulla. Havaittuja heikkouksia Cisco on paikkaillut päivityksillä, eikä uusimissa versioissa (Cisco PI 3.7 / 3.8) ole havaittu useaa kriittistä haavoittuvuutta. (Cisco Security Advisories, 2020)

Muiden järjestelmien kohdalla CVE-Details on kerännyt tietokantaansa kattavan listauksen tunnetuista tietoturva-aukoista, jotka eroavat vakavuudellaan toisistaan. CVE-Details on taulukon 9 mukaisesti löytänyt tutkituilta hallintajärjestelmiltä avoimia tieto-turvapuutteita, jotka ovat avoimia vielä huhtikuussa 2020. Tarkempaa tarkastelua varten tarjolla taulukossa myös linkki kyseiseen sivustoon.

CVE-Detailsin listauksissa on laaja kirjo erillisiä heikkouksia. Yleisimmät CVE-Detailsin ilmoittamat hyökkäyspinta-alat taulukossa 9 listatuista verkonhallintajärjestelmistä on WEB-pohjaiset hyökkäykset. Näistä WEB-pohjaisista heikkouksista useat ovat toteutettuna *Cross-site Ccripting* (XSS) metodilla. XSS mahdollistaa mahdollisen kuulumattoman tekijä lähettämään selainpohjaisen käyttöliittymän kautta injektion, joka sisältää vahingoittavan koodin, ja voi mahdollistaa kuulumattoman tekijän pääsyn järjestelmään. Myös verkonhallintajärjestelmien ylläpitämät SQL-tietokannat ovat alttiita hyökkäyksille erinäisten SQL-injektioiden kautta. Kriittisimmät listatut heikkoudet ovat kuitenkin *Exec Code*-pohjaiset toteutukset, joilla etähallinnan kautta kuulumaton tekijä voi syöttää erinäisten verkonhallintajärjestelmän tarjoamien palveluiden kautta vahinkoa tuottavan koodin järjestelmään.

Taulukko 9. CVE-Detailsin ilmoittamien haavoittuvuuksien määrät hallintajärjestelmille

Hallintajärjestelmä	**Tunnettujen haavoittuvuuksien määrä**	**CVE-Detailsin HTTPS-linkki haavoittuvuuksille**
Cisco Prime Infrastructure	52	Linkki
SolarWinds	42	Linkki
MangeEngine OpManager	45	Linkki
What's Up Gold	13	Linkki

Verkonhallintajärjestelmien avulla pystytään jakamaan käyttäjiä ryhmiin sekä antamaan käyttäjille tai ryhmille erillisiä oikeuksia järjestelmien käyttämisen suhteen. Näillä eri hallintaoikeustasoilla voidaan määritellä kuka tai mikä organisaatio voi tehdä muutostöitä hallittuun verkkoon, ja lisänä voidaan määritellä, tuleeko nämä muutostyöt hyväksyttää vielä toisen vastuuhenkilön toimesta.

3.2 Muiden sovellusten yhdistäminen palveluun

Yhtenä tutkittavana asiahaarana on myös selvittää, voidaanko jo aikaisemmin käytössä olevalta järjestelmältä tuoda sen keräämää informaatiota keskitetylle verkonhallintajärjestelmälle. Useat tutkituista keskitetyistä verkonhallintasovelluksista tukevat REST API-rajapintojen hyödyntämisen palvelussaan. Näille API-rajapinnoille on valmistajat luoneet erilliset dokumentaatiot käyttöä varten, joiden avulla helpotetaan ohjelman kirjoittamista, jolla haetaan attribuuttia, tai muokataan haluttuja objekteja.

API-rajapintojen ollessa ohjelmistovalmistajan luomia rajapintoja, on ne näin ollen yksilöllisiä omassa ympäristössään. Niiden lukemista varten keskityn hallintasovelluksen käyttöliittymässä, tulee olla valmistajalta luotuna sille front-end tuki, jotta se saataisiin käyttäjälle helposti ymmärrettävään muotoon.

Vaihtoehtoisesti monitorointijärjestelmän ja hallintasovellusjärjestelmien välille voitaisiin kehittää ohjelmistosovitin, joka toimii tulkkina näiden REST API-rajapintojen välillä, ja kääntää datan molemmille ymmärrettävänä muotoon.

Tutkituista keskitetyistä verkonhallintasovelluksista ei löytynyt suoraa mahdollisuutta käyttöliittymän näkymästä yhdistää erillisen palvelun tuottamaa dataa hyödynnettäväksi. Tämä toiminne tulee toteuttaa erillisien sovittimen avulla, jota ei valmistajilta tule suoraan hyllystä. Feature requestin avulla voidaan saada tuki valmistajilta erillisten sovittimien kehitystä varten, sekä uusien avoiminen API-rajapintojen luontia varten.

3.3 Tulevaisuus

Cisco Prime Infrastructure

Ciscolla on vankka asema markkinoilla tietoliikennelaitteiden sekä ohjelmistojen kehittäjänä, joten siltä on odotettavissa vahva tuki pidemmäksi aikaa tuottamilleen tuotteilleen. Cisco Prime Infrastructure on ollut markkinoilla vuodesta 2012 versionumerolla 1.1. Prime Infran versio 1.1 järjestelmävalmistajan tuki lopetettiin toukokuussa 2018. (End-of-Sale and End-of-Life Announcement for the Cisco NCS, WCS, LMS and Prime Infrastructure PIDs for versions 1.X, 2.X, and 3.0, heinäkuu 2018)

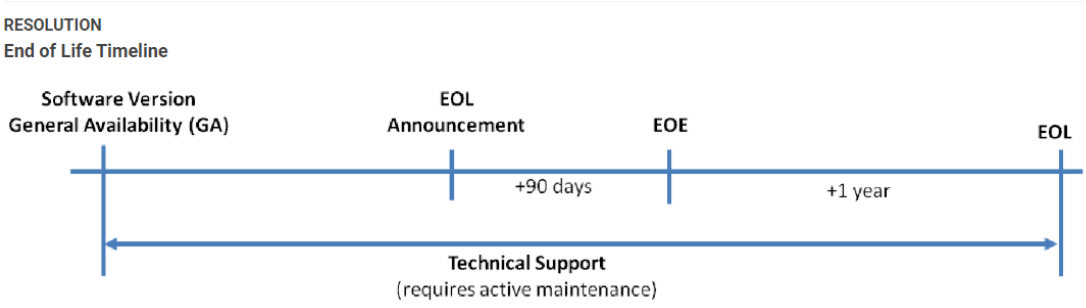
Viimeisin Cisco Prime Infrastucturen End-of-Life ilmoitus on suunnattu Hardware Gen2 Appliancelle sekä Prime Infrastructure versioille 3.1/3.2. Näiden versioiden myynti on lopetettu marraskuussa 2019 ja järjestelmäkehittäjän tuki lopetetaan kesäkuussa 2022. (End-of-Sale and End-of-Life Announcement for the Cisco Prime Infrastructure HW Gen2 Appliance and 3.1 and 3.2 Software, 2019). Uusin versio 3.8 on julkaistu 25.09.2019, eikä tälle ole ilmoitettuna vielä End-of-Sales/End-of-Life päivämäärää.

Aikaisempiin Prime Infran versioihin peilaten voidaan tehdä johtopäätös, että tuki kyseiselle uusimmalle versiolla 3.8 on vielä voimassa järjestelmäkehittäjältä ainakin 5 vuodeksi eteenpäin. Tässä tulee myös huomioida, että Cisco antaa käyttäjiensä päivittää Prime Infra versionsa uusimpaan niiden julkaisuiden myötä ilman lisäkustannuksia. (Cisco Prime Infrastructure versions, 2019)

SolarWinds

Solarwindin toimiessa vahvana kilpailijana verkonhallintajärjestelmien parissa, on siltä odotettavissa tuki valmistamilleen sovelluksilleen vuosiksi eteenpäin. Heidän toimiessaan alalla jo vuodesta 1999, voidaan tehdä johtopäätös, että yhtiö on vakaa, ja mahdollistaa tuen asiakkaillensa pidemmäksikin aikaa. SolarWinds julkaisee tasaisen aikavälein uusia sovellusversioita tarjoamilleen tuotteilleen ja näiden elinkaari ilmoitetaan heidän sivustollaan. (SolarWinds Currently Supported Software Versions, 2019)

Tutkimustyössä tarkastelujen SolarWindsin työkalujen End-of-Life päivämääriä ei ole julkaistu, mutta niiden astetta aikaisempien versioiden päivämäärät ovat julkisia tietoja. SolarWindsilla on standardisoitu tapa määritellä sovellusversioidensa elinkaari sekä kuinka heidän tulee informoida käyttäjiään sovellusversioiden elinkaaren päättymisestä. Tästä SolarWindsin tarjoama informoiva kuvio, kuviossa 2.



Kuvio 2. Solarwindsin ohjelmistojen elinkaari. (SolarWinds, End of Life Policy, 2018)

ManageEngine OpManager

Zoho corporationin omistaman OpManagerin nykyinen sovellusversio 12.3 on julkaistu elokuussa 2017. Sille ei toistaiseksi ole huhtikuussa 2020 ilmoitettuna End-of-Life kaaren päättymistä (Product Life Cycle Plan)

What's Up Gold

IpSwitch takaa tuotteillensa vähintään 2,5 vuoden mittaisen elinkaaren teknisen tuen kanssa. Viimeisin versio What's Up Goldille on julkaistu 15.10.2019, joten tuki uusimmalle versiolle on vielä taattu. Ensimmäinen versio on julkaistu nimikkeellä WhatsUp vuonna 1998, ja uusi versio on julkaistu markkinoille noin vuoden välein. Näiden tietojen perusteella voidaan tehdä johtopäätös, että What's Up Goldin tukea ei heti olla lopettamassa. (What's up Gold Documentation, 2019). Uusia ominaisuuksia ollaan lisäämässä Road-mappiin mukaan ja lisää ominaisuuksia lisätään asiakkaiden toiveiden mukaisesti.

NetBrain

Suhteellisen nuorena yrityksenä, perustettu 2004, on NetBrainilla vielä oman paikkansa hakeminen markkinoilla. Suurien kilpailijoiden seassa oleva yritys kilpailee omasta markkinaosuudestaan, ja on saanutkin hyvin jalansijaa useiden isojen asiakkaiden myötä. End-Of-Life ilmoituksia ei NetBrainin sivustoilla ole dokumentoitu. Uusin versio 8.01 Netbrainista on julkaistu 11.08.2019, joten voidaan tehdä olettamus, että tukea järjestelmälle vielä vuosiksi.

4 Hallintajärjestelmien testaaminen

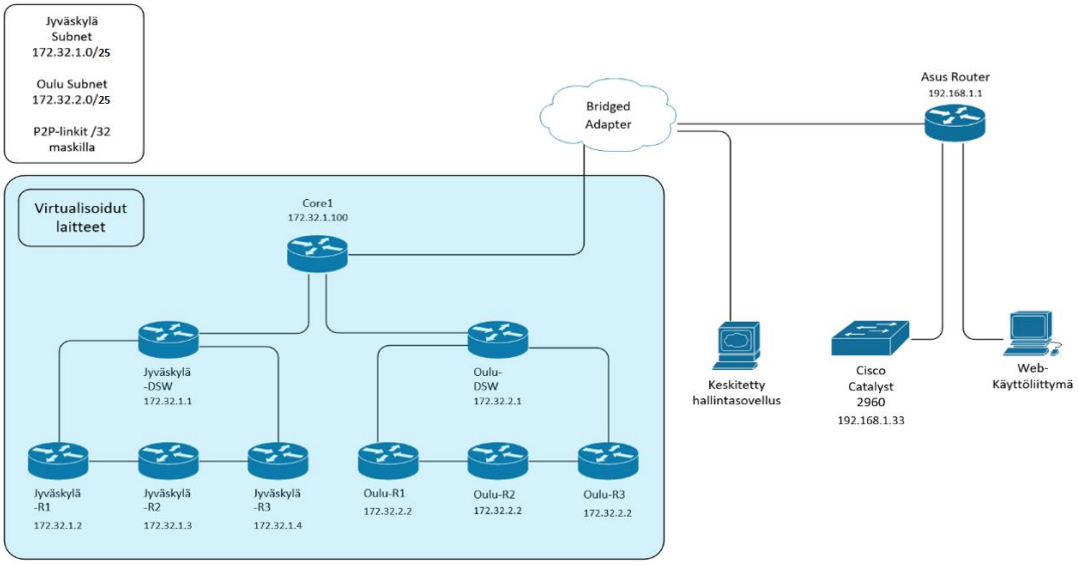
4.1 Yleistä

Hallintajärjestelmien käytännön testaamista varten on luotuna virtuaalinen ympäristö. Virtuaalinen ympäristö on pääpainotteisesti aktiivisena yhdellä palvelimella, jolla on käytössä Windows 10 käyttöjärjestelmä. Eri valmistajien tarjoamat ratkaisut

kuitenkaan eivät natiivisti välttämättä ole luotuna pelkästään Microsoftin tarjoamalle alustalle ja näitä varten käytetään VMwaren Workstation Pro 15:sta.

Virtuaaliset laitteistot kattavat melkein oikean hardwaren toiminnallisuudet, mutta osittaisia puutteita virtuaalisista reitittimistä löytyy. Tärkeimmät ominaisuudet hallintajärjestelmien toimintaa varten olevat protokollat kuten SSH, TELNET, ja SNMP ovat kuitenkin tuettuja. Tukea virtuaalisille lähiverkoille (VLAN) ei ole näillä virtuaalilaitteilla, koska OSI-mallin tasoa 2 ei ole ohjelmoitu ympäristön virtuaalisille reitittimille.

Testiympäristön topologia on OSI-mallin L2-tasoltaan kuvion 2 mukainen. Ympäristössä olevat virtuaaliset reitittimet ovat VMwarella virtualisoituja Ciscon Catalyst 7200 imagen omaavia reitittimiä. Virtuaaliset reitittimet yhdistetään GNS3-ohjelmalla keskenään sekä Bridged Adapterin kautta virtuaaliympäristöstä Web-käyttöliittymälle. Huomioitavaa virtuaalisissa reitittimissä on, etteivät ne tue kaikkia ominaisuuksia mitä todellinen reititin voi tukea.



Kuvio 3. Testiympäristön verkkotopologia

Ympäristöön on rakennettuna kuvitteelliset Jyväskylä ja Oulu toimialueet demonstroimaan erillisiä järjestelmäkokonaisuuksia. Nämä kaupunkikohtaiset järjestelmät

liikennöivät Core-reitittimen kautta Bridged adapterille. Päätelaitteita ei ole virtualisoituna, kun niiden tutkiminen tai seuranta keskitetyllä verkonhallintajärjestelmällä ei ole painotettuna. Testiympäristössä on myös yksittäinen fyysinen Cisco Catalyst 2960 kytkin, jota käytetään hyödyksi automatisoitujen sovelluspäivitysten testaamisessa. Virtuaalisten reitittimien ohjelmistoversioita ei voida päivittää.

Testattaviksi verkonhallintajärjestelmiksi päätyi lopullisesti 4 tuotetta. NetBrainilta ei saatu selvitystyön aikataulun puitteisiin järjestelmää testattavaksi, vaikkakin tämän testaaminen olisi tuonut hyvän lisäyksen muiden testattujen tuotteiden ohella. ManageEngine OpManagerin testattava evaluaatio versio oli erittäin riisuttu malli, ja siitä uupui täysin vaatimusmäärittelyihin listattu konfiguraatiomuutosten tekeminen. OpManagerin testaaminen näin ollen jäi pintapuoliseksi.

4.2 Cisco Prime Infrastructure 3.7

Laboraatioympäristöön testattavaksi versioksi valikoitui 60 päivän kokeilujaksolla oleva Express edition 3.7 versio Prime Infrastructuresta. Express edition on Prime Infrastructuresta kevyin versio ajaa virtualisoidusti, ja näin ollen valikoitui testattavaksi. Asennus on erittäin suoraviivainen työvaihe, kun OVA-tiedosto tuodaan VMwaren käynnistettäväksi. Express edition ei tosin omaa vaatimuksissa mainittua Compliance toimintoa, joten sen testaaminen on jäänyt pois.

Käyttäjäoikeuksien ryhmittely

Käyttäjien ryhmittelyssä voidaan määritellä tarkastikin minkä tasoiset oikeudet eri käyttäjille tai ryhmille annetaan. Oikeuksissa voidaan sallia osalle käyttäjistä mahdollisuus muutosten tekoon, ja osalle sallitaan pelkän monitoroinnin näkymä.

Tietoliikenneverkon kartoitus

Seurattavien noodien kartoitusta varten voidaan käyttää useampiakin protokollia hyödyksi. Prime kykenee löytämään halutut noodit seuraavien protokollien avulla:

- PingSweep Module (Ciscon oma ICMP-pakettien lähettäjä)
- Cisco Discovery Protocol (Ciscon oma naapurilaitteiden kartoittaja)
- Link Layer Discovery
- Routing Table
- Address Resolution Protocol
- Border Gateway Protocol
- Open Shortest Path First

Testiympäristön kartoitus toteutui suoraviivaisesi, kun käytettiin eksakteja IP-osoitteita laitteille, eikä aikaa kulunut minuutteja enempää tehtävän suorittamisessa. IP-alue tai aliverkko skannaukset jättivät kuitenkin useiden kartoittamistehtävien ajojen aikana löytämättä halutut tietoliikennelaitteet, eikä niitä voinut kokea luotettaviksi.

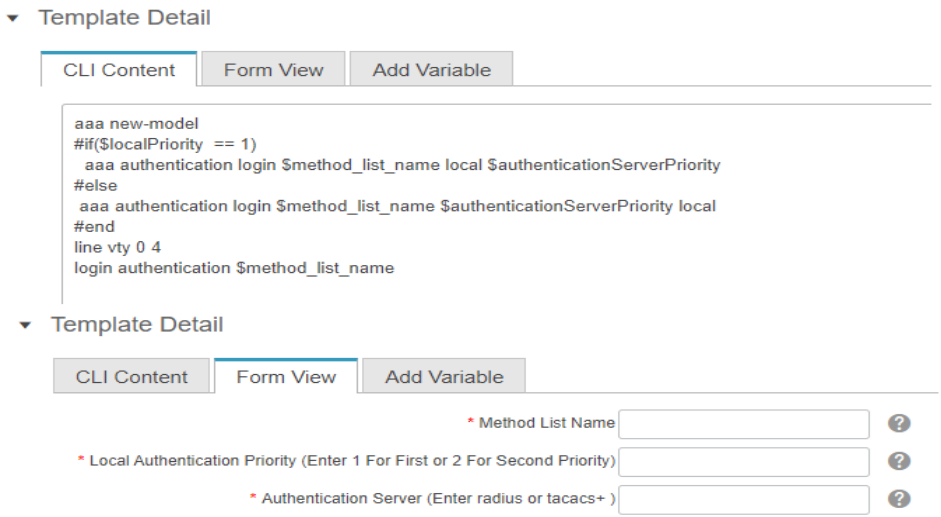
Testiympäristön kartoituksen lisäksi toteutettiin asiakasympäristön 100 tietoliikennekytkimen kartoitus Cisco Prime Infrastructurella. Aikaa vievin osuus kartoitustehtävän luomiseksi on listata halutut laitteet ja tähän kului aikaa 2,5 tuntia. PingSweep-moduulille voidaan hyödyntää CSV-tiedostoa, mutta kirjautumistunnusten käyttöä varten tulee lisätä samat laitteet uudelleen manuaalisesti Credentials-listalle.

Konfiguraatiomuutosten teko

Konfiguraatiomuutosten teko onnistuu Prime Infralla valmiin CLI-kirjaston avulla nopeasti. Tosin kaikkia haluttuja muutostehtäviä ei ole siellä valmiina, ja tulee luoda omia. Oman tehtävän luominen onnistuu helpoiten kopioimalla jo valmis työ, ja tekemällä siihen tarvittavat muutokset.

Uuden konfiguraatiopohjan myötä, kun muutostyö halutaan tehdä, ei tarvitse sen muutostyön suorittavan henkilön tietää komentorivisyntaksista, ja hän vain lisää tarvittavat arvot muuttujien kohdalle tehtävälomakkeeseen. Valmiit Primen konfiguraa-

tiopohjan-tehtävät ovat todella lyhyitä yhden ominaisuuden mahdollistavia komentoja. Kuviosta 4 nähdään, kuinka konfiguraatiopohja luodaan ja miten IF-ELSE lausekkeita sekä muuttujia käytetään komentorivi tulosteen seassa.



Kuvio 4. Cisco Prime Infrastructurella muutospohja lomakkeen rakentaminen

konfiguraatiopohjan ajaminen ei onnistu kolmannen osapuolen laitekannalle. Prime ei näytä käyttöliittymässään valittavien laitteiden listasta kolmannen osapuolen laitteitta, vaikka tehtävä konfiguraatiopohjan olisikin tehty esimerkiksi HP:n tai Juniperin CLI-syntaksia noudattaen.

Ohjelmistoversioiden päivityksen toteutus

Ohjelmistoversioiden päivitykset onnistuvat sille luodun välilehden kautta Cisco Prime Infrastructuren käyttöliittymässä. Päivitystehtävä on jaettuna kolmeen välivaiheeseen. Ensin ladataan sovelluspalvelimelle haluttu image. Sovelluspalvelimelle voidaan määrittää käyttääkö se FTP/TFTP/SFTP/SCP protokollia. Toisessa välivaiheessa jaetaan ladattu image sovelluspalvelimen valikoimasta päivitettäville laitteille. Samalla toisessa välivaiheessa voidaan valita, poistetaanko ajossa olevat sovellusversiot laitteilta sekä tuleeko päivityksen yhteydessä uudelleen käynnistää laitteet. Päivitys-

työlle voidaan myös määrittää lopettaako se tehtävänsä tekemisen, jos päivitys epäonnistuu jollakin päivitettävistä laitteista. Kolmannessa välivaiheessa aktivoidaan jaetut sovellusversiot aikaisemmassa välivaiheessa määritellyiltä laitteilta.

Kolmannen osapuolen laitteille ei sovelluspäivityksiä saada lähetettyä, koska Prime Infra ei käyttöliittymässään esitä valittavaksi eri valmistajien laitteita.

Testiskenaariossa, jossa ohjelmistoversioiden päivitykset ajettiin asiakasverkon viidellekymmenelle tietoliikennekytkimelle, huomattiin useita ongelmia. Cisco Prime Infrastructure ei voinut toimia FTP/TFPT/SFTP/SCP-palvelimena asiakasverkon arkkitehtuurillisista syistä, ja tuli käyttää erillistä palvelinta ohjelmistotiedostojen siirtoa varten. Tämän vuoksi Ciscon tarjoama työkalu päivitystehtävää varten jäi täysin käyttämättömäksi, ja tehtävä tuli luoda erillisillä muutospohjilla. Lataustehtävä tuli luoda interaktiivisena muutospohjana, joka on nähtävissä taulukossa 10. Muutospohjassa määritetään *#MODE_ENABLE*:lla ajamaan komento *exec*-modessa, koska oletuksena muutospohjat menevät Cisco Prime Infrastucturessa *configuration terminal*-moodiin. *#INTERACTIVE* komennon tehtävä taulukon 10 rivillä 2 on vastata tietoliikennekytkimen kysymyksiin esiasetetuilla vastauksilla. Taulukko 10 muutospohjan tapauksessa määritetään tallentamaan tiedoston nimi sellaisenaan kuin se on FTP-palvelimella. SW-image latausta varten tulee luoda myös ladatun imagen MD5-hashin tarkistusta varten erillinen muutospohjat, sekä erillinen muutospohja myös SW-imagen aktivointia varten.

Taulukko 10. Cisco primen usean laitteen yhtäaikainen SW-imagen copy-muutospohja.

#MODE_ENABLE *#INTERACTIVE* *Copy tftp://192.168.10.10/Jakelu/newest-bestest-image.bin flash: <IQ>Destination filename[newest-bestest-image.bin]?<R>newest-bestest-image.bin* *#ENDS_INTERACTIVE* *#MODE_END_ENABLE*

4.3 Solarwinds Orion

Käyttäjäoikeuksien ryhmittely

SolarWindsillä kyetään jakamaan käyttäjien välillä järjestelmän käyttöä varten eri tasoisia oikeuksia. Näiden oikeuksien perusteella joku käyttäjä voi tehdä muutostyön odottamaan järjestelmävalvojan hyväksyntää ennen sen toteuttamista tuotantoympäristöön.

Tietoliikenneverkon kartoitus

Kartoitus SolarWindsillä tapahtuu Network Topology Mapper-työkalun avulla. Verkkojen kartoitusta varten tulee määrittää IP-alue, IP-aliverkko tai yksittäiset IP-osoitteet. IP-määrittelyiden jälkeen määritellään käytettävät SSH ja SNMPv2/v3 tunnukset. Nämä tiedot syöttämällä SolarWinds hakee laitteet järjestelmänsä seurantaan ja esittää ne tietokannassaan.

SolarWindsin aliverkon skannaus ei löydä kuin murto-osan verkossa olevista laitteista, joka todettiin käyttöönoton suhteen huolestuttavaksi. Toinen skannaus toteutettiin 100 kytkiminen asiakasympäristössä ja tulos oli vastaava. Manuaalinen listaaminen seuraavaa skannausta varten vaati aikaa 1 tunnin verran.

Konfiguraatiomuutosten teko

Konfiguraatiotöitä varten SolarWindsillä on tarjolla muutamia valmiita komentopohjia Ciscon, Lenovon sekä Juniperin eri laitemalleille. Pääpaino kuitenkin on Ciscon valmistamien laitteiden päivittämisessä. Thwack-community:stä voidaan hakea muiden SolarWindsin käyttäjien lisäämiä pohjia, jotka sopivat eri valmistajien komentorivikehotteisiin.

Testissä luotiin ACL-sääntö, joka sidottiin VTY-rajapintoihin. Tehtävä määriteltiin kysymään ennen sen suorittamista mikä tule ACL-listan nimeksi. Taulukossa 11 nähtävissä kuinka SolarWindsille luodaan tehtävä-scriptit.

Taulukko 11. SolarWindsillä luotu ACL-säännön lisäystehtävä

/* <- Parametrien määrittelykenttä alkaa
.CHANGE_TEMPLATE_DESCRIPTION
Luodaan uusi ACL ja liitetään se vty rajapintoihin
.CHANGE_TEMPLATE_TAGS
Cisco
.PLATFORM_DESCRIPTION
Cisco IOS
.PARAMETER_LABEL @ContextNode
NCM Node
.PARAMETER_DESCRIPTION @ContextNode
The node the template will operate on. All templates require this by default. The target node is selected during the first part of the wizard so it will not be available for selection when defining values of variables.
 	
.PARAMETER_LABEL @aclextendedname
Uuden ACL-listan nimi:
.PARAMETER_DESCRIPTION @aclextendedname
ACL-nimike
Parametrien määrittelykenttä loppuu ->
*/
 	
Jatkuu viereisessä solussa ->
	script AddACLMountVTYCiscoIOS (
	NCM.Nodes @ContextNode,
	string @aclextendedname)
	{
	CLI
	{
	Configure terminal
	!
	ip access-list extended @aclextendedname
	!
	remark LOCAL
	permit ip 192.168.1.0 0.0.0.255 any
	remark VPN-clients
	permit ip 172.16.1.0 0.0.1.255 any
	!
	remark Zabbix-server
	permit ip host 172.61.61.1 any
	!
	remark Keskitetty-verkonhallintajarjestelma
	permit ip host 192.168.1.94 any
	!
	remark Log-denied-packets
	deny ip any any log
	!
	line vty 0 15
	access-class @aclextendedname in
	!
	end
	write memory
	y
	!
	}
	}

Sovelluspäivitykset

Sovellusversioiden päivitykset SolarWindsin firmware-upgrade osion kautta on suunnattu vain Cisco laitemallien suuntaan. Solarwindsin image-repositorioon voidaan siirtää useitakin ohjelmistotiedosto, mutta se osaa tunnistaa niistä ainoastaan .bin päätteiset Ciscon ohjelmistoversiot. Luomalla erillisen komentorivitehtävän, joka käskee laitteita hakemaan tietyltä palvelimelta juuri tietyn niminen image, voitaisiin toteuttaa SolarWindsilla muidenkin laitevalmistajien sovellusversiopäivityksiä hallintajärjestelmällä. Tuloste tarkistetaan jokaiselta päivitettävältä laitteelta erikseen ja vah-

vistetaan sen oikeellisuus ennen komentojen ajamista tietoliikennelaitteille. SolarWinds lähettää Firmware Repositoriostaan lasketun MD5-hash summan varmistettavaksi ennen imagen siirtämistä. Taulukosta 12 nähdään, minkälainen tarkistus tulee päivitystehtävän luojan tehdä jokaisen laitteen kohdalta, jolle on määritetty ohjelmistoversionpäivitys.

Taulukko 12. SolarWindsin firmware/software päivityksen komentotarkistus

write memory *copy flash:c2960-lanbasek9-mz.122-55.SE11.bin tftp://192.168.1.94* *verify /md5 flash:c2960-lanbasek9-mz.122-55.SE11.bin ${BackupImageHash}* *${SuccessRegEx:Verified}* *delete flash:c2960-lanbasek9-mz.122-55.SE11.bin* *copy tftp://192.168.1.94/c2960-lanbasek9-mz.122-55.SE12.bin flash:* *dir flash: ${SuccessRegEx:c2960-lanbasek9-mz.122-55.SE12.bin}* *verify /md5 flash:c2960-lanbasek9-mz.122-55.SE12.bin* *1504e5d9342eabf6f7b2376e94ace46f ${SuccessRegEx:Verified}* *config terminal* *no boot system* *boot system flash:c2960-lanbasek9-mz.122-55.SE12.bin* *end* *write memory* *show boot ${SuccessRegEx:c2960-lanbasek9-mz.122-55.SE12.bin}* *reload* *y* *y*

Testiympäristön lisäksi SolarWindsillä toteutettiin asiakasympäristön viidellekymmenelle tietoliikennekytkimelle ohjelmistoversion päivitykset. Asiakasverkon arkkitehtuurillisten rajausten vuoksi SolarWinds järjestelmä ei voinut toimia FTP/TFTP/SFTP/SCP-palvelimena, ja tämän vuoksi ei SolarWinds voinut luoda taulukon 10 mukaista tarkistuslistaa. Tehtävän toteuttamista varten tulee ohittaa valmiin työnkalun käyttäminen, ja luoda manuaalisesti useampia muutospohjia erillisten välivaiheiden suorittamista varten. Haasteena myös toimi ”puu”-rakenteinen verkko, jonka vuoksi laitteiden uudelleenkäynnistämiset tuli suorittaa aloittaen viimeisestä

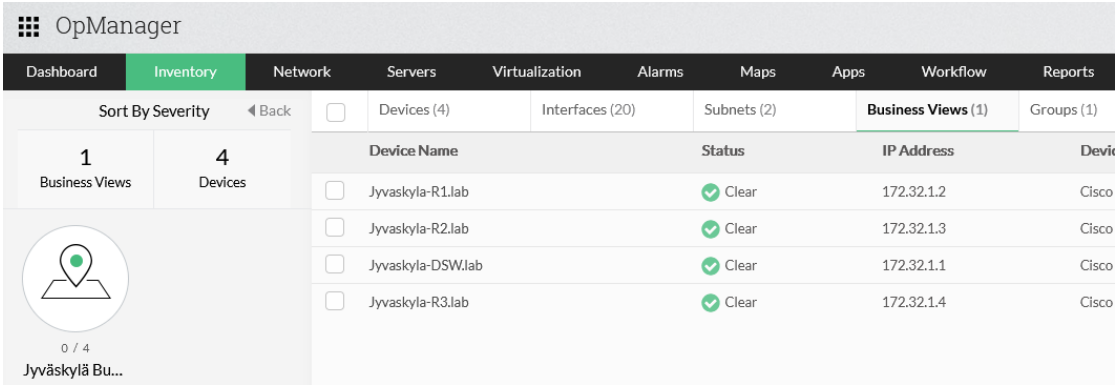
kytkimestä (Leaf). Nämä saatiin toteuttaa ryhmittämällä viimeiset kytkimet omiin ryhmiin

4.4 ManageEngine OpsManager

Testiympäristössä käytetty ManageEngine OpManager Professional edition ei kyennyt konfiguraatiomuutoksiin, tai tietoliikennelaitteiden sovelluspäivityksiin. Muutostöitä varten ManageEngine OpManagerilla on NCM lisätyökalu, joka ei ole evaluaatio versiossa mukana. Tätä hallintajärjestelmää ei täten kyetty testaamaan muussa kuin kartoitustoiminteissa ja laitekantojen ryhmittelyissä. Tuki kuitenkin konfiguraatiomuutoksille, compliance audit:ille sekä firmware/software päivitykselle hallintajärjestelmällä tuotevalmistajan mukaan on. (OpManager NCM, n.d.)

Käyttäjäoikeuksien ryhmittely

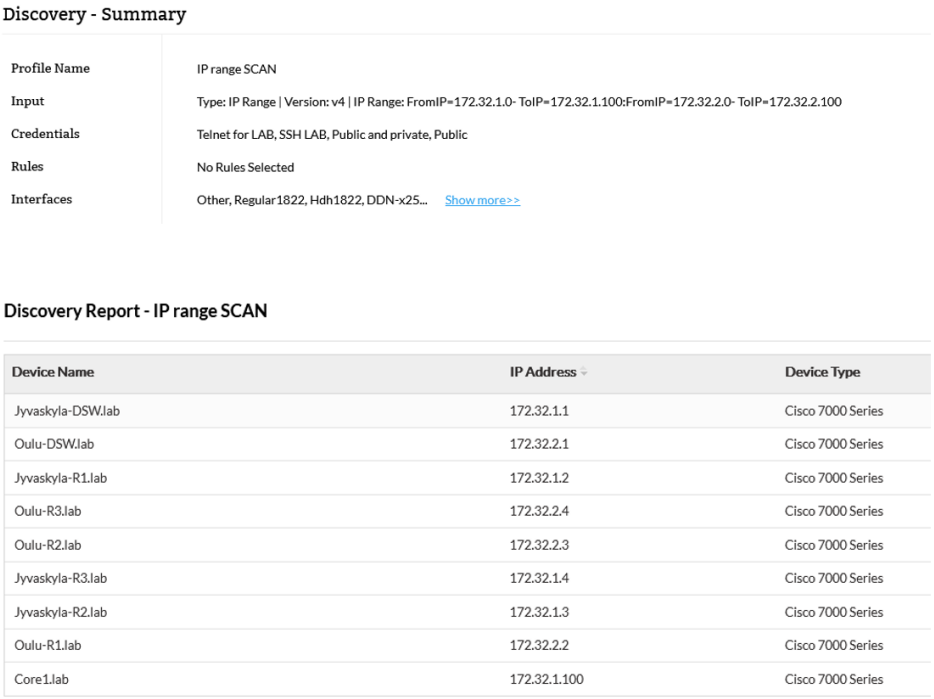
Käyttäjäoikeuksien ryhmittelyssä voidaan rajoittaa ManageEnginellä käyttäjien näkymää halutuille laitteille. Laitteet tulee kategorisoida ”Business View” näkymään omiin ryhmiin, ja käyttäjille erikseen määrittää pääsy näihin ryhmiin. Käyttäjien oikeudet rajoittuvat myös niiden roolien perusteella ja yleisin on ”Operator”-rooli, jolla voidaan vain tarkastella laitteiden tilaa. Kuviossa 5 on rajoitettu näkymä käyttäjälle vain Jyväskylä-alueen tietoliikennelaitteille.



Kuvio 5. ManageEnginellä operaattorikäyttäjän rajoitettu näkymä

Tietoliikenneverkon kartoitus

Tietoliikenteen kartoituksesta ManageEngine selviytyy muihin järjestelmiin verrattuna paremmin, sen löytäessä aliverkon sekä IP-alueen skannauksella kaikki testiverkon laitteet. Visuaalisen kartan piirtäminen ei onnistunut virtuaalisen testiverkon rajoitteen vuoksi. Kuviossa 6 voidaan tarkastella ennen skannauksen aloittamista järjestelmän tulostama tiivistelmä suoritettavasta skannauksesta. Skannauksessa on määritetty 2 aluetta 172.32.1.0 – 100 sekä 172.32.2.0 -100 alueilta. Kuviossa 6 myös voidaan nähdä raportti skannauksen tuloksesta, ja kaikki testiverkon laitteet löydettynä.



Discovery - Summary

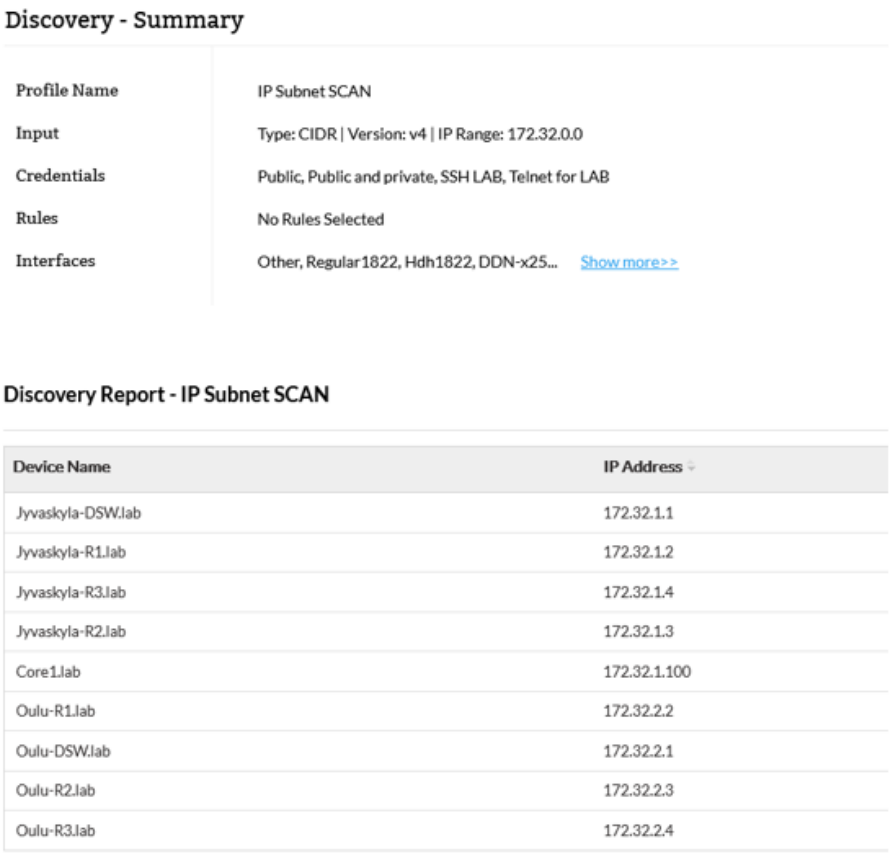
Profile Name	IP range SCAN
Input	Type: IP Range | Version: v4 | IP Range: FromIP=172.32.1.0- ToIP=172.32.1.100:FromIP=172.32.2.0- ToIP=172.32.2.100
Credentials	Telnet for LAB, SSH LAB, Public and private, Public
Rules	No Rules Selected
Interfaces	Other, Regular1822, Hdh1822, DDN-x25... Show more>>

Discovery Report - IP range SCAN

Device Name	IP Address	Device Type
Jyvaskyla-DSW.lab	172.32.1.1	Cisco 7000 Series
Oulu-DSW.lab	172.32.2.1	Cisco 7000 Series
Jyvaskyla-R1.lab	172.32.1.2	Cisco 7000 Series
Oulu-R3.lab	172.32.2.4	Cisco 7000 Series
Oulu-R2.lab	172.32.2.3	Cisco 7000 Series
Jyvaskyla-R3.lab	172.32.1.4	Cisco 7000 Series
Jyvaskyla-R2.lab	172.32.1.3	Cisco 7000 Series
Oulu-R1.lab	172.32.2.2	Cisco 7000 Series
Core1.lab	172.32.1.100	Cisco 7000 Series

Kuvio 6. ManageEngine OpManagerilla suoritettu IP-alueen skannaus

Aliverkon skannauksessa käytettiin aluetta 172.32.0.0 /22 (255.255.252.0), joka kattaa IP-alueen 172.32.0.0 – 172.32.3.254. Kuviosta 7 voidaankin todeta ennen skannauksen aloittamista järjestelmän tuottama tiivistelmä suoritettavasta skannauksesta sekä skannauksen jälkeisistä tuloksista. Tuloksissa nähdään, että ManageEnginen aliverkon skannaus toimii halutulla tavalla.



Discovery - Summary

Profile Name	IP Subnet SCAN
Input	Type: CIDR | Version: v4 | IP Range: 172.32.0.0
Credentials	Public, Public and private, SSH LAB, Telnet for LAB
Rules	No Rules Selected
Interfaces	Other, Regular1822, Hdh1822, DDN-x25... Show more>>

Discovery Report - IP Subnet SCAN

Device Name	IP Address
Jyvaskyla-DSW.lab	172.32.1.1
Jyvaskyla-R1.lab	172.32.1.2
Jyvaskyla-R3.lab	172.32.1.4
Jyvaskyla-R2.lab	172.32.1.3
Core1.lab	172.32.1.100
Oulu-R1.lab	172.32.2.2
Oulu-DSW.lab	172.32.2.1
Oulu-R2.lab	172.32.2.3
Oulu-R3.lab	172.32.2.4

Kuvio 7. ManageEngine OpManagerilla suoritettu IP-aliverkon skannaus verkolle 172.32.0.0/22

4.5 What’s Up Gold

Käyttäjäoikeuksien ryhmittely

Käyttäjien ja käyttäjäryhmien oikeuksien jakaminen eri tehtävien perusteella on suoraviivaista. Ryhmälle voidaan määritellä oikeus pelkkään monitorointiin, tai sallia näille jopa itse hallintajärjestelmän järjestelmänvalvojan oikeuksia.

Tietoliikenneverkon kartoitus

What’s Up Goldin virtuaalisessa testiympäristössä toteutetun tietoliikenneverkon kartoittaminen ei toisinaan tuottanut odotettuja tuloksia. Vaikkakin testiympäristön laitteilla oli identtiset SNMP/telnet/SSH kredentiaalit, ja eroavaisuutena Loopback-rajapinnan osoite, ei välttämättä What’s Up Gold siltikään löytänyt määriteltyjä lait-

teita aliverkko tai IP-alueet määrittämällä. Ajamalla Discovery-tehtävä useaan otteeseen tai määrittämällä eksaktit hallinta IP-osoitteet, löysi järjestelmä kuitenkin määritellyt laitteet.

Konfiguraatiomuutosten teko

Yksinkertaisen konfiguraatio muutosten tekeminen muutospohjien avulla vaatii kokonaisten komentorivien lisäämisen ajettavaan tehtävään. Käyttäjän kirjoittamassa tehtävässä voidaan käyttää What's Up Goldin Custom Script Language Guide:n opastetta (Using the WhatsConfigured Custom Script Language, 2012.) hyödyksi, jossa opastetaan erinäisten valmiiden muuttujien, funktioiden sekä käyttäjän itse luotujen muuttujien hyödyntämistä konfiguraatio-scriptissä. Esimerkiksi, jos halutaan usealta Ciscon laitteelta running-config tiedosto ladattua, luo järjestelmä SSH/Telnet yhteydellä taulukon 13 mukaisen komennon.

@login funktio ajaa tarpeelliset komennot CLI-yhteyden luomiseksi, jonka jälkeen What's Up Gold tallentaa output-komennot tietokantaansa. Jokaiselle käskylle tulee asettaa [funktio]-funktio. Ilman funktiota ei järjestelmä osaa syöttää komentoja oikealla tavalla laitteen komentoriville

Taulukko 13. What's Up Goldin esimerkki muutospohjasta

@login *[-] @enable* *[-] copy tftp:/* *[-] snmp-server community NOTpublic ro* *end* *writ mem* *@logout*

Komentoriviyhteydessä ollessaan hallintajärjestelmä lukee laitteen antamia output-viestejä, jotka tulkitaan määriteltyjen sanojen mukaisesti. Eri laitevalmistajilla sekä -malleilla on eri komentorivisyntaksit ja tässä tulee listata kaikki mahdolliset vastausvaihtoehdot.

Sovelluspäivitykset

Sovelluspäivityksen What's Up Goldilla tulee ajaa itsekirjoitetun komentorivi scriptin mukaan. Ciscon laitekannalle tulee siis määritellä taulukko 14 mukainen script-pohja. Taulukossa 14 parametri *@login* suorittaa laitteelle kirjautumisen, jossa käytetään esimääriteltyjä kredentiaaleja tietokannasta. *@enable* komento rivillä 2 taulukossa 14 määrittää seuraavat komennot ajettavaksi Cisco-syntaksissa enable-moodissa, eikä configure-moodissa. Loput taulukon 14 riveistä määrittää laitteen lataamaan uuden SW-imagen, asettamaan sen aktiiviseksi ja tallentamalla tehdyt muutokset järjestelmän konfiguraatiotiedostoon. Tämän askeleen jälkeen tulee vielä erikseen ajaa uudelleenkäynnistys tehtävä jokaiselle laitteelle.

Taulukko 14. Cisco kytkimen ohjelmistoversion päivittäminen What's Up Goldin scriptillä.

@login
[-] @enable
[-] copy tftp://192.168.1.100/testi.bin
[-] configure terminal
[-] boot system flash:/testi.bin
y
y
end
write memory
y
y
@logout

4.6 Testattujen järjestelmien vertailu

Järjestelmillä toteutettiin testiympäristössä tehtäviä, jotka kuuluivat luvussa 2.2 määriteltyihin vaatimuksiin, ja näiden suorittaminen kuului osana järjestelmien testaukseen. Testauksissa toteutettiin yksinkertaisten tehtävien tekeminen testiympäristön virtuaalisille tietoliikennereitittimille ja näiden tehtävien onnistumiset/epäonnistumiset taulukoitiin taulukkoon 15.

Käyttäjälle näkyvänä ja tuntuvana eroavaisuutena järjestelmien kesken oli muutospohjien luonti. Cisco Primellä muutospohjien luonnit tulee palastella erittäin pieniksi

kokonaisuuksiksi, joka on ymmärrettävää tehtävää ajaessa. Cisco Primen Form-pohjainen muutospohjan luonti helpottaa paljon L1-tason vianselvityksessä/-korjauksessa, eikä tekijällä tarvitse olla ymmärrystä komentorivisyntaksista. Solarwindsin muutospohjan luonti hipoo python-ohjelmointia, ja muutospohjan voi pienellä vaivalla saada kattamaan montakin tehtävää kerralla.

What's up Goldin muutospohjien tekeminen voi olla haasteellista alkuun, koska järjestelmä ei anna valmiita esimerkkipohjia käytettäväksi, ja järjestelmän tuottajan dokumentaatio järjestelmän kustomoidusta script-pohjasta ei toiminut tukea antavana tietona.

Taulukko 15. Järjestelmien testaustaulukko

Testattava tehtävä	Cisco Prime Infrastructure 3.7	SolarWinds	ManageEngine OpsManager	What's Up Gold
Käyttäjäoikeuksien ryhmittely	✓	✓	✓	✓
Tietoliikenneverkon kartoitus	✓	✓	✓	✓
Laitekantojen ryhmittely	✓	✓	✓	✓
Konfiguraatiomuutosten teko (Cisco)	✓	✓	✗ (Add-on puuttui testeistä)	✓
Konfiguraatiomuutosten teko (Non-Cisco)	✗ Ei pysty luomaan CLI-yhteyttä kolmannen osapuolen laitteisiin.	✓	✗ (Add-on puuttui testeistä)	✓
Sovelluspäivitykset (Cisco)	✓	✓	✗ (Add-on puuttui testeistä)	✓/✗ Ei sovelluksen avulla. Mahdollisuus kirjoittaa CLI-script, joka tekee päivityksen.
Sovelluspäivitykset (Non-Cisco)	✗ Ei pysty luomaan CLI-yhteyttä kolmannen osapuolen laitteisiin.	✓/✗ Ei sovelluksen avulla. Mahdollisuus kirjoittaa CLI-script, joka tekee päivityksen.	✗ (Add-on puuttui testeistä)	✓/✗ Ei sovelluksen avulla. Mahdollisuus kirjoittaa CLI-script, joka tekee päivityksen.

5 Tulokset ja pohdinta

Tutkiessa tehtyjen havaintojen perusteella voidaan saada hyvä tämänhetkinen tilanne keskitetyistä verkonhallintajärjestelmistä. Useat näistä sovelluksista kykenevät tekemään suuriakin työmääriä lyhyessä aikavälissä, näin ollen säästäen rutkasti aikaa muutostöihin kuuluvissa tehtävissä. Näiden työtehtävien (ohjelmistopäivitykset, konfiguraatiomuutokset, compliance audit, jne.) suorittamista varten vaaditaan kuitenkin paljon itse räätälöityjä muutospohjia. Järjestelmien alkukäyttöönoton ja tarvittavien tehtävien luonnin jälkeen käyttö on suoraviivaista sekä nopeaa. Tutkitut verkonhallintajärjestelmät kykenevät pitkälle täyttämään vaatimusmääreissä olevat tehtävät.

Konfiguraatiomuutokset ja sovelluspäivitykset hallintajärjestelmillä

Yleinen huomio on siinä, että kaikki tässä selvitystyössä tutkituista verkonhallintajärjestelmistä tukevat Ciscon laitteita sekä Ciscon komentorivi syntaksia oletuksena. Kuitenkin muiden valmistajien tuottamiin laitteisiin on huomattavasti vajavaisempi tuki verkonhallintajärjestelmillä, ja näitä varten tulee tehdä itseluotuja ”käsikirjoja” hallintajärjestelmän ajettavaksi. Cisco Prime Infrastucture on pitkälti vain Ciscon omien tuotteiden konfigurointia varten. Useat eri ominaisuudet jäävät pois käytöstä kolmannen osapuolen tietoliikennelaitteiden osalta ja jäljelle jää pelkkä SNMP/ICMP-monitorointi. Erittäin suuri osa Primen ominaisuuksista on suunnattu tukiasemien ja langattomien verkkojen seurantaan, eli sen alkuperäinen käyttötarkoitus on campusverkkojen hallintaa varten.

SolarWindsin järjestelmällä saadaan tehtyä usean eri valmistajan laitteille konfiguraatiomuutokset komentorivipohjaisesti. Vaikkei suoraa valmista muutospohjaa olisikaan, sen voi helposti itse räätälöidä, kunhan tietää miten komennot rakentuvat CLI-rajapinnassa sekä on tiedossa laitekannan CLI-rajapintojen out-put promptit. SolarWindsilla mahdollisesti joku muu kommuunin käyttäjä on voinut tehdä jo tarvittavat skript-muutospohjat, ja ne voi ladata Thwack-yhteisöstä.

What’s Up Gold tarjoaa valmiina script-pohjana pelkästään Ciscon laitteille suunnatun copy running-/startup-config scriptin, joka sisältää kirjautumista varten olevat

parametrit. Tämä nähtävillä sivulla 36. What's Up Goldille tulee näin ollen luoda jokainen config-tehtävä erikseen. Ipswitch myös tarjoaa verkkokursseja omien scriptien käyttämisen helpottamiseksi, jossa käydään läpi VBscript sekä JScript.

Virheellisten konfiguraatiotehtävien ajamiseen kuitenkaan ei millään tutkituista hallintajärjestelmistä ollut fallback-ominaisuutta. Jos virheellinen konfiguraatio tietoliikennelaitteessa katkaisee hallintayhteydet verkonhallintajärjestelmään, ei järjestelmä kykene sitä palauttamaan entiselleen. Fallback-ominaisuus tulisi näin ollen löytyä itse tietoliikennelaitteilta, joka vaatisi käyttäjältä tai verkonhallintajärjestelmältä toimenpiteen, että vasta tehty muutos ei palautuisi aikaisempaan konfiguraatioversioon. Jotkin laitevalmistajat ovatkin ottaneet kyseisen ominaisuuden yleisestikin käyttöönsä tuotteillaan, ja kyseisen toiminteen pystyisi myös toteuttamaan Ciscon, HP, ja Juniper laitteilla tekemällä kustomoidun Shell-scriptin laitteelle.

Muiden järjestelmien integroiminen keskitettyihin hallintasovelluksiin

Kaikki selvitystyössä tutkitut hallintajärjestelmät mainitsevat dokumenteissaan olevan mahdollista yhdistää jo valmiita omia järjestelmiä heidän palveluunsa. Tutkittujen tuotteiden REST API-dokumentaatioita tutkimalla voidaan tehdä johtopäätös, että niiden pääpaino käyttötarkoituksessa on hakea seuratuiksi määritellyiltä objekteilta informaatiota API-rajapinnoista. Suurin osa dokumentoiduista API-rajapinnoista on itse keskitetyn hallintasovelluksen muuttujien muokkaamista varten tai seurattujen tietoliikenne objektien (kytkimet, reitittimet) seurantaa tai muokkaamista varten luotuja GET/PUT/DELETE-komentoja. Erillisen ulkopuolisen järjestelmän (Zabbix, Nessus) keräämän informaation tuominen näille keskitetyille hallintasovelluksille vaatisi valmistajilta lisää ohjelmistokehitystä sekä useiden uusien API-rajapintojen luontia. Jos monitorointijärjestelmä ja hallintasovellus haluttaisiin yhdistää, tulisi kahden erillisen järjestelmän väliin ohjelmoida uusi työkalu, joka toimisi sovittimena järjestelmien välillä. Tämä toisi järjestelmän käyttöönottoon huomattavan lisätyön, joka vaatisi asiantuntijuutta usealta eri toimialalta.

Havainnot ja omat kokemukset

Verkonhallintajärjestelmiä tutkiessa, ja käyttäessä usein heräsi ajatus, kuinka itse toteuttaisi vastaavan muutospohjan toteutuksen usealle laitteelle. Samat muutospohjat kyettäisiin toteuttamaan esimerkiksi Ansiblella suoritettavilla tehtävillä ja määrittelemään ne ajettaviksi useille laitteille. Pienelläkin ohjelmointiosaamisella saataisiin toteutettua muutospohjien suorittamiset, mutta itsetoteutetut ratkaisut olivat rajattuna pois tutkimuksesta.

Cisco Prime Infran käyttö jää selkeästikin vajaaksi kolmannen osapuolen laitekannan kanssa, eikä käytännössä niille voida tehdä mitään muuta kuin monitoroida SNMP-, ja ICMP-kyselyiden kanssa. Itse Ciscon oman käyttöjärjestelmän omaavien laitteiden hallinta sekä muutostöiden teko on nopeaa ja yksinkertaista. Myös itse tehtyjen Task-muutospohjien luonti on jouhevaa. Valmiin muutospohjan käyttäminen ei vaadi tämän jälkeen enää käyttäjältä tietämystä komentorivisyntaksista. Jokainen konfiguraatiomuutos on jaoteltuina pieniin osiin Prime Infrassa, eli laajempien muutostöiden tekemistä varten tulee ajaa useita task-muutospohjia. Tämä ominaisuus yksinkertaistaa töiden hyväksymistä järjestelmävalvojan roolissa.

What’s Up Goldin kautta onnistuisi tekemään eri laitevalmistajien laitteille useita eri omia muutospohjia samalla tavalla kuin SolarWindsillä. Omien muutospohjien tekeminen What’s Up Goldilla tosin vaatii tekijältä vahvan tuntemuksen CLI-syntakseista sekä niiden määrittelyistä. Pelkkä tuntemus CLI-syntaksista ei kuitenkaan What’s Up Goldin käytön kanssa riitä, ja muutospohjien luontia varten tulee ymmärtää kuinka What’s Up Goldin muutospohjat rakennetaan. Tähän löytyy heidän sivuiltaan ohjeistus. Tosin kokeilemalla testiympäristössä, yleisin lopputulema oli ”Task Failed”-ilmoitus järjestelmältä, vaikkakin käytettiin tarjolla olevaa What’s Up Goldilta ohjeistusta skriptien, heidän omien funktioiden sekä muuttujien käyttämiseen.

NetBrain vaikuttaa mielenkiintoiselta ratkaisulta, joka tukee useita eri valmistajia. Sen lähestymistapa eroaa täysin muista järjestelmistä, kun se tallentaa tietokantaansa jokaisen komennon mitä CLI-rajapinnan kautta voidaan syöttää laitteelle. Sen myötä se järjestelmä kehittyy laitekannan vaihtuessa tai päivittyessä. NetBrainin reaaliajassa päivittyvä digitaalinen kaksonen verkosta tuo varmasti vianselvitykseen

helpottavan työkalun, ja vika voidaan paikantaa jopa ennen sen syntymistä. Myös valmistajan aktiivinen laitteiden tuettujen laitteiden lisääminen tarpeen mukaan tuo arvostettavan lisän tälle järjestelmälle.

Loppulause

Oma kokemus kyseisistä verkonhallintajärjestelmistä on osittain ristiriitainen. Järjestelmät tarjoavat isolle määrälle laitteita paljon ominaisuuksia niiden monitorointiin ja hallintaan. Silti päällimmäiseksi ajatukseksi on jäänyt niiden ”yksinkertaisuus”. Järjestelmät eivät vielä kykene luomaan itsenäisesti mitään päätöksiä muutostöistä, ja ne tukeutuvat täysin asetuksiin, jotka niille on ennalta määritelty. Luodakseen jotain interaktiivista tehtävää, tulee erikseen määritellä hallintajärjestelmälle mitkä ovat minkäkin laitevalmistajan outputlausekkeet komentorivillä. Pienenkin virheen sattuessa luotavalle tehtävälle, voi se pahimmassa tapauksessa lamaannuttaa koko verkon, eikä palautumismekaniikkaa ole, muuta kuin paikallisesti ajossa olevien konfiguraatioiden muuttaminen serial-konsolin avulla.

Vaikkakin nämä hallintajärjestelmät ovat vielä hieman yksinkertaisia, helpottaa silti niiden käyttäminen suurien muutostöiden tekemistä. Manuaaliseen työhön verrattuna toistamalla samaa tehtävää manuaalisesti, sanoisin että virheen mahdollisuus nousee potentiaalisesti ja näillä hallintajärjestelmillä virhemahdollisuudet eliminoitaisiin pois.

Lähteet

Auditing Device Configurations for Compliance. N.d. Cisco.com-verkkosivut. Viitattu 29.3.2020.
https://www.cisco.com/c/dam/en_us/training-events/product-training/prime-infrastructure-30/ja-audit/PI30_JA1_Audit.pdf

Cisco PI 3.7 Quick Start guide. 2019. Cisco.com-verkkosivut. Viitattu 23.01.2020.
https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/quickstart/guide/bk_Cisco_Prime_Infrastructure_3_7_0_Quick_Start_Guide.html#con_1070036

Cisco PI 3.7 User Guide. 2020. Cisco Prime Infrastructuren käyttöopas. Viitattu 23.01.2020.
https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide.html

Cisco Prime Infrastructure 3.0 User Guide. Cisco.com-verkkosivut 2018. Viitattu 29.03.2020.
https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/user/guide/pi_ug/compliance.html

Cisco Prime Infrastructure versions. 2019. Cisco.com-verkkosivut. Viitattu 19.02.2020.
https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/tsd-products-support-series-home.html

Cisco Security Advisories. N.d. Cisco.com-verkkosivut. Viitattu 1.4.2020.
https://tools.cisco.com/security/center/publicationListing.x?resourceIDs=190324&apply=1&totalbox=1&cp0=190324#~FilterByProduct

Compatibility information. N.d. Cisco.com-verkkosivut. Viitattu 29.3.2020.
https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-device-support-tables-list.html.

Corporation Fact Sheet. N.d. Zoho-yhtiön esittelyartikkeli, verkkojulkaisu. Viitattu 10.4.2020.
https://download.manageengine.com/pdf/factsheet.pdf

Currently Supported Software Versions. 2019. Solarwinds.com-verkkojulkaisu. Viitattu 19.2.2020.
https://support.SolarWinds.com/SuccessCenter/s/article/Currently-supported-software-versions

Danner, T. 2018. REST. Orion-SDK dokumentaatio. Viitattu 21.01.2020.
https://github.com/SolarWinds/OrionSDK/wiki/REST

Dynamic Map. N.d. Netbraintech.com-verkkosivusto. Viitattu 29.03.2020.

https://www.netbraintech.com/features/dynamic-map/

Editions and pricing. N.d. Manageengine.com-verkkojulkaisu. Viitattu 18.4.2020 https://www.manageengine.com/network-monitoring/opmanager-editions.html

End of Life Policy. 2020. Solarwinds.com-verkkojulkaisu. Viitattu 1.4.2020. https://support.solarwinds.com/SuccessCenter/s/article/End-of-Life-Policy

End-of-Sale and End-of-Life Announcement for the Cisco NCS, WCS, LMS and Prime Infrastructure PIDs for versions 1.X, 2.X, and 3.0. 2018. Cisco.com-verkkosivut. Viitattu 31.02.2020. https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-infrastructure/eos-eol-notice-c51-741107.html

End-of-Sale and End-of-Life Announcement for the Cisco Prime Infrastructure HW Gen2 Appliance and 3.1 and 3.2 Software. 2019. Cisco.com-verkkosivut. Viitattu 29.02.2020. https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-infrastructure/eos-eol-notice-c51-742181.html

Hay, R. 2012. Windowsobserver.com-verkkojulkaisu. Viitattu 18.4.2020. https://www.windowsobserver.com/2012/12/18/rhinosoft-acquired-by-solarwinds-ftp-voyager-now-offered-as-free-tool/

How can IT be easier for you? N.d. Solarwinds.com-verkkojulkaisu. Viitattu 18.4.2020. https://www.solarwinds.com/solutions/orion

Järvenpää, E. Laadullinen tutkimus. 2006. Verkkojulkaisu. Viitattu 13.4.2020 http://www.cs.tut.fi/~ihtesem/k2007/materiaali/luento4.pdf

ManageEngine System Requirements, N.d. Manageengine.com-verkkojulkaisu. Viitattu 1.4.2020. https://www.manageengine.com/network-configuration-manager/system-requirements.html

Morrison C. 2009. Venturebeat.com-verkkojulkaisu. Viitattu 18.4.2020. https://venturebeat.com/2009/01/06/is-network-management-growing-solarwinds-picks-up-kiwi-enterprises/

Multi-module system guidelines for the Orion Platform. N.d. Solarwinds.com-verkkojulkaisu. Viitattu 23.01.2020. https://documentation.SolarWinds.com/en/Success_Center/orionplatform/Content/Core-Multi-Module-System-Guidelines.htm

Multi-Vendor Support List. N.d. Netbraintech.com-verkkosivusto. Viitattu 29.03.2020. https://www.netbraintech.com/ftp/EE62/OnlineHelp/index.html?multi-vendor-support-list.htm

NetBrain features. 2020. Netbraintech.com-verkkosivut. Viitattu 23.01.2020. https://www.netbraintech.com/features/

NetBrain System Specification. N.d. Netbraintech-verkkosivut. Viitattu 15.02.2020. https://www.netbraintech.com/wp-content/uploads/2019/11/NetBrain_System_Specification.pdf

Network Management Licensed Products. N.d. Solarwinds.com-verkkojulkaisu. Viitattu 29.03.2020.
https://www.solarwinds.com/network-management-software

Network Monitoring Software, N.d. Ipswitch.com-verkkojulkaisu. Viitattu 29.03.2020. https://www.whatsupgold.com/network-monitoring-software

OpManager - System Requirements. 2019. Manageengine.com-verkkojulkaisu. Viitattu 21.01.2020.
https://www.manageengine.com/network-monitoring/help/hardware-and-software-requirements.html

OpManager NCM. N.d. Manageengine.com-verkkojulkaisu. Viitattu 19.02.2020. https://www.manageengine.com/network-monitoring/network-configuration-management.html

OpManager Network monitoring features. 2020. Manageengine.com-verkkojulkaisu. Viitattu 21.01.2020.
https://www.manageengine.com/network-monitoring/features.html

Prime Infrastructure 3.x Data Sheet. 2020. Cisco.com-verkkojulkaisu. Viitattu 23.01.2020.
https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-infrastructure/datasheet-c78-735696.html

Product Life Cycle Plan. N.d. Manageengine.com-verkkojulkaisu. Viitattu 1.4.2020. https://www.manageengine.com/eol_support.html

Rokka, H. 5FeetNetworks. 2020. Verkkojulkaisu. Viitattu 07.01.2020. https://www.5feetnetworks.com/2020/01/21/it-verkon-vaatimustenmukaisuus-jasen-tarkastus-oli-vaikeaa-ei-ole-enaan/

Rouse, M. Network Management System. 2018. Verkkojulkaisu. Viitattu 29.01.2020. https://searchnetworking.techtarget.com/definition/network-management-system

Sathayan, J. Fundamentals of EMS, NMS and OSS/BSS. 2010. Library.books24x7.com-E-kirja. Viitattu 13.4.2020.

Solarwinds. N.d. Solarwinds.com-verkkosivujen tuoteryhmät. Viitattu 18.4.2020. https://www.solarwinds.com/

SolarWinds Orion Requirements. 2019. solarwinds.com-verkkojulkaisu. Viitattu 21.01.2020.
https://documentation.SolarWinds.com/en/Success_Center/orionplatform/Content/Core-Orion-Requirements-sw1916.htm

Suunnitteluosaaminen. N.d. Nodeon Oy:n verkkojulkaisu. Viitattu 4.4.2020.
https://www.nodeon.com/palvelut/suunnittelupalvelut

Using the WhatsConfigured Custom Script Language. N.d. Ipswitch.com-dokumentti-kirjaston julkaisu. Viitattu 10.4.2020.
https://docs.ipswitch.com/NM/78_WhatsConfigured%20v3.0/02_Guides/Custom%20Script%20Language/Using%20the%20WhatsConfigured%20Custom%20Script%20Language.pdf

What's Up Gold Documentation. 2019. Ipswitch.com-verkkojulkaisu. Viitattu 21.1.2020.
https://docs.ipswitch.com/en/whatsup-gold.html

WhatsUp Gold RESTful API (V1). 2019. Ipswitch.com-verkkojulkaisu. Viitattu 21.01.2020.
https://docs.ipswitch.com/nm/whatsupgold2019_2/02_Guides/rest_api/#

Liitteet

Liite 1. Alkuselvityksissä kartoitettuja järjestelmiä.

Verkonhallintajärjestelmä	Monitorointi	Tietoliikennelaitteiden hallinta	Multiven-dor	Compliance Audits	Muiden järjestel-mien integrointi
Cisco Prime Infrastructure 3.7	✓	✓**	Osittainen	✓	API-rajapintojen kautta
SolarWinds	✓	✓	✓	✓	API-rajapintojen kautta
ManageEngine OpsManager	✓	✓	✓	✓	API-rajapintojen kautta
What's Up Gold	✓	✓	✓	✓*	API-rajapintojen kautta
NetBrain	✓	✓	✓	✓	API-rajapintojen kautta
HP ICM / Aruva Airwave	✓	✓	Osittainen	-	-
OpenSwitch	✓	✓	Osittainen	-	-
rConfig	×	✓	✓	×	×
PRTG	✓	×	✓	***	***
RANCID	✓	×	✓	***	***
Splunk	✓	×	✓	***	***
Nagios	✓	×	✓	***	***
Cacti	✓	×	✓	***	***
Zabbix	✓	×	✓	***	***