



System Center 2012 Configuration Manager

Testaus ja käyttöönotto

Matti Uotila

Opinnäytetyö
Joulukuu 2013
Tietojenkäsittely
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkkopalvelut

UOTILA, MATTI:
System Center 2012 Configuration Manager
Testaus ja käyttöönotto

Opinnäytetyö 57 sivua
Joulukuu 2013

Opinnäytetyön aiheena oli Microsoft System Center 2012 Configuration Manager -ohjelmiston testaus ja käyttöönotto Ahlmanin koulun Säätiön toimeksiannosta. Toimeksiannon tavoitteena oli tehostaa työasemien keskitettyä hallintaa ja vähentää ylläpitotoimiin käytettävää kokonaisaikaa. Lähtötilanteessa Ahlmanilla oli käytössä hallintaohjelmisto työasemia varten, mutta se oli ominaisuuksiltaan huomattavasti Configuration Manageria suppeampi eikä ollut enää päivittäisessä käytössä. Työ aloitettiin rakentamalla testiympäristö, johon asennettiin Configuration Manager 2012 -ohjelmisto ja erilaisia työasemia testaamista varten. Onnistuneen testijakson jälkeen suunniteltiin ja toteutettiin ohjelmiston asentaminen ja käyttöönotto Ahlmanin tuotantoympäristössä.

Käyttöönotto onnistui pienten ongelmien jälkeen hyvin, ja asetettuihin tavoitteisiin päästiin. Configuration Manager 2012 sisältää paljon erilaisia ominaisuuksia, joista otettiin Ahlmanin ympäristössä käyttöön vain osa. Näistä nykyisessä tilanteessa tärkeimpiä olivat tietoturvaohjelmisto Endpoint Protectionin, ohjelmistopäivitysten ja sovellusten käyttöönoton saaminen hallintaan.

Configuration Manager 2012 -ohjelmistoon tutustuminen oli opettavainen ja mielenkiintoinen kokemus. Ohjelmiston laajuus tuntui aluksi valtavalt haasteelta, mutta kirjallisuuteen ja Microsoftin dokumentaatioon paneutumalla sekä testiympäristössä kokeilemalla asiat alkoivat selkiytyä. Tässä vaiheessa otettiin käyttöön ohjelmiston koko potentiaaliin nähden vain pieni osa toiminnoista, joten tämä työ mahdollistaa Ahlmanin IT-prosessien tehostamisen tulevaisuudessa.

Asiasanat: Configuration Manager, keskitetty hallinta, järjestelmänhallinta.

ABSTRACT

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

UOTILA, MATTI:
System Center 2012 Configuration Manager
Testing and Deployment

Bachelor's thesis 57 pages
December 2013

The subject of this thesis was testing and deploying Microsoft System Center 2012 Configuration Manager software. The objective was to improve the centralized management of IT systems at Ahlman School Foundation in Tampere, Finland. The previous centralized management software used at Ahlman did not meet the current requirements. The commission was started by building a test environment, into which the Configuration Manager 2012 software was installed and tested versatily. After the testing phase, installation to the production environment was planned and implemented.

After a number of little problems were solved, the deployment of Configuration Manager was successful. Configuration Manager 2012 contains a lot of different system management features, and only part of them was introduced within the framework of this commission. These features were the antimalware and security solution Endpoint Protection 2012, software updates, and application deployment.

Getting to know the software was an interesting and educational experience. At first, the scope of Configuration Manager 2012 seemed a major challenge. After reading the source material and testing features in practice, things started to become clear. At this stage, only a part of the software's potential was capitalized. However, this work allows improving the IT processes of Ahlman in the future.

Key words: Configuration Manager, centralized management, systems management.

SISÄLLYS

| | | |
|-------|---|----|
| 1 | JOHDANTO..... | 5 |
| 2 | CONFIGURATION MANAGER 2012..... | 8 |
| 2.1 | Ominaisuudet | 8 |
| 2.2 | Historiaa..... | 9 |
| 2.3 | Muut System Center 2012 -tuotteet | 9 |
| 2.4 | Teknistä taustaa..... | 11 |
| 2.5 | Saittipalvelimet (Site Servers) | 13 |
| 2.5.1 | Keskitetyn hallinnan saitti (Central Administration Site)..... | 13 |
| 2.5.2 | Ensisijainen saitti (Primary Site)..... | 14 |
| 2.5.3 | Toissijainen saitti (Secondary Site)..... | 14 |
| 2.6 | Saittijärjestelmäroolit (Site System Roles) | 14 |
| 2.7 | Configuration Manager -asiakkaat..... | 18 |
| 2.8 | Sovellusten käyttöönoton hallinta..... | 19 |
| 2.8.1 | Paketit (Packages) | 20 |
| 2.8.2 | Sovellukset (Applications) | 20 |
| 2.9 | Ohjelmistopäivitysten hallinta | 22 |
| 2.9.1 | WSUS ja WUA | 23 |
| 2.9.2 | Ohjelmistopäivityksiin liittyviä termejä..... | 24 |
| 2.10 | Endpoint Protection | 25 |
| 3 | LÄHTÖKOHDAT JA TESTAUS..... | 27 |
| 3.1 | Lähtötilanne | 27 |
| 3.2 | Configuration Managerin asentaminen ja konfigurointi testiympäristöön | 27 |
| 3.2.1 | Ennakkotoimenpiteet Active Directory -ympäristössä | 28 |
| 3.2.2 | SQL-palvelimen asentaminen | 30 |
| 3.2.3 | Saittipalvelimen asentaminen..... | 31 |
| 3.2.4 | Saittipalvelimen konfigurointi | 33 |
| 3.3 | Havaintoja testauksesta..... | 36 |
| 4 | SUUNNITTELU JA TOTEUTUS | 41 |
| 4.1 | Suunnittelu | 41 |
| 4.2 | Asentaminen | 42 |
| 4.3 | Endpoint Protection 2012:n käyttöönotto | 46 |
| 4.4 | Ohjelmistopäivitysten käyttöönotto | 49 |
| 4.5 | Sovellusten käyttöönotto..... | 50 |
| 5 | POHDINTA..... | 53 |
| | LÄHTEET..... | 56 |

1 JOHDANTO

Tausta

Tämä opinnäytetyö käsittelee Microsoft System Center 2012 Configuration Managerin testausta ja käyttöönottoa Ahlmanin koulun Säätiön työ- ja oppilaitosympäristössä. Ahlmanin koulun Säätiö on yksityinen koulutusta ja palveluja tarjoava organisaatio, joka sijaitsee Tampereella. Ahlman koostuu kolmesta toimijasta, Ahlmanin ammattiotopistosta, Ahlman-instituutista, sekä kokous- ja majoituspalveluja tarjoavavasta Ahlmanin Kartanosta (Ahlmanin koulun Säätiö 2013). Ahlmanin IT-osaston vastuulla on noin 200 työaseman ja 10 palvelimen ylläpito. Käyttäjätunnuksia Active Directory -ympäristössä on yli 800.

Aloitin Ahlmanilla työharjoittelujakson maaliskuussa 2013, ja harjoittelun aikana ilmeni, että työasemien keskitetty hallinta kaipaisi tehostusta. Tilanteeseen oli kaksi selkeää syytä. Käytössä ollut keskitetyn hallinnan ohjelmisto oli useamman vuoden vanha, ja toisaalta opetuskäytössä olevien tietokoneiden määrää oli hiljattain lisätty merkittävästi uusien opetustilojen käyttöönoton yhteydessä. Nämä syyt yhdessä olivat aiheuttaneet tilanteen, jossa järjestelmänhallintaan tarvittiin uusi ratkaisu. Kävimme tilannetta läpi Ahlmanin IT-asiantuntijan kanssa, ja hän ehdotti minulle opinnäytetyön aiheeksi keskitetyn hallinnan ohjelmiston käyttöönottoa. Pohdittuamme eri vaihtoehtoja, ohjelmistoksi valikoitui Configuration Manager 2012.

Configuration Manager, tai lyhyemmin ConfigMgr, on järjestelmänhallintaohjelmisto jonka avulla voidaan tehdä useita hallinnointitehtäviä keskitetysti asiakastietokoneista koostuvassa ympäristössä (Agerlund 2012). ConfigMgr on osa Microsoftin laajaa System Center -tuoteperhettä. System Center on pilvi- ja palvelinympäristö, joka helpottaa palvelinkeskusten, loppukäyttäjien laitteiden ja pilviympäristöjen tehokasta keskitettyä hallintaa (System Center 2012 Product Details 2013).

Palvelinten, työasemien ja mobiililaitteiden hallinnointi on aikaa vievä, mutta välttämätön ja tärkeä työtehtävä. Ohjelmistoista ilmestyy nykyään nopeaan tahtiin tietoturvapäivityksiä, joiden asentaminen erikseen jokaiselle laitteelle vie suhteettoman paljon ylläpidosta vastaavien henkilöiden työaikaa. ConfigMgr mahdollistaa keskitettyjen ohjelmistopäivitysten lisäksi paljon muitakin ylläpitotehtäviä, kuten esimerkiksi ohjelmisto-

asennukset, käyttöjärjestelmien jakelun, laitteiden seurannan päivitysten asentumisen osalta, laitteiston ja ohjelmiston tietojen listaamisen sekä laitteiden etähallinnan (Documentation Library for...2013, 25–27). Ohjelmiston tuomat edut järjestelmän ylläpitäjälle ovat ilmeisiä ympäristössä, jossa hallittavia laitteita on paljon.

Tavoitteet ja tarkoitus

Toimeksiannon tavoitteena oli Ahlmanin opetuskäytössä ja henkilökunnan työkäytössä olevien tietokoneiden keskitetyn hallinnan tehostaminen, ja ylläpitotoimiin käytettävän kokonaisajan pienentäminen. Opinnäytetyön kirjallisen osan tavoitteeksi asetettiin tiiviin mutta informatiivisen raportin kirjoittaminen Configuration Managerista niin, että pääpaino oli toimeksiannon kannalta keskeisten ominaisuuksien kuvaamisessa. Tarkoituksena oli kirjoittaa raportti, joka tarjoaisi hyvän tietopaketin ohjelmistosta niille, joille ConfigMgr on ennestään tuntematon ohjelmisto, mutta myös niille joilla on jo jonkin verran kokemusta järjestelmänhallintaohjelmiston toiminnasta. Omana tavoitteenani oli lisäksi myös ammatillisen osaamiseni kehittäminen järjestelmänhallinnan osalta.

Ennen työn aloittamista Ahlmanilla käytössä ollut keskitetyn hallinnan ohjelmisto oli kyllä toimiva, mutta sen ominaisuudet eivät olleet enää riittäviä nykyiseen ympäristöön. Käyttöönottovaiheessa oli tarkoitus asentaa Configuration Manager 2012, ja saada keskitetysti hallintaan ohjelmistopäivitysten jakelu laitteille, sekä sovellusten ja Endpoint Protection 2012:n käyttöönotto. Ennen todelliseen ympäristöön asentamista ohjelmistoa testattiin ja sen ominaisuuksiin tutustuttiin huolellisesti rakennetun testiympäristön avulla.

Merkitys ja lähteet

Toivon että tästä työstä on hyötyä toimeksiantajan lisäksi myös lukijoille, jotka haluavat yleistä tietoa Configuration Managerista, tai pohtivat eri järjestelmänhallintavaihtoehtoja, ja haluavat lukea tämän ohjelmiston asentamisen ja käyttöönoton käytännön kokemuksista. Configuration Managerista ei ole saatavilla juuri lainkaan suomenkielistä materiaalia, joten tämäkin huomioiden uskon työn olevan hyödyllistä luettavaa asiasta kiinnostuneille.

Olen käyttänyt työssä pääasiallisina lähteinä teoksia, joiden kirjoittajat ovat alalla tunnettuja Configuration Manager -ammattilaisia. Ohjelmistosta ei ole julkaistu kovin montaa kirjaa, joten siltä osin lähteiden valitseminen oli helppoa. Verkkolähteitä käyttä-

essäni pyrin tarkastamaan kirjoittajan tai sivuston taustat huolellisesti, jotta kaikkia työssä käytettyjä lähteitä voitaisiin pitää luotettavina. Käytin pääasiallisina lähteinä kolmea kirjaa, joista kaksi oli Kent Agerlundin System Center 2012 Configuration Manager Mastering the Fundamentals -teoksen eri versioita. Agerlundin kirjoissa ei käsitellä kovin perusteellisesti ohjelmiston historiaa tai teknisiä taustoja, mutta asennusoppaana se on erittäin selkeä ja toimiva. Kolmas pääasiallinen lähde oli Kerrie Meylerin ja neljän muun kirjoittajan System Center 2012 Configuration Manager Unleashed -kirja, joka on syvälinen kuvaus Configuration Managerin historiasta ja nykyisestä versiosta. Kirjassa käsitellään perusteellisesti myös teknisiä taustoja, esimerkiksi mitä taustalla tapahtuu ohjelmiston erilaisissa asennus- ja konfigurointivaiheissa.

Pääasiallisten lähteiden luotettavuutta pidän erittäin hyvänä, koska kaikki kirjoittajat ovat kokeneita ja pitkään Configuration Managerin parissa toimineita ammattilaisia. Meylerin kirjan kirjoittajista yhtä lukuun ottamatta kaikki on mainittu System Center tai Configuration Manager MVP -palkinnon saajiksi. Toisaalta se, että kaikilla kirjoittajilla on läheiset suhteet Microsoftiin, pitää ottaa huomioon lähteitä lukiessa. Agerlund esimerkiksi työskentelee konsulttina Coretechissa, joka on Microsoftin yhteistyökumppani. Meylerin kirjan kirjoittajista kukaan ei työskentele suoraan Microsoftin alaisuudessa, joten kirjoissa on otettu myös kriittisesti kantaa sellaisiin ohjelmiston ominaisuuksiin, joiden toimintaan kirjoittajat eivät ole täysin tyytyväisiä. Tervettä kriittisyyttä ohjelmistoa kohtaan esiintyy molemmissa kirjoissa. Sitä ei ole paljon, mutta kuitenkin sen verran, etten lukiessa ajatellut kirjoja tehdyn pelkäksi ohjelmiston mainokseksi, vaan rehelliseksi kuvaukseksi Configuration Managerin käytöstä ja ominaisuuksista.

Rakenne

Configuration Manager 2012 on Microsoftin tuotteista ylivoimaisesti monimutkaisin kokonaisuus (Agerlund 2012), ja siksi tässä opinnäytetyössä käsitellään tarkasti vain osaa ohjelmiston monista ominaisuuksista. Opinnäytetyö koostuu neljästä osasta. Ensimmäisessä luodaan yleiskatsaus Configuration Manageriin, sen historiaan ja nykyhetkeen massiivisena järjestelmänhallintatyökaluna. Tämän jälkeen käydään läpi lähtökohdat, joista tuotteen käyttöönotto Ahlmanilla aloitettiin, sekä testausympäristön rakentamisen vaiheet. Kolmas osa sisältää suunnittelun ja käyttöönoton toteuttamisen tuotantoympäristössä. Lopun pohdinnassa käydään työ vielä kokonaisuudessaan läpi, tarkastellaan työn onnistumista ja luodaan katse myös tulevaisuuteen.

2 CONFIGURATION MANAGER 2012

2.1 Ominaisuudet

ConfigMgr on yritystason hallinnointityökalu, joka tarjoaa ratkaisun mm. Windows-asiakkaiden ja -palvelinten keskitettyyn hallintaan. Se tarjoaa mahdollisuuden asiakastietokoneen laitteiston ja ohjelmiston listaamiseen, ohjelmistopäivityksiin, sovellusten käyttöönottoon ja käyttöjärjestelmien asennukseen. ConfigMgr kerää myös jatkuvasti tietoa asiakkaista näkyville hallintakonsoliin, mikä mahdollistaa asiakastietokoneiden tilan seurannan ohjelmiston avulla. Yhtenä esimerkkinä tästä voidaan mainita *ohjelmistojen seuranta* -ominaisuus. Sen avulla voidaan valvoa, miten paljon jotain tiettyä ohjelmistoa käytetään hallittavissa asiakaskoneissa. Näin esimerkiksi vähän käytetyistä ohjelmistoista voidaan yrityksessä luopua, ja säästää lisensointikuluissa. Näiden lisäksi ConfigMgrin yhteyteen voidaan integroida Microsoftin tietoturvaohjelmisto Endpoint Protection 2012, jota hallitaan keskitetysti samasta konsolista kuin ohjelmiston muitakin toimintoja. Järjestelmänhallinta helpottuu, kun ylläpitäjällä on näkymä ja kontrolli kaikkiin järjestelmiin yhden hallintakonsolin kautta (Meyler, Holt, Oh, Sandys & Ramsey 2012). Kuvassa 1 hallintakonsolin yläosan valintanauha, josta valitaan halutut toiminnot kulloisessakin työtilassa.



KUVA 1. Hallintakonsolin valintanauha on tyyliltään samankaltainen kuin Microsoftin muissa tuotteissa, esim. Wordissa (Configuration Manager 2012 SP1 2013, kuvankaappaus)

2.2 Historiaa

Configuration Managerin historia yltää lähes 20 vuoden päähän kesään 1994, jolloin Microsoft julkaisi Systems Management Server (SMS) 1.0:n. Seuraavina vuosina ohjelmasta julkaistiin uusia versioita (1.x), mutta ne eivät saavuttaneet laajaa suosiota ohjelmiston osoittauduttua mm. hankalaksi asentaa ja käyttää. Alkuvuodesta 1999 Microsoft julkaisi SMS 2.0:n, mutta myös sen raportoitiin olleen epävakaa. Lisäksi ohjelmisto ei tässä vaiheessa sisältänyt Active Directory -integraatiota, vaikka AD tuli pian SMS 2.0:n julkaisun jälkeen markkinoille yhdessä Windows 2000:n kanssa (Meyler ym. 2012).

Active Directory -integrointi lisättiin ominaisuuksiin ohjelmiston seuraavassa versiossa, SMS 2003:ssa. Tämä versio sisälsi muutenkin paljon uusia ominaisuuksia, joiden myötä mahdollisiksi tulleet toiminnallisuudet ovat edelleen osa Configuration Manageria. Tällaisia olivat mm. BITS-integrointi asiakkaan ja palvelimen väliseen liikennöintiin, sekä asiakkaan konfigurointitietojen tallentaminen WMI:n avulla tiedostojärjestelmän sijaan (Meyler ym. 2012).

Tuotteen seuraavan julkistuksen yhteydessä elokuussa 2007 Microsoft muutti nimeämiskäytäntöä, kun Configuration Manager 2007 julkaistiin. Tuote sisälsi jälleen paljon uusia ominaisuuksia, ja niitä saatiin lisää vain vuosi alkuperäisen julkistuksen jälkeen R2-version myötä. Näihin kuuluivat mm. Application Virtualization ja tuki SQL-raportointipalveluille. Isoja muutoksia elinkaarensa aikana nähnyt ohjelmisto sai huhtikuussa 2012 jälleen uuden ja paljon muutoksia edeltäjäänsä nähneen julkistuksen, kun viralliselta nimeltään System Center 2012 Configuration Manager esiteltiin (Meyler ym. 2012).

2.3 Muut System Center 2012 -tuotteet

System Center on Microsoftin brändi yritystason järjestelmänhallintaan, ja se tarjoaa kokonaisvaltaisen sarjan tuotteita, joiden avulla pystytään hallinnoimaan datakeskuksia, loppukäyttäjien laitteita ja pilviympäristöjä (Microsoft. System Center 2012 Product Details 2013). Configuration Manager 2012 on yksi keskeisimmistä osista System Center -tuoteperheessä, ja sen käyttöönotto voidaan toteuttaa yksittäin tai yhdessä muiden

tuoteperheen osien kanssa (Agerlund 2012). Seuraavaksi tutustutaan lyhyesti muihin System Center -tuotteisiin.

App Controller

App Controller on loppukäyttäjien itsepalveluportaali, joka helpottaa sovellusten jakelua ja hallinnointia pilviympäristöissä. Se tarjoaa yhden hallintakonsolin, jonka kautta voidaan hallita useita yksityisiä ja julkisia pilviä sekä tarjota virtuaalikoneita ja palveluja yksittäisille liiketoiminnan osille (Meyler ym. 2012).

Operations Manager

Operations Manager tai lyhyemmin OpsMgr on Microsoftin järjestelmien valvonta- ja hallintaohjelmisto. Se tarjoaa informaatiota kohteen tilasta, terveydestä ja suorituskyvystä. OpsMgr voidaan asettaa tuottamaan hälytyksiä, kun kohteen suorituskyky, saataavuus tai turvallisuus ei vastaa asetettuja kriteerejä (Agerlund 2012).

Orchestrator

Orchestrator on IT-prosessien automatisointityökalu, joka toimii yhdistävänä osana muiden System Center -tuotteiden välissä. Sen avulla voidaan organisoida eri tehtäviä esim. Configuration Managerin, Operations Managerin, Service Managerin ja kolmannen osapuolen hallinnointityökalujen välillä. Orchestratorin avulla voidaan manuaalisia ja virheherkkiä toimintoja korvata automatisoiduilla ja standardisoiduilla prosesseilla. Näin voidaan tehostaa IT-toimintoja sekä laskea niiden kustannuksia (Agerlund 2012; Meyler ym. 2012).

Service Manager

Service Manager on keskitetty helpdesk-järjestelmä, johon voidaan vastaanottaa tikettejä esim. muiden System Center -tuotteiden kautta. Configuration Manager -yhdistin mahdollistaa Service Managerin käyttäjä tietoja joita ConfigMgr saa laitteita inventoidessaan (Meyler ym. 2012; Pott 2012).

Virtual Machine Manager

Virtual Machine Manager (VMM) on hallinnointialusta heterogeenisille virtualisointi-infrastruktuureille. Se tarjoaa mahdollisuuden hallita keskitetysti virtuaalikoneita usealla suositulla virtualisointialustalla, kuten Windows Server 2008 ja 2008 R2 Hyper-V, VMware ESX 3.x ja Citrix XenServer (Meyler ym. 2012).

Data Protection Manager

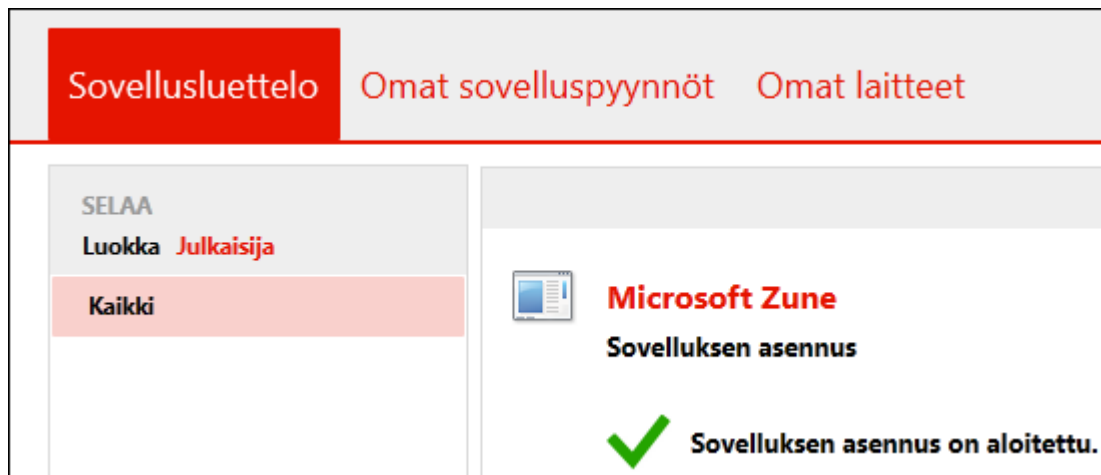
Data Protection Manager eli DPM tarjoaa varmuuskopiointiratkaisun Windows-palvelimille ja työasemille. Se käyttää Microsoftin Virtual Disk Service ja Shadow Copy -teknologioita, ja toimii varmuuskopiointiratkaisuna riippumatta siitä, säilytetäänkö tietoa nauhoilla, levyillä vai pilvipalvelimilla (Agerlund 2012; Meyler ym. 2012).

Endpoint Protection

Endpoint Protection on Microsoftin yritystason tietoturvaohjelmisto, entiseltä nimeltään Forefront Endpoint Protection. System Centerin osana Endpoint Protection on mahdollista integroida Configuration Manageriin, jolloin niitä voidaan käyttää yhdessä saman hallintakonsolin kautta (Meyler ym. 2012).

2.4 Teknistä taustaa

Configuration Manager toimii yhdessä olemassa olevien Microsoftin teknisten ratkaisujen kanssa ja niihin tukeutuen. Kaksi tärkeintä Windows-alustan komponenttia, joita ConfigMgr tarvitsee toimintoihinsa, ovat Active Directory ja WMI (Windows Management Instrumentation). ConfigMgr käyttää esim. Active Directory -toimialueen palveluja (Active Directory Domain Services) paikantamaan käyttäjiä ja laitteita, joita halutaan hallinnoida. BITS (Background Intelligent Transfer Service) on käytössä saata-villa olevan verkkokaistan käytön rajoittamiseksi. Eri saittijärjestelmäroolit, jotka tarjoavat toiminnallisuutta hallinnointiin perustuvat IIS Web -palveluiden pohjalle (Meyler ym. 2012; Documentation Library for...2013, 24). Kuvassa 2 on näkymä sovellusluettelosta, joka on toteutettu IIS:llä.



KUVA 2. Selaimen kautta käytettävä sovellusluettelo on yksi esimerkki IIS:n avulla toteutetuista toiminnallisuuksista. (Configuration Manager 2012 SP1 2013, kuvankaappaus)

ConfigMgr käyttää Microsoftin SQL-palvelintietokantaa ja yhdessä SQL-raportointipalveluiden (SQL Reporting Services) kanssa se mahdollistaa erilaisten raporttien tuottamisen ja hallinnointitehtävien tulosten valvomisen. Configuration Managerin saittietokanta sisältää tietoja ConfigMgr-infrastruktuurista ja objekteista, sekä hallittavista asiakkaista. Tietokannan koko vaihtelee, mutta yleisesti ottaen voidaan sanoa ConfigMgr-saittietokannan sisältävän useita tuhansia objekteja. Hallintasovellukset, esimerkiksi ohjelmiston hallintakonsoli, käyttävät tietokantaa WMI:n avulla (Meyler ym. 2012; Documentation Library for...2013, 24).

WMI (Windows Management Instrumentation) on ollut hallintainfrastruktuurin ydin kaikille Windowsin työasema- ja palvelinkäyttöjärjestelmille Windows 2000:sta lähtien. WMI toimii virtualisointikerroksena hallintasovellusten tai komentosarjojen ja niiden hallinnoimien fyysisten ja loogisten resurssien välissä. WMI:tä käyttämällä voidaan esimerkiksi muuttaa Windows-käyttöjärjestelmän sisäänrakennetun Administrator-käyttäjätunnuksen nimeä, tai kerätä lista saatavilla olevista väritulostimista. WMI:llä on oma kyselykielensä WQL (WMI Query Language), jolla voidaan tehdä kyselyjä ConfigMgr-hallintakonsolin kautta ja hakea tietoa hallittavista laitteista. ConfigMgr-kokoelmat, jotka ovat merkittävässä osassa ohjelmiston päivittäisessä käytössä, perustuvat myös WQL-kyselyihin (Meyler ym. 2012).

WMI:n toimintaperiaate on tiivistettynä seuraavanlainen: hallintasovellus lähettää pyynnön WMI-infrastruktuurille, joka välittää kyselyn oikealle WMI-palvelulle. Palvelu

käsittelee tämän jälkeen toiminnon järjestelmäresurssin kanssa ja palauttaa vastauksen WMI:lle, joka välittää sen edelleen takaisin hallintasovellukselle. ConfigMgr:n asiakasagentti käyttää WMI:tä mm. silloin, kun se tekee laitteiston inventointia. Tiedot, joita agentti kerää, määritellään asiakasasetuksissa ConfigMgr:n hallintakonsolin kautta. ConfigMgr-palvelimen esimerkkitapaukseksi voidaan ottaa SMS-tarjoaja. Se on WMI-palvelu, joka asennetaan yleensä saittipalvelimelle tai saittitietokantapalvelimelle. Sen avulla palvelin pystyy kommunikoimaan saittitietokannan kanssa (Meyler ym. 2012; Documentation Library for...2013, 358).

2.5 Saittipalvelimet (Site Servers)

Saitti on ConfigMgr:n ydinrooli, ja organisaation tarpeista riippuen niitä voi olla yksi tai useampia. Saitti asentuu automaattisesti samalla, kun asennetaan ensimmäisen kerran ConfigMgr 2012 ja saittipalvelin. Saittipalvelin on yksi saittijärjestelmärooli, jota ei voi asentamisen jälkeen siirtää millekään muulle palvelimelle, eikä poistaa ilman että koko saitti poistetaan (Documentation Library for...2013, 113). Samassa yhteydessä saitti saa nimen ja kolmemerkkisen saittikoodin. Usein saittihierarkia koostuu vain yksittäisestä ensisijaisesta saitista. Monimutkaisia hierarkioita ei suositella, koska se hidastaa tiedonkulkua asiakkaiden ja hierarkian huipulla olevan palvelimen välillä (Meyler ym. 2012).

2.5.1 Keskitetyn hallinnan saitti (Central Administration Site)

Keskitetyn hallinnan saitti, eli CAS, on muiden saittien hallintaan käytettävä saittipalvelin. Sitä edellytetään, kun yhdistetään useita ensisijaisia saitteja toisiinsa. Sitä ei kuitenkaan tarvita muulloin, eikä se käsittele asiakkaiden tietoja. Tapauksissa, joissa CAS:n asentaminen on välttämätöntä, tulee se asentaa ensimmäisenä saittina hierarkiaan. Jos CAS:a ei asenneta, on ensimmäinen asennettava saitti erillinen ensisijainen saitti (Documentation Library for...2013, 111).

2.5.2 Ensisijainen saitti (Primary Site)

Jokainen Configuration Manager 2012 -toteutus edellyttää vähintään yhtä ensisijaista saittia. Tähän saittiin liitetään asiakkaat, ja sitä hallinnoidaan ConfigMgr-konsolin kautta. Ensisijainen saitti tallentaa SQL-tietokantaan kaikkien asiakkaiden tiedot, jotka siihen on liitetty. Yksi ensisijainen saitti voi tukea jopa 100 000 asiakasta, joten useamman tällaisen saitin asentaminen ei monissa käyttötapauksissa ole tarpeellista (Agerlund 2012; Meyler ym. 2012).

2.5.3 Toissijainen saitti (Secondary Site)

Toissijainen saitti on aina ensisijaiseen saittiin nähden alisteisessa asemassa, joten sitä hallinnoidaan ensisijaisen saitin hallintakonsolista käsin, eikä siihen liitetä suoraan asiakkaita. Toissijainen saitti välittää asiakkailta saamaansa informaatiota ensisijaiselle saittilleen. Toissijainen saitti on käyttökelpoinen tapauksissa, joissa etäällä olevaan sijaintiin tarvitaan yhteys, mutta verkkokaistan käyttöä joudutaan kontrolloimaan. Muutoksena edellisiin versioihin nähden, ConfigMgr 2012:ssa toissijainen saitti edellyttää myös SQL-palvelintietokantaa (Meyler ym. 2012).

2.6 Saittijärjestelmäroolit (Site System Roles)

Saittijärjestelmärooleja käytetään Configuration Managerissa tukemaan eri hallinnointitehtäviä sailla. Mikä tahansa tietokone, palvelin tai työasema voi isännöidä saittijärjestelmärooleja. Tällaista yhdenkin roolin isännöivää laitetta kutsutaan saittijärjestelmäpalvelimeksi (Site System Server). Rooleja voidaan siis jaotella useamman palvelimen isännöitäväksi, mutta myös yhdelle fyysiselle tai virtuaaliselle palvelimelle voidaan hyvin toteuttaa kaikki roolit pienessä tai keskisuuressa toteutuksessa (Agerlund 2012; Documentation Library for...2013, 113; Meyler ym. 2012).

Saittijärjestelmäroolien avulla ConfigMgr-ympäristössä tarjotaan asiakastietokoneille ne palvelut, jotka halutaan ottaa käyttöön (Rachui, Agerlund, Martinez & Daalmans 2012). Jos halutaan esimerkiksi asentaa ohjelmistoja asiakastietokoneille, täytyy ensin ottaa

käyttöön jakelupiste-saittijärjestelmärooli. Seuraavaksi käydään lyhyesti läpi eri saittijärjestelmärooleja.

Jakelupiste (Distribution Point)

Kun asiakas haluaa asentaa sovelluksen tai ohjelmistopäivityksen, ladataan se jakelupisteeltä. Jakelupisteelle tallennetaan kaikki sisältö, jota tarvitaan ConfigMgr:n tarjoamissa palveluissa. Edellä mainittujen lisäksi tällaista sisältöä ovat esim. käyttöjärjestelmä-asennuksissa tarvittavat WIM-tiedostot. Jakelupisteitä voi olla useita, jolloin niistä voidaan tehdä hallinnoinnin helpottamiseksi jakelupisteryhmiä. Service Pack 1:stä lähtien ConfigMgr 2012:ssa on ollut kaksi erilaista jakelupistetyyppiä, paikallinen ja pilvipalvelustainen jakelupiste. Pilvipalvelustaisen jakelupisteen käyttö edellyttää Windows Azure -tilausta (Agerlund 2013).

Hallintapiste (Management Point)

Asiakkaat ja saittipalvelin ovat yhteydessä toisiinsa hallintapisteen kautta. Hallintapiste tarjoaa asiakaskäytännöt, ja ottaa asiakkailta vastaan mm. tilatietoja ja ohjelmistomittautustietoja, jotka se välittää saittipalvelimelle (Agerlund 2012).

Ohjelmistopäivityspiste (Software Update Point)

Ohjelmistopäivityspiste on WSUS-palvelin, jota ConfigMgr hallinnoi. Asiakkaat eivät lataa päivityksiä suoraan ohjelmistopäivityspisteeltä, vaan pelkästään metatiedot päivityksistä. Niiden perusteella asiakkaat raportoivat ConfigMgr:lle, joka saa tiedot, mitä päivityksiä asiakas tarvitsee ja mitä ei (Agerlund 2013; Meyler ym. 2012).

Endpoint Protection -piste (Endpoint Protection Point)

Tämä saittijärjestelmärooli tarvitaan, kun halutaan hallinnoida Endpoint Protection -asiakkaita ConfigMgr-hallintakonsolin kautta (Agerlund 2013).

Sovellusluettelon verkkopalvelupiste (Application Catalog Web Service Point)

Tämä saittijärjestelmärooli tarjoaa tiedot hallintakonsolin Software Library -työtilassa olevista ohjelmistoista sovellusluettelon verkkosivulle (Agerlund 2013).

Sovellusluettelon verkkosivustopiste (Application Catalog Website Point)

Sovellusluettelon verkkosivustopiste on loppukäyttäjää varten oleva selaimella käytettävä Web-portaali, josta käyttäjät voivat pyytää ja ladata tarvitsemiaan ohjelmistoja (Agerlund 2013).

Saittitietokantapalvelin (Site Database Server)

Saittitietokantapalvelin on palvelin, johon on asennettu tuettu versio Microsoftin SQL Serveristä. Saittitietokantapalvelin isännöi ConfigMgr-saittitietokantaa. Jokainen ConfigMgr-toteutus edellyttää vähintään yhtä palvelinta, jolla on saittitietokantapalvelinrooli (Meyler ym. 2012; Rachui ym. 2012).

Saittipalvelin (Site Server)

Saittipalvelin, jolle ConfigMgr-ohjelmisto on asennettu, hallinnoi itse tätä roolia. Roolia ei voida manuaalisesti lisätä, eikä poistaa. Saittipalvelin vastaa sitin toiminnoista ja kommunikoi kaikkien muiden järjestelmien kanssa, jotka isännöivät eri saittijärjestelmärooleja sitilla (Rachui ym. 2012).

Saittijärjestelmä (Site System)

Kaikki järjestelmät, jotka isännöivät vähintään yhtä roolia, saavat myös automaattisesti saittijärjestelmäroolin. Tätäkään roolia ei voida manuaalisesti lisätä, eikä poistaa (Rachui ym. 2012).

Resurssitietojen synkronointipiste (Asset Intelligence Synchronization Point)

Tämän roolin avulla voidaan ladata resurssitietoja System Center Online -palvelusta. Rooli asennetaan aina hierarkiassa ylimpänä olevalla saittipalvelimelle (Agerlund 2013).

Järjestelmän kunnontarkistuspiste (System Health Validator Point)

Järjestelmän kunnontarkistuspiste on saittijärjestelmärooli, jota isännöi Windows Server -palvelin, jolla on käytössä Network Policy -palvelinrooli. Verkkokäytäntöpalvelimet tarkistavat asiakaslaitteet kun ne pyrkivät verkkoon, ja myöntävät tai kieltävät pääsyn riippuen siitä, täyttävätkö asiakkaat vaaditut käytännöt. Järjestelmän kunnontarkistuspiste ei kommunikoi suoraan saittipalvelimen kanssa, vaan hakee tarkistustiedot Active Directory -toimialueen palveluista, jonne saittipalvelin ne julkaisee (Rachui ym. 2012).

Tilatietojen siirtopiste (State Migration Point)

Tilatietojen siirtopiste on saittijärjestelmärooli, joka tarjoaa turvallisen sijainnin käyttäjän tilatiedoille käyttöjärjestelmäasennuksen aikana (Rachui ym. 2012).

Varatarkistuspiste (Fallback Status Point)

Asiakkaat käyttävät varatarkistuspistettä tilanteissa, joissa ne eivät pysty kommunikoi-
maan hallintapisteen kanssa. Tällainen tilanne saattaa syntyä esimerkiksi asiakasohjel-
man asentamisen aikana (Agerlund 2013).

Raportointipalvelupiste (Reporting Services Point)

Raportointipalvelupiste on ainoa tuettu raportointiratkaisu ConfigMgr 2012:ssa. Se tar-
joaa ConfigMgr:n ja SQL-raportointipalveluiden välisen integroinnin, ja tuottaa raport-
teja ConfigMgr:n toiminnoista graafisessa muodossa (Agerlund 2013; Rachui ym.
2012).

Out of Band -palvelupiste (Out of Band Service Point)

Out of Band -palvelupiste mahdollistaa AMT-perustaisten tietokoneiden hallinnan.
AMT on Intelin kehittämä tekniikka, joka mahdollistaa tietokoneiden hallinnan jopa
silloin, kun niistä on kytketty virta pois (Rachui ym. 2012).

Komponenttipalvelin (Component Server)

Tätä saittijärjestelmäroolia ei voida manuaalisesti lisätä, eikä poistaa. Saittipalvelin hal-
linnoi tätä roolia, jonka Configuration Manager asentaa automaattisesti. Tällä palveli-
mella ajetaan SMS_Executive-palvelua, jonka tehtävänä on tukea muita rooleja, kuten
esim. hallintapistettä (Documentation Library for...2013, 2660; Rachui ym. 2012).

Rekisteröintipiste (Enrollment Point) ja Rekisteröinnin välityspiste (Enrollment Proxy Point)

Näitä rooleja käytetään, kun rekisteröidään vanhempia mobiililaitteita ja Applen Macin-
tosh OS X -tietokoneita ConfigMgr-ympäristöön. Vanhemmilla mobiililaitteilla tarkoite-
taan esim. Windows Mobile 6.x - tai Nokian Symbian-laitteita (Agerlund 2013; Rachui
ym. 2012).

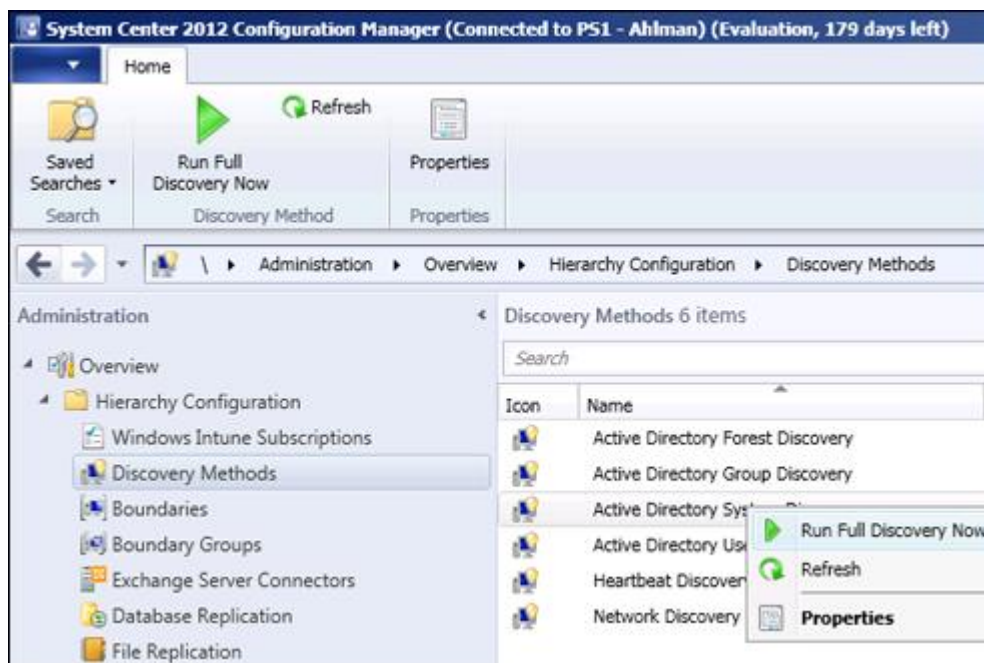
Windows Intune -yhdistin (Windows Intune Connector)

Windows Intune -yhdistin on ConfigMgr 2012 Service Pack 1:n myötä esitelty saittijärjestelmärooli, joka edellyttää Windows Intune -tilauksen tekemistä. Tämä saittijärjestelmärooli ja Intunen tarjoama pilvi-infrastruktuuri mahdollistavat mobiililaitteiden hallinnan ConfigMgr:n kautta. Tuettuja alustoja ovat mm. Android, Applen iOS, Windows 8 RT ja Windows Phone 8 (Agerlund 2013).

2.7 Configuration Manager -asiakkaat

ConfigMgr-agentti, eli asiakasohjelma sijaitsee hallittavissa laitteissa. Se suorittaa monia erilaisia tehtäviä. Näitä ovat mm. tietokoneen inventointi, isäntäkoneen tietoturva-päivitysten noudattamisen tarkistaminen, etähallinnan toteuttaminen, sovellusten asentamisen, poistamisen ja päivittämisen hallinnointi, sekä käytäntöjen lataaminen ConfigMgr-palvelimelta. Lukuisien tehtävien lisäksi asiakasohjelma on tietoinen käytettävästä verkkokaistasta ja säätelee sen käyttöä BITS:n avulla (Meyler ym. 2012).

Ennen asiakasohjelman asentamista täytyy ConfigMgr:n etsiä järjestelmät verkosta. Tähän on kuusi erilaista tapaa, joista neljä perustuu Active Directoryn kautta tehtävään etsimiseen. Jos halutaan käyttää jotain AD:hen perustuvista etsintätavoista, on hyvä muistaa, että ConfigMgr tuo kaikki löytämänsä objektit, myös sellaiset, jotka eivät välttämättä ole enää käytössä. Onkin suositeltavaa, että Active Directoryä siivotaan säännöllisesti, mikäli sitä halutaan käyttää ConfigMgr:n toimintoihin. Heartbeat-etsintä otetaan käyttöön oletuksena, kun ConfigMgr-saitti asennetaan. Se on myös ainoa etsintätapa, jonka täytyy olla asetettuna, koska ConfigMgr käyttää sitä määrittämään asiakkaiden terveydentilaa ja saavutettavuutta. Oletuksena asiakas lähettää heartbeat-etsintätietueen ConfigMgr-palvelimelle seitsemän päivän välein (Meyler ym. 2012). Kuvassa 3 on hallintakonsolin näkymä etsintätavoista.



KUVA 3. Verkon resursseja voidaan etsiä kuudella eri tavalla. (Configuration Manager 2012 SP1 2013, kuvankaappaus)

Asiakasohjelma voidaan asentaa usealla eri tavalla. Kohdekoneelta asiakas voidaan asentaa manuaalisesti komentoriviltä, jolloin tarvittavat tiedostot haetaan saittipalvelimelta tai hallintapisteeltä SMS-<saittikoodi>-jaon alikansioista. Client push -asennustavassa asennus aloitetaan ConfigMgr-hallintakonsolista käsin. Muita asennustapoja ovat kirjautumiskomentosarjalla tehtävä asennus, ohjelmistopäivitys tai ryhmäkäytännöllä tehtävä asennus (Agerlund 2012; Meyler ym. 2012).

2.8 Sovellusten käyttöönoton hallinta

Sovellusten käyttöönoton hallinta on suunniteltu ConfigMgr 2012:ssa siten, että sovelluksia voidaan kohdistaa tehokkaasti sekä käyttäjille että laitteille aiemmin käytössä olleen laitekeskeisen lähestymistavan sijaan. Käyttäjille voidaan määritellä yksi tai useampia ensisijaisia laitteita, joihin heidän tarvitsemiaan sovelluksia voidaan asentaa (Meyler ym. 2012). Jos sovellus kohdistetaan käyttäjille, voidaan se asettaa saataville sovellusluetteloon. Se on WWW-portaali, josta käyttäjät voivat ladata ja asentaa tarvitsemiaan sovelluksia siirtymällä selaimella sovellusluettelon osoitteeseen. Laitteille kohdistetut sovellukset asennetaan automaattisesti tai käyttäjien suorittamana Software Center -ohjelman kautta, joka on asennettu laitteelle ConfigMgr-asiakasohjelman asennuksen yhteydessä.

Jakelupiste on saittijärjestelmärooli, jossa sijaitsee kaikki asiakkaiden ladattavaksi tarkoitettu sisältö, kuten paketit, sovellukset, ohjelmistopäivitykset, laiteohjaimet ja levykuvat. Jakelupisteitä voi olla myös useita, esim. etäsijaintiin voidaan asentaa oma jakelupiste, jolloin käytettävissä olevaa verkkokaistaa ei tarvitse kuormittaa, vaan asiakkaiden ja jakelupisteen välinen liikenne tapahtuu paikallisesti. Jakelupisteistä voidaan tehdä myös ryhmiä, jolloin samaa sisältöä voidaan hallinnoida usealla jakelupisteellä (Agerlund 2012).

2.8.1 Paketit (Packages)

Ohjelmistopaketteja on käytetty ohjelmistojen jakeluun siitä asti, kun ensimmäinen System Management Server (SMS) julkaistiin. Ohjelmistopaketti sisältää tiedot ohjelmasta, ja miten se jaellaan laitteille. Paketti voi koostua määritystiedoista (esim. MSI- tai PDF-tiedostoista) tai se voidaan tehdä manuaalisesti. ConfigMgr mahdollistaa mm. suoritustiedostojen, komentosarjatiedostojen tai JavaScript-tiedostojen jakelun. Paketteja käytetään tavallisten ohjelmistojen jakeluun, mutta niitä voi käyttää myös asiakasasetusten konfiguroimiseen, kuten rekisterimuutoksiin. Paketti voi sisältää yhden tai useamman ohjelman, joka määrittää, mitä pitäisi tapahtua, kun asiakas vastaanottaa sille suunnatun paketin. Esimerkiksi suurin osa MSI-tiedostoista tarjoaa kuusi oletusohjelmaa, joista jokainen tarjoaa erilaisen tavan ajaa ohjelmistopaketti. Näitä ovat esimerkiksi hiljainen järjestelmäasennus, joka ei edellytä käyttäjän toimia, tai käyttäjän toimia vaativa normaali asennus. Jokainen ohjelma määrittelee erikseen komentorivikomennot, joilla ohjelma ajetaan (Meyler ym. 2012).

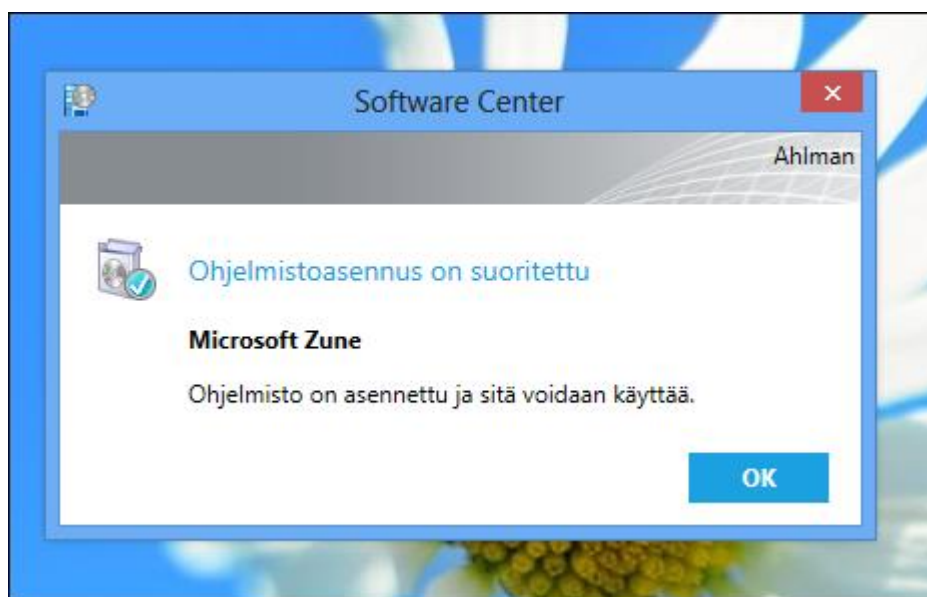
Laitteille suunnatut perustehtävät, kuten ylläpitokomentosarjatiedoston ajaminen ja tiedostojen tai varmenteiden kopiointi, on kätevää tehdä luomalla niistä paketti (Agerlund 2012). Uutta sovelluksiin perustuvaa mallia suositellaan kuitenkin käytettäväksi ohjelmistojen jakeluun aina kun mahdollista (Meyler ym. 2012).

2.8.2 Sovellukset (Applications)

Sovellus on yksi Configuration Manager 2012 -ohjelmiston uusista ominaisuuksista edellisiin versioihin nähden. Pakettiin verrattuna sovellus on ”älykkäämpi” tapa jaella

ohjelmistoja, ja se mahdollistaa ylläpitäjälle paremman hallinnan tapahtumien kulusta. Sovellus ei ole yksittäinen MSI-paketti tai .exe-tiedosto, vaan se voidaan jaella laitteille tai käyttäjille edellä mainittujen tapojen lisäksi esim. virtuaalisesti App-V:n avulla (Agerlund 2012). Sovellukset ovat malleja ohjelmistosta, ja ne sisältävät muutakin kuin lähdetiedostot ja ohjelman ajamiseen liittyvät ohjeet. Mallit määrittelevät ohjelmiston asetukset ja sisältävät käyttöönottoavan (Meyler ym. 2012).

Sovellusten avulla on myös mahdollistettu Configuration Manager 2012:lle ominainen käyttäjäkeskeinen lähestymistapa ohjelmistojen jakeluun. Sovellus voidaan jaella laitteille tai käyttäjille saatavilla olevana tai edellyttävänä pakollisena asennuksena. Kun sovellus suunnataan tietyille käyttäjäkokoelmille ja se asetetaan saatavilla olevaksi, voivat käyttäjät itse suorittaa asennuksen selaimen kautta sovellusluettelosta. Kaikissa muissa tapauksissa asennus tehdään Software Centerin kautta (Agerlund 2012). Kuvassa 4 on Software Centerin ilmoitusikkuna, kun ohjelmisto on asennettu sen kautta.



KUVA 4. Software Centerin ilmoitus, kun ohjelmisto on asennettu (Configuration Manager 2012 SP1 2013, kuvankaappaus)

Luonnollisesti sovelluksia pitää pystyä myös poistamaan tai korvaamaan uudemmalla versiolla tai eri ohjelmalla. Sovellus voidaan korvata toisella sovelluksella niin kauan kuin molemmat sovellukset on tehty ConfigMgr-hallintakonsolin kautta (Agerlund 2012).

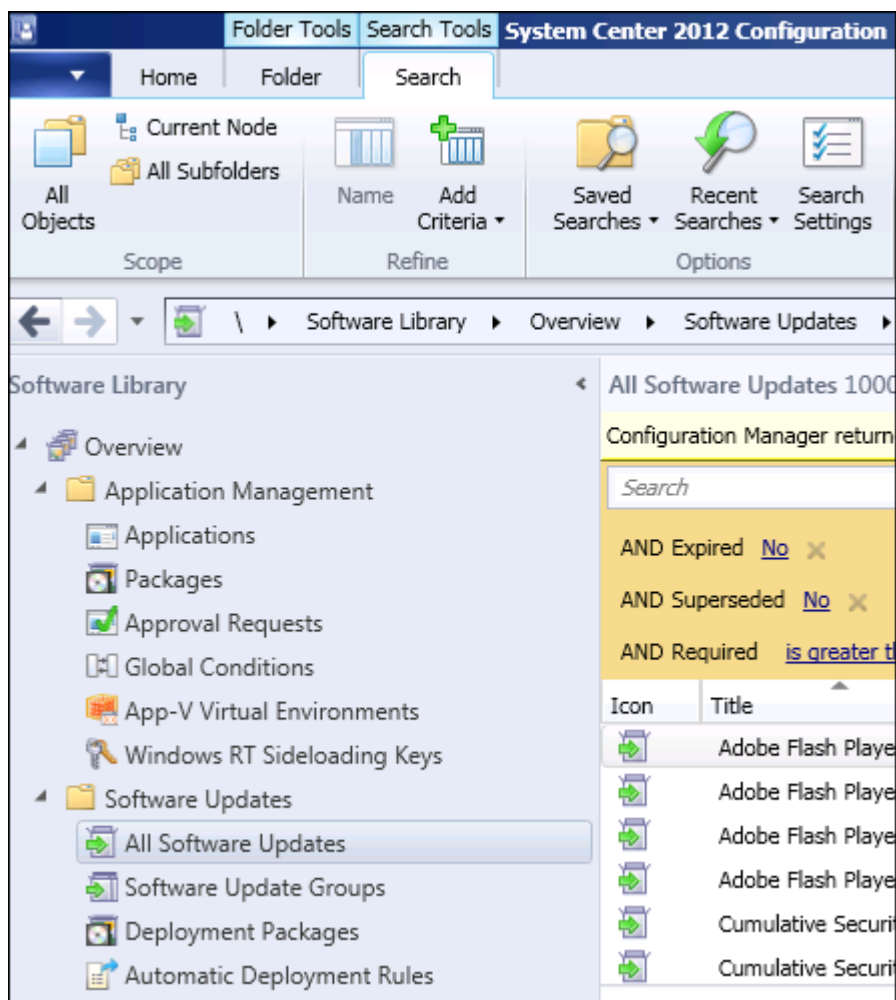
Käyttöönototavan valitseminen on merkittävä kohta sovellusta luotaessa. Käyttöönototapaa voisi verrata ohjelmistopakettien ohjelmaan, eli se sisältää komentorivikomennot ja alustavaatimukset (vaatimuksena voisi olla esim. 64-bittinen Windows 7), mutta näiden lisäksi vielä paljon muuta informaatiota. Tällaista tietoa on mm. tunnistamistapa, jolla vahvistetaan, onko sovellus asentunut, ja määritetään, korvataanko sovelluksella joku toinen. Käyttöönototapa määrittää myös loppukäyttäjäkokemuksen, eli milloin ja kuinka paljon käyttäjille näytetään ilmoituksia sovelluksen asentamisen aikana. Yhdelle sovellukselle voi olla useita käyttöönototapoja, eli ohjelmasta voi olla eri asennukset x86- ja x64-suoritinarkkitehtuuria käyttäville käyttöjärjestelmille. Kun käyttöönototapa on tehty oikein ja sovellus jaeltu, ohjelmisto arvioi käyttöönototavan, jonka jälkeen määritetään oikea tapa kyseessä olevalla järjestelmälle. Näin esimerkiksi x86-version Windows 7:lle asennetaan sovelluksen x86-versio. Myös sovelluksen riippuvuus jostain muusta voidaan määrittää, eli jos järjestelmässä täytyy olla asennettuna esimerkiksi .NET Framework 3.5 ennen kuin sovellusta voidaan asentaa, tämä tieto voidaan lisätä käyttöönototapaa luotaessa (Meyler ym. 2012).

ConfigMgr 2012 SP1:ssä on useita erityyppisiä käyttöönototapoja. Käyttöönototavan luomiseen tarkoitettu asennusvelho osaa myös tunnistaa käyttöönototavan tiedot erilaisista asennustiedostoista. Tämä on kätevää esimerkiksi siinä tapauksessa, että ohjelmistosta on olemassa Windows Installer -tiedosto (MSI-tiedosto), jonka tiedot asennusvelho osaa tunnistaa automaattisesti. Tällöin ylläpitäjän ei välttämättä tarvitse itse asettaa komentorivikomentoja tai muita sovelluksen tietoja. Muita käyttöönototapoja ovat mm. Windows Mobile Cabinet -tiedosto (CAB-tiedosto), Microsoft Application Virtualization (.xml-tiedosto), Microsoft Application Virtualization 5 (.appv-tiedosto) ja Windows Phone app -paketti (.xap-tiedosto). Myös Android app -pakettien (.apk-tiedosto) ja iOS app -pakettien käyttöönototyypit ovat tulleet mukaan ConfigMgr 2012 SP1:stä lähtien (Documentation Library for...2013, 1503–1505).

2.9 Ohjelmistopäivitysten hallinta

Tehokas ohjelmistopäivitysten hallinta on erittäin tärkeä osa-alue verkkoinfrastruktuurin tietoturvan ja vakauden kannalta (Documentation Library for...2013, 1592). Kyberturvallisuutta käsittelevässä Hacking Exposed 7 -teoksessa on kymmenen kohdan lista turvallisuushaavoittuvuuksista, ja päivittämättömät ohjelmistot ovat listalla heti toisena

heikkojen salasanojen jälkeen (McClure, Scambray & Kurtz 2012). Configuration Manager 2012 mahdollistaa päivitysten tarkastamisen ja jakelun kaikille tuetuille Microsoftin käyttöjärjestelmille, suurimmalle osalle palvelintuotteita, ja tietyille työpöytäsovel-
luksille kuten esim. Microsoft Officelle (Meyler ym. 2012). Kuvassa 5 on näkymä oh-
jelmistopäivityksistä hallintakonsolissa.



KUVA 5. Näkymä hallintakonsolin Software Library -työtilasta (Configuration Manager 2012 SP1 2013, kuvankaappaus)

2.9.1 WSUS ja WUA

ConfigMgr:lle ominaisesti se käyttää ohjelmistopäivityksissä jo olemassa olevia komponentteja, WSUS:a ja Windows Update -agenttia (WUA) (Meyler ym. 2012). Ohjelmistopäivitysprosessiin käytetään Microsoft Update -palvelua josta WSUS-palvelin synkronoi päivitysten metatiedot (Documentation Library for...2013, 1593). Aktiivinen ohjelmistopäivityspiste synkronoi vuorostaan metatiedot WSUS-palvelimelta, joiden

perusteella ConfigMgr-asiakkaat suorittavat skannauksen ja raportoivat yhteensopivuus-tilatiedot ConfigMgr-palvelimelle hallintapisteen kautta. Skannaukseen käytetään Windows Update -agenttia, joka määrittää, mitkä päivitykset ovat välttämättömiä järjestelmälle. Agentti hoitaa myös päivitysten asentamisen sen jälkeen, kun ne on ConfigMgr:n kautta toimitettu jakelupisteelle (Agerlund 2012; Meyler ym. 2012).

WUA:n osalta on hyvä muistaa, että se voidaan konfiguroida manuaalisesti tai ryhmäkäytäntöjen kautta lataamaan ja asentamaan päivityksiä automaattisesti. Vaikka ConfigMgr olisi konfiguroitu suorittamaan ohjelmistopäivityksiä, ja siten käyttämään agenttia, voi agentti silti olla myös itsenäisesti toiminnassa ja aiheuttaa näin ongelmia ylläpitäjälle laitteiden yllättävien uudelleenkäynnistysten ja päivitysasennusten myötä (Meyler ym. 2012). Asetukset kannattaakin tarkistaa siinä vaiheessa, kun ohjelmistopäivityksiä aletaan tehdä Configuration Managerin avulla.

2.9.2 Ohjelmistopäivityksiin liittyviä termejä

Ohjelmistopäivityspaketti on kuin mikä tahansa paketti ConfigMgr:ssä, mutta se sisältää pelkästään ohjelmistopäivitysten binääritiedostot (Agerlund 2012). Pakettiin voidaan koota kaikki päivitykset tietyltä ajalta, mikä helpottaa ja selkeyttää niiden hallittavuutta. Ohjelmistopäivitysryhmiin (Software Update Group) voidaan koota päivityksiä ja jaella niitä yhdessä samoilla parametreilla. Päivitysryhmät eivät kuitenkaan sisällä itse päivityksiä, vaan pelkän lähdeluettelon niistä, mikä helpottaa päivitysten organisointia hallintakonsolissa. Kun päivityksiä halutaan jaella asiakkaille, täytyy ne ladata ja asettaa saataville käyttöönottopakettien (Deployment Package) avulla. Käyttöönottopaketti on kuten ohjelmistopaketti. Se sisältää tiedostot, jotka tarvitaan päivityksen tekemiseen (Meyler ym. 2012).

Automaattinen käyttöönottosääntö (Automatic Deployment Rule, ADR) on ConfigMgr 2012:n uusi ominaisuus ja iso parannus edelliseen versioon nähden, jossa ei ollut mahdollisuutta automaattisesti ladata ja asentaa ohjelmistopäivityksiä. Etenkin Endpoint Protection -tietoturvaohjelmiston viruskuvausten määritystiedostojen päivittämisen kannalta ADR on todella hyödyllinen ominaisuus, koska näitä tiedostoja joudutaan päivittämään laitteille useita kertoja päivässä (Meyler ym. 2012).

2.10 Endpoint Protection

Microsoftin päätös integroida tietoturvaohjelmisto Endpoint Protection kokonaan ConfigMgr 2012:n yhteyteen oli looginen askel, joka mahdollistaa ConfigMgr-asiakkaiden hallinnan ja tietoturvasta huolehtimisen saman hallintakonsolin avulla (Meyler ym. 2012). Täyden integroinnin ansiosta Endpoint Protectionille ei tarvitse asentaa omaa raportointipalvelinta tai tietokantaa (Agerlund 2012).

ConfigMgr:ssä on Endpoint Protectionia varten oma saittijärjestelmäroolinsa, Endpoint Protection -piste. Sen konfiguroiminen on suhteellisen yksinkertainen tehtävä, mutta ensin kannattaa suunnitella tarkasti, miten Endpoint Protection -asiakasohjelma suunnataan erilaisille laitteille kuten työasemille tai palvelimille. On myös hyvä käytäntö tehdä erilliset muokattavat haittaohjelmakäytännöt ja kohdistaa ne haluttuihin kokoelmiin, koska erilaisille laitteille (esim. SQL-palvelin vrt. Windows-työasema) joudutaan kuitenkin konfiguroimaan erilaiset tietoturvaohjelman asetukset. Microsoft tarjoaa useita ennalta määritettyjä käytäntöjä esim. erityyppisille palvelimille, joita voi muokata oman ympäristönsä tarpeiden mukaisiksi (Meyler ym. 2012).

Endpoint Protection -asiakkaiden viruskuvaukset voidaan päivittää useasta eri lähteestä. Jos halutaan täysi kontrolli ja yksi päivityslähde, voidaan asiakaskoneet määrätä hakemaan päivitykset aina ConfigMgr:n kautta. Asiakkaiden voidaan kuitenkin sallia hakea päivitykset tarvittaessa muistakin lähteistä, esim. jostain tietystä verkkojaosta tai suoraan Windows Updaten kautta. Tämä lisää tietoturvaa tilanteissa, joissa laitteella ei ole yhteyttä hallintapisteeseen, jolloin uudet viruskuvaukset eivät yhteysongelman takia jää päivittämättä (Meyler ym. 2012).

Endpoint Protection voidaan konfiguroida lähettämään hälytyksiä sähköpostilla, kun se löytää joltain laitteelta viruksen tai haittaohjelman. Hallittavan ympäristön haittaohjelmatilannetta voidaan valvoa päivittäin myös ConfigMgr-konsolista käsin tai Endpoint Protection -raporttien avulla (Agerlund 2012). Kuvassa 6 on nähtävillä erilaiset sähköpostihälytystyyppit, jotka Configuration Manager sisältää.

New Subscription

Specify a name, one or more email addresses and a selected language for this subscription. You can separate multiple email addresses with a semicolon (;).

Subscription name: Hälytykset

Email address: [redacted]@ahlman.fi

Email language: English (United States)

Selected alerts:

Filter...

| Alert |
|--|
| <input checked="" type="checkbox"/> Generate alert when malware detected - Malware detection alert for collection: EP ... |
| <input checked="" type="checkbox"/> The same malware detected on a number of computers - Malware outbreak alert for... |
| <input checked="" type="checkbox"/> Same malware repeatedly detected on a computer - Repeated malware detection a... |
| <input checked="" type="checkbox"/> Multiple types of malware detected on a computer - Multiple malware detection alert... |
| <input checked="" type="checkbox"/> Critical low free space alert for database on site: PS1 |
| <input checked="" type="checkbox"/> Warning low free space alert for database on site: PS1 |
| <input checked="" type="checkbox"/> Database Replication component failed to run on site PS1 |
| <input checked="" type="checkbox"/> Low Sideload Activation |
| <input checked="" type="checkbox"/> Synchronization failure alert for software update point: [redacted]Ahlman.fi (PS1) |
| <input checked="" type="checkbox"/> Site backup task failure alert at site: Ahlman (PS1) |

OK Cancel

KUVA 6. ConfigMgr voidaan konfiguroida lähettämään tarvittaessa erilaisia sähköpostihäilytyksiä (Configuration Manager 2012 SP1 2013, kuvankaappaus).

3 LÄHTÖKOHDAT JA TESTAUS

3.1 Lähtötilanne

Työ aloitettiin siitä lähtökohdasta, että valitaan Microsoftin keskitetyn hallinnan ratkaisu, koska sen tiedettiin olevan edullinen vaihtoehto oppilaitosympäristöön hankittaessa. Myös se, että lähes kaikki Ahlmanilla käytössä olevat laitteet palvelimia myöten käyttävät Windows-käyttöjärjestelmää, vaikutti ratkaisuun.

Tässä vaiheessa ratkaisuvaihtoehtoja oli kaksi, Windows Intune ja System Center 2012 Configuration Manager. Intuneen tutustuttiin nopeasti ja pintapuolisesti asentamalla 180 vuorokauden mittainen kokeiluversio testiympäristöön ja testaamalla muutaman pienen ohjelman jakelua testilaitteille. Intune toimi moitteitta ja oli helppo ja nopea asentaa, mutta ohjelmiston luonne täysin pilvipohjaisena ratkaisuna ei sovellu kovin hyvin Ahlmanin tyypiseen ympäristöön, jossa hallittavia laitteita on paljon. Kun kaikki ylläpito-toimiin liittyvä verkkoliikenne kulkee jokaiselta hallittavalta laitteelta Internet-yhteyden kautta Microsoftin pilveen, kuormittaisi Intunen käyttö valtavasti Ahlmanin yhteyksiä sisäverkon ja ulko-verkon välillä. Configuration Manager on myös kokonaisuudessaan huomattavasti laajempi ohjelmisto ja sisältää paljon ominaisuuksia, joita Intunessa ei ole. Intune on kuitenkin mahdollista integroida myöhemmin käyttöön yhdessä ConfigMgr:n kanssa, joka mahdollistaa esim. mobiililaitteiden keskitetyn hallinnan.

3.2 Configuration Managerin asentaminen ja konfigurointi testiympäristöön

Keskitetyn hallinnan suunnitteleminen aloitettiin testiympäristön toteuttamisella. Ympäristöön päätettiin asentaa aluksi kaksi palvelinta (SERVER11 ja SERVER12) ja kaksi asiakaskonetta (ASIAKAS1 ja ASIAKAS2). Testiympäristön rakentamiseen ei käytetty virtualisointia, vaan kaikki neljä konetta olivat fyysisiä laitteita. Palvelinten käyttöjärjestelmäksi valittiin Windows Server 2008 R2, koska se on käytössä myös muissa organisaation palvelimissa. Asiakaskoneiden käyttöjärjestelmänä käytettiin 64-bittistä Windows 7 Enterprise N:ää. SERVER11-palvelimelle perustettiin toimialue TESTIHUONE.LOCAL, joten palvelimesta tuli myös toimialueen ohjauskone. Ohjauskoneelle

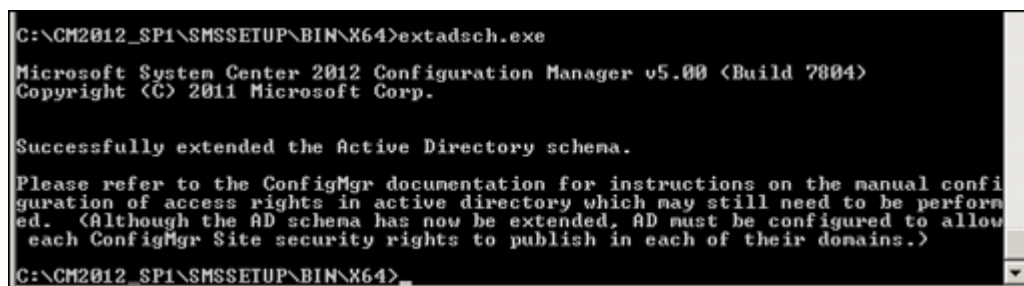
asennettiin lisäksi myös DNS-nimipalvelurooli. Kaikissa laitteissa käytettiin staattisia IP-asetuksia, joten DHCP-palvelua ei testiympäristöön asennettu.

3.2.1 Ennakkotoimenpiteet Active Directory -ympäristössä

Ennen Configuration Managerin asentamista Active Directory -ympäristöön voidaan tehdä joitain toimenpiteitä helpottamaan ohjelmiston käyttöönottoa. Active Directory -rakenteen laajentaminen ei ole välttämätöntä, mutta se helpottaa ylläpidon työskentelyä (Agerlund 2012). Kaikki objektit, kuten käyttäjät, tietokoneet ja tulostimet ovat AD-rakenteessa määritettyjen luokkien ilmentymiä. Luokilla on omat attribuutinsa, joilla luokan jäseniä kuvaillaan, esim. tietokone-luokan objektilla on nimi, käyttöjärjestelmä jne. Järjestelmänvalvojat voivat määrittää rakenteeseen uusia luokkia ja muokata jo olemassa olevia (Meyler ym. 2012).

Kun rakennetta laajennetaan, voidaan siten tietoja julkaista AD-toimialueen palveluissa (Documentation Library for...2013, 363). Yhtenä esimerkkinä tästä on asiakkaan ja palvelimen väliseen liikenteeseen käytettävien porttien konfigurointi. Kun asiakasohjelma asennetaan, konfiguroidaan se tiedolla, mitä porttia palvelimen kanssa kommunikoidessa käytetään. Jos porttitietoja muutetaan siten asetuksista, voi asiakas saada tiedon muutoksesta AD-toimialueen palveluiden kautta. Jos rakennetta ei ole laajennettu, täytyy muutos saada asiakasohjelman tietoon muulla tavoin, esim. komentosarjan avulla (Documentation Library for...2013, 366). Jos rakennetta on laajennettu esim. Configuration Manager 2007:ää varten, ovat samat laajennukset voimassa, eikä laajennusta tarvitse tehdä uudelleen (Agerlund 2012).

Active Directory -rakenteen laajennus tehdään ohjauskoneella ConfigMgr 2012 -asennustiedostojen avulla. Ensiksi avataan komentokehote järjestelmänvalvojana, siirrytään asennustiedostot sisältävään sijaintiin ja ajetaan extadsch.exe. Tämän jälkeen varmistetaan C:n juuressa olevasta extadsch.log-tiedostosta laajennuksen onnistuminen (Agerlund 2012). Testiympäristössä AD-rakenne laajennettiin SERVER11:llä. Kuvassa 7 on komentokehote AD-rakenteen laajentamisen jälkeen.



```

C:\CM2012_SP1\SMSSETUP\BIN\X64>extadsch.exe

Microsoft System Center 2012 Configuration Manager v5.00 (Build 7804)
Copyright (C) 2011 Microsoft Corp.

Successfully extended the Active Directory schema.

Please refer to the ConfigMgr documentation for instructions on the manual configuration of access rights in active directory which may still need to be performed. (Although the AD schema has now been extended, AD must be configured to allow each ConfigMgr Site security rights to publish in each of their domains.)

C:\CM2012_SP1\SMSSETUP\BIN\X64>

```

KUVA 7. AD-rakenteen laajentaminen (Windows Server 2008 R2 2009, kuvankaappaus)

Kun rakenne on onnistuneesti laajennettu, täytyy tehdä vielä joitain toimenpiteitä ennen kuin ConfigMgr voi tallentaa tietoa Active Directoryyn. Näistä ensimmäinen on System Management -säiliön luominen, jossa ConfigMgr-objektit AD:ssa sijaitsevat (Meyler ym. 2012). Saittipalvelin osaisi luoda säiliön asennuksen aikana, mutta se edellyttäisi täysiä järjestelmänvalvojan oikeuksia saittipalvelimen tietokonetilille System Management -säiliöön nähden. Tietoturvasyistä kaikki saittipalvelimet ja hallintapisteet kannattaa sijoittaa paikalliseen käyttöoikeusryhmään ja tehdä säiliö manuaalisesti adsiedit.msc -työkalulla, jolloin saittipalvelimen tietokonetilille ei tarvitse antaa ylimääräisiä käyttöoikeuksia (Agerlund 2012). Kun System Management -säiliö on tehty, luodaan paikallinen käyttöoikeusryhmä ja annetaan sille oikeudet säiliön käyttämiseen. Testiympäristössä luotiin tätä tarkoitusta varten Service Accounts -organisaatioyksikkö ja sinne käyttöoikeusryhmä ConfigMgr_Servers, johon lisättiin SERVERI2.

ConfigMgr 2012 ja SQL Server 2008 R2 voidaan ajaa paikallisen järjestelmätilin alaisuudessa, mutta tietoturvasyistä molemmille kannattaa tehdä käyttäjätilejä rajoitetuin käyttöoikeuksin ja käyttää niitä palvelutileinä eri tehtäviä varten. Palvelutilejä tehtiin testiympäristöön kaikkiaan kuusi aiemmin luodun Service Accounts -nimisen organisaatioyksikön alle. Luodut tilit olivat CM_NA (Configuration Manager Network Access), CM_JD (Configuration Manager Join Domain), CM_CP (Configuration Manager Client Push), CM_SR (Configuration Manager SQL Reporting), CM_EX (Configuration Manager Exchange Connector) ja CM_SQ (Configuration Manager SQL Service). Taulukossa 1 on lyhyt selvitys jokaisen palvelutilin käyttötarkoituksesta.

TAULUKKO 1. Palvelutilit (Agerlund 2012, muokattu)

| | |
|-------|---|
| CM_NA | Käytetään kun asiakas tarvitsee pääsyn ConfigMgr-infrastruktuuriin eikä voi käyttää sisäänkirjautuneen käyttäjän tunnistetietoja. |
| CM_JD | Käytetään tehtäväjakson aikana kun tietokonetili liitetään toimialueeseen. |
| CM_CP | Käytetään yhdessä client push -asennustavan kanssa. Tili yhdistää admin\$-jakoon asiakkaalla, lataa asiakasohjelman käynnistystiedostot ja luo ccmsetup-palvelun. |
| CM_SR | Käytetään kun halutaan päästä SQL Reporting Services -raportteihin. |
| CM_EX | Käytetään synkronoimaan tietoja Exchange Server 2010:ltä. |
| CM_SQ | Käytetään aloittamaan ja ajamaan tarvittavat SQL Server -palvelut. |

Seuraavaksi lisättiin CM_CP-tili paikallisten järjestelmävalvojen ryhmään ohjauskone SERVER1:n ryhmäkäytäntöjen hallintakonsolin kautta. Tämän jälkeen konfiguroitiin Windowsin palomuuuri saman hallintakonsolin kautta. Palomuuuri asetettiin sallimaan sisäänpäin tuleva tiedostojen ja tulostimien jakamisen poikkeus, sekä etähallinnan poikkeus. WSUS-käytännöt konfigurointiin niin, että sallittiin allekirjoitettu sisältö sisäverkon Microsoft Update -palvelusijainnista, ja automaattiset päivitykset otettiin pois päältä (Agerlund 2012).

3.2.2 SQL-palvelimen asentaminen

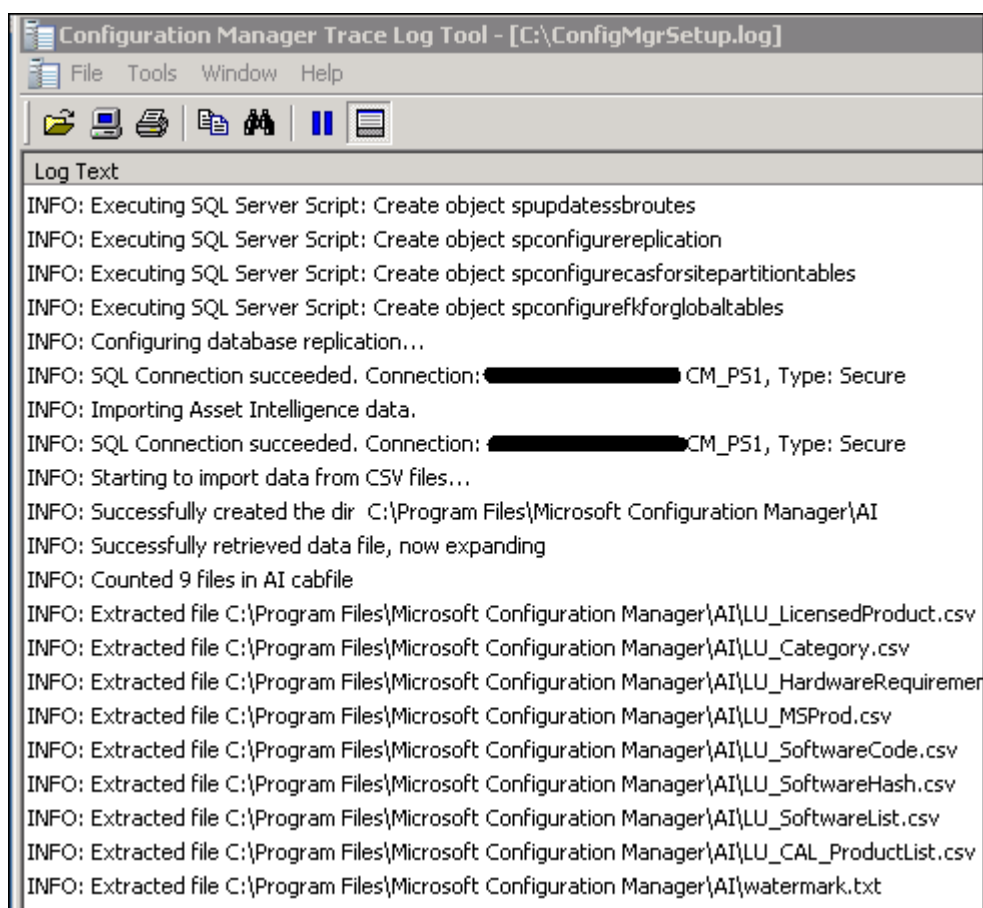
Testiympäristön saittitietokantaa varten asennettiin SQL Server 2008 R2, johon päivitettiin Service Pack 1 ja Cumulative Update 6. Usein tässä vaiheessa Configuration Managerin käyttöönottoprojektia joudutaan tekemään päätös paikallisen SQL-palvelimen ja SQL-etäpalvelimen välillä. Paikallinen SQL-palvelin on yksinkertainen ja aikaa säästävä valinta, ja sen ainoa huono puoli on, ettei se tue yli 50 000 asiakkaan ympäristöä. Testiympäristössä olikin helppo päätyä asentamaan paikallinen SQL-palvelin SERVER12-palvelimelle. Asennus tehtiin komentorivin kautta komentosarja-asennuksena, johon löytyi ohje Agerlundin kirjasta. Asennuksen onnistuminen varmistettiin SQL Server Management Studio -ohjelmiston avulla tietokantakyselyllä, joka palautti tietokannan tuoteversion (Agerlund 2012).

SQL-palvelimen asentamisen jälkeen sille oli konfiguroitava vielä riittävästi muistia. Ilman muistin käytön rajoittamista SQL-palvelin varaa itselleen usein lähes kaiken saatavilla olevan muistin, joten sitä tulee allokoida niin, että huomioidaan myös käyttöjärjestelmän ja muiden sovellusten tarpeet. Yhtenä hyvänä käytännön sääntönä voidaan pitää seuraavaa; 2 gigatavua käyttöjärjestelmälle, 2 gigatavua muille palvelimen sovelluksille, 4 gigatavua ConfigMgr:lle ja 8 gigatavua tai enemmän SQL Server 2008 R2:lle. Tämä edellyttää palvelimella olevan 16 gigatavua muistia, mutta pienissä ympäristöissä (esim. alle 500 käyttäjää) myös 4–8 gigatavua riittää. Tällöin SQL:n muisti pitäisi rajoittaa puoleen kaikesta käytössä olevasta fyysisestä muistista. Muisti konfiguroidaan SQL Management Studio -ohjelmiston kautta (Agerlund 2012).

Lopuksi konfiguroitiin vielä SQL-palvelimen palvelutilit siten, että niillä on domain-käyttäjän oikeudet. Tämä on tietoturvan kannalta parempi ratkaisu kuin ajaa SQL-palveluja paikallisella järjestelmätillä tai toimialueen järjestelmävalvojan tilillä, joiden käyttöoikeudet ovat huomattavasti isommat kuin domain-käyttäjällä. Kun palvelutilinä käytetään käyttäjätiliä, on SPN-nimet eli palvelun päänimet rekisteröitävä toimialueeseen manuaalisesti komentokehoteen kautta (Agerlund 2012).

3.2.3 Saittipalvelimen asentaminen

Ennen saittipalvelimen asentamisen aloittamista halutun hierarkian täytyy olla selvillä, koska ensisijaista saittipalvelinta ei asennuksen jälkeen voi siirtää toiseen hierarkiaan (Agerlund 2012). System Center 2012 Configuration Manager SP1:stä lähtien on kuitenkin ollut mahdollista laajentaa erillinen ensisijainen saitti hierarkiaan keskitetyn hallinnan saitin kanssa (Documentation Library for...2013, 658). Testiympäristöön yksi ensisijainen saittipalvelin oli helppo valinta, koska se nähtiin todennäköiseksi valinnaksi myös Ahlmanin tulevaan ConfigMgr-infrastruktuuriin. Saittipalvelimen asennus suoritetaan asennusvelhon kautta, ja se on melko suoraviivainen toimenpide. Kuvassa 8 on saittipalvelimen asennusprosessin seuranta ConfigMgrSetup.log-tiedostosta.



KUVA 8. Saittipalvelimen asennusprosessia voi seurata CMTrace-ohjelman avulla (Configuration Manager 2012 SP1 2013, kuvankaappaus).

Configuration Managerin asennustiedostoista löytyy CMTrace.exe-ohjelma, joka on tarkoitettu lokitiedostojen lukemiseen. Kaikki ohjelmiston lokitiedostot ovat yksinkertaisia tekstitiedostoja, joten niiden lukemiseen voidaan käyttää montaa eri ohjelmaa, esim. Windowsin Muistiota. Microsoft on kuitenkin perinteisesti lisännyt SMS:n tai Configuration Managerin mukaan tehokkaamman työkalun lokien seuraamiseen. Se parantaa luettavuutta mm. korostamalla eri väreillä erityyppiset rivit (virhe punaisella, varoitus keltaisella jne.). CMTrace päivittää myös lokitiedostoa reaaliaikaisesti ja sisältää hyvät hakutoiminnot lokien tarkasteluun (Meyler ym. 2012). Kun saittipalvelimen asennusvelho on suoritettu loppuun, voidaan asennuksen edistymistä seurata ConfigMgrSetup.log-tiedostosta CMTracen avulla. Kun ydinpalveluiden asentaminen on suoritettu, tapahtuu taustalla edelleen paljon eri komponenttien konfigurointia ja asentamista. Näiden edistymistä ja onnistumista voidaan seurata sijainnista Program Files\Microsoft Configuration Manager\Logs, josta löytyvät lokitiedostot Sitecomp.log ja hman.log. Näistä ensiksi mainittu on ConfigMgr-komponenttien asentamisesta vastuus-

sa olevan Site Component Managerin lokitiedosto. Jälkimmäinen on mm. AD:n päivittämisestä vastuussa olevan Hierarchy Managerin lokitiedosto (Agerlund 2012).

System Center 2012 Configuration Manager asennettiin SERVER12-palvelimelle, joloin siitä tuli automaattisesti ensisijainen saittipalvelin. Samalle palvelimelle oli jo aiemmin asennettu palvelinroolit Windows Deployment Services ja Web Server (IIS), jota Configuration Manager käyttää eri toiminnallisuuksien, kuten esimerkiksi sovellusluettelon toteuttamiseen (Meyler ym. 2012).

Saittipalvelimen asentamisen jälkeen luotiin lähdehakemisto kaikille tiedostoille, joita tullaan tarvitsemaan esim. sovellusten jakelussa, ohjelmistopäivityksissä ja muissa Configuration Managerin avulla suoritettavissa tehtävissä. Testiympäristössä tehtiin saittipalvelimelle C-aseman juureen jaettu kansio Sources\$, ja sinne alikansiot Updates, Software ja OSD. Updates-kansioon tallennetaan ohjelmistopäivitysten lähdetiedostot, Software-kansioon sovellusten lähdetiedostot ja OSD-kansioon käyttöjärjestelmien jakeluun liittyvät tiedostot.

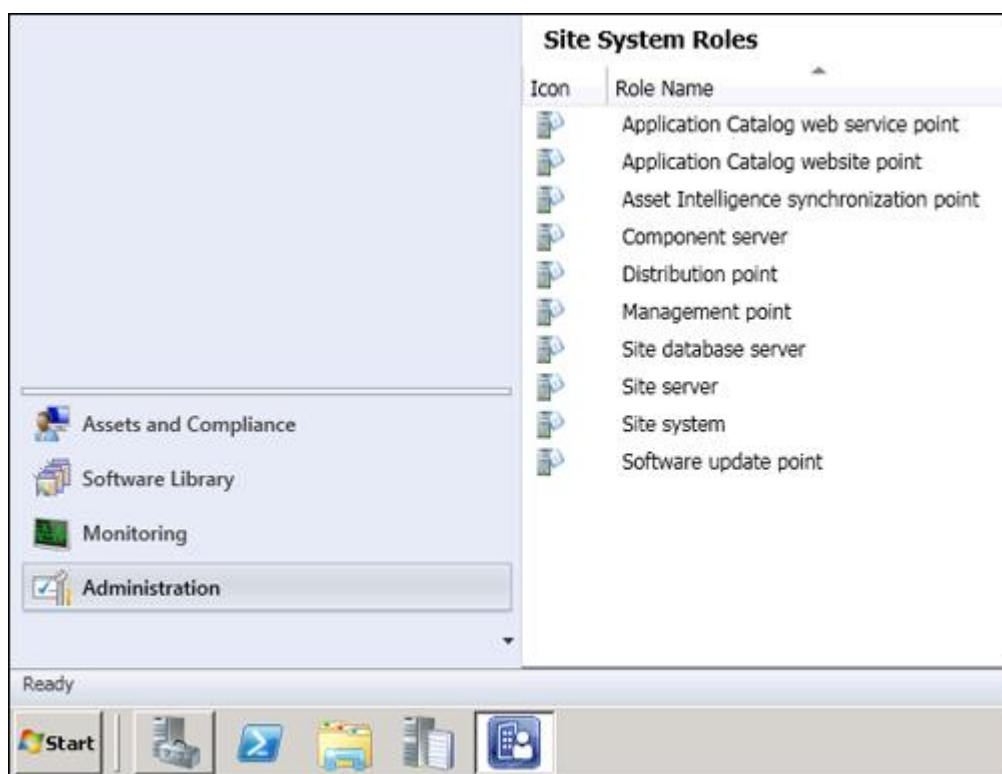
Seuraavaksi asennettiin WSUS-palvelin, joka tarvitaan jokaiselle ensisijaiselle saitille ja CAS-saitille. Vaikka ohjelmistopäivityksiä hallitaan ConfigMgr-hallintakonsolin kautta, on WSUS kuitenkin aina asennettava. Lopuksi konfiguroitiin vielä SQL -raportointipalvelut, joiden avulla voidaan tuottaa erilaisia raportteja ConfigMgr-tietokannasta, esim. asiakkaiden tilanteesta (Documentation Library for...2013, 862).

3.2.4 Saittipalvelimen konfigurointi

Saittipalvelimen konfigurointi edellyttää enemmän suunnittelua ja pohtimista kuin asentaminen, koska ohjelmistossa on paljon ominaisuuksia, ja ne voidaan asentaa yhdelle tai useammalle palvelimelle. Eri ominaisuuksilla on omat saittijärjestelmäroolinsa, joiden asentaminen riippuu siitä, mitä ominaisuuksia ympäristössä halutaan ottaa käyttöön. Keskisuurissa ja yritystason asennuksissa on yleistä, että käyttäjien kanssa kontaktissa olevia saittijärjestelmärooleja ei asenneta ensisijaiselle saittipalvelimelle suorituskysyistä. Tämä ei kuitenkaan ole välttämätöntä (Agerlund 2012). Testiympäristössä päätettiin keskittyä ohjelmistopäivitysten ja sovellusten jakelun kokeilemiseen, koska ne olivat ominaisuuksia, joille katsottiin olevan pian tarvetta myös oikeassa tuotantoympä-

ristössä. Testausvaiheen lopussa kokeiltiin vielä nopeasti Endpoint Protection 2012:n, eli Microsoftin tietoturvaohjelmiston asentamista laitteille. Tämä tehtiin sen jälkeen, kun oli tehty päätös, että se otetaan käyttöön myös todellisessa ympäristössä.

Kaikki saittijärjestelmäroolit päätettiin asentaa SERVERI2-palvelimelle. ConfigMgr-saitin asennuksen yhteydessä asentuu oletuksena joitain saittijärjestelmärooleja, jotka ovat välttämättömiä saitin ydintoimintojen kannalta. Näitä rooleja ovat mm. saittipalvelin, saittijärjestelmä ja saittitietokantapalvelin. Näiden lisäksi myös jakelupiste ja hallintapiste asennetaan saittipalvelimelle automaattisesti, kun asennetaan ensisijainen tai toissijainen saitti (Documentation Library for...2013, 431–433). Automaattisesti asennettujen roolien lisäksi SERVERI2:lle asennettiin sovellusluettelon verkkopalvelupiste, sovellusluettelon verkkosivustopiste, resurssitietojen synkronointipiste, raportointipalvelupiste ja ohjelmistopäivityspiste. Ohjelmistopäivityspisteen asentamisen yhteydessä valittiin tuotteet (esim. Windows Server 2008 R2 ja Windows 7) joiden päivityksiä voidaan sen kautta asentaa. Päivitettäviä tuotteita voidaan tarvittaessa lisätä myöhemmin hallintakonsolin kautta. Jos esim. kolmannen osapuolen ohjelmistojen päivittämiseen tarkoitetun System Center Updates Publisher -ohjelman kautta tehdyt ohjelmistopäivitykset eivät synkronoidu, kannattaa käydä tarkistamassa asetuksista, että kaikki halutut tuotteet on varmasti konfiguroitu synkronoitumaan ohjelmistopäivityspisteelle. Kuvassa 9 on näkymä ohjelmiston Administration-työtilasta, jossa nähdään asennetut saittijärjestelmäroolit.



KUVA 9. Asennetut saittijärjestelmäroolit Administration-työtilanäkymässä (Configuration Manager 2012 SP1 2013, kuvankaappaus)

Roolien asentamisen jälkeen suoritettiin järjestelmien etsiminen AD-ympäristöstä. Pienessä testiympäristössä etsintä suoritettiin koko toimialueesta, mutta isommissa toteutuksissa on tärkeää eritellä tarkka LDAP-polku objektien sijaintiin (Agerlund 2012). Testiympäristössä käytettiin viittä etsintätapaa eri tarkoituksiin. AD Forest etsii AD-saitteja ja IP-osoitealueita, AD System tietokoneobjekteja, AD User käyttäjäobjekteja ja AD Group käyttöoikeusryhmiä. Heartbeat-tapa on käytössä oletuksena (Agerlund 2012). Etsinnän aloittamisen jälkeen AD-objekteja alkoi ilmestyä melko nopeasti näkyviin ConfigMgr-hallintakonsoliin.

Seuraavaksi kokeiltiin yhtä ohjelmiston tärkeimmistä ominaisuuksista (Meyler ym. 2012), käyttäjä- ja tietokonekokoelmien tekemistä. Kokoelmat ovat loogisia käyttäjistä ja tietokoneista koostuvia ryhmiä, joita käytetään esim. asiakasasetusten tai sovellusten jakelun kohdentamiseen. Aiemmissa Configuration Managerin versioissa yksi kokoelma on voinut sisältää sekä tietokoneita että käyttäjiä, mutta ConfigMgr 2012:ssa voidaan tehdä pelkästään tietokoneista tai käyttäjistä koostuvia kokoelmia (Meyler ym. 2012). Kokoelmia voidaan tehdä erikseen ohjelmiston eri käyttötavoille, eli omat kokoelmat esim. ohjelmistopäivityksiä, Endpoint Protectionia ja sovellusten jakelua varten. Testiympäristössä tehtiin ohjelmistopäivityksiä varten useita erilaisia kokoelmia, esim.

palvelimille ja työasemille omansa. Näiden lisäksi molempiin tehtiin vielä erilliset pilot-tikokoelmat, minkä tarkoituksena on, että ohjelmistopäivitykset voidaan ensin kohdistaa pienemmälle kokeiluryhmälle ja vasta toimivuuden varmistuttua kaikille laitteille.

Lopuksi asennettiin vielä asiakasohjelmat kaikille testiympäristön neljälle laitteelle. Ennen tätä tarkastettiin asiakkaiden oletusasetukset, jotka jokainen asiakas lataa itselleen automaattisesti. Eri kokoelmille voidaan tehdä omia asiakasasetuksia, ja ristiriitatilanteessa ConfigMgr-agentti hyväksyy alhaisimman prioriteetin asetukset (Agerlund 2012). Asennus tehtiin client push -tavalla ConfigMgr-hallintakonsolin kautta.

Kun testiympäristö oli ollut toiminnassa jo jonkin aikaa, päätettiin kokeilla vielä SCEP:n eli System Center Endpoint Protectionin asentamista ja keskitettyä hallintaa ConfigMgr-konsolin kautta. Kokeilu tehtiin tässä vaiheessa, koska aiemmin ei ollut vielä täyttä varmuutta tietoturvaohjelmiston vaihtamisesta. Aluksi tietoturvaohjelmistoa varten tehtiin omat kokoelmat, joiden avulla erilaisia käytäntöjä voidaan jaella erityyppisille laitteille. Tämän jälkeen SERVERI2-saittipalvelimelle lisättiin Endpoint Protection -piste, joka asentaa automaattisesti myös EP-asiakasohjelman saittipalvelimelle. Viruskuvausten päivityksiä varten tehtiin ADR eli automaattinen käyttöönottosääntö, joka määritettiin tarkastamaan uudet päivitykset 8 tunnin välein ja asentamaan ne asiakkaille välittömästi. SCEP:n asentamista ConfigMgr-asiakkaille hallitaan asiakasasetusten kautta. Kun asetuksista käydään vahvistamassa kohta Install Endpoint Protection client on client computers, alkaa tietoturvaohjelmiston asennus niillä asiakkailla, joille asiakasasetukset on kohdistettu. Asennuksen jälkeen määritettiin vielä haittaohjelmakäytännöt, joiden avulla voidaan vaikuttaa mm. siihen, milloin tietokone tarkistetaan haittaohjelmien ja virusten osalta, asetetaanko reaaliaikainen suojaus päälle, ja mistä lähteistä EP-asiakasohjelma lataa viruskuvauksia (Agerlund 2012).

3.3 Havaintoja testauksesta

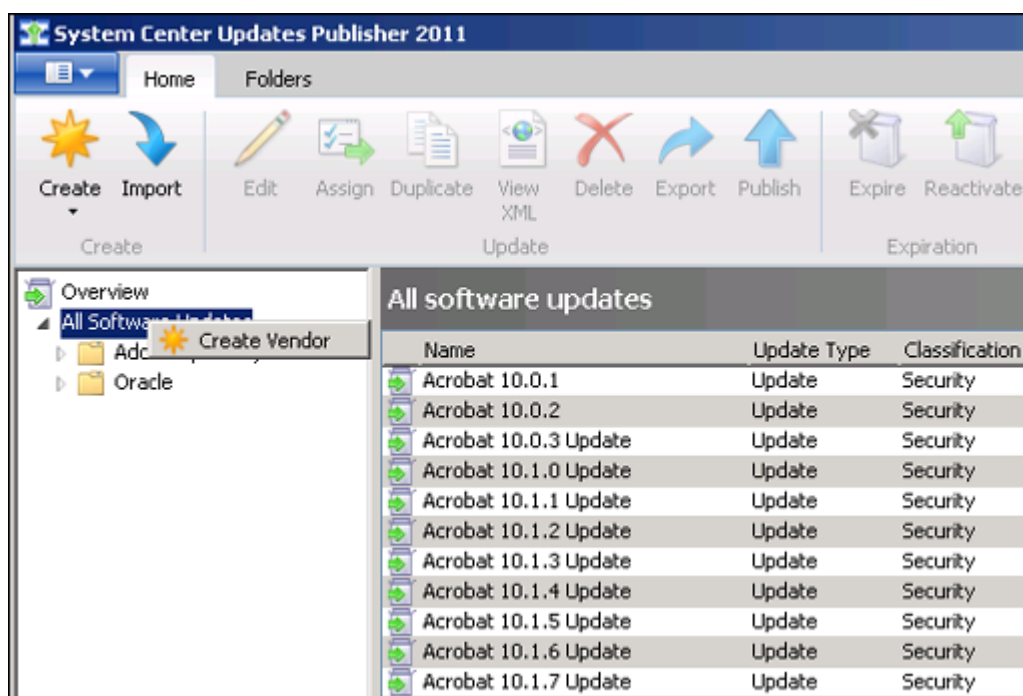
Configuration Manager 2012 saatiin asennettua testiympäristöön ilman suuria ongelmia. Myös asiakasohjelma asentui ASIAKAS1- ja ASIAKAS2-koneille ongelmitta hallintakonsolin kautta client push -asennuksena. Asennusvaiheen jälkeen testiympäristöön lisättiin vielä kaksi asiakaskonetta (ASIAKAS3 ja ASIAKAS4), joissa käytettiin 32-bittistä versiota Windows 7:sta, koska sellaisia on vielä jonkin verran käytössä Ahlma-

nin henkilökunnalla ja opetuskäytössä. Myös nämä AD:hen lisätyt uudet tietokoneobjektit ilmestyivät nopeasti näkyviin ConfigMgr:n hallintakonsoliin.

Configuration Managerin ominaisuuksia kokeiltiin testiympäristössä monipuolisesti, mutta kuitenkin niin, että keskityttiin tarkemmin toimintoihin, jotka aiottiin ottaa käyttöön heti myös oikeassa ympäristössä. Testausvaiheen alussa pidettiin tärkeimpinä Windowsin ohjelmistopäivitysten ja erilaisten sovellusten jakelua laitteille, ja myöhemmin kokeiltiin myös Endpoint Protectionin käyttöä.

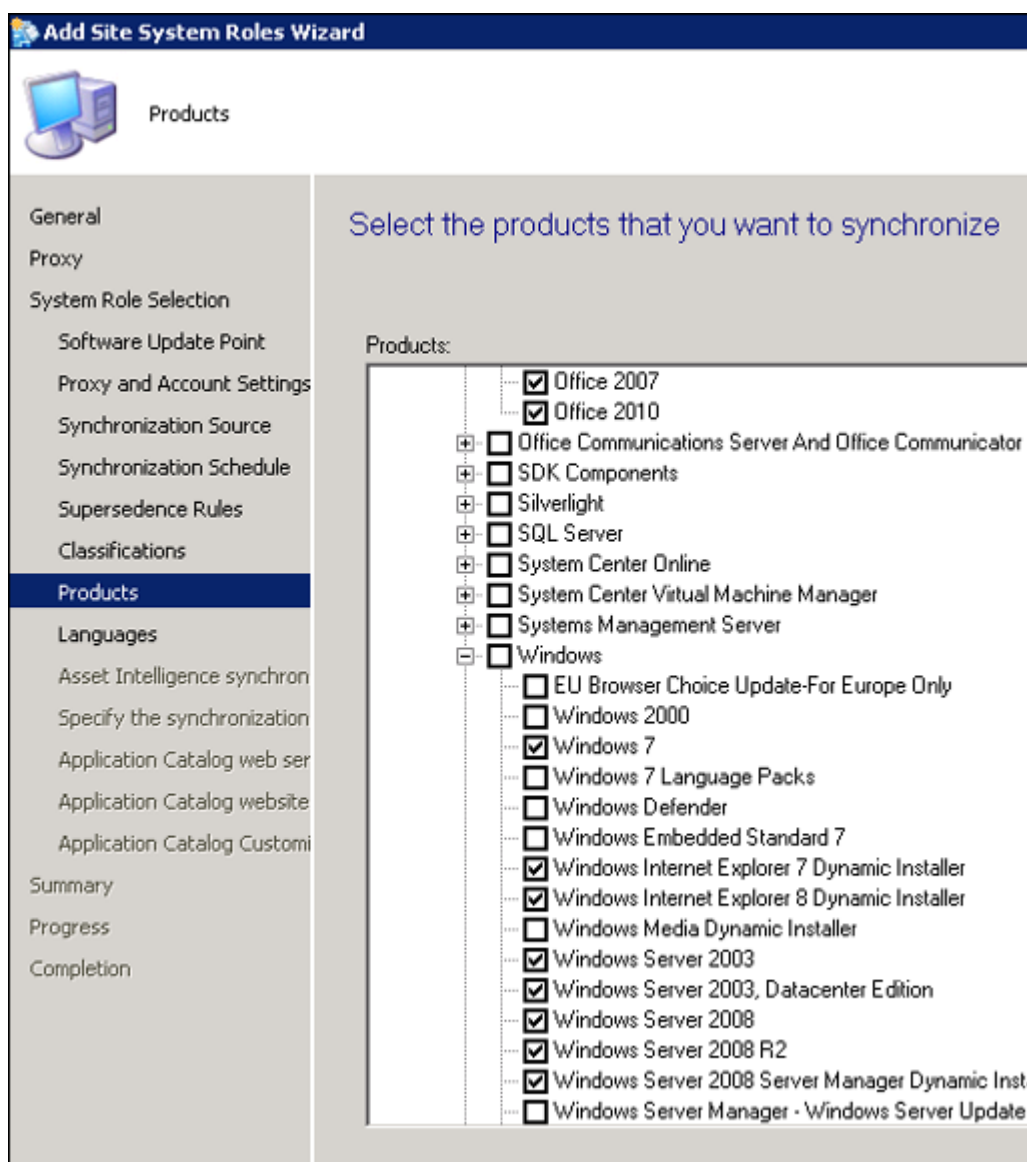
Testauksen aikana ilmeni pieniä ongelmia, joihin löydettiin kuitenkin lopulta ratkaisut. WSUS:n integroiminen ohjelmiston yhteyteen ei onnistunut ensimmäisellä yrityksellä, eikä hallintakonsolin All software updates -näkymään listautunut yhtään päivitystä. Ongelmaan löydettiin selkeä ratkaisu wcm.log-tiedostoa lukemalla. Lokitiedostoon tallentuu WSUS-konfiguraation tapahtumia, ja yhdellä rivillä luki selkeästi, miksei integrointi onnistu; Checking for supported version of WSUS (min WSUS 3.0 SP2 + KB2720211 + KB2734608). Koska en ollut asentanut kuin WSUS 3.0 SP2:n ilman mainittuja päivityksiä, oli ongelman ratkaisu ilmeinen. Kun lokitiedostossa mainitut päivitykset oli ladattu ja asennettu, WSUS ja ConfigMgr alkoivat toimia yhdessä. Näin ohjelmistopäivityspisteen synkronoinnin jälkeen päivitykset alkoivat näkyä ConfigMgr:n hallintakonsolissa.

Toinen ongelma liittyi myös ohjelmistopäivityksiin. Koska Configuration Managerissa ei ole mitään valmista ratkaisua kolmannen osapuolen ohjelmistojen päivittämiseen, otettiin testiympäristössä käyttöön erillinen SCUP 2011 -ohjelmisto. Siihen voidaan ladata vapaasti saatavilla olevia luetteloita eri valmistajien ohjelmille olevista päivityksistä. Käytännössä SCUP:n kautta on saatavilla melko vähän valmiita päivityksiä, ja testauksen myötä kävi selväksi, että useimmiten kolmannen osapuolen ohjelmia päivittäessä ratkaisu täytyy etsiä eri tuotteille erikseen. Kuvassa 10 on näkymä SCUP:n päivityksistä Adobe Acrobat -ohjelman osalta.



KUVA 10. SCUP:n kautta on vapaasti päivitettävissä joitain ohjelmistoja (System Center Updates Publisher 2011 2011, kuvankaappaus)

Adobe on yksi valmistajista, joka tarjoaa SCUP:n kautta tuotteilleen päivityksiä. Testiympäristössä niistä kokeiltiin Flash Playerin päivittämistä. Kun päivitys oli julkaistu SCUP:n kautta WSUS-palvelimelle, suoritettiin manuaalinen ohjelmistopäivityspisteen synkronointi, jotta päivitykset saatiin näkyville myös ConfigMgr-hallintakonsolissa. Päivitykset eivät kuitenkaan ilmestyneet konsoliin, mikä aiheutti ihmetystä, koska ne kuitenkin oli onnistuneesti julkaistu WSUS:lle. Ratkaisu löytyi lopulta ohjelmistopäivityspisteen konfiguroinnista, jossa määritellään, mitä tuotteita, ja minkä tyyppisiä päivityksiä ohjelmistopäivityspisteelle synkronoidaan. Adobe täytyi lisätä niiden valmistajien joukkoon, joiden päivitykset synkronoidaan, ja tämän jälkeen käynnistettiin uudelleen ohjelmistopäivityspisteen synkronointi. Kun se oli valmis, saatiin Flash Player -päivitykset näkyville ohjelmiston hallintakonsoliin ja niiden jakeleminen asiakkaille pystyttiin aloittamaan. Kuvassa 11 on ohjelmistopäivityspisteen asennusvelhon kohta, jossa synkronoitavat tuotteet valitaan.



KUVA 11. Ohjelmistopäivityspisteelle pitää määrittää tuotteet, joiden päivitykset halutaan synkronoida näkyville hallintakonsoliin (Configuration Manager 2012 SP1 2013, kuvankaappaus).

Testausvaiheessa myös kokoelmien merkitys ConfigMgr:n toiminnan kannalta selkeni. Niitä käytetään ohjelmistojen, päivitysten ja korjaustiedostojen jakeluun, asetusten hallinnoimiseen ja moniin muihinkin tehtäviin. Samalla kun kokoelmat ovat ehkä Configuration Managerin tärkein objekti (Meyler ym. 2012), saattavat ne olla myös vaarallisia, jos niiden käyttöä ei harkitse ja suunnittele riittävän tarkasti. Ylläpitäjän täytyy aina olla tietoinen siitä mihin asioihin kokoelman jäsenyyksien muuttaminen voi vaikuttaa. Sovellusten jakelun yhteydessä havaittiin, että kun uuden laitteen lisää olemassa olevaan kokoelmaan, alkaa laite automaattisesti ladata ja asentaa sovelluksia, joita kokoelmalle on aiemmin kohdistettu. Tämä on yksi Configuration Managerin ominaisuuksista, jonka

kanssa pitää olla tarkkana, ettei kokoelmaan lisätylle koneelle vahingossa lataudu ei-haluttuja sovelluksia tai ohjelmistopäivityksiä.

Testausvaihe oli kokonaisuudessaan onnistunut, ja vahvisti edelleen käsitystä siitä, että Configuration Manager 2012 on oikea valinta Ahlmanin IT-ympäristöön työasemien ja palvelimien keskitetyn hallinnan työkaluksi.

4 SUUNNITTELU JA TOTEUTUS

4.1 Suunnittelu

Testausvaiheen jälkeen alettiin valmistella Configuration Manager 2012 SP1:n asentamista ja käyttöönottoa Ahlmanin työ- ja oppilaitosympäristössä. Tavoitteeksi asetettiin kolmen nykyisen ympäristön kannalta erittäin tärkeän perustoiminnon käyttöönotto. Opetuskäytössä ja henkilökunnan käytössä olevien tietokoneiden päivittäminen, sovelusten jakelu ja tietoturvaohjelmisto Endpoint Protection 2012:n käyttöönotto. Endpoint Protectioniin päädyttiin pienentyvien taloudellisten kustannusten perusteella, mutta myös siksi että ohjelmiston hallinta voidaan toteuttaa Configuration Managerin hallintakonsolin kautta. Palvelinten osalta päätettiin niiden päivittäminen hoitaa jatkossakin manuaalisesti.

Lähes kaikki opetuskäytössä olevat työasemat ja osa henkilökunnan käyttämistä koneista sijaitsevat samassa uudessa rakennuksessa, mutta kaikkiaan hallittavia laitteita on n. kymmenessä eri sijainnissa. Rakennusten välisestä tiedonsiirrosta vastaa 1 gigabitin kuiturunkoverkko. Koko sisäverkon reitityksen hoitaa yksi laite, joka toimii samalla palomuurina sisä- ja ulkoverkon välillä. Kytкимиä on n. 10 kappaletta, konfiguroituna useaan eri sijaintiin. Verkossa on neljä virtuaalista lähiverkkoa eli VLANia. Henkilökunnan koneet ovat Toimisto-VLANissa (10.10.10.0/24), opetuskäytössä olevat koneet Oppilaat-VLANissa (10.10.30.0/24). Lisäksi käytössä on langaton Guest-VLAN (10.10.50.0/24) omia laitteita käyttäviä vierailijoita varten, sekä Management-VLAN (10.10.1.0/24) ylläpitotoimia varten.

Suunnitteluvaiheessa jouduttiin pohtimaan, miten Configuration Managerin toimintaan vaikuttaa se, että osa laitteista on pelkästään langattomassa verkossa, koska alueella on muutama rakennus, joihin kuituverkkoa ei ole asennettu. Henkilökunnalla on myös henkilökohtaisessa käytössä olevia kannettavia tietokoneita, jotka eivät ole koko ajan yhteydessä Ahlmanin AD-ympäristöön. Nämä esille otetut seikat eivät kuitenkaan osoittautuneet ongelmaksi, koska testauksen perusteella ConfigMgr voidaan asentaa myös langattoman verkon yli. Se on WLAN-yhteydellä vain jonkin verran hitaampaa. Samanlaisia asennuksia ei myöskään kannata aloittaa liian montaa, koska sen huomattiin kuormittavan langatonta verkkoa. Tämä ei kuitenkaan ole ongelma, koska henkilökun-

nan ConfigMgr-asennuksia ei tehdä samanaikaisesti, vaan usealle päivälle jaoteltuna. Opetuskäytössä olevat koneet, joita asennetaan enemmän samanaikaisesti, ovat langallisessa verkossa.

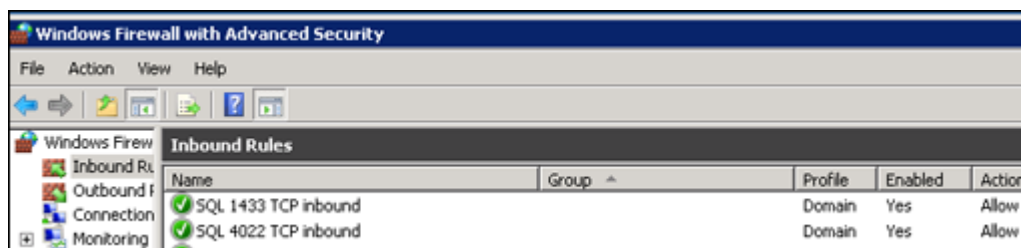
4.2 Asentaminen

Asennusvaiheessa noudatettiin samoja ohjeita kuin testiympäristöön tehdyssä asennuksessa, joten kaikkia kohtia ei enää tässä raportin osassa käsitellä uudelleen. Testiympäristöasennuksen aikana tehdyt muistiinpanot osoittautuivat tärkeäksi apuvälineeksi myös todelliseen käyttöympäristöön tehdyn asennuksen kannalta, koska vaikka testivaiheesta ei vielä ollut kulunut paljoa aikaa, kaikkia asennukseen liittyviä yksityiskohtia oli mahdotonta muistaa tarkasti.

Configuration Manager 2012 SP1:n asentaminen aloitettiin aiemmin käytössä olleen System Center Essentials 2007:n poistamisella. Technetistä löydettiin tähän ohjeet, joiden avulla ohjelmisto saatiin poistettua. Aluksi kirjauduttiin sisään palvelimelle johon SCE:n hallintakonsoli oli asennettu, ja ohjelmisto poistettiin Ohjauspaneelin kautta. Tämän jälkeen ajettiin vielä ohjelmakoodi, jolla varmistetaan, että kaikki AD DS -objektit poistetaan varmasti AD-ympäristöstä. Lopuksi varmistettiin vielä, että ohjelmiston oletussijainnista Program Files\System Center Essentials 2007 ei löydy enää mitään tiedostoja tai kansioita (How to Uninstall System Center Essentials 2013).

Kun SCE 2007 oli poistettu, tehtiin AD-ympäristöön yhden ohjauskoneen kautta samat ennakkotoimenpiteet kuin testiympäristössä. Tämän jälkeen aloitettiin saittipalvelimen asentaminen. Asentaminen tehtiin virtuaalipalvelimelle, josta käytetään tässä raportissa nimeä Ahlman_CM. Se sijaitsee Windows Server 2008 R2 -palvelimella Hyper-V-tekniikan avulla toteutettuna. Kaikki palvelimet sijaitsevat myös Toimisto-VLAN:ssa. Virtuaalipalvelimia on ympäristössä käytössä useampia, joten oli luontevaa asentaa myös ConfigMgr sellaiselle. Saittitietokantaa varten asennettiin SQL Server 2012 asennusvelhoasennuksena (Hampson 2013). Kaikkiin SQL-palveluihin käytettiin tietoturvasyistä samaa toimialuekäyttäjätiliä (CM_SQ) palvelutunnuksena. Tämän jälkeen SQL Server 2012 päivitettiin vielä Service Pack 1- ja Cumulative Update 3 -päivityksillä, ja sille konfiguroitiin neljä gigatavua muistia. Kun saittipalvelimen asennusvelho oli valmis ja Configuration Managerin hallintakonsolista tarkasteltiin saittikomponenttien ti-

laa, huomattiin, että Hierarchy Managerin tila oli kriittinen. Lokitiedostosta hman.log saatiin selville, että SQL-palvelimella (Ahlman_CM) ei ollut konfiguroituna palomuuripoikkeusta, joka sallisi liikenteen portteihin 1433 ja 4022. Kun Windowsin palomuurille konfigurointiin poikkeus näitä portteja varten (Daalmans 2012), ei lokitiedostoon tullut enää tästä syystä lisää virherivejä ja Hierarchy Managerin tilaksi muuttui OK. Kuvassa 12 näkyvät palomuurisäännöt, jotka konfiguroitiin käyttöön Windowsin palomuurin asetuksista.



KUVA 12. Palomuurisäännöt SQL-palvelimelle (Windows Server 2008 R2 2009, kuvankaappaus)

Saittipalvelin konfiguroitiin kuten testiympäristössäkin, eli kaikki saittijärjestelmäroolit asennettiin Ahlman_CM-palvelimelle. Tämä katsottiin selkeäksi ratkaisuksi, koska hallinnoitava ympäristö on sen verran pieni. WSUS asennettiin ja päivitettiin siten, että se voitiin onnistuneesti integroida Configuration Managerin kanssa.

Seuraavaksi etsittiin verkon resursseja samalla periaatteella kuin testivaiheessakin. Käyttäjä- ja tietokoneobjektit alkoivat näkyä ohjelmiston hallintakonsolissa ongelmitta ja nopeasti. Tämän jälkeen tehtiin alustavat tietokonekokoelmat. Kolmelle opetuskäytössä olevalla tietokoneluokalle tehtiin jokaiselle oma kokoelmansa, sekä yksi iso kokoelma, joka sisältää kaikki opetuskäytössä olevat kannettavat koneet ja pöytätietokoneet. Henkilökunnan tietokoneille tehtiin myös oma kokoelmansa. Näiden neljän tietokonekokoelman lisäksi tehtiin vielä pienempiä kokoelmia, joita on tarkoitus käyttää ohjelmistopäivityksissä ja sovellusten jakelussa testausta varten. Käyttäjäkokoelmia ei tässä vaiheessa tehty.

Asiakasohjelman asentuminen tietokoneille ei odotetusti onnistunut ilman lisätoimenpiteitä. Ensin ongelmaksi osoittautui käytössä ollut F-Securen tietoturvaohjelmisto Client Security, joka esti ConfigMgr-asiakasohjelman asentumisen. F-Secure oli tarkoitus muutenkin poistaa, koska Configuration Managerin asentamisen yhteydessä oli päätetty

siirtyä käyttämään Endpoint Protection 2012 -tietoturvaohjelmistoa. EP-asennusohjelma kykenee poistamaan automaattisesti joitakin tietokoneella jo olevia tietoturvaohjelmistoja, mutta F-Secure Client Security ei kuulu tähän joukkoon. Ohjelmisto jouduttiinkin poistamaan kaikista laitteista manuaalisesti, jotta ConfigMgr-asiakasohjelman asennusprosessia voitiin jatkaa. Tämän jälkeen asennus onnistui tietokoneelle, joka oli samassa Toimisto-VLAN:ssa kuin saittipalvelin Ahlman_CM. Kun asiakasohjelmistoa yritettiin asentaa Oppilaat-VLAN:ssa oleville koneille, ei asentaminen onnistunut. Syyksi epäiltiin reititin-palomuuuri-laitetta, joka ei sallinut VLAN:ien välistä liikennettä ja esti näin eri virtuaalisessa lähiverkossa olevien tietokoneiden yhteydenotot Ahlman_CM-saittipalvelimelle. Kun palomuuuriin tehtiin tarvittavat säännöt, alkoi liikenne kulkea myös virtuaalisten lähiverkkojen välillä. Taulukossa 2 on esitetty portit, joita käytetään asiakkaan ja palvelinten väliseen kommunikointiin Configuration Managerissa, ja joiden perusteella palomuurisäännöt tehtiin. Ensimmäinen sarake kuvaa, mitä protokollaa kommunikointiin käytetään. Seuraavissa sarakkeissa on porttinumero sen mukaan, onko käytettävä kuljetuskerroksen protokolla TCP vai UDP. ConfigMgr sallii myös joissain tapauksissa vaihtoehtoisten porttien konfiguroimisen. Mikäli ei haluta käyttää oletusportteja, kannattaa tarkastaa Microsoftin dokumentaatiosta, mihin kommunikointeihin muita porttinumeroita voidaan käyttää.

- > tarkoittaa, että yksi tietokone alustaa kommunikoinnin ja toinen vastaa
 < > tarkoittaa, että kumpikin tietokoneista voi alustaa kommunikoinnin.

TAULUKKO 2. Asiakkaan ja palvelimen välisen liikenteen portit (Documentation Library for...2013, 900–903)

Asiakas > Application Catalog Website -piste

| Kuvaus | UDP | TCP |
|--|-----|-----|
| Hypertext Transfer Protocol (HTTP) | - | 80 |
| Secure Hypertext Transfer Protocol (HTTPS) | - | 443 |

Asiakas > Pilviperustainen jakelupiste

| Kuvaus | UDP | TCP |
|--------|-----|-----|
| HTTPS | - | 443 |

Asiakas > Jakelupiste

| Kuvaus | UDP | TCP |
|--------|-----|-----|
| HTTP | - | 80 |
| HTTPS | - | 443 |

Asiakas > Global Catalog -ohjauskone

| Kuvaus | UDP | TCP |
|-------------------------|-----|------|
| Global Catalog LDAP | - | 3268 |
| Global Catalog LDAP SSL | - | 3269 |

Asiakas > Hallintapiste

| Kuvaus | UDP | TCP |
|---|-----|-------|
| Asiakkaan ilmoitus (oletusilmoitus ennen kuin siirrytään takaisin HTTP:hen tai HTTPS:ään. | - | 10123 |
| HTTP | - | 80 |
| HTTPS | - | 443 |

Asiakas > Ohjelmistopäivityspiste

| Kuvaus | UDP | TCP |
|--------|-----|--------------|
| HTTP | - | 80 tai 8530 |
| HTTPS | - | 443 tai 8531 |

Portit joita käytetään client push -asennuksessa

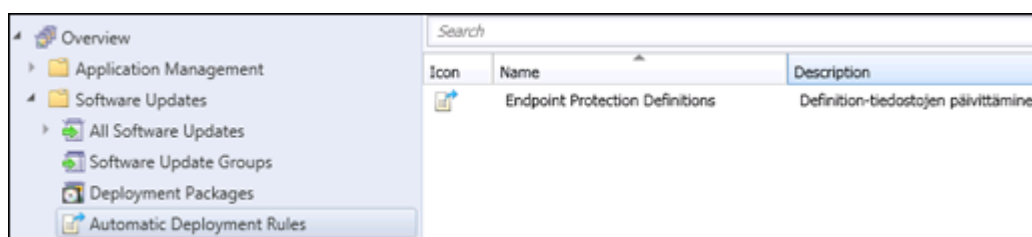
| Kuvaus | UDP | TCP |
|--|-----|------------|
| Server Message Block (SMB) saittipalvelimen ja asiakaskoneen välillä | - | 445 |
| RPC-päätepistekartoitin saittipalvelimen ja asiakaskoneen välillä | 135 | 135 |
| RPC dynaamiset portit saittipalvelimen ja asiakaskoneen välillä | - | Dynaaminen |
| HTTP asiakaskoneelta hallintapisteelle | - | 80 |
| HTTPS asiakaskoneelta hallintapisteelle | - | 443 |

4.3 Endpoint Protection 2012:n käyttöönotto

Endpoint Protectionin käyttöönotto aloitettiin määrittämällä Endpoint Protection -piste saittipalvelimelle. Saittijärjestelmärooli lisätään ConfigMgr-hallintakonsolin Administration-työtilasta, josta valitaan Site configuration, Servers and Site System Roles. Konsolissa näkyy lista ConfigMgr-palvelimista, josta valittiin haluttu palvelin eli tässä tapauksessa Ahlman_CM. Tämän jälkeen valitaan Add Site System Roles, ja avautuvasta valikosta valitaan Endpoint Protection Point. Saittijärjestelmäroolin asennusta voidaan tämän jälkeen seurata saittipalvelimelta EPSetup.log-tiedostosta. Automaattisesti saittipalvelimelle roolin myötä asentuva EP-asiakasohjelma ei ole täydellisesti suojattu, vaan siihen on liitetty erityinen haittaohjelmakäytäntö Reporting Server Default Policy. Reaaliaikainen suojaus ei ole käytössä tässä käytännössä (Agerlund 2012).

EP-pisteen asentamisen jälkeen luotiin viruskuvausten päivitystiedostoja varten samanlainen ADR eli automaattinen käyttöönottosääntö kuin testausvaiheessa. Tämä tehdään hallintakonsolin Software Library -työtilan kohdasta Software Updates, Automatic Deployment Rules. Säännölle annettiin nimeksi Endpoint Protection Definitions, ja se suunnattiin EP Kaikki -kokoelmalle, johon kuuluvat kaikki laitteet, joihin EP asennettiin.

ADR-asennusvelhon Software Updates -sivulta valittiin tuotteeksi Forefront Endpoint Protection 2010 (valikossa käytössä vielä tuotteen vanha nimi!) ja päivityksen luokitte-
luksi Definition Updates. Evaluointiaikatauluksi määritettiin kahdeksan tuntia, jonka
välein automaattinen käyttöönottosääntö toistetaan. Asennuksen takarajaksi asetettiin
As soon as possible, eli viruskuvaukset asennetaan asiakkaille välittömästi, kun ne ovat
saatavilla. Seuraavaksi määritettiin User Experience -sivulta hiljainen asennus, eli Soft-
ware Center ei ilmoita käyttäjälle mitään, kun viruskuvaukset päivitetään. Viruskuvauk-
sille luotiin Deployment Package -sivulta oma käyttöönottopaketti, ja paketille luotiin
oma Definitions-kansio saittipalvelimen Sources\$\Updates-sijaintiin. Tämän jälkeen
valittiin vielä jakelupiste, eli Ahlman_CM. Automaattinen käyttöönottosääntö otetaan
käyttöön valitsemalla sääntö listasta, ja painamalla valintanauhan kohtaa Run Now.
Prosessia voidaan seurata saittipalvelimen ruleengine.log-tiedostosta (Agerlund 2012).
Kuvassa 13 on automaattinen käyttöönottosääntö hallintakonsolinäkymässä.



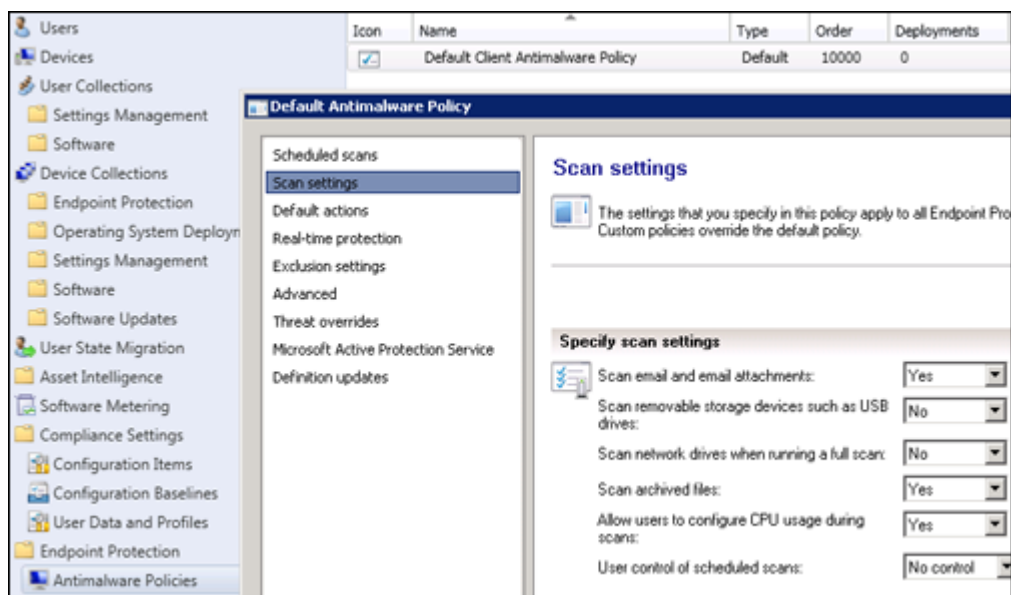
KUVA 13. Automaattinen käyttöönottosääntö hallintakonsolinäkymässä (Configuration Manager 2012 SP1 2013, kuvankaappaus)

SCEP-asiakasohjelman asentumista kontrolloidaan ConfigMgr-asiakasasetusten kautta. Kun ConfigMgr-asiakasohjelma oli asennettu ensimmäisiin opetuskäytössä oleviin tietokoneisiin, asetettiin viidelle koneelle muokatut asiakasasetukset, joissa sallittiin myös SCEP-asiakasohjelman asentaminen. Näin Endpoint Protectionin asentumista haluttiin ensin kokeilla ennen kaikille koneille asentamista. Asiakasohjelma asentui tietokoneille hyvin, mutta viruskuvausten päivittyminen aiheutti ihmetystä, koska joillain asiakkailla saattoi kulua kymmeniä minuutteja tai kauemminkin, että tiedostot päivittyivät.

Ongelmaan löytyi ratkaisu asiakasasetuksia tarkastelemalla. Configuration Manager 2012:ssa on oletuksena päällä asetus, joka estää EP-asiakkaita lataamasta ensimmäisiä asennuksen jälkeisiä viruskuvausten määrittystiedostoja vaihtoehtoisista lähteistä, eli esim. suoraan Internetistä Microsoft Updaten kautta. Jos asetus on päällä, ei asiakas lataa uusimpia viruskuvauksia välittömästi asennuttuaan, vaan vaihtelevan ajan kuluessa

Configuration Managerin kautta (Microsoft Tuotetuki 2012). Kun asetus otettiin pois päältä asiakasasetuksista, lasivat asiakkaat viruskuvaukset heti asennuksen jälkeen ja ilmoittivat tietokoneen tilan olevan suojattu. Ilmeisesti tällainen oletusasetus on tilanteita varten, joissa asennetaan kerralla suuri määrä EP-asiakkaita, eikä haluta, että kaikki hakevat uusimmat viruskuvaukset samanaikaisesti Internetistä. Tämä saattaisi kuormittaa joissain tapauksissa liikaa verkon Internet-yhteyksiä, kun isossa toteutuksessa tuhannet asiakkaat hakisivat yhtä aikaa päivityksiä Microsoft Update -palvelusta. Ahlmän ympäristössä tällaista tilannetta ei kuitenkaan ole, ja viruskuvausten haluttiin päivittyvän heti, kun EP-asiakas on asennettu tietokoneelle, joten oletusasetus otettiin pois käytöstä pysyvästi.

Haittaohjelmakäytäntöjen avulla voidaan hallita, miten asiakkaat suojataan erityyppisiä haitallisia ohjelmia vastaan. Configuration Managerissa on oletuksena käytössä Default Client Antimalware Policy -niminen käytäntö, jonka asetuksia muuttamalla voidaan vaikuttaa Endpoint Protectionin toimintaan (Agerlund 2012). Muutoksia pääsee tekemään hallintakonsolin Assets and Compliance -työtilan kohdasta Endpoint Protection, Antimalware Policies. Kuvassa 14 on näkymä Default Antimalware Policy -asetuksista.

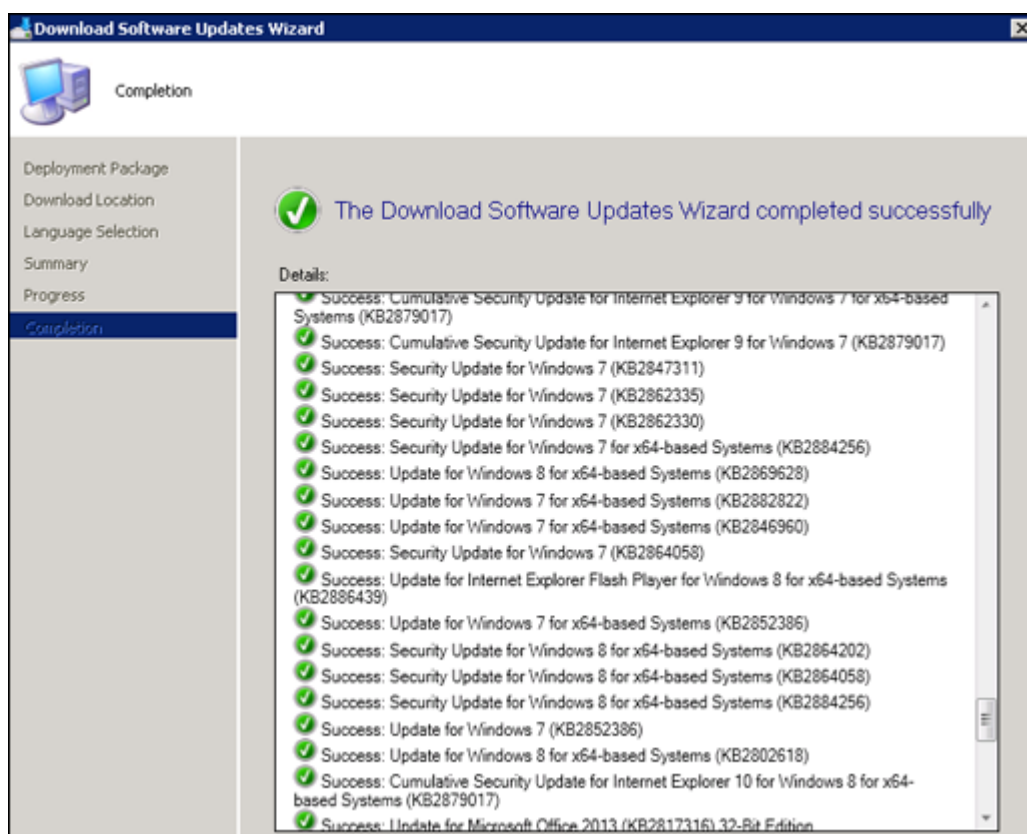


KUVA 14. Skannausasetuksista voidaan valita, mitä kohteita EP tarkistaa (Configuration Manager 2012 SP1 2013, kuvankaappaus)

4.4 Ohjelmistopäivitysten käyttöönotto

Ohjelmistopäivitysten käyttöönotto aloitettiin määrittelemällä niitä varten omat tietokonekokoelmat. Opetuskäytössä oleville koneille määritettiin kuuden koneen pilottikokoelma, jolle ohjelmistopäivitykset asennetaan ensimmäisenä ja näin varmistetaan, että mahdollisen rikkoutuneen ohjelmistopäivityksen vaikutukset rajoittuvat vain pienelle joukolle koneita. Kun päivitykset on onnistuneesti asennettu pilottikokoelmalle, voidaan päivittää loput opetuskäytössä olevat koneet. Henkilökunnan tietokoneille tehtiin kokoelmat samalla periaatteella. Kokoelmille voidaan määrittää myös ylläpitoikkunoita, joiden perusteella ohjelmistoja voidaan asentaa tietokoneille. Laite vastaanottaa ylläpitoikkunat kaikilta kokoelmilta, joihin se kuuluu, joten ikkunoiden luominen edellyttää huolellista suunnittelua (Agerlund 2012).

Vaikka automaattisen käyttöönottosäännön käyttäminen on kätevä tapa ohjelmistopäivityksiä varten, päätettiin ohjelmistopäivitykset ainakin alkuvaiheessa tehdä manuaalisesti. Päivitysryhmän tekeminen aloitetaan ConfigMgr-hallintakonsolin Administration-työtilan kohdasta Software Updates, All Software Updates. Search-kohdasta pääsee antamaan kriteereitä, joilla konsoli päivityksiä listaa, ja kun näytettävien päivitysten kriteereiksi annetaan Required sekä No Expired ja No Superseded, saadaan listattua halutut päivitykset. Kriteerit tarkoittavat, että pitää olla yksi tai useampi asiakas, joka tarvitsee päivityksen, eikä päivitys saa olla asetettu vanhentuneeksi tai tarpeettomaksi. Näin konsoliin saadaan listattua vain ne päivitykset, joita ympäristön asiakastietokoneet tarvitsevat. Haku voidaan myös tallentaa, jolloin seuraavan kerran, kun halutaan tehdä samoilla kriteereillä ohjelmistopäivitysryhmä, voidaan käyttää aiemmin tallennettua hakua. Kun halutut päivitykset on listattu konsoliin, voidaan ne valita listasta ja klikata hiiren oikealla napilla, jonka jälkeen valitaan Create Software Update Group. Kun ohjelmistopäivitysryhmä on luotu, voidaan se ladata ja jaella asiakastietokoneille valitsemalla Deploy, ja seuraamalla asennusvelhon ohjeita (Agerlund 2012). Kuvassa 15 ohjelmistopäivitykset on ladattu onnistuneesti hallintakonsolin kautta.



KUVA 15. Ohjelmistopäivitysten lataaminen on suoritettu onnistuneesti hallintakonsolin kautta. Tämän jälkeen päivityksiä voidaan alkaa jaella asiakastietokoneille. (Configuration Manager 2012 SP1 2013, kuvankaappaus)

Ohjelmistopäivitysten käyttöönotto sujui hyvin, ja päivitykset saatiin jaettua ja asennettua asiakkaille ilman isompia ongelmia. Ensimmäisellä kerralla tosin havaittiin, että kaikki asiakaskoneet eivät saaneet ladattua kaikkia päivityksiä, vaan Software Centeristä katsottaessa osa latauksista jäi pitkäksi aikaa näyttämään 0 %. Tässä vaiheessa havaittiin, että jakelupisteryhmää ei oltu asennusvaiheessa luotu ollenkaan, koska ympäristöön otettiin käyttöön vain yksi jakelupiste, eikä näin ollen ryhmän luomista katsottu tarpeelliseksi. Ryhmä päätettiin kuitenkin varmuuden vuoksi luoda, ja kun jakelupiste lisättiin siihen, alkoivat ohjelmistopäivitykset toimia odotetulla tavalla.

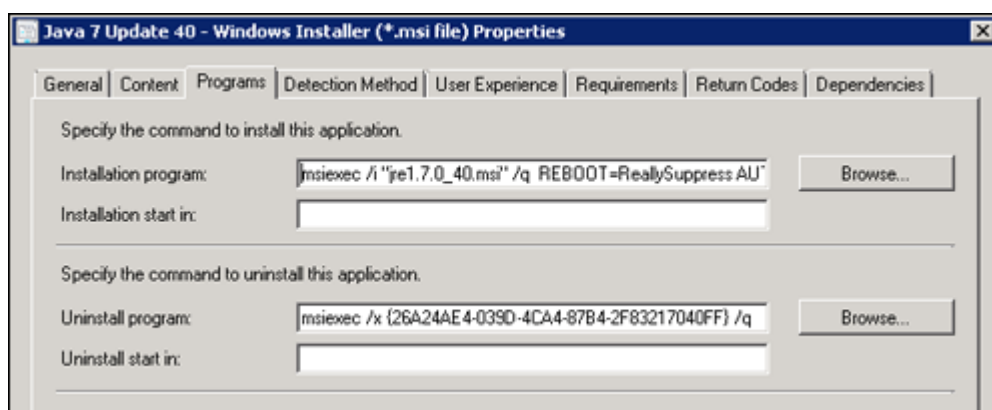
4.5 Sovellusten käyttöönotto

Sovellusten käyttöönoton suunnittelu aloitettiin määrittämällä tärkeimmät sovellukset, jotka haluttiin saada nopeasti keskitetyn jakelun piiriin. Tällaisiksi katsottiin Java sekä käytössä olevat selaimet Internet Explorer, Mozilla Firefox ja Google Chrome. Internet

Explorerin päivittäminen ja uusien versioiden asentaminen onnistuu ohjelmistopäivitysten kautta, joten siitä päätettiin olla tekemättä erillistä sovellusta.

Java on ohjelmointikieli ja tietojenkäsittelyyn käytettävä alusta, jota ilman tietyt sovellukset ja nettisivut eivät toimi (What is Java and why do I need it? 2013). Tietoturvan kannalta Javan käyttö on ongelmallista, koska hyökkääjät ovat käyttäneet sen haavoittuvuuksia hyväkseen hyökkäyksissään. Tästä syystä mm. Viestintävirasto on elokuussa 2012 kehottanut poistamaan Javan käytöstä selaimissa (Tietoturva nyt! 2012). Tämä ei kuitenkaan ole vaihtoehto Ahlmanin ympäristössä, koska tietyt sovellukset, joita opetuksessa käytetään, edellyttävät Javan käyttöä. Tästä syystä on erityisen tärkeää saada päivitettyä Javan uusin versio käyttöön niin opetuskäytössä oleville tietokoneille kuin henkilökunnan kannettaville koneillekin.

Javan päivittämiseen ei ole olemassa yhtä hyvää käytäntöä Configuration Managerin avulla, koska ohjelmisto ei tarjoa mitään tiettyä tapaa kolmannen osapuolen ohjelmistojen päivittämiseen (Agerlund 2012). System Center Updates Publisherin eli SCUP:n avulla voidaan päivittää joidenkin valmistajien ohjelmistoja, mutta sitä ei haluttu ottaa ympäristössä käyttöön ainakaan vielä tässä vaiheessa. Ainoaksi vaihtoehdoksi Javan päivittämiseen jäi sovelluksen tai paketin tekeminen ja sen jakeleminen organisaation tietokoneille. Kuvassa 16 on näkymä Javan päivittämiseen tehdyn sovelluksen asetuksista.



KUVA 16. Sovelluksen tietoja pääsee katsomaan ja muokkaamaan asetuksista (Configuration Manager 2012 SP1 2013, kuvankaappaus)

Sovelluksen tekeminen osoittautui hallintakonsolissa helpoksi, jos asennettavasta ohjelmistosta löytyy esim. MSI-paketti, jonka informaation asennusvelho osaa tunnistaa

automaattisesti. Tämä vähentää virheiden mahdollisuutta, kun ylläpitäjän ei tarvitse itse huolehtia esim. komentorivikomentojen asettamisesta. Valitettavasti ohjelmistoille ei aina ole saatavilla suoraan MSI-pakettia, tai se ei välttämättä sovellu jaeltavaksi asiakas-tietokoneille sellaisenaan. Javan tapauksessakin täytyy ensin ladata asennustiedosto (.exe), jonka purkamalla saadaan esille MSI-tiedosto. Sen avulla voitiin aloittaa sovel-luksen tekeminen ConfigMgr-hallintakonsolin kautta. Google Chrome -selaimesta on saatavilla yritysversio MSI-pakettina, joten myös siitä saatiin tehtyä sovellus ongelmit-ta. Mozilla Firefoxista ei valmista MSI-pakettia löytynyt, joten sen asentamisessa jou-duttiin etsimään ohjeet .exe-asennustiedoston hiljaista asennustapaa varten erikseen.

Kaikki halutut ohjelmistot saatiin asennettua sovelluksina Configuration Managerin kautta opetuskäytössä oleville pöytätietokoneille sekä henkilökunnan kannettaville ko-neille. Yksinkertaisempia toimenpiteitä, kuten pelkän .exe-tiedoston sisältävän CMTra-ce-ohjelman jakelu kaikille laitteille tehtiin luomalla siitä ohjelmistopaketti (Agerlund 2012). Käytännössä huomattiin, että kaikille sovelluksille erikseen tehtävä asennusoh-jeiden etsintä ja kokeileminen vei ensimmäisellä kerralla melko paljon aikaa. Jatkossa käytetty aika toki pienenee, koska esimerkiksi uudelle Mozilla Firefoxin versiolle käy todennäköisesti sama asennustapa kuin aiemmalle.

5 POHDINTA

Configuration Manager 2012:n testaus ja käyttöönotto sujuivat kokonaisuudessaan hyvin, ja myös toimeksiantaja oli lopputulokseen tyytyväinen. Ennen työn aloittamista rajasimme ohjelmistosta perusominaisuudet, jotka haluttiin ottaa käyttöön ensimmäisenä. Näitä olivat ohjelmistopäivitykset, sovellusten jakelun käyttöönotto sekä Endpoint Protection 2012:n integrointi Configuration Managerin yhteyteen. Rajausta oli etenkin jälkeinpäin katsottuna välttämätön toimenpide, koska ohjelmiston laajuudesta johtuen kaikkiin ominaisuuksiin ei olisi millään tämän työn puitteissa ehditty paneutumaan tarkasti. Valitut perustoiminnot saatiin otettua käyttöön, ja tavoitteena ollut keskitetyn hallinnan tehostaminen onnistui odotetulla tavalla. Huomasin ohjelmiston hyödyt myös itse käytännössä, koska olin työharjoittelun aikana päivittänyt uusien tietokoneiluokkien koneita yksitellen manuaalisesti.

Kun keskitetty hallinta saatiin käyttöön ja toimintakuntoon, ylläpitotoimiin käytettävä kokonaisaika väheni selkeästi. Toki esimerkiksi sovellusten käyttöönotossa ei riitä pelkkä Configuration Managerin käynnistäminen, vaan jokaiselle sovellukselle täytyy erikseen etsiä sopivin tapa, jolla niistä tehdään asennuspaketti. Tämä on osa-alue, joka vie eniten ylläpidon aikaa sen jälkeen, kun ConfigMgr on otettu käyttöön omassa ympäristössä. Siitä huolimatta käytettävää kokonaisaika saatiin vähennettyä erittäin paljon, kuten ennen työn aloittamista odotettiin. Myös yksittäisten koneiden seuranta ja valvonta saatiin Configuration Managerin myötä paremmin hallintaan. Kun tietoturvaohjelmisto Endpoint Protectioniakin voidaan hallita samasta konsolista kuin ohjelmiston toiminnot, antaa se ylläpitäjälle selkeämmän kokonaiskuvan hallittavien tietokoneiden tilasta.

Testausympäristön rakentaminen ja Configuration Managerin asentaminen siihen osoittautui työn haastavimmaksi osuudeksi. Kokonaiskuva alkoi hahmottua kunnolla vasta, kun ohjelmisto oli ensimmäisen kerran saatu asennettua, ja Kent Agerlundin kirja luetuuta ajatuksella läpi. Kirjassa on käsitelty ohjelmiston asennus tarkasti, mutta koska halusin tehdä asennuksen kohta kohdalta itse, enkä käyttää mitään valmiita asennuspaketteja, piti joissain kohdissa asioita vain itse kokeilla. Käyttöönotettu Configuration Manager 2012 SP1 erosi myös joiltain osin RTM-versiosta, jota käyttämäni lähdekirjallisuus yhtä työn loppuvaiheessa hankittua kirjaa (Agerlund 2013) lukuunottamatta käsiteli. Service Pack 1 -versio ohjelmasta julkaistiin alkuvuodesta 2013, joten siitä ei vielä

työtä aloitettaessa ollut saatavilla e-kirjoja, joita käytin pääasiallisina lähteinä. Erot RTM- ja Service Pack 1 -version välillä olivat kuitenkin loppujen lopuksi pieniä, eikä tästä aiheutunut ongelmia.

Testausympäristön asennusvaiheessa tuli myös hetkiä, jolloin työn eteneminen pysähtyi paikoilleen, eikä asennusohjeista ollut mahdollista löytää, että jotain olisi tehty väärin. Yksi tällainen tilanne oli, kun WSUS-palvelinta ei onnistuttu heti integroimaan Configuration Managerin kanssa. Tässä tapauksessa päästiin eteenpäin, kun löydettiin tilanteeseen liittyvä lokitiedosto. Siitä ilmeni, mitä lisäasennuksia palvelimelle tarvittiin, jotta WSUS-palvelimen integrointi saatiin onnistumaan. Tällaisista käytännössä ilmenivistä yksittäisistä ongelmista on se hyöty, että ne samalla opettavat myös yleisellä tasolla, miten Configuration Managerin käyttöön liittyviä ongelmia voidaan lähteä ratkaisemaan. Ohjelmistoon liittyy todella paljon erilaisia lokitiedostoja, joista voidaan tarkkailla toimintojen tilaa joko palvelimella, tai asiakastietokoneella. Usein ne kertovat myös selkokielisesti ongelmien syyn, kunhan vaan onnistuu löytämään oikean lokitiedoston josta etsiä.

Minulla ei ollut Configuration Managerista aiempaa kokemusta, joten ohjelmistoon tutustuminen lähdekirjallisuuden ja Internetistä löytyneen erilaisen materiaalin avulla veison osan käytetystä kokonaisajasta. Ennakkotiedot Active Directorysta ja Windows Server -käyttöjärjestelmästä olivat välttämättömiä ja erittäin tärkeässä osassa, koska iso osa testiympäristön rakentamisesta perustui omiin tietoihin ja taitoihin, jotka olen opintojen aikana hankkinut. Myös Configuration Managerin luonne Microsoftin olemassa oleviin tekniikoihin perustuvana ohjelmistona auttoi siihen, ettei kaikki työtä aloitettaessa ollut uutta ja outoa.

Huolimatta ennakkotiedoista, ja siitä, että ohjelmisto saatiin asennettua ja valitut ominaisuudet halutulla tavalla käyttöön, on myönnettävä, että ohjelmistossa on edelleen paljon ominaisuuksia joita en voi sanoa tuntevani perusteellisesti. Myös niiden toimintojen osalta, jotka otettiin käyttöön, riittää edelleen opittavaa ja kehitettävää. Kirjallisten lähteiden tutkimiseen olisi voinut käyttää työn aikana vieläkin enemmän aikaa, jotta luettu teoria olisi tukenut vahvemmin käytännön tekemistä. Jälkeenpäin ajatellen myös asennustyö olisi voitu suunnitella hieman perusteellisemmin ja hyödyntää enemmän ohjelmiston Active Directory -integraatiota esimerkiksi kokoelmien luomisessa. Näistä asioista huolimatta olen kuitenkin kokonaisuuteen tyytyväinen ja koen, että kehityin

paljon myös ammatillisesti tämän toimeksiannon ja opinnäytetyön tekemisen aikana. Järjestelmänhallinnan osalta minulla on nyt Microsoftin ratkaisuiden osalta hyvät perustiedot, joita on jatkossa hyvä lähteä kehittämään. Opinnäytetyöstä sain kirjoitettua lähestulkoon sellaisen mitä enakkoon ajattelin. Raportti on informatiivinen, ja sain omasta mielestäni nostettua perustietojen lisäksi esille myös sellaisia yksityiskohtia, joista voi olla hyötyä vastaavanlaisessa Configuration Managerin käyttöönottilanteessa oleville lukijoille.

Käyttöön otettujen perusominaisuuksien lisäksi Configuration Manager mahdollistaa IT-infrastruktuurin keskitetyn hallinnan tehostamisen Ahlmanilla myös jatkossa. Esimerkiksi asiakastietokoneiden käyttöjärjestelmäasennukset on mahdollista siirtää tulevaisuudessa tehtäväksi ConfigMgr:n avulla. Mobiililaitteiden kuten tablettien hyödyntäminen opetuskäytössä tulee myös tulevaisuudessa lisääntymään, ja niiden saaminen keskitetyn hallinnan piiriin on tärkeää etenkin, kun laitteiden lukumäärä kasvaa. Myös henkilökunnan työpuhelimet on mahdollista lisätä hallittavaksi ConfigMgr:n kautta, mikä tehostaisi erilaisten laitteiden keskitettyä hallintaa edelleen.

Hieman ennen tämän työn valmistumista, lokakuun puolivälissä 2013, Microsoft julkaisi ohjelmistosta uuden Configuration Manager 2012 R2 -version. Julkaisu sisältää paljon uusia ominaisuuksia, mm. tuen uusille Windows 8.1 - ja Windows Server 2012 R2 -käyttöjärjestelmille. Myös mobiililaitteiden hallintaan on tuotu uudessa julkaisussa jälleen paljon uutta. Ohjelmiston merkityksen voi nähdä tulevaisuudessa vain koko ajan kasvavan, kun yritykset ja yhteisöt haluavat saada yhä moninaisemman laitekantansa keskitetyn hallinnan piiriin.

LÄHTEET

Agerlund, K. 2012. System Center 2012 Configuration Manager: Mastering the Fundamentals. Kindle Edition.

Agerlund, K. 2013. System Center 2012 Configuration Manager SP1: Mastering the Fundamentals, 2nd Edition. Kindle Edition.

Ahlmanin koulun Säätiö. 2013. Internet-sivut. Luettu 20.9.2013.
<http://www.ahlman.fi/organisaatio>

Configuration Manager 2012. SP1. 2013. Microsoft.

Daalmans, P. 2012. ConfigMgrBlog.com. Blogiteksti. Luettu 3.9.2013.
<http://configmgrblog.com/2012/05/21/configuration-manager-2012-needs-windows-firewall-enabled/>

Documentation Library for System Center 2012 Configuration Manager. 2013. Microsoft. PDF-tiedosto. Julkaistu 1.2.2013. Tallennettu 10.9.2013.

Hampson, G. 2013. Gerry Hampson ConfigMgr. Blogiteksti. Luettu 12.9.2013.
<http://gerryhampsoncm.blogspot.fi/2013/02/welcome-to-my-sccm-2012-sp1-step-by.html>

How to uninstall System Center Essentials. 2013. Technet. Luettu 2.9.2013.
<http://technet.microsoft.com/en-us/library/ff730594.aspx>

McClure, S., Scambray, J., Kurtz, G. 2012. Hacking Exposed 7. Kindle Edition.

Meyler, K., Holt, B., Oh, M., Sandys, J., Ramsey, G. 2012. System Center 2012 Configuration Manager (SCCM) Unleashed. Kindle Edition.

Microsoft Tuotetuki. 2012. Luettu 9.10.2013.
<http://support.microsoft.com/kb/2688242>

Microsoft. System Center. 2012. Product Details. Luettu 6.9.2013.
<http://www.microsoft.com/en-us/server-cloud/system-center/default.aspx>

Pott, T. 2012. The Register. Windows System Center 2012: The review. Luettu 6.9.2013.
http://www.theregister.co.uk/2012/10/01/windows_system_center_2012_overview/

Rachui, S., Agerlund, K., Martinez, S., Daalmans, P. 2012. Mastering System Center 2012 Configuration Manager. E-kirja.

System Center 2012 Product Details. 2013. Microsoft. Luettu 6.9.2013.
<http://www.microsoft.com/en-us/server-cloud/system-center/default.aspx>

System Center Updates Publisher 2011. 2011. Microsoft.

Tietoturva nyt! 2012. Viestintävirasto. Luettu 15.10.2013.
<http://www.cert.fi/tietoturvanyt/2012/08/ttn201208281337.html>

What is Java and why do I need it? 2013. Java.com. Luettu 15.10.2013.
http://www.java.com/en/download/faq/whatis_java.xml

Windows Server 2008. R2. 2009. Microsoft.