PÄÄTELAITTEIDEN TIETOTURVA YRITYSVERKOSSA

Niilo Tarkkanen

Opinnäytetyö
Marraskuu 2013
Tietojenkäsittely
Tietoverkkopalvelut

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkkopalvelut

TARKKANEN, NIILO:
Päätelaitteiden tietoturva yritysverkossa

Opinnäytetyö 49 sivua
Marraskuu 2013

Opinnäytetyön tavoitteena oli tutkia, kuinka päätelaiteturvallisuudesta voidaan huolehtia Tampereen ammattikorkeakoulun (TAMK) WPK-verkossa. Työssä tutkittiin erityisesti Microsoft System Center 2012 Endpoint Protection -tietoturvaohjelmiston toimivuutta ja soveltuvuutta WPK-verkon käyttöön. Opinnäytetyössä tuotiin myös esiin, mitä muita vastaavia tietoturvajärjestelmiä markkinoilla tällä hetkellä on. Työn toimeksiantajana oli Tampereen ammattikorkeakoulu.

Tutkimus tehtiin siten, että luotiin eristetty virtuaalinen testiympäristö, johon System Center 2012 Endpoint Protection asennettiin ja jossa tutkittiin sen toimintaa. Samalla tutkittiin, miten asennukset tehtäisiin WPK-verkkoon ja miten toiminta muuten eroaisi testiympäristön ja tuotantoympäristön välillä. Asennuksista, konfiguroinneista, käyttöönotosta sekä ylläpidosta tuli luoda dokumentaatiot.

Työn alkuosassa käsiteltiin yleistä teoriaa tietoturvasta, tietoturvaohjelmistoista sekä käytetyistä työympäristöistä, minkä jälkeen siirryttiin esivaatimusten ja työssä käytettävien ohjelmistojen asennuksiin ja käyttöönottoihin. Loppuosa käsitteli itse tietoturvaohjelmiston käyttöönottoa ja ylläpitoa. Lopputuloksena syntyi teoriaosuuden lisäksi kattava dokumentaatio System Center 2012 Endpoint Protection -ohjelmiston käyttöönotosta päätelaitteille yritysympäristössä, siihen tarvittavista ohjelmistoista ja niiden konfiguraatioista sekä ylläpidosta.

Työssä käytetyn tietoturvaohjelmiston etuina Microsoft-ympäristöissä on muun muassa sen helppo käytettävyys, integroituvuus muihin Microsoftin tuotteisiin ja päätelaitteiden keskitetty hallinta. Ohjelmisto helpottaa ylläpitäjien työtä ja näin ollen pienentää kustannuksia yrityksissä. Ohjelmiston käyttöönotto varsinkin WPK-verkossa parantaa verkon toimintaa, sillä tällä hetkellä käytössä olevassa tietoturvaohjelmistossa ei edellä mainittuja ominaisuuksia ole. Opinnäytetyötä voidaan käyttää oppaana System Center 2012 Endpoint Protectionin käyttöönotossa WPK-verkon lisäksi myös muissa pienissä yritysverkoissa.

Asiasanat: päätelaitteiden tietoturva, Microsoft, Configuration Manager, Endpoint Protection

ABSTRACT

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

TARKKANEN, NIILO:
Endpoint Security on a Corporate Network

Bachelor's thesis 49 pages
November 2013

The objective of this thesis was to study how endpoint security can be achieved on the WPK network of Tampere University of Applied Sciences (TUAS). The focus was especially on the functionality and the suitability of the Microsoft System Center 2012 Endpoint Protection software on the WPK network. Other popular endpoint security systems were also introduced. The thesis was commissioned by TUAS.

The research was conducted in a virtualized test environment where the System Center 2012 Endpoint Protection was installed and its functionality was studied. In addition, the variation of the installation and the functionalities between the test environment and the production network (WPK) was studied. The installation, the configuration, the implementation and the maintenance sections were documented.

The first part of the thesis dealt with the general theory of information security and security software. After the theory section, the environments and the prerequisites were introduced and the installations and the implementations of the used software were conducted. Finally, the System Center 2012 Endpoint Protection software was implemented and configured. Furthermore, the main points of maintenance were discussed. As a result, a comprehensive document about the prerequisites, the implementation, the configuration and the maintenance of Endpoint Protection was produced in addition to a brief theory section of information security.

The benefits of the System Center 2012 Endpoint Protection in a Microsoft environment include, for example, easy usability, integrability with other Microsoft products and centralized administration of end devices. The software eases the work of administrators and therefore reduces costs in companies. The implementation of the software especially in the WPK network would improve the functionality of the network because the currently used software does not have the above-mentioned features. This thesis can be used as a manual for the implementation of the System Center 2012 Endpoint Protection in the WPK network, but also in other small corporate networks.

Key words: endpoint security, Microsoft, Configuration Manager, Endpoint Protection

SISÄLLYS

LYHENTEET JA TERMIT

AD	*Active Directory*, Microsoft Windows -toimialueen käyttäjätietokanta, johon kuuluvat käyttäjät, tietokoneet ja muita verkon resursseja.
DC	*Domain Controller*, palvelinrooli Windows Server -ympäristössä, on vastuussa toimialueen resurssien sallimisesta käyttäjille.
Feature	Windows Server -ympäristön ohjelma, joka tukee roolien toiminnallisuutta.
Hyper-V	Microsoftin kehittämä ohjelmisto virtualisointiin Windows Server -käyttöjärjestelmissä.
Isäntäpalvelin	Virtuaalikoneiden hallinnoimiseen tarkoitettu palvelin.
Malware	*Malicious Software*, yleisnimitys haittaohjelmille, jotka on tehty aiheuttamaan vahinkoa tietokoneissa tai tietojärjestelmissä.
Rooli	Ohjelma, joka tarjoaa tietyn toiminnallisuuden Windows Server -ympäristöihin.
Rootkit	Haittaohjelmistopaketti, joka piilottaa käyttöjärjestelmään asennetun malwaren estäen sen havaitsemisen.
SCCM	*System Center Configuration Manager*, Microsoftin järjestelmien hallintaan tarkoitettu ohjelmisto.
SCEP	*System Center Endpoint Protection*, SCCM:ssa rooli, joka tarjoaa tietoturvaratkaisun päätelaitteille.
Site	Hallittava alue SCCM:ssa ja AD:ssa.
Toimialue	*Domain*, Windows-työasemien ja -palvelimien muodostama yhteinen joukko, jota voidaan hallita keskitetysti.
Virtualisointi	Tekniikka, jolla fyysisiä resursseja voidaan muuttaa loogisiksi ja päinvastoin. Tässä tapauksessa yhteen fyysiseen palvelimeen luodaan kaksi loogista palvelinta ja työasemaa, jotka toimivat kuten fyysiset laitteet.
Virus	Haittaohjelmatyyppi, joka yleensä tuhoaa tiedostoja ja aiheuttaa epäsuorasti muutakin haittaa.
Windows Server	Microsoftin kehittämä käyttöjärjestelmä palvelinkäyttöön.

Windows Update	Microsoftin palvelu, josta saadaan päivityksiä Microsoftin tuotteisiin.
Wizard	Windows-ympäristöistä tuttu suoraviivainen ja graafinen asennuksen opastus.

1 JOHDANTO

1.1 Opinnäytetyön tausta, tavoite ja tarkoitus

Suoritin osan harjoittelustani Tampereen ammattikorkeakoulun (TAMK) tietojenkäsittelyn koulutusohjelman laboratorioverkon eli WPK-verkon ylläpitotehtävissä. Tietoturvaohjelmisto, jota ympäristön päätelaitteissa tällä hetkellä käytetään, ei ole kovin hyvin hallittavissa keskitetysti, joten uudistukselle oli tarvetta. Harjoitteluni ohjaaja, joka toimii myös WPK-verkon yhtenä vastuuhenkilönä, ehdotti opinnäytetyöni aiheeksi uuden tietoturvaratkaisun käyttöönottoa WPK-verkossa. Harjoitteluaikanani WPK-ympäristö tuli itselleni kohtalaisen tutuksi, joten omasta mielestänikin aihe on hyödyllinen sekä ajankohtainen toimeksiantajalle, mutta myös mielenkiintoinen ja sopiva oman koulutukseni syventämiseksi. Työn toimeksiantajana on siis TAMK.

Opinnäytetyön tavoitteena on tutkia, kuinka päätelaiteturvallisuudesta voidaan huolehtia TAMKin WPK-verkossa. Työssä tutkitaan erityisesti Microsoft System Center 2012 Endpoint Protection -tietoturvaohjelmiston toimivuutta ja soveltuvuutta WPK-verkon käyttöön. Opinnäytetyössä tuodaan myös esiin, mitä muita vastaavia tietoturvajärjestelmiä markkinoilla tällä hetkellä on.

Tarkoituksena on tehdä tutkimus siten, että luodaan eristetty virtuaalinen testiympäristö, johon System Center 2012 Endpoint Protection asennetaan ja tutkitaan sen toimintaa. Samalla tutkitaan, miten asennukset tehtäisiin WPK-verkkoon ja miten toiminta muuten eroaisi testiympäristön ja WPK-verkon välillä. Järjestelmän käyttöönottoa tutkitaan WPK-verkossa niin, että ainakin yhden WPK-verkon luokan työasemien turvallisuus voidaan taata sen avulla. Järjestelmän käyttöönoton tutkiminen tehdään siten, että järjestelmä voi jäädä käyttöön pysyvästi. Tutkimuksessa otetaan huomioon myös järjestelmän laajennettavuus koko WPK-verkkoon ja tehdään siitä ohjeistus. Järjestelmän käyttöönotto kokonaisuudessaan dokumentoidaan ja ylläpitoa varten luodaan ohjeistus.

1.2 Tietoturvan periaatteet

Tietoturva on nykyään tärkeä osa jokaisen yrityksen arkipäivää, sillä tietoturvauhat lisääntyvät ja kehittyvät jatkuvasti. Yritysten tietoverkoissa on ensisijaisen tärkeää, että päätelaitteet ja järjestelmät toimivat niin kuin pitääkin, jotta päivittäiset työt saadaan tehtyä, eikä yrityksen sisäinen tieto leviä ulkopuolisille. Yritysten tulee panostaa tietoturvaansa, sillä sen puuttuminen voi vaikuttaa tietojen leviämisen ja tuhoutumisen lisäksi myös yrityksen maineeseen ja taloudellisiin menetyksiin.

Tietoturvan määritelmä on hyvin laaja. Yleisesti käytössä olevassa määritelmässä tietoturva on jaettu kuuteen osaan: kolmeen pääosa-alueeseen ja kolmeen niitä täydentävään osa-alueeseen. Näihin periaatteisiin pitäisi jokaisen yrityksen pyrkiä tietoturva-asioita mietittäessä. Pääosa-alueet ovat

- Luottamuksellisuus (Confidentiality) – Tietoa saavat käyttää vain ne henkilöt, joilla on siihen lupa
- Eheys (Integrity) – Tiedon pysyminen muuttumattomana, luvattomat henkilöt eivät pääse muuttamaan tietoja
- Saatavuus (Availability) – Tietojen ja palvelujen tulee olla saatavissa ja tietojärjestelmien toimia silloin, kun niitä tarvitaan. (Järvinen 2002, 22–28.)

Täydentäviin osa-alueisiin kuuluvat

- Todentaminen (Authentication) – Todennetaan, onko käyttäjä juuri se, jota väittääkin olevansa
- Pääsynvalvonta (Access control) – Valvotaan, onko käyttäjällä oikeus päästä järjestelmän tietoihin
- Kiistämättömyys (Non-repudiation) – Toimien osapuolet eivät voi kiistää olleensa osapuolina (esimerkiksi sähköisessä kaupankäynnissä). (Järvinen 2002, 22–28.)

Yrityksillä on tärkeää olla selkeä tietoturvapolitiikka sekä tietoturvastrategia, jotka määritetään uhkien ja riskien kartoituksen perusteella. On tärkeää, että luodaan yhteiset pelisäännöt tietoturvan osalta ja opetetaan ne yrityksen työntekijöille. Vastuu pelisääntöjen noudattamisesta on kaikilla järjestelmän käyttäjillä. Säännöt voidaan tehdä

koskemaan esimerkiksi varmuuskopiointia, salasanojen määritystä, eri verkkojen käyttöä (esimerkiksi langattomat verkot), Internetin käyttöä, sähköpostin käyttöä, etätöitä sekä kulunvalvontaa. (Järvinen 2002, 113–120.)

Tietoturva on käsitteenä siis hyvin laaja. Siihen liittyy paljon teknisiä sekä psykologisia asioita. Tekniset tietoturvajärjestelmät ovat hyvin hallittavissa, mutta yleensä näistä järjestelmistä ja asioista vastaavat kuitenkin ihmiset, jotka tekevät tietoturvakokonaisuudesta vaikeasti hallittavan. Ihmisillä on taipumus tehdä virheitä, he eivät välttämättä tiedä tai muuten vain noudata annettuja toimintatapoja tai vahinkoa aiheutetaan tahallaan. (Järvinen 2002, 47.)

Yksi tärkeä osa yrityksen tietoturvaa on päätelaitteiden tietoturva. Koska liiketoiminnassa käytetään koko ajan enemmän Internetiä, yritysten päätelaitteiden tietoturvaohjelmistojen tulee olla toiminnassa ja ajan tasalla jatkuvasti, jotta uhkilta voidaan suojautua. Ajan tasalla oleva tietoturvaohjelmisto suojaa päätelaitteita ja koko tietoverkon järjestelmiä erilaisilta haittaohjelmilta sekä muilta tietoturvariskeiltä. Tässä opinnäytetyössä keskitytäänkin tietoturvan tekniseen toteutukseen, tarkemmin juuri päätelaitteiden turvallisuuteen.

2 TIETOTURVAOHJELMISTOT

2.1 Markkinoilla olevat tietoturvaohjelmistot

Tällä hetkellä markkinoilla on useita eri tietoturvaohjelmistoja, sillä tietoturva-ala on suurta bisnestä. Ohjelmistot vaihtelevat maksullisista ilmaisiin, ja niitä suunnitellaan sekä yritysympäristöihin että yksityiseen kotikäyttöön. Tietoturvaratkaisuja on moneen tarpeeseen, siksi niitä hankittaessa onkin syytä miettiä, mitä niillä halutaan saavuttaa. Normaalille kotikäyttäjälle yleensä riittää suojaksi ”maalaisjärjen” lisäksi ilmaisen virustorjuntaohjelmiston asentaminen, sillä esimerkiksi Windows-työasemissa on nykyisin palomuuriohjelma jo valmiina. Yrityksille asia on kuitenkin hieman monimutkaisempi ja ratkaisu kannattaa ostaa käyttötarpeen mukaan.

Yrityksille tarkoitetut tietoturvaohjelmistot ovat harvoin ilmaisia. Ohjelmistojen käyttölisenssit ovat maksullisia ja ohjelmistojen ominaisuudet ovat huomattavasti laajemmat. Yrityksille suunnatut maksulliset ohjelmistot tarjoavat yleensä reaaliaikaisen päätelaitteiden haittaohjelmatorjunnan lisäksi esimerkiksi palomuurin, suojauksen eri palvelimille, kuten sähköpostipalvelimille ja tiedostopalvelimille, roskapostisuodattimen, suojauksen selaimelle, nykyään myös suojauksen mobiililaitteille sekä keskitetyn hallinnan koko ohjelmistolle. Tuotteita on räätälöity erikokoisille yrityksille, joten lisenssejä myydään ohjelmistoa käyttävien laitteiden määrän mukaan ja eri ominaisuuksia ostetaan yritysten tarpeiden mukaan. Esimerkiksi muutamien työasemien pienyrityksille ja keskisuurille ja suurille yrityksille on tarjolla erikokoisia tietoturvaratkaisuja.

Tunnettuja ja yleisesti käytössä olevia tietoturvaohjelmistoja yrityskäyttöön ovat muun muassa Kaspersky Endpoint Security, McAfee Endpoint Protection Suite, Bitdefender Endpoint Security, Trend Micro Enterprise Security, F-Secure Internet Security, Panda Global Business Protection, ESET Endpoint Security, Avast! Endpoint Protection Suite (Plus) ja Microsoft System Center 2012 Endpoint Protection. Näiden tuotteiden ominaisuudet vaihtelevat, joten yksiselitteisesti parhaan tuotteen valinta on vaikeaa, sillä siihen vaikuttavat monet tekijät, kuten tuotteiden hinnat ja yritysten tarpeet. Internetissä on kuitenkin useita eri sivustoja, joissa on testituloksia tietoturvaohjelmistojen eri osa-alueiden vertailuista, esimerkkinä AV-comparatives.

Tässä työssä ei kuitenkaan keskitytä tarkemmin tietoturvaohjelmistojen vertailuun, vaan tutkittavaksi on valittu toimeksiantajan pyynnöstä Microsoft System Center 2012 Endpoint Protection.

2.2 Microsoft System Center 2012 Endpoint Protection SP1

Microsoft System Center 2012 Endpoint Protection SP1 (SCEP) on Microsoftin oma maksullinen tietoturvaohjelmisto työasemille ja palvelimille yritysverkkoon. SCEP:n tarkoituksena on suojata tietokonetta uusimmilta viruksilta, malwareilta, rootkiteiltä ja muilta uhkilta. Se on kehittyneempi versio aikaisemmasta Forefront Endpoint Protectionista. SCEP toimii integroituna roolina Microsoft System Center 2012 Configuration Managerissa (SCCM), jonka kautta kaikki SCEP:n hallintaan liittyvät asiat pystytään hoitamaan keskitetysti, vaivattomasti ja tehokkaasti yhdestä hallintakonsolista. (System Center 2012 Endpoint… 2013, 1-2.)

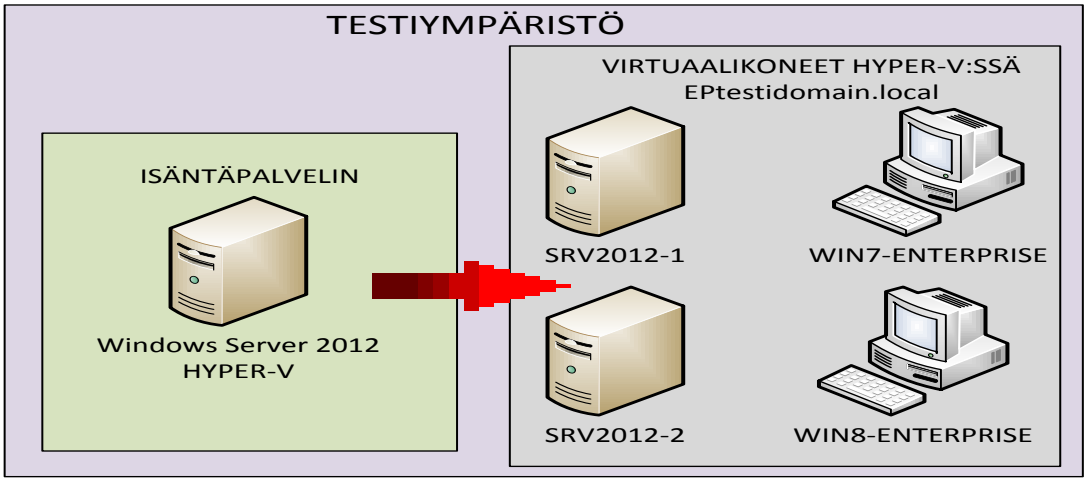
Etuna SCEP:ssä on, että Windows-työasemien palomuurin hallinta integroituu hyvin SCCM:iin ja SCEP:iin. Palomuuripolitiikkojen sekä yleisesti tietoturvapolitiikkojen luonti ja jakaminen tietyille ryhmille on helppoa. SCCM:n avulla voidaan myös keskitetysti jakaa ohjelmia, ohjelmistojen päivityksiä, sekä tärkeimpänä uusia virustietokantapäivityksiä SCEP:lle. SCEP:ssa on myös hyvät reaaliaikaiset raportointimahdollisuudet löydetyistä uhkista. (System Center 2012 Endpoint… 2013, 1-2.) Arvokkaana etuna SCEP:ssa on Microsoft-ympäristöissä juuri sen integroituvuus Microsoftin muihin tuotteisiin. SCCM:n avulla on helppo hallita suureenkin toimialueeseen kuuluvia päätelaitteita sekä muodostaa niistä kokoelmia, jolloin hallintaa pystytään tehostamaan. SCCM löytää esimerkiksi AD:ssa olevat tietokoneet, joten on helppo jaotella kokoelmat esimerkiksi luokittain, jos halutaan jakaa SCEP tietylle ryhmälle. SCEP:n toimeenpano on helppoa suurillekin ympäristöille, sillä SCEP:n asiakasohjelman jakaminen työasemille on vaivatonta SCCM:n avulla (Rachui, Agerlund, Martinez & Daalmans 2012, 700).

3 TYÖSSÄ KÄYTETYT YMPÄRISTÖT

3.1 Virtuaalinen testiympäristö

Testiympäristössä käytettiin yhtä fyysistä isäntäpalvelinta, jossa käyttöjärjestelmänä oli Windows Server 2012 Datacenter ja siihen asennettiin rooliksi ainoastaan Hyper-V. Hyper-V:n ”sisälle” asennettiin ulkomaailmalta eristettyyn verkkoon neljä virtuaalista tietokonetta: kaksi Windows Server 2012 Datacenter -palvelinta, SRV2012-1 ja SRV2012-2, joille asennettiin SCEP:n tarvitsemat palvelut sekä kaksi työasemaa SCEP:n testausta varten, WIN7-ENTERPRISE ja WIN8-ENTERPRISE. Toiseen työasemaan asennettiin käyttöjärjestelmäksi Windows 7 Enterprise ja toiseen Windows 8 Enterprise nimiensä mukaisesti. Kaikki käyttöjärjestelmät olivat 64-bittisiä versioita.

Ennen työn varsinaista aloitusta jokainen virtuaalikone sekä isäntäpalvelin päivitettiin Windows Updaten kautta ladatuilla päivityksillä ajan tasalle. Testiympäristössä kaikki toiminnallisuudet olivat virtuaalikoneilla ja ainoastaan Hyper-V:n virtuaalikoneet yhdistettiin samaan toimialueeseen, jolle annettiin nimeksi EPtestidomain.local. Palvelimille ja työasemille annettiin kiinteät IP-osoitteet 192.168.1.0 / 24 -osoiteavaruudesta, jolloin niiden väliset yhteydet saatiin toimimaan. Isäntäpalvelin toimi tässä tapauksessa vain Hyper-V -alustana, eikä se kuulunut toimialueeseen, sillä testiympäristö haluttiin eristää mahdollisten konfliktien välttämiseksi. Kuvassa 1 havainnollistetaan käytettyä testiympäristöä.



KUVA 1. Testiympäristön topologiakuva

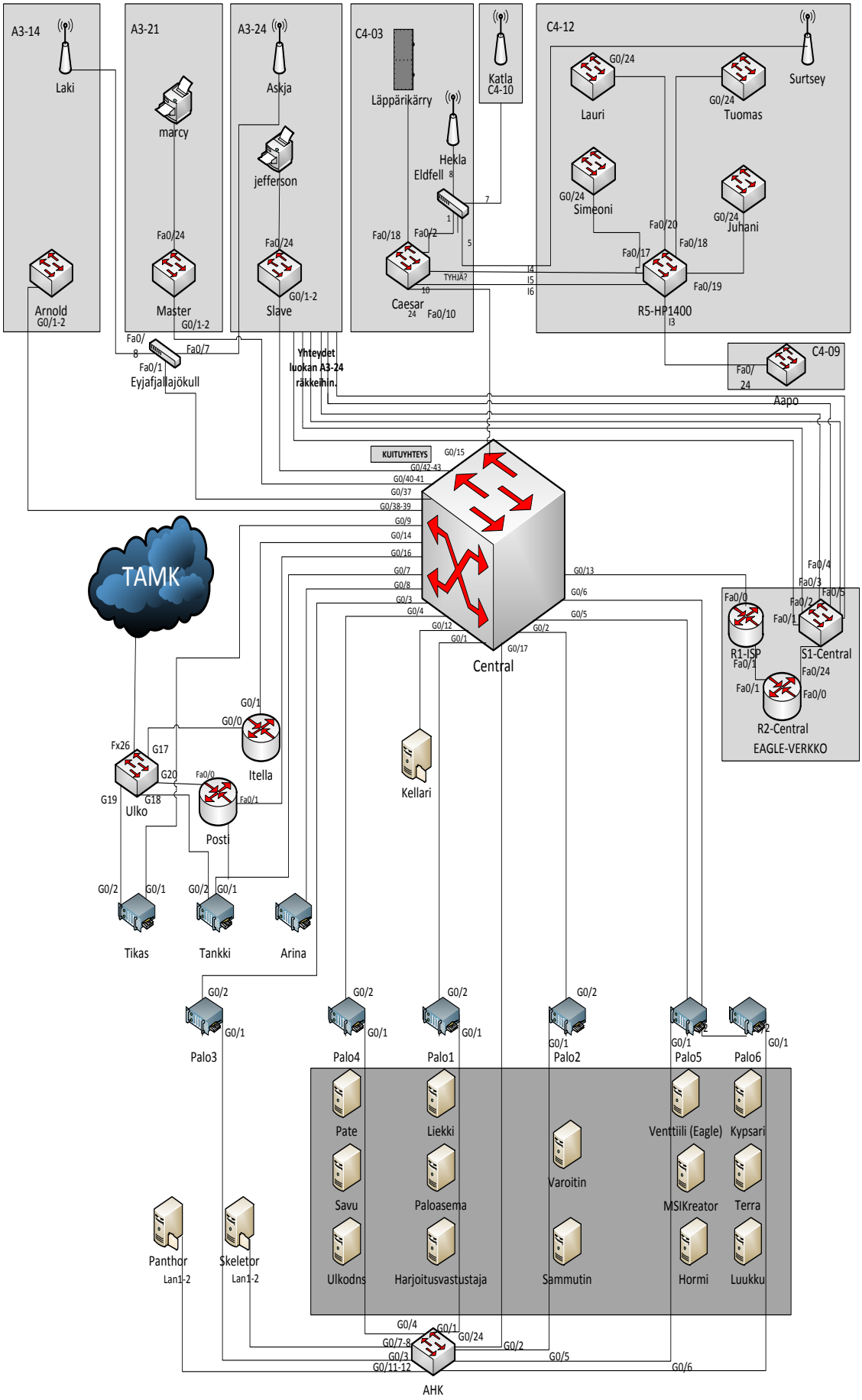
3.2 Tuotantoympäristö – TAMKin WPK-verkko

Tuotantoympäristönä työssä on TAMKin WPK-verkko. WPK-verkko on TAMKin tietojenkäsittelyn koulutusohjelman harjoittelijoiden ja opettajien ylläpitämä tietoverkko, joka on osa TAMKin verkkoa, mutta kuitenkin erillinen kokonaisuus. WPK-verkko toimii oppimisympäristönä lähinnä tietoverkko-opiskelijoille ja siihen kuuluu

- neljä luokkaa ja pieni konesali, jossa verkon hallinta pääsääntöisesti hoidetaan
- n. 100 Windows-työasemaa ja useita Windows Server -palvelimia
- n. 20 kannettavaa Windows-työasemaa
- n. 80 reititintä
- n. 70 kytkintä
- kolme levypalvelinta
- UPS-laitteita
- kaksi WLAN-kontrolleria ja viisi tukiasemaa.

Suuri osa laitteistosta on luokissa opiskelijoiden harjoitustöiden käytössä, joten kaikki laitteet eivät ole merkittäviä verkon topologian kannalta. Luokat ovat kuitenkin opetuskäytössä päivittäin ja työasemilla on Internet-yhteys, joten verkko on täysin tuotantoympäristöä vastaava ja muun muassa siksi tarvitseekin tietoturvaratkaisun toimintakyvyn ylläpitämiseksi.

WPK-verkon kaikissa työasemissa on käytössä Microsoft Windows 7 -käyttöjärjestelmä ja palvelimissa suurimmassa osassa Microsoft Windows Server 2008 R2. Palo-palvelimia ja niiden virtuaalikoneita on yhdistetty pieneksi ”pilveksi” System Center Virtual Machine Managerin avulla. Opetuskäytössä on nykyään myös Windows Server 2012:n kokeiluversioita, jotka asennetaan erillisille vaihdettaville kovalevyille ja voidaan tarpeen tullen vaihtaa työasemien Windows 7:n tilalle. Tuotantoympäristössä kuitenkaan ei Windows Server 2012 -palvelimia vielä ole. Kuva 2 havainnollistaa WPK-verkon topologiaa.



KUVA 2. WPK-verkon topologiakuva

4 ESIVAATIMUKSET JA OHJELMISTOJEN ASENNUS

4.1 Esivaatimukset

Kun asennetaan tyhjään ympäristöön SCEP, niin kuin tässä tapauksessa tehtiin, on tutkittava ja asennettava lukuisia määriä eri asioita ennen ohjelmistojen varsinaista asennusta. Yleensä Windows-ympäristössä asennukset ovat helppoja ja suoraviivaisia, mutta tässä tapauksessa joutui ottamaan huomioon monia eri muuttujia. Ensin on syytä selvittää, että ohjelmistot, joita asennetaan, ovat yhteensopivia keskenään sekä yhteensopivia käytettyjen käyttöjärjestelmien kanssa. Toiseksi on luotava toimialue asentamalla Windows Server 2012 -palvelimelle Active Directory Domain Services -rooli, sekä liitettävä ympäristössä käytettävät palvelimet ja työasemat siihen. Samalla varmistetaan, että palvelimet ja työasemat löytävät toisensa. Sen jälkeen voidaan alkaa tutkia muita vaatimuksia.

Suurimmat ohjelmistovaatimukset SCEP:ia varten ovat Microsoft SQL Server ja SCCM. Näillä ohjelmistoilla on myös omat esivaatimuksensa, jotka pitää täyttää asennusten mahdollistamiseksi. Testiympäristössä jaettiin asennukset niin, että toisella Windows Server 2012 -palvelimella oli SQL Server ja toinen palvelimista toimi DC:na sekä SCCM:n ja SCEP:n hallintapalvelimena kuormituksen jakamiseksi. Turvallisuussyistä SQL Serveriä ei suositella muutenkaan asennettavaksi DC-palvelimelle (Hardware and Software Requirements… 2013). Tässä tapauksessa valikoitiin ohjelmistoista 2012 SP1 -versiot, sillä ne olivat valintahetkellä kohtalaisen uusia sekä yhteensopivia keskenään ja käytettyjen käyttöjärjestelmien kanssa. Koska esimerkiksi SQL Server ja SCCM ovat niin laajoja ohjelmistoja, niitä ei käsitellä tässä työssä kokonaan yksityiskohtaisesti, vaan niiltä osin, kuin on tarpeellista asennuksen ja SCEP:n toiminnan kannalta. Ensin on asennettava SQL Server, jotta SCCM:n voidaan asentaa.

4.1.1 Microsoft SQL Server 2012 SP1

Microsoft SQL Server on Microsoftin kehittämä relaatiotietokantojen hallintaohjelmisto, joka on edellytys SCCM:n asennukselle. SQL Serveristä on useita

eri versioita eri käyttötarkoituksia ja käyttöjärjestelmäversioita varten. Ohjelma tarvitsee käyttöä varten lisenssin. Kun asennusta tehdään oikeaan tuotantoympäristöön, kuten tässä tapauksessa WPK-verkkoon, tulee lisenssit ostaa Microsoftilta. Testiympäristössä kuitenkin asennettiin vain Microsoftin sivuilta ladattavissa oleva ilmainen kokeiluversio, joka toiminnallisuudeltaan on täysin samanlainen, mutta se toimii vain rajoitetun ajan.

SQL Server 2012 SP1:n vaatimuksena ovat .NET Framework 3.5 SP1- sekä .NET Framework 4.0 -komponentit. Myös Windows PowerShell 2.0 vaaditaan. Käytettäessä Windows Server 2012 -käyttöjärjestelmää, SQL Serverin asennusohjelma lataa .NET Frameworkit automaattisesti Internet-yhteyden ollessa toiminnassa, mutta PowerShell joudutaan asentamaan erikseen, jos sitä ei vielä ole. Vanhemmilla käyttöjärjestelmillä kuten Windows Server 2008 R2:lla, joita WPK-verkossakin on, tarvitsee komponentit asentaa erikseen ennen SQL Serverin asennusta. SQL Server 2012:n asennus on tuettu Hyper-V -virtuaaliympäristössä Windows Server 2008 SP2:ssa ja siitä uudemmissa käyttöjärjestelmissä. (Hardware and Software Requirements… 2013)

SQL Server 2012 tarvitsee kovalevytilaa vähintään 6 GB + 2,2 GB SP:lle, mutta tarve vaihtelee riippuen siitä, mitä SQL Serverin ominaisuuksia asennetaan. Prosessorin vähimmäissuositus on 2.0 GHz ja muistia tulisi olla vähintään 4 GB, mutta parhaan suorituskyvyn saavuttamiseksi on suositeltavaa lisätä muistia tietokantojen kasvaessa. (Hardware and Software Requirements… 2013) Kuitenkin esimerkiksi SCCM vaatii SQL Serveriä varaamaan vähintään 8 GB muistia SCCM:ia varten, joten muistia on syytä olla enemmän, varsinkin siinä tapauksessa, jos SQL Serverillä on muitakin käyttötarkoituksia.

4.1.2 System Center 2012 Configuration Manager SP1

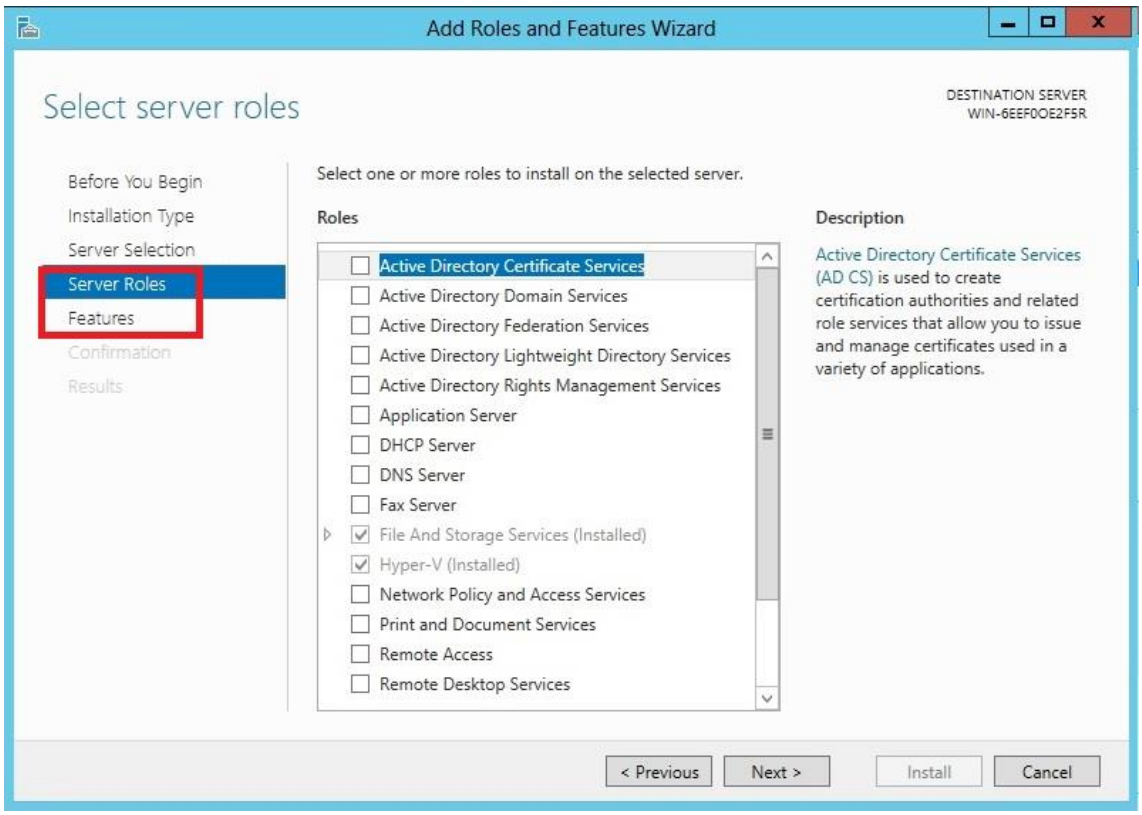
System Center 2012 Configuration Manager eli SCCM on Microsoftin järjestelmien hallinnoimiseen tarkoitettu ohjelmisto. Se on tehty hallinnoimaan laajoja ryhmiä työasemia sekä palvelimia, mutta se tukee myös monia mobiililaitteita. SCCM tarjoaa laiteryhmille esimerkiksi valvontaa, etähallintaa, ohjelmistojen ja päivitysten jakamista ja käyttöjärjestelmien toimeenpanoa. (Configuration Manager 2013.) SCCM helpottaa huomattavasti verkon ylläpitäjien työtä, joten se vähentää myös yrityksen kuluja

(VALUE PRISM CONSULTING 2013, 14). Sen kautta hallitaan ja toimeenpannaan täysin myös SCEP, jonka vuoksi SCCM on välttämätön myös tässä tapauksessa. Myös SCCM ja SCEP tarvitsevat maksullisen lisenssin tuotantoympäristöön asennettaessa. Kuitenkin samoin kuin SQL Serverin osalta, testiympäristössä ladattiin niin ikään kokeiluversio Microsoftin sivuilta SCCM:sta ja SCEP:sta, jotka olivat yhdessä paketissa.

Laitteistovaatimuksina SCCM:lle on vähintään 1.4 GHz:n prosessori, muistia 2 GB, sekä vapaata tilaa 10 GB ja yhteensä 50 GB. Nämä laitteistovaatimukset ovat kuitenkin tarkoitettu ympäristöön, jossa on 100 asiakaskonetta. (Supported Configurations for Configuration… 2013.) Testiympäristöön ne pätevät, mutta WPK-verkossa on hieman enemmän client-koneita, joten on syytä käyttää myös tehokkaampaa laitteistoa, joka WPK-verkossa onkin käytössä. Jos suunnitellaan asennettavaksi SQL Server ja SCCM samalle palvelimelle, johon asennetaan yksi standalone site, nousevat vaatimukset suuresti. Silloin tarvitaan jo 8-ydin -prosessori (Intel Xeon E5504 tai vastaava) , 32 GB muistia sekä 550 GB kovalevytilaa. (Planning for Hardware Configurations… 2012.)

Myös SCCM tarvitsee useita komponentteja, jotta se voidaan asentaa. Tarvittavat komponentit vaihtelevat riippuen siitä, mitä site system -rooleja SCCM:iin asennetaan. Windows Server 2012:ssa on hieman eri esivaatimukset SCCM:lle kuin aikaisemmissa käyttöjärjestelmissä. Tämä tulee ottaa huomioon, jos tuotantoverkossa asennus tehtäisiin vielä vanhoille palvelimille.

Palvelin, jolle SCCM asennetaan, tarvitsee .NET Framework 3.5-, .NET Framework 4.5-, sekä Remote Differential Compression (RDC)- ja Background Intelligent Transfer Service (BITS) -komponentit. Nämä ovat Windowsin featureita, jotka voidaan asentaa Windows Server 2012:n Server Manager -hallintakonsolin kautta suoraviivaisella Add Roles and Features -wizardilla (kuva 3). Samaa kautta asennetaan myös vaadittavat Internet Information Services- (IIS) sekä Windows Server Update Services (WSUS) -roolit. IIS-roolin yhteydessä asennetaan oletuksien lisäksi seuraavat featuret: Basic Authentication, IP and Domain Restrictions, URL Authorization, Windows Authentication, ASP, ASP.NET 3.5, ASP.NET 4.5, IIS Management Scripts and Tools, Management Service ja IIS 6 WMI Compatibility. (Supported Configurations for Configuration… 2013.)



KUVA 3. Kuvakaappaus Windows Server 2012 -käyttöjärjestelmän Add Roles and Features -wizardista

Ennen SCCM:n asennusta on ladattava Windows Assessment and Deployment Kit (ADK). Sen saa helposti yhtenä asennuspakettina Microsoftin sivuilta. ADK sisältää useita eri featureita, joista kuitenkin asennetaan vain SCCM:n vaatimat kolme komponenttia, jotka ovat Deployment Tools, Windows Preinstallation Environment (Windows PE) ja User State Migration Tool (USMT). Kaikki näistä sisältävät pienen kokoelman tarvittavia työkaluja.

Kaikkien SCCM:n ominaisuuksien toimimiseksi on suositeltavaa tehdä myös AD:n schema-laajennus, vaikka se ei olekaan asennuksen kannalta pakollista. Laajennus tehdään suorittamalla järjestelmänvalvojana extadsch.exe-tiedosto, joka löytyy SCCM:n asennusmediasta hakemistosta SMSSETUP\BIN\X64. Tiedoston suorittaminen luo extadsch.log-lokitiedoston järjestelmäaseman juureen, mistä nähdään, onnistuiko laajennus. (How to Extend the… 2012.)

SCCM-palvelimella pitää ennen asennusta olla myös oikeudet julkaista AD:hen. Tämä tarkoittaa sitä, että SCCM-palvelimen tietokonetilille pitää antaa täydet oikeudet System

Management -containeriin AD-domainissa. Oikeudet annetaan ADSI Edit -konsolissa, joka löytyy valmiina Windows Server 2012:ssa. Siellä luodaan uusi container-objekti CN=System-kansion alle, jolle annetaan arvoksi System Management. Juuri luodun containerin ominaisuuksista Security-välilehdeltä lisätään objektityyppeihin tietokoneet, jolloin itse SCCM-palvelin, joka testiympäristössä on SRV2012-1, löytyy ja se pystytään lisäämään. Sen jälkeen SRV2012-1 näkyy ominaisuuksissa lisättynä, minkä jälkeen sille annetaan täydet oikeudet samalta välilehdeltä sekä vielä Advanced-valikon kautta sen alaobjekteillekin.

Vielä viimeisenä täytyy huomioida, että SCCM-palvelimella on oikeudet myös palvelimeen, jossa SQL Server sijaitsee. Käytännössä siis lisätään SQL Server -palvelimen (SRV2012-2) paikalliseen Administrators -ryhmään SCCM-palvelimen tietokonetili. Lisäys tehdään navigoimalla SQL Server -palvelimella Computer Management -konsolilla kohtaan Local Users and Groups - Groups ja valitaan Properties Administrators-objektista. Siellä lisätään SCCM-palvelin (SRV2012-1) Administrators-ryhmään, jolloin oikeudet on annettu. Ennen SCCM:n asennusta tarvitsee myös asettaa SQL Serverin asetuksista rajoitukset, kuinka paljon muistia SQL Server voi käyttää. Asetukset sijaitsevat SQL Server Management Studiossa, jossa navigoidaan käytetyn instanssin ominaisuuksiin ja valitaan Memory-välilehti. Tämä tehdään luonnollisesti vasta SQL Serverin onnistuneen asennuksen jälkeen.

4.1.3 Muuta huomioitavaa vaatimuksista

Myöhempien asennusvaiheiden helpottamiseksi kannattaa jo tässä vaiheessa tehdä palomuuriin hieman poikkeuksia. Jotta yhteydet SQL Serveriin olisivat kunnossa, avataan SQL Serverin käyttämät portit Windowsin palomuurista. Tämä tehdään avaamalla Windows Firewall with Advanced Security palvelimella, jossa SQL Server sijaitsee. Sieltä luodaan uusi Inbound Rule, johon määritellään aukaistavaksi SQL Serverin käyttämät TCP-portit 4022 ja 1433.

Windowsin palomuuriin lisätään myös toinen poikkeus, jotta SCCM:n kautta voidaan asentaa työasemille SCCM- ja SCEP -clientit. Asennus tapahtuu ”push”-asennuksena, eli client-ohjelmat pusketaan SCCM:n avulla halutuille asiakaskoneille. Toiminnon käyttämiseksi pitää palomuurin asetuksissa luoda sääntö, jossa sallitaan File and Printer

Sharing sekä outbound- että inbound -säännöissä ja Windows Management Instrumentation (WMI), joka sallitaan vain inbound-säännöissä (Windows Firewall and Port… 2013). Palomuuripoikkeuksen jakaminen onnistuu helposti ryhmäpolitiikan (Group Policy) avulla. Ryhmäpolitiikan asetuksissa navigoidaan kohtaan Computer Configuration - Policies - Windows Settings - Security Settings - Windows Firewall with Advanced Security. Kun valitaan uuden säännön luominen, voidaan käyttää esimääriteltyä listaa, tässä tapauksessa WMI:lle ja File and Printer Sharingille on molemmille olemassa valmis lista, jotka sallitaan. Ryhmäpolitiikka jaetaan niille päätelaitteille, joille SCCM- ja SCEP -clientit halutaan jakaa.

Koska esivaatimuksia on hyvin paljon, on sekä SQL Serverin että SCCM:n asennusohjelmissa helpotettu asian hoitamista. Molemmissa asennusohjelmissa on esivaatimusten tarkistus ennen varsinaisen asennuksen aloittamista, mikä ilmoittaa, jos jokin esivaatimuksista puuttuu ja antaa siitä lisätietoja. Jos suositeltavia, mutta ei pakollisia vaatimuksia puuttuu, ilmoittaa asennusohjelma siitä Warning-huomautuksella. Kun pakollisia vaatimuksia puuttuu, ilmoitetaan se Failed-merkinnällä, jolloin asennusta ei suoriteta, ennen kuin puuttuvat vaatimukset on asennettu. Tällä tavalla varmistetaan, että tarpeelliset komponentit ovat varmasti olemassa ennen asennusta, eikä asennuksen jälkeen huomata, että ohjelmistot eivät toimi tiettyjen komponenttien puuttuessa.

4.2 Ohjelmistojen asennus

Kun esivaatimukset on vihdoin täytetty, voidaan itse ohjelmistojen asennus aloittaa. Tässä vaiheessa suurin työ asennuksista on jo tehty ja enää tarvitsee vain huomioida oikeat asetukset asennusten yhteydessä, muuten asennukset etenevät hyvin suoraviivaisesti ja helposti. Kuten aiemmin on jo mainittu, asennetaan SQL Server ensin, sillä se on esivaatimuksena SCCM:lle.

Asennukset kuvataan niin kuin ne tehtiin testiympäristöön. Kuitenkin asennusvaiheissa otetaan huomioon oleellisilta osin myös se, miten asennus eroaisi WPK-verkkoon asennettaessa. Suurimmaksi osaksi asennukset kuitenkin menevät samalla tavalla sekä testiympäristössä että WPK-verkossa. On tärkeää, että asetukset valitaan huolella

asennuksen yhteydessä, sillä jälkikäteen niiden muuttaminen voi olla työlästä tai jopa mahdotonta.

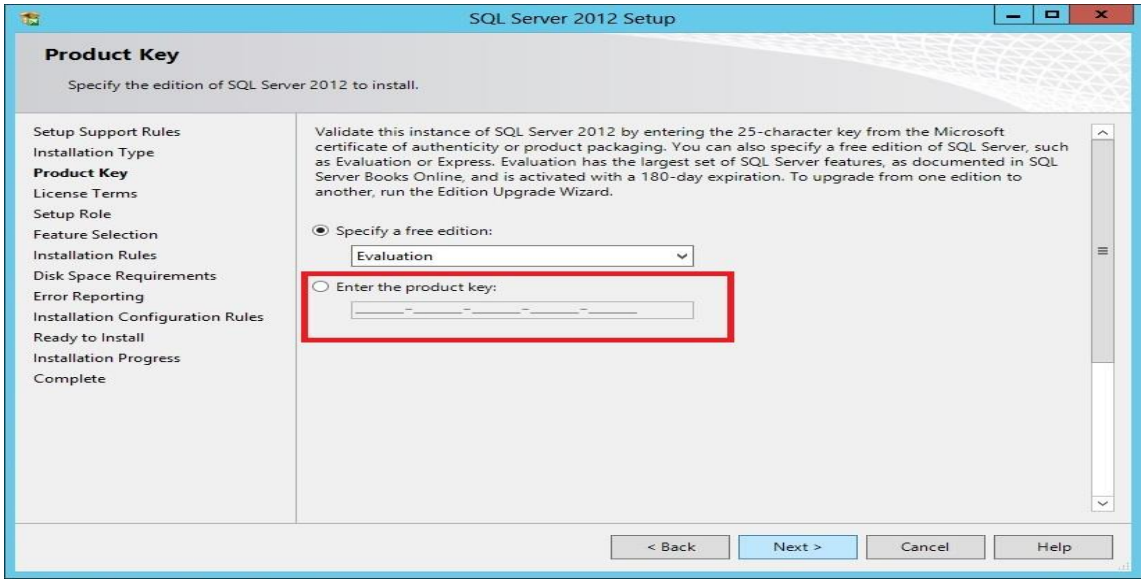
4.2.1 Microsoft SQL Server 2012 SP1

SQL Serverin asennusohjelmassa on paljon muutakin kuin vain asennuksen aloitus. Suunnittelulle, asennukselle, ylläpidolle, työkaluille, resursseille ja muille asetuksille löytyvät erikseen välilehdet, joten asennusohjelmalla pystytään muun muassa muokkaamaan ja tekemään eri asioita jo valmiiksi olemassa olevalle SQL Serverille. Testiympäristössä keskitytään kuitenkin asentamaan ohjelma puhtaalta pöydältä, joten valitaan Installation-välilehdeltä New SQL Server stand-alone installation or add features to an existing installation (kuva 4). WPK-verkossa on käytössä SQL Server 2008 R2 -versio, joten tuotantoympäristössä voisi olla vaihtoehtona myös ”Upgrade from SQL Server 2005, SQL Server 2008 or SQL Server 2008 R2”, jossa vanha versio päivitetään 2012-versioon.

KUVA 4. Kuvakaappaus SQL Server Installation Centeristä

Sen jälkeen käynnistyy itse SQL Serverin asennus-wizard. Heti alkuun tarkistetaan mahdolliset päivitykset, jos tietokone on yhteydessä Internetiin, minkä jälkeen ”Setup Support Rules” tarkistaa mahdollisia ongelmia asennuksessa, jotka täytyy korjata ennen asennuksen jatkamista, mikäli niitä löytyy. Seuraavana valitaan asennuksen tyyppi, joka

tässä tapauksessa on uusi asennus SQL Serveristä. Seuraavalla välilehdellä on tärkeä kohta, jossa päätetään, minkälainen asennus on kyseessä. Testiympäristössä käytetään ilmaista Evaluation-versiota, mutta sitä ei voida käyttää tuotantoympäristössä. WPK-verkossa siis valitaan alempi kohta ja lisätään siihen oikea tuotantokäyttöön tarkoitettu tuotetunnus, joka saadaan ohjelmistoa ostettaessa (kuva 5).

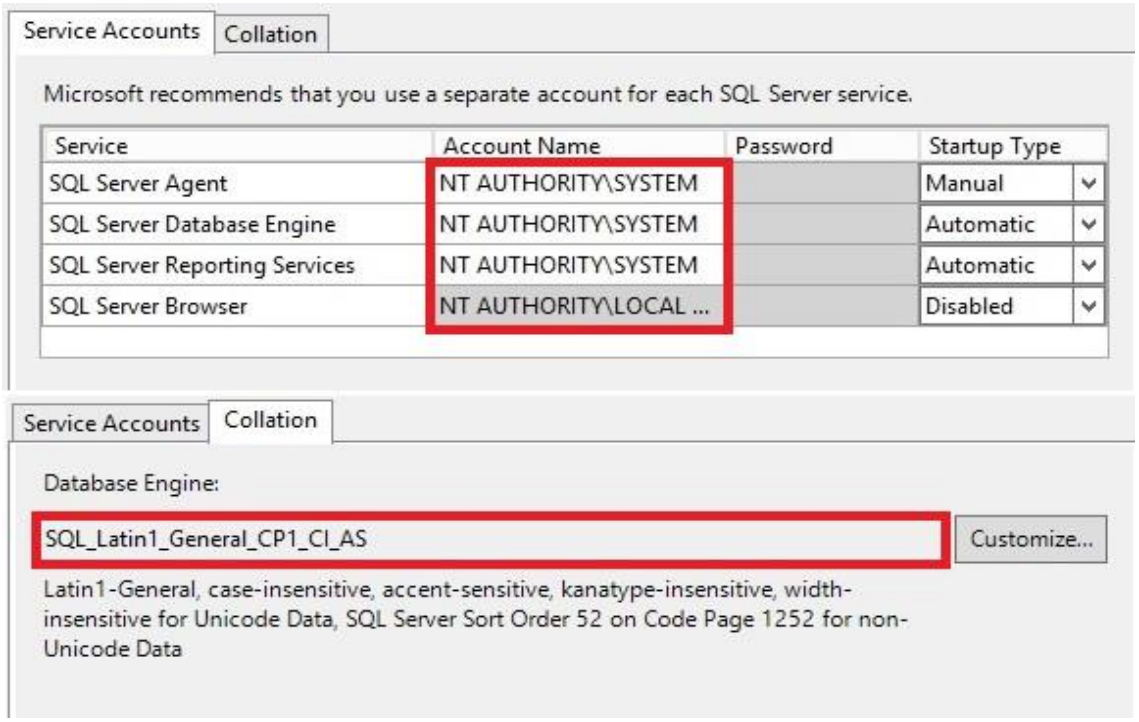


KUVA 5. Kuvakaappaus SQL Server -tuotetunnuksen määrittämisestä

Asennus jatkuu hyväksymällä käyttöoikeudet, minkä jälkeen valitaan mitä SQL Serverin ominaisuuksia asennetaan. Tässä tapauksessa on tarpeetonta asentaa kaikkia ominaisuuksia, joten valitaan ylin kohta SQL Server Feature Installation. Seuraavaksi valitaan ne ominaisuudet, jotka halutaan asentaa. Listassa on useita eri ominaisuuksia eri käyttötarpeisiin, tässä tapauksessa asennetaan vain Database Engine Services, Reporting Services - Native sekä Management Tools - Basic ja Management Tools - Complete. Ominaisuuksien lisäys jälkikäteen on mahdollista, jos niitä tarvitaan.

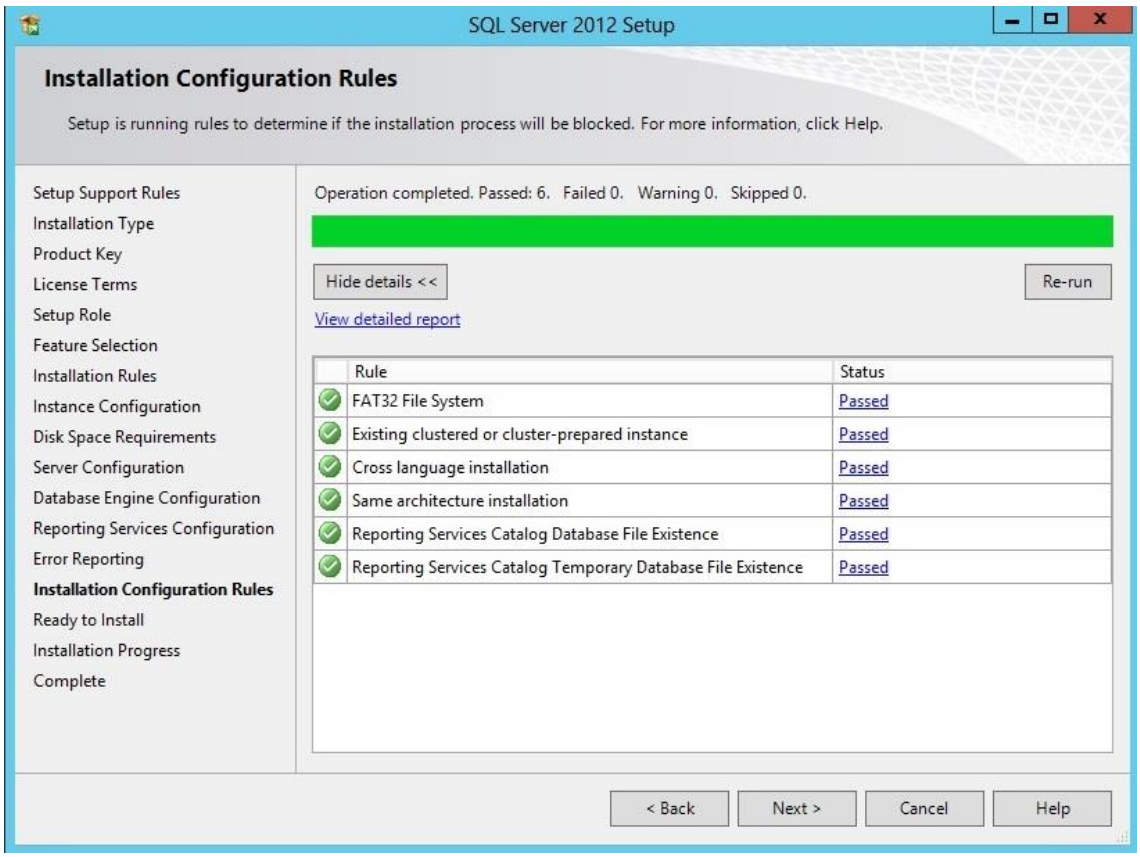
Installation Rules -välilehdellä on taas tarkistus, voidaanko asennusta jatkaa. Kun nämä on hyväksytty, siirrytään määrittelemään SQL Server -instanssia. Instanssille voidaan määritellä nimi ja ID, mutta testiympäristössä oletusasetukset ovat riittäviä. Seuraava välilehti näyttää kovalevytilavaatimukset, minkä jälkeen tullaan Server Configuration -välilehdelle, jossa on erittäin tärkeitä asetuksia. Logon-tili SQL Server servicelle ei voi olla paikallinen käyttäjätili, NT SERVICE\<sql-palvelunimi> tai LOCAL SERVICE. SQL Server Service täytyy konfiguroida käyttämään oikeaa toimialueen tiliä,

NETWORK SERVICEÄ tai LOCAL SYSTEMIÄ. Collation-välilehdellä on niin ikään tärkeä asetus, eli siinä tulee käyttää SQL_Latin1_General_CP1_CI_AS -merkistöä. Nämä asetukset ovat välttämättömiä myöhemmin asennettavan SCCM:n kannalta (kuva 6).



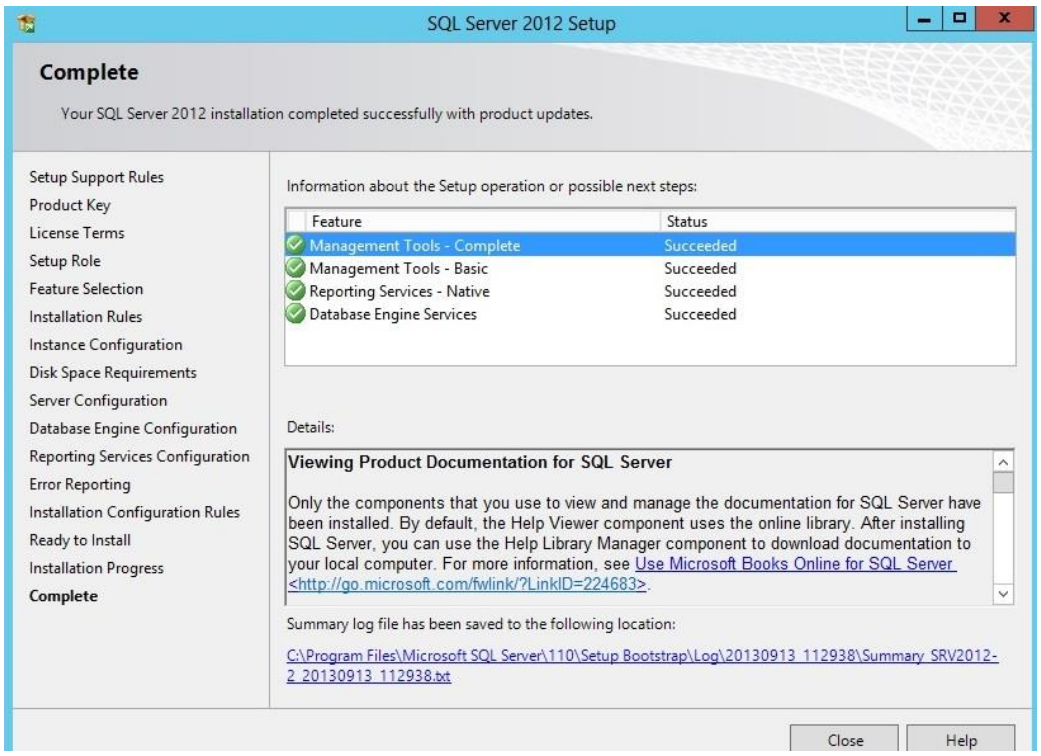
KUVA 6. Kuvakaappaus tilien ja collationin asetuksista

Database Engine Configuration -välilehdeltä määritellään autentikointitapa ja tilit, jotka voivat hallita SQL Serveriä. Windows authentication -moodi, joka oletuksena on valittuna, on riittävä. Hallinointitileihin lisätään nykyinen käyttäjä, joka tässä tapauksessa on EPTESTIDOMAIN\Administrator, mutta siihen voidaan lisätä myös muita käyttäjiä, joille halutaan antaa SQL Serverin hallintaoikeudet. Seuraavaksi määritellään Reporting Services Configuration mode, jossa valitaan oletuksena oleva Install and configure. Virheiden raportoinneista voidaan valita käytettäväksi asetus, jolloin virheraportit lähetetään Microsoftille tai yrityksen raportointipalvelimelle. Installation Configuration Rules -välilehdellä tarkistetaan jälleen, voidaanko asennusta jatkaa (kuva 7).



KUVA 7. Kuvakaappaus Installation Configuration Rules -välilehdestä

Ready to install -välilehdelle tultaessa kaikki asetukset on jo määritelty. Kertauksen vuoksi näytetään yhteenveto valituista asetuksista ja asennus on valmiina aloitettavaksi. Install-nappia painamalla itse asennus käynnistyy. Jos kesken asennuksen asennusohjelma huomauttaa NetFx3:n käyttöönotosta, sen voi helposti ottaa käyttöön komentoriviltä komennolla dism /online /enable-feature /featurename:netfx3 /all /source:d:\sources\sxs. Tällöin edellytyksenä on, että D-asema on DVD-asema, jossa on Windows Server 2012 -asennuslevy sisällä. Kun asennus on valmis, ohjelma vielä ilmoittaa, että asennus on suoritettu onnistuneesti (kuva 8).



KUVA 8. Kuvakaappaus SQL Serverin asennuksesta valmiina

4.2.2 System Center 2012 Configuration Manager SP1

SQL Serverin onnistuneen asennuksen jälkeen voidaan aloittaa SCCM:n asennus. Koska SCEP on täysin integroitu SCCM:iin ja kaikki SCEP:n asennukseen sekä hallintaan liittyvät toiminnot suoritetaan SCCM:n avulla, on luonnollisesti asennettava SCCM ennen SCEP:n käyttöönottamista. Asennusvaiheessa on jälleen huomioitava muutama tärkeä kohta ohjelmistojen oikein toimimiseksi. SCCM:n asennus voidaan aloittaa käynnistämällä asennusohjelma ja valitsemalla aukeavasta ikkunasta Install.

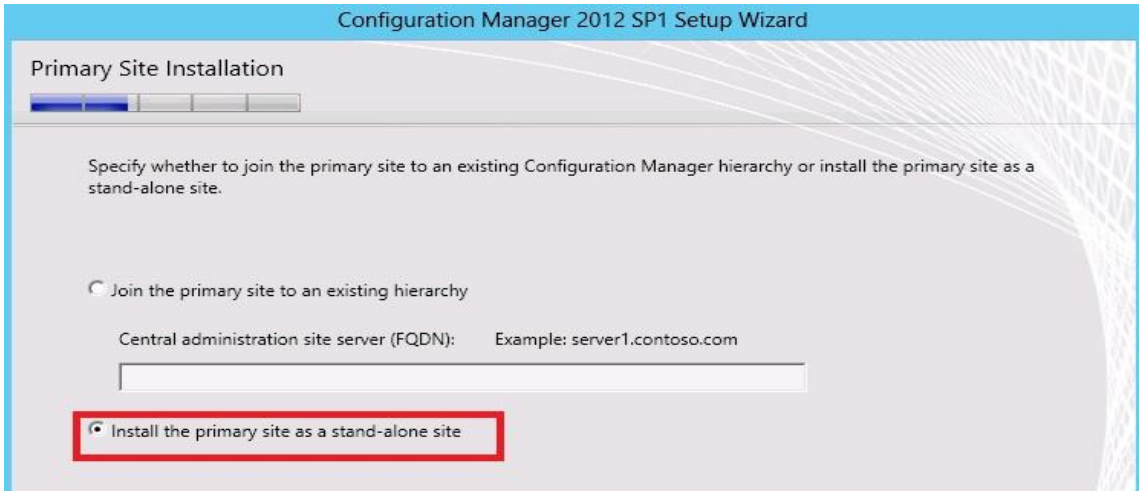
Ensimmäisenä valitaan asennettavan siten tyyppi. Primary siten asennus on oikea vaihtoehto molempiin ympäristöihin, mikä on oletuksena valittuna. Seuraavaksi valitaan tuotetunnus. Testiympäristössä asennetaan kokeiluversio, mutta WPK-verkkoon asennettaessa annetaan ostetun tuotteen mukana tullut tuotetunnus, samoin kuin SQL Serverinkin asennuksessa (kuva 9).

KUVA 9. Kuvakaappaus SCCM-tuotetunnuksen määrittämisestä

Seuraavat kaksi välilehteä käsittelevät lisenssiehtoja, jotka asennuksen jatkamiseksi on hyväksyttävä. Sen jälkeen asennusohjelma kysyy tarvittavista esivaatimustiedostoista, joita tarvitaan asennuksen jatkamiseksi. Jos Internet-yhteys on toiminnassa, voidaan määritellä polku, johon tiedostot ladataan. Ne voidaan myös ladata etukäteen, jolloin syötetään polku, jossa ne sijaitsevat. Kahdella seuraavalla välilehdellä kysytään SCCM-palvelimen ja client-ohjelmien kieliasetuksista. Molemmissa on oletuksena englanti, joten ne ovat kunnossa. Site and Installation Settings -välilehdellä valitaan site-koodi, siten nimi ja asennuskansio. Samoin valitaan Configuration Manager consolen asennus. Testiympäristössä koodiksi annettiin EP1 ja nimeksi EP Testi Site. Asennuskansio voidaan pitää oletuksena (kuva 10).

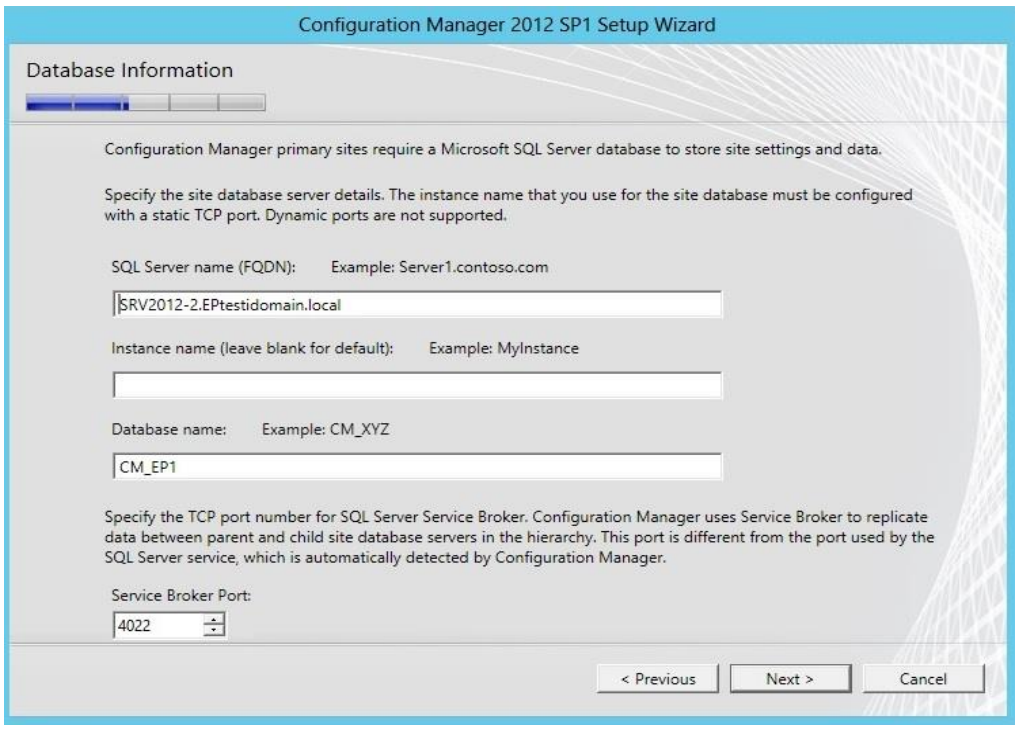
KUVA 10. Kuvakaappaus siten asetusten määrittämisestä

Tässä vaiheessa määritellään, liitetäänkö asennettava primary site olemassa olevaan hierarkiaan vai luodaanko stand-alone site (kuva 11). Olemassa olevaa hierarkiaa ei tietenkään puhtaaseen ympäristöön asennettaessa ole, joten valitaan stand-alone site. Stand-alone siten asennus on varsin riittävä sekä testiympäristöön että WPK-verkkoon, sillä ympäristöt ovat suhteellisen pieniä, eikä tarvetta suuremmalle hierarkialle ole. Kuitenkin, jos verkkoa päätetään laajentaa myöhemmin, voidaan stand-alone site liittää jälkikäteenkin hierarkiaan, jolloin joudutaan asentamaan myös Central Administration Site.



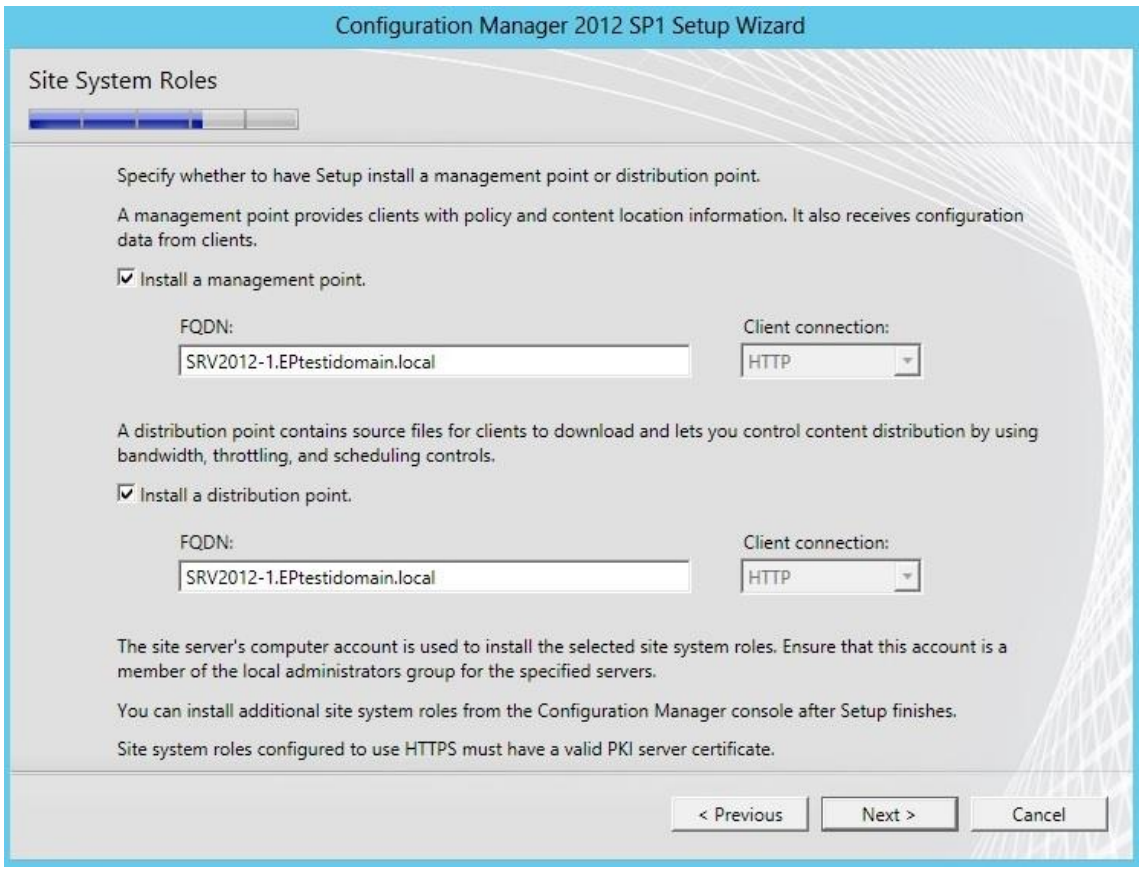
KUVA 11. Kuvakaappaus stand-alone siten valinnasta

Seuraavana määritetään SCCM:n käyttämät tietokanta-asetukset. SCCM käyttää Microsoft SQL Serverin tietokantaa. SQL Server name -kohtaan annetaan SQL Server -palvelimen FQDN-nimi, joka testiympäristössä on SRV2012-2.EPtestidomain.local. Vastaavasti WPK-verkossa annetaan palvelimen nimeksi se palvelin, johon SQL Server on asennettu. Instanssin nimen voi jättää tyhjäksi, jolloin se on oletusarvo. Tietokannan nimi on oletuksena CM_<site-koodi>, joka tässä tapauksessa on EP1. Nämä asetukset voivat jäädä oletuksiksi, jos ei haluta erikseen antaa selventävää nimeä, mikä on toki suositeltavaa, jos esimerkiksi SQL Serverillä on paljon muitakin käyttötarkoituksia ja tietokantoja. Huomioi myös käytettävä Service Broker -portti 4022, joka sallittiin palomuurista. Kuvassa 12 näkyy tietokanta-asetusten määritykset.



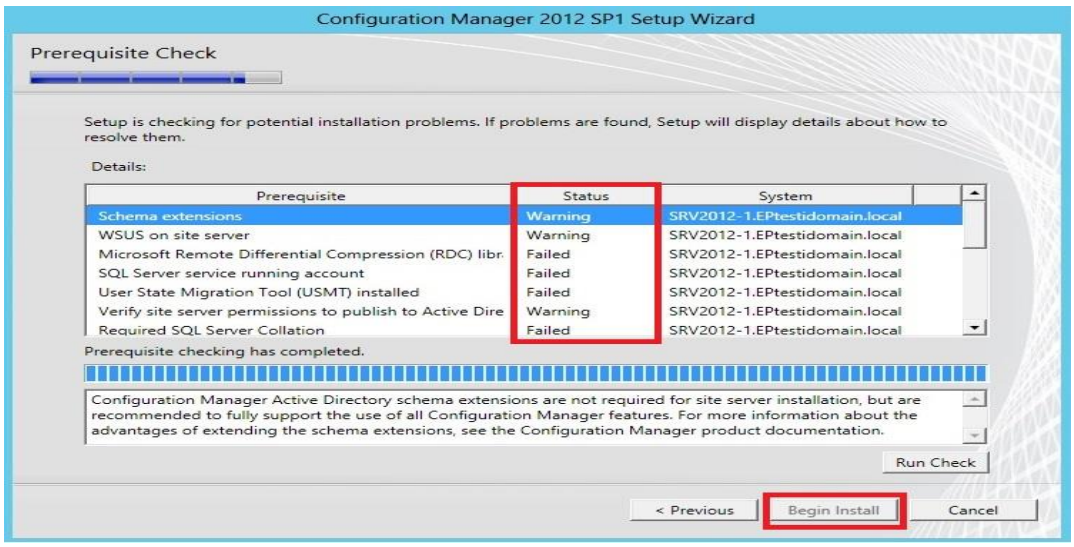
KUVA 12. Kuvakaappaus SCCM:n tietokanta-asetuksista

SMS Provider Settings -välilehdellä määritetään käytettävä SMS-provider. SCCM-konsoli käyttää SMS provideria kommunikointiin siten tietokannan kanssa. Tähän sopii hyvin SCCM-palvelin itsessään, eli testiympäristössä SRV2012-1 ja WPK-verkossa se palvelin, johon SCCM päätetään asentaa. Client Computer Communication Settings -välilehdellä voidaan päättää, käytetäänkö client-yhteyksissä HTTP- vai HTTPS-protokollaa. HTTP-protokolla on riittävä, joten valitaan Configure the communication method on each site system role. Site system -roolien asennukset tulevat seuraavalla välilehdellä, jossa määritellään management point- ja distribution point -roolien palvelimet (kuva 13). Testiympäristössä asennetaan molemmat samalle SCCM-palvelimelle (SRV2012-1). WPK-verkossa voidaan asentaa myös samalle tai mahdollisuuksien mukaan hajauttaa muillekin palvelimille riippuen siitä, kuinka paljon palvelimia SCCM-ympäristöön otettaisiin mukaan.



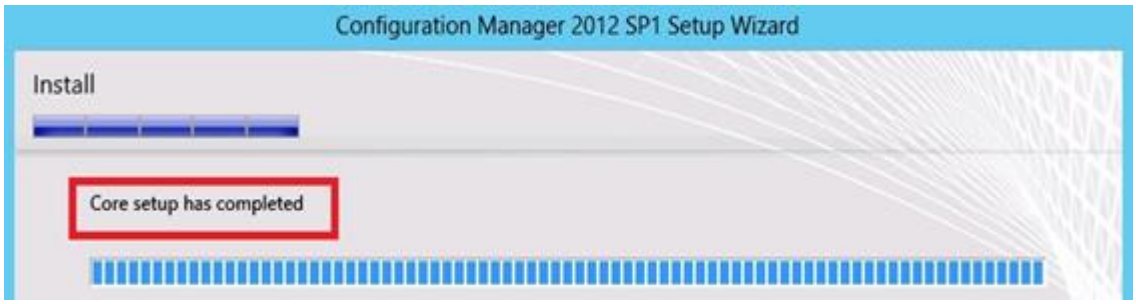
KUVA 13. Kuvakaappaus Site System -roolien asetuksista

Asetusten määrittäminen alkaa olla lopuillaan. Vielä valitaan, liitytäänkö Customer Experience Improvement Programiin, joka kerää nimettömästi tietoa tietokoneesta ja SCCM-käytöstä ja lähettää sitä Microsoftille. Ennen asennuksen aloitusta näytetään vielä yhteenveto valituista asetuksista, minkä jälkeen tulee viimeisenä esivaatimusten tarkistus. Tässä ikkunassa näkyvät puuttuvat esivaatimukset, jos sellaisia on jostain syystä jäänyt asentamatta. Varsinaista asennusta ei voida aloittaa ennen kuin esivaatimukset on täytetty, eikä listassa ole yhtään vaatimusta Failed-tilassa. Tästä syystä työssä on käyty läpi erikseen esivaatimukset. Kuvassa 14 on havainnollistettu asiaa esimerkin vuoksi yrittämällä asentaa SCCM ennen kuin esivaatimukset ovat kunnossa.



KUVA 14. Esivaatimusten tarkistus – kuvakaappaus ennen esivaatimusten asennusta

Kun vaatimukset ovat kunnossa, aloitetaan asennus. Ohjelma vielä ilmoittaa, kun asennus on suoritettu onnistuneesti, minkä jälkeen ikkuna voidaan sulkea. Asennuksesta voidaan katsoa loki-tiedosto, jos halutaan tarkempaa informaatiota asennetuista osista. Tässä vaiheessa kuitenkin tarpeelliset asennukset on tehty, joten voidaan aloittaa SCEP:n asennus ja konfigurointi. Kuvassa 15 SCCM on asennettu onnistuneesti.



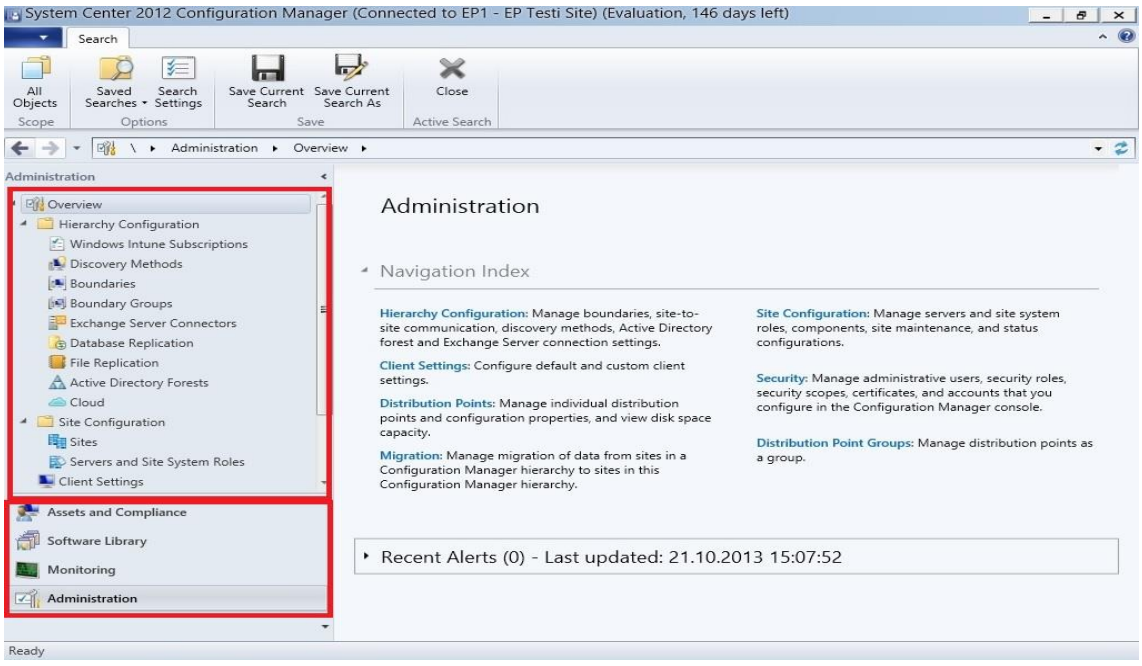
KUVA 15. Kuvakaappaus SCCM:n asennuksesta valmiina

5 KONFIGUROINTI JA SCEP:N KÄYTTÖÖNOTTO

5.1 SCCM:n yleinen konfigurointi

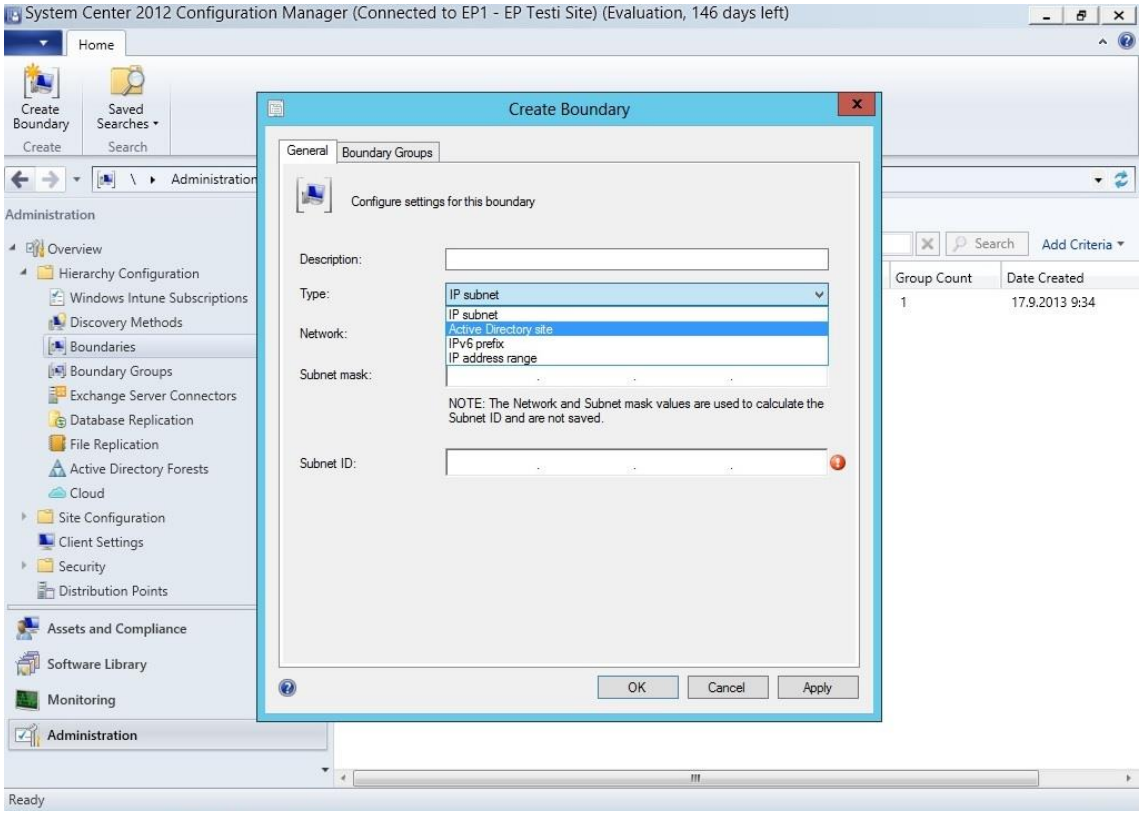
SQL Serverin ja SCCM:n asennusten jälkeen päästään pikku hiljaa itse asiaa kohti, eli SCEP:n käyttöönottoon ja konfigurointiin. SCCM sisältää itsessään SCEP:n, joka asennetaan SCCM:n käyttöliittymän kautta yhtenä site system -roolina. Itse asennus siis ollaan tehty erittäin helpoksi, mutta täyden toiminnan kannalta konfiguroitavaa on huomattavasti enemmän. Ennen SCEP:n varsinaista käyttöönottoa on syytä konfiguroida muutama kohta SCCM:sta.

SCCM:ssa on neljä eri päävalikkoa, jotka sijaitsevat vasemmassa alakulmassa. Ylimmäisenä on Assets and Compliance, jossa näkyvät laitteet ja käyttäjät, sekä tuleva Endpoint Protection -rooli, toisena Software Library, jossa ovat ohjelmistoihin ja niiden päivityksiin liittyvät asiat, kolmantena Monitoring, josta voidaan valvoa hälytyksiä ja raportointeja sekä esimerkiksi SCEP:n tilaa, ja viimeisenä Administration, jossa sijaitsevat hallinnolliset asiat koskien esimerkiksi hierarkiaa, siteä ja rooleja. Päävalikoiden yläpuolelle tulevat näkyviin alavalikot siitä päävalikosta, joka on valittuna. Kuva 16 havainnollistaa SCCM:n käyttöliittymää.



KUVA 16. Kuvakaappaus SCCM:n yleisnäkymästä

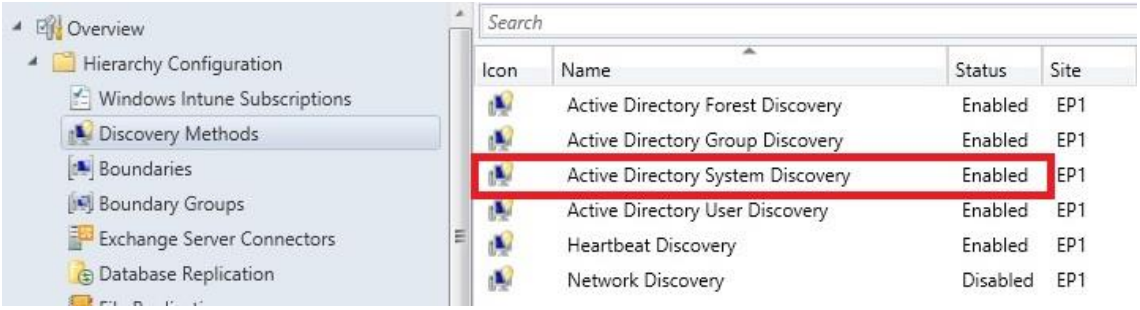
Ensin konfiguroidaan Administration-päävalikosta Boundaries-kohta. Boundary eli raja on laitteita sisältävä verkkoryhmä sisäverkossa, ja se voidaan määrittää IP-aliverkon, AD-siten, IPv6-prefixin tai IP-osoitevälin mukaan (Planning for Boundaries and… 2013). Tässä tapauksessa toimiva vaihtoehto on AD-siten perusteella määrittäminen, niin testiympäristössä kuin WPK-verkossakin, sillä molemmat sisältävät vain yhden AD-siten, ja siksi sen perusteella voidaan löytää kaikki toimialueeseen kuuluvat laitteet. Rajat voidaan liittää myös osaksi Boundary Groupia eli rajaryhmää, joka voi sisältää useita boundaryjä. Boundary Group luodaan Boundary Groups -alavalikosta Boundary-valikon alapuolelta. Samassa ryhmän luonnin yhteydessä liitetään se käytettävään siteen References-välilehdeltä. Kuvassa 17 luodaan raja AD:n siten perusteella.



KUVA 17. Kuvakaappaus rajan luomisesta

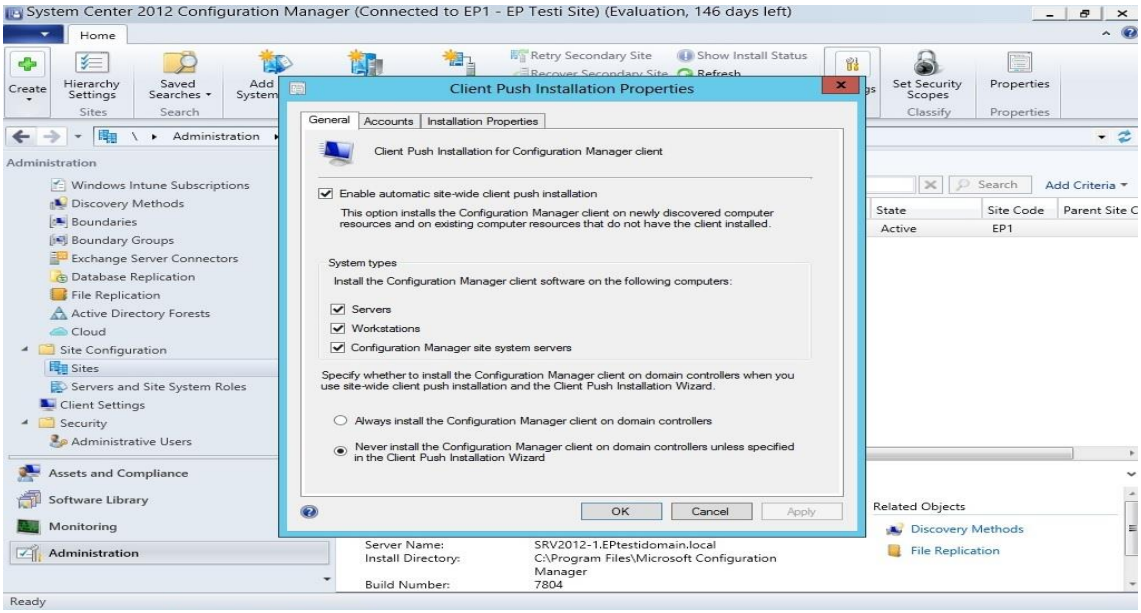
Rajojen ja rajaryhmien määrittämisen jälkeen tutkitaan saman alavalikon alta SCCM:n asetuksia, jolla se etsii resursseja AD:sta. Discovery Methods -alakohdasta laitetaan päälle Active Directoryn Discovery-asetukset, jolloin AD:n resurssit löydetään SCCM:n käytettäväksi (kuva 18). Tärkeimpänä kohtana otetaan käyttöön Active Directory System Discovery, joka etsii AD:n tietokoneet ja määritellään, mistä niitä etsitään. Tässä tapauksessa etsitään Computers-containerista, jossa kaikki AD:n tietokoneet

sijaitsevat. Etsinnän jälkeen löydetyt laitteet tulevat näkyviin Assets and Compliance -päävalikon Devices-kohtaan.



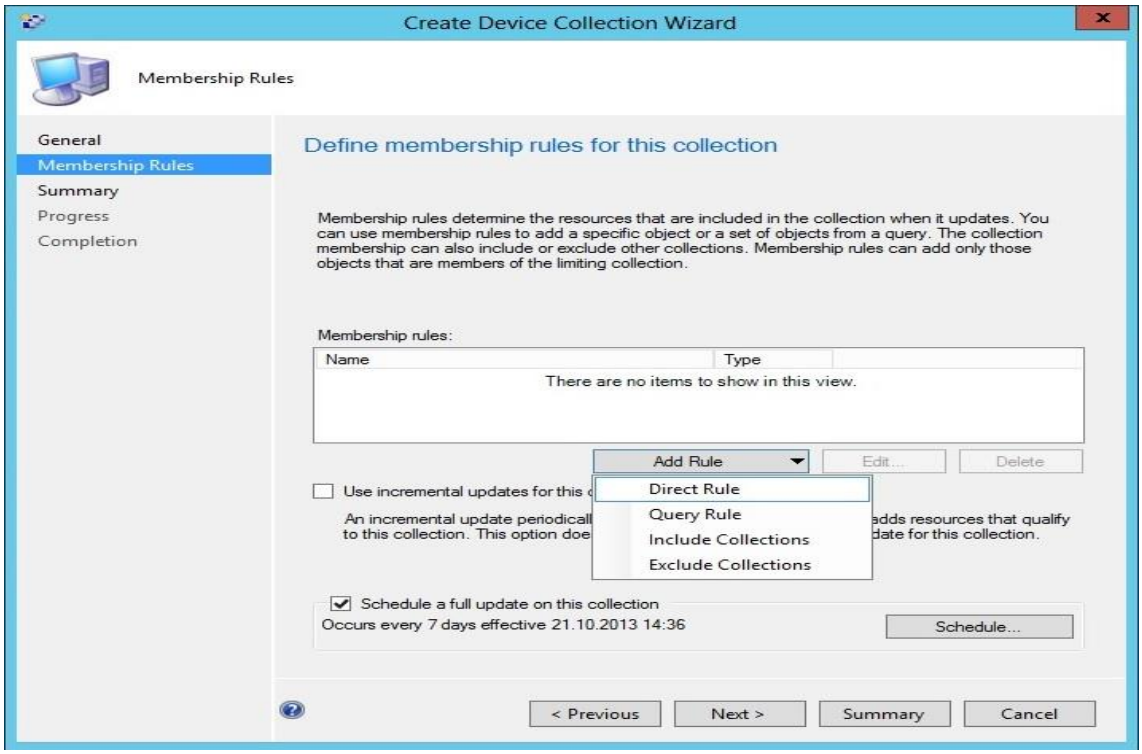
KUVA 18. Kuvakaappaus Discovery Methods -asetuksista

Päätelaitteille täytyy asentaa SCCM:n client-ohjelma, jotta niitä voidaan hallita täysin SCCM:n avulla. Asennus tapahtuu push-asennuksena, jossa SCCM:llä ”pusketaan” ohjelmiston asennus laitteille. Tarkastellaan hieman push-asennuksen asetuksia, joihin päästään Administration-valikon kautta navigoimalla kohtaan Site Configuration - Sites ja sieltä valitaan oma site. Ohjelman yläriviltä valitaan Settings - Client installation Settings - Client Push Installation. Asetuksista voidaan määrittää muun muassa minkä tyyppisille tietokoneille ohjelma asennetaan (kuva 19). Kun asetukset on määritetty, voidaan SCCM-client asentaa halutulle laitteelle tai laitekokoelmalle Assets and Compliance -valikon kautta valitsemalla haluttu ryhmä ja Install Client.



KUVA 19. Kuvakaappaus SCCM-clientin asetuksista

Tässä vaiheessa on myös hyvä tehdä jo valmiiksi löydetyistä laitteista halutut kokoelmat. Kokoelmat ovat nimensä mukaisesti ryhmiä, jotka sisältävät useita laitteita. Ne voidaan määrittää lukuisilla eri perusteilla, esimerkiksi käyttöjärjestelmän tai tietokoneen nimen mukaan. Koska toimeksiannossa haluttiin, että WPK-verkossa otetaan SCEP käyttöön aluksi yhdellä luokalla, otetaan esimerkiksi kokoelman luominen tietylle luokalle. Kokoelmien luominen tapahtuu Assets and Compliance -valikosta, Device Collections -alavalikon alta. Määritelmät tehdään eri sääntöjen avulla. Sääntöjen tekemisessä voidaan käyttää Query Ruleja, jotka ovat dynaamisia, eli lisäävät koneita kokoelmaan automaattisesti sitä mukaa, kun kriteerit täyttyvät ja vastaavasti poistavat, kun kriteereitä ei enää täytetä. Direct Rulessa sen sijaan määritellään manuaalisesti, mitkä koneet kokoelmaan kuuluvat. Kuvassa 20 valitaan sääntötyyppi, jolla määritetään kokoelman koneiden kriteerit.



KUVA 20. Kuvakaappaus kokoelman luonnista

WPK-verkossa työasemat on nimetty käyttöjärjestelmän (Windows 7) ja luokan mukaan, esimerkiksi A3-21 -luokan työasemat on nimetty WA321-alkuisesti. Tämän vuoksi on helppo tehdä kokoelma, jonka sääntönä käytetään esimerkiksi Query Rulea, jossa määritelmänä on työaseman nimi ja arvona WA321%, jossa %-merkki korvaa mitkä tahansa merkit. Kyseinen sääntö siis ottaa nimeltään WA321-alkuiset tietokoneet

kokoelmaan, joten samalla periaatteella kaikkien WPK-verkon luokkien määrittäminen eri kokoelmiin on hyvin helppoa. WPK-verkossa kannattaa myös tehdä kokoelmat erikseen palvelimia varten, sillä niiden hallinta on yleensä erilaista kuin työasemien. Tässä tapauksessa erona on se, että niille jaetaan eri SCEP-politiikka kuin työasemille.

5.2 SCEP:n konfigurointi ja käyttöönotto

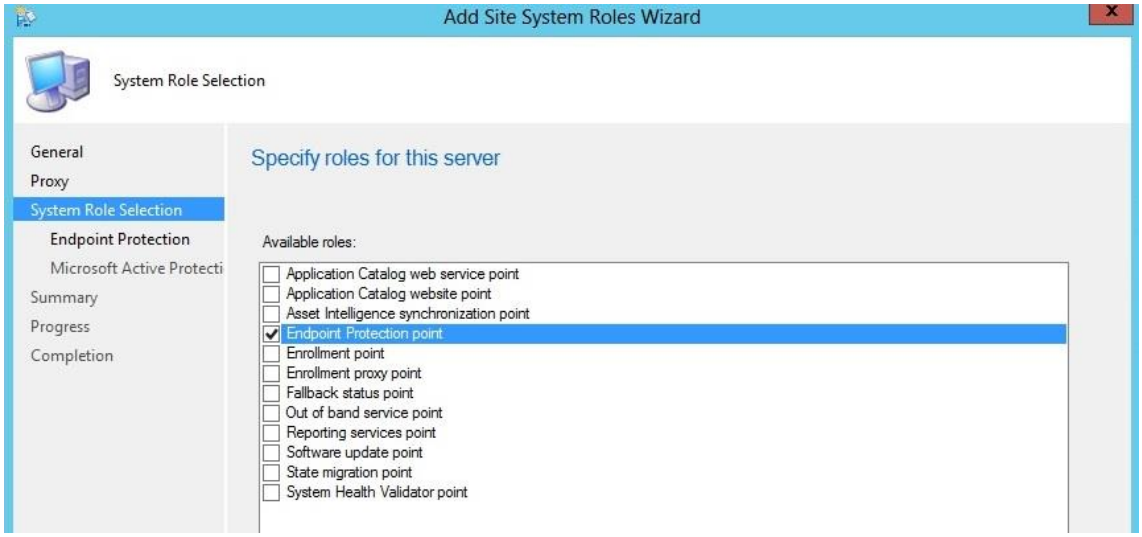
Tässä vaiheessa tarvittavat yleiset ympäristövalmistelut on tehty SCCM:ssa, jotta voidaan alkaa tutkia itse SCEP:in konfigurointia ja käyttöönottoa. SCEP:n käyttöönotto oli koko työn päätarkoitus, ja sen asennusta piti tutkia WPK-verkkoon sopivaksi. Siksi tässäkin vaiheessa on keskitytty miettimään toimintaa ja asennuksen eri vaiheita WPK-verkossa, vaikka itse asennus tehtiinkin testiympäristöön.

Suurimmilta osin asennukset ovat samanlaisia sekä testiympäristöön että oikeaan tuotantoympäristöön. Asetuksissa, kuten kokoelmien ja politiikkojen määrittämisessä tulee kuitenkin olla tarkkana. Testiympäristössä käytettiin vain kahta työasemaa ja palvelinta, mutta WPK-verkossa niitä on yli sata, joten useampien kokoelmien sekä politiikkojen määrittäminen laiteryhmille on välttämätöntä. Politiikkojen sisältöönkin tulee kiinnittää huomiota, sillä SCEPin ei haluta käyttäytyvän samalla tavalla esimerkiksi palvelimilla ja työasemilla.

5.2.1 SCEP-roolin käyttöönotto

Nyt voidaan ottaa käyttöön itse SCEP-rooli. SCEP-rooli asennetaan SCCM:n käyttöliittymästä kuin mikä tahansa site system -rooli. Administration-valikossa navigoidaan kohtaan Site Configuration - Servers and Site System Roles, jossa valitaan haluttu palvelin SCEP-roolille. Tässä tapauksessa asennettiin samalle palvelimelle, kuin muutkin SCCM-roolit (SRV2012-1), mutta WPK-verkossa voidaan asennusta hajauttaa riippuen siitä, kuinka monta palvelinta otetaan mukaan ympäristöön. Asennus käynnistyy painamalla hiiren oikealla näppäimellä palvelinta ja valitsemalla Add Site System Roles.

Wizard on hyvin yksinkertainen. Asetukset ovat oletuksena jo niin kuin pitääkin. System Role Selection -välilehdellä valitaan vain rasti kohtaan Endpoint Protection point (kuva 21), minkä jälkeen hyväksytään käyttöehdot ja päätetään, liitytäänkö Microsoftin MAPS-palveluun, jossa lähetetään tietoa ohjelmasta Microsoftille. Lopuksi näytetään yhteenveto, minkä jälkeen asennus aloitetaan ja ilmoitetaan, kun se on valmis.



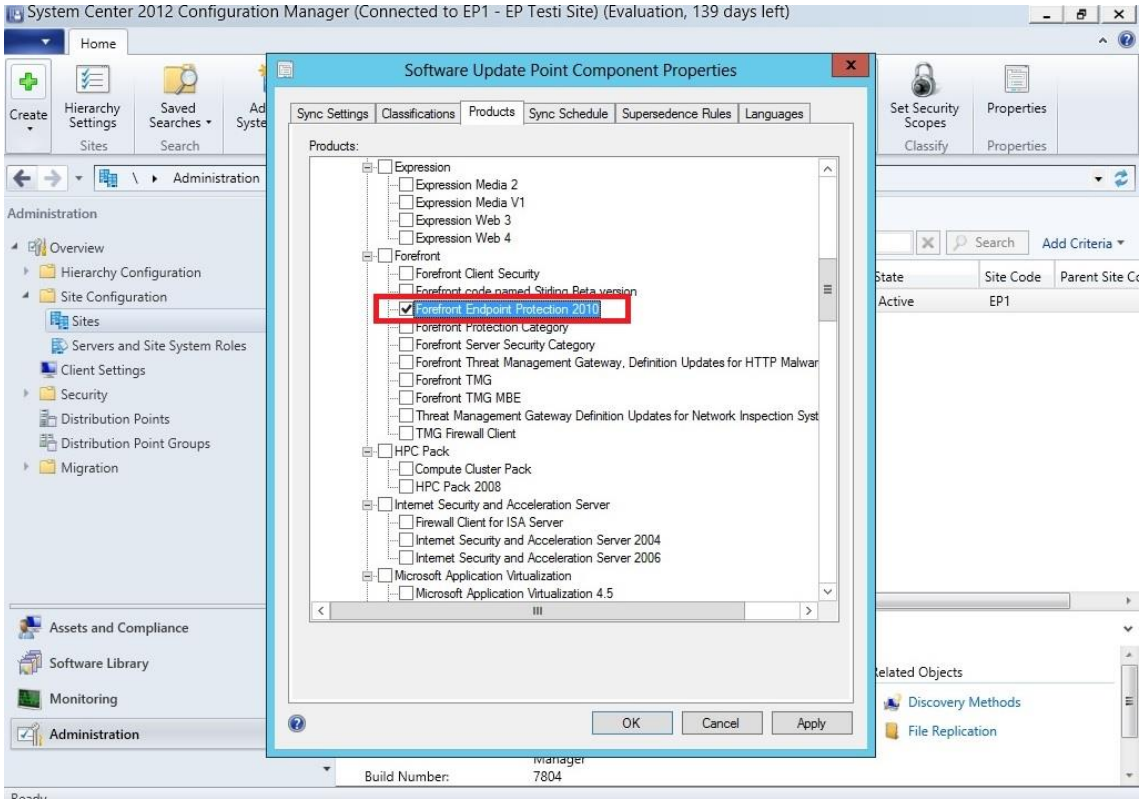
KUVA 21. Kuvakaappaus Add Site System Roles Wizardin Site System -roolien valinnasta

5.2.2 Virustietokantapäivitykset

Uhkien torjumisen kannalta on tärkeää, että SCEP pysyy ajan tasalla. Sen on saatava uusimmat virustietokantapäivitykset (definition files) automaattisesti, sillä niitä päivitetään hyvin usein. Manuaalisesti niiden lataaminen ja asentaminen on hyvin työlästä. Onneksi SCCM tarjoaa tähän tehokkaan keinon, jonka avulla ylläpito helpottuu huomattavasti. Päivitykset voidaan toteuttaa ADR:n (Automatic Deployment Rules) avulla. ADR:t ovat sääntöjä, joiden perusteella ladataan tietyt kriteerit täyttävät ohjelmistopäivitykset. Tässä tapauksessa niitä käytetään virustietokantapäivitysten lataamiseen.

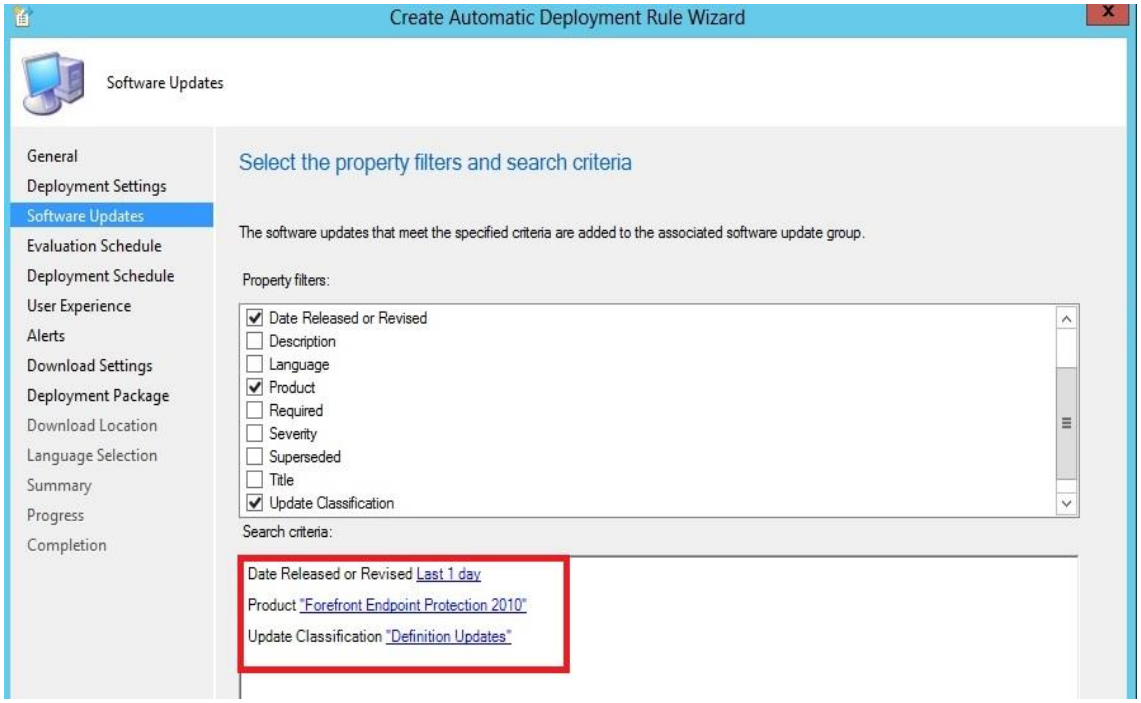
Ensin on varmistettava, että SCCM-palvelimella on asennettuna myös Software update point -rooli. Rooli asennetaan täysin samalla tavalla kuin Endpoint Protection point -roolikin eli Add Site System Roles Wizardin kautta, mutta valitaan System Role

Selection -välilehdeltä Endpoint protection pointin sijaan Software update point (kuva 21). Sen jälkeen navigoidaan Administration-välilehdelle, josta valitaan siten Configure Site Components -asetuksista Software Update Point. Sieltä valitaan Products-välilehti, josta valitaan vielä vanhalla nimellä oleva Forefront Endpoint Protection 2010, jolloin päivitysten lataaminen ADR:n kautta on mahdollista. Kuvassa 22 näkyvät Software update point -roolin valittavat asetukset.



KUVA 22. Kuvakaappaus Software update point -roolin asetuksista

Tämän jälkeen voidaan siirtyä ADR:n tekoon, mikä tapahtuu Software Library -valikossa kohdasta Software Updates - Automatic Deployment Rules. ADR:n luonti tehdään wizardia apuna käyttäen. Aluksi luodaan säännölle nimi ja annetaan kohdekokoelma, jolle päivitykset halutaan asentaa. Seuraava tärkeä kohta on Software Updates -välilehti, jolla määritellään etsintäkriteerit päivityksille (kuva 23). Tässä tapauksessa valitaan Date Released or Revised, johon annetaan arvoksi Last 1 day. Listasta valitaan myös Product, johon arvoksi annetaan Forefront Endpoint Protection 2010 ja Update Classification, johon arvoksi annetaan Definition Updates. Näin sääntö osaa automaattisesti etsiä uusia virustietokantapäivityksiä SCEP:iin.



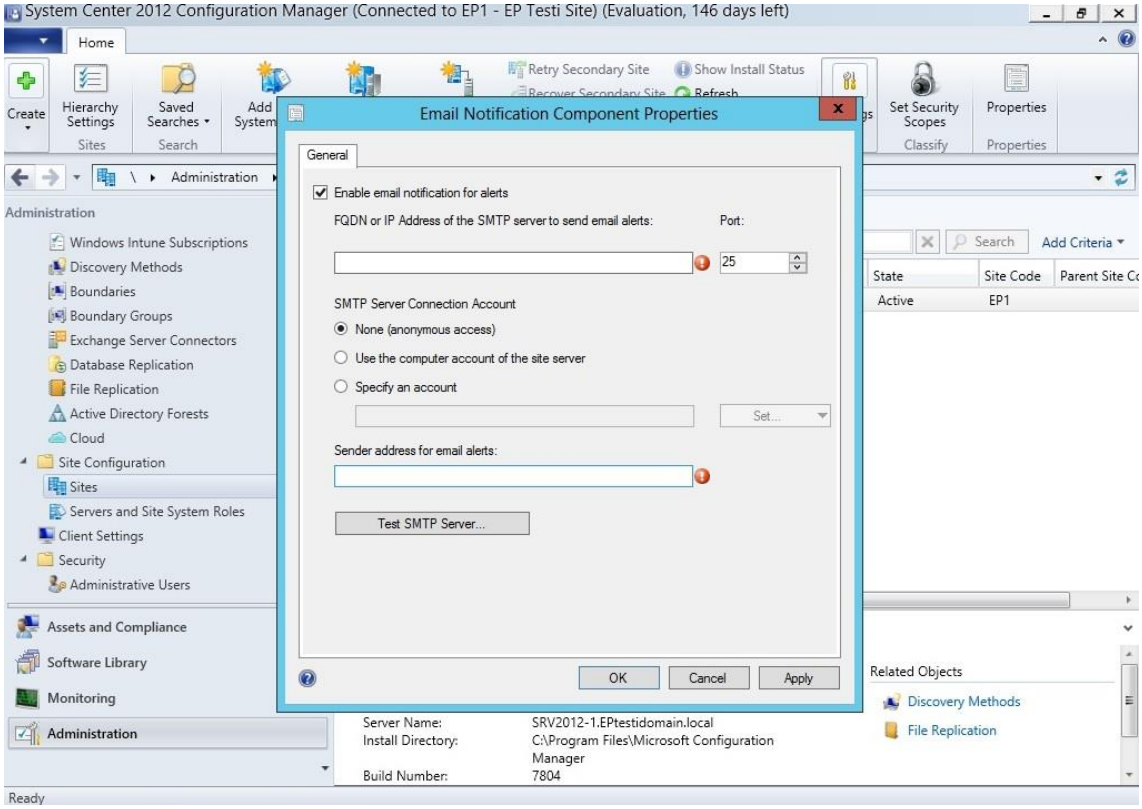
KUVA 23. Kuvakaappaus ADR:n luonnista – ladattavien päivitysten määrittäminen

Seuraavana wizard kysyy vielä aikatauluasetuksia luodulle säännölle, esimerkiksi milloin sääntö toteutetaan ja milloin löydetyt päivitykset asennetaan. Sääntö pitää suorittaa päivittäin ja jopa paljon useammin kuin kerran päivässä, jolloin kohdelaitteet pysyvät ajan tasalla. Ennen kuin sääntö on valmis, määritetään vielä käyttäjän ilmoitukset, hälytykset, päivitysten latausten asetukset ja valitaan kansio paketille, jonka sääntö luo automaattisesti. Valitaan vielä distribution point, johon ADR replikoidaan ja päätetään, mistä päivitykset ladataan. Sitten päätetään kieli, joka on englanti, minkä jälkeen wizard näyttää vielä yhteenvedon asetuksista ja asennuksen voi aloittaa. Kun sääntö on valmis, se tulee näkyviin Software Library -valikon Software Updates -kansion alle kohtaan Automatic Deployment Rules. Myös itse ladatut päivitykset näkyvät jatkossa Software Updates -kansion alla kohdassa All Software Updates.

5.2.3 Hälytysten asetukset

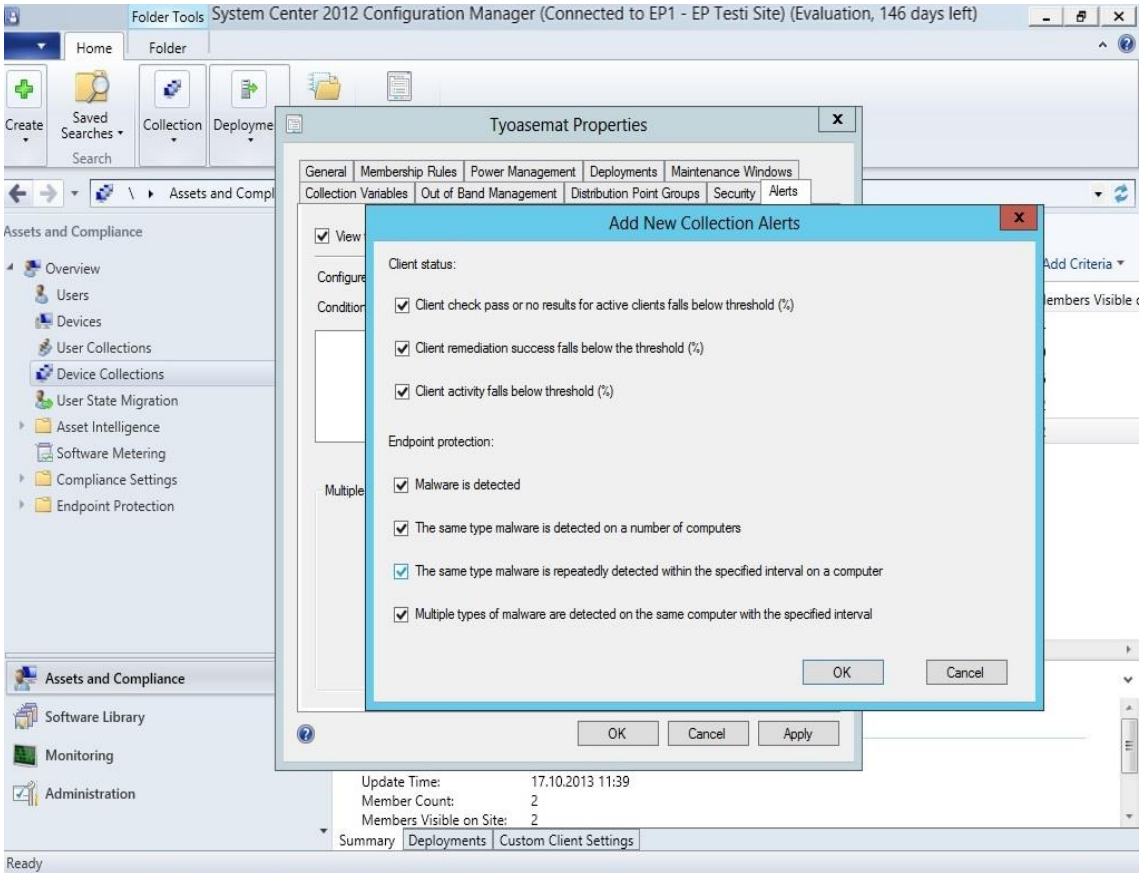
Hälytykset eri tietoturvauhkista voidaan määrittää lähetettäväksi esimerkiksi järjestelmänvalvojan sähköpostiin. Tämä edellyttää, että toimialueessa on käytössä sähköpostipalvelin, joka esimerkiksi WPK-verkossa on. Tietoturvauhkat on tärkeää

huomioida heti, joten sähköposti on siihen hyvä väline Monitoring-välilehden lisäksi. Hälytysten asetukset määritetään Administration-valikon alta. Sieltä valitaan Site, josta valitaan Configure Site Settings ja Email Notification (kuva 24).



KUVA 24. Kuvakaappaus sähköpostihälytysten asetuksista

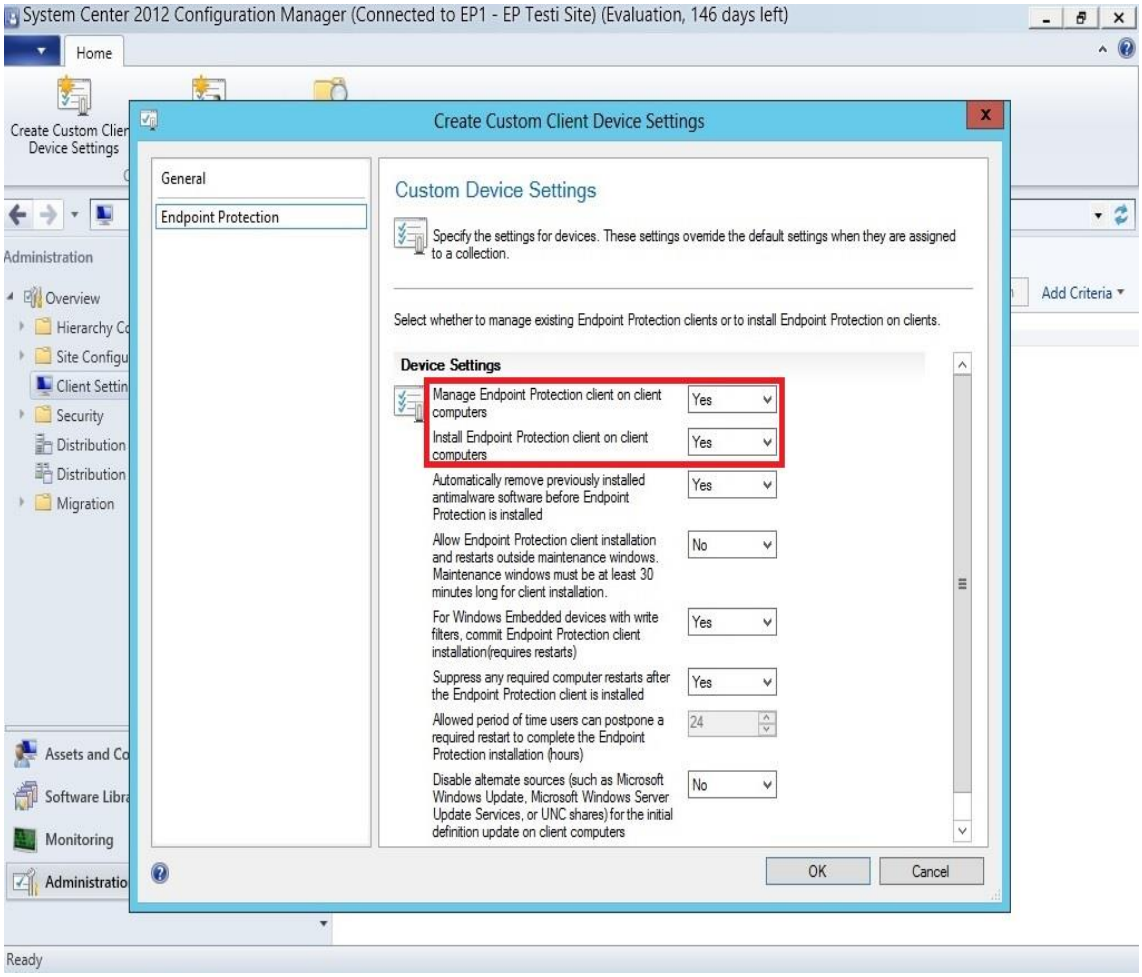
Hälytykset täytyy vielä toimeenpanna haluttuun kokoelmaan. Tämä tapahtuu Assets and Compliance -valikon alta, josta löytyvät kokoelmat laitteista. Esimerkiksi WPK-verkon tapauksessa, kun kokoelma on tehty sisältämään vaikka tietyn luokan koneet, valitaan luokan kokoelmasta ominaisuudet. Ominaisuuksien Alerts-välilehdellä voidaan valita, mistä uhkista tehdään hälytykset (kuva 25). Monitoring-valikon alta kohdasta Alerts - Subscriptions voidaan vielä valita, minkä tyyppisiä hälytyksiä lähetetään sähköpostitse ja mihin osoitteisiin.



KUVA 25. Kuvakaappaus kokoelman hälytysasetuksista

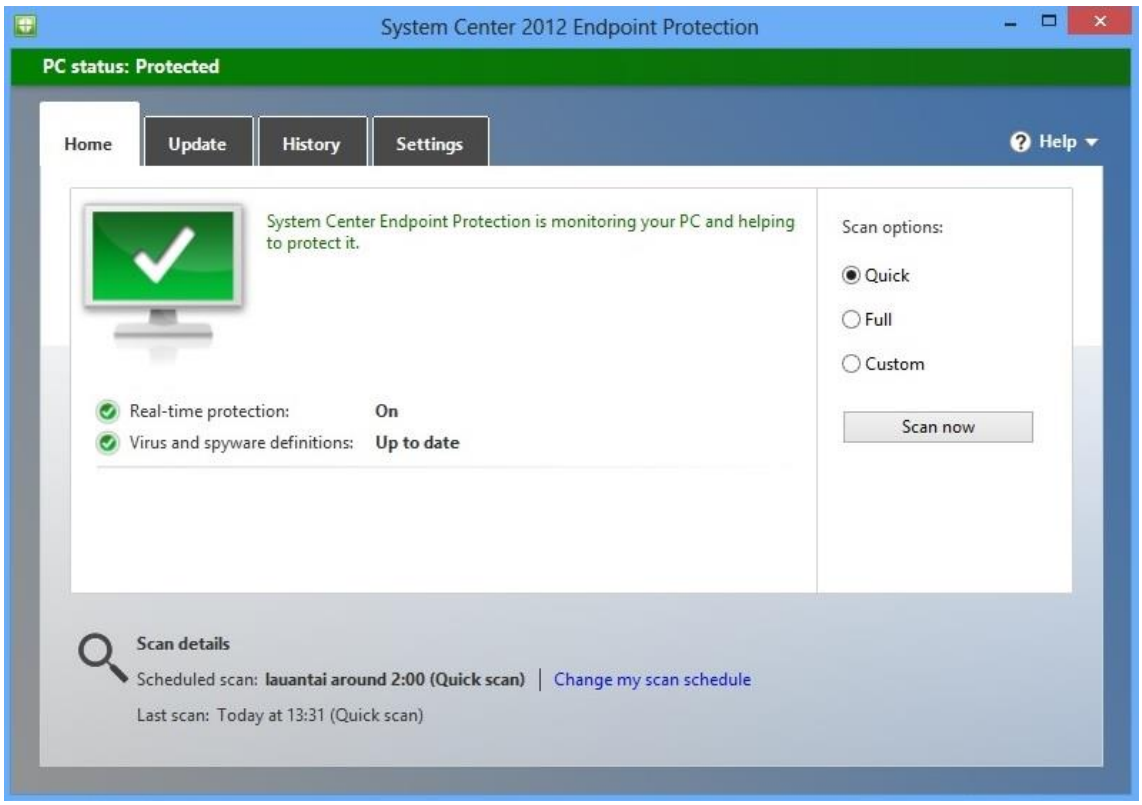
5.2.4 Client-ohjelmien jako ja politiikkojen määrittäminen

SCEP:n client-ohjelman jakaminen päätelaitteille tehdään Administration-valikosta kohdasta Client Settings. Client Settingseille on olemassa oletusasetus, mutta sen käyttöä kannattaa välttää, sillä tuskin on järkevää antaa jokaiselle laitteelle samat asetukset koko toimialueessa. Tehdään siis uusi Client Setting pelkästään SCEP:iä varten. Painetaan Client Settings -kohta aktiiviseksi ja valitaan Create Custom Client Device Settings. General-välilehdellä annetaan asetukselle nimi ja valitaan Endpoint Protection. Wizardin vasempaan reunaan ilmestyvältä Endpoint Protection -välilehdeltä valitaan kaksi ylintä kohtaa käytettäväksi, jolloin asetus mahdollistaa SCEP-clientin asennuksen (kuva 26). Myös muita asetuksia voidaan muokata tarpeen mukaan.



KUVA 26. Kuvakaappaus Client Settingseistä

Kun sääntö on luotu, se tulee näkyviin Client Settings -kohtaan Administration-valikossa. Se pitää vielä toimeenpanna tietylle kokoelmalle, mikä tapahtuu painamalla hiiren oikealla näppäimellä tehtyä sääntöä ja valitsemalla Deploy. Sen jälkeen SCCM kysyy vielä kokoelmaa, johon kyseinen sääntö astuu voimaan. Valitaan haluttu kokoelma, esimerkiksi WPK-verkossa haluttu luokka, ja painetaan OK, jolloin SCEP-clientin asennus alkaa kokoelman laitteille. Kuvassa 27 SCEP-client toiminnassa Windows 8 -työasemalla.

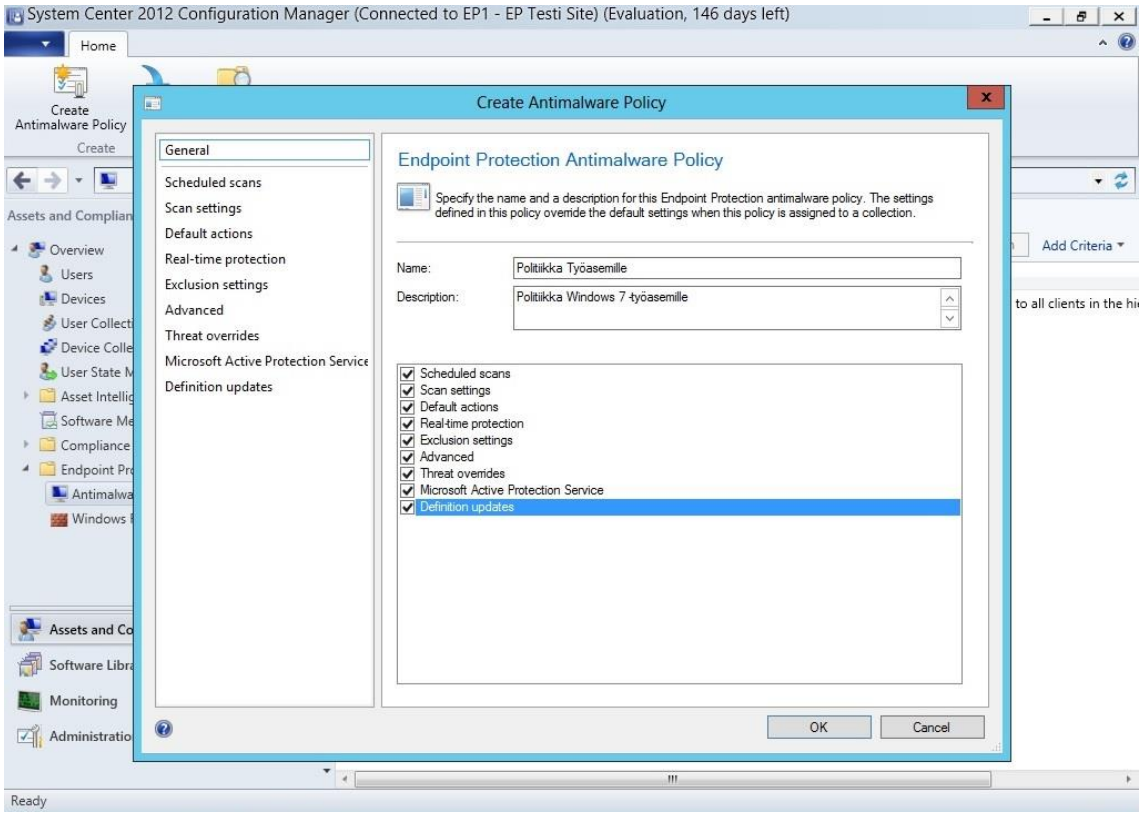


KUVA 27. Kuvakaappaus SCEP-clientista toiminnassa ja ajan tasalla Windows 8 -työasemalla

Politiikat ovat tärkeitä SCEP:n käyttämiä ”asetuskokoelmia”. SCEP:n politiikkojen asetukset ovat Assets and Compliance -valikon kansiosta Endpoint Protection. Kansiosta löytyvät sekä antimalware-politiikat että palomuuripolitiikat. Ohjelmassa on valmiina oletuspolitiikka SCEP:lle, joka tulee käyttöön kaikille. Tämä ei kuitenkaan ole haluttua, sillä eri kokoelmat saattavat tarvita eri politiikkoja. Tästä syystä ei muokata oletuspolitiikkaa käyttöön, vaan luodaan oma politiikka, joka ”yliajaa” oletuspolitiikan. Luotujen politiikkojen yhteydessä näkyy Order-numero, joka kertoo politiikan prioriteetin. Mitä pienempi numero on, sitä korkeampi on prioriteetti. Eri palomuuripolitiikkojakin voidaan määrittää tarpeen mukaan eri kokoelmille, mutta tässä tapauksessa niihin ei perehdytä tarkemmin.

Luonti aloitetaan painamalla Create Antimalware Policy, josta aukeaa sille tarkoitettu wizard. Politiikalle annetaan nimi (ja kuvaus), minkä jälkeen alapuolelta valitaan, mitä asetuksia halutaan konfiguroida. Kun asetuksia valitaan, ilmestyy joka valitusta asetuksesta välilehti wizardin vasempaan reunaan. Välilehdet sisältävät niihin otsikoihin liittyvät asetukset. Esimerkiksi valittaessa Scheduled scans -asetus, ilmestyy sen otsikon

välilehti vasempaan reunaan, ja sieltä pystytään määrittämään asetukset liittyen virustarkastuksiin. Näitä asetuksia ovat muun muassa tarkastusajat, tarkastuksen tyyppi ja prosessorin käytön rajoitus tarkastuksen aikana. Politiikat toimeenpannaan kokoelmakohtaisesti. Kun politiikan luonti on valmis, painetaan hiiren oikealla näppäimellä haluttua politiikkaa ja valitaan deploy. Sen jälkeen valitaan kokoelma, johon politiikka halutaan toimeenpanna. Kuvassa 28 on yleisnäkymä politiikan luonnista.



KUVA 28. Kuvakaappaus tietoturvapolitiikan luonnin asetuksista

Se, miten asetukset kannattaa valita politiikkoihin, riippuu muun muassa ympäristöstä, laitteista ja käyttäjistä. WPK-verkkoon toteutettaessa on syytä tehdä omat kokoelmat ja politiikat palvelimille, työasemille sekä kannettaville työasemille, jolloin asetukset saadaan täysin optimoiduiksi. SCEP:n politiikoissa voidaan myös käyttää valmiita pohjia, jotka löytyvät samalta välilehdeltä kuin politiikkojen luonti painettaessa Import-kuvaketta vasemmasta yläkulmasta. Valmiita politiikkoja on lukuisia eri käyttötarkoituksia varten. Esimerkiksi palvelimille, kuten DC:lle, DHCP:lle, DNS:lle ja Exchangelle on omat valmiit politiikat. Niitä on myös työasemille ja niissä on otettu huomioon myös eri turvallisuustasot, kuten korkea turvallisuus tai optimoitu

suorituskyky. Politiikkoja voidaan myös muokata helposti valitsemalla haluttu politiikka ja Properties.

5.2.5 Ylläpito ja testaus

Monitoring-välilehdellä nimensä mukaisesti valvotaan SCEP:n toimintaa. Sieltä näkyvät ylläpitäjän kannalta tärkeimmät tapahtumat liittyen verkon toimintaan. Välilehti sisältää muun muassa hälytykset, raportit, client-ohjelmien tilan, mahdollisesti löydetyt malwaret ja muutenkin yleiskatsauksen SCEP:n toimintaan esimerkiksi kokoelmakohtaisesti. Monitoring-välilehteä on syytä vilkaista kohtuullisen usein, sillä kaikki ongelmat tulevat sinne näkyviin lähes reaaliaikaisesti (Rachui ym. 2012, 702). Kuva 29 havainnollistaa Monitoring-välilehden näkymää ja tarkemmin SCEP:n tämänhetkistä tilaa kohdassa Endpoint Protection Status - System Center 2012 Endpoint Protection.

KUVA 29. Kuvakaappaus SCEP:n tilasta Monitoring-välilehdellä

Malware Detected -alavalikkoon tulee näkyviin mahdolliset löydetyt malwaret. Kun malwareja löydetään, niistä näkyy valikossa tiedot, kuten mistä kokoelmasta se löydettiin, uhkan nimi, uhkan tyyppi, saastuneet koneet ja uhkan tila, eli ollaanko se

pystytty tekemään vaarattomaksi. Lisätietoa uhkista saadaan valitsemalla samalta välilehdeltä haluttu uhka ja malware detail sivun ylälaidasta. Monitoring-välilehdellä on lisäksi Reporting-kansio, josta saadaan haettua eri kriteereillä raportteja löydetyistä uhkista. Raportit voidaan luoda esimerkiksi PDF-tiedostoina, jolloin niitä voidaan jakaa esimerkiksi henkilöiden kanssa, joilla ei ole pääsyä SCCM:iin (Plue 2012).

Ylläpitäjille on lisäksi syytä määrittää sähköpostiin saapuvaksi jo aiemmin esitellyt hälytykset. Hälytysten avulla ylläpitäjät näkevät heti, jos jotain tietoturvariskejä havaitaan. Siksi niihin voidaan puuttua myös nopeasti, mikä on tärkeää ongelman korjaamisen kannalta. Hälytyksien vuoksi ylläpitäjien ei tarvitse koko ajan olla seuraamassa Monitoring-välilehteä, sillä sähköpostihälytykset saadaan reaaliaikaisesti esimerkiksi puhelimen sähköpostiohjelmaan, joka kulkee aina mukana.

Koska juuri asennetusta SCEP-ympäristöstä tuskin löydetään heti malwareja, voidaan SCEP:n toimintaa testata esimerkiksi yleisessä testikäytössä olevalla vaarattomalla EICAR-testiviruksella. Lyhyt koodi saadaan osoitteesta http://www.eicar.org/, ja se tallennetaan tekstitiedostona halutulle päätelaitteelle, jolloin se simuloi haittaohjelman pääsyä tietokoneelle. SCEP:n pitäisi heti havaita se ja ilmoittaa siitä viiden minuutin kuluessa SCCM-palvelimelle. Tällä tavoin ylläpitäjät voivat testata täysin vaarattomasti muun muassa client-ohjelmistojen toimivuutta, Monitoring-valikon Alerts- ja Malware Detected -välilehtiä, raportointimahdollisuuksia sekä sähköpostihälytyksiä.

6 POHDINTA

Työn tavoitteena oli tutkia, kuinka TAMKin WPK-verkon päätelaiteturvallisuudesta voidaan huolehtia. Työhön valittiin toimeksiantajan pyynnöstä tutkittavaksi erityisesti Microsoft System Center 2012 Endpoint Protection -tietoturvaohjelmisto, ja sen toimivuus ja soveltuvuus WPK-verkon käyttöön. Opinnäytetyössä tuotiin lisäksi esiin lyhyesti markkinoiden muut suositut tietoturvaohjelmistot.

Tarkoitus oli asentaa SCEP testiympäristöön, jossa voitiin tutkia sen käytettävyyttä ja toimivuutta WPK-verkkoa varten. Kaikissa työvaiheissa, jotka testiympäristöön toteutettiin, otettiin huomioon toiminnot ja asetukset myös WPK-verkon näkökulmasta. Lisäksi työssä esiteltiin, miten järjestelmä voidaan ottaa käyttöön yhdessä WPK-verkon luokassa sekä koko WPK-verkon ympäristössä pysyvästi. Kaikki käyttöönoton eri vaiheet asennuksista testaukseen otettiin huomioon ja dokumentoitiin sekä huomioitiin myös ylläpidon keskeisimmät asiat.

Ensin työssä esiteltiin työn tausta, tavoitteet ja tarkoitus, minkä jälkeen käytiin läpi hieman tietoturvan teoriaa, tietoturvaohjelmistoja sekä käytettävät ympäristöt ja ohjelmat. Esivaatimusten asennus ja selvitys oli niin suuri osa työtä, että koin tarpeelliseksi paneutua niihin huolella SCEP:n käyttöönoton mahdollistamiseksi. Sen jälkeen asennettiin ja konfiguroitiin tarvittavat ohjelmistot ja otettiin käyttöön itse SCEP, sekä luotiin dokumentaatio ja ohjeistukset.

Työn tuloksena syntyi siis kattava dokumentaatio SCEP-tietoturvaohjelmiston käyttöönotosta päätelaitteille yritysympäristössä, siihen tarvittavista ohjelmistoista ja niiden konfiguraatioista sekä ylläpidosta. Tutkimus onnistui mielestäni hyvin tavoitteisiin ja tarkoitukseen nähden, vaikka teknisessä toteutusosuudessa muutamat kohdat aiheuttivatkin aluksi hieman ongelmia. Työssä joutui selvittämään ja ottamaan huomioon monia asioita, jotta ympäristö saatiin toteutettua oikein. Tutkimuksen tuotos auttaa varmasti tulevaisuudessa SCEP-ohjelmiston toimeenpanossa, kun se päätetään ottaa käyttöön WPK-verkossa. Tietenkin sitä voidaan käyttää yleisohjeena myös muissa yritysympäristöissä.

SCEP:n käyttöönottoa ei kuitenkaan toteutettu vielä tässä vaiheessa oikeaan tuotantoympäristöön ajankäytöllisistä syistä sekä WPK-verkon tulevien

rakennemuutosten vuoksi, sillä tarkoitus oli vain tutkia ohjelmiston sopivuutta WPK-verkkoon. WPK-verkon tuotantoympäristössä ei vielä käytetä Windows Server 2012 -versioita, vaikka lähitulevaisuudessa migraatio tullaankin tekemään palvelinten osalta 2012-versioihin koko verkossa. Samalla mielestäni olisi syytä myös korvata vanhat versiot muista ohjelmistoista uudemmilla, sillä yhteensopivuusongelmat tulevat varmasti jossain vaiheessa eteen. Tämä oli suurin syy, miksi testiympäristössä asennukset tehtiin Windows Server 2012 -käyttöjärjestelmäversiolla, eikä tällä hetkellä tuotantokäytössä olevilla 2008 R2 -versioilla. Samasta syystä tulevaisuutta ajatellen myös SQL Serverin ja SCCM:n versiot korvattiin työssä uudemmilla versioilla verrattuna tämänhetkisiin WPK-verkon käytössä oleviin versioihin.

Työ ja sen ohjeet tehtiin tulevaisuuden muutokset huomioiden, sillä SCEP:n käyttöönotto on järkevää tehdä konkreettisesti vasta 2012-migraation jälkeen. Ennen SCEP:n asennusta tulisi kuitenkin myös poistaa käytöstä vanha tietoturvaohjelmisto ja minimoida aika vanhan ohjelman poistamisen ja SCEP:n käyttöönoton välistä, jolloin suojaa ei ole.

WPK-verkkoon asennettaessa SCEP olisi huomattava parannus, sillä tällä hetkellä käytössä olevaan tietoturvaohjelmistoon ei ole keskitettyä hallintaa, eikä se integroidu hyvin Microsoftin järjestelmiin, kuten AD:hen. Microsoft-ympäristöissä SCCM-ohjelmalla on lukuisia muitakin etuja keskitettyyn hallintaan liittyen, kuten etähallinta, ohjelmien ja päivitysten jakaminen sekä käyttöjärjestelmien toimeenpano. Tästä syystä tulevaisuudessa SCCM:n käyttöönotto WPK-verkossa muitakin tarkoituksia kuin SCEP:ia varten olisi mielestäni vähintäänkin harkitsemisen arvoista. Yritysympäristössä se voisi parantaa yrityksen ja ylläpitäjien tehokkuutta, sillä se helpottaa ylläpitäjien työtä ja näin ollen vähentää kustannuksia. Tähän tarkoitukseen voitaisiin ottaa käyttöön WPK-verkossa migraation jälkeen jo olemassa olevia palvelimia, joilla ei varsinaista käyttöä tällä hetkellä ole, tai hankkia täysin uusia palvelimia, jos budjetti antaisi siihen mahdollisuuden.

Toimeksiantajan etujen lisäksi työ syvensi myös henkilökohtaista tietotaitoani muun muassa tietoturvasta yleisesti, Microsoftin SCCM-ohjelmasta sekä Windows Server 2012 -käyttöjärjestelmästä, koska esimerkiksi SCCM, SCEP ja Windows Server 2012 -versio eivät olleet itselleni entuudestaan kovinkaan tuttuja. Näistä taidoista voi olla

suurtakin hyötyä tulevaisuuteni työuralla, sillä Microsoftin tuotteet ovat hyvin suosittuja yritysympäristöissä maailmanlaajuisesti.

LÄHTEET

Järvinen, P. 2002. TIETOTURVA & YKSITYISYYS. 2. painos. Jyväskylä: Docendo Finland Oy.

Microsoft TechNet. 2012. How to Extend the Active Directory Schema Using ExtADSch.exe. Luettu 16.10.2013.
http://technet.microsoft.com/en-us/library/bb680608.aspx

Microsoft TechNet. 2012. Planning for Hardware Configurations for Configuration Manager. Luettu 16.10.2013.
http://technet.microsoft.com/en-us/library/hh846235.aspx

Microsoft TechNet. 2013. Configuration Manager. Luettu 4.10.2013.
http://technet.microsoft.com/en-us/library/gg682129.aspx

Microsoft TechNet. 2013. Hardware and Software Requirements for Installing SQL Server 2012. Luettu 4.10.2013.
http://technet.microsoft.com/en-US/ms143506.aspx

Microsoft TechNet. 2013. Planning for Boundaries and Boundary groups in Configuration Manager. Luettu 22.10.2013.
http://technet.microsoft.com/en-us/library/gg712679.aspx

Microsoft TechNet. 2013. Supported Configurations for Configuration Manager. Luettu 4.10.2013.
http://technet.microsoft.com/en-us/library/gg682077.aspx

Microsoft TechNet. 2013. Windows Firewall and Port Settings for Client Computers in Configuration Manager. Luettu 16.10.2013.
http://technet.microsoft.com/en-us/library/gg682180.aspx

Microsoft. 2013. System Center 2012 Endpoint Protection. Luettu 14.10.2013.
http://download.microsoft.com/download/9/4/6/946AD448-B644-48DC-A3EA-080C12E1922A/SC_EP_ds_FINAL%20102511.pdf

Plue, A. 2012. Microsoft System Center 2012 Endpoint Protection Cookbook. Birmingham, UK: Packt Publishing Ltd.
http://proquest.safaribooksonline.com.elib.tamk.fi/9781849683906?uicode=tamk

Rachui, S., Agerlund, K., Martinez, S. & Daalmans, P. 2012. Mastering System Center 2012 Configuration Manager. Somerset, NJ, USA: Wiley.
http://site.ebrary.com.elib.tamk.fi/lib/tamperepoly/docDetail.action?docID=10560613

VALUE PRISM CONSULTING. 2013. Business Value of Microsoft System Center 2012 Configuration Manager. Luettu 16.10.2013.
http://download.microsoft.com/download/6/9/2/6929CB82-0FD4-49C9-897D-717B2AF9AE5E/System_Center_Configuration_Manager_2012_Business_Value_White_Paper.pdf