Palvelinten tietoturvapäivitysten automatisointi

Case Pohjantähti Keskinäinen Vakuutusyhtiö

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Visamäki, syksy 2013

Tomi Kraft

Tomi Kraft

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Visamäki
Tietojenkäsittelyn koulutusohjelma
Systeemityö

TIIVISTELMÄ

Tekijä Tomi Kraft **Vuosi** 2013

Työn nimi Palvelinten tietoturvapäivitysten automatisointi
Case Pohjantähti Keskinäinen Vakuutusyhtiö

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli luoda päivitysten automatisointiratkaisu, jolla aikaansaadaan parannuksia palvelimien tietoturvatason ylläpitoon. Lisäksi tavoitteena oli tarjota kattavaa tietoa palvelimien tilasta sekä toimintakunnosta. Aiheen työlle tarjosi Pohjantähti Keskinäinen Vakuutusyhtiö.

Työssä tutustuttiin teoriatasolla tietoturvaan, automatisointiin sekä päivittämisratkaisuihin osana automatisointiprosessia. Lisäksi tutkittiin päivittämisratkaisun mahdollistavia hallintaohjelmistoja sekä tekniikoita. Työssä käytiin käytännössä läpi, kuinka palvelinten tietoturvapäivitysten automatisointi Pohjantähdessä tapahtui osana tätä opinnäytetyötä ja kuinka seurantaratkaisu luotiin.

Lähteinä opinnäytetyössä käytettiin laajalti alan viimeisintä tietämystä, jota löytyi runsaasti Internetistä sekä kirjoista. Päivittäminen on suosittu aihe, sillä sitä tapahtuu kaikkialla maailmassa jatkuvasti, eikä sen tarvetta enää nykyisin väheksytä. Lähteiden monipuolisuus tarjosi kattavaa tietoa aiheesta.

Työn lopputuloksena oli ratkaisu, jossa luokiteltiin ja automatisoitiin Pohjantähden Windows-palvelimia päivitysten osalta. Suurin osa palvelimista määritettiin luodun automatisoinnin piiriin. Työstä saadun tiedon ja parhaiden käytänteiden pohjalta päätettiin kuitenkin olla automatisoimatta kriittisimpiä palvelimia. Lisäksi luotiin ratkaisu, joka tarjoaa kattavaa ajantasaista tietoa palvelimien tilasta vastuuhenkilöille sähköpostitse sekä tekstiviestillä.

Työn ansiosta Pohjantähden tietoturvataso sekä palvelimien seuranta ja hallinta kokivat parannuksia. Palvelimet ja niiden päivitykset saivat osakseen tarvitsemansa huomion ja päivittämisille määritettiin tarkat aikaikkunat. Jatkokehitys ja muutoksien tekeminen luotuun ratkaisuun tehtiin mahdollisimman helpoksi.

Avainsanat tietoturva, päivitys, palvelimet, automaatio

Sivut 46 s. + liitteet 2 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Visamäki
Degree Programme in Business Information Technology
System Engineering

Author Tomi Kraft **Year** 2013

Subject of Bachelor's thesis Automating server security updates
Case Pohjantähti Mutual Insurance Company

ABSTRACT

The purpose of the thesis was to generate an automation solution which will bring out improvements in the information security of servers. Furthermore, the goal was to provide comprehensive information about status of servers. The thesis was commissioned by Pohjantähti Mutual Insurance Company.

Theoretical parts of the thesis explored information security, automation and updating as part of the automation process. Also, management software and technologies enabling the updating process were explored. In practice, the thesis covered the entire process of automating the servers at Pohjantähti and how the server tracking solution was made.

The latest knowledge of IT field was used as a main source of the thesis. Plenty of information was found in Internet and books. Updating is a common subject in everyday life of IT professionals and it is not underrated nowadays as it used to be. Versatile sources secured that the information used in the thesis was valid.

Automated updating and classification of the Windows servers at Pohjantähti were the final result of the thesis. Most of the servers were defined to be a part of the automation process. However, the most critical ranked servers were not automated because the information and best practices learned during the thesis proved so. In addition, a solution offering information about servers to the person in charge was made using e-mail and SMS technologies.

Thanks to the thesis, information security, server security and server management improved at Pohjantähti. Status and updates of the servers received the attention they needed. Maintenance time was determined. Further development was made as easy as possible.

Keywords information security, update, servers, automation

Pages 46 p. + appendices 2 p.

KÄSITELUETTELO

Active Directory (AD)
Microsoftin tarjoama hakemistopalvelu, jonka avulla tunnistetaan ja hallitaan käyttäjiä sekä tietokoneita.

Group Policy (GP)
Ryhmäkäytäntö on yksi keino, jolla Active Directoryssa olevia käyttäjiä ja koneita hallitaan. Sen avulla keskitetään halutut hallintakomennot ja säännöt luoduille ryhmille.

Group Policy Management Console (GPMC)
Ryhmäkäytäntöjen hallintaa ja luomista varten suunniteltu ilmainen työkalu.

Komentotulkki
Ohjelma, jonka avulla ohjataan käyttöjärjestelmää kirjoittamalla komentoja komentoriville. Windowsissa tunnetaan nimellä cmd.exe.

Microsoft
Maailman suurin ohjelmistoyritys, joka valmistaa tuotteita toimisto-ohjelmista käyttöjärjestelmiin. Yritys on tunnettu erityisesti valmistamistaan Windows-käyttöjärjestelmistä.

Organizational Unit (OU)
Suomeksi organisaatioyksikkö. Active Directoryn sisällä oleva yksikkö, jota käytetään tiedon säilömiseen. Yleensä OU sisältää käyttäjiä tai tietokoneita.

Palvelin
Palvelimella tarkoitetaan tietokoneessa suoritettavaa palvelinohjelmistoa tai palvelinohjelmistoa suorittavaa tietokonetta.

Patch Tuesday
Kuukauden toinen tiistai, päivä jolloin Microsoft julkaisee viimeisimmät päivitykset tuotteisiinsa Windows Update palvelun kautta.

SCCM 2012
Microsoft System Center Configuration Manager 2012. Microsoftin tarjoama tuote, jolla voidaan keskitetysti hallita suuria työasema- ja palvelinympäristöjä. Mahdollistaa myös päivitysten ja asennuspakettien jakelun.

Script/Skripti
Komentosarja, joka ajetaan useimmiten komentotulkissa. Tavallista tekstiä, joka sisältää tietokoneen ymmärtämiä komentoja. Kirjoitetaan usein pelkästään tekstitiedostoon. Käytetään automatisoinnissa.

Service Pack (SP)
Service Pack on Microsoftin Windows-tuotteisiin tarjoama huoltopäivitys, johon on koottu korjaukset ohjelmassa esiintyneisiin virheisiin. Yleensä Service Pack ilmestyy muutaman vuoden kuluttua ohjelman alkuperäisestä julkaisusta.

Sysinternals
Joukko ilmaisia työkaluja, joilla voidaan hallita Windows-ympäristöjä. Mahdollistavat komentojen ja tehtävien suorittamisen etänä, ilman varsinaisia asennuksia. Ajetaan useimmiten komentotulkissa.

Virtuaalikone
Yhdellä fyysisellä tietokoneella toimiva virtuaalinen kone. Virtuaalikoneet käyttävät isäntäkoneensa resursseja mahdollistaen sen, että yhden tietokoneen sisällä toimii useampi virtuaalinen tietokone.

Windows Server 2003 & Windows Server 2008
Palvelimille tarkoitettu, erittäin suosittu Microsoftin valmistama käyttöjärjestelmä, joka tarjoaa kattavia ominaisuuksia palvelimille.

VMware
Virtualisointiohjelmistoja tuottava yhdysvaltalainen yritys. Yrityksen tunnetuimpia ohjelmistoja ovat virtualisointimahdollisuuksia tarjoavat alustat.

WSUS
Windows Server Update Services. Ilmainen ohjelma, jonka avulla päivitysten keskitetty hallinta ja jakaminen onnistuvat Windows-laitteille. Ohjelma on suosittu työväline päivitysten hallitsemiseksi.

SISÄLLYS

Liite 1 SYSTEMINFO
Liite 2 PSINFO
Liite 3 LOGI.TXT

1 JOHDANTO

Tietoturvan merkitys on kasvanut viime vuosina, sillä riskejä on paljon ja uusia ilmaantuu tasaiseen tahtiin. Tietoturvassa olevat aukot ovat vaaraksi niin yksityisille käyttäjille kuin erityisesti yrityksille. Yritysten verkossa liikkuu usein tietoa, joka on yrityksen toiminnan kannalta ensiarvoisen tärkeää. Tietoturvatason ylläpitämiseksi useat valmistajat julkaisevat uusia päivityksiä, joilla turvallisuustasossa olevia aukkoja pyritään paikkaamaan. Päivitysten julkaisutahti on tiuha, joten palvelimien toimintakunnon ja tietoturvan ajantasaisena pitäminen vaatii jatkuvaa huomiota ja resursseja.

Työn toimeksiantajana toimi Pohjantähti Keskinäinen Vakuutusyhtiö, josta myöhemmin käytetään nimitystä Pohjantähti. Pohjantähti on keskinäinen vakuutusyhtiö, joka on perustettu vuonna 1895. Yrityksellä on toimintaa ympäri Suomen noin 40 toimipisteessä. Työntekijöitä Pohjantähdessä on tällä hetkellä 332, joista hieman yli puolet työskentelee pääkonttorilla Hämeenlinnassa ja loput palvelukonttoreilla ympäri Suomen. Pohjantähti on keskinäinen yhtiö, joka tarkoittaa sitä, että vakuutuksenottajat ovat yhtiön omistajia.

Tässä opinnäytetyössä selvitettiin, mikä on kohdeyrityksen näkökulmasta tarkasteltuna paras ja tehokkain tapa toteuttaa yrityksen Windows-palvelinympäristön paras mahdollinen tietoturvatason ylläpito. Työn tavoitteena oli toteuttaa ratkaisu, jolla palvelimien tietoturvapäivitysten lataaminen ja asentaminen automatisoidaan mahdollisimman pitkälle, säilyttäen kuitenkin tietoturvan ja tuotannon kannalta parhaan tasapainon. Päivitysten onnistumisesta ja palvelinten toimintakunnosta oli edellisten ohella tarkoitus tuottaa tietoa.

Päivitysten automatisoinnilla pyritään takaamaan tietoturvan korkea taso, palvelinten toimintakyky ja häiriöttömän tuotantokäytön varmistaminen. Määriteltyjen palvelinten uudelleenkäynnistäminen ajoitetaan ennalta määrättyyn ajankohtaan ja käynnistymisaikojen seuraamiseen saadaan työkalu. Työtehokkuus lisääntyy, kun päivityksiä ei tarvitse erikseen ajaa jokaiselle palvelimelle käsin.

Työn kirjoittamishetkellä Pohjantähdellä oli käytössään 60 Windows-palvelinta, joista noin puolet oli toteutettu virtuaalisesti VMware-ohjelmistoa hyödyntäen. Fyysiset palvelimet sijaitsivat pääosin konesalissa yhtiön pääkonttorilla Hämeenlinnassa. Osa palvelimista sijaitsi lisäksi yhtiön aluekonttoreilla. Työssä ei käsitelty yhtiöllä käytössä olevia IBM iSeries -palvelimia eikä Linux-käyttöjärjestelmää hyödyntäviä palvelimia.

Työssä keskityttiin tutkimuskysymyksiin, joissa käsiteltiin sitä, onnistuvatko päivitys, jakelu ja asennus saman työkalun avulla. Lisäksi tutkittiin miten varmistetaan, etteivät päivitykset aiheuta ongelmia palvelimille. Työssä saadaan myös vastaus siihen, miten palvelinten päivitysprosessi Pohjantähdessä tapahtui.

2 TIETOTURVA

Tämän kappaleen tavoitteena on käsitellä tietoturvaa ja päivittämistä alustavasti. Lisäksi on tarkoitus perehtyä päivittämisen merkitykseen tietoturvatason ylläpitämisen kannalta. Päivittämisen osalta keskitytään käyttöjärjestelmän valmistajan tarjoamiin päivityksiin. Tietoturvallisuus on kiinteä ja keskeinen osa yritysten liiketoimintaa, ja liiketoiminta on nykyisin hyvin paljon sidoksissa tietojärjestelmiin. Se aiheuttaa alalla tarpeen, minkä johdosta tietoturvan merkitystä ei pidä missään nimessä aliarvioida.

Perinteisesti tietoturvalla tarkoitetaan tiedon perusominaisuuksien, kuten eheyden, luottamuksellisuuden ja käytettävyyden turvaamista. (Laaksonen, Nevasalo & Tomula 2006, 17). Käytettävyyden turvaaminen tarkoittaa käytännössä sitä, että tietoa on saatavilla silloin kun sitä tarvitaan. Tiedon luottamuksellisuuden turvaamisen tarkoituksena on, että tieto on saatavilla vain heille, joilla siihen on oikeudet. Kun tiedon luottamuksellisuus on kunnossa, ei ulkopuolisilla ole pääsyä tietoihin. Tiedon eheydellä tavoitellaan pistettä, jossa tieto pysyy muuttumattomana ja luotettavana. Tieto ei muutu, vaan säilyy myös mahdollisten vikatilanteiden sattuessa.

Tietoturvan ylläpitäminen on nykyaikana yhä merkityksellisempää. Varsinkin ulkoiset uhkat ovat lisääntyneet. On tärkeää, että yrityksissä on aitoa kiinnostusta tietoturvatason ylläpitämiseksi. Tietoturvallisuutta voidaan pitää pieninä tekoina osana jokapäiväistä toimintaa. Hyvä tietoturvallisuus on osa organisaatiokulttuuria, jossa kaikki ymmärtävät tietoturvan merkityksen ja työskentelevät yhteisten hyvien tavoitteiden eteen. (Laaksonen ym. 2006, 17.)

Useat yritykset ja yksityishenkilöt ovat vasta viime vuosina havahtuneet heikon tietoturvatason vaikutuksiin. Pohjantähdessä tietoturva on otettu huomioon laatimalla koko yhtiön kattava tietoturvaohjeistus, jossa informoidaan työntekijöitä tietoturvallisuuden merkityksestä ja vaikutuksesta heidän ympäristössään. (Pohjantähti tietoturvaperiaatteet 2011.)

2.1 Tietoturvan perusperiaatteet

Tietoturva jaetaan perinteisesti kahdeksaan eri osa-alueeseen (Laakso 2010, 9). Osa-alueista ensimmäinen ja tietoturvan toimivuuden kannalta hyvin oleellinen on tieto ja varmuus siitä, että yrityksen hallinnolliset ja organisatoriset keinot ovat kunnossa. Tällä osa-alueella tarkoitetaan käytännössä sitä, että on olemassa tietty organisaatio tai vähintään yksi henkilö, joka vastaa tietoturvasta ja sen käytännöistä sekä käytännön toimeenpanosta. Osa-alueen piiriin kuuluu myös se, että tarvittavat tietoturvaohjeistukset on laadittu ja niitä pyritään noudattamaan. (Rosendahl n.d.)

Toinen tietoturvan perusrakenteiden ylläpidon kannalta oleellinen tietoturvan osa-alue on fyysinen tietoturva. Tietoturvasta puhuttaessa fyysinen tietoturva jää usein taustalle. Fyysisen tietoturvan suuresta merkityksestä huolimatta se miellettäneen usein vähäpätöiseksi tai ainakin vähemmän tunnetuksi osa-alueeksi.

Tämä voidaan selittää sillä, että fyysinen tietoturva ei liity yksinomaan tietoon, kuten tietoturvan yleisesti mielletään liittyvän (Koskinen 2002). Fyysisellä tietoturvalla tarkoitetaan sitä, miten tieto on suojattu fyysisesti. Yleisiä fyysisiä suojaustoimenpiteitä ovat erilliset konesalit, kulunvalvontaratkaisut ja lukot. Näiden avulla saadaan helposti estettyä asiattomien henkilöiden pääsy heille kuulumattoman fyysisen tiedonlähteen ääreen. (Laakso 2010, 18.)

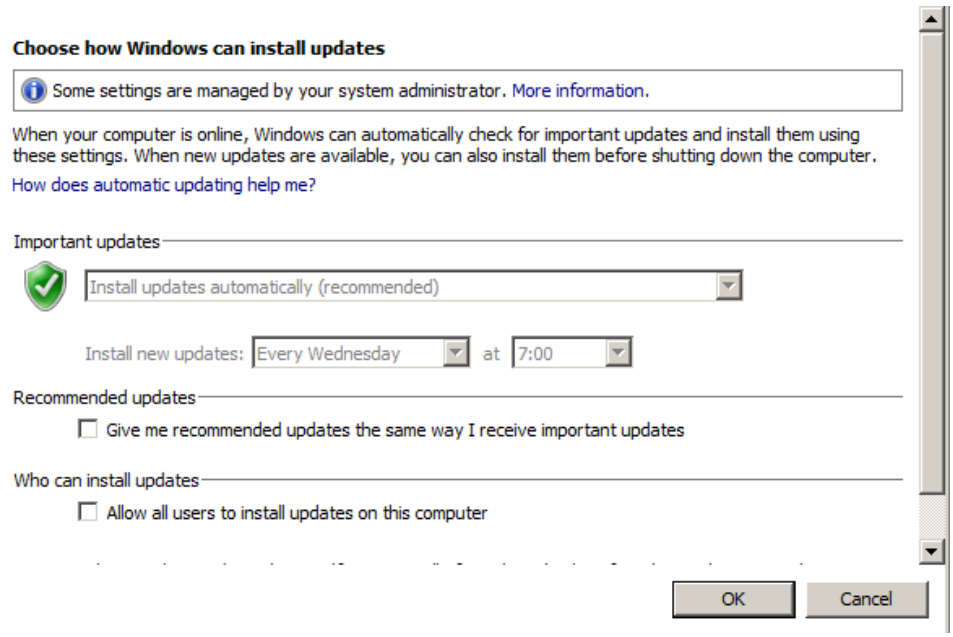
Kolmas tietoturvan perusrakenteiden osa-alue on henkilöstöturvallisuus. Laaksonen ym. (2006, 138) kertovat, että henkilöstöturvallisuudella tarkoitetaan henkilöstön toimista aiheutuvia ja heihin kohdistuvia tietoturvauhkia ja niiden hallintaa. Tärkeät tiedot tulee suojata henkilöstön aiheuttamilta väärinkäytöksiltä ja tahattomilta virheiltä, jotta toiminnalle ei aiheudu keskeytystä tai haittaa. Henkilöstöturvallisuudella tarkoitetaan myös niitä toimia, joita tehdään suoritettaessa uuden työntekijän rekrytointia. Useimmiten tällaisia toimia ovat erilaiset taustatarkastukset.

Nämä kolme tietoturvan osa-aluetta muodostavat yhdessä tietoturvan perustason, jonka tulisi olla kunnossa jokaisessa yrityksessä. Kun perustaso on saavutettu, on mahdollista kehittää tietoturvaa yhä kattavampaan suuntaan. Perusasioiden ollessa kunnossa voidaan keskittyä seuraaviin tietoturvan vaiheisiin, kuten käyttöturvallisuuteen, laitteistoturvallisuuteen ja tietoliikenneturvallisuuteen. Niiden avulla pyritään varmistamaan tieto siitä, että laitteet on inventoitu ja niiden sijainti tiedetään, käyttäjäoikeudet ovat asianmukaiset ja tietoliikenne ja päätelaitteet on suojattu tarvittavin toimenpitein, kuten palomuurein ja virustorjuntaohjelmistoin. (Rosendahl n.d.)

Tämän opinnäytetyön kannalta mielenkiintoisimmat tietoturvan osa-alueet ovat ohjelmistoturvallisuus ja laitteistoturvallisuus. Palvelinten osalta laitteistoturvallisuus on yleisesti otettu huomioon varmistamalla kriittisten palvelimien virran saanti myös sähkökatkosten aikaan, hoitamalla asianmukaiset varmistukset ja varmuuskopioinnit sekä kovalevyjen kahdennukset. (Laakso 2010, 22.) Ohjelmistoturvallisuuden osalta palvelimilla keskeistä on ohjelmistojen ajantasaisuus ja tietoturvaukkojen paikkaaminen. Tietoturvaukkojen paikkaaminen tapahtuu lähes poikkeuksetta laite- ja ohjelmistovalmistajan tarjoamilla päivityksillä. Näiden päivitysten automatisointiratkaisun kehittämistä ja toteuttamista tullaan tässä opinnäytetyössä tarkastelemaan lähemmin myöhemmässä vaiheessa.

2.2 Windows Update

Tärkeä palanen tietoturvallisuuden osalta on laitteiston ajantasaisuus ja toimintakyky uusimpia uhkia vastaan. Windows Update on palvelu, joka on suunniteltu varta vasten vastaamaan tähän haasteeseen. Windows-käyttöjärjestelmät ovat hyvin suosittuja työasemien lisäksi myös palvelimissa. (Kuva 1.) Windows Update on Microsoftin kehittämä apuväline, jolla yritys hoitaa päivitysten jakamisen käyttäjille. Windows Updaten avulla toimitetaan päivityksiä kaikkiin Microsoftin tuen piirissä oleviin tuotteisiin. Tietoturvapäivitysten lisäksi jakeluun kuuluu valinnaisia ja suositeltuja päivityksiä. (Windows Update Explained 2010.)



Kuva 1. Windows Update näkymä Windows Server 2008 R2 -palvelimella

Windows Update tarjoaa kolmen eri tason päivityksiä. Päivitystasoja ovat valinnaiset päivitykset, suositellut päivitykset ja tärkeät päivitykset. Valinnaiset päivitykset ovat usein vähemmän merkityksellisiä. Ne sisältävät lisäosia tai uusien ohjelmien testiversioita. Varsin usein valinnaisia päivityksiä ovat kolmannen osapuolen tuotteiden ajurit (Brinkmann 2010). Johtuen päivitysten luonteesta, ei niitä kannata asentaa automaattisesti palvelimille, sillä varsinaista hyötyä ne eivät tarjoa.

Brinkmann (2010) kertoo, että suositellut päivitykset sisältävät usein päivityksiä toiminnallisuuteen tai kokonaan uusia ominaisuuksia. Tällaisia ovat toiminnallisuuspäivitykset, ohjetiedostojen päivitykset, uudet ominaisuudet käyttöjärjestelmässä sekä uudet ominaisuudet muissa tuotteissa. Suositeltujen päivitysten kanssa on sama käytäntö kuin valinnaistenkin kanssa. Näiden automaattisen lataukseen ja asennukseen ei ole mitään merkittävää tarvetta, sillä ne eivät tarjoa toiminnan kannalta olennaisia päivityksiä. Sen sijaan mukavat lisät, jota suositeltuina päivityksinä tarjotaan, voivat usein sotkea palvelimen harmonian ja toimintakunnon.

Tärkeät päivitykset ovat nimensä mukaisesti tärkeitä. Ne suojaavat tietokonetta haittaohjelmilta ja lisäävät tietokoneen luotettavuutta. Päivitykset ovat tyypiltään tietoturvapäivityksiä, suojauspäivityksiä sekä haittaohjelmien havaitsemiseksi ja poistamiseksi tarkoitettuja työkaluja. Tärkeät päivitykset tulisi asentaa koneisiin mahdollisimman pian. (Brinkmann 2010.)

Tuotteen toimivuuden ja turvallisuuden kannalta on tärkeää, että viimeisimmät tärkeät päivitykset ja korjaukset ovat asennettuina. Vanhentuneet versiot aiheuttavat yrityksen toiminnalle turhan tietoturvariskin. Kohonneesta riskitasosta huolimatta yhä valitettavan usein monien yritysten tärkeidenkin tietokoneiden osalta ovat päivitykset myöhässä tai puutteellisia. (F-Secure 2013.)

2.3 Kuukausittaiset päivityspaketit

Microsoft julkaisee tuotteilleen tietoturvapäivityksiä kuukausittain. Päivitysten julkaisu on määritetty joka kuukauden toiseen tiistaihin (Neumann 2006). Kuukausittaiset päivityspaketit tunnetaankin paremmin nimellä Patch Tuesday, josta käy ilmi päivitysten julkaisu aina tiistaisin. Tapana on julkaista suurempi määrä päivityksiä parillisina kuukausina, ja pienempiä määriä parittomina kuukausina (Keizer 2011).

Kuukausittaisten päivityspakettien jakelu sai alkunsa vuonna 2003 Microsoftin suunnitellessa uutta tietoturvallisuussuunnitelmaa pääasiassa silloisten lippulaivojensa, Windows XP:n ja Windows Server 2003:n tueksi. Yhtiön ylimmän johtoportaan mukaan Microsoft kaksinkertaisti panostuksensa käyttäjien tietoturvallisuuden parantamiseksi. Syitä panostuksen lisäämiseen oli monia. Tietoturvauhkat olivat kasvaneet ja Microsoftia syytettiin siitä, että sen tuotteet ovat liian herkkiä ulkoisille uhille. Viikoittaisia päivityksiä pidettiin liian tiuhana tahtina, joten uudeksi strategiaksi päädyttiin valitsemaan kuukausittaiset päivityspaketit. (Lemos 2003.)

Kuukausittaiset päivityspaketit ovat kohdanneet olemassaolonsa aikana laajalti kritiikkiä. Kritiikki on ymmärrettävästi aiheellista, sillä tarkasti tiedossa olevat tietoturva-aukkojen korjausajankohdat ovat haittaohjelmien tekijöiden kannalta edullisia. Ei ole lainkaan poikkeavaa, että haittaohjelmien julkaisu on keskitetty tarkoituksellisesti juuri päivityksistä seuraavaan keskiviikkoon (Leffal 2007). Näin ollen haittaohjelmille on pyritty takaamaan kuukausi aikaa vaikuttaa, ennen kuin Microsoft on julkaissut uudet päivitykset, joilla asia on korjattu. Toisena tapana on pidetty haittaohjelmien julkaisua muutamia päiviä ennen virallisten pakettien julkaisua, sillä Microsoft ei ole ehtinyt laatimaan korjaavia päivityksiä saataville riittävän ajan kuluessa.

Yhtä ja ainoaa ratkaisua yllä mainittuun ongelmaan ei ole. Microsoft on kuitenkin päättänyt julkaista tarvittaessa myös toisen päivityspaketin kuukauden aikana, jos tarvetta tälle ilmenee. Lisäksi kriittisimpiä päivityksiä julkaistaan tarvittaessa ilman määriteltyä aikataulua, jopa päivittäin (Brinkmann 2010).

Tämänkaltaisten kuukausittaisten tietoturvapäivitysten hyötynä voidaan pitää tietoa ja varmuutta siitä, että uudet päivitykset julkaistaan tiettynä ajankohtana kuukaudesta. Näin ollen erityisesti yritykset, mutta myös yksityishenkilöt, voivat suunnitella laitteidensa päivitykset jo hyvin etukäteen. Useampien laitteiden kanssa toimittaessa on suuri hyöty siitä, että tiedossa on milloin ja mitä päivityksiä julkaistaan. Automaattiset päivitykset ja uudelleenkäynnistykset on mahdollista ajastaa päivitysten ilmaantumisesta seuraavaan toiminnan kannalta parhaaseen ajankohtaan. Tämä helpottaa ylläpitohenkilöstön työtä ja halutun tietoturvatason ylläpitoa päivitysten hallinnan avulla.

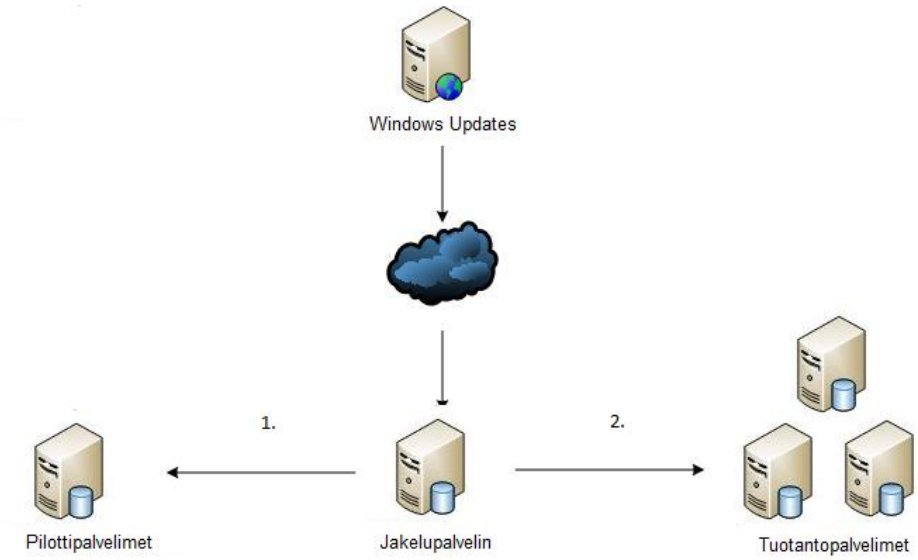
2.4 Päivitysten jakelu

Päivitysten jakelu on päivitysketjun ja tietoturvan toimivuuden kannalta keskeinen osa. Päivitysten jakelulla tarkoitetaan toimenpiteitä, joiden avulla päivitykset saadaan alkuperäisestä lähteestään toimitettua halutuille tietokoneille. Useimmiten tällaisia lähteitä ovat ohjelmistovalmistajien sivut, kuten Microsoftin Windows Update. Päivitysten jakaminen voidaan jättää myös täysin päivityksiä tarjoavan tahon vastuulle. Tällöin tietokoneen päivitysasetuksista on määritetty, että tietokone lataa ja asentaa uusimmat päivitykset automaattisesti. Vaihtoehtoisesti päivityksien lataaminen, jakelu ja asentaminen voidaan keskittää ja suorittaa hallitusti, mutta silti automaatiota hyödyntäen.

Palvelimien päivitysten jakamiseen liittyen on olemassa ammattilaisten suosimia käytäntöjä. Tällaisia ovat esimeriksi keskitetyt jakelukäytännöt. On käytännöllisempää, että jakelu hoidetaan keskitetysti, mikäli palvelimia on useampia. Tämän avulla vältetään se, että kaikki palvelimet olisivat yhteydessä Microsoftin palvelimiin kysellen päivityksiä ja näin mahdollisesti hidastaen yrityksen verkkoa ja altistavan sen ulkoisille tietoturvauhille. (Kuva 2.) Vaihtoehtoisesti jakelu on mahdollista hoitaa yhden palvelimen avulla, jos siihen on kyseistä käyttöä varten asennettu vaadittava hallintaohjelmisto. Toinen tärkeä seikka jakelussa on se, että päivityksiä ei suin päin jaeta kaikille palvelimille. Tämä tarkoittaa käytännössä sitä, että päivitykset jaetaan tarvittaville testi- ja pilottiryhmille, jotta saadaan tietoa siitä, että päivitykset varmasti toimivat kyseisten ohjelmistojen kanssa. (Budd 2006.)

Useimmiten normaalille kotioloissaan Windowsia käyttävälle henkilölle päivitysten jakelusta huolehtiminen ei aiheuta päänvaivaa tai toimenpiteitä ja jakelu hoituukin usein automaattisesti taustalla käyttäjän tätä välttämättä edes huomaamatta. Tämä käytäntö on Windows Updaten mukaan myös suositus ja mainio keino ylläpitää esimerkiksi kotikoneen päivityksiä ajantasalla. Siirryttäessä yhdestä koneesta isompiin ympäristöihin, kuten yrityksiin, joissa on kymmeniä, satoja tai tuhansia koneita, kasvaa jakelun merkitys yhä suuremmaksi. Tällöin on syytä miettiä, mitkä kaikki päivitykset jaellaan automaattisesti ja mitkä manuaalisesti. Kaikkia päivityksiä ei myöskään välttämättä ole kannattavaa ladata, sillä ne eivät ole toiminnan kannalta oleellisia. Sen sijaan ne voivat olla jopa olla haitallisia. (Rosato n.d.)

Päivitysten jakelun hallitseminen, keskittäminen ja automatisointi ovat usein hallintaohjelmien tarjoamien palveluiden piirissä. Nämä hallintaohjelmat ovat työkaluja, jotka on tehty helpottamaan suurien laiteympäristöjen hallintaa. Tämänkaltaisia työkaluja käsitellään opinnäytetyön kappaleessa viisi.



Kuva 2. Yleinen käytössä oleva päivitysten jakeluratkaisu

3 AUTOMATISOINTI

Tässä kappaleessa käsitellään automatisointia ja sen tarjoamia mahdollisia hyötyjä ja riskejä yrityksen toiminnan kannalta. Automatisoinnin historia tekniikan alalla kantautuu pitkälle, mutta varsinkin viimeisinä vuosikymmeninä tietotekniikan yleistyessä sitä on pyritty soveltamaan myös it-alalla. Automatisoinnin perimmäisenä tarkoituksena on pyrkiä tehostamaan palveluita vähentämällä ihmisten manuaalisesti suorittamia, usein pitkiä, rutiininomaisia tehtäviä. Jotkin ohjelmat ja laitteistot ovat niin monimutkaisia, että automatisointi on niiden kannalta jopa välttämätöntä. Toiminnan tehostamisen taustalla on usein taloudelliset seikat. Automatisoinnin saamasta huomiosta huolimatta on täysautomatisointi vielä verrattain harvinaista. Yleensä automaatioprosessit tarvitsevat edelleen myös ihmisen vuorovaikutusta.

3.1 Hyödyt

Automatisoimatonta prosessia pidetään usein hitaana. Hitaus syö aikaa muulta toiminnalta, kuten kehittämistyöltä ja liiketoiminnan haasteisiin valmistautumiselta. Ilmeisimpänä automatisoinnin hyötynä pidetäänkin sen tuomaa säästöä ajallisesti ja työllisesti. Sutisen (2013) mukaan vain käsitöitä vähentämällä saadaan toimintaan virtaviivaisuutta, nopeutta ja joustavuutta, joka näkyy integroitavuutena organisaation läpi. Perinteistä käsityötä pidetään yleisesti laadukkaana. Näin ei kuitenkaan aina välttämättä ole, sillä rutiineihin kangistuneet työntekijät häviävät usein automatisoiduille prosesseille. Esimerkiksi työaseman asennuksen automatisoinnin

avulla voidaan olla varmoja, että työasemaan tulee juuri ne ohjelmat, jotka asennusketjussa sille on määritelty. Satoja koneita asentava ihminen saattaa inhimillisistä syistä johtuen helposti unohtaa jonkin painalluksen tai ohjelman.

Automatisointi tarjoaakin it-osastoille oivan mahdollisuuden karsia sekä kuluja että vähentää manuaalisissa prosesseissa tapahtuneita virheitä. Sen avulla voidaan nopeuttaa arkisia rutiinitöitä sekä parantaa niin ylläpito- kuin palveluprosessiakin. Suosittuja automatisoinnin kohteita perinteisen tietohallinnon toiminnassa on useita. Näitä ovat sellaiset perustoiminnot, kuten salasanojen resetointi, käyttäjien oikeuksien määrittely ja ohjelmistojen asennus. Edellä mainitut työt aiheuttavat laajalti työtä erityisesti järjestelmistä vastaavalle henkilöstölle. Automatisoinnilla työtä voidaan tehostaa, ja toiminnan tältä osin on automatisoinnista realistista hyötyä. Automatisointi ei myöskään ole tietoturvatonta. Automatisoinnilla ei pyritä vähentämään prosesseihin liittyviä kontrolleja ja mahdollista oikeuksien määrittämistä. Automatisoinnin perimmäinen pyrkimys tässä suhteessa on ainoastaan vähentää työhön liittyvää rutiinia, johon tuhlaantuu arvokasta työaikaa. (Vuokko 2012.)

Suurta osaa automatisoinnin puoltamisessa esittää raha. Onnistuneet automaatioprosessit järjestelmähallinnassa auttavat positiivisella tavalla useimpia organisaatioita. Usein pelkällä ympäristön uudelleen järjestelyllä löydetään käyttämättömiä ohjelmia tai laitteita, joista luopuminen on järkevää. Täyden hyödyn irti saamiseksi automatisoitavia prosesseja tulee miettiä tarkkaan. Nyrkkisääntönä pidetään, että sellaiset prosessit, joita suoritetaan usein ja aina lähestulkoon saman kaavan mukaan, ovat oivia kohteita automatisoinnin kannalta. Hyvinä automatisointikohteina pidetään myös keskivolyymisia prosesseja, joiden automatisointi on helppoa ja niiden avulla saadaan nopeita voittoja. Myös osittainen automatisointi on joissain tapauksissa toiminnan ja tehokkuuden kannalta paras vaihtoehto. (Vuokko 2012; Vehviläinen 2013.)

Päivityksien jakelu ja asennus ovat oiva kohde automatisoinnille. Kun prosessi on mietitty tarkkaan ja tiedetään, mille kohteille päivittäminen kannattaa automatisoida ja kuinka pitkälle automatisointi kannattaa viedä, saadaan aikaan merkittäviä säästöjä varsinkin ajallisesti. Automatisoinnissa on kuitenkin otettava huomioon, että kaikki sujuu, kuten pitääkin ja lopputuloksesta on oikeasti hyötyä. Päivityksiä, kuten muitakin tuotantoon vaikuttavia asioita automatisoitaessa on syytä muistaa erityisesti yksi asia. Hyötyjen tulee aina olla suurempia kuin riskien.

3.2 Riskit

Automaatioon investoimiseen suhtautuminen vaihtelee. Osa alan vaikuttajista suhtautuu siihen kriittisesti, sillä ajatellaan oman it-ympäristön olevan niin pieni, että automatisoinnista saatava hyöty ei vastaa mahdolliseen hallintaohjelmaan tehtyä investointia. (Vehviläinen 2013.) On totta, että muutamien kymmenien koneiden ympäristössä ei ole järkevää sijoittaa suuria summia automatisointia tukevan hallintaohjelmiston ostamiseen. Syytä on

kuitenkin muistaa, että käyttöjärjestelmätkin sisältävät laajalti ominaisuuksia automatisoinnin ja hallinnan helpottamiseksi. Satojen koneiden ympäristöissä automatisoinnilla on jo merkittäviä vaikutuksia, mutta valinnat tulee aina suorittaa organisaatiokohtaisesti ottaen huomioon hyötyjen ja riskien suhteen.

Automaation kannalta ongelmallista on liiallisen luottamussuhteen syntyminen automatisoituun prosessiin. Useimmiten automatisoidut prosessit ovat luotettavia ja toimivat kuten pitääkin, mutta on mahdollista, että jokin menee pieleen. Johtuen skenaarion harvinaisuudesta ja syntyneestä luottamussuhteesta prosessia kohtaan, on todennäköistä, että asiaan ei välittömästi puututa. Jokin pieni muutos automatisoituun asennusketjuun saattaa sekoittaa valmiin asennuksen täydellisesti. Vuosia automatisoidun prosessin avulla työskennelleet henkilöt eivät välttämättä tiedä, mitä tulisi tehdä ongelman korjaamiseksi, koska eivät ole itse luoneet automaatioprosessia, ainoastaan hyödyntäneet sitä. (Parasuraman & Riley 1997, 238.)

Työntekijöiden taitotason laskeminen on riski. Automaation hyötyihin tottunut työntekijä ei välttämättä osaa enää itse esimerkiksi asentaa www-palvelinta. Tilanteita, joissa automaatioon ei voida juuri sillä hetkellä turvautua, tulee toiminnassa eteen lähes poikkeuksetta. Automaatiota ei tulisikaan pitää isäntänä, vaan renkinä. Sen avulla on hyvä helpottaa ja tehostaa työntekoa, mutta sen ei pidä antaa ottaa ylivaltaa. Vaikka ihminen poistettaisiin ketjusta, ei inhimillisiä virheitä silti välttämättä saada kokonaan pois.

Tavallisesti tietotekniikan parissa työskentelevät henkilöt suhtautuvat omien tehtäviensä automatisointiin epäluuloisesti. Ajatuksena automatisoinnin lisääminen herättää pelkoa, että työntekijää ei kohta enää tarvita, sillä automaatio korvaa tällä hetkellä käsin tehdyt työtehtävät. Asia on kaksijakoinen, sillä toisaalta järjestelmien ja ohjelmien hallinnan yhä vaikeutuessa ja lisääntyessä tulee niiden saatavuuden ja toimivuuden kuitenkin parantua. Se jättää työntekijät vaikeaan välikäteen, sillä tuotannon kyvyttömyys ja tehokkuus ovat omiaan antamaan syyn ulkoistaa tai vaihtaa henkilökuntaa. Automatisoinnin avulla prosesseihin saadaan kaivattua tehokkuutta ja hallinta helpottuu. (Vizard 2011.)

Automatisoinnin riskit ovat todellisia. Emme elä ideaalimaailmassa, joten muutokset saattavat aiheuttaa ongelmia käyttäjille sekä palveluiden tarjoajille. Jotta suurimpien riskien realisoitumiselta vältyttäisiin, tulee automatisointiprosessia suunniteltaessa ottaa riskit huomioon. Erilaisia virheskenaarioita tulee käsitellä. Testaamisen tulee olla suoritettu huolellisesti ja kunnolla. Tärkeää on myös tietää, miten toimia ongelmatilanteissa ja kuinka niistä informoidaan niin loppukäyttäjää kuin tuotteen parissa työskenteleviäkin henkilöitä. (Vuokko 2012.)

4 VARMISTAMINEN

Tässä kappaleessa tutkitaan, millaisia varmistusmenetelmiä on olemassa tiedon säilyvyyden ja tuotantokäytön turvaamiseksi. Kotilaisen (2005) mukaan tietojen varmistaminen on yksi kaikkein pahimmin laiminlyötyjä alueita yksityishenkilöiden ja jopa yritysten tietokoneiden kohdalla. Varsinkin palvelinten osalta tiedon ja toiminnan varmistaminen on ensiarvoisen tärkeää, sillä ne sisältävät usein toiminnan kannalta kriittisiä tietoja ja toimintoja.

Kuten tiedetään, on päivitysten perimmäisenä tarkoituksena pitää tuotteet ajan tasalla niin toimintojensa puolesta kuin uusimpia tietoturvauhkiakin vastaan. Yleensä päivitykset toimivat kuten pitääkin, ja korjaavat puutteet. Tällöin ne ovat täyttäneet perimmäisen tarkoituksensa, turvan ja toiminnan tehostamisen. Vaikkakin päivitykset yleisesti ottaen ovat hyvin toimivia, aiheuttavat ne välillä ongelmia. Useat päivitykset ja ohjelmat sekä niiden eri versiot saattavat keskenään aiheuttaa jopa niin suuria ongelmia, että tietokone ei päivitysten jälkeen enää käynnisty. Tämänkaltaisilta ongelmilta voidaan välttyä huolellisen valmistautumisen, testauksen ja varmistuksen avulla. (Fisher n.d.)

4.1 Valmistautuminen päivityksiin

Kuten tietoteknisellä alalla yleensä on tapana, on oleellinen osa päivityksiä suunniteltaessa huolellinen valmistautuminen. Alan käytäntöjen mukaan valmistautumisen osalta pohdittavia kohteita on useita. Ensinnäkin tulee valita ajankohta, jona päivitykset asennetaan ja päivitysten asennusten tarvitsemat uudelleenkäynnistykset suoritetaan. Uudelleenkäynnistysten tulisi tapahtua pikimmiten asennusten jälkeen, sillä ilman uudelleenkäynnistymistä eivät päivityksien asennukset ole valmiita. Tällöin päivittämisestä ei ole saatu täyttä hyötyä ja alttius tietoturvauhille pysyy korjaantumattomana. (Griffin 2012.)

Päivittämisajankohdan valmistelun kannalta on syytä ottaa huomioon aika, joka kuluu päivitysten asentamisen aloittamisen, asennusprosessin ja uudelleenkäynnistymisen osalta. Palvelimen käynnistymiseen kannattaa varata mielellään hieman liikaa aikaa kuin liian vähän. Normaalisti käynnistymiselle varattua aikaa on viisi minuuttia. Päivitysten asentaminen on päivitysten määrästä riippuen käynnistämisestä hitaampaa. Päivitysten asentamista varten suositellaan valmistautumaan noin 20 minuutin aikaikkunalla. Kaikkineen yhden palvelimen päivitysprosessi voi viedä aikaa puoli tuntia. (Griffin 2012.)

Useampia palvelimia uudelleen käynnistettäessä ajantarve kasvaa. Shields (2011, 32.) kertoo esityksessään, että kovin montaa palvelinta ei kannata käynnistää uudelleen samanaikaisesti. Sen sijaan käynnistämiset on suositeltua suorittaa porrastetusti. Automatisoinnin osalta tämä tulee valmistautuessa päivityksiin ottaa huomioon ja huolellisesti tarkistaa tarvittavat hienosäädöt. Sama sääntö pätee päivitysten lataamiseen ja asentamiseen. Ne on syytä tehdä porrastetusti, ettei verkko kuormitu liikaa.

Valmistautumisen osalta toinen tärkeä keino on tutustua tulevaan päivityspakettiin etukäteen. Tiedot tulevat Microsoftin sivuilta löytyvään Security TechCenteriin yleensä hyvissä ajoin. Sivuilta löytyy tulevan päivityspaketin lisäksi laajasti tietoa ja hyödyllisiä työkaluja tietoturvaan liittyen (Security TechCenter). Päivityksien ennakkotiedoista selviää, mille käyttöjärjestelmälle ja mille ohjelmalle päivityksiä on tulossa. Lisäksi tarkempaa tietoa uudelleenkäynnistysten tarpeesta löytyy laajalti.

Varsinkin tuotannon kannalta kriittisimpien palvelimien osalta tulee päivityksiin kiinnittää huomiota. Kriittisten palvelinten päivityksiin on ehdottoman suositeltavaa tutustua etukäteen. Palvelinten käyttöjärjestelmäversiot ja ohjelmistoversiot tulee tuntea tarkasti, jotta palvelimille ei lisättäisi merkityksettömiä päivityksiä ja jotta voidaan varmistua, että oikeat tärkeät päivitykset tulevat varmasti perille. Päivitykset saattavat aiheuttaa palvelimille kahdenlaisia ongelmia; odottamattoman uudelleenkäynnistyksen tai toiminnan heikkenemisen. Toiminnan heikkenemistä ovat esimerkiksi jonkin ohjelman toimimattomuus päivitysten sotkiessa sen. Hyvällä valmistautumisella on tärkeä rooli ongelmilta vältyttäessä, mutta varmuutta asiaan se ei tuo. Siksi onkin tärkeää, että päivitykset testataan huolellisesti oikeassa testiympäristössä. (Griffin 2012.)

4.2 Päivitysten testaaminen

Tärkeä osa päivitysprosessia on päivitysten testaaminen. Testaaminen tulee suorittaa realistisessa ympäristössä, sellaisin järjestelmin ja ohjelmin, jotka ovat käytössä myös tuotannossa. Todellisen tuotantoympäristön mukailemisella pyritään aina tehostamaan myös ympäristöllisistä tekijöistä johtuvien virheiden löytämistä. Testauksen päämääränä pidetään kahta asiaa. Testaamisen avulla pyritään saamaan selvyys siitä, että haluttu testauksen kohteena oleva yksikkö, tässä tapauksessa päivitys, tekee sen mitä sen on tarkoitus tehdä. Vastavuoroisesti halutaan saada myös varmuus, että päivitys ei tee mitään sellaista, jota sen ei kuulu tehdä. (Suomalainen 2013, 3.)

Testiympäristön toiminnan kannalta on keskeistä, että päivitykset jaetaan testaukseen määritellyille palvelimille välittömästi niiden julkaisun jälkeen. Testauksen onnistumisen ja mahdollisten ongelmien varalta tulee testipalvelimilla oleville päivityksille varata aikaa useita päiviä. Ongelmat eivät aina ilmaannu välittömästi, vaan saattavat vaatia aikaa tullakseen havaituksi tai aloittaakseen ongelmien aiheuttamisen. Ongelmien selvittäminen ja korjaaminen vievät oman aikansa, joten on pidetty parempana pitää testipalvelimina palvelimia, jotka eivät ole tuotannon kannalta tärkeitä. Kuten Rosato (n.d.) sanoo, päivityksien käyttöönoton tulee aina olla riskiltään pienempi kuin riski olla ottamatta päivityksiä käyttöön.

Huolellisesti suoritettu testaus antaa päivityksien asennuksesta vastaavalle pääkäyttäjälle hyvän pohjan myös kriittisimpien palvelimien päivittämiselle. Kun on havaittu, että päivitykset eivät aiheuttaneet ongelmia tai aiheutuneiden ongelmien syy on selvitetty, voidaan seuraavaksi päivittää lo-

putkin palvelimet. Päivitysprosessi alun valmistelusta lopulliseen asennukseen on aikaa vievä ja pitkä prosessi, kun se tehdään huolella. Tällä tavoin on kuitenkin mahdollista edesauttaa tuotannon tehokkuutta ja taata sen toimivuus. Vaikka Microsoft testaakin jo ennen julkaisua päivitykset huolellisesti, aiheuttavat jotkin niistä ongelmia. Syy on usein ajureissa tai erillisissä ohjelmistoissa tai niiden kombinaatioissa. Aina ei moneenkaan kertaan suoritettu testaus ole riittävä toimenpide, vaan voi tulla eteen tilanne, jossa tarvitaan viimeistä oljenkortta – tietojen varmuuskopiointia. (Fisher n.d.)

4.3 Varmuuskopiointi

Yrityksen toiminnan kannalta sen laitteissa käsiteltävää ja säilytettävää tietoa tulee varjella, sillä sitä pidetään yleisesti ottaen hyvin tärkeänä. Yrityksen it-osaston tehtävänä on pyrkiä turvaamaan tieto ja sen saatavuus parhaansa mukaan. Varmuuskopioinnilla varaudutaan tilanteisiin, joissa tieto voi vahingoittua, hävitä tai muuttua. Edellä mainitun kaltaisia tilanteita saattavat aiheuttaa tietokantojen korruptoituminen, laitteiden rikkoutuminen, käyttäjien virheet, virheelliset päivitykset, jopa luonnonkatastrofit. (Stanek 2012, 519.)

Päivityksien aiheuttamien ongelmien suhteen varmuuskopioinnilla pyritään takaamaan se, että tiedot eivät lopullisesti vahingoittuisi. Vialliset päivitykset on mahdollista poistaa päivityksistä riippuen joko Windows Updaten avulla tai mahdollisesti täysin manuaalisesti. Ongelmat saattavat ratketa päivityksen poistamisen jälkeen. Tilanteissa, joissa ongelmat eivät ratkea ja tiedot pysyvät saavuttamattomissa tai vioittuneina, tulee tarve varmuuskopioinnille. Varmuuskopioinnin onnistumisen ja hyödyn kannalta on välttämätöntä, että on olemassa varmuuskopiointisuunnitelma.

Varmuuskopiointisuunnitelmassa on Stanekin (2012, 520) mukaan useita avainkysymyksiä, jotka tulee ottaa huomioon. On syytä tietää, minkälaista tietoa varmuuskopioidaan. On olemassa tietoa, joka saattaa vaikuttaa merkityksettömältä, mutta sillä voi olla yllättäviä vaikutuksia suuremman kuvan kannalta. Tiedot muuttuvat usein. Tällä on varsinkin vaikutusta siihen, miten usein ja milloin varmuuskopioinnin tulisi tapahtua. Datan muuttuessa päivittäin tulisi varmuuskopioinninkin tapahtua päivittäin, ettei pääse syntymään yli päivän mittaisia aukkoja tietojen talteenottoon. Varmuuskopiointi on hidas prosessi, varsinkin jos varmistettavia kohteita on useampia. Siitä syystä pidetään suunnitelmaa laatiessa ensiarvoisena myös varmistamiselle sopivan ajankohdan löytämistä.

Yleisimpiä varmuuskopiointitapoja ovat täydellinen varmuuskopiointi, kasvavan vedostuksen menetelmä, varovaisen korvaamisen menetelmä, differentaalimenetelmä sekä useiden eri menetelmien yhdistelmät. Täydellisellä varmuuskopioinnilla kopioidaan kaikki tieto, esimerkiksi kokonainen palvelin. Kasvavan vedostuksen menetelmällä vain muuttunut tieto varmistetaan. Varovaisella korvaamisella tarkoitetaan sitä, että päivityksiä ei tehdä suoraan itse tietokantaan vaan sen osiin tai kopioihin. Vasta päivityksien jälkeen kopio korvaa varsinaisen tietokannan. Täydellinen varmuuskopiointi vaatii usein suuria määriä tallennustilaa, sillä varmuuskopioitava

kohde voi sisältää lukemattoman määrän tietoa. Kasvavan vedostuksen menetelmällä tallennettavan tiedon määrä pysyy pienempänä, mutta tarvittava tieto on silti saatavilla. (Helenius, 2003.)

Varmistusmenetelmistä suosituimpia ovat varmistusnauhat, sillä niitä on helppo arkistoida turvalliseen paikkaan ja niihin mahtuu paljon tietoa. Lisäksi nauhat ovat verrattain edullisia. Varmistuksia ei tule pitää koskaan samassa tilassa varmistettavan tiedon kanssa, sillä silloin kaiken tiedon menettämisen riski kasvaa. Tiedon menettämiseltä suojautumiseksi on varmuuskopioinnin lisäksi muitakin laajalti käytössä olevia keinoja. Erityisesti suosittua nykyisillä toimintatavoilla on pitää kovalevyjä, joilla tärkeää tietoa sijaitsee, RAID (redundant array of independent disks) tilassa. Se tarkoittaa sitä, että kovalevyt ovat vähintään kahdennetut. Yhden kovalevyn tuhoutuminen ei siis vielä vaaranna toimintaa. Tietojen kahdentamista ei silti pidetä yksinään riittävänä ratkaisuna, vaan varmuuskopioinnista huolehtiminen on paras keino säilyttää tuottavuus halutulla tasolla. (Helenius 2003.)

5 HALLINTAOHJELMAT

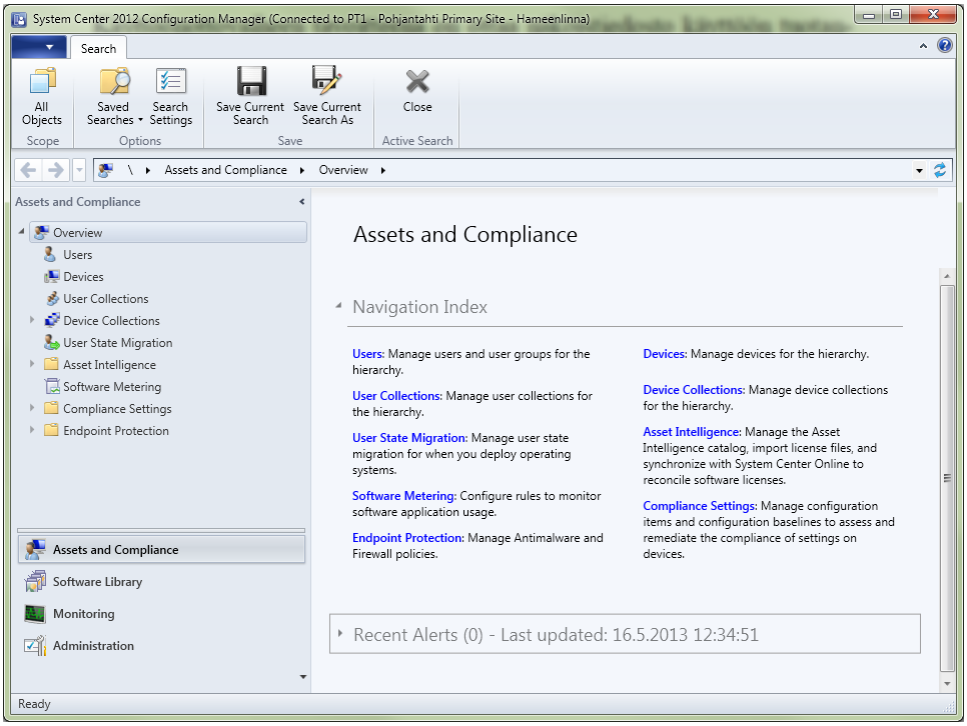
Tässä luvussa tarkastellaan suurien laiteympäristöjen hallintaa helpottamaan luotuja hallintaohjelmistoja ja niiden tarjoamia mahdollisuuksia palvelinten päivitysten automatisointiin. Hallintaohjelmalla tarkoitetaan sovellusta, joka mahdollistaa useampien työasemien tai palvelimien hallitsemisen ohjelman avulla yhdeltä koneelta käsin. Järjestelmien keskitettyä hallintaa käytetään erityisesti suurissa ja keskisuurissa yrityksissä. Jos yrityksessä on alle kymmenen tietokonetta, on yleisesti pidetty tehokkaampana tehdä tarvittavat toimenpiteet jokaiselle koneelle paikan päällä kuin opetella uuden ohjelman käyttöä tai hankkia verrattain arvokas lisenssi ohjelmaan.

Erityisesti hallintaohjelmien hyöty tulee esiin, kun yrityksellä on useita toimipisteitä, joissa koneita sijaitsee. Yrityksen it-henkilökunta ei välttämättä voi aina mennä paikan päälle, eikä se useimmiten ole järkevääkään pitkien välimatkojen takia. Yleisimpiä käyttökohteita hallintaohjelmille ovat keskitetty sovellusten ja tietokoneiden hallinta. Lisäksi on hyvin tavanomaista, että tietoturvaa ja tallennuskapasiteettia hallitaan samaisen ohjelmiston avulla.

5.1 Älykkään hallinnan ohjelmisto SCCM 2012

SCCM 2012 on Microsoftin System Center -tuoteperheeseen kuuluva tuote. Se on työn kirjoittamishetkellä tuorein Microsoftin tätä tarkoitusta varten luoma hallintaohjelmisto. Ohjelmassa on satoja toimintoja ja ominaisuuksia, joiden avulla IT-alan ammattilaiset voivat hallita ja ylläpitää järjestelmiään. Keskeisimpiä toimintoja ovat ohjelmien jakelu, laitteistojen hallinta, tietoturvan ylläpito sekä erilaiset raporttityökalut. (Moilanen 2012.)

Amaris, Morimoto, Handley & Ross (2012, 11-12) kertovat ohjelman tärkeimmistä toiminnoista tarkemmin. Ohjelma tarjoaa kaikki tarvittavat työkalut, joita tarvitaan käyttöjärjestelmän asentamiseen ja asennuskuvan luomiseen sekä asennuksien suorittamiseen etänä. (Kuva 3.) Ohjelman valikoimiin kuuluu myös ohjelmaan määriteltyjen laitteiden ominaisuuksien ja komponenttien seuraamiseen tarkoitettu työkalu. Sen avulla ylläpitohenkilökunta on aina tietoinen, millainen käyttöjärjestelmä ja mitä ohjelmia ja komponentteja on koneessa, johon he ovat tekemässä toimenpiteitä. Kattavien integroitujen etähallintatyökalujen avulla ylläpitohenkilökunnan on mahdollista ottaa etäyhteys haluttuun järjestelmässä olevaan tietokoneeseen, sijaitsi tietokone sitten fyysisesti missä päin maailmaa tahansa. Etäyhteyden hyöty on varsin merkittävä, sillä se säästää resursseja ja aikaa. Etäyhteys mahdollistaa ongelmien nopean ratkaisun ja asennuksien suorittamisen ja seurannan reaaliajassa.



Kuva 3. SCCM 2012 hallintakonsolin etusivunäkymä

Muita ohjelman merkittäviä ominaisuuksia Amarisin ym. (2012, 12) mukaan ovat ohjelmistojen jakelu sekä raportointityökalut. Ohjelmistojen jakelu helpottaa varsinkin suurten ympäristöjen parissa toimiessa työtaakkaa huomattavasti. Yrityksessä käytössä olevista ohjelmistoista, kuten Office 2013 -ohjelmistosta tehdään paketti, joka sitten voidaan SCCM 2012 ohjelman avulla jakaa kaikille käyttäjille, jotka sen tarvitsevat. Näin ollen käyttäjän itse ei tarvitse huolehtia asennukseen liittyen mistään. Asennuspaketti lähetään halutulle koneelle ja se asentuu koneeseen huomaamattomasti taustalla. Raportointityökalujen avulla taasen on mahdollista saada tietoa kattavasti lähes kaikesta, mikä vain on liitettynä järjestelmään. Yleisimpiä tietoja ovat tietokoneiden tiedot, päivitystasot sekä ohjelmistot.

Palvelinten tietoturvapäivitysten näkökulmasta asiaa tarkastellen voidaan SCCM 2012 pitää hyvänä ohjelmana. Se tarjoaa kattavat ominaisuudet päivitysten keskitettyyn hallintaan, jakeluun ja asentamiseen. Lisäksi ohjelma tarjoaa kattavia raportteja päivityksistä. Raportteja voi tarkistella päivityskohtaisesti. Raportista käy ilmi hyvin yksityiskohtaisia tietoja, kuten se, mitkä järjestelmässä olevat tietokoneet tarvitsevat minkäkin päivityksen. Jakelun kannalta ohjelmassa on tarjolla ajastetut jakelut. Niitä käytetään laajalti automaatioratkaisujen yhteydessä. Ohjelmaan voidaan määrittää erilaisia määrityksiä, joissa kerrotaan mihin aikaan päivitykset saa lähettää valituille koneille. Näin ollen päivitykset voidaan jaella tietokoneilla haluttuna ajankohtana. Tällaisia ajankohtia ovat ne, jotka eivät aiheuta minkäänlaista haittaa tuotannolle. Usein se tarkoittaa sitä, että päivitykset jaetaan kohdekoneille yöaikaan tai viikonloppuisin. (Nilsson 2012.)

Kriittisesti tarkasteltuna voidaan SCCM:n 2012 mainioista toiminnallisuuksista huolimatta ohjelmasta löytää myös yritysten kannalta huonoja puolia. Kuten useimmissa Microsoftin merkittävissä tuotteissa, on myös SCCM 2012 -ohjelmistossa olemassa lisenssimaksut. Lisenssimaksuja tulee maksaa jokaisesta työasemasta sekä palvelimesta, jotka ohjelmaan on liitetty. Kun koneita ja palvelimia on yhteensä satoja, tulee summasta monen yrityksen kannalta merkittävä. Palvelinten osalta lisenssimaksut ovat selvästi työasemia korkeammat. (System Center 2012 Licensing Pricing and SKU Overview 2011.)

Yritysten maksaessa lisenssimaksuja monista käytössä olevista ohjelmistoistaan ja laitteistaan vuositasolla tuntuvia summia, kasvaa mielenkiinto ratkaisuun olla käyttämättä kaikkia SCCM 2012 -hallintaohjelmiston tarjoamia päivityskeinoja varsinkin palvelinten osalta. Nykyisessä taloustilanteessa houkutus välttää kalliit lisenssimaksut kasvaa. Asia on täysin ymmärrettävä, sillä on olemassa myös laadukkaita ilmaisia ohjelmia, joilla pystyy suorittamaan lähes täydellisesti samat tehtävät. Tällaisesta ohjelmasta oiva esimerkki on tässä työssä seuraavaksi käsiteltävä Windows Server Update Services, eli WSUS.

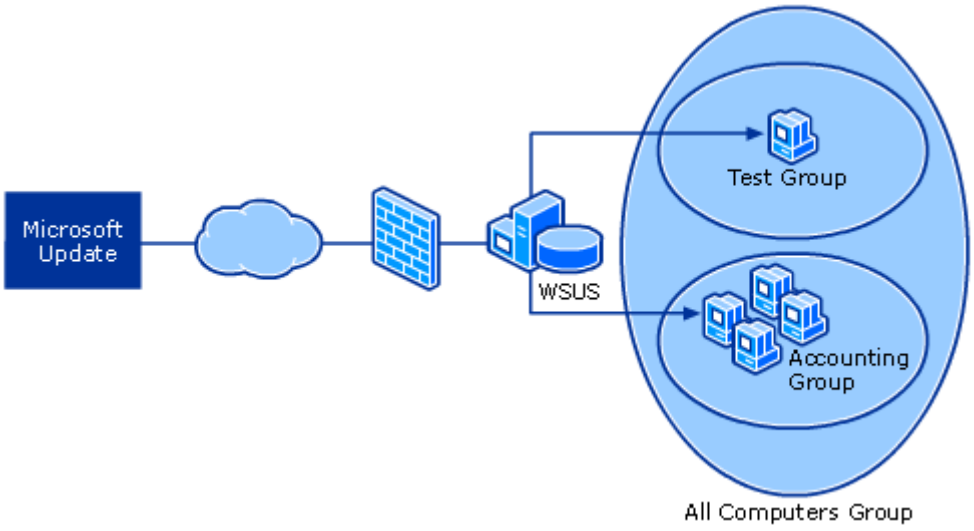
5.2 Ohjelmistopäivitysten jakelu- ja synkronointityökalu WSUS

Windows Server Update Services (WSUS), joka aikaisemmin tunnettiin nimellä Software Update Services (SUS), on Microsoftin tarjoama ilmainen ohjelmisto. Se on suunniteltu päivitysten jakelun keskittämisen helpottamiseksi erityisesti yritysten ympäristöissä. Viimeisin versio ohjelmasta on 3.0 SP2, joka julkaistiin 26. tammikuuta 2009. WSUS tukee kaikkia Microsoftin tarjoamia palvelinkäyttöjärjestelmiä, joilla on elinkaarta jäljellä. Näistä yleisimmät ja laajimmin käytössä ovat Windows Server 2008 R2 SP1 sekä Windows Server 2003 SP2 -käyttöjärjestelmät. (Microsoft Technet 2013.)

Ohjelman toimintamalli on suunniteltu helpottamaan tärkeiden päivitysten hallinnointia erityisesti useamman päätelaitteen kohteissa. Ohjelma lataa Microsoftin tarjoamat päivitykset palvelimelle, johon WSUS on asennettu. Latausten ajankohta – synkronointi – on mahdollista määrittää haluttuun

ajankohtaan. Microsoft suosittelee, että synkronointi tapahtuisi päivittäin, jotta varmistetaan myös mahdollisten kriittisten yllättäen julkaistujen päivitysten nopea hyödynnettävyys. (Microsoft Technet 2013.)

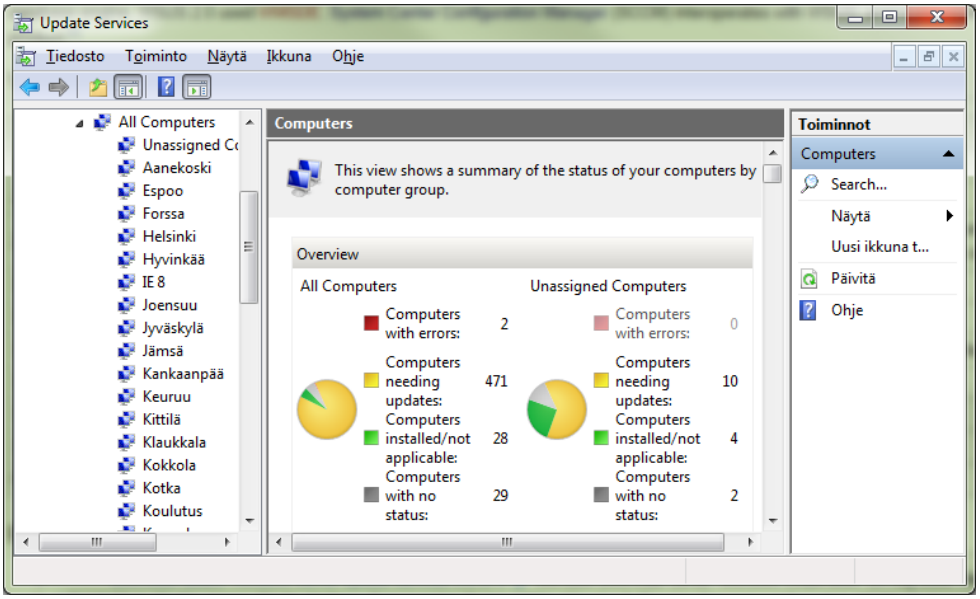
Synkronoidut päivitykset ovat tallessa WSUS-palvelimella. Kyseiseltä palvelimelta käsin päivitykset jaetaan eteenpäin verkon tietokoneille. (Kuva 5.) Näin ollen jokaisen päätelaitteen ei tarvitse erikseen muodostaa yhteyttä verkon ulkopuolelle saadakseen tarvittavat päivitystiedot. WSUS-palvelimen yksi keskeisimpiä ominaisuuksia on, että pääkäyttäjä, joka hallinnoi ohjelmaa voi valita ja ryhmittää, mitkä päivitykset jaellaan millekin koneelle. Päivityksiä voi ryhmitellä ohjelmassa esimerkiksi tuotteen mukaan. Näin ollen on helppo ryhmittää palvelimille tarkoitetut tietoturvapäivitykset omaksi ryhmäkseen.



Kuva 5. Windows Server Update Services -ohjelman toimintaperiaate (Microsoft Technet 2013.)

Päivitysten toiminnallisuuden puolesta WSUS muistuttaa hyvin paljon aikaisemmin käsiteltyä SCCM 2012 -tuotetta. Asia onkin varsin ilmeinen, sillä SCCM 2012 hyödyntää sisällään WSUS:n versiota 6.2 joka on suunniteltu vain kyseisen ohjelmiston käyttöön (Amaris ym. 2012). Tässä osiossa käsitellään kuitenkin ohjelman versiota 3.0 SP2, joka on viimeisin itsenäinen WSUS-ohjelma.

WSUS tarjoaa käyttäjilleen kattavia raportteja päivityksistä. Ohjelman avulla on mahdollista seurata kaikkien ohjelmaan syötettyjen päätelaitteiden päivitystilannetta. (Kuva 6.) Tietoja päivityksistä saa päivityskohtaisesti joko tekstimuodossa tai erilaisina piirakkakuvioina, kun on kyse suuremmista kokonaisuuksista. Ohjelman tarjoaa lisäksi tarvittavia automaatio-ominaisuuksia. Ohjelman avulla on mahdollista määrittää, minkälaisia päivityksiä ja mille laitteelle kyseiset päivitykset jaellaan ja ladataan. Lopullinen hienosäätö WSUS:n tapauksessa tapahtuu Windows-laitteisiin sisällytettyjen ryhmäkäytäntöjen avulla.



Kuva 6. Windows Server Update Services -ohjelman etusivunäkymä

Tarkasteltaessa ohjelmaa palvelinten tietoturvapäivitysten automatisoinnissa käytettäväksi työkaluksi, löytyy siitä useita hyviä puolia. Suurimpana etuna ohjelmassa on sen käyttöfilosofia. Ohjelman on tarkoitus olla ilmainen, kaikkien käytettävissä oleva yksinkertainen apuväline. Sen avulla pystyy hoitamaan päivitykset kaikille yleisimmille käytössä oleville palvelintyypeille Windows ympäristöstä puhuttaessa. Tilastojen valossa WSUS on erityisen suosittu keskikokoisten ja suurten yritysten käytössä. Vuoden 2011 tilastojen mukaan ohjelmaa käytti 60 % suurista ja keskisuurista yrityksistä. (Shields 2011, 6.)

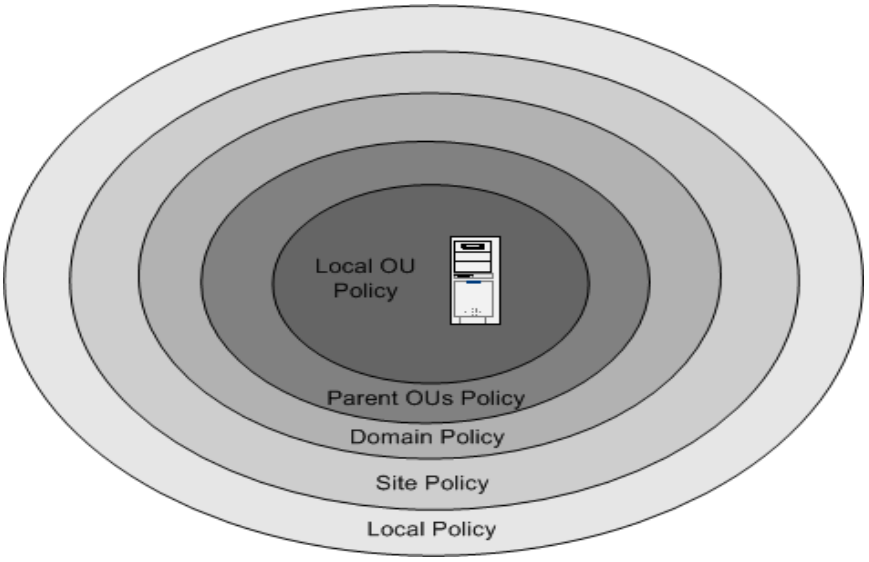
Ohjelman kannalta epäedullisena voidaan pitää tietämättömyyttä sen tulevaisuudesta. Ohjelman toiminnallisuuksia on jo nyt integroitu maksullisiin hallintasovelluksiin. Vaikkakin ohjelmaa on vielä päivitetty, jotta sen avulla voitaisiin tukea uusimpia Windows Server 2008- ja Windows 8 -käyttöjärjestelmiä, lienevät uudet päivitykset jatkossa yhä harvinaisempia ja pienimuotoisempia. Lisäksi työn tehokkuuden ja rakenteiden yksinkertaisuuden takia on olemassa perusteita, joiden vuoksi erillisen WSUS-palvelimen ylläpito jo SCCM 2012 -hallintaohjelmistoja käyttävissä ympäristöissä on turhaa.

5.3 Ryhmäkäytännöt

Hallintaohjelmien lisäksi on osa vastaavista toiminnoista mahdollista toteuttaa Windows käyttöjärjestelmiin integroidun Group Policy (ryhmäkäytäntö) -ominaisuuden avulla. Ryhmäkäytäntö löytyy kaikista Microsoft Windows -tuotteista, jotka ovat julkaistut Windows 2000 -käyttöjärjestelmän jälkeen. Pääasiassa se kattaa kaikki nykyaikaiset ja hieman vanhemmatkin käyttöjärjestelmät. Ryhmäkäytäntö on yksi Active Directoryn (AD) tarjoamia keskeisimpiä työkaluja ympäristöjen hallintaa varten. Useamman työaseman tai palvelimen skenaarioissa, joissa AD on käytössä, on mahdollista ja suotavaa käyttää myös ryhmäkäytäntöjä. (Moskowitz 2010.)

Ryhmäkäytäntöjen tärkein tehtävä on yksinkertainen. Sen tarkoituksena on tehdä laitteisto- ja käyttäjäympäristöjen hallinnasta yksinkertaisempaa ja helpompaa. Sen avulla pääkäyttäjien ja ylläpitäjien ei tarvitse erikseen suorittaa jokaista tehtävää fyysisesti käyttäjän koneella tai sen äärellä. Pienten säätöjen ja muokkausten kohdalla hyöty käy varsin selvästi ilmi. Pienen muutoksen tekeminen sadoille koneille ei olekaan työmäärältään ja ajankäytöltään enää pieni tehtävä. Ryhmäkäytäntöjen avulla sama säätö voidaan määrittää yhdeltä tietokoneelta käsin kaikille saman verkkoympäristön tietokoneille. Ryhmäkäytäntö antaa ylläpitäjille ja pääkäyttäjille vallan määrittää loppukäyttäjien tietokoneen käyttökokemusta suuresti. (Moskowitz 2010.)

Ryhmäkäytäntöjä voidaan määritellä eri tasoille. Näitä tasoja ovat paikallisen koneen käytännöt, verkkoympäristön käytännöt, domainin käytännöt ja viimeisimpänä organisaatioyksikön käytännöt. (Kuva 7.) Jokaiselle käytännölle voidaan määritellä erilaisia asetuksia, mutta käytännöt toimivat siten, että organisaatioyksikkö on vahvin ja paikallinen heikoin. Niinpä esimerkiksi domainille määritelty ryhmäkäytäntö kumoutuu, jos käyttäjä tai tietokone saa erilaisen käskyn organisaatioyksikön ryhmäpolitiikalta, johon kuuluu. Taso, jolle määritykset määritellään, tulee ottaa huomioon, jotta saadaan aikaan haluttu vaikutus.



Kuva 7. Ryhmäkäytäntöjen hierarkia (Microsoft Technet)

Käytännössä ryhmäkäytäntöjen avulla voidaan määritellä lukematon määrä erilaisia määrityksiä sen alaiseksi määritellyille tietokoneille. Määrityksiä voi tehdä lisäksi myös käyttäjätileille. Mahdollisia määrityksiä ovat kaikki aina virranhallinta-asetuksista salasanojen vaatimusmäärittelyihin. Jotta saadaan paras mahdollinen teho irti ryhmäkäytännöistä, tarvitaan niiden muokkaamiseen ja käyttöönottamiseen erillinen hallintakonsoli (GPMC). Hallintakonsoli on mahdollista ladata Microsoftin verkkosivuilta ilmaiseksi. (Zinman 2004.)

Päivittämisten osalta ryhmäkäytännöt eivät tarjoa aivan kaikkea sitä toiminnallisuutta, jota hallintaohjelmilla saadaan aikaiseksi. Ryhmäkäytäntöjä voidaan kuitenkin osaltaan käyttää tehostamaan toimintaa ja niiden avulla voidaan tehdä päivityksien automatisoinnin vaatimia säädöksiä. Ryhmäkäytännöistä löytyy alasivu Windows Update -palvelun säätöjen muokkaamiseen.

6 POHJANTÄHDEN PALVELINYMPÄRISTÖ

Tässä luvussa on tarkoituksena perehtyä Pohjantähden tämänhetkiseen palvelinympäristöön ja sen hallintaan sekä tehdä huomioita ja ehdotuksia toiminnan kehittämiseksi. Pohjantähti tarjoaa vakuutuspalveluita yrityksille ja yksityishenkilöille. Vakuutusten käsittely ja käsittelyohjelmat tarvitsevat tuekseen kattavan palvelinverkoston, jotta tuotantotoiminta säilyy häiriöttömänä.

Asiakaspalvelun sujuvuus ja tyytyväiset asiakkaat ovat tavoite, johon Pohjantähti panostaa. Siksi on tärkeää, että yhtiön palvelimet ovat ajan tasalla ja palvelevat tuotantokäyttöä mahdollisimman hyvin. Palvelimilla sijaitsee toiminnan kannalta kriittisiä ohjelmia, joten on tärkeää, että niiden toimintakunto varmistetaan parhaalla mahdollisilla tavalla. Lisäksi asiakkaiden henkilökohtaisia vakuutustietoja käsitellään yhtiön palvelimilla.

Tiedot ovat luottamuksellisia, joten tietoturvan ylläpito on senkin osalta tärkeää. (Pohjantähti 2013.)

Pohjantähdessä palvelinten ylläpidosta vastaa yhtiön käyttöpalveluhenkilökunta. Palvelinten ylläpitoa ei ole virallisesti määritelty yhdelle henkilölle.. Palvelinten päivittämisen kannalta ajateltuna tämä ei ole ideaaliratkaisu, sillä toimintatavat saattavat vaihdella. Päivittämiselle ei myöskään ole määritelty päivämääriä, joten jotkin palvelimet saattavat päivityskierroksen yhteydessä unohtua. Päivittämättömät palvelimet aiheuttavat yhtiölle tietoturvariskin (F-Secure 2013).

Tärkeimpien palvelinten osalta päivityskäytännöt ovat tällä hetkellä toimivat. Päivitykset jaellaan Windows Server Update Services (WSUS) -ohjelman avulla manuaalisesti. Kunkin päivityskierroksen yhteydessä määritetään suojaus- ja tietoturvapäivitykset, jotka toimitetaan WSUS-ohjelmassa kategorisoiduille palvelimille. Päivityksien toimivuutta ja varmuutta testataan ensin testiryhmässä, johon on määritelty myös palvelimia. Testiryhmän palvelimia seuraamalla voidaan todeta, jos jokin päivitys aiheuttaa haittaa palvelinten tehokkaalle tuotantokäytölle tai ilmaantuu muita ongelmia, jotka mahdollisesti ovat päivitysten aiheuttamia.

Testiryhmän palvelimista suurin osa on tällä hetkellä Windows Server 2003 -käyttöjärjestelmää käyttäviä palvelimia. Koska yhtiöllä on myös laajalti käytössä Windows Server 2008 -pohjaisia palvelimia, tullaan testiryhmä muokkaamaan uudenlaiseksi osana palvelinten tietoturvapäivitysten automatisointiprosessia. Näin voidaan olla varmempia siitä, että päivitysten pilotointivaihe on tehokas ja hyödyllinen koko prosessin kannalta.

6.1 Käytössä olevat palvelimet

Pohjantähdellä on tällä hetkellä käytössä 60 Windows-palvelinta. Fyysisesti palvelimet sijaitsevat pääosin pääkonttorin tiloissa, erillisessä konesalissa. Muutamia palvelimia sijaitsee kuitenkin myös yhtiön aluekonttoreissa. Palvelinten rooli aluekonttoreilla on toimia paikallisina tulostinpalvelimina sekä tiedostopalvelimina. Pohjantähden Tampereen konttorilla palvelin toimii nimipalvelimena.

Teknisesti tarkasteltuna Pohjantähden palvelinympäristö on kirjava. Fyysiset konesalissa sijaitsevat palvelimet ovat pääosin saman laitevalmistajan, IBM:n palvelimia. Aluekonttoreilla sijaitsevat palvelimet ovat osaltaan Dellin valmistamia. Iältään ja malleiltaan palvelimet eroavat jonkin verran toisistaan. Vaikkakin osa palvelimista on jo elinkaarensa loppupuolella, ajavat ne vielä asiansa. Palvelinkaluston uusiminen ja mahdollinen uudelleenorganisointi esimerkiksi virtualisoinnin osalta tulisi kuitenkin suorittaa viimeistään vuonna 2015 osana käyttöjärjestelmän päivittämistä Windows Server 2003 -versiosta uudempaan versioon.

Käyttöjärjestelmien osalta Pohjantähden palvelinympäristö on selkeä ja toimiva. Käyttöjärjestelminä palvelimissa ovat käytössä Microsoft Windows Server 2003 ja 2008. Kyseisistä palvelimille tarkoitetuista käyttöjärjestelmistä on asennettuna viimeisimmät versiot: Windows Server 2003 SP2 sekä

Windows Server 2008 R2 SP1 (LeBlanc 2011.) Käyttöjärjestelmät ovat tuettuja Microsoftin osalta. Se tarkoittaa, että järjestelmiin julkaistaan tietoturvapäivityksiä kuukausittain. On kuitenkin todettava, että konesalin perältä löytyvät Windows NT -käyttöjärjestelmällä pyörivät palvelimet, joiden tehtävänä on toimia ainoastaan yhtiön sisällä ilmestyvänä henkilökuntalehden alustana, tulisi poistaa pikimmiten ja korvata ajanmukaisella ratkaisulla. Windows NT:n viimeisimmän version tuki loppui vuonna 2004. Uusia korjauksia ja tietoturvapäivityksiä ei ole siis tullut liki kymmeneen vuoteen. Päivitysten avulla taataan, että järjestelmistä havaitut uudet tietoturvaukot paikataan, eikä haavoittuvuus täten lisäänny.

Yhtiön palvelimille asennettavia käyttöjärjestelmiä mietittäessä on syytä ottaa huomioon palvelimien tuelle luvattu elinkaari. Tässä tapauksessa Pohjantähdellä laajasti käytössä olevalla Windows Server 2003 -käyttöjärjestelmällä elinkaari tulee päätökseensä 14. heinäkuuta 2015. Kirjoittamishetkellä tarkasteltuna järjestelmällä on tuettua elinkaarta jäljellä siis vain kaksi vuotta. Windows Server 2008 R2 -käyttöjärjestelmän osalta elinkaarta on jatkettu tammikuuhun 2020. (Microsoft elinkaarituki 2013.) Palvelinten kattavaa tietoturvatasoa myös tulevaisuudessa pohdittaessa on syytä miettiä, asennetaanko palvelimiin enää Windows Server 2003 -käyttöjärjestelmää. Tämä on Pohjantähdessä otettu huomioon, sillä uudet palvelinasennukset ovat uudempaa Windows Server 2008 R2 -mallia. Nykyisten palvelimien kohdalla vanhempi käyttöjärjestelmä on vielä hyvin toimiva, kunhan varmistetaan, että viimeisimmät tietoturvapaketit ja päivitykset ovat varmasti asennetut.

6.2 Virtuaalipalvelimet

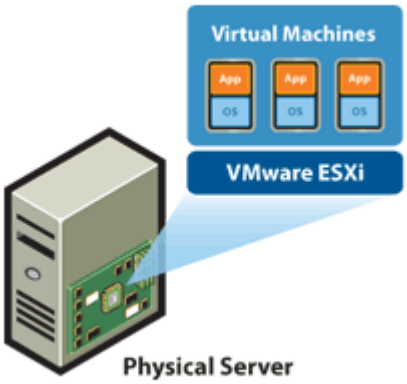
Tässä opinnäytetyössä käsiteltävistä Pohjantähden palvelimista merkittävä osa on toteutettu virtuaalisina. Virtualisointi on yksi viime aikojen kuumimmista trendeistä IT-alalla. Sen avulla on mahdollista asentaa ja käyttää useita käyttöjärjestelmiä yhden fyysisen koneen sisällä. Käytännössä se tarkoittaa sitä, että yhden tietokoneen sisällä ajetaan esimerkiksi kuutta virtuaalista tietokonetta jakaen fyysisen koneen resurssit näiden kuuden virtuaalisen tietokoneen kesken.

Virtualisointialustoja tarjoavia yrityksiä ja tuotteita on monia. Pohjantähden virtuaalipalvelimet ovat toteutettu VMware-alustalla. VMware on yksi tunnetuimmista ja arvostetuimmista virtualisointialustojen tarjoajista ja sen tuotteita on laajasti käytössä monilla yrityksillä. VMwaren etuna pidetään sen joustavuutta, helppoutta, vakautta ja hyvää tukea. (Troy & Hemke 2009, 1-2.)

Virtualisoinnin tarjoamat hyödyt alan ammattilaiselle ovat huomattavat. Sen avulla koneiden, tässä tapauksessa palvelimien, tehoista saadaan irti suurempi osa, joten koneet eivät turhaan ole tyhjäkäynnillä käyttäen vain 10-15 % kapasiteetistaan. Virtualisoinnin avulla pääkäyttäjät ja suunnittelijat voivat rakentaa kattavia testiympäristöjä, jossa on useita eri käyttöjärjestelmillä ja ominaisuuksilla varustettua tietokonetta. Ilman virtualisointia tällaisen ympäristön rakentaminen vaatisi useampia koneita ja paljon aikaa.

Virtualisoinnin avulla kaikki onnistuu yhden laitteen sisällä. Yksi syy virtualisoinnin yleistymiseen on sen tuoma rahallinen ja ajallinen sekä hallinnollinen hyöty. Hyödyt käyvät ilmi varsinkin ympäristöissä, jossa on käytössä useampia palvelimia, jotka ovat mahdollista virtualisoida. (Troy & Hemke 2009, 2.)

Virtuaalipalvelimet toimivat aivan kuten fyysisetkin palvelimet ja niissä on mahdollista ajaa vastaavia ohjelmia. Virtuaalipalvelimia rakentaessa tulee ottaa huomioon, että isäntäkoneessa on tarpeeksi tehoa, jotta virtuaalikoneet voivat pyöriä moitteettomasti. Esimerkiksi palvelin, jossa on käytössä keskusmuistia 8 gigatavua ja kovalevytilaa 500 gigatavua käyttää resursseistaan vain murto-osan. Tällainen palvelin voidaan virtualisoida siten, että se pyörittäisikin sisällään kolmea virtuaalipalvelinta, jotka saavat kukin käyttöönsä keskusmuistia 2 gigatavua ja kovalevytilaa 120 gigatavua. Näin saataisiin yhden palvelimen sijasta kolme virtuaalipalvelinta. (Kuva 8.)



Kuva 8. Virtuaalikoneen perusperiaate

Tässä työssä käsiteltävät virtuaalipalvelimet toimivat itsenäisinä palvelimina pitäen osaltaan yllä Pohjantähden tuotantotoimintaa. Virtuaalipalvelimet, kuten fyysisetkin palvelimet, tulee pitää ajan tasalla uusimpien tietoturvapäivitysten osalta. Virtuaalikoneiden päivittämisprosessi ei tässä tapauksessa eroa fyysisien koneiden päivitysprosessista lainkaan.

6.3 Palvelinten kategorisointi

Päivitysten automatisointiprosessin helpottamiseksi palvelimet luokitellaan. Ensimmäiseen testiluokkaan kuuluvat palvelimet ovat virtuaalipalvelimia. Kyseisillä virtuaalipalvelimilla suoritetaan päivitysten jakelun, testauksen ja toimivuuden varmistaminen, eli niin sanottu raakatestaus.

Pilottiluokkaan kuuluvat palvelimet, jotka eivät ole tuotannon kannalta kriittisiä. Nämä palvelimet toimivat myös testauksen pääasiallisina kohteina. Pilottiryhmän palvelimiin jaetaan ja asennetaan päivitykset lähes välittömästi niiden ilmestyttyä. Pilottipalvelimissa päivityksien toiminnallisuutta testataan viikon ajan. Viikon ajalta saadaan tietoon, jos jokin päivitys haittaa palvelimien toimintaa tai päivityspaketissa on muuten puutteita. Kun

on saatu tarpeeksi tietoa päivitysten toiminnasta, voidaan päivitykset jakaa kriittisille tuotantopalvelimille.

Tuotantopalvelimilla tarkoitetaan niitä palvelimia, jotka ovat yrityksen toiminnan kannalta tärkeässä asemassa. Palvelimissa liikkuu hyvin tärkeitä tietoja ja ne ylläpitävät Pohjantähden kannalta tärkeitä ohjelmia. Näitä ohjelmia ovat sellaiset ohjelmat, joita tarvitaan päivittäiseen työntekoon vakuutusten parissa. Palvelinten on kyettävä toimimaan tehokkaasti ilman turhia katkoja. Palvelinten tietoturvan tason tulee myös ehdottomasti olla korkein mahdollinen. Johtuen palvelinten herkkyydestä, tulee niihin asennettujen päivitysten olla testattuja. Tämä aiheuttaa omat haasteensa automatisoinnille (Budd 2006.)

Palvelinten käynnistäminen tuottaa pohdittavaa palvelinten päivitysten automatisointia suunniteltaessa. Uudelleenkäynnistys on uuden päivityskierroksen jälkeen lähes poikkeuksetta välttämätön, jotta uudet päivitykset asentuvat ja tulevat voimaan. Toisaalta tärkeimpiä palvelimia tulee voida käyttää katkeamattomasti tuotantokäytössä ilman uudelleenkäynnistyksen aiheuttamia viiveitä ja häiriöitä. Tämän ongelman ratkaisemiseksi tärkeimpien palvelimien uudelleenkäynnistys on suositeltua asettaa ajankohtaan, jolloin uudelleenkäynnistys ei aiheuta haittaa yhtiön toiminnalle. Tällaisia aikoja ovat viikonloput sekä arkipäivisin yöajat.

Pohjantähdessä käytäntönä on ollut asettaa uudelleenkäynnistyminen tapahtumaan arkipäivisin yölliseen aikaan. Tällöin uudelleenkäynnistyminen, myös mahdollinen viivästynyt sellainen, ei aiheuta katkoksia itse yrityksen avaintoimintaan. Uudelleenkäynnistymisestä seuraavana aamuna on mahdollista tarkistaa, että kaikki palvelimet ovat käynnistyneet halutulla tavalla.

Päivitysten automatisointiprosessin kannalta uudelleenkäynnistäminen on asia, joka tulee harkita tarkkaan. Automatisoinnin tarkoituksena on toimia työtä tehostavana toimenpiteenä, ei lisätyön aiheuttajana (Vuokko 2012). On siis ensiarvoisen tärkeää, että automatisointiprosessissa ei aseteta palvelimia käynnistymään yhtiön toiminnan kannalta epäedullisiin aikoihin. Tämä tullaan ottamaan huomioon ja uudelleenkäynnistykset – siltä osin kuin niitä automatisoidaan – tullaan suorittamaan nykyisen käytännön mukaisesti.

6.4 Hallintaohjelmien käyttö

Pohjantähdessä on käytössä työssä aikaisemmin käsitellyt hallintaohjelmat SCCM 2012 sekä WSUS. Ohjelmien käyttötarkoitus- ja historia on hyvin vaihteleva. Ohjelmien sisältämistä samoista ominaisuuksista huolimatta käytetään niitä varsin eri tarkoituksiin.

System Center Configuration Manager 2012 on otettu käyttöön Pohjantähdessä loppuvuoden 2012 aikana osana käyttöjärjestelmämigraatiota Windows XP -käyttöjärjestelmästä Windows 7 -käyttöjärjestelmään. Ohjelman avulla on saatu luotua uusien työasemien asennus- ja migraatioprosessista lähes täysin automatisoitu, joka on osaltaan helpottanut suuresti vaativan

prosessin suorittamisessa. Ohjelmaa tullaan lisäksi käyttämään pääasiallisena hallintaohjelmana, jonka avulla hallitaan kaikkia yhtiön työasemia. (Pohjantähti 2013.)

Johtuen ohjelman lyhyestä käyttöhistoriasta, ei ohjelmaa ole yhtiössä vielä päästy käyttämään aivan täydellä teholla. Pääasialliset ominaisuudet, kuten asennuspakettien teko ja jakelu sekä asennusautomaatio ovat eniten käytetyt ominaisuudet. Kyseisiä ominaisuuksia on käytetty kattavasti osana migraatioprosessia ja näin osaltaan tehostettu toimintaa. Sen sijaan ohjelman tarjoamaan päivitysten jakeluun ei ole tartuttu sen tarjoamien toiminnallisuuksien osalta kovinkaan kattavasti. Mahdollisuuksia on tutkittu ja työasemien päivitysten osalta asennusketjun säädökset ja konfiguraatiot on tehty ja testattu, mutta käyttöönottoa ei ole viety sen pidemmälle. Osasyynä tähän on jo käytössä olevan päivitysratkaisun toimivuus, joten tarvetta ei ole ilmaantunut tai sitä ei ole oltu halukkaita muuttamaan. Toimintojen keskittäminen yhden ohjelman sisään olisi joka tapauksessa järkevä ratkaisu.

Ohjelmaa pääasiallisesti käyttäviä Pohjantähden työntekijöitä on aikomus vuoden 2013 aikana kouluttaa, jotta ohjelmasta saataisiin suurempi hyöty irti. Tällä hetkellä osaaminen on pääasiassa itse hankittua, muutamia lyhyitä laitetoimittajan pitämiä koulutuksia lukuun ottamatta. Ohjelman tärkeimmät ominaisuudet ovat kuitenkin tiedossa ja sen käyttö on työasemahallinnan ylläpidon kannalta ehdottomasti toimivaa.

Pohjantähden tietohallinnolla on lisäksi käytössään viimeisin versio WSUS-hallintaohjelmasta. Sillä hallitaan pääasiassa yhtiön työasemien päivitysten jakelua. Palvelinten suhteen päivitykset jaellaan myös WSUS:n avulla, mutta prosessi on lähes täysin täysin manuaalinen. Ehtojen mukaan määritellyt päivitykset ladataan keskitetysti WSUS-palvelimelle, josta ne päivityskohtaisesti yksi kerrallaan jaetaan eteenpäin palvelimille. Nykyinen ratkaisu ei kuitenkaan ole ainoa olemassa oleva vaihtoehto. Ohjelma tarjoaa automatisointimahdollisuuksia, joiden avulla palvelinten tietoturvapäivitysten automatisointi on mahdollista toteuttaa. Lisäominaisuuksia ohjelman käyttöön ja automatisointiin on mahdollista saada ryhmäkäytäntöjen avulla säädetyillä komennoilla.

Vaikkakin WSUS on tällä hetkellä laajalti käytössä ja tehtävässään toimiva ratkaisu, löytyy siitä myös negatiivisia asioita. Kriittisesti tarkasteltuna erillisen WSUS-palvelimen ylläpito Pohjantähden ympäristössä on tarpeetonta. Microsoft on päättänyt integroida Windows Server Update Services palvelun System Center Service Manager 2012 ohjelmaan (Amaris ym. 2012, 11). Kyseinen ohjelma on otettu Pohjantähdessä käyttöön vuoden 2013 aikana (Pohjantähti 2013). Kahden erillisen ylläpidettävän järjestelmän sijaan olisi mahdollista saada sama toiminnallisuus yhden, uudemman ohjelman avulla. Tällä hetkellä WSUS:n avulla hoidettavat työasemien päivitykset on jo osittain siirretty SCCM 2012 -ohjelmaan, mutta niiden käyttöönottoa ei ole saatettu loppuun asti.

WSUS ei ole enää kovin uusi ohjelma. Sen viimeisin versio on vuodelta 2009. Tukea on kuitenkin osittain jatkettu, ja vuonna 2012 ilmestyneen päivityksen avulla on ohjelmalla mahdollisuus hallinnoida myös Windows 8-

ja Windows Server 2012 -käyttöjärjestelmien päivityksiä (SUS Blog 2012). Luopuminen järjestelmästä saattaa olla ajankohtaista viimeistään siinä vaiheessa, kun saadaan kattavampaa tietoa järjestelmän tuen ja päivitysten jatkuvuudesta.

Ohjelmaa puoltaa siitä kertynyt aikaisempi käyttökokemus käyttöpalveluhenkilökunnan keskuudessa. Mahdollisten virhetilanteiden ja uusien määritysten kohdalla on todennäköistä, että ratkaisu syntyy ilman suurempia ponnisteluja. Eduksi katsotaan lisäksi se, että ohjelma on ilmainen. Verrattuna aikaisemmin läpikäytyyn Microsoft System Center Configuration Manager 2012 ohjelmaan, on lisenssimaksuissa säästettävä summa huomattava. Yrityksen näkökulmasta katsottuna erillisen ohjelman tarjoama palvelu on riittävä, verrattuna lisähintaan, joka maksettaisiin täydellisestä yhteen järjestelmään siirtymisestä.

7 AUTOMATISOINTIRATKAISUN KÄYTÄNNÖN TOTEUTUS

Tässä luvussa käsitellään Pohjantähden palvelinten tietoturvapäivitysten automatisoinnin toteuttamista, valittua menetelmää ja toimintatapoja. Luvussa käydään läpi tehdyt määritykset ja muutokset sekä tarkastellaan ratkaisujen toimivuutta. Työn tarkoituksena oli tehostaa Pohjantähden palvelinhallintaa ja tietoturvatason ylläpitoa, joten työssä käytettyjä ratkaisuja on pyritty tutkimaan ja toteuttamaan siten, että ne tukisivat tavoitetta parhaalla mahdollisella tavalla.

Työn kirjoittamishetkellä Pohjantähden palvelinympäristön ja erityisesti tietoturvapäivitysten hallinta oli pitkälti manuaalista. Päivittämisille varatut ajankohdat olivat hyvin vaihtelevia ja palvelimien toiminta-aikoja tutkittaessa kävi ilmi, että tietoturvan taso osassa palvelimista oli heikentynyt. Heikentyminen johtui pitkälti siitä, että päivityksistä ja niiden asentamisesta saattoi olla aikaa useamman päivityskuukauden verran. Tällaiset puutokset juontavat juurensa siitä, että tarkkaa päivityssykliä ei ole. Työssä tutkittujen automatisointimahdollisuuksien valossa asiaan on saatavilla muutos. Päivitysprosessin automatisointi kiinteään ajankohtaan on osaltaan tehokas keino hallita palvelinten tietoturvapäivityksiä. Automatisointi ja tarkka ajankohta helpottavat henkilökunnan osalta päivitysrutiinista aiheutuvaa taakkaa. Toisaalta se myös taholtaan vaatii, että henkilökunta tarkistaa päivitysten ja palvelinten toimintakunnon ja kiinnittää näin ollen huomiota niiden toimintaan.

Tutkittaessa automatisointiprosessia palvelinten päivittämisen osalta kävi useista lähteistä ilmi, että täydellinen automatisointi ei ole aina paras vaihtoehto. Varsinkin tuotannon ja toiminnan kannalta tärkeiden palvelinten osalta tulee olla hyvin tarkkana, mitä automatisoi. Turhat katkokset ja mahdolliset ongelmat aiheuttavat yhtiölle huomattavasti enemmän haittaa verrattuna hyötyyn, joka saadaan kuukaudessa mahdollisena työajan tehostamisena. Ongelmatilanteissa työaikakaan ei tehostu, vaan sitä menee hukkaan. Jotta palvelinten tietoturvapäivitysten automatisoinnista saataisiin pa-

ras teho irti, ilman että asetettaisiin palvelimia tai Pohjantähden tuotantotoimintaa kuitenkaan turhan riskin alaiseksi, todettiin parhaaksi ratkaisuksi palvelinten tietoturvapäivitysten osittainen automatisointi.

7.1 Toteutuksen apuvälineiden valinta

Työssä tutkittiin Pohjantähdellä jo käytössä olevia hallintaohjelmia, joiden avulla tietoturvapäivitysten automatisointi olisi mahdollista toteuttaa. Järjestelmät olivat Windows Server Update Services (WSUS) sekä System Center Configuration Manager 2012 (SCCM 2012).

Vaikka järjestelmät ovat toiminnallisuudeltaan hyvin samankaltaisia, on näistä WSUS selkeästi suppeampi ohjelma. Se on tarkoitettu vain päivitysten hallintaan, kun taas SCCM 2012 on täysiverinen hallintaohjelma. Sen avulla on mahdollista suorittaa useita erilaisia yrityksen tietohallinnon joka päiväisessä toiminnassa tarvittavia tehtäviä. Optimaalisessa tilanteessa ei näitä kahta järjestelmää käytettäisi rinnakkain ja ylläpidettäisi periaatteessa turhaan ylimääräistä palvelinta.

Työssä tarkastellussa skenaariossa Pohjantähden osalta SCCM:n 2012 tarjoamaa täyttä hyötyä ei saatu irti. Työasemien osalta päivittäminen ohjelman avulla on jo osittain aloitettu ja vaadittavia määriteltyjä tehty. Palvelinten osalta ohjelmaa ei tulla käyttämään, sillä tarvittavia palvelinlisenssejä ei ole hankittu. Lisenssien hankkiminen ainakaan lähiaikoina ei myöskään ole ajankohtaista, sillä lisenssien hinta on suhteellisen korkea verrattuna realistiseen hyötyarvoon, joka niistä saataisiin.

Työssä päädyttiin ratkaisuun, jossa automatisoinnin toteuttamista tukevaksi järjestelmäksi valittiin jo käytössä oleva WSUS. Ohjelmaa puoltaa siitä kertynyt kokemus palvelimia ylläpitävien henkilöiden parissa, sen helppous ja taloudelliset syyt. Rahallinen säästö verrattuna SCCM 2012 -ohjelman lisenssien hankkimiseen on huomattava, sillä WSUS on ilmainen. Ohjelma tarjoaa riittävät ominaisuudet, jotta automatisointia voidaan toteuttaa. WSUS:n tulevaisuuden osalta ei ole asiantuntijapiireissä täyttä varmuutta. Ohjelmaa voidaan kuitenkin pitää tällä hetkellä Pohjantähden palvelinympäristön tietoturvapäivitysten hallinnan kannalta kustannustehokkaimpana ja täysin riittävänä vaihtoehtona.

WSUS itsessään ei mahdollista päivitysten hallintaa kattavimmalla tasolla. Se toimii kuitenkin saumattomasti yhteen Windows-ympäristöissä käytössä olevien ryhmäkäytäntöjen kanssa. Työssä tullaan käyttämään halutun automaatiotason saavuttamiseksi ryhmäkäytäntöjä, joita muokataan määrittämään päivitysasetuksia halutulla tavalla. Ryhmäkäytäntöjen avulla saadaan määritykset ja päivityskäytännöt toimimaan halutulla tavalla, jotta kaikkien palvelinryhmien osalta toiminta on kuvatun kaltaista.

7.2 Toteutusmenetelmä

Toteuttamisen kannalta parhaaksi vaihtoehdoksi todettiin palvelinten tietoturvapäivitysten automatisoinnin osalta niiden osittainen automatisointi. Se

tarkoittaa käytännössä sitä, että aivan kaikkien palvelinten osalta päivityskäytäntöjä ei automatisoida. Palvelimet päätettiin jakaa kahteen ryhmään, joiden avulla saadaan käyttöön järkevin ja turvallisin ratkaisu. Näitä ryhmiä ovat yhä manuaalisesti päivitettävät palvelimet sekä automatisoidut palvelimet.

Tärkeimpien palvelinten osalta toimintavarmuus on olennaista. Näiden palvelinten tapauksissa hyödyt eivät ole merkittävästi riskejä korkeampia, joten paras ratkaisu on huolehtia päivittämiset ihmisvoimin valvovan silmän alla. Tämä ryhmä on kooltaan selvästi pienempi. Ryhmään kuuluvien palvelinten osalta automatisointia ei ratkaisuna voitu eikä haluttu toteuttaa täydellä potentiaalilla. Päivitysten vaatimia uudelleen käynnistyksiä ei haluttu määrittää erikseen tietylle ajankohdalle, sillä palvelimien tulee palvella käyttäjiä parhaalla mahdollisella tavalla eri ajankohtina. Palvelimilla sijaitsevat tiedot ovat myös yhtiön kannalta hyvin oleellisia, joten päivitykset haluttiin jakaa edelleen käsin ja suorittaa asennus valvotusti sopivalla hetkellä, jotta voidaan olla täysin varmoja, ettei automatisointiratkaisu aiheuta haittaa tältä osin yhtiön toiminnalle.

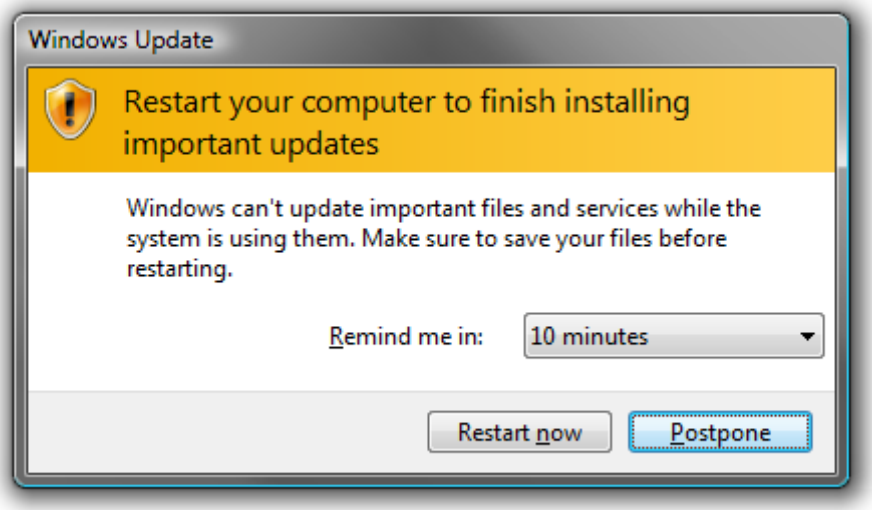
Automatisoitu palvelinryhmä, johon sisältyy eniten palvelimia, rakennettiin täysin automatisoitavista palvelimista. Ryhmän palvelimiin jaetaan, ladataan ja asennetaan päivitykset automaattisesti. Lisäksi uudelleen käynnistykset suoritetaan automaattisesti ennalta määriteltynä ajankohtana. Tämän ryhmän osalta ajankohdaksi valittiin päivityksien julkaisusta seuraava maanantai. Päivitykset julkaistaan aina joka kuukauden toinen tiistai. Testiryhmälle päivitykset asennetaan heti päivityksien julkaisemista seuraavana keskiviikkona, eli välittömästi vuorokauden kuluessa päivitysten julkaisusta.

Näiden palvelinten osalta ylläpito tehostuu, sillä ne saavat tarvittavat tietoturvapäivitykset ilman suurempaa ylläpitoa. Ylläpidon osalta riittää, että tarkistetaan ovatko palvelimet käynnistyneet uudelleen, kuten pitää. Lisäksi on syytä aika ajoin tarkistaa, että päivitykset ovat onnistuneet kuten pitääkin. Päivityksien seuranta on mahdollista jo olemassa olevalla hallintaohjelmalla.

Alun perin oli toimeksiantajan puolelta toiveissa, että palvelimet tultaisiin jakamaan kolmeen ryhmään. Kolmannen ryhmän osalta päivittämisen automatisointiratkaisuksi oli suunniteltu Pohjantähden toiveiden mukaista ratkaisua, jossa päivitykset jaetaan, ladataan ja asennetaan automaattisesti. Uudelleen käynnistykset olisi kuitenkin tultu suorittamaan tässä tapauksessa manuaalisesti. Tällaisessa ratkaisussa tulee ottaa huomioon, että palvelimen toiminnan kannalta ei ole ideaalitilanne, että päivityksien asentamisen jälkeen päivitysten toimintakunnon ja viimeistelyn vaatima uudelleen käynnistys jää odottamaan taustalle. Tarkistelluissa lähteissä tämänkaltaista ratkaisua pidettiin toiminnan kannalta huonona, eikä sitä suositeltu. (Kuva 9.)

Ratkaisun riskialttiuden ja osittain sen vaatimien laajojen säätöjen tai kolmannen osapuolen palveluiden käyttämisen vuoksi päädyttiin ratkaisuun, jossa päivitysten automatisointi suoritetaan kahden ryhmän voimin. Näitä

ryhmiä ovat pienempi, jatkossakin manuaalisesti päivitettävä kriittisten palvelinten ryhmä sekä laajempi, automatisoitavien palvelimien ryhmä. Varsinaisten ryhmien lisäksi osa automatisoitavista palvelimista kuuluu testiryhmään.



Kuva 9. Päivitysten toimivuuden kannalta palvelinten uudelleen käynnistys tulisi suorittaa pian asennuksen jälkeen

7.3 Testiympäristöt

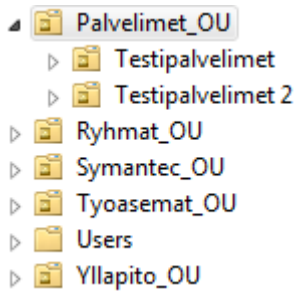
Valmisteltaessa ja suunniteltaessa päivitysprosessia, tuli sen tarjoamista hyödyistä ja laadusta varmistua ennen varsinaista käyttöönottoa. Testaamisessa käytettiin kahta erilaista käytäntöä. Ensin suoritettiin pienempimuotoisempi raakatestaus, jotta saatiin varmuus ratkaisun toimivuudesta ja toteuttamismahdollisuuksista. Raakatestaus tarjosi kattavasti tietoa, mitä tulee tehdä ja mitä korjata. Pohjan oltua kunnossa, oli vielä saatava varmuus käytännön toimivuudesta. Se suoritettiin oikeilla palvelimilla suoritetulla testaamisella.

7.3.1 Raakatestaus virtuaaliympäristössä

Valitun päivittämismenetelmän perusteelliseksi testaamiseksi toimintaympäristössä tehtiin testausprosessia varten kaksi eri testiryhmää. Ensimmäinen raakatestaukseen tarkoitettu testiryhmä toteutettiin täysin riippumattomina virtuaalipalvelimina virtuaaliympäristössä. Kyseinen virtuaaliympäristö luotiin vain tätä tarkoitusta varten rakennetulle VMware-alustalle. Alustan isäntäkoneena toimi itsenäinen Dell Optiplex 390 -työasema, johon on lisätty tarvittava määrä muistia palvelinkäyttöjärjestelmien käyttöä varten.

Luoduille virtuaalipalvelimille rakennettiin oma organisaatioyksikkö Pohjantähden toimialueeseen. (Kuva 10.) Organisaatioyksiköllä tarkoitetaan yksikköä, johon voidaan lisätä tietokoneita tai käyttäjiä. Organisaatioyksikölle voidaan antaa määrityksiä ja sääntöjä, jotka vaikuttavat kaikkiin sen

sisällä oleviin objekteihin. Testausta varten rakennettu organisaatioyksikkö luotiin jo olemassa olevan Palvelimet-organisaatioyksikön sisään. Tällä varmistetaan se, etteivät mahdolliset säädökset ja komennot sekoita muita ympäristössä olevia laitteita. Komennot ja konfiguroinnin määritetään suoraan testiorganisaatioyksikölle.



Kuva 10. Luodut testiryhmät

Testattavat virtuaalipalvelimet päätettiin luoda perusasetuksilla ilman oikeassa ympäristössä olevia ominaisuuksia, kuten tiedostojen jakoa tai käyttöjärjestelmän lisänä olevia ohjelmistoja, sillä kyseessä ei ole viimeisin testausvaihe. Tällä tavoin säästettiin niin resursseja kuin aikaakin. Käyttöjärjestelmiksi valittiin Pohjantähdessä laajalti käytössä olevat käyttöjärjestelmät Windows Server 2003 SP2 sekä Windows Server 2008 R2. Testiryhmän koneet päätettiin liittää Pohjantähdellä käytössä olevaan toimialueeseen, joten ne olivat realistinen osa yhtiön verkkoa. Koneisiin asennettiin viimeisimmät Windows Updaten tarjoamat tietoturvapäivitykset, jotta koneiden lähtötaso saatiin mahdollisimman lähelle nykytilannetta. Itse testaamiseen käytettävät päivitykset olivat myöhemmin kuukausittaisten päivityspakettien mukana julkaistavia päivityksiä.

Rajallisten resurssien vuoksi virtuaalista testiympäristöä ei päätetty kasvattaa kahta palvelinta suuremmaksi ympäristöksi. Vaikkakaan kahden palvelimen tarjoama ympäristö ei ole laajuutensa puolesta ideaalinen, todettiin se vielä raakatestauksen vaiheessa riittäväksi. Palvelinten lukumäärää enemmän raakatestausvaiheessa puutteita aiheuttaa mahdollisten lisäohjelmien puuttuminen, joita tuotantokäytössä olevissa palvelimissa hyödynnetään. Näin ollen testausprosessi ei vielä tässä vaiheessa anna täyttä kuvaa päivitysten toimivuudesta. Virtuaalisen testiryhmän pääasiallisena tarkoituksena on kuitenkin toimia suunnannäyttäjänä testauksen suhteen.

Raakatestauksessa saatujen kokemuksien mukaan päivittämisten automatisointi on mahdollista järkevällä tavalla toteuttaa myös tuotantokäytössä oleviin palvelimiin. Testauksessa käytetty menetelmä, johon päädyttiin päivitysratkaisua mietittäessä, osoittautui toimivaksi. WSUS-ohjelmassa määritettiin automaattinen jakelu valituille päivityksille. Päivitykset valittiin ohjelman tarjoamien suodattimien avulla. Päivitykset valittiin niiden luokan ja kohteen mukaan. Valittuja luokkia olivat kaikki suojauspäivitykset, tärkeät päivitykset sekä määrityspäivitykset. Päivitysten tulee kuulua edellä

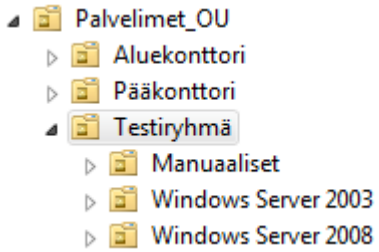
mainittuihin ryhmiin. Lisäksi päivitysten tulee olla suunnattu Windows Server 2003:n ja Windows Server 2008:n eri versioille. Molempien sääntöjen toteutuessa julkaistun päivityksen kohdalla, jakaa WSUS kyseiset päivitykset automaattisesti valitulle ryhmälle.

Päivitysten asentaminen testiryhmässä tapahtui ryhmäkäytäntöjen määrityksien avulla. Määrityksillä valittiin haluttu ajankohta, tässä tapauksessa keskiviikkoiltapäivä. Aina uusien päivityksien ilmestyessä keskiviikkoisin WSUS-palvelin jakaa sen suodattimien avulla määritellyt päivitykset, ja palvelinryhmän ryhmäkäytännön mukaisesti päivitykset asentuvat keskiviikkona iltapäivällä. Lisäksi toinen virtuaalipalvelin määriteltiin käynnistymään uudelleen kahdeksan minuuttia päivitysten asentamisen jälkeen, jotta voitiin todeta automaattisten uudelleenkäynnistysten viivästysten toimivuus osana automaatioprosessia.

7.3.2 Pilottivaiheen testaus

Kahden virtuaalipalvelimen avulla suoritetun testauksen pohjalta päätettiin testiympäristöä kasvattaa oikeilla käytössä olevilla palvelimilla. Laajempaan testiryhmään valittiin palvelinten luokittelun mukaisesti vähemmän kriittisiä palvelimia. Kyseisten palvelimien osalta mahdolliset ongelmat eivät olisi tuotannon kannalta merkittäviä, mutta niiden avulla saatu aito ja kattava palaute päivitysprosessista on työn kannalta merkittävä.

Pilottiryhmän rakentaminen aloitettiin pitäen silmällä rakenteen yhtenäisyyttä myös tulevaa rakennemuutosta ajatellen. Olemassa olevan Palvelimet-organisaatioyksikön alle luodut testiyksiköt liitettiin yhdeksi kokonaiseksi organisaatioyksiköksi, jolle luotiin kolme alayksikköä. Alayksiköt nimettiin palvelimissa käytettävien käyttöjärjestelmien mukaan. Palvelimet jaotellaan yksiköihin testausvaiheessa käyttöjärjestelmänsä mukaan. Lisäksi on luotu yksi organisaatioyksikkö palvelimille, joiden osalta testattiin osittaista automatisointiratkaisua. (Kuva 12.)



Kuva 12. Luotu testiryhmä

Testiryhmä koostuu kolmesta alayksiköstä. Yksiköissä on yhteensä 10 palvelinta. Palvelimet jakautuvat siten, että Windows Server 2003 -palvelimia on niille varatussa ryhmässä yhteensä viisi kappaletta. Windows Server 2008 R2 -palvelimia on puolestaan kolme kappaletta. Osittaisen automatisoinnin mahdollistamassa osaltaan manuaalisesti päivitettävien palvelimien ryhmässä on kaksi palvelinta. Näiden kahden palvelimen kohdalla päivitykset asennetaan automaattisesti, mutta uudelleen käynnistäminen tapahtuu

pääkäyttäjän valitsemana ajankohtana. Pilottivaiheen testaus päätettiin asettaa suoritettavaksi samaan aikaan kuin raakatestauksessakin oli tehty.

Ensimmäisellä testauskierroksella oikean tuotannon palvelimilla saatiin paljon arvokasta tietoa nykyisten määritysten toimivuudesta ja muutoksien tarpeista. Testauksen aikana huomattiin, että yhden testiryhmään määritellyn palvelimen kello oli väärässä ajassa. Tilanne oli mystinen, sillä palvelimen tulisi saada aikansa samalta palvelimelta, jolta muutkin. Aikavyöhyke oli kuitenkin väärä, joten kellonajan mukaan määritellyt päivitykset eivät kyseiselle palvelimelle haluttuna ajankohtana menneet.

Arvokasta tietoa testaus tarjosi myös palvelinten uudelleen käynnistymisien osalta. Käynnistymiseen tarvittavat porrastukset olivat melko lyhyet, joten niiden osalta tehtiin muutoksia parempaan suuntaan. Varsinkin puhuttaessa virtuaalipalvelimista tulee käynnistymisien tapahtua suuremmalla aikavälillä vähintään saman virtuaaliympäristön sisällä olevien palvelimien osalta. Liian usean virtuaalipalvelimen uudelleen käynnistymisen lyhyen aikavälin sisällä saattaa aiheuttaa isäntäkoneelle tukoksen, mistä syystä käynnistymisprosessi hidastuu huomattavasti.

Ratkaisu, jossa päivitykset asennetaan valmiiksi ja uudelleen käynnistykset suoritetaan erillisenä kellon aikana, osoittautui toiminnan kannalta huonoksi ratkaisuksi. Asennetut päivitykset vaativat uudelleen käynnistyksen, eikä sen viivästyttäminen ole järkevää. Ratkaisu on lisäksi hankala toteuttaa valitun menetelmän avulla. Ratkaisun järkevämmäksi toteuttamiseksi olisi vaadittu kolmannen osapuolen ohjelma tai vaihtoehtoisesti jokaiselle palvelimelle sisäänkirjaututeena oleva käyttäjä. Kumpikaan ratkaisuista ei ollut tässä tapauksessa järkevä, joten ratkaisun miettimisestä päätettiin luopua.

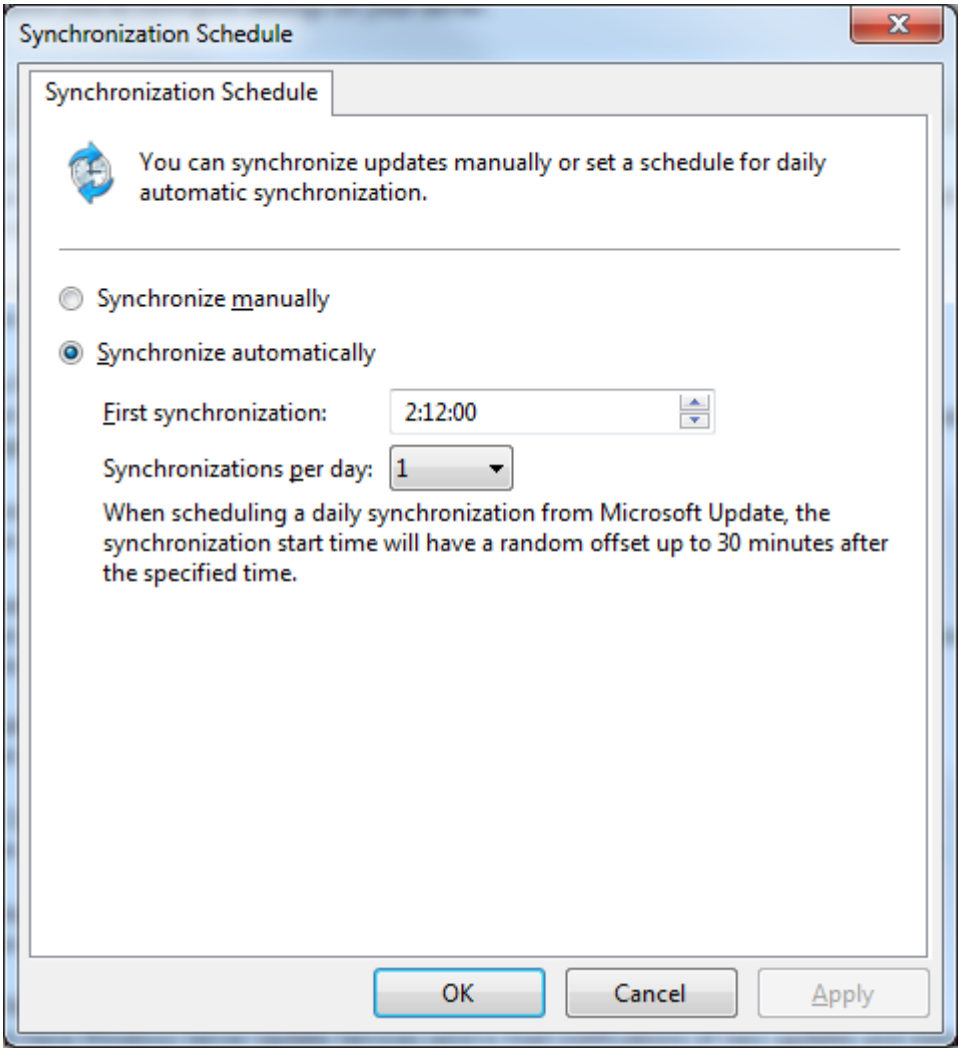
7.4 Päivitysten määritykset

Päivitysprosessin onnistumisen kannalta olennaista on se, miten eri välineitä käytetään toimimaan yhdessä, jotta lopputulos olisi halutun kaltainen. Työssä saavutetun lopputuloksen saavuttamiseksi käytettiin useita eri tekniikoita ja palveluita. Päivitykset jaettiin WSUS:n avulla, asennus ja käynnistämiset hoidettiin ryhmäkäytäntöjen avulla ja varmistukset Windowsin tarjoaman tehtävien hallinnan avulla suoritetuilla komentojonoilla ja skripteillä.

7.4.1 Hallintaohjelman määritykset

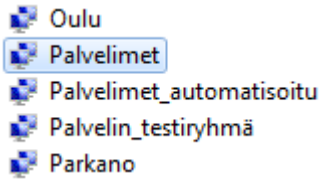
WSUS-ohjelman synkronointeja määrittäessä päädyttiin samaan ratkaisuun, joka oli käytössä jo ennen työn aloittamista. Ohjelma oli määritelty synkronoimaan päivitykset Windows Update -palvelusta aina päivittäin kello 02:12:00. Ajankohta sopi myös tässä opinnäytetyössä käsiteltävän ratkaisun kannalta mainiosti, joten sitä ei päätetty muuttaa. Synkronointeja oli määritelty tapahtuvaksi kerran päivässä. Määrä on täysin riittävä, sillä päivityksien julkaisutahti on pääsääntöisesti kerran kuukaudessa, aina kuukauden toinen tiistai. Harvemmissa tapauksissa korjauspäivityksiä ilmestyy

myös kuukauden toisen tiistain jälkeen. Tällöinkin päivittäinen synkronointi on riittävä ratkaisu. (Kuva 13.)



Kuva 13. Työssä käytössä oleva päivitysten synkronointiratkaisu

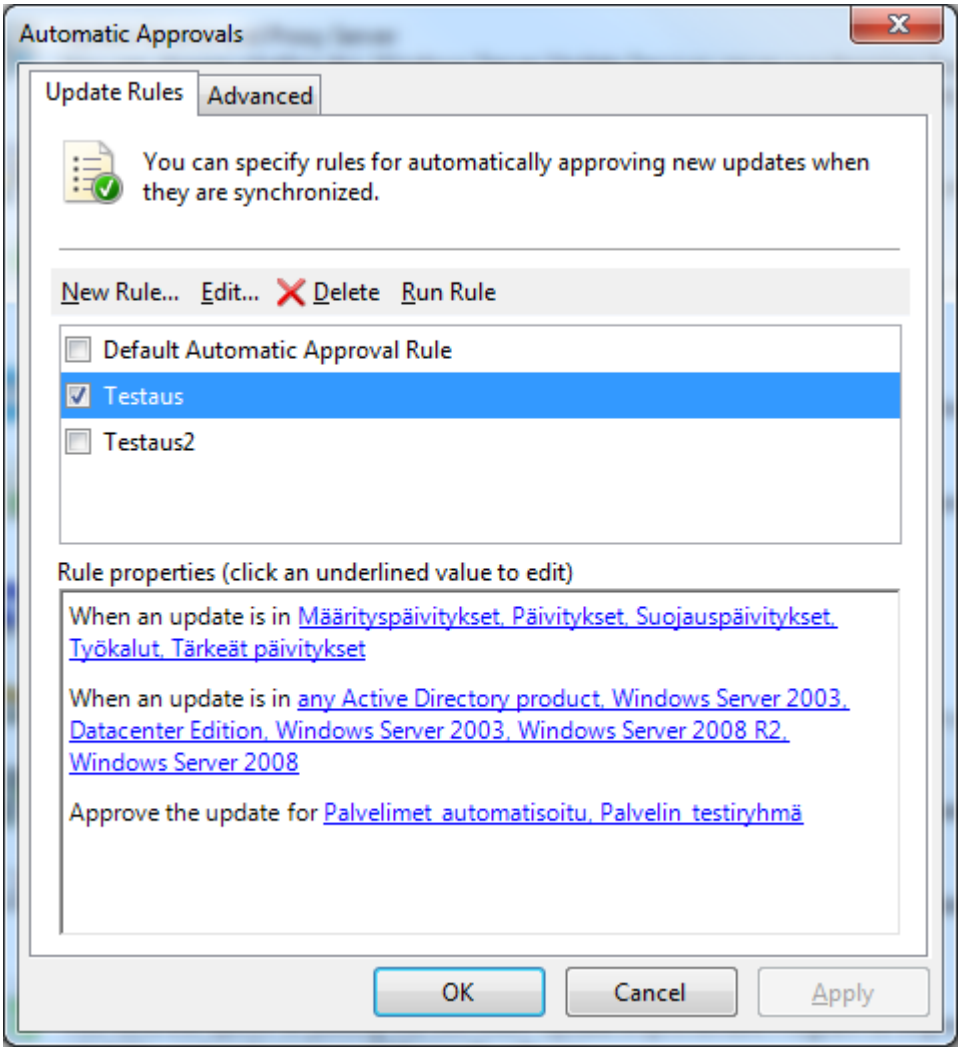
Synkronointiasetuksien jälkeen päätettiin tarkistella palvelinten jakoa ryhmiin. WSUS-ohjelmassa on jo olemassa ryhmät konttoreittain, tehtyinä halutuin määrityksin. Ryhmien osalta työssä toteutettiin hienosäätöä, mutta vain palvelimien osalta. Alun perin käytössä oli vain ryhmä nimeltään Palvelimet, jossa sijaitsi kaikki Pohjantähden päivitysten piirissä olevat palvelimet. Tämän palvelinryhmän lisäksi päätettiin työssä luoda kaksi ryhmää. Näistä ensimmäisenä luotiin testiryhmä, jossa päivityksiä testataan. Toiseksi luotiin ryhmä, joka nimettiin ”palvelimet_automatisoitu” nimellä. Tähän ryhmään kuuluu kaikki ne palvelimet, jotka ovat automatisoinnin piirissä. Alkuperäiseen palvelinryhmään kuuluu yhä ne palvelimet, joiden osalta automatisointia ei nähty järkeväksi toteuttaa. (Kuva 14.)



Kuva 14. Luodut palvelinryhmät Windows Server Update Services -ohjelmassa

Päivitysten jakelun automatisoinnin mahdollistamiseksi määritettiin WSUS:n asetuksista synkronoitavien päivitysten automaattiset hyväksynnät päälle. Päivitysten hyväksyntää varten luotiin sääntö, jonka avulla karsittiin päivityksiä vastaamaan kohdekoneiden tarpeita. Määritykset asetettiin niin, että päivitykset olivat merkitykseltään tärkeitä ja kohdennettu suoraan kohdepalvelimilla oleviin käyttöjärjestelmiin. Sääntöjä on mahdollista luoda useita. (Kuva 15.)

Säännöistä jätettiin valitsematta tuotteiden toiminnan kannalta tärkeät Service Pack -päivitykset. Kyseiset päivityspaketit ovat kooltaan todella laajoja, ja niiden asentaminen kestää huomattavasti pidempään kuin normaalien suojauspäivitysten asennus. Toinen syy kyseisten päivitysten pois jättämiseen oli se, että Microsoft julkaisee Service Pack -päivityksiä hyvin harvakseltaan. Kyseisten päivityspakettien ilmaantuessa niistä tiedotetaan laajasti jo etukäteen. Onkin järkevämpää, että kyseiset paketit päivitetään kaikkiin tarvitseviin tuotteisiin manuaalisesti.

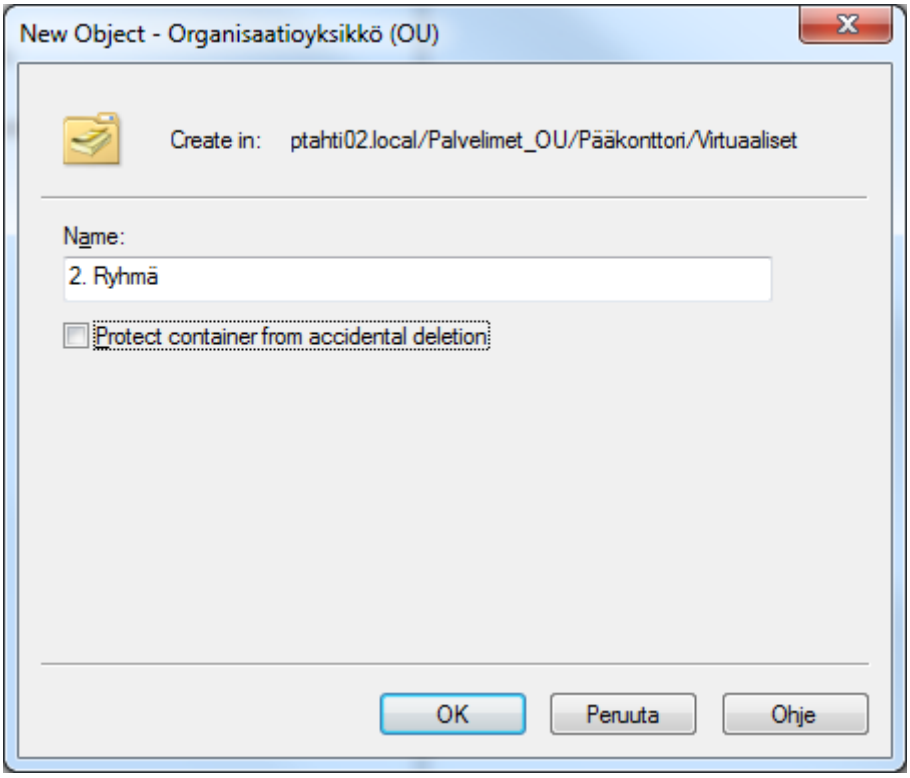


Kuva 15. Esimerkki automaattisen jakelun määrityksistä

7.4.2 Active Directoryn määritykset

Active Directoryssa, eli AD:ssa luotiin valitun päivittämisratkaisun toteuttamiseksi uusia organisaatioyksiköitä (OU), jotta palvelimet saatiin kategorisoitua paremmin. Uusia organisaatioyksiköitä luotiin, jotta niille saatiin kohdennettua tarkemmin päivitysten toiminnan kannalta halutut ryhmäkäytäntöpolitiikat. Pohjantähden domainissa oli valmiina jo ennestään luotuna organisaatioyksikkö palvelimille. Tässä yksikössä sijaitsi kaikki yhtiön palvelimet, jotka olivat liitetty domainiin.

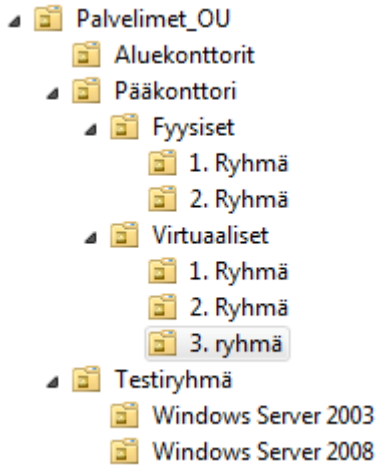
Organisaatioyksiköiden luominen tapahtui tietokoneella olevan Active Directory Users and Computers (ADUC) työkalun avulla. Organisaatioyksiköjen luomista varten pitää ohjelma käynnistää tunnuksella, jolla on tarvittavat oikeudet muokkauksien tekoon. Uusia organisaatioyksiköitä luotaessa otettiin huomioon valintaruutu, joka kysyy suojataanko organisaatioyksikkö poistamiselta. Tätä valintaa ei työssä otettu käyttöön. (Kuva 16.)



Kuva 16. Organisaatioyksikköä luotaessa ei organisaatioyksiköitä suojattu

Olemassa olevan Palvelimet_OU organisaatioyksikön sisään päätettiin luoda uusia organisaatioyksiköitä. Ensimmäisiksi alayksiköiksi luotiin ryhmät konttoreittain sekä lisäksi testiryhmä. Konttoreittain luomisella tarkoitetaan tässä tapauksessa jakoa kahteen, eli aluekonttoreihin ja pääkonttoriin. Aluekonttorit organisaatioyksikköön ei luotu alayksiköitä, sillä kyseiseen organisaatioyksikköön kuuluu vain kahdeksan palvelinta. Näiden palvelinten osalta suoritetaan mahdolliset lataukset, uudelleen käynnistykset ja muut samanaikaisesti.

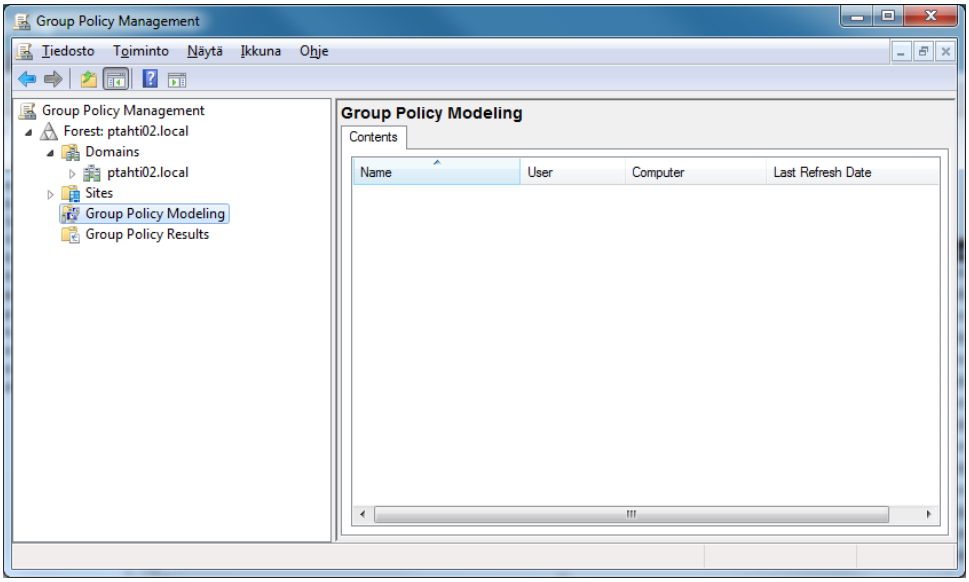
Organisaatioyksikkö, joka luotiin Pohjantähden pääkonttorin palvelimia varten, jaettiin kahteen alaorganisaatioyksikköön. Nämä yksiköt valittiin periaatteella, jossa palvelimet jaetaan joko virtuaalisiin tai fyysisiin palvelimin. Lisäksi pääkonttorin virtuaalisten palvelimien organisaatioyksikkö jaettiin vielä kolmeen alaorganisaatioyksikköön, jotta saadaan eroteltua palvelimen uudelleen käynnistykset entistä paremmin. Fyysisissä päädyttiin kahteen alayksikköön, sillä niiden osalta ei ole suurta pelkoa liiallisesta hetkellisestä kuormituksesta. (Kuva 17.)



Kuva 17. Työssä luotiin uudenlainen Active Directory hakemistorakenne

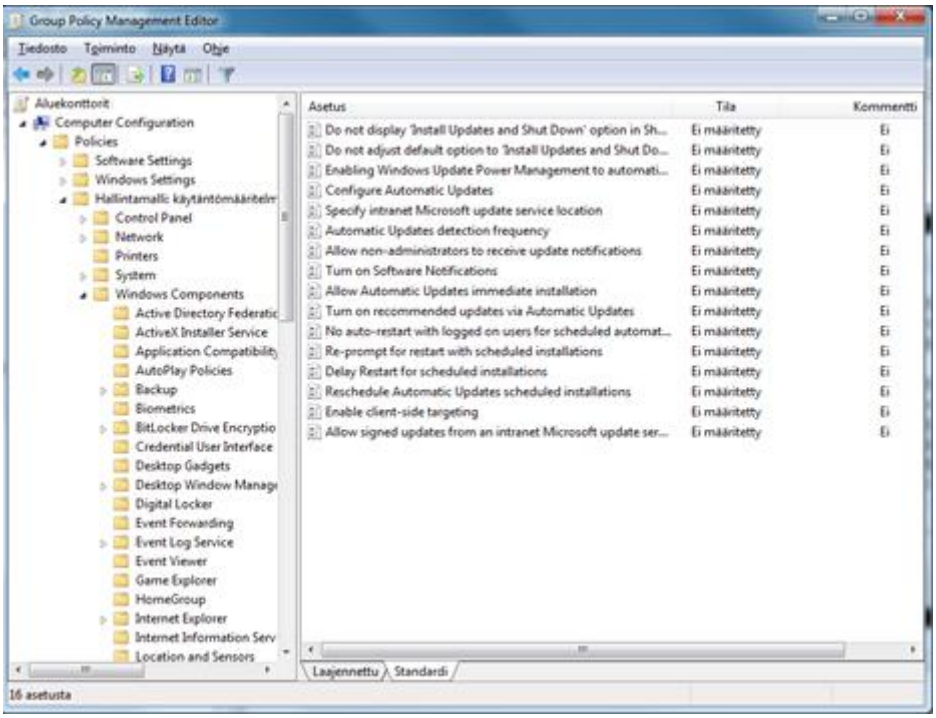
7.4.3 Ryhmäkäytäntöjen määritykset

Työssä muokattiin halutun lopputuloksen saamiseksi ryhmäkäytäntöjä, englanniksi Group Policy. Jotta muokkaaminen onnistui, tuli ladata Microsoftin sivuilta ryhmäkäytäntöjen hallintaa varten suunniteltu erillinen konsoli. Group Policy Management Console (GPMC) on oivallinen työkalu, jonka avulla ryhmäkäytäntöjä on helppo muokata ja luoda. (Kuva 18.) Työssä rakennettiin työkalun avulla kokonaan uusia ryhmäkäytäntöjä. Käytäntöjä luotiin jokaiselle uudelle organisaatioyksikölle, jotka työssä aikaisemmin oli tehty.



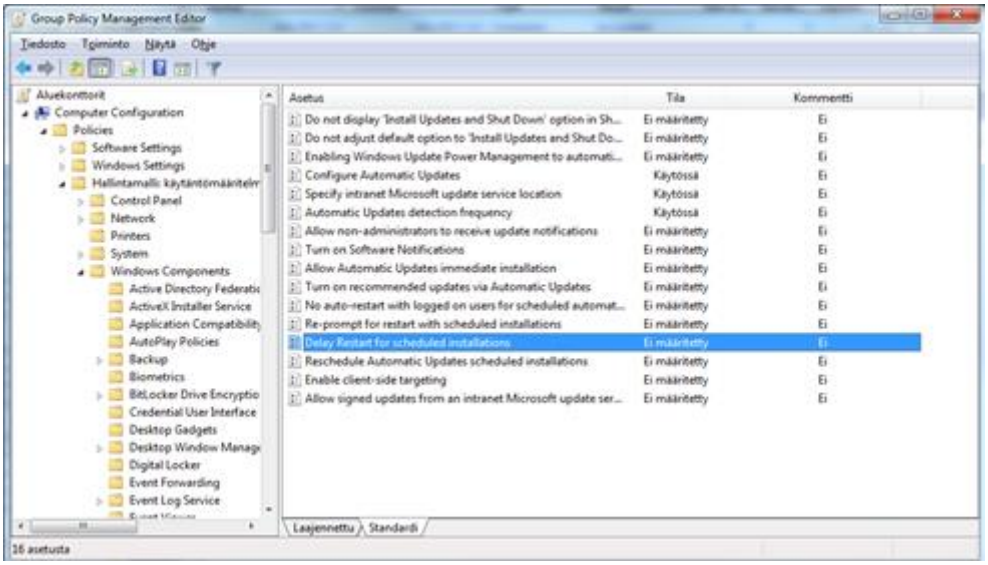
Kuva 18. GPMC eli ryhmäkäytäntöjen hallintakonsoli

Ryhmäkäytäntöjen luominen hallintakonsolin avulla osoittautui helposti lähestyttäväksi työksi. Luomista helpottivat tarkat määritykset ja tiedot siitä, miten määritysten halutaan toimivan. Ryhmäkäytäntöjen lisääminen ja muokkaaminen tapahtuu klikkaamalla hiiren oikealla GPMC konsolissa haluttua organisaatioyksikköä tai sen alayksikköä. Tämän jälkeen valitaan, halutaanko muokata tietokoneeseen vai käyttäjään liittyviä käytäntöjä. Tietokoneen ryhmäkäytäntöjen alta löytyy valikko, jolla voidaan määritellä hallintamalleja. Hallintamallien alta löytyy valikko, josta valitaan Windowsin osat. Windowsin osien alta löytyy Windows Update, jonka määrityksiä tässäkin työssä muokataan. (Kuva 19.)



Kuva 19. Windows Updaten muokkaamiseksi on tarjolla useita ryhmäkäytäntöjä

Uusia ryhmäkäytäntöjä luotiin kolme erilaista. Pienempiä eroja tehtiin myös uudelleen käynnistyksen viivästyttämiseksi, jotta palvelimien uudelleen käynnistykset tapahtuisivat järkevästi porrastaen. Ensimmäisenä luotiin ryhmäkäytäntö Pohjantähden aluekonttoreiden palvelimille, joita on kahdeksan kappaletta. Näiden palvelinten osalta ryhmäkäytännössä määritettiin palvelimille keskitetty automaattisten päivitysten asetus. Päivitykset asennetaan ryhmäkäytännön alaisille palvelimille joka maanantai kello 18:00. Uudelleen käynnistykset suoritetaan välittömästi sen jälkeen, kun päivitykset ovat palvelimille asentuneet. WSUS-palvelimen osoite tuli lisäksi määrittää ryhmäkäytäntöön, jotta palvelimet osaavat hakea halutut päivitykset oikeasta paikasta. Päivitysten tarkistusten sykliksi valittiin kuusi tuntia, alkuperäisen 22 tunnin sijaan. Uudelleen käynnistysten viivästyksiä ei määritelty. Kuvassa 20 näkyy tehdyt määritykset.



Kuva 20. Aluekonttoreiden ryhmäkäytännöt

Pääkonttoreiden ryhmäkäytäntöjen osalta käytäntö erottui hieman aluekonttoreiden ryhmäkäytännöistä. Pääkonttorit organisaatioyksiköllä on useampia alayksiköitä, minkä vuoksi jokaiselle tuli tehdä omat määrityksensä. Organisaatioyksiköt on jaettu siten, että toisen alaisuudessa ovat fyysiset palvelimet, jotka automatisoidaan, ja toisessa virtuaaliset. Virtuaalisten palvelimien organisaatioyksikön sisällä on lisäksi useampi ryhmä, jotta voidaan olla varmoja päällekkäisten ja ruuhkautettujen uudelleen käynnistysten välttämisestä. Fyysisiin palvelimiin tehtiin kaksi ryhmää, jotta aivan kaikki eivät tapahtuisi samanaikaisesti.

Fyysisille palvelimille luotiin kaksi ryhmäkäytäntöä, joista toisessa määriteltiin päivitys tapahtumaan kello 18:00 ja toisessa 20:00. Lisäksi määritettiin WSUS- palvelimen sijainti. Uusien päivitysten havaitsemisen sykliksi tuli tässä tapauksessa neljä tuntia, jotta voidaan olla täysin varmoja palvelimien havaitsevan jaetut päivitykset ennen haluttua asennusaikaa. Virtuaalisille palvelimille luotiin kolme ryhmää, joiden avulla porrastettiin päivitykset ja käynnistymiset tapahtumaan ryhmittäin tunnin välein 18:00 – 20:00.

7.5 Palvelinten seuranta

Työssä rakennettiin palvelinten päivitysten automatisointiratkaisun tueksi myös palvelinten seurantaratkaisu. On tärkeää, että automatisoitavien palvelimien osalta voidaan olla varmoja siitä, että päivitykset ovat onnistuneet. Palvelimien uudelleen käynnistymisistä tulee myös olla varmuus. Käynnistymättä jääneet palvelimet aiheuttavat loven yhtiön toimintaan, eikä se ole ratkaisun tarkoitus. Ratkaisua määriteltäessä oli Pohjantähden puolelta toiveena saada ratkaisu, jossa palvelimien tiedot lähetetään vastuuhenkilöille sähköpostilla. Sähköpostista tulisi käydä ilmi, ovatko palvelimet käynnistyneet uudelleen, ja palvelinkohtaisesti tieto, jos näin ei ole tapahtunut.

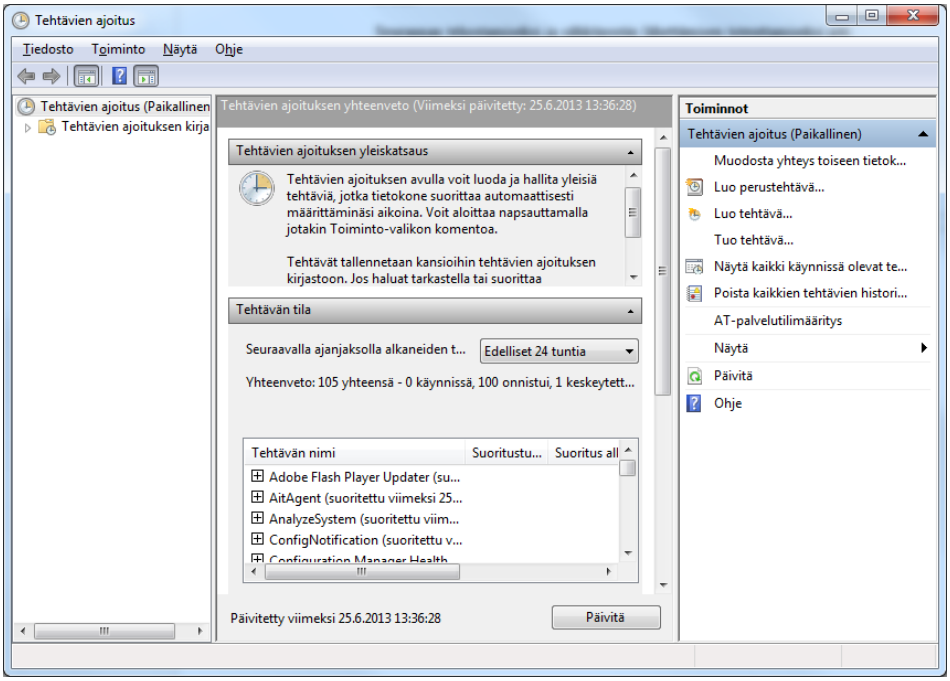
Palvelinten seurannan keskittämiseksi ja helpottamiseksi tutkittiin työssä erilaisia menetelmiä, joiden avulla saataisiin aikaan halutun kaltainen ratkaisu. Parhaimmin sopivaksi menetelmäksi todettiin lähdeteosten ja testikokemusten perusteella ajastetut komentojonot. Windowsiin sisäänrakennettujen komentojonojen avulla saadaan helposti saman toimialueen koneiden tietoja esiin. Ensimmäinen seurantaratkaisu toteutettiinkin komentotulkissa ajettavan ”systeminfo” komennon ympärille rakennetun komentojonon avulla (Liite 1.) Ratkaisussa haetaan erillisistä tekstitiedostosta palvelimet, joiden tiedot komento tarkistaa. Tarkistuksen jälkeen komentojono syöttää tiedot uuteen tekstitiedostoon. Ratkaisu on toimiva, mutta testauksessa se osoittautui hyvin aikaa vieväksi. Useiden kymmenien palvelimien kohdalla jokaisen palvelimen tarkkojen tietojen tutkiminen vei komentojonolta aikaa huomattavasti enemmän kuin työssä käsitelty toinen ratkaisu.

Toisena ratkaisuna työssä käytettiin Sysinternals Suite -paketista löytyvää PsInfo-työkalua. Sysinternals on Mark Russinovichin ja Bryan Cogswellin yhdessä luoma joukko työkaluja, joilla voidaan tehokkaasti hallita eri Windows-käyttöjärjestelmiä. Nykyisin Sysinternals on Microsoftin omistuksessa. PsInfo toimii hyvin samankaltaisesti kuin aikaisemmin mainittu systeminfo, mutta on rakenteeltaan selkeämpi. Sen avulla saadaan koneiden tietoja ottamalla etäyhteys niiden rekisteriin. Työssä rakennettiin komentojono, joka hyödyntää PsInfo- työkalua. (Liite 2.)

Komentojonon idea on hyvin samankaltainen kuin ensimmäisessä luodussa komentojonossa. Komentojono tarkistaa tiedostoon määritetyt koneet. Tämän jälkeen komentojono kirjoittaa koneista saadut tiedot ylös. Tästä tiedostosta käy ilmi aika, jonka tietokone on ollut käynnissä. Erityisesti tämä tieto helpottaa palvelinten käynnistysaikojen seurantaa. (Liite 3.) PsInfon avulla luotu ratkaisu osoittautui testauksen yhteydessä huomattavasti selkeämmäksi ja nopeammaksi ratkaisuksi, joten palvelinten seuranta päätettiin toteuttaa sen avulla.

7.5.1 Seurannan ajoitus

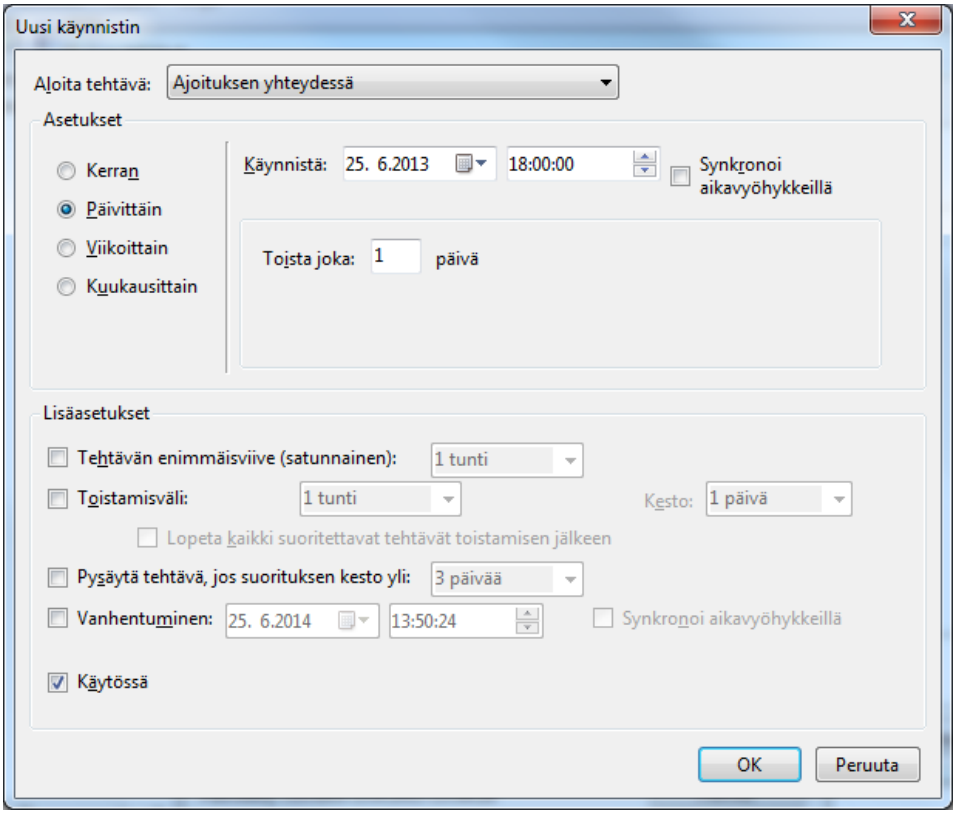
Seurannan tehostamiseksi piti lisäksi luoda ratkaisu, joka ajaisi luodun palvelinten seurantaa helpottavan komentojonon ajastetusti, ja lähettäisi sen tiedot sähköpostitse eteenpäin. Tämänkaltainen ratkaisu päätettiin toteuttaa Windows-käyttöjärjestelmään integroidun tehtävien ajastus -työkalun avulla. Työkalun avulla on mahdollista määrittää tietokone suorittamaan tietty ohjelma tai komentojono haluttuna ajankohtana tai jonkin tapahtuman sattuessa. Tapahtumia ovat esimerkiksi koneen käynnistyminen ja sammuminen. (Kuva 21.) Työssä halutun lopputuloksen kannalta valittiin halutun ajankohdan mukaan suoritettavaksi aikaisemmin luotu komentojono.



Kuva 21. Tehtävien ajoitus -työkalu tarjoaa useita automatisointia helpottavia vaihtoehtoja

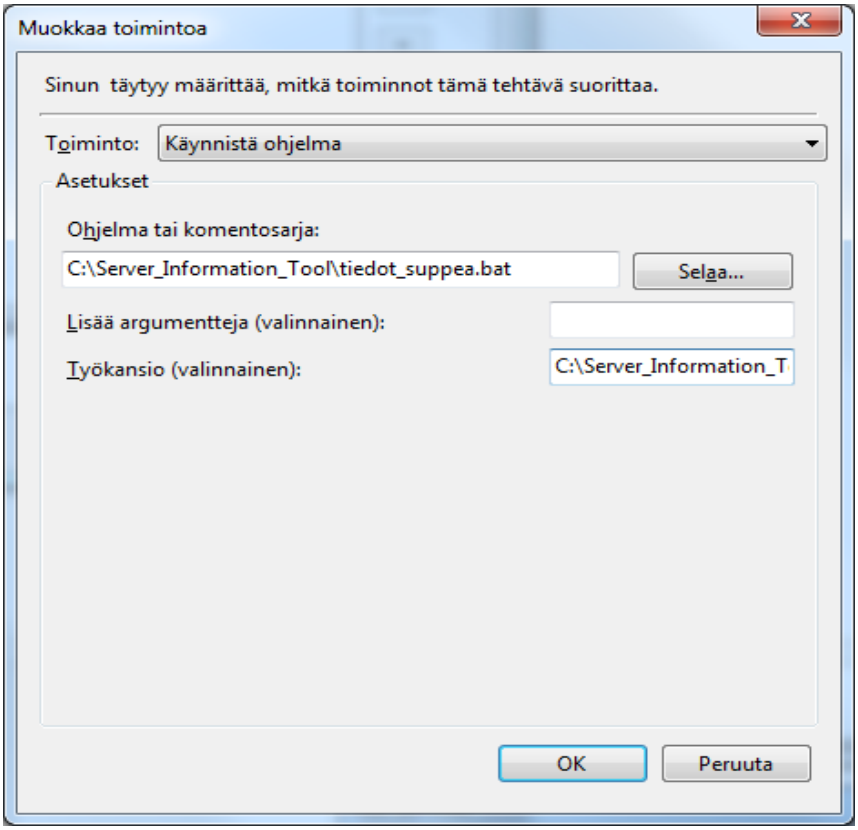
Ajastetun tehtävän luominen työkalun avulla vaatii osaltaan muutamia määrityksiä. Näistä ensimmäisenä uuden tehtävän luomisen yhteydessä määriteltiin tehtävälle haluttu nimi. Nimen lisäksi lisättiin lyhyt kuvaus, mitä ajastettu tehtävä pitää sisällään. Tämän jälkeen valittiin käyttäjätunnus, jolla ajastettu tehtävä suoritetaan. Tunnuksella tulee olla tarvittava määrä oikeuksia, jotta kaikkien valittujen toimintojen osalta voidaan olla varmoja niiden toiminnasta. Työssä valittiin käytettäväksi tunnukseksi opinnäytetyön tekijän käytössä ollut pääkäyttäjätason oikeuksilla varustettu tunnus. Lisäksi määriteltiin, että kyseinen tehtävä voidaan suorittaa ilman että käyttäjätunnuksen tarvitsee olla kirjautuneena.

Yleisten määritysten jälkeen valittiin käynnistimet, joita tässä tapauksessa on vain yksi. Käynnistimellä tarkoitetaan niitä ehtoja, joiden täyttyessä haluttu tehtävä suoritetaan. Käynnistimeksi valittiin ajankohdan mukainen käynnistys. Ajankohta on mahdollista määrittää useiden eri vaihtoehtojen joukosta mieleisekseen. (Kuva 22.) Ajastetun tehtävän vähäisen kuormittavuuden vuoksi päädyttiin ratkaisuun, jossa palvelinten tiedot tarkistava komentojono ajetaan päivittäin kello 17:00 sekä 20:40. Nämä ajankohdat siksi, että 17:00 ajettava komentojono kirjoittaa ylös tiedot palvelinten tilasta ennen päivityksiä, ja 20:40 ajettava komentojono päivitysten jälkeen. Näitä vertaamalla saadaan selville, että kaikki sujui kuten pitikin ja mahdolliset ongelmalliset palvelimet osataan havaita ja virheet korjata.



Kuva 22. Työssä käytettiin ajastettuja tehtäviä haluttujen määritysten aikaansaamiseksi

Halutun ajankohdan valitsemisen jälkeen määritettiin tehtävien ajoitukseen haluttu komentojono. Toiminnoksi valittiin ohjelman käynnistäminen. Käynnistettävä komentojono lisätään kenttään, minkä jälkeen tulee määrittää työkansioksi se kansio, jossa itse komentojono sijaitsee. Argumentteja ei tässä tapauksessa lisätty. (Kuva 23.)



Kuva 23. Komentojonon käynnistäminen onnistuu tehtävien ajoituksen avulla

Näiden määritysten jälkeen on lisäksi mahdollista määrittää ehtoja ja tarkempia asetuksia. Näitä ehtoja ja asetuksia ei tämän tehtävien ajoituksen toiminnan kannalta nähty oleelliseksi muuttaa. Kun luotu ajoitettu tehtävä on valmis, ilmestyy se tehtävien ajoitus -työkalussa olevaan listaan. Tästä listasta on mahdollista kokeilla, toimiiko luotu tehtävä. Testaaminen onnistuu klikkaamalla hiiren oikealla haluttua tehtävää ja klikkaamalla se käyntiin.

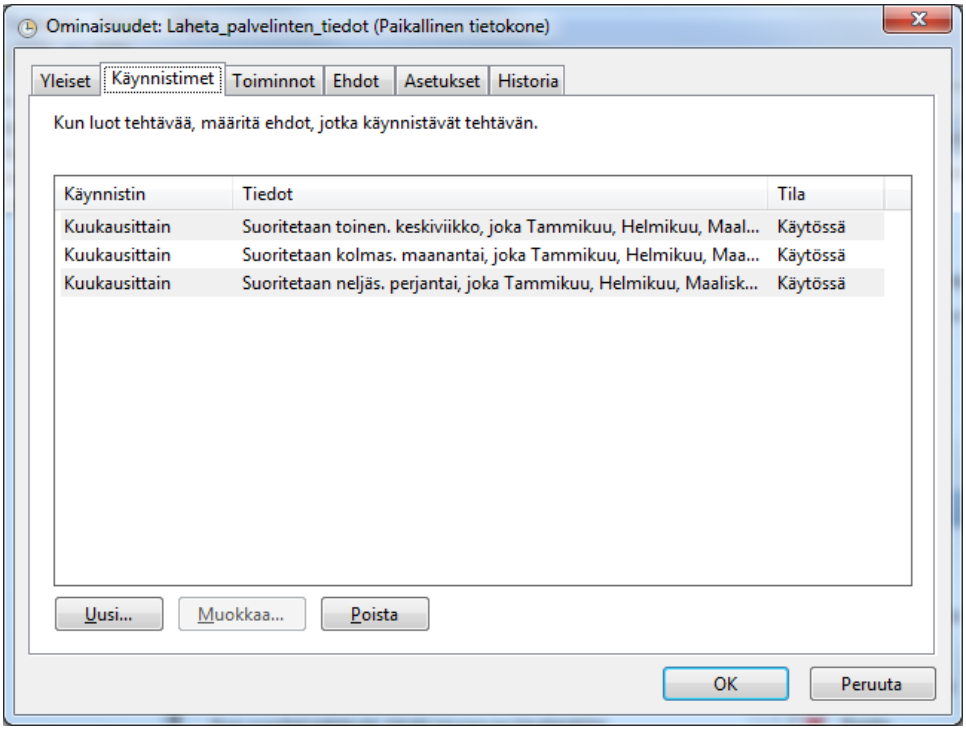
7.5.2 Sähköpostin lähetys

Palvelinten seurannan osalta oli työn toimeksiantajan taholta toiveena, että palvelinten käynnistymisiä ja muita tietoja voitaisiin seurata kattavasti. Tähän pyrittiin ratkaisulla, joka lähettää palvelimista tietoja haluttuun sähköpostiosoitteeseen. Tämänkaltainen ratkaisu todettiin onnistuvaksi samaisen tehtävien ajoitus -työkalun avulla, jolla myös palvelinten tietoja keräävä komentojono ajetaan. Näiden kahden tehtävän yksinkertainen ja käyttäjäystävällinen suorittaminen saman työkalun avulla oli omiaan vahvistamaan päätöstä siitä, että palvelinten seurantaratkaisua pohdittaessa päädyttiin Windowsin tarjoamaan tehtävien ajoitukseen.

Sähköpostin lähettämisen määrittäminen tehtävien ajoitus -työkalussa tapahtuu hyvin samankaltaisesti kuin ajastetun tehtävänkin määrittäminen. Ensimmäisenä annetaan tehtävälle nimi ja kuvaus, mitä tehtävällä pyritään

saavuttamaan. Tämän jälkeen valitaan käyttäjätunnus, jolla tehtävä suoritetaan. Käyttäjätunnukseksi valittiin sama pääkäyttäjätason tunnus, jota jo aikaisemmassa ajastetussa tehtävässä käytettiin.

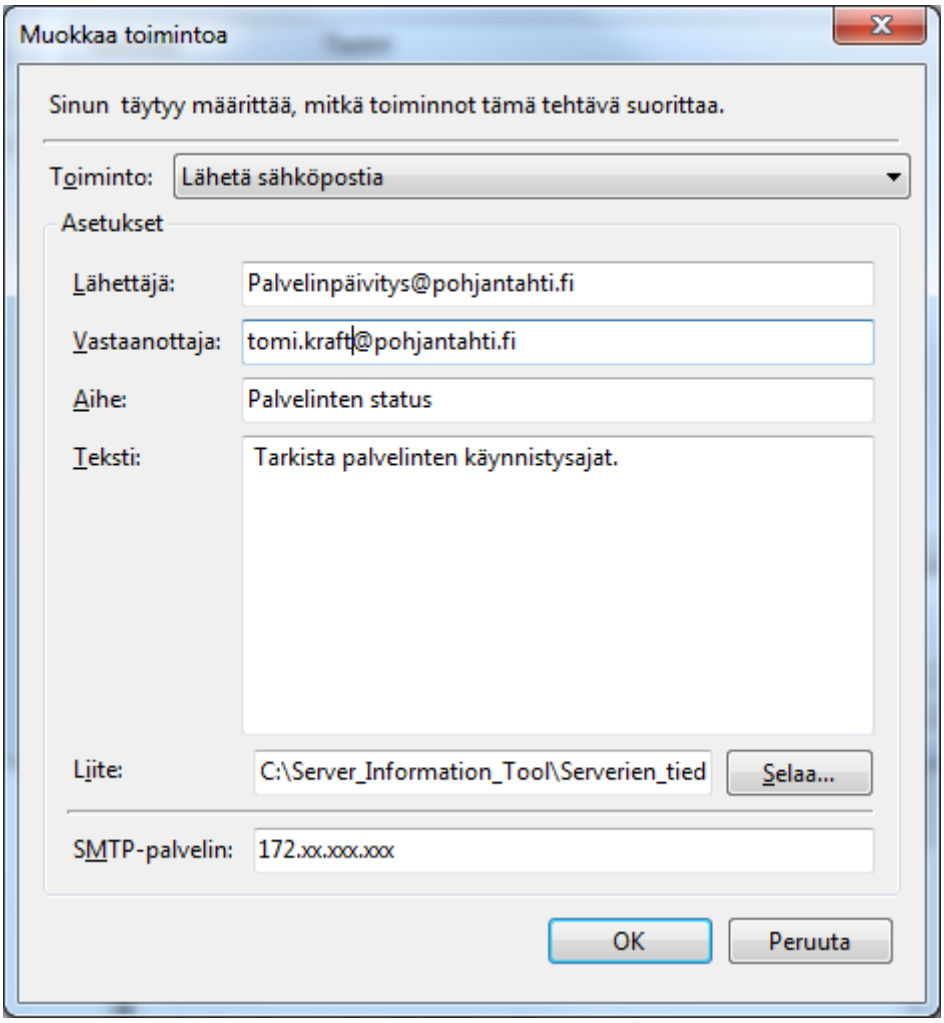
Käynnistimeksi päätettiin tässä tapauksessa valita myöskin ajoitetut käynnistimet. Sähköpostin lähetys tapahtuu kuukausittain. Lähetyspäiviä ovat joka kuukauden toinen keskiviikko, kolmas maanantai ja neljäs perjantai. Näistä keskiviikko on seuraava arkipäivä päivitysten julkaisusta. Joka kuukauden toisena keskiviikkona saadaan täten tieto testiryhmän päivitysten onnistumisista ja palvelinten uudelleen käynnistymisistä. Toinen tärkeä sähköpostin lähetyspäivä on joka kuukauden kolmas maanantai, jolloin saadaan sähköpostitse tieto tuotantopalvelimien osalta päivitysten ja käynnistymisten onnistumisesta. Lisäksi suoritetaan joka kuukauden neljäs perjantai sama sähköpostin lähetys, joka tarjoaa tietoa palvelimista. Sähköposteja lähtee aina päivityspäivisin kaksi kappaletta. Ensin 17:30 lähetetään tieto palvelinten statuksesta ennen päivityksiä. Seuraava sähköposti saapuu 20:55, ja siitä käyvät ilmi uudet päivittyneet tiedot käynnissäoloajan osalta. (Kuva 24.)



Kuva 24. Sähköpostin lähettämisessä on käytetty useita käynnistimiä

Käynnistimien määritysten jälkeen tuli määritellä itse toiminto, eli sähköpostin lähettäminen. Sähköpostin lähettämisen määrittäminen on yksinkertaista, kunhan on tiedossa käytettävän SMTP-palvelimen osoite. Tässä työssä käytettiin Pohjantähden SMTP-palvelinta. Toiminnoissa tuli määritellä haluttu toiminto, joka valittiin valmiiden vaihtoehtojen joukosta sähköpostin lähettämiseksi. Täten ei tarvitse sähköpostia lähettää erillisten komentojonojen avulla. Seuraavaksi tuli valita lähettäjän sähköpostiosoite.

Osoitteeksi valittiin tätä tarkoitusta varten luotu palvelinpäivitys@pohjantahti.fi. Vastaanottajaksi määritettiin palvelimien päivittämisestä vastaavat henkilöt. Tärkein asia tässä tapauksessa sähköpostin lähetyksen määrityksissä on liitteeksi määritelty tiedosto. Tiedosto on sama, jonka aikaisemmin tässä työssä käsitelty palvelinten seurantaan suunniteltu komentojono tuottaa. Tästä tiedostosta käy ilmi palvelimien käynnistymisajat ja muuta tärkeää tietoa. Lisäksi määriteltiin Pohjantähden SMTP-palvelimen osoite, jotta sähköposti löytää perille. (Kuva 25.)



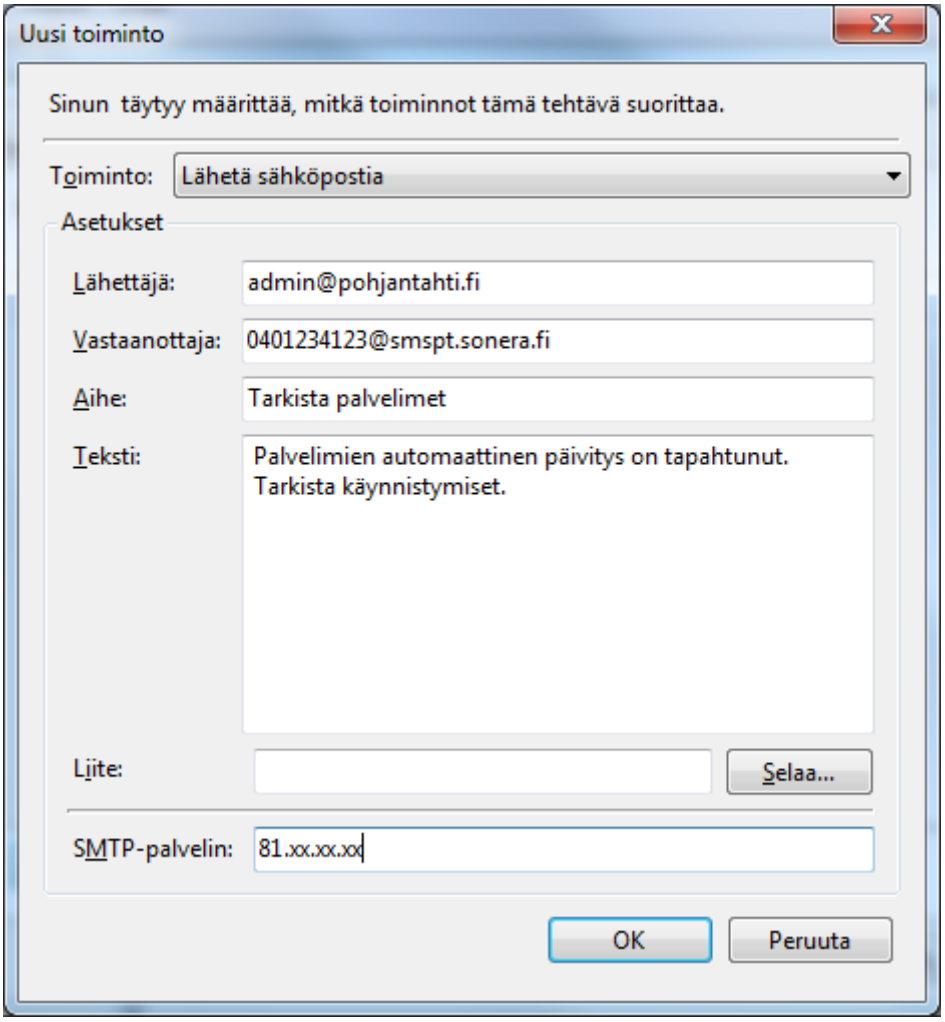
Kuva 25. Työssä käytetyt sähköpostin lähetystä varten luodut määritykset

7.5.3 Tekstiviestin lähetys

Sähköpostin lisäksi päätettiin toteuttaa ratkaisu, joka lähettää tekstiviestin välityksellä muistutuksen, että palvelimien automaattinen päivittäminen on tapahtunut. Viesti lähetetään vastuuhenkilölle, joka sen johdosta muistaa tarkistaa palvelinten tilan. Tekstiviestin lähetys tapahtuu kuten edellä mainittu sähköpostin lähettäminenkin. Ainoastaan pienet muutokset ovat tarpeellisia.

Tekstiviestin lähetystä määrittäessä luotiin uusi ajastettu tehtävä, joka nimettiin kuvaavasti. Käyttöoikeuksien osalta käytettiin edelleen samaa käyttäjätunnusta kuin aikaisemmissakin määrityksissä. Käynnistimiksi määritettiin samat käynnistimet, kuin sähköpostinkin osalta. Ainoana erona se, että joka kuukauden neljäntenä perjantaina lähtevän sähköpostin kanssa samaan aikaan ei määritelty tekstiviestiä. Tekstiviestin lähetykselle annettiin siis käynnistimiksi joka kuukauden toinen keskiviikko sekä kolmas maanantai. Kellonajaksi valittiin kello 20:55, sillä päivitykset ovat siihen mennessä tapahtuneet.

Suurimpana eroavaisuutena pelkän sähköpostin lähettämiseen on tekstiviestin lähettämisessä se, että vastaanottajaksi tulee määritellä haluttu puhelinnumero. Lisäksi SMTP-palvelin on eri kuin normaalisissa tapauksessa. Tässä skenaariossa viesti kiertää Soneran kautta, jonka jälkeen se tulee määriteltyyn puhelinnumeroon tekstiviestinä. (Kuva 26.)



Kuva 26. Tekstiviestin lähettämisen määritykset eroavat hieman sähköpostin määrityksistä

8 YHTEENVETO

Opinnäytetyön tarkoituksena oli tehostaa Pohjantähden Windows-palvelinympäristön ylläpitoa ja tietoturvatason ylläpitoa. Tehostamisratkaisuna käytettiin palvelinten tietoturvapäivitysten osittaista automatisointia. Työssä päädyttiin ratkaisuun, joissa herkimpiä ja tuotannon kannalta välttämättömimpiä palvelimia lukuun ottamatta kaikki yhtiön käytössä olevat Windows-palvelimet automatisoitiin tietoturvapäivitysten osalta.

Automatisoinnin toteuttamiseksi luotiin ratkaisu, jossa palvelimet saavat keskitetysti jaellut päivitykset tietoonsa kuukausittain päivitysten julkaisun jälkeisenä ajankohtana. Testiryhmään kuuluville palvelimille päivitykset jaellaan aikaisemmin, jotta saadaan luotettua tietoa päivitysten toimivuudesta. Automatisoinnin piiriin määritetyt palvelimet suorittavat päivitysten asentamisen ja tarvittavat uudelleenkäynnistymiset erikseen määritetyn huoltoikkunan aikana.

Automatisoinnin lisäksi työssä rakennettiin seurantaratkaisu, jolla toteutetaan tietoa palvelinten tilasta niin sähköpostitse kuin tekstiviestitsekin. Ratkaisut toteutettiin Pohjantähden tietohallinnolla jo käytössä olevien menetelmien ja järjestelmien avulla. Automatisoinnin aikaansaamiseksi käytettiin apuna Windows Server Update Services -ohjelmistoa sekä Windows-ympäristöstä löytyviä ryhmäkäytäntöjä. Valittujen menetelmien avulla saatiin aikaan lisenssikohtaisia säästöjä, ominaisuuksien kuitenkin pysyessä riittävän kattavina. Sähköpostin ja tekstiviestien lähettämisessä käytettiin Windowsin sisäänrakennettua tehtävien ajoitus -toimintoa sekä Pohjantähden SMTP-palvelinta.

Työssä tehtiin havaintoja Pohjantähden palvelinympäristön kehittämisen kannalta. Jatkokehitys tehtiin mahdollisimman yksinkertaiseksi. Osana jatkokehityksen helpottamista luotiin uusia hakemistorakenteita sekä lisättiin uusia organisaatioyksiköitä. Tehtyä ratkaisua on helppo muokata palvelinympäristön uusiutuessa. Virtualisoinnin lisääminen ja uudemmat käyttöjärjestelmät on otettu huomioon joustavuutta ja muokattavuutta suunniteltaessa.

Työn lopputuloksena oli Pohjantähden palvelinympäristön hallinnan tehokkuutta lisäävä ratkaisu. Palvelimien päivittäminen saa jatkossa osakseen huomiota, jota se herkkyytensä puolesta kaipaa. Päivityksille määriteltiin kiinteät ajankohdat sekä seurantaratkaisut, joiden avulla päivittämistä on helppo seurata ja toteuttaa. Työn avulla aikaansaatiin parannuksia Pohjantähden tietoturvatasoon sekä palvelimien toimintavarmuuteen ja sen seurantaan.

LÄHTEET

Amaris, C., Morimoto, R., Handley, P. & Ross, D. 2012. Microsoft System Center 2012 Unleashed.

Brinkmann, M. 2010. Microsoft Windows Update Overview, All You Need To Know.
http://www.ghacks.net/2010/12/20/microsoft-windows-update-overview-all-you-need-to-know/
Viitattu 20.5.2013.

Budd, C. 2006. Ten Principles of Microsoft Patch Management.
http://technet.microsoft.com/library/cc512589.aspx
Viitattu 21.5.2013.

Fisher, T. n.d. How To Fix Problems Caused by Windows Updates.
http://pcsupport.about.com/od/system-security/a/fix-problems-caused-by-windows-updates.htm
Viitattu 23.5.2013.

Griffin, D. 2012. Patch Management on Business-Critical Servers.
http://technet.microsoft.com/en-us/security/hh778967.aspx
Viitattu 21.5.2013

Helenius, M. 2003. Varmistukset ja palautukset. Oppimateriaali. Tietojenkäsittelytieteen laitos. Tampereen yliopisto.

Hornbeck, J.C. 2012. An update for Windows Server Update Services 3.0 Service Pack 2 is available (KB2734608)
http://blogs.technet.com/b/sus/archive/2012/09/04/an-update-for-windows-server-update-services-3-0-service-pack-2-is-available-kb2734608.aspx
Viitattu 21.5.2013.

Keizer, G. 2011. TechWorld: Microsoft ready to patch critical Windows Server vulnerability.
http://news.techworld.com/operating-systems/3278043/microsoft-to-patch-critical-windows-server-vulnerability/
Viitattu 20.5.2013.

Koskinen, J. 2002. Tietoturvallisuuden perusteet.
http://www.cs.tut.fi/~8306000/fy.html
Viitattu 22.5.2013.

Kotilainen, S. 2005. Pc:n varmistusohjelmat.
http://www.tietokone.fi/lehti/tietokone_11_2005/pc_n_varmistusohjelmat_2210
Viitattu 23.5.2013.

Laakso, M. 2010. PK-yrityksen tietoturvasuunnitelman laatiminen. Turun ammattikorkeakoulu. Tietojenkäsittelyn koulutusohjelma. Opinnäytetyö.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja – ohjeistus, toteutus, käytäntö.

LeBlanc, B. 2011. Announcing availability of Windows 7 and Windows server 2008 R2 SP1.
http://blogs.windows.com/windows/b/bloggingwindows/archive/2011/02/09/announcing-availability-of-windows-7-and-windows-server-2008-r2-sp1.aspx
Viitattu 21.5.2013.

Leffall, J. 2007. Are Patches Leading to Exploits?
http://redmondmag.com/articles/2007/10/12/are-patches-leading-to-exploits.aspx
Viitattu 20.5.2013.

Lemos, R. 2003. Microsoft details new security plan. 9.10.2003.
http://news.cnet.com/Microsoft-details-new-security-plan/2100-1002_3-5088846.html
Viitattu 5.6.2013.

Microsoft elinkaarituki.
http://support.microsoft.com/lifecycle/search/default.aspx?sort=PN&alpha=Windows+Server+2008+R2
Viitattu 21.5.2013

Moilanen, A. 2012. Microsoft System Center 2012 Configuration Manager – Käyttöönottosuunnitelma ja testimigraatio. Metropolia ammattikorkeakoulu. Tietotekniikan koulutusohjelma. Insinöörityö.

Neumann, B. 2006. .NET Framework 1.1 Servicing Releases on Windows Update for 64-bit Systems.
http://blogs.technet.com/b/blairn/archive/2006/03/28/netfx1164annc.aspx
Viitattu 20.5.2013.

Nilsson, J. 2012. Top 11 reasons why you should use ConfigMgr 2012 for managing Software Updates.
http://ccmexec.com/2012/08/top-11-reasons-why-you-should-use-configmgr-2012-for-managing-software-updates/
Viitattu 22.5.2013.

Parasuraman, R. & Riley, V. 1997. Humans and Automation: Use, Misuse, Disuse, Abuse.
http://stuff.mit.edu:8001/afs/athena/course/16/16.459/www/parasuraman.pdf

Pohjantähti – SCCM 2012 ympäristön suunnittelu ja käyttöönotto. 2013. Pohjantähti Keskinäinen Vakuutusyhtiö. Pintra. [intranet]
Viitattu 21.5.2013.

Pohjantähti Tietoturvaperiaatteet. 2011. Pohjantähti Keskinäinen Vakuutusyhtiö. Pintra. [intranet].Viitattu 17.5.2013.

Päivittämättömät ohjelmistot nopeasti kasvava uhka liiketoiminnalle. F-Secure.
http://www.f-secure.com/fi/web/home_fi/news-info/product-news-offers/view/story/915554/P%C3%A4ivitt%C3%A4m%C3%A4tt%C3%B6m%C3%A4t%20ohjelmistot%20nopeasti%20kasvava%20uhka%20liiketoiminnalle
Viitattu 21.5.2013.

Rosato, R. n.d. Best Practices for Applying Service Packs, Hotfixes and Security Patches.
http://technet.microsoft.com/en-us/library/cc750077.aspx
Viitattu 22.5.2013.

Rosendahl, M. n.d. Tietoturva palvelee kaikkia. http://www.helsinki.fi/atk/lehdet/103/Tietoturva%20palvelee%20kaikkia.html
Viitattu 22.5.2013.

Shields, G. 2011. Best Practices in Architecting and Implementing Windows Server Update Services. Microsoft Teched. PowerPoint.
Viitattu 28.5.2013.

Stanek, W. 2012. Windows Server 2012 : Pocket Consultant.

Suomalainen, J. 2013. www-sovelluspalveluiden integraatiotestien automatisointi. Metropolia ammattikorkeakoulu. Tietotekniikan koulutusohjelma. Insinöörityö.

Sutinen, P. 2013. Vieläkö teillä nyplätään IT-käsitöitä? 14.2.2013.
http://www.talouselama.fi/kumppaniblogit/tieto/vielako+teilla+nyplataan+itkasitoita/a2169191
Viitattu 28.5.2013.

System Center 2012 Licensing Pricing and SKU Overview. 2011. Microsoft.
https://partner.microsoft.com/download/HK/40179089
Viitattu 22.5.2013.

Technet. 2013. Planning for Software Updates Server Settings.
http://technet.microsoft.com/en-us/library/bb693485.aspx

Troy, R. & Helmke, M. 2010. Vmware Cookbook.

Vehviläinen, T. 2013. Puhutaanko taas atk:sta? 15.5.2013.
http://www.tietoviikko.fi/viisaat/tieturi/puhutaanko+taas+atksta/a901612
Viitattu 28.5.2013.

Vizard, M. 2011. The Benefits Versus Risks of IT Automation 3.10.2011.
http://www.itbusinessedge.com/cm/blogs/vizard/the-benefits-versus-risks-of-it-automation/?cs=48745
Viitattu 28.5.2013.

Vuokko, J. 2012. Lisätehokkuutta it-palveluprosessiin automatisoinnilla. http://www.tietoviikko.fi/cio/artikkelit/parhaat_kaytannot/lisatehokkuutta+itpalveluprosessien+automatisoinnilla/a828900
Viitattu 21.5.2013.

Windows Update Explained. 2008. http://download.microsoft.com/download/a/9/4/a94af289-a798-4143-a3f8-77004f7c2fd3/Windows%20Update%20Explained.docx
Viitattu 17.5.2013.

Windows Server Update Services. 2013.
http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx
Viitattu 21.5.2013.

Zinman, A. 2004. Group Policy Management Console (GPMC)
http://www.windowsecurity.com/articles-tutorials/misc_network_security/Group-Policy-Management-Console.html
Viitattu 5.6.2013.

SYSTEMINFO Liite 1

```
@ECHO OFF
echo **********Ladataan palvelinten tietoja**********

for /f "delims=" %%a in (koneet.txt) do (
systeminfo /s %%a /u asentaja /p asentaja1234 >> C:\ServeriTiedot1.txt
)

findstr /C:"Is„nt„nimi:" /C:"K„ytt”j„rjestelm„:" /C:"K„ytt”j„rjestelm„n valmistaja:"
/C:"J„rjestelm„n k„ynnistysaika:" /C:"J„rjestelm„n valmistaja:" /C:"J„rjestelm„n malli:"
/C:"Ensiasennusp„iv„:" C:\ServeriTiedot1.txt > c:\ServeriTiedot.doc

DEL C:\ServeriTiedot1.txt

c:\ServeriTiedot.doc
EXIT
```

PSINFO Liite 2

```
del logi.txt

echo ALKUAIKA >> logi.txt
time /T >> logi.txt

echo ---------- TESTIRYHMAN PALVELIMET ---------- >>logi.txt

echo PALVELIN1 >> logi.txt
psinfo \\palvelin1 -d | find "Uptime" >> logi.txt

echo PALVELIN2 >> logi.txt
psinfo \\palvelin2 -d | find "Uptime" >> logi.txt

echo LOPPUAIKA >>logi.txt
time /T >>logi.txt
```

LOGI.TXT Liite 3

ALKUAIKA
08:12
---------- TESTIRYHMAN PALVELIMET ----------
PALVELIN1
Uptime: 21 days 13 hours 41 minutes 41 seconds
PALVELIN2
Uptime: 7 days 16 hours 13 minutes 46 seconds
LOPPUAIKA
08:13