

Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

NTIVIS14

2016

Mira Samsten

VERKONHALLINTATYÖKALUN HYÖDYNTÄMINEN KONESALISSA

Mira Samsten

VERKONHALLINTATYÖKALUN HYÖDYNTÄMINEN KONESALISSA

Opinnäytetyön toimeksiantajan, System Partners Oy:n toiveena oli selvittää, miten Cisco Prime Infrastructure 3.0 -verkonhallintatyökalu toimisi yrityksen pienehkössä konesaliympäristössä, erityisesti uusien laitteiden käyttöönotossa sekä mahdollisten ongelmatilanteiden selvityksessä ja ratkaisussa.

Teoriaosuudessa on esitelty lyhyesti lähiverkkoihin ja niiden ylläpitoon liittyviä asioita ja käsitteitä. Termien yksityiskohtiin ei kuitenkaan menty liian syvälle.

Toimeksiantaja tarjosi opinnäytetyön käyttöön testiympäristön, joka piti sisällään virtuaalipalvelimen ja kytkimen. Prime Infrastructuren kokeiluversio asennettiin palvelimelle, jotta ohjelman eri ominaisuuksia ja toimintoja saatiin tutkittua tarkemmin. Suuri osa työstä jäi pelkästään teoreettiseksi pohdinnaksi, aikataulullisten haasteiden ja testiympäristön suppeuden takia. Käytännön testaaminen jäi siis hyvin vähäiseksi.

Testien perusteella voidaan todeta, että Prime Infrastructure on hyvin kattava valvonta- ja ylläpityökalu, joka vaatii melko paljon säätöä ennen kuin sitä voidaan hyödyntää verkkojen ylläpidossa. Laitteiden valvonta onnistuu melko hyvin oletusasetuksilla, mutta esimerkiksi uusien laitteiden käyttöönotto vaatii ylläpitohenkilöstöltä jonkin verran perehtymistä ja työtunteja, jotta laitteiden mallipohjat ja määritykset saadaan tallennettua järjestelmään. Konfiguraatioiden sisältävien mallipohjien luonnin jälkeen työkalu tulee nopeuttamaan verkkolaitteiden konfigurointia ja käyttöönottoa. Vikatilojen selvitykseen Prime Infrastructuraa pystyy hyödyntämään useammalla eri tavalla, joten sen pitäisi nopeuttaa prosessia. Työkalu tarjoaa mahdollisiin ohjelmisto- tai laitevikoihin erilaisia toimintoja, esimerkiksi hälytysten valvonnalle, ohjelmiston palautukselle tai konfiguraation kopioinnille uuteen laitteeseen laiterikon sattuessa.

Opinnäytetyön perusteella voidaan todeta, että Prime Infrastructure pitää sisällään hyvin paljon erilaisia toimintoja, joita toimeksiantaja voi hyödyntää. Ohjelma on kuitenkin selkeästi suunnattu suuremmille verkkoympäristöille, joten se saattaa olla vähän liiankin laaja kokonaisuus toimeksiantajan konesalin tämän hetkiseen kokoon nähden. Toisaalta koska ohjelma tukee suoraan laajempaa verkkokokonaisuutta, on se mahdollisen konesalin laajennuksen kannalta hyvä asia.

ASIASANAT:

Cisco, verkonhallinta, konesali

Mira Samsten

USABILITY OF A NETWORK MANAGEMENT TOOL IN A DATA CENTER

System Partners Ltd, which is the commissioner of this thesis, wanted to know if their data center could benefit from a network management tool called Cisco Prime Infrastructure 3.0. In particular, they wanted to know if the tool could provide help with device deployment as well as with solving and handling error situations.

The theoretical section of this thesis briefly introduces local area networks and their management as well as key terms relating to local area networks so that the reader can understand the management processes better.

System Partners Ltd provided the test environment which included a virtual server and a network switch. The Prime Infrastructures evaluation version was installed to the server in order to obtain more details of its different features and functions. Only some of the features and function tests were carried out in practice because of the time and test environment's limits, so some features and function tests were handled only at a theoretical level.

The tests carried out that Prime Infrastructure is a comprehensive tool for monitoring and maintenance but it requires considerable tuning before it can be used in network management. Device monitoring works quite well with the default settings but, for example, the deployment of new devices will require some work from the maintenance personnel, in order to be able to save different templates for device configurations. After the templates are saved, the tool will likely speed up the deployment of a new network device. Prime Infrastructure can be used in different ways to solve error situations, so it should also speed up the process. There are different functions to solve software or hardware issues, for example different options for alarm monitoring, rollback option for software, and if the old device breaks or stops responding the old configuration can be deployed in the new device.

On the basis of this thesis it can be stated that Prime Infrastructure includes an extensive range of functions, which System Partners Ltd can use. However, the tool is clearly aimed for larger network environments, so it might be slightly too large for the commissioner's current data center. On the other hand, because the tool supports larger network, the possible expansion of the data center will not be an issue in the future.

KEYWORDS:

Cisco, network management, data center.

SISÄLTÖ

LYHENTEET JA SANASTO	6
1 JOHDANTO	8
2 VERKOT JA NIIDEN HALLINTA JA YLLÄPITO	9
2.1 Palvelinkeskus eli konesali	9
2.2 Laitteiden käyttöönotto	10
2.3 Verkkojen hallinta ja ylläpito	10
3 CISCO PRIME INFRASTRUCTURE 3.0	13
3.1 Version valinta	13
3.2 Laitteisto- ja ohjelmistovaatimukset	14
4 ASENNUS JA KÄYTTÖÖNOTTO	15
4.1 Asennusvaiheet	15
4.2 Selainohjelman käyttö	24
5 PRIME INFRASTRUCTUREN KÄYTTÖ	29
5.1 Käyttäjätunnusten lisääminen	29
5.2 Laitteiden lisääminen	30
5.3 Laitteiden ryhmittely	34
5.4 Verkon valvonta-asetusten määrittely	35
5.5 Verkkolaitteiden konfigurointi	38
5.6 Vianmäärittely ja ongelmanratkaisu	43
6 YHTEENVETO	47
LÄHTEET	48

KUVAT

Kuva 1. Source-näkymä.	16
Kuva 2. OVF Template Details -näkymä.	16
Kuva 3. End User License Agreement -näkymä.	17
Kuva 4. Name and Location -näkymä.	17
Kuva 5. Deployment Configuration -perusnäkymä.	18

Kuva 6. Deployment Configuration -näköymä laajennetulla pudotusvalikolla.	18
Kuva 7. Disk Format -näköymä.	19
Kuva 8. Network Mapping -näköymä.	20
Kuva 9. Ready to Complete -näköymä.	20
Kuva 10. Palvelimen luonnin jälkeinen näköymä.	21
Kuva 11. Virtuaalikoneen asetusten määrittely.	22
Kuva 12. Kirjautumisenäköymä selaimessa.	24
Kuva 13. Näköymä ensimmäisen kirjautumisen jälkeen.	25
Kuva 14. Getting Started -näköymän yläosa.	25
Kuva 15. Eri valikkorakenteet selainnäköymässä.	26
Kuva 16. Käyttöliittymänäköymän valinta.	26
Kuva 17. Perusnäköymä testiympäristössä.	27
Kuva 18. Info-näköymä prosessorikuormituksesta.	27
Kuva 19. 360°-näköymän valinta verkkotopologia-näköymästä.	28
Kuva 20. 360°-näköymä testiympäristön kytkimestä.	28
Kuva 21. Käyttäjien hallintänäköymä.	29
Kuva 22. Uuden käyttäjätunnuksen luominen.	30
Kuva 23. Laitenäköymä.	31
Kuva 24. CSV-tiedoston tuominen Prime Infrastructureen.	32
Kuva 25. Laitteen lisääminen.	33
Kuva 26. Ryhmän lisääminen.	34
Kuva 27. Lisätty ryhmä.	35
Kuva 28. Valmiit mallipohjat valvontaa varten.	36
Kuva 29. Kytkimen valvonta-dashletit.	36
Kuva 30. Valvontakäytännön lisäys.	37
Kuva 31. Network Devices -näköymä	38
Kuva 32. Features & Technologies -näköymä.	39
Kuva 33. App Visibility -mallipohjan luominen.	40
Kuva 34. Configure Interface -mallipohja.	41
Kuva 35. Configure Interface -mallipohjan CLI-sisältö.	42
Kuva 36. Tyhjä CLI-pohja.	42
Kuva 37. Alarm Summary -näköymä.	44
Kuva 38. My Preferences -valinta.	44
Kuva 39. Hälytysasetusten muokkaus.	45
Kuva 40. Testikytkimen laitetiedot.	45

TAULUKOT

Taulukko 1. Minimilaitteistovaatimukset Prime Infrastructure -palvelimelle. (Cisco Systems 2016a)

LYHENTEET JA SANASTO

AAA-suojaus	AAA security, Authentication, Authorization, Accounting. Käyttäjien todennus ja valtuutus, sekä tietojen kerääminen ja kirjaaminen lokiin.
CLI	Command-line Interface. Komentorivi eli tekstipohjainen käyttöliittymä.
Dashlet	Prime Infrastruktuuren käyttöliittymässä erikseen näytetty valvontaruutu, joka voi sisältää esimerkiksi tilastoja ja kaavioita laitteiden ja verkon tilasta.
ICMP	Internet Control Message Protocol. TCP/IP-protokolla, jonka avulla verkon laitteet voivat jakaa virhe- ja tilatietoja. Yleisin käytetty ICMP-työkalu on Ping.
IPS	Intrusion prevention system. Tunkeilijan havaitsemisjärjestelmä, jolla pyritään tunnistamaan verkkoon suuntautuvat hyökkäysyritykset.
IPsec	Internet Protocol Security. Tietoliikenneprotokolla IP-yhteyksien turvaamiseen.
Konfigurointi	Asetusten säätö siten, että laite tai ohjelma saadaan otettua käyttöön.
OVF-malli	Open Virtual Machine Format template. VMware Sphere -työkalun hyödyntämä mallipohja, jolla saadaan luotua virtuaalikoneita ja -palvelimia.
Ping	Työkalu, joka kokeilee määrätyn laitteen saavutettavuutta verkossa.
QoS	Quality of service. Verkon suoritus- ja palvelukyky.
SNMP	Simple Network Management Protocol. Kehitettiin alkuun IP-verkkojen hallintaa ja valvontaa varten.
TCP/IP	Transmission Control Protocol / Internet Protocol. Verkkojen kommunikointiprotokolla. Alemman tason IP-protokolla vastaa päätelaitteiden osoitteista ja pakettien reitittämisestä. TCP-protokolla vastaa päätelaitteiden välisistä tiedonsiirtoyhteyksistä.
TrustSec	Ciscon oma teknologia, jolla käyttäjän tai laitteen verkkoliikenne merkitään Security Group Tag (SGT) -tiedolla. Tämän jälkeen verkkoliikennettä ohjataan pääsyylojen avulla SGT-tietoa hyödyntäen.
Verkkotopologia	Kuvaa tapaa, jolla verkon laitteet on liitetty toisiinsa.

VLAN	Virtual Local Area Network. Fyysinen verkko jaetaan loogisiin osiin kytkinten tai reitittimien avulla, esimerkiksi eri osastot voivat olla omissa VLAN-ryhmissään, osastojen käytössä olevien laitteiden fyysisestä sijoittelusta riippumatta.
VMware ESXi	Palvelinvirtualisointialusta.
VPN	Virtual Private Network. Virtuaalinen erillisverkko, jolla yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.

1 JOHDANTO

Opinnäytetyössä perehdytään projektiin, jossa tutkittiin mahdollisuutta automatisoida pienehkön konesalin ylläpitotoimintoja. Projektissa keskityttiin verkkolaitteisiin, pääasiallisesti Cisco Systems (yleisemmin tunnettu nimellä Cisco) kytkimiin ja siihen, miten hallita niiden ylläpito- ja käyttöönotto-tilanteita.

Projektin toimeksiantaja on System Partners Oy, joka oli kiinnostunut mahdollisuudesta saada automatisoitua kytkinten peruskonfigurointi sen sijaan, että jokaisen laitteen asennus- ja käyttöönottoimenpiteet suoritetaan manuaalisesti. Toimeksiantajan toiveena olikin löytää mahdollinen ratkaisu laitteiden käyttöönottojen ja vikatilanteiden selvitysten tehostamiseen.

System Partners Oy käyttää konesalissaan pääasiassa Cisco Catalyst -sarjan kytkimiä sekä joitain Ciscon reitittimiä, joten päätettiin, että eri ohjelmavaihtoehtoja ei tutkita, vaan keskitytään ainoastaan Cisco Prime Infrastructure -ohjelmaan (myöh. Prime Infrastructure). Työ toteutettiin System Partners Oy:n tarjoamassa virtuaalisessa testiympäristössä.

Konesaleja eri näkökulmista tarkastelevia opinnäytetöitä löytyy useampia. Prime Infrastructure -ohjelmaa on hyödynnetty langattomien verkkojen valvontaa koskevassa opinnäytetyössä Oulun seudun ammattikorkeakoulussa (Lapinoja 2013). Opinnäytetöitä, jossa selvitetään Prime Infrastructure -ohjelman käytön hyödyllisyyttä pienemässä konesalissa, ei ole aikaisemmin tehty.

Opinnäytetyön alussa käsitellään verkkojen hallintaa ja ylläpitoa teoriassa. Luvussa 3 esitellään Prime Infrastructure -ohjelma. Lopuksi käydään läpi Prime Infrastructuren käyttöönottoa ja käyttöä testiympäristössä.

2 VERKOT JA NIIDEN HALLINTA JA YLLÄPITO

Yrityksillä on käytössään erilaisia verkkoratkaisuja. Eri verkkokokonaisuuksia ovat

- lähiverkko – LAN eli Local Area Network
- kaupunkiverkko – MAN eli Metropolitan Area Network
- laajaverkko – WAN eli Wide Area Network.

Lähiverkko voi pienimmillään olla kotitaloudessa käytössä oleva muutaman laitteen verkko, mutta yrityksillä se voi tarkoittaa useamman kymmenen tai jopa useamman sadan koneen kokonaisuutta. Lähiverkko siis kytkee työasemat, tulostimet, palvelimet ja muut verkkolaitteet toisiinsa pienellä maantieteellisellä alueella, esimerkiksi yhdessä tai useammassa lähekkäin olevassa rakennuksessa. Kaupunkiverkolla voidaan yhdistää lähiverkot maantieteellisesti lähekkäin olevilla alueilla, esimerkiksi kaupunki ja sen lähikunnat. Laajaverkko puolestaan yhdistää lähiverkot ja kaupunkiverkot yhdeksi suureksi verkoksi maantieteellisten etäisyyksien juuri vaikuttamatta asiaan. Internet voidaan luokitella kaikkein suurimmaksi laajaverkoksi. Yrityksillä saattaa olla käytössään useampia lähiverkkoja, jotka on yhdistetty toisiinsa joko kaupunki- tai laajaverkkoa tai kumpaakin hyödyntäen.

Lähiverkkojen yhdistäminen isompiin kokonaisuuksiin vaatii käyttöönsä kytkimiä ja reitittimiä, joiden avulla saadaan määriteltä, että lähiverkkojen liikenne kulkee oikeita reittejä pitkin. Kytkinten, reitittimien ja palomuurien asetuksilla määritellään, kenellä on pääsy yrityksen sisäverkkoon ja mihin eri verkkoliikenteet tulee ohjata (Cisco Systems, 2012.)

2.1 Palvelinkeskus eli konesali

Palvelinkeskus (Data center), josta suomen kielessä käytetään yleisesti myös termiä konesali, on tila tai laitos, jossa ylläpidetään tietoteknisiä laitteita ja niihin liittyviä asioita, kuten tietoliikennelaitteita ja tallennusjärjestelmiä. Yleensä konesalit ja niiden sisältämät laitteet on varmennettu vaihtoehtoisilla sähkön- ja tiedonsiirtoväylillä, turvattu ympäristötekijöiltä, esimerkiksi tehokkaalla ilmastoinnilla ja palonsammutusjärjestelmillä sekä suojattu erilaisilla turvalaitteilla (Wikipedia 2016). Konesaleissa ylläpidetään usein muun muassa seuraavia palveluita:

- tiedostojen tallentamiseen tarkoitettuja levyjärjestelmiä

- palvelimia, jotka nykyään pyritään virtualisoimaan fyysisten laitteiden määrän vähentämiseksi ja käytön tehostamiseksi
- hyvät tietoliikenneyhteydet palveluiden nopean saatavuuden takaamiseksi.

2.2 Laitteiden käyttöönotto

Laitteiden käyttöönottoon liittyy termi provisiointi, joka tarkoittaa laitteen valmistelua sellaiseen tilaan, että se voidaan ottaa sille tarkoitettuun käyttöön automatisoidusti ilman, että IT-asiantuntijoiden tarvitsee osallistua käyttöönottoon (Suomi Sanakirja 2015). Provisioinnilla voidaan myös tarkoittaa laitteen, esimerkiksi kytkimen konfigurointia käyttövalmiiksi joko manuaalisesti tai automatisoidusti.

Verkkolaitteiden, esimerkiksi kytkinten, reitittimien ja langattomien tukiasemien, osalta konfigurointi pitää yleensä sisällään muun muassa IP-osoitteen tai -osoitteiden, turvallisuusasetusten, VLAN-ympäristöjen ja muiden porttiasetusten määrittelyt. Kun laitteen asetusten konfigurointi ja dokumentointi on saatu valmiiksi, voidaan laite kytkeä verkkoon ja ottaa käyttöön.

2.3 Verkkojen hallinta ja ylläpito

Verkon hallinta voi pitää sisällään eri asioita verkon koon perusteella. Joissain tapauksissa se pitää sisällään vain yksittäisen verkkokonsultin, joka valvoo verkon aktiivisuutta. Muissa tapauksissa siihen voi liittyä jaettuja tietokantoja, verkkolaitteiden automaattista valvontaa ja tehotyöasemien tuottamaa ajantasaista, graafista näkymää verkkotopologian muutoksista ja verkkoliikenteestä. Yleisesti ottaen verkon hallinta on kuitenkin palvelua, jossa ylläpitohenkilöstö hyödyntää erilaisia työkaluja, ohjelmistoja ja laitteita verkkojen valvonnassa ja ylläpidossa. (Cisco Systems 2012.) Verkkojen hallintaan ja ylläpitoon kuuluvat olennaisesti verkon dokumentointi, turvallisuus, toimintakyky ja luotettavuus.

Dokumentointi

Dokumentoinnin avulla ylläpitäjät pysyvät perillä esimerkiksi laitteiden fyysisistä ja loogisista kytköksistä. Verkon dokumentoinnilla voidaan myös säästää huomattavasti aikaa,

mikäli vikatilanteita ilmenee. Lisäksi dokumentoinnin avulla voidaan havaita mahdollisten verkkomuutosten tarpeellisuus, kun verkkokokonaisuuksien hahmottaminen onnistuu paremmin. Kun dokumentointi on kirjattu riittävän tarkasti ja kattavasti, voidaan sen avulla rakentaa uusi vastaava verkkoympäristö alusta lähtien, mikäli tarvetta ilmenee.

Dokumentointiin kuuluvat olennaisesti seuraavat asiat:

- verkotopologia, sekä fyysinen että looginen, joka kuvaa laitteiden välisiä kytköksiä
- palvelinten nimien, roolien ja IP-osoitteiden kirjaaminen
- muutoslokien kirjaaminen ja ylläpito
- ohjelmistoversioiden kirjaaminen
- verkkolaitteiden dokumentointi
 - o miten laitteet ovat kytketty verkkoon
 - o miten ne ovat konfiguroitu
 - o mitkä laiteohjelmaversiot ovat käytössä
- varmuuskopioinnin suoritus eli miten se suoritetaan ja millaisella syklillä
- laitteiden nimeäminen myös fyysisesti, ei vain paperille
- dokumentaation evaluointi eli onko dokumentaatio tarpeeksi kattava ja perusteellinen, jotta sen perusteella voidaan rakentaa tarvittaessa koko verkko uudelleen.

Dokumentointi on tarpeellista erityisesti verkon ylläpidon kannalta, mutta myös asiakkuuksien hallintaa varten. (Posey 2008.)

Verkkojen turvallisuus

Verkkojen turvallisuudella tarkoitetaan mitä tahansa toimintaa, jolla pyritään suojaamaan verkkoinfrastruktuuria sekä fyysisten laitteiden että ohjelmistojen näkökulmasta. Erityisesti näillä toimilla pyritään suojaamaan verkon ja tietojen käytettävyys, luotettavuus, toimintavarmuus ja turvallisuus. Tehokas tietoturva huomioi eri uhat ja pyrkii estämään niiden pääsyn ja leviämisen verkossa. Verkon tietoturva pohjautuu yleensä useampaan suojauskerrokseen, sisältäen muun muassa verkon valvonnan ja tietoturvaohjelmistot, kuin myös laitteistojen fyysisen suojauksen. Seuraavaksi on listattu muutamia suojaustoimenpiteitä:

- virus- ja haittaohjelmientorjunta
- palomuri

- tunkeilijan havaitsemisjärjestelmä (IPS)
- VPN-yhteyksien käyttö.

Verkon turvallisuus saavutetaan huomioimalla sekä laitteiston että ohjelmiston suojaus-tarpeet. (Cisco Systems.)

Verkon suorituskyky ja luotettavuus

Verkon suorituskyky ja luotettavuus ovat tärkeitä erityisesti käyttäjien näkökulmasta sekä tiedostojen ja palveluiden saatavuuden kannalta. Suorituskykyä pyritään parantamaan esimerkiksi verkkopalveluiden vasteajan ja hallinnan optimoinnilla sekä johdonmukais-tamalla ja lisäämällä laatua yksittäisille ja yleisille verkkopalveluille (Cisco Systems 2007). Verkon toimintakykyä pyritään parantamaan myös eliminoimalla niin sanotut pul-lonkaulat, jotka pahimmillaan estävät verkkoliikenteen kokonaan, mutta saattavat vain hidastaa sitä huomattavasti.

Redundanssi on olennainen osa verkon luotettavuutta ja vikasietoisuutta. Käytännössä redundanssi tarkoittaa esimerkiksi kahden vastaavan fyysisen laitteen hankintaa. Jos pääasiallisessa käytössä oleva laite vikaantuu, varalaite saadaan otettua käyttöön, eikä vikatilanteesta aiheudu pitkää katkosta, mahdollisesti jopa niin, että varalaite otetaan au-tomaattisesti käyttöön heti, kun valvontajärjestelmä havaitsee ensisijaisen laitteen vi-kaantuneen. Verkkojen osalta redundanssia saadaan hallinnoitua myös ohjelmallisesti määrittämällä reitittimiin ja kytkimiin varareitit verkkoliikenteitä varten. Jos ensisijaisesti käytössä oleva reitti jostain syystä ei ole saatavilla, vaihtoehtoinen reititys saadaan yleensä otettua käyttöön automaattisesti, jolloin käyttäjät eivät välttämättä edes huomaa vikatilannetta. Tällöin verkon ylläpitäjille jää enemmän aikaa vian selvittämiseen, kun vika ei vaikuta verkkoliikenteeseen käyttäjien näkökulmasta. (TechTerms 2011.)

3 CISCO PRIME INFRASTRUCTURE 3.0

Prime Infrastructure on verkkojen hallintatyökalu, joka tukee koko verkon elinkaaren ylläpitoa yhdessä graafisessa näkymässä. Prime Infrastructure tukee sekä langallisia että langattomia laitteita. Ohjelman avulla ylläpitäjät voivat muun muassa hallita uusien laitteiden käyttöönotot, verkkojen valvonnan, optimisoinnin ja vianmääritykset. Graafisen käyttöliittymän avulla laitteiden käyttöönotot ja eri ylläpitotoimenpiteet saadaan suoritettua yksinkertaisesti ja kustannustehokkaasti. (Cisco Systems 2016b.)

3.1 Version valinta

Prime Infrastructure on saatavilla kahdella eri tavalla:

- Virtuaalinen versio. Toimitetaan asiakkaalle OVA-tiedostona (Open Virtualisation Archive). Prime Infrastructuren asennus suoritetaan tarvittavat resurssit sisältävään palvelimeen, jossa on asennettuna VMware ESXi -virtuaaliympäristö. Asiakas saa siis itse päättää, mitä laitteistoa käytetään. Asennuspaketti pitää sisällään neljä eri asennusvaihtoehtoa, jotka on suunnattu eri kokoisille yrityksille – Express, Express-Plus, Standard ja Professional.
- Fyysinen versio. Toimitetaan palvelinkaappiin asennettavissa olevana laitteena, jossa Prime Infrastructure on esiasennettuna ja konfiguroituna.

Ennen Prime Infrastructuren asentamista tulee selvittää, millaisen verkon hallintaan ohjelman käyttöä suunnitellaan. Express-versio tukee yhteensä viittäsataa laitetta, mukaan lukien sekä langattomat että langalliset laitteet, kun taas Professional-versio tukee 14 000 laitetta. Professional-versio tukee jopa 150 000 langatonta ja 50 000 langallista asiakasyhteyttä. Express tukee vastaavasti 4 000 langatonta ja 6 000 langallista asiakasyhteyttä. Laitteiston mukana hankittava Prime Infrastructure tukee vastaavasti 24 000 laitetta, 200 000 langatonta ja 50 000 langallista asiakasyhteyttä. Valintaa suoritettaessa tulee ottaa huomioon myös muita rajoituksia ja määrittäviä, joista löytyy tarkemmin tietoja Ciscon omilta sivuilta. (Cisco Systems 2015.)

3.2 Laitteisto- ja ohjelmistovaatimukset

Prime Infrastructure asennetaan virtuaalipalvelimelle, mutta sitä käytetään selainohjelmalla. Version valinta vaikuttaa palvelimen vaatimuksiin taulukon 1 mukaisesti.

Taulukko 1. Minimilaitteistovaatimukset Prime Infrastructure -palvelimelle. (Cisco Systems 2016a)

	Express	Express-Plus	Standard	Professional
VMware-versio	ESXi 5.1 tai 5.5	ESXi 5.1 tai 5.5	ESXi 5.1 tai 5.5	ESXi 5.1 tai 5.5
Virtuaaliset prosessorit ¹	4	8	16	16
Muisti (DRAM)	12 GB	16 GB	16 GB	24 GB
Kiintolevytila	300 GB	600 GB	900 GB	1,2 TB
Levyn luku- ja kirjoitusnopeus	200 MB/s	200 MB/s	200 MB/s	320 MB/s

¹ Mikä tahansa yhdistelmä prosessoreita ja niiden ytimiä käy, kunhan niitä on riittävä määrä minimivaatimuksiin verrattuna.

Selainohjelman käytölle ei ole erityisiä laitevaatimuksia. Käytössä tulee olla Mac- tai Windows-käyttöjärjestelmällä oleva kannettava- tai pöytätietokone, jolla pystyy käyttämään seuraavia selaimia:

- Google Chrome 40 tai uudempi versio
- Microsoft Internet Explorer 10 tai 11
- Mozilla Firefox ESR 31, 38
- Mozilla Firefox 35 tai uudempi versio

Näytön tarkkuuden osalta Prime Infrastructure tukee 1366 x 768 tarkkuutta, mutta Cisco suosittelee selainohjelmaa käytettäväksi 1600 x 900 tarkkuudella. (Cisco Systems 2015.)

4 ASENNUS JA KÄYTTÖÖNOTTO

Prime Infrastructuren asennus voidaan suorittaa joko aikaisemman version päivityksellä tai uuden asentamisella OVA-tiedostoa hyödyntäen. Riippuen asiakkaan ja Ciscon välisestä sopimuksesta, OVA-tiedosto voi olla joko saatavilla Cisco.com-sivujen kautta ladattuna tai erillisellä asennusmedialla. Koska projektissa käytetään Prime Infrastructuren kokeiluversiosta, version päivittämistä ei käsitellä erikseen.

Palvelinlaitteessa, jolle Prime Infrastructuren asennus suoritetaan, tulee olla VMware ESXi asennettuna. Asennusvaiheessa käytetään VMware vSphere -ohjelmaa. Navigoimalla selaimella ESXi-palvelimen IP-osoitteeseen, saa avautuvalta sivustolta asennettua vSpheren. Prime Infrastructuren asentamiseen tarvittavan OVA -tiedoston tulee olla tallennettuna samalle koneelle, johon vSphere on asennettuna. (Cisco Systems 2016a.)

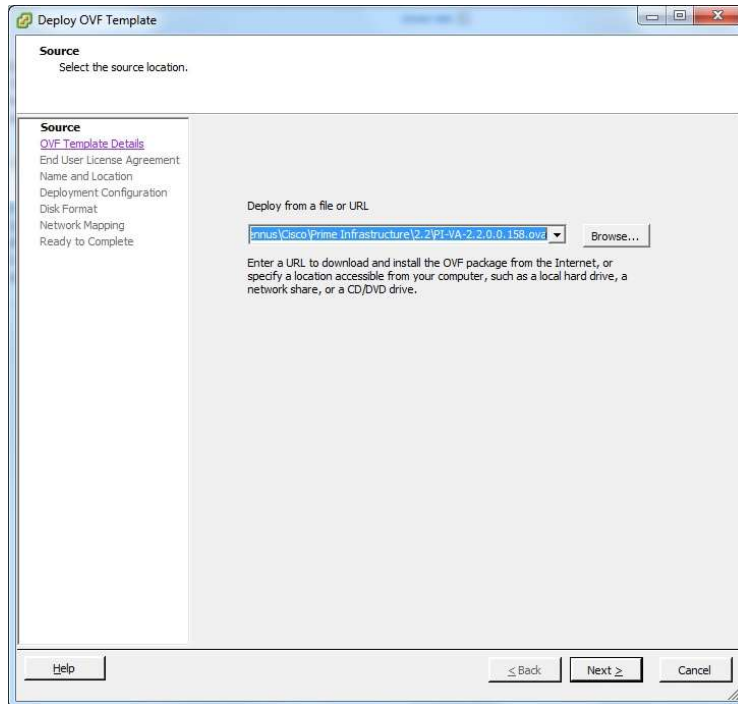
4.1 Asennusvaiheet

Asennus suoritettiin projektin alussa Prime Infrastructure 2.2 -kokeiluversiolla, mutta aikataulullisista viivästyksistä johtuen projekti suoritettiin loppuun 3.0-kokeiluversiolla. Eri asennusvaiheiden kuvakaappaukset eivät siis välttämättä vastaa kaikilta osiltaan 3.0-version asennusta. Olennaiset asiat ja valinnat ovat kuitenkin säilyneet samoina.

Prime Infrastructuren asennus oli selkeä prosessi. Asennusnäköymät olivat selkeitä ja informatiivisia. Cisco Prime Infrastructure 3.0 Quick Start Guide (Cisco Systems 2016a) auttaa kuitenkin eri asennusvaihtoehtojen valinnassa, mikäli niiden suhteen on jotain kysyttävää.

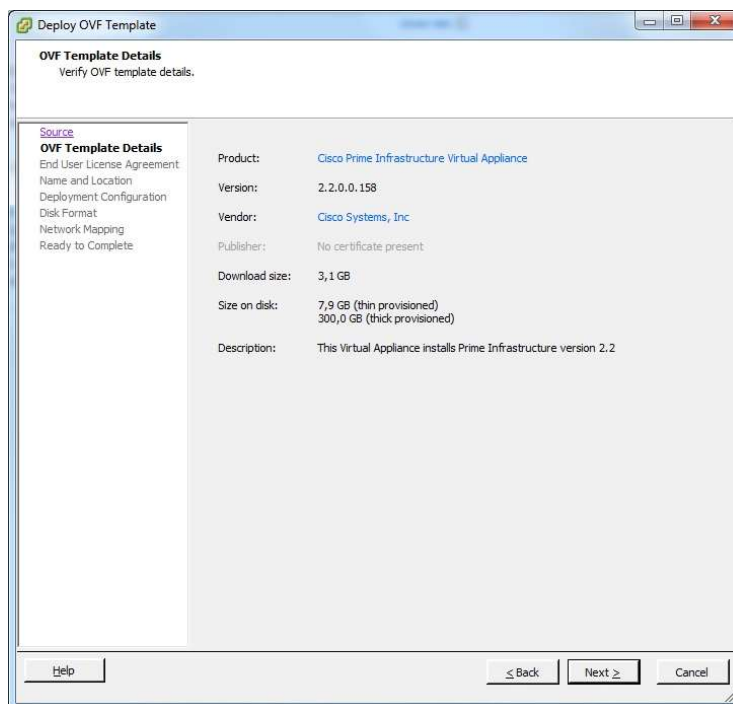
Asennusvaiheet kohta kohdalta

Ensimmäiseksi käynnistetään VMware vSphere, jolla otetaan yhteys ESXi-ympäristöön. Tämän jälkeen asennusprosessi eli virtuaalipalvelimen luominen aloitetaan valitsemalla File > Deploy OVF Template. Source-näkymästä etsitään OVA-tiedosto Browse-painikkeella, tämän jälkeen valitaan Next (Kuva 1).



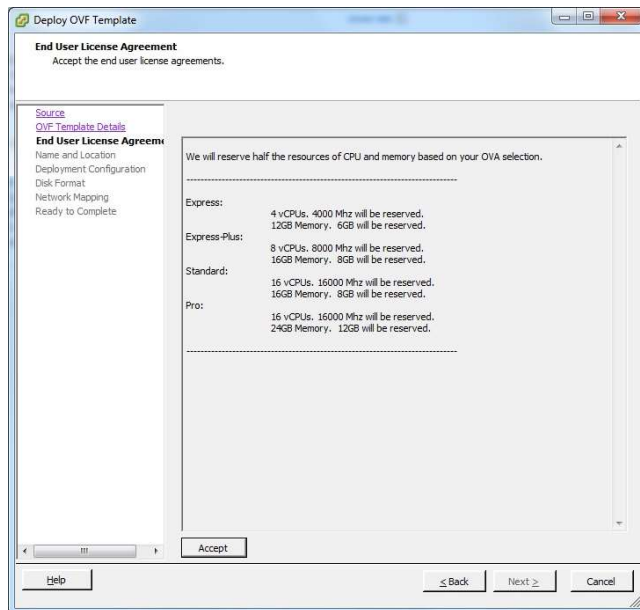
Kuva 1. Source-näkymä.

OVF Template Details -näkymässä varmistetaan, että tiedot täsmäävät, tämän jälkeen valitaan Next (Kuva 2).



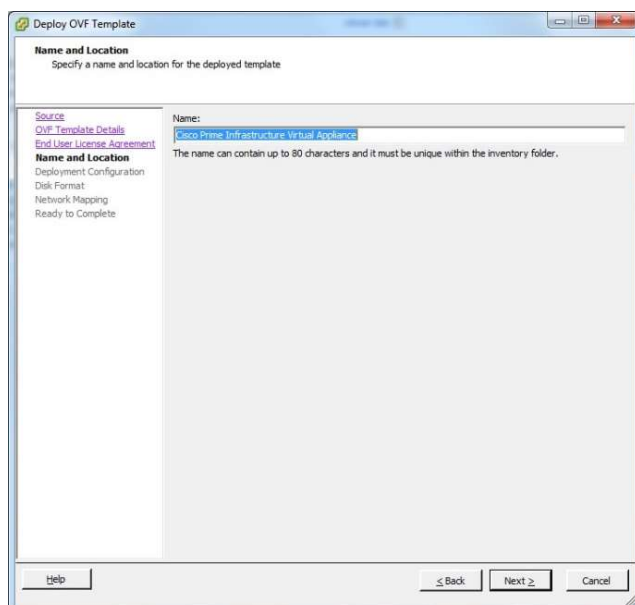
Kuva 2. OVF Template Details -näkymä.

End User License Agreement -näköymässä valitaan ensin Accept ja tämän jälkeen Next (Kuva 3).



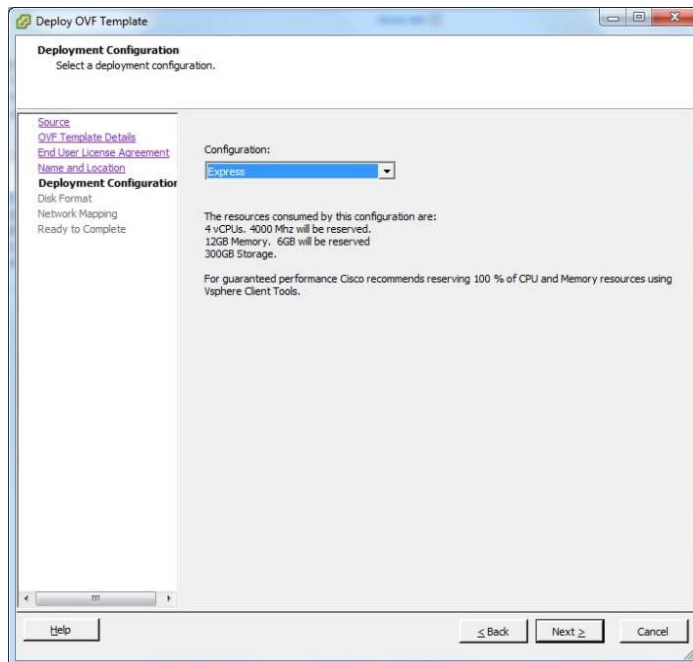
Kuva 3. End User License Agreement -näköymä.

Name and Location -näköymässä kirjoitetaan Name-kenttään uuden virtuaalikoneen nimi, jolla se näkyy ESXi-palvelimen listauksessa. Inventory Location area -kenttään valitaan oikea kansio. Mikäli vSphere ohjelma on kytkettynä ESXi-isäntään, tätä vaihtoehtoa ei ole nähtävissä (Kuva 4).

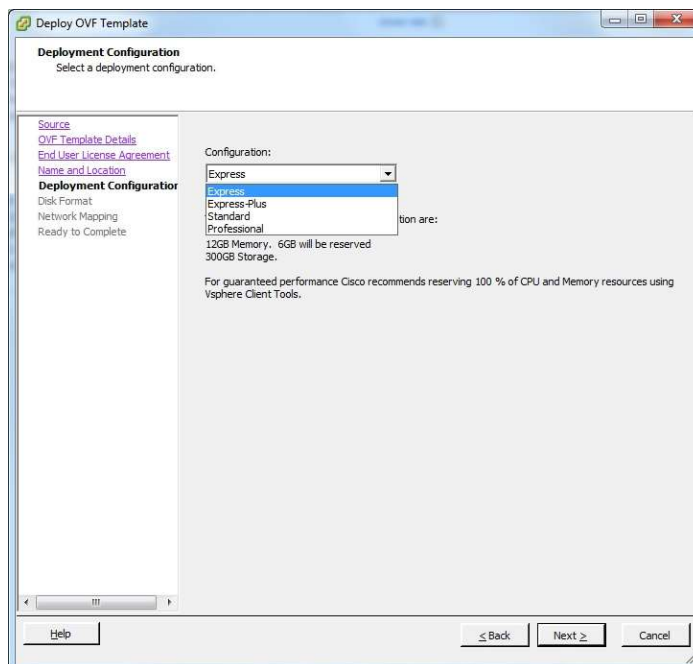


Kuva 4. Name and Location -näköymä.

Deployment Configuration -näkyssä valitaan luotava konfiguraatio eli Express, Express Plus, Standard tai Professional. Valitsemalla eri vaihtoehtoja, näkymän alaosassa näkyy eri konfiguraatioiden järjestelmävaatimukset. Sopivan konfiguraation valinnan jälkeen siirrytään eteenpäin valitsemalla Next (Kuvat 5 ja 6).



Kuva 5. Deployment Configuration -perusnäky.



Kuva 6. Deployment Configuration -näky laajennetulla pudotusvalikolla.

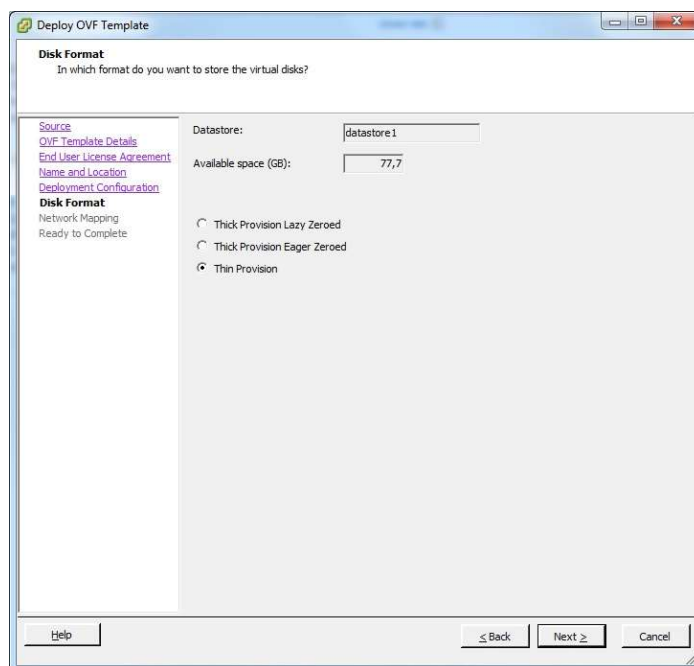
Host/Cluster-näkymästä valitaan isäntä tai klusteri, johon OVF-malli tullaan asentamaan. Mikäli vSphere ohjelma on suoraan kytkettynä ESXi-isäntään, tätä vaihtoehtoa ei ole nähtävissä.

Storage-näkymästä valitaan oikea tallennustila (datastore), jonka koko vastaa aiemmin mainittuja järjestelmävaatimuksia.

Disk Format -näkymässä valitaan kolmesta vaihtoehdosta yrityksen tarpeisiin sopivin – nämä kolme vaihtoehtoa liittyvät luotavan virtuaalipalvelimen varaamaan levytilaan:

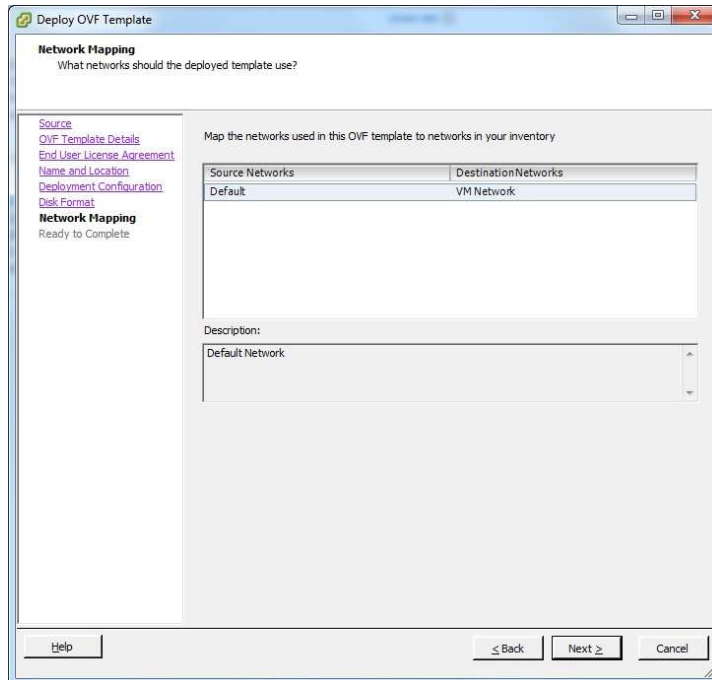
- Thick Provision Lazy Zeroed. Cisco suosittelee tätä vaihtoehtoa
- Thick Provision Eager Zeroed
- Thin Provision. Tätä vaihtoehtoa Cisco ei suosittele; jos verkkolevyn tallennustila loppuu kesken, Prime Infrastructure lakkaa toimimasta.

Prime Infrastructure 2.2 -versiossa Storage- ja Disk Format -näkymät on yhdistetty yhdelle sivulle, joten kuvakaappaus eroaa tältä osin 3.0-version asennusvaiheista (Kuva 7).



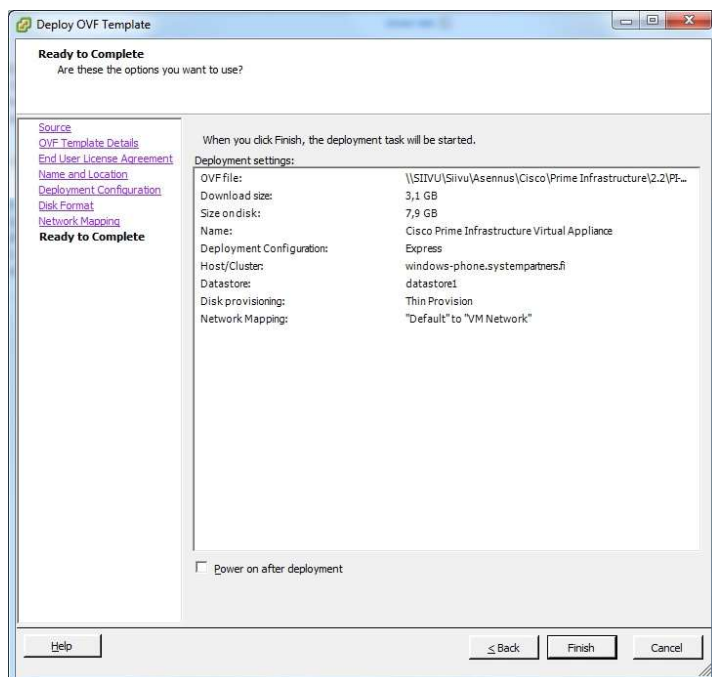
Kuva 7. Disk Format -näkymä.

Network Mapping -näkymästä valitaan oikea verkkoympäristö, jota virtuaalikone tulee käyttämään (Kuva 8).



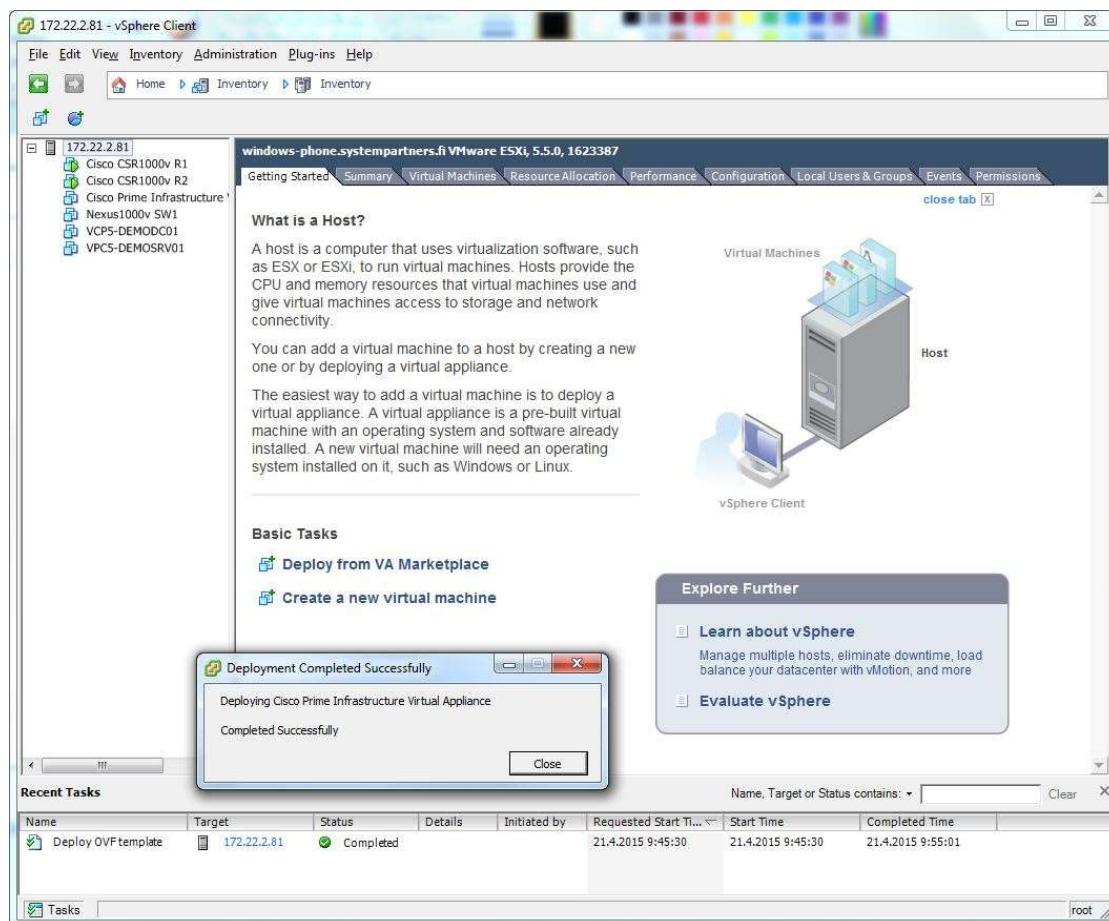
Kuva 8. Network Mapping -näköymä.

Ready to Complete -näköymässä tarkistetaan valitut asetukset, Power on after deployment -kohtaan voi halutessaan laittaa ruksin. Mikäli ruksi on valittuna, virtuaalipalvelin käynnistyy automaattisesti luontiprosessin valmistuttua (Kuva 9).



Kuva 9. Ready to Complete -näköymä.

Virtuaalipalvelimen luonnin yhteydessä vSphere-näkymästä pystyy seuraamaan prosessin tilannetta. Palvelimen luonnin valmistuttua prosessi muuttuu Completed-tilaan ja ponnahdusikkuna kertoo onnistumisesta (Kuva 10).



Kuva 10. Palvelimen luonnin jälkeinen näkymä.

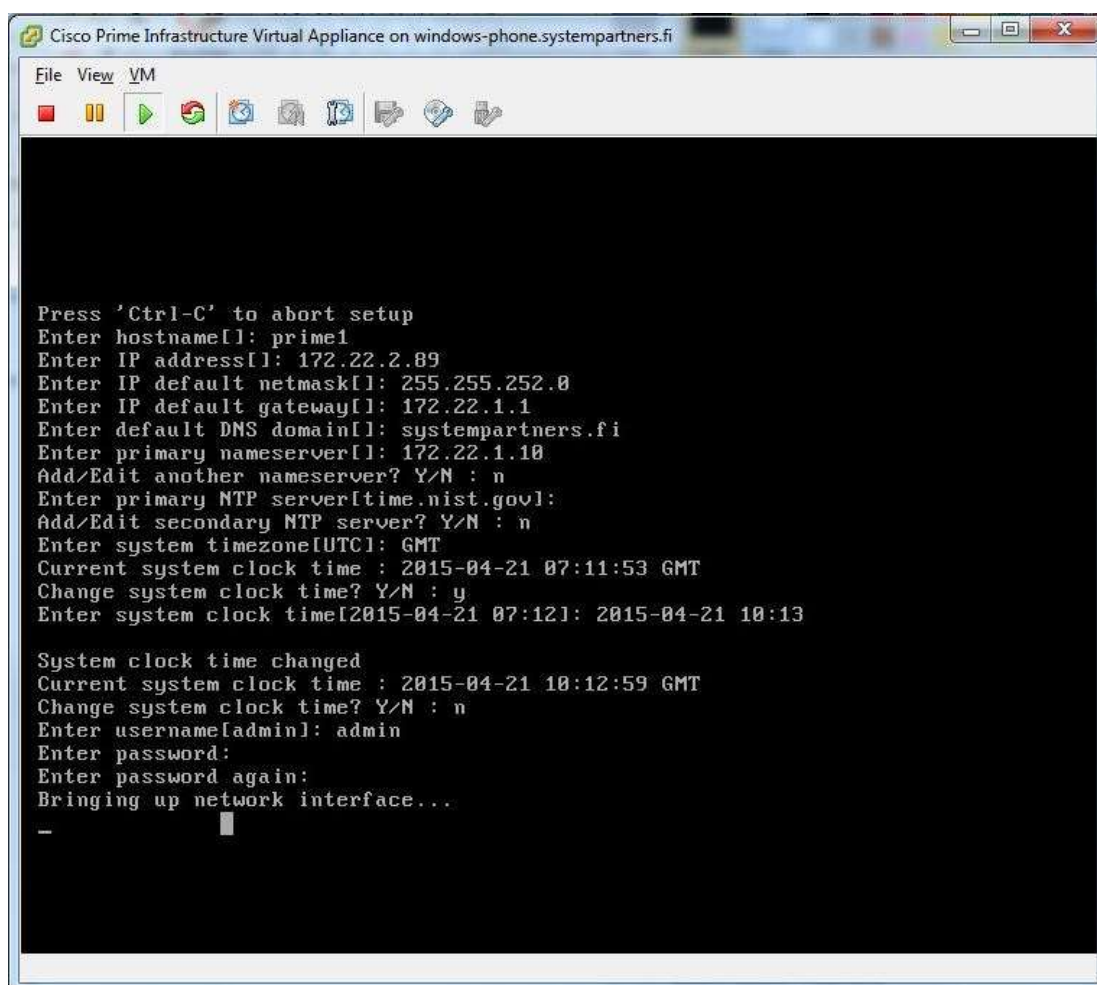
Asennuksen viimeistely

Virtuaalipalvelimen luonnin jälkeen tulee vielä suorittaa lopullinen konfigurointi, jotta Prime Infrastructure -palvelin saadaan asennettua ja otettua käyttöön. Ensimmäisenä toimenpiteenä tulee käynnistää luotu virtuaalipalvelin, jos se ei käynnistynyt automaattisesti asennuksen jälkeen.

Palvelimen ollessa käynnissä tai käynnistyessä, valitaan Console-välilehti. Näkyviin tulee palvelimen kirjautumisnäkymä. Näkymästä valitaan Setup, jonka avulla pääsee määrittämään palvelimelle seuraavat asetukset:

- Hostname: virtuaalikoneen nimi

- IP Address: virtuaalikoneen IP-osoite
- IP default netmask: verkon peite
- IP default gateway: oletusyhdysoikeava
- Default DNS domain: oletusnimipalvelimen verkkotunnus
- Primary nameserver: ensisijaisen nimipalvelimen IP-osoite
- Secondary name servers: vaihtoehtoisten nimipalvelinten IP-osoitteet, jos kyy-
tossa. Vaihtoehtoisia nimipalvelinten IP-osoitteita voi olla enintaan kolme.
- Primary NTP server: IP-osoite tai nimi ensisijaiselle Network Time Protocol -pal-
velimelle, time.nist.gov -osoite on oletusarvona.
- Secondary NTP servers: vaihtoehtoisten NTP-palvelinten osoitteet
- System Time Zone: järjestelmän käyttämä aikavyöhyke
- Clock time: palvelimen kellonaika
- Username: pääkäyttäjän käyttäjätunnus, oletuksena admin
- Password: pääkäyttäjän salasana (Kuva 11).



Kuva 11. Virtuaalikoneen asetusten määrittely.

Tietojen syötön jälkeen asennusohjelma testaa määritellyt verkkoasetukset. Mikäli testit menevät läpi, Prime Infrastructure -ohjelman asennus alkaa.

Asennuksen valmistuttua järjestelmä kysyy vielä seuraavat tiedot:

- High Availability Role Selection: tähän valitaan kyllä- tai ei-vaihtoehto.
 - o kyllä, jos palvelin halutaan liittää toissijaiseksi palvelimeksi korkean saatavuustason järjestelmään. Tämän jälkeen järjestelmä kysyy varmenneavainta rekisteröintiä varten.
 - o ei, jolloin palvelin toimii pääasiallisena palvelimena
- Web Interface Root Password: selainkäyttöliittymän pääkäyttäjän salasana. Käyttäjä tunnus on "root". Tällä tunnuksella kirjaututaan Prime Infrastruktuuren selainohjelmaan ensimmäisellä kerralla ja luodaan järjestelmän muut mahdolliset käyttäjätunnukset.

Kun asennus on valmis, virtuaalipalvelin käynnistyy uudelleen ja antaa seuraavaksi Console-näkymään kirjautumisruudun. Kirjautuminen onnistuu tämän jälkeen aiemmin määritellyllä palvelimen pääkäyttäjän tunnuksella (admin) ja salasanalla, ei siis selainkäyttöliittymän tunnuksella. Kirjautumisen jälkeen on suositeltavaa ajaa "ncs status" -komento, jolla saa varmistettua kaikkien tarvittavien prosessien käynnistymisen. Mikäli kaikki on kunnossa, pitäisi ruudulle tulla näkyviin tieto "All Processes are up and running".

Muuta huomioitavaa ennen käytön aloittamista

Ylläpitäjän näkökulmasta tulee suorittaa vielä seuraavat toimenpiteet ennen Prime Infrastructure -palvelimen käyttöä.

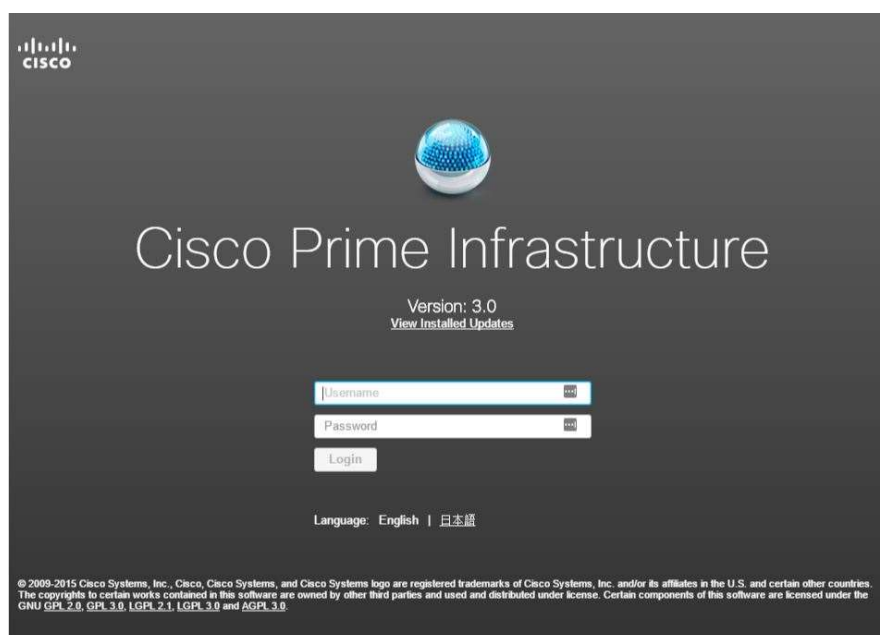
- Käyttäjätunnusten lisääminen. On suositeltavaa jättää root-tunnus pääkäyttäjäksi ja lisätä muille käyttäjille omat tunnukset. Käyttäjien lisäämisestä kerrotaan luvussa viisi lisää.
- Levytilan asetusten määrittelyt. Prime Infrastructure -palvelimen levytilan täytyessä 90-prosenttisesti, palvelin antaa ison hälytyksen (Major alert) alhaisesta levytilasta. Hälytykset ja levytilan määrittelyt ovat suositeltavaa suorittaa heti ensimmäisenä toimenpiteenä, jotta levytilan täytyminen ei tulevaisuudessa aiheuta ongelmia.

- AAA-suojauksen asetusten tarkistus. Mikäli Prime Infrastructure päivitettiin uudempaan versioon ja vanhassa oli kyseiset suojausasetukset määriteltynä, tulee ne päivittää ajan tasalle.
- Ohjelmistopäivitysten tarkistus. Cisco julkaisee Prime Infrastructurea koskevia päivityksiä, joten heti asennuksen jälkeen on hyvä asentaa mahdolliset saatavilla olevat päivitykset.

Prime Infrastructure käyttää myös erilaisia portteja, joten mikäli tiettyä palvelua halutaan käyttää, tulee siihen kuuluva portti avata palomuurista. Ciscon Quick Start Guide listaa tarkemmin porttimäärittelyt. (Cisco Systems 2016a.)

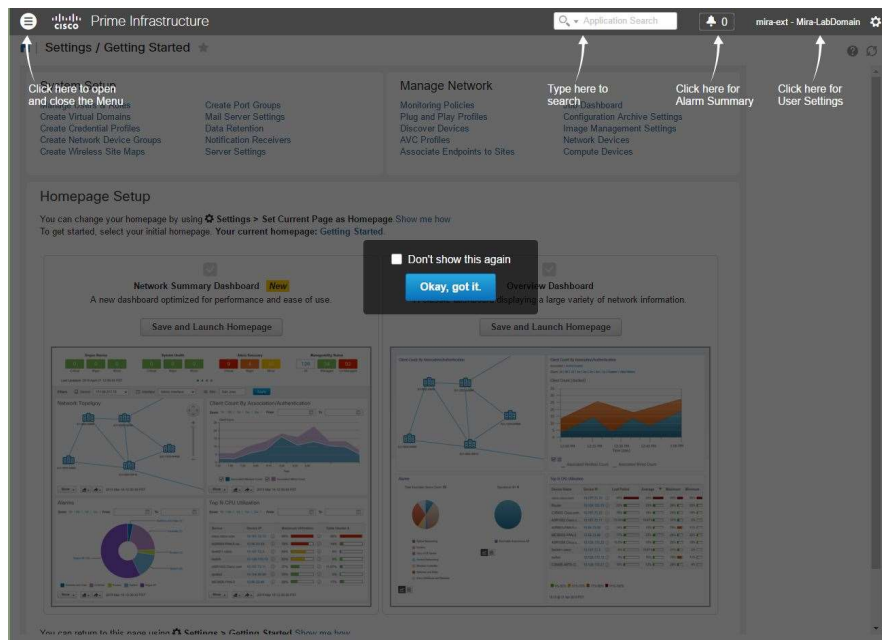
4.2 Selainohjelman käyttö

Prime Infrastructure -palveluun saa yhteyden kirjoittamalla asennusvaiheessa määritellyn IP-osoitteen selaimen osoiteriville (alun tulee olla muodossa "https://") eli testiympäristön tapauksessa osoite on https://172.22.2.89. Esiin avautuu kirjautumisnäky (Kuva 12). Kun Prime Infrastructure -palvelun osoitetta käytetään ensimmäistä kertaa, selain antaa varoituksen epäluotettavasta sivustosta. Jatkoa varten on hyvä luoda poikkeussääntö selaimen ja ladata sertifikaatti Prime Infrastructure -palvelimelta. Tämän jälkeen selain tunnistaa Prime Infrastructuren turvalliseksi sivustoksi, joten se sallii suoraan kirjautumisnäkyman lataamisen, ilman erillistä varoitusta.



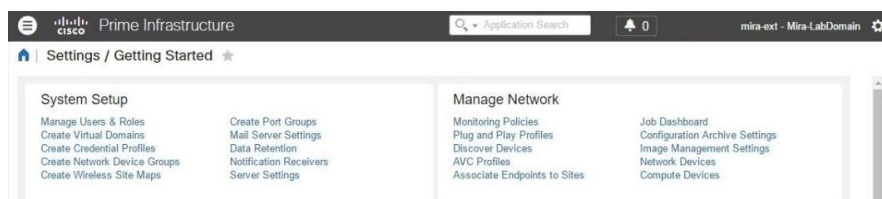
Kuva 12. Kirjautumisnäky selaimessa.

Ensimmäisellä kirjautumiskerralla näkymään syötetään asennusvaiheessa selainkäyttöliittymälle määritelty pääkäyttäjän root-tunnus ja salasana. Kirjautumisen jälkeen tulee näkymä, jossa ohjeistetaan saatavilla olevista ominaisuuksista (Kuva 13).



Kuva 13. Näkymä ensimmäisen kirjautumisen jälkeen.

Okay, got it -valinnan jälkeen käyttäjä näkee Getting Started -näytön. Tällöin yläosassa näkyvät selainohjelman valikkorakenne ja järjestelmäasetusten olennaisimmat linkit (Kuva 14).

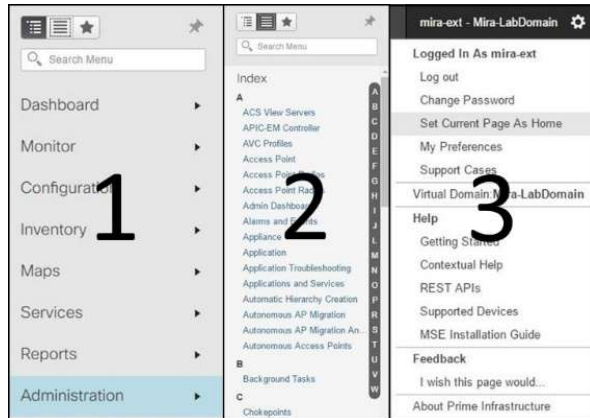


Kuva 14. Getting Started -näytön yläosa.

Näytön yläosassa vasemmalla on päävalikon kuvake, eli valkoinen ympyrä harmailla viivoilla. Prime Infrastructure -teksti vie ohjelman yleisnäkymään (Overview). Keskellä on hakukenttä ja sen oikealla puolella näkyvät mahdolliset hälytykset, jos niitä valvottavassa verkkoympäristössä ilmenee. Oikeassa reunassa näkyy käyttäjäasetukset-valikko, eli käyttäjätunnus (mira-ext), jolla Prime Infrastruktuuriin on kirjaututtu sekä virtuaaliverkotunnus (Mira-LabDomain).

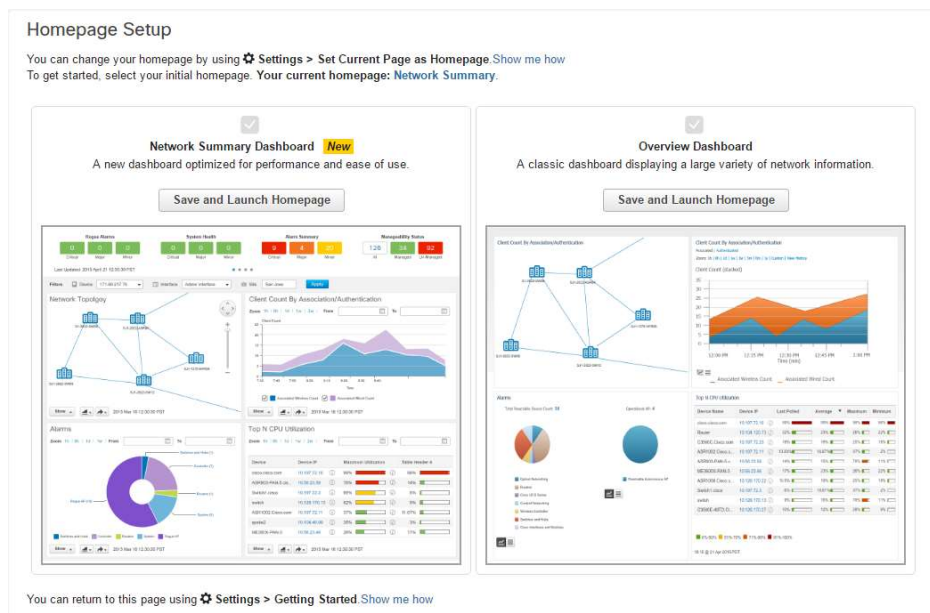
Kuvassa 15 näkyvät eroteltuna eri valikkorakenteet seuraavasti:

1. vasemman yläkulman päävalikko
2. aakkosjärjestyksessä oleva päävalikko
3. käyttäjäasetukset-valikon rakenne.



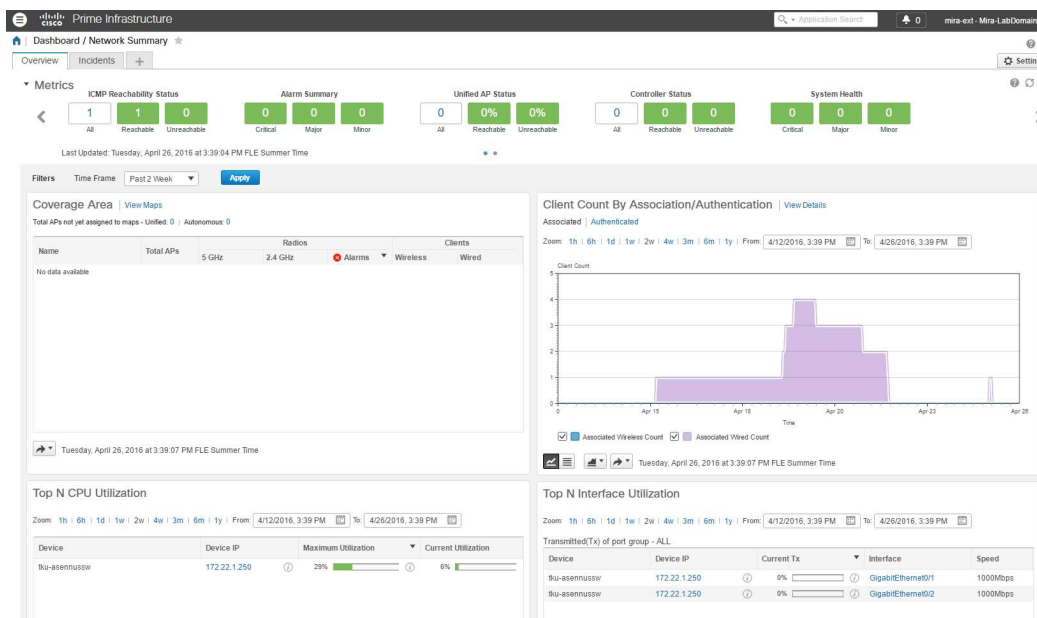
Kuva 15. Eri valikkorakenteet selainnäkyessä.

Ensimmäisellä käyttökerralla käyttäjä saa valita kahdesta eri vaihtoehdosta, millaisella Dashboard- eli käyttöliittymänäkymällä haluaa Prime Infrastructuraa käyttää (Kuva 16). Network Summary Dashboard on uusi vaihtoehto, kun Overview Dashboard puolestaan oli käytössä jo aiemmassa Prime Infrastructure 2.2 -versiossa.



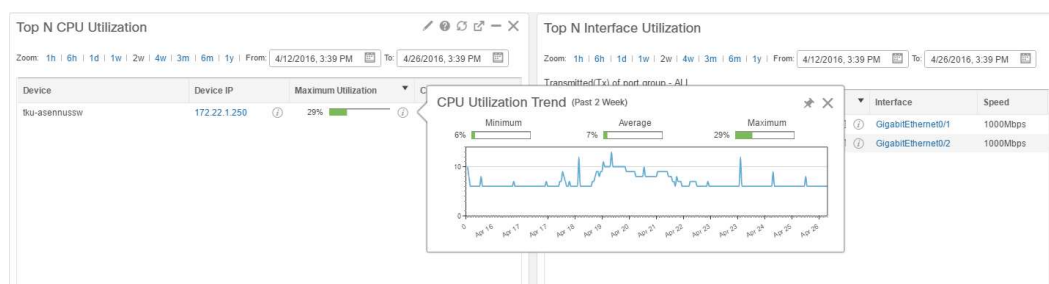
Kuva 16. Käyttöliittymänäkymän valinta.

Käyttöliittymän näkymä saattaa vaihdella sen mukaan, mikä oletusnäkymä on valittuna ja mitä valvontaruutuja (dashlets) näkymään on määritelty. Testiympäristöön valittiin uusi Network Summary Dashboard -näkymä (Kuva 17).



Kuva 17. Perusnäkymä testiympäristössä.

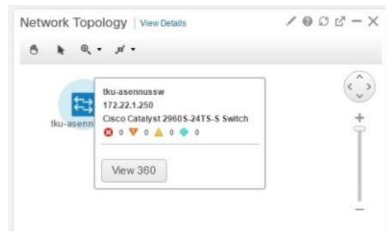
Perusnäkymässä on ympyröityjä i-kirjaimia, jotka näyttävät lisätietoja, kun hiiren kursorin siirtää kyseisen merkin päälle (Kuva 18).



Kuva 18. Info-näkymä prosessorikuormituksesta.

360°-näkymä

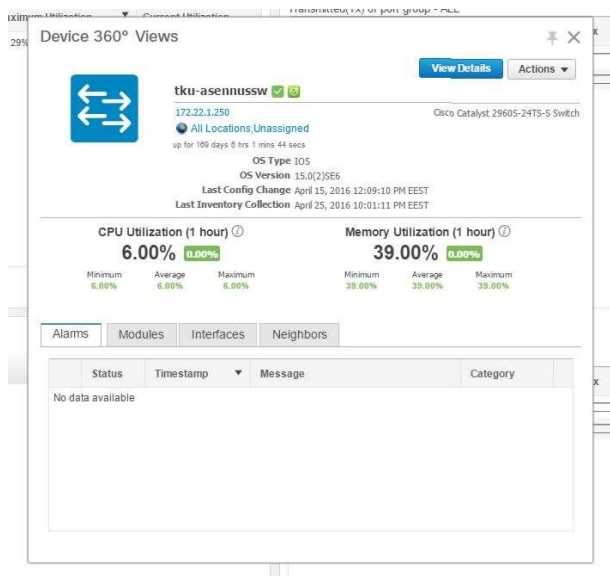
Prime Infrastructuressa on mahdollista tarkastella laitteen tietoja 360°-näkymästä. Tämä tapahtuu siten, että hiiren kursori siirretään laitteen päälle, jolloin esiin tulee joko suoraan 360°-näkymä tai vaihtoehtoisesti sen saa valittua erillisestä napista (Kuva 19).



Kuva 19. 360°-näkömän valinta verkkotopologia-näkymästä.

360°-näkömä näyttää laitteen tiedot tarkemmin erillisessä ponnahdusikkunassa (Kuva 20), eli käyttäjän ei tarvitse siirtyä eri sivuille laitteen tietojen tarkastelun takia. 360°-näkömä pitää sisällään seuraavat tiedot laitteesta:

- nimi
- malli
- IP-osoite
- sijainti, mikäli se on määritettynä
- käyttöjärjestelmätyyppi ja -versio
- konfiguroinnin viimeisin muutos aika
- prosessorin ja muistin kuormitus
- mahdolliset hälytykset
- laitteeseen kytketyt moduulit
- eri liitännät
- mahdolliset naapurit.



Kuva 20. 360°-näkömä testiympäristön kytkimestä.

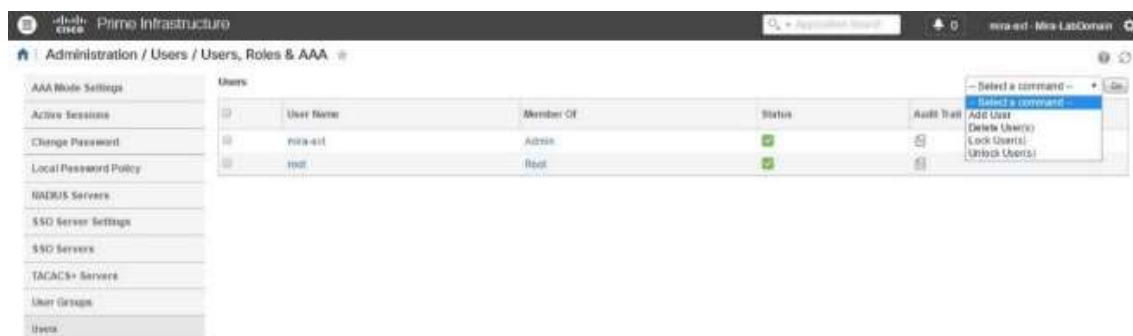
5 PRIME INFRASTRUCTUREN KÄYTTÖ

Testiympäristö asennettiin System Partners Oy:n tiloihin. Saatavilla oli valmiina VMware ESXi -palvelin, jossa oli riittävästi levytilaa ja muita tarvittavia resursseja, joten ei ollut erikseen tarvetta hankkia laitteistoa projektia varten. Testiympäristössä oli kytkettynä yksi Cisco Catalyst 2960S-24TS-S -kytkin. Ikävä kyllä kytkin oli kuitenkin myös muuten testausympäristön käytössä, joten siihen ei voinut juuri kohdistaa testaustoimia Prime Infrastructuren toimintojen osalta. Erilaisten häiriötilanteiden ja konfiguraatioiden muutosten testaukset jäivät siis lähinnä teorialtason pohdiskeluksi. Tässä luvussa hyödynnettiin pdf-muodossa olevaa Cisco Prime Infrastructure 3.0 User Guide -kirjaa (Cisco Systems 2015), josta oli apua eri toimintojen tutkimisessa.

5.1 Käyttäjätunnusten lisääminen

Prime Infrastructureen on suositeltavaa luoda eri käyttäjätunnukset ja jättää root-tunnus pääkäyttäjän rooliin. Käyttäjien lisääminen tapahtuu Administration > Users > Users, Roles & AAA -valikkopolun kautta.

Testiympäristöön lisättiin mira-ext-tunnus Admin-ryhmän oikeuksilla (Kuva 21).



Kuva 21. Käyttäjien hallintanäkymä.

Pudotusvalikosta valitaan Add user -vaihtoehto ja tämän jälkeen Go. Esiin tulee näkymä, jossa määritellään uusi käyttäjätunnus, salasana ja kyseisen käyttäjätunnuksen rooli tai roolit (Kuva 22).

Kuva 22. Uuden käyttäjätunnuksen luominen.

5.2 Laitteiden lisääminen

Laitteiden lisääminen Prime Infrastructuureen onnistuu useammalla eri tavalla:

- käyttämällä automatisoitua prosessia eli Discovery-toimintoa
- lisäämällä laitteet CSV-tiedoston (Comma-separated values) avulla, mikä nimensä mukaisesti pitää sisällään arvot, jotka ovat pilkuilla eroteltuna.
- lisäämällä laitteen tiedot, IP-osoite ja muut laitetiedot, manuaalisesti järjestelmään.

Discovery-toimintoa on suositeltavaa käyttää, mikäli verkossa on paljon laitteita. Jos käytössä puolestaan on jokin toinen verkonhallintatyökalu, jonka laitteet halutaan liittää Prime Infrastructuureen, onnistuu se CSV-tiedoston avulla. Yksittäisten laitteiden lisääminen onnistuu parhaiten manuaalisesti. Tästä syystä myös testiympäristön kytkin lisättiin Prime Infrastructuureen manuaalisesti.

Prime Infrastruktuuren laitteet löytyvät muun muassa Configuration > Network > Network Devices -näköymästä (Kuva 23).



Kuva 23. Laitenäkymä.

Langattomien laitteiden lisääminen Prime Infrastruktuureen onnistuu vastaavasti kuin langallistenkin.

Discovery-toiminto

Prime Infrastructure pitää sisällään Discovery-toiminnon, jolla saadaan automaattisesti lisättyä laitteita Prime Infrastruktuuren ympäristöön. Cisco suosittelee Discoveryn käyttöä, joten se löytyy heti Getting Started -aloitusnäköymästä.

Prime Infrastructure käyttää SNMP-kyselyjä (SNMP polling) verkkolaitteiden tietojen keräämiseen määritellyn IP-avaruuden sisällä. Mikäli verkkolaitteissa on CDP-palvelu (Cisco Discovery Protocol) otettuna käyttöön, Prime Infrastructure etsii sen avulla kyseisen verkon laitteet.

Verkkolaitteiden etsimisen voi suorittaa kahdella eri tavalla:

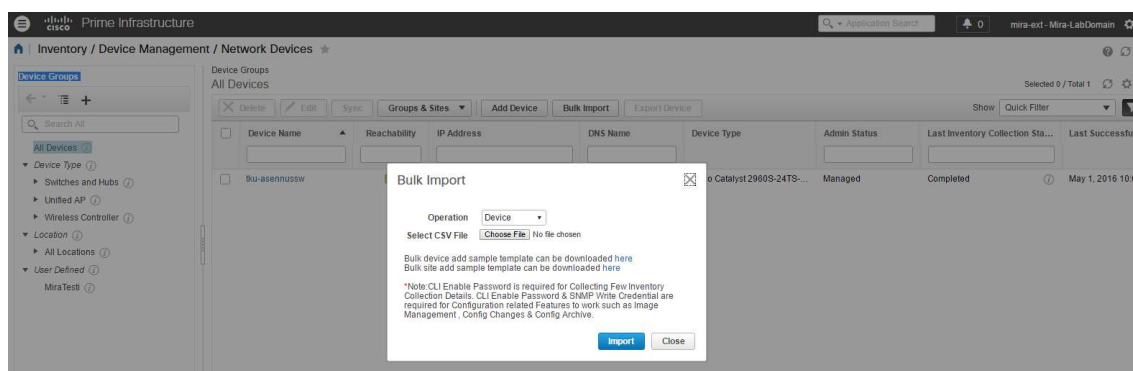
1. Konfiguroimalla etsintäasetukset manuaalisesti, mikä on suositeltavaa, jos halutaan tarkemmin määrittää asetukset ja ajaa etsintätoiminto tulevaisuudessa samoilla asetuksilla.
2. Ajamalla pikaetsintä eli Quick Discovery -toiminto, joka käy nopeasti läpi verkon ja käyttää SNMP-kyselyitä laitetietojen keräämiseen.

Discovery-prosessi hyödyntää ICMP Ping -toimintoa selvittääkseen verkkolaitteiden saatavuuden. Tämän jälkeen SNMP-tiedot varmistetaan. Mikäli laite vastaa Ping-toimintoon ja SNMP-tietojen tarkistus onnistuu, Discovery-prosessi suorittaa myös muita

toimintoja haun aikana. Mikäli prosessi kerää haun aikana tarvittavat tiedot, laitteet lisätään Inventory > Network Devices -näkymään.

CSV-tiedoston parametrit

CSV-tiedostoa hyödynnetään, kun halutaan liittää laitteita toisesta lähteestä Prime Infrastructuuren piiriin. Lisäys onnistuu avaamalla Inventory > Device Management > Network Devices -näkymä ja valitsemalla Bulk Import (Kuva 24).



Kuva 24. CSV-tiedoston tuominen Prime Infrastructuureen.

Tiedoston tulee pitää sisällään seuraavat laitetiedot:

- laitteen IP-osoite
- SNMP-versio
- SNMP read-only community -asetukset
- SNMP write community -asetukset
- SNMP retry -arvo
- SNMP aikakatkaisun arvo.

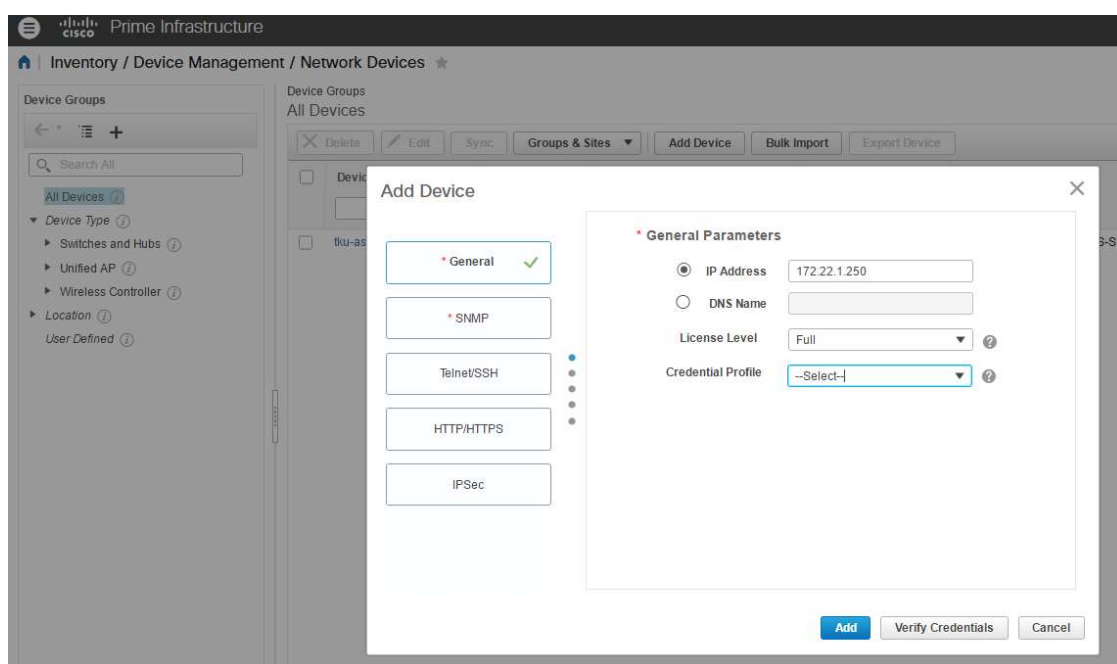
Edellä olevilla tiedoilla saa suoritettua osittaisen laitehaun. Lisäämällä CSV-tiedostoon myös seuraavat tiedot, saa suoritettua täydellisen haun.

- Protokolla
- CLI-käyttäjätunnus
- CLI-salasana
- CLI enable -salasana
- CLI aikakatkaisun arvo.

Prime Infrastructure tarjoaa malliesimerkin, jota verkon hallinnasta vastaavat voivat hyödyntää oman CSV-tiedoston luomiseen.

Laitteen manuaalinen lisääminen

Laitteen manuaalinen lisääminen onnistuu valitsemalla Inventory > Device Management > Network Devices -näköymästä Add Device -toiminto ja täyttämällä tarvittavat kentät (Kuva 25).



Kuva 25. Laitteen lisääminen.

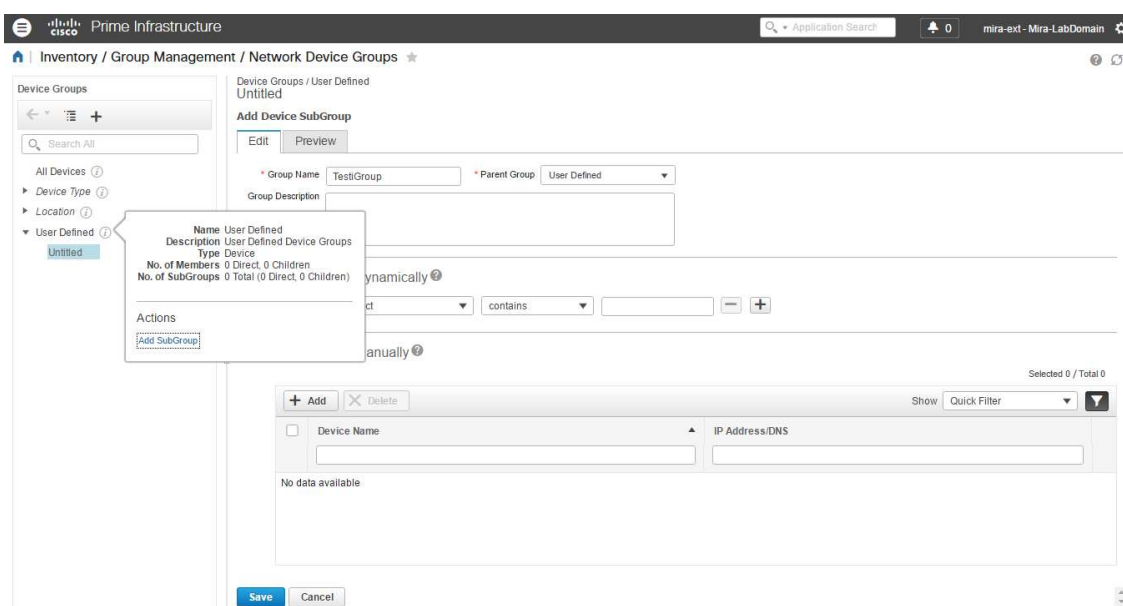
License Level -kentästä valitaan joko Full- tai Switch Port Trace Only -vaihtoehto. Full kerää kaikki laitetiedot ja sallii Prime Infrastrukturen hallinnoida laitetta. Switch Port Trace Only -vaihtoehto kerää vain osittaiset laitetiedot eli isännän nimen, laitteen nimen, laitetypin ja tavoitettavuuden tilan, ja sallii Prime Infrastrukturen näyttää, miten laite on liitetty verkkoon.

5.3 Laitteiden ryhmittely

Lisätyt laitteet kannattaa ryhmitellä loogisiin ryhmiin hallinnan, ylläpidon ja konfiguroinnin helpottamiseksi. Ryhmittelyn avulla voi suorittaa toimintoja koko ryhmän laitteille, eikä vain yksittäiselle laitteelle. Laiteryhmiä voi olla kolmea erilaista:

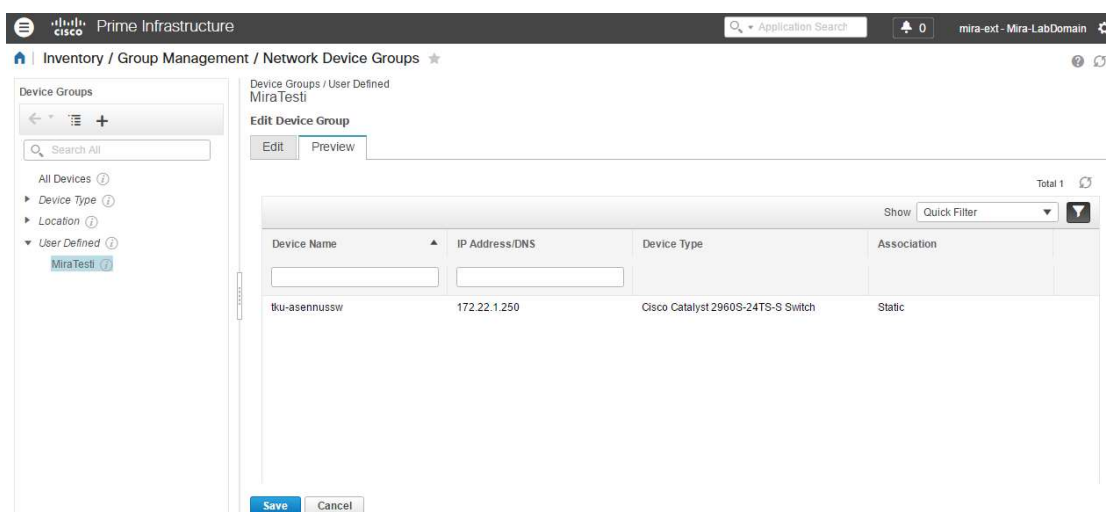
- Staattinen (Static). Luo ja nimeää uuden laiteryhmän, johon voi lisätä laitteita käyttämällä Add to Group -toimintoa.
- Dynaaminen (Dynamic). Luo ja nimeää uuden laiteryhmän sekä määrittelee säännöt, jotka laitteiden tulee täyttää, ennen kuin ne voidaan lisätä kyseiseen ryhmään. Dynaamiseen ryhmään ei siis lisätä erikseen laitteita vaan Prime Infrastructure lisää ne automaattisesti, kun määritellyt ehdot täyttyvät.
- Sekoitettu (Mixed). Luo ja nimeää uuden laiteryhmän, johon voi lisätä laitteita manuaalisesti ja määritellä erikseen säännöt, joiden tulee täytyä ennen laitteen lisäämistä kyseiseen ryhmään.

Laiteryhmän saa luotua joko Inventory > Device Management > Network Devices tai Inventory > Group Management > Network Device Groups -näkymistä. Uuden ryhmän luominen onnistuu Device Group -näkymän kautta, siirtämällä hiiren kursori vasemmalla listauksessa olevan User Defined -vaihtoehdon vieressä olevan ympyröidyn i:n päälle ja valitsemalla esiin tulevasta ikkunasta Add SubGroup (Kuva 26).



Kuva 26. Ryhmän lisääminen.

Ryhmälle annetaan ensin nimi ja valitaan Parent Group -valikosta sopiva vaihtoehto, jos on tarvetta. Ryhmälle voi määritellä myös kuvauksen, mutta se ei ole pakollista. Nimeämisen ja kuvauskentän tekstin suhteen tulee huomioida, että Prime Infrastructure ei salli skandinaavisten merkkien käyttöä, eli å-, ä- ja ö-kirjaimia ei voi käyttää. Laitteet voi lisätä luotavaan ryhmään käyttämällä Add Device Manually -valintaa, eli laitteen nimi ja IP-osoite lisätään ryhmään manuaalisesti. Vaihtoehtoisesti tai manuaalisen lisäyksen rinnalla voi käyttää Add Device Dynamically -valintaa, eli määritellään ensin säännöt, jotka tulee täyttyä ennen kuin laitteen voi liittää kyseiseen ryhmään. Ryhmän lisäys -sivulla näkyy Preview-välilehti, josta pystyy tarkistamaan määriteltyjen sääntöjen mukaan automaattisesti lisätyt laitteet sekä myös manuaalisesti lisätyt laitteet. Lisätyt ryhmät tulevat näkyviin User Defined -kansioon (Kuva 27).



Kuva 27. Lisätty ryhmä.

5.4 Verkon valvonta-asetusten määrittely

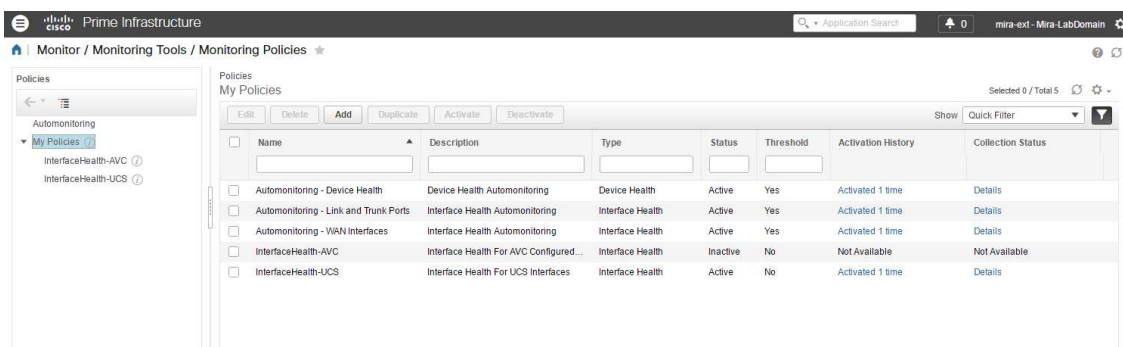
Laitteiden lisäysten ja ryhmittelyn jälkeen luodaan valvontaa varten eri mallipohjat, esimerkiksi:

- prosessorin-, muistin- ja käyttöliittymän kuormitukselle
- verkon suorituskyvyn (QoS) valvonnalle
- VPN-tunnelien statistiikalle.

Valvontakäytäntöjen luonnin ja käyttöönoton jälkeen, Prime Infrastructure kerää tiedot laitteista ja näyttää ne käyttöliittymässä, yksittäisissä dashleteissa ja raporteissa.

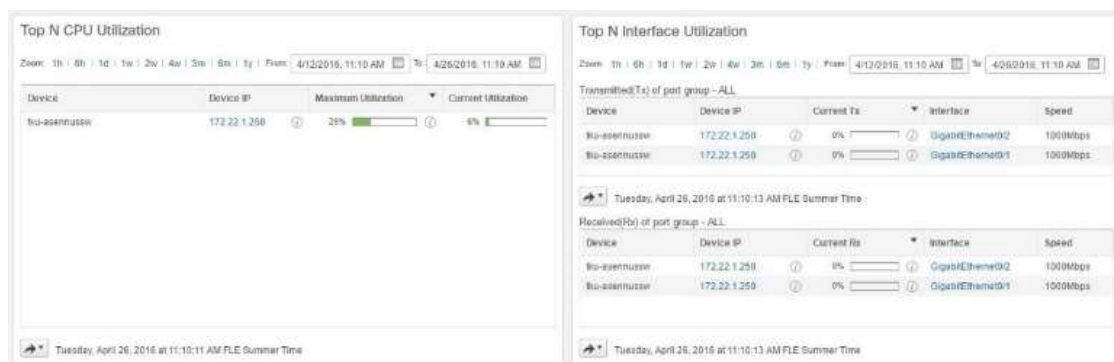
Valvontakäytännöt

Prime Infrastructuressa on oletuksena valmiina myös muutamia valvontamalleja verkon ja sen laitteiden valvontaa varten, muun muassa laitteen kunnon ja liitäntöjen kuormituksen valvonnalle (Kuva 28).



Kuva 28. Valmiit mallipohjat valvontaa varten.

Kytkin liitettiin testiympäristöön manuaalisesti, eikä sille erikseen määritelty ryhmiä tai valvontakäytäntöjä. Prime Infrastructure lisäsi sen kuitenkin automaattisesti muun muassa prosessorin ja liitäntöjen kuormitusten valvonnan piiriin, eli etusivun dashletit näyttivät automaattisesti kytkimestä kerättyjä tietoja (Kuva 29).



Kuva 29. Kytkimen valvonta-dashletit.

Valvontakäytännön lisäys tapahtuu Monitoring > Monitoring Tools > Monitoring Policies -näkökulman kautta, Add-nappia painamalla (Kuva 30).

Prime Infrastructure

Monitor / Monitoring Tools / Monitoring Policies

Policy Types

Traffic Analysis

Device Selection

Name

Description

Author mira-ext

Contact

Feature Category Threshold

Parameters and Thresholds

Parameter Condition Reaction

Please input Metric selection to view Threshold parameters.

Save and Activate Cancel

Kuva 30. Valvontakäytännön lisäys.

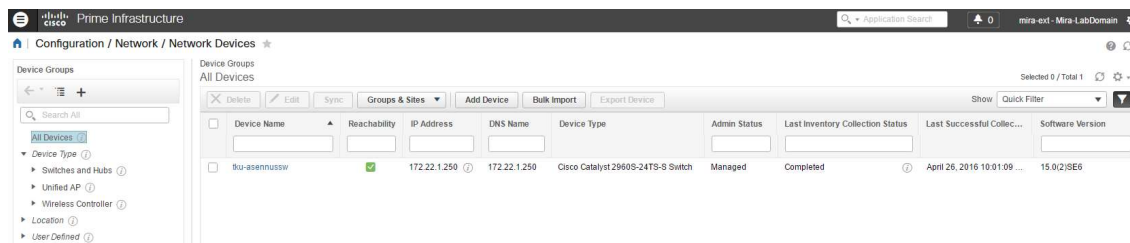
Valvontakäytännöille löytyy eri vaihtoehtoja:

- Traffic Analysis: verkkoliikenteen analysointi
- Application Response Time: sovellusten vasteaikojen valvonta
- Voice Video Data: ääni-, video- ja data-liikenteiden valvonta
- Interface Health: liitännöjen tilan valvonta
- Device Health: laitteen tilan valvonta
- GETVPN (Group Encrypted Transport VPN) Poller: Ciscon GETVPN-kyselyiden valvonta
- Wireless Controller: langattomien verkkojen hallintalaitteen valvonta
- DMVPN (Dynamic Multipoint VPN): skaalautuvien IPsec VPN -yhteyksien valvonta
- WirelessAP (Wireless Access Point): langattomien tukiasemien valvonta
- Custom MIB (Management Information Base) Polling: mukautettujen MIB-kyselyiden valvonta
- NAM (Network Analysis Module) Health: verkon analysointimoduulin tilan valvonta.

Testiympäristön pitäessä sisällään vain Prime Infrastructure -palvelimen ja yhden kytkimen hyvin rajoitetulla hallintaoikeudella, eri valvontatilojen testaaminen ei ollut käytännössä mahdollista.

5.5 Verkkolaitteiden konfigurointi

Verkkolaitteiden konfigurointi onnistuu Configuration > Network > Network Devices -näkökymästä, joka listaa Prime Infrastructuureen liitetyt laitteet. Listauksesta näkee muun muassa laitteen nimen, toimii linkkinä kyseisen laitteen tarkempiin tietoihin, laitteen tavoitettavuuden (Reachability), IP- ja DNS-osoitteen ja tyyppin (Kuva 31).



Kuva 31. Network Devices -näkökymä

Network Devices -sivulta pääsee tekemään seuraavia toimia:

- Laitteiden hallinta. Uusien lisäys, vanhojen muokkaus tai poisto, Export Device -toiminnon käyttö, laitteiden poisto ryhmistä ja sijainneista
- Laitteiden perustietojen ja tilan tarkistus. IP-osoite, laitetyyppi, tietojen keräilytila
- Laiteryhmien hallinta. Prime Infrastructure lisää laitteet oletusryhmiin niiden tyyppin mukaan. Ylläpitäjä voi itse luoda uusia ryhmiä myös tätä kautta
- Laitteiden lisäys eri sijaintiryhmiin
- Laitteen tarkempien tietojen tarkistus. Muistin, porttien, ympäristön ja liitäntöjen tarkempi näkökymä
- Laitteiden konfigurointi. Laitteen eri toimintojen muokkaus
- Laitteen konfiguroinnin arkistointi ja tarvittaessa myös palautus. Konfiguroinnin automatisoidun arkistoinnin saa ajastettua tätä kautta
- Ohjelmistoversion tarkistus. Ohjelmistoversion päivitys ja mahdollisesti myös jakelu muille laitteille onnistuu tätä kautta
- Liitäntöjen tietojen tarkistus
- TrustSec-konfiguroinnin tarkistus, mikäli laite sitä tukee.

Laitteiden konfigurointia ei pystytty käytännössä testaamaan, joten tämä osio koostuu lähinnä teoreettisista mahdollisuuksista.

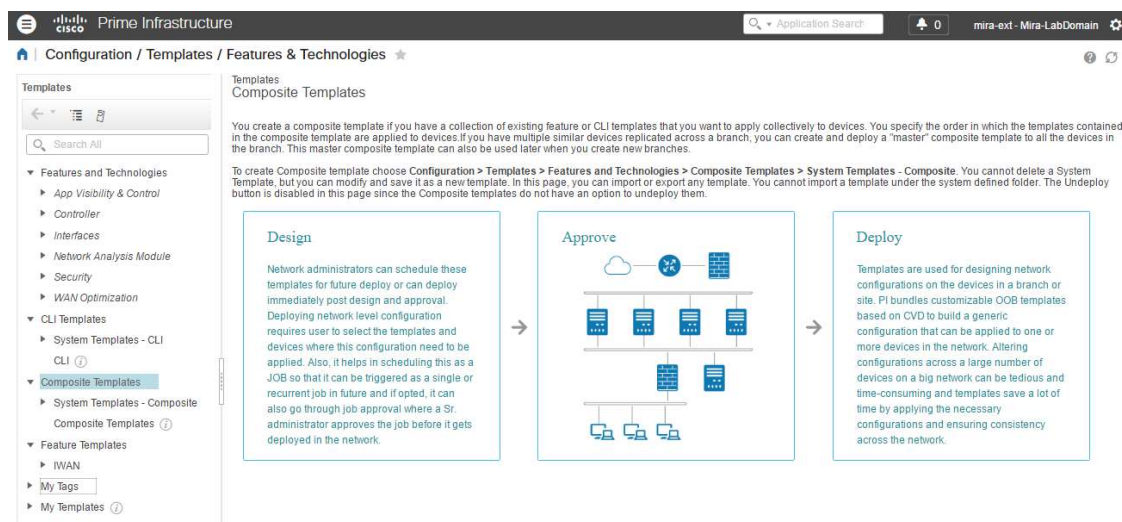
Mallipohjien käyttö laitteiden konfiguroinnissa

Konfigurointien mallipohjat helpottavat ylläpitäjien työkuormaa, mikäli konfiguroitavana on useampia samanlaisia laitteita, samanlaisella käyttökohteella. Ennen mallipohjien käyttöönottoa tulee miettiä esimerkiksi seuraavia seikkoja:

- Minkä kokoinen verkkoympäristö on kyseessä?
- Millaista laite- ja palvelukirjoa tuetaan?
- Montako verkkosuunnittelijaa yrityksellä on?

Mikäli verkko on pieni, suunnittelijoita vain yksi tai kaksi ja laitteet ovat pääasiassa samanlaisia, kannattaa mallipohjan luonti aloittaa hyväksi todettujen CLI-konfiguraatioiden kopioinnista ja luoda konfiguraatio- ja valvontamallit niiden avulla. Jos taas käytössä on iso verkko usealla erilaisella laitteella, kannattaa yrittää tunnistaa ne konfiguraatiot ja asetukset, jotka voidaan ottaa yleisemmin käyttöön. (Cisco Systems 2015.)

Prime Infrastructure tarjoaa eri vaihtoehtoja konfiguraatiomallipohjien luomiseen. Mallipohjan saa luotua ominaisuuksien ja teknologioiden mukaan Configuration > Templates > Features and Technologies -näkyvästä (Kuva 32).



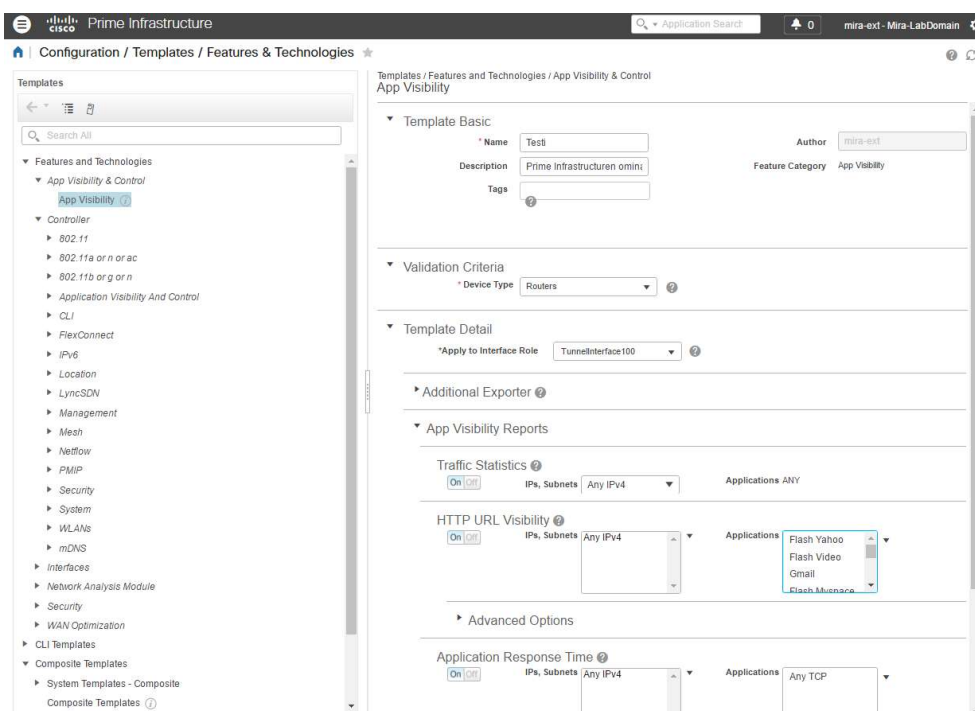
Kuva 32. Features & Technologies -näkymä.

Features & Technologies -näkymän vasemmasta reunasta valitaan mallipohja, jollainen halutaan luoda:

- Features and Technologies: koskee jotain tiettyä ominaisuutta tai teknologiaa laitteen konfiguraatiossa, esimerkiksi hallintalaitetta, liitäntöjä tai turvallisuutta.
- CLI Template: käyttäjän määrittelemä mallipohja, joka perustuu käyttäjän omiin parametreihin. Prime Infrastructure tarjoaa muuttujia, jotka käyttäjä määrittää haluamikseen arvoiksi. Mallipohjia voi myös tuoda Cisco Prime LAN Management -työkalusta.
- Composite Templates: yhdistelmä eri mallipohjista. Kaksi tai enemmän ominaisuutta tai vaihtoehtoisesti useampi CLI-malli ryhmitelty yhdeksi mallipohjaksi. Käyttäjä määrittelee, missä järjestyksessä yhdistetyn mallipohjan eri mallit ladataan laitteisiin.

Features and Technologies -mallit

Erilaisia ominaisuuksiin ja teknologioihin liittyviä malleja löytyy paljon, joten ylläpitäjillä on useita valmiita vaihtoehtoja, joista lähteä eri ominaisuuksia määrittämään. App Visibility -vaihtoehdon avulla luotiin Testi-niminen mallipohja, joka koskee reitittimiä ja niiden TunnelInterface100-liitäntää (Kuva 33). Käyttöön otettaessa kyseinen malli valvoisi IPv4-verkkoliikennettä kaikkien sovellusten osalta. Tällaisen mallipohjan luominen ja käyttöönotto ei ole oikeassa verkkoympäristössä kovin hyödyllistä, vaan sitä kannattaisi tämentää tarpeen mukaan.

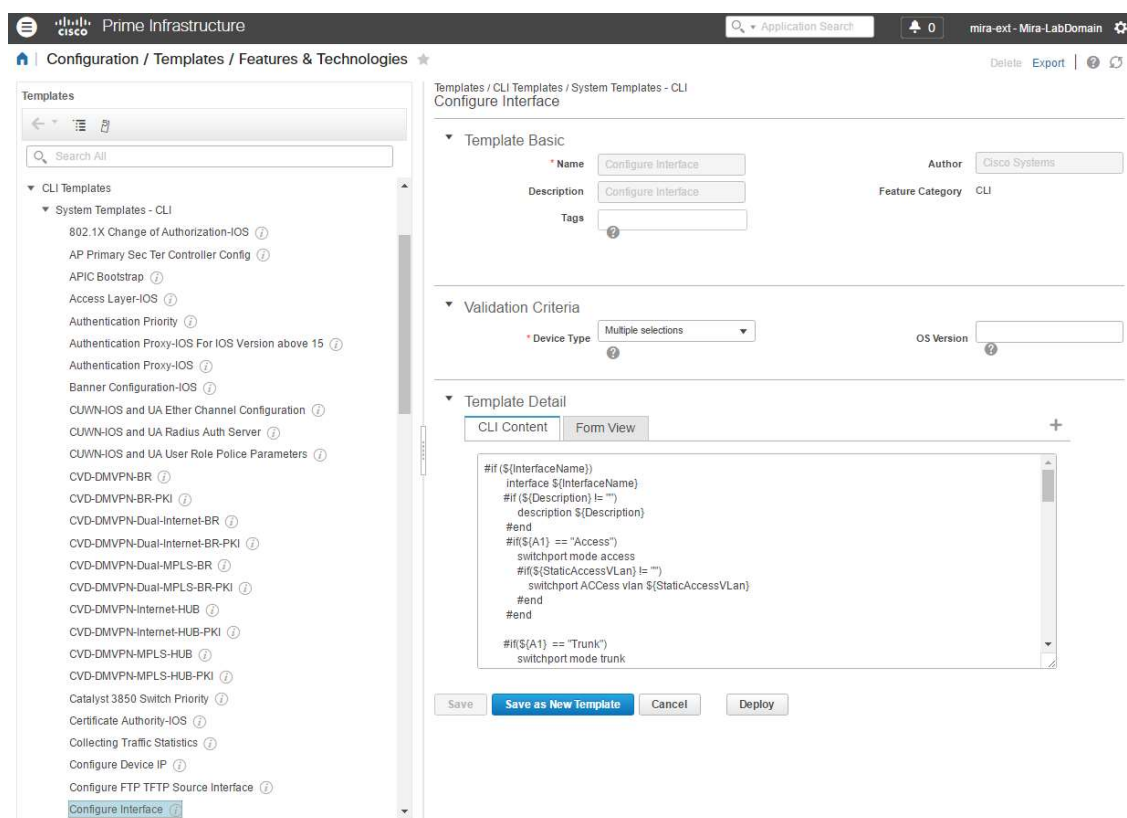


Kuva 33. App Visibility -mallipohjan luominen.

CLI-mallit

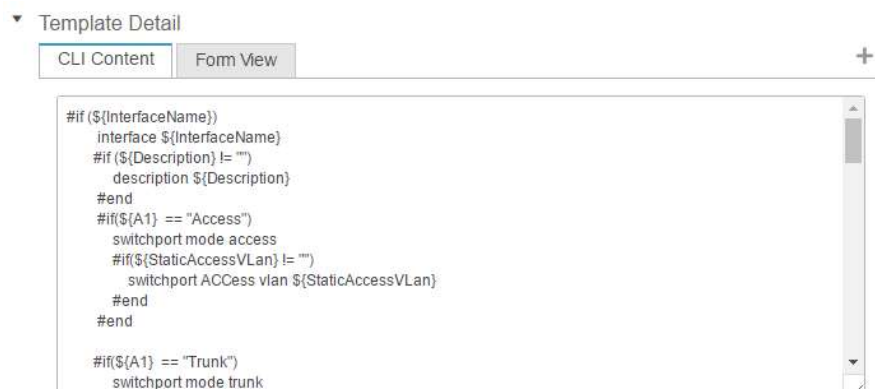
Prime Infrastructuresta löytyy useita valmiita CLI-mallipohjia, esimerkiksi laitteen IP-osoitteen, liitännöiden, salasanojen ja monien muiden ominaisuuksien määrittelyyn. Mallien nimet ovat pääsääntöisesti lukittu, eli käyttäjä ei pääse niitä erikseen nimeämään. Lisäksi mallipohjan tekijäksi on usein määritelty joko root tai Cisco Systems, toisin kuin esimerkiksi App Visibility -pohjassa, jossa käyttäjä määriteltiin automaattisesti mallin tekijäksi.

Configure Interface -mallipohjassa nimeä ja kuvausta ei voi muokata, mutta käyttäjä voi määrittellä erikseen tunnisteen, jonka perusteella mallipohjat ryhmitellään (Kuva 34). Seuraavaksi tulee valita, mitä laitteita tai laiteryhmiä luotava pohja tulee koskemaan. Ohjelmistoversio voidaan myös määrittää erikseen; mikäli kenttä jätetään tyhjäksi, mallipohjaa käytetään kaikilla ohjelmistoversioilla, jos kenttään taas syötetään esimerkiksi versio numero 15.3, kaikki laitteet, joissa on vanhempi ohjelmistoversio, suodatetaan pois, eikä mallia käytetä niihin.



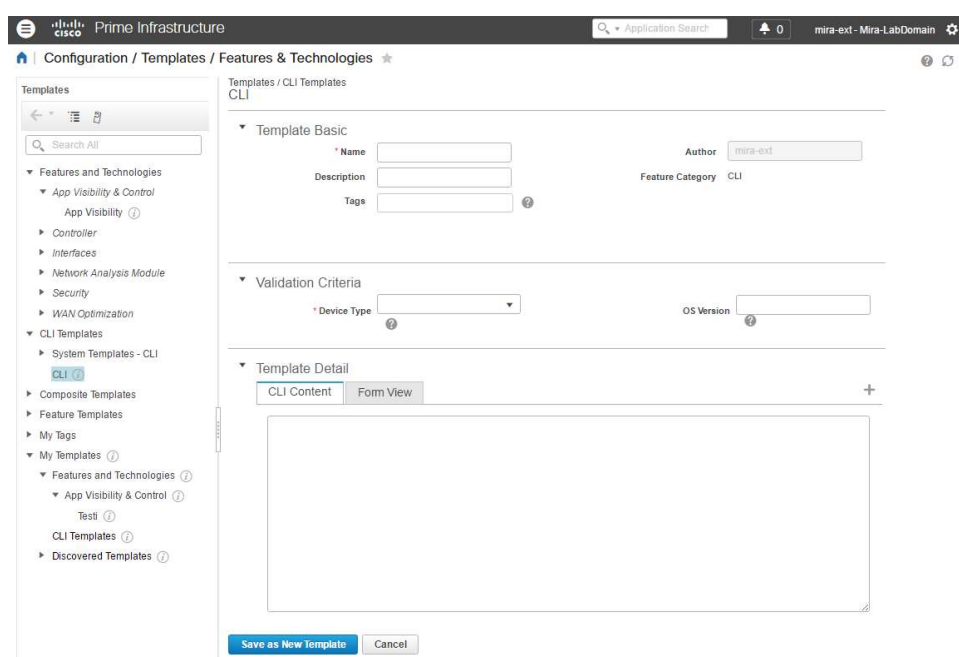
Kuva 34. Configure Interface -mallipohja.

CLI Content -kenttään määritellään halutut asetukset (Kuva 35). Jotta CLI Content -kenttää ymmärtää, tulee käyttäjän hallita CLI-komennot sekä lisäksi ymmärtää jonkin verran ohjelmoinnin käsitteitä.



Kuva 35. Configure Interface -mallipohjan CLI-sisältö.

CLI-pohja on mahdollista luoda myös täysin tyhjästä. CLI Templates -listauksen alta löytyy System Templates - CLI -valikko, josta löytyvät kaikki valmiit mallipohjat, mutta viimeisenä on nähtävissä pelkkä CLI-valinta info-merkkeineen. Tämän kautta saa valittua New-vaihtoehdon, uuden pohjan luomista varten. Esiin tulee tyhjä pohja, johon käyttäjä saa itse määritellä halutut laitteet, ohjelmistoversiot ja CLI-komentojen sisällön (Kuva 36).



Kuva 36. Tyhjä CLI-pohja.

Aiemmin listattujen mallipohjien lisäksi Prime Infrastructuren avulla saa luotua muun muassa langattomille laitteille, pääsilystoille ja erilaisille turvallisuusasetuksille omat mallipohjat.

5.6 Vianmääritys ja ongelmanratkaisu

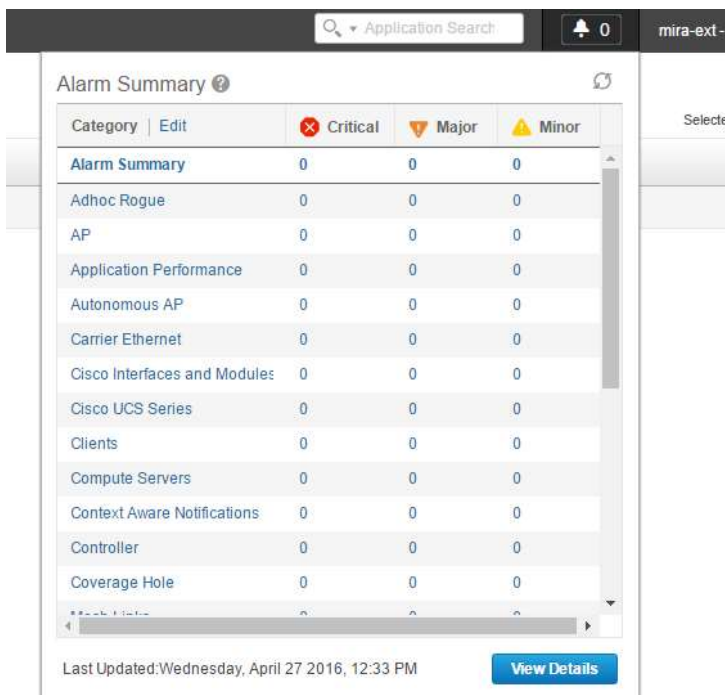
Prime Infrastructure tarjoaa verkkojen ylläpitäjille työkaluja, joilla voi olla suoraan yhteydessä Ciscon asiantuntijoihin vian diagnosoinnin ja ongelmanratkaisun osalta. Yksi tapa vian selvitykseen on avata yhteys Ciscon tukifoorumille, josta voi etsiä apua ongelmiin. Tämä tapahtuu valitsemalla yksi hälytyslistauksen riveistä (Monitor > Monitoring Tools > Alarms & Events) ja valitsemalla Troubleshoot > Support Forum. Tämän toiminnon käyttö vaatii Cisco.com-tunnuksen.

Toinen vaihtoehto on avata tukipyynnö Ciscon asiantuntijoille suoraan Prime Infrastructuren kautta. Prime Infrastructure kerää tällöin asiaan kuuluvat tiedot ja liittää ne tukitapaukseen. Tukipyynnön avaaminen tapahtuu valitsemalla Monitor > Monitoring Tools > Alarms & Events -näkymä. Tämän jälkeen hiiren kursori siirretään sen laitteen IP-osoitteen päälle, missä hälytys on tapahtunut. Esiin pitäisi tulla laitteen 360°-näkymä ja Actions-pudotusvalikko, josta saa valittua Support Request. Tämän jälkeen syötetään Cisco.com-tunnus. Esiin tulee Update or Create a Support Case -ikkuna, josta saa avattua Create-valinnan avulla uuden tukipyynnön.

Vianmääritystä ei pystytty käytännössä testaamaan ollenkaan, joten tämä osio koostuu lähinnä teoreettisista mahdollisuuksista.

Alarms-näkymä

Alarms- eli hälytyslistauksesta näkee, mikäli jossain tietyssä verkko-osiossa, -alueessa, -ohjelmassa tai -laitteessa on ongelmia. Prime Infrastructuren etusivulle saa näkyviin Alarm Summary -listauksen, josta pystyy nopeasti tarkistamaan, onko verkon suhteen ongelmia (Kuva 37).



Application Search [] 0 mira-ext-

Alarm Summary ?

Category Edit	Critical	Major	Minor
Alarm Summary	0	0	0
Adhoc Rogue	0	0	0
AP	0	0	0
Application Performance	0	0	0
Autonomous AP	0	0	0
Carrier Ethernet	0	0	0
Cisco Interfaces and Modules	0	0	0
Cisco UCS Series	0	0	0
Clients	0	0	0
Compute Servers	0	0	0
Context Aware Notifications	0	0	0
Controller	0	0	0
Coverage Hole	0	0	0

Last Updated: Wednesday, April 27 2016, 12:33 PM View Details

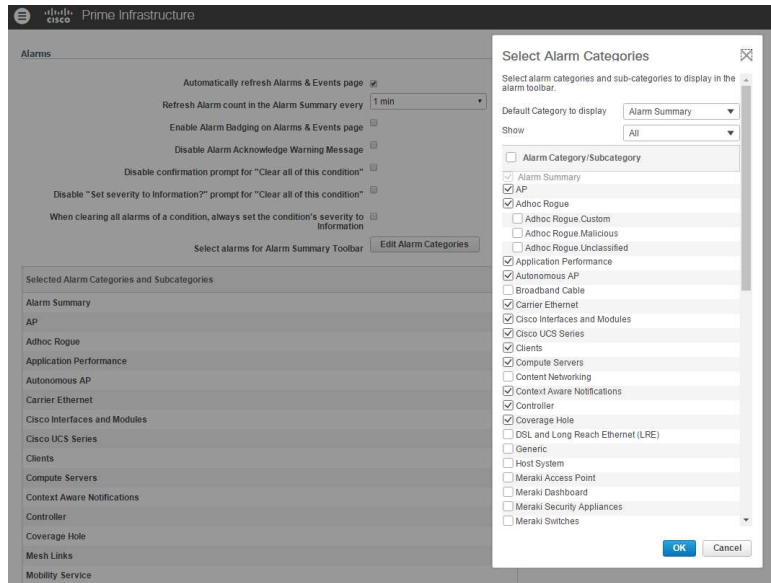
Kuva 37. Alarm Summary -näkymä.

Alarm Summary -näkymää pystyy muokkaamaan yrityksen käyttötarpeiden mukaan. Muokkaus onnistuu siirtämällä hiiren kursori Alarm Summary -tekstin vieressä olevan kysymysmerkin päälle ja valitsemalla esiin tulevasta näkymästä My Preferences (Kuva 38).



Kuva 38. My Preferences -valinta.

Esiin avautuu Settings > My Preferences -sivu, josta pääsee muokkaamaan käyttäjätileskohtaisia asetuksia. Hälytysten osalta pystyy muokkaamaan muun muassa, miten usein hälytyslistaus päivitetään, oletus on minuutin välein, ja mitä hälytyksiä näytetään etusivulla (Kuva 39).

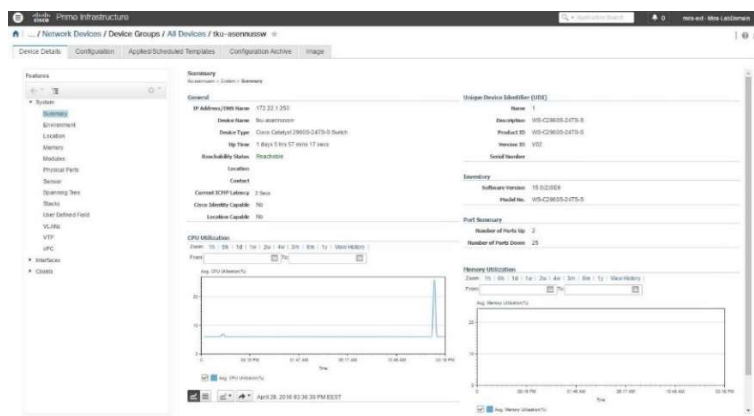


Kuva 39. Hälytysasetusten muokkaus.

Alarm Summary on etusivun oletusnäkyvä, mutta sen tilalle saa valittua myös muita, tarkemmin määriteltyjä vaihtoehtoja. Asetuksista löytyy reilusti yli viisikymmentä eri kategoriavaihtoehtoa, joten hälytysten valvonta on suunniteltu hyvin kattavaksi (Kuva 38). Näitä ei ikävä kyllä päästy testaamaan käytännössä testiympäristön rajoituksista johtuen.

Laitteisto- tai ohjelmistovikojen tutkiminen

Network Devices -näytteen kautta pystyy tarkistamaan eri verkkolaitteiden tilan. Näytelmästä saa valittua tietyn laitteen tiedot tarkemman tarkastelun kohteeksi (Kuva 40).



Kuva 40. Testikytkimen laitetiedot.

Välilehtien sisällöt ovat:

- Device Details: näyttää laitteen yleiskatsauksen.
- Configuration: eri liitäntä- ja turvallisuusasetusten määrittely.
- Configuration Archive: saa tarvittaessa valittua Schedule Rollback -vaihtoehdon, mikäli ongelma on ohjelmisto- tai konfiguraatiopuolella ja on tarvetta palata aiempaan versioon takaisin. Täältä saa myös ajastettua konfiguroinnin arkistoinnin.
- Image: Näyttää asennetun ohjelmistopakettin ja listaa muita suositeltavia ohjelmistopaketteja. Prime Infrastructure kerää nämä sekä paikallisesta että Cisco.com-kannoista. Tätä kautta pystyy tuomaan tai jakelemaan valitun ohjelmistopakettin.

6 YHTEENVETO

Projektin tavoitteena oli tutkia System Partners Oy:n mahdollisuutta hyödyntää Prime Infrastructure -verkonhallintaohjelmistoa omassa konesalissaan. Aikataulullisten haasteiden vuoksi projekti toteutettiin jossain määrin suppeammin, kuin mitä alun perin oli tarkoituksena.

Ohjelmiston testaus suoritettiin toimeksiantajan tarjoamassa testiympäristössä, jossa oli virtuaalipalvelin ja yksi kytkin. Prime Infrastructure asennettiin palvelimelle ja kytkin liitettiin sen hallinnan ja valvonnan piiriin. Asennus- ja käyttöönottoprosessit dokumentoitiin opinnäytetyöhön.

Prime Infrastructureen perehtyminen varmisti melko nopeasti käsityksen sen laajuudesta. Ohjelma on suunniteltu hyvin isoille ja monimutkaisille verkkoratkaisuille, vaikka sillä pystyy luonnollisesti hallitsemaan ja valvomaan myös pienempiä verkkoympäristöjä. System Partners Oy:n konesali ei ole tällä hetkellä laitteistomäärältään kovin iso, mutta mahdollisesta konesalin laajennuksesta ei siis tule aiheutumaan ongelmia ainakaan Prime Infrastruktuuren puolesta.

Eri toimintojen testaus jäi lähinnä teoreettiselle tasolle aikataulullisten haasteiden ja testiympäristön rajoitusten vuoksi. Kytkimen konfiguraatioon ei ollut pääsyä, koska se oli yrityksen muiden työntekijöiden testikäytössä. Tämä rajoitti hyvin paljon käytännön testausta; vianmäärittystä ja häilytyksiä ei saatu testattua, eikä myöskään ohjelmiston palautusta, konfigurointia tai muuttamista erilaisilla mallipohjilla voitu kokeilla.

Prime Infrastructure tukee laitteiden konfiguroinnin automatisointia, mutta se vaatii melko paljon ennakotyöstöä konfigurointimallien tallennusten osalta, jotta automatisointitoiminnot saadaan otettua käyttöön. Verkkolaitteiden valvonnat toimivat oletuksena kohtalaisesti, mutta niiden säätäminen on myös tarpeellista yrityskohtaisesti. Mahdollisten laitevikojen sattuessa nopea korjaus onnistuu myös, mutta sekin vaatii jonkin verran työstöä, jotta laiteprofiilit ja -konfiguroinnit ovat ajantasaisesti tallennettuna järjestelmään. Kunhan tiedot ovat saatavilla, uuden laitteen käyttöönotto vanhan laitteen konfiguraatiolla pitäisi onnistua melko helposti.

Jotta Prime Infrastruktuuren todelliset hyödyt saataisiin selvitettyä, tulisi sitä testata joko enemmän laitteita sisältävässä testiympäristössä tai kokeilla aidossa verkkoympäristössä.

LÄHTEET

Cisco Systems 2007. Performance Management: Best Practices White Paper. Viitattu 18.4.2016. <http://www.cisco.com/c/en/us/support/docs/availability/high-availability/15115-perfmgmt.pdf>

Cisco Systems 2012. Internetworking Technology Handbook. Viitattu 12.4.2016. http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook

Cisco Systems 2015. Cisco Prime Infrastructure 3.0 User Guide. Viitattu 20.4.2016. http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/user/guide/pi_ug.pdf

Cisco Systems 2016a. Cisco Prime Infrastructure 3.0 Quick Start Guide. Viitattu 20.4.2016. http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/quickstart/guide/cpi_qsg.pdf

Cisco Systems 2016b. Cisco Prime Infrastructure 3.0 Administrator Guide. Viitattu 23.4.2016. http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/administrator/guide/PIAdminBook.pdf

Cisco Systems. What Is Network Security? Viitattu 18.4.2016. http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html

Posey, B. 2008. Ten steps for network documentation: Channel checklist. Viitattu 15.4.2016. <http://searchitchannel.techtarget.com/feature/Channel-Checklist-10-steps-for-network-documentation>

Suomi Sanakirja 2015. Mitä tarkoittaa provisiointi. Viitattu 13.4.2016. <http://vastaukset.fi/q/Mit%C3%A4+tarkoittaa+provisiointi>

TechTerms 2011. Redundancy. Viitattu 18.4.2016. <http://techterms.com/definition/redundancy>

Wikipedia 2016. Data center. Viitattu 20.4.2016. https://en.wikipedia.org/wiki/Data_center