SYSTEM CENTER CONFIGURATION MANAGER -TOIMINNAN AUTOMATISOINTI JA TEHOSTAMINEN

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Hämeenlinna, kevät 2018

Niko Luodonpää

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Hämeenlinna

Tekijä Niko Luodonpää **Vuosi** 2018

Työn nimi System Center Configuration Manager -toiminnan automatisointi ja tehostaminen

Työn ohjaaja/t Lasse Seppänen

TIIVISTELMÄ

Opinnäytetyö käsittelee työasemahallintaympäristön toiminnan automatisointia ja tehostamista. Käytettävänä hallintatuotteena on Microsoftin System Center Configuration Manager. Käytettävän tuotteen määritteli opinnäytetyön tilaaja Hämeen ammattikorkeakoulu. Tilaajan tavoitteena oli saada mahdollisimman kustannustehokas ympäristö, joka palvelee joustavasti käyttäjiä. Korkeakoulun säästöpaineiden sekä tietotekniikan monimuotoistumisen seurauksena lisääntynyt työmäärä vaati työaikasäästöjä taustapalveluista.

Työssä käydään asioita läpi enemmän toiminnallisuuden kannalta, mutta myös teknistä näkökulmaa on otettu huomioon. Päätelaitehallintaympäristö suunniteltiin mahdollisimman tehokkaaksi, toimintavarmaksi ja automatisoinnin mahdollistavaksi. Tavoitteena oli parantaa ympäristön tavanomaista toimintaa eri menetelmin sekä hankkia siitä lisäarvoa. Lisäarvoa saatiin muun muassa mahdollistamalla loppukäyttäjille itsepalvelua ja hyödyntämällä ympäristön dataa uudella tavalla.

Työasemaympäristöstä saatiin toimintavarma kokonaisuus, jossa suurin osa ongelmista korjaantuu automaattisesti käyttäjiä juurikaan häiritsemättä. Käyttäjille pystyttiin tarjoamaan joustavuutta tietoturvaa vaarantamatta. Ympäristön toiminnasta syntyvästä datasta saatiin luotua lisäarvoa sekä rahallista säästöä laajentamalla ja rikastamalla sitä. Työmäärällisesti merkittäviä säästöjä saatiin työasemahallinnan asiantuntijoille sekä lähitukihenkilöille.

Avainsanat Työasemahallinta, SCCM, toimistoautomaatio, Windows

Sivut 38 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree programme in Business Information Technology
Hämeenlinna

Author Niko Luodonpää **Year** 2018

Subject Automation and Enhancement of System Center Configuration Manager

Supervisor Lasse Seppänen

ABSTRACT

This Bachelor's thesis deals with the automation and enhancement of the workstation management environment. The used management product is the Microsoft System Center Configuration Manager. The subscriber of the thesis, Häme University of Applied Sciences, defined the product to be used. The goal of the subscriber was to get as cost-effective environment as possible that is flexible for the users. Because of the increased workload caused by IT industry diversification and the university's saving needs, there was a need to get workload savings from background services.

The thesis studies the matter mostly in terms of functionality, but the technical aspect has also been taken into account. The workstation management environment was designed to be as efficient, robust and automated as possible. The aim was to improve normal performance of the environment and acquire added value from it. Extra benefit was achieved by enabling end-users self-service possibilities and by utilizing environmental data in a new way.

As a result, the thesis managed to get mostly self-healing and reliable workstation environment with minimal user interrupts. For users flexibility was offered without compromising security. The added value from environmental data and financial savings was gained by expanding and enriching the existing data. Significant savings to workload were obtained for workstation management specialist and for onsite support persons.

Keywords Desktop management, SCCM, automation, Windows

Pages 38 pages

SISÄLLYS

1 JOHDANTO

Hämeen ammattikorkeakoulu on siirtynyt käyttämään Microsoft System Center Configuration Manager (SCCM) työasemien hallintajärjestelmää. Projektia lähdettiin tekemään tyhjältä pöydältä, jolloin pystyttiin vapaasti suunnittelemaan ympäristö ja käytännöt. Aiemmin käytössä olleeseen järjestelmään verrattuna SCCM:n tapa tehdä muutoksia on hitaampi. Aikaisempi järjestelmä käytti työasemamuutosten tekemiseen push-menetelmää. Tällöin palvelin työntää muutoksen työasemille heti kun määritys on niille kytketty. SCCM puolestaan käyttää pull-menetelmää, jossa järjestelmään kytketyt koneet tarkistavat aika ajoin palvelimelta asioiden ajantasaisuuden. Tämän vuoksi ei voida tarkalleen tietää, milloin tehdyt muutokset menevät kohdetyöasemalle. Työasemalla voi myös olla monenlaisia asioita, jotka estävät muutosten asentumista. Tällöin muutoksia voi kertyä paljon jonoon, mikä puolestaan voi aiheuttaa ohjelmien asennuksia käytön aikana, ja häiritä koneen käyttöä. Mikäli muutoksien asentumisen estää käytön aikana, muutokset eivät astu kaikilla koneilla ollenkaan voimaan. Myös muutoksien voimaantulo tällöin kestää tietoturvan tai tarpeen kannalta kohtuuttoman kauan. Lisäksi verkko saattaa ruuhkautua suurien asennusten ja päivitysten vuoksi. Windows vaatii toimiakseen uudelleenkäynnistyksiä tarvittaessa, ehjän WMI-rajapinnan sekä toimivat käytännöt, joilla koneita voidaan käskeä tarvittaessa.

Uuden työasemahallintajärjestelmän käyttöönoton yhteydessä myös työasematukihenkilöiden määrää vähennettiin. Näiden asioiden vuoksi on tarvetta kehittää ympäristön automatisointia, itsestään korjaantuvuutta, toimintavarmuutta, käytäntöjä, ja tarjota asiakkaille itsepalvelumahdollisuuksia. Tavoitteiden onnistuessa saadaan tietohallinnon työmäärää vähennettyä. Lisäksi asiakkaille voidaan tarjota lisäarvoa nopeammin ja varmemmin toimivilla tietokoneilla, tietoturvalla, nopeammin käyttöön saatavilla sovelluksilla ja itsepalvelumahdollisuuksilla. Opinnäytetyö on toiminnallinen opinnäytetyö, joka sisältää laboratorio, kenttä, tilastoanalyysi ja kvantitatiivista tutkimusta sekä avoimia haastatteluja.

Opinnäytetyön tarkoitus on vastata automatisointia, toimintavarmuutta ja käyttäjäkokemusta koskeviin tutkimuskysymyksiin.

- Miten työasemaympäristön toiminta saadaan automatisoitua mahdollisimman pitkälle?
- Miten uusien koneiden asennus automatisoidaan?
- Miten sovellusten asentaminen automatisoidaan?
- Miten työasemien toimivuus varmistetaan?
- Miten minimoidaan käyttäjälle kohdistuva haitta sovellusasennusten ja päivitysten yhteydessä?
- Mitä palveluita kannattaa ja voidaan tuottaa itsepalveluna, ja miten ne toteutetaan?

2 TYÖASEMAHALLINTA

Työasemahallintajärjestelmän tarkoitus on lisätä tuottavuutta ja tehokkuutta automatisoimalla työasemalle tehtäviä toimenpiteitä, jotka muuten hoidettaisiin käsityönä. Tällaisia toimenpiteitä ovat esimerkiksi työasemien asennus, sovellusten ja päivitysten jakelu, asetusten hallinta ja vianetsintä. Myös inventaarion ylläpito on osa työasemahallintajärjestelmän toimintaa. Kuvassa 1 näkyvän Gartnerin selvityksen mukaan Microsoft on johtava hallintajärjestelmän valmistaja. Gartner muistuttaa kuitenkin, että tuote täytyy valita ympäristön koon ja tarpeiden mukaan. (Gartner 2015.)

Kuva 1. Gartner Magic Quadrant -taulukko työasemahallintajärjestelmien asemasta (Gartner 2015).

Työasemahallinnalla voidaan tehostaa laitteiden käyttöä asentamalla ohjelmat ja päivitykset silloin, kun käyttäjä ei ole koneella. Sovellushankinnoista saadaan myös enemmän hyötyä, koska sovelluksia voidaan asentaa ja poistaa vaivattomasti tarpeen mukaan. Päätelaitehallinta pitää sisällään myös raportointia, jolla saadaan hallituista koneista esimerkiksi inventaario-, sovellus- ja laitteistotietoa.

Työasemahallinnalla on suuri merkitys työasemien tietoturvan kannalta. Työasemahallinnat pitävät sisällään päivitysten jakelun, tiedon asennetuista sovelluksista ja niiden versioista. Yleensä virustorjunta jaetaan työasemille työasemahallinnan kautta. Työasemahallinta koostuu useista palvelimista sekä työasemille asennettavasta client-sovelluksesta. (Microsoft 2015a.)

3 SCCM-YMPÄRISTÖN SUUNNITTELU

Hämeen ammattikorkeakoulun (HAMK) työasemahallinnan piirissä oli vuoden 2018 toukokuussa noin 2300 työasemaa, sekä lisäksi virtuaalisten VDI-koneiden mallikoneet. Korkeakoululla on paljon eri sovelluksia, ja koneiden sovelluskokoonpanot vaihtelevat luokittain. Sovellusten jakelupaketteja oli noin 1500 kappaletta, joissa varsinaisten sovellusten lisäksi oli paljon asetus-, päivitys- ja korjauspaketteja. Erillisiä sovelluksia ympäristössä oli noin 500 kappaletta. Sovellusjakeluita oli kytkettynä 2243 kappaletta. Sovellusjakelu muodostuu, kun sovelluksen jakelupaketti kytketään asentumaan jollekin koneryhmälle.

SCCM-ympäristö suunniteltiin tyhjältä pöydältä. Tilaajan toiveesta ympäristö suunniteltiin mahdollisimman kustannustehokkaaksi, toimintavarmaksi ja automaattiseksi. Käyttäjille haluttiin tarjota myös itsepalvelumahdollisuuksia. Automaatiota varten oli tarve suunnitella käytäntö, jolla oikeat jakelut kytkeytyvät koneille automaattisesti, jotta asennus, päivitys ja asetusjakeluita ei tarvitse erikseen kytkeä koneille.

Automaation kannalta pidettiin tärkeänä koneiden nimeämiskäytäntöä. Käytäntönä päätettiin käyttää neljätoistamerkkistä nimeämistapaa, jossa kaksi ensimmäistä merkkiä kertovat korkeakouluyksikön, seuraavat viisi merkkiä rakennuksen ja huonenumeron, kolme seuraavaa onko kyseessä kannettava vai pöytäkone ja monesko sellainen kyseisessä tilassa. Viimeisestä merkistä näkee, onko työasema opiskelija- vai henkilökuntakäytössä (esim. vi-c0350-p01-o). Viimeisenä merkkinä on käytetty myös -t-merkintää, joka tarkoittaa, että koneelle asennetaan vain pakolliset tietoturvapäivitykset. Nimeämistavalla pyrittiin saamaan aikaan automaattinen yksikkö-, rakennus-, tila- ja ryhmäkohtaisten sovellusten ja asetusten asentuminen pelkällä koneen nimeämisellä.

3.1 Ryhmät eli Collectionit

SCCM-Collectionit ovat työasemaryhmiä. Collectionin voi luoda staattiseksi, jolloin ryhmään kuuluu määrätyt koneet. Toinen tapa on luoda Collection sääntöjen avulla (Query rule). Säännöt voivat perustua lähes mihin tahansa SCCM-tietokannasta löytyvään tietoon. Koneet jotka täyttävät ehdot tulevat automaattisesti kyseisen ryhmän jäseneksi.

HAMKin ympäristössä suurin osa Collectioneista tehtiin työaseman nimeen pohjautuvilla säännöillä. Tällä tavalla saatiin ryhmäjäsenyydet päivittymään automaattisesti. Esimerkiksi sääntö ”VI-C0305-%-O” lisää ryhmään kaikki Visamäki yksikön C-talon 305 luokan opiskelijoiden käytössä olevat koneet. Taulukossa 1 on kuvattu Collectionit, joihin Vi-c0305-p01-o niminen työasema saa automaattisesti jäsenyyden.

Taulukko 1. Vi-c0305-p01-o nimisen koneen automaattiset Collection-jäsenyydet.

Collentionin nimi	*Sääntö*	*Kuvaus*
All-Student-Desktops	%-%-P%-O	Opiskelijapöytäkoneet
Staff-Student-All	%-O or %-H	Muut paitsi -t koneet
Student-All	%-O	Opiskelijakoneet
Vi-All	VI-%-O or VI-%-H	Visamäki-yksikön koneet
Vi-c0305-O	VI-C0305-%-O	Vi-c305-luokan koneet
Vi-C-Student	VI-C%-O	Visamäen C-talon koneet
Vi-Student	VI-%-O	Visamäen opiskelijakoneet

Vi-c0305-p01-o -työasema saa Collection-jäsenyyksiä muidenkin kriteerien perusteella. Koneelle tulee automaattisesti jäsenyys dell-devices, adobe-reader-dc, levytila vahissa, w10 1607 nimisiin Collectioneihin, sekä sisäänrakennettuihin SCCM-Collectioneihin kuten All Systems. Esimerkiksi vapaaseen kovalevytilaan perustuvaan levytila vahissa -Collectioniin kuuluu koneet, joiden C:-asemalla on sääntöön määritettyä vähemmän vapaata levytilaa jäljellä. Ryhmälle voidaan kytkeä toimintoja, jolloin ne suoritetaan automaattisesti, kun koneilla alkaa kiintolevytila olla vähissä. Ryhmästä voidaan myös listata nämä koneet, jolloin saadaan raportti koneista, joiden kiintolevytila on vähissä.

3.2 **Automaation vaatimat lähiverkon muutokset**

Configuration Manager vaatii toimiakseen paljon porttiavauksia lähiverkkoon ja virtuaaliverkkojen (VLAN) yli. Microsoft on listannut TechNet sivustolle SCCM:n tarvitsemat porttien avaukset (Microsoft 2015b).

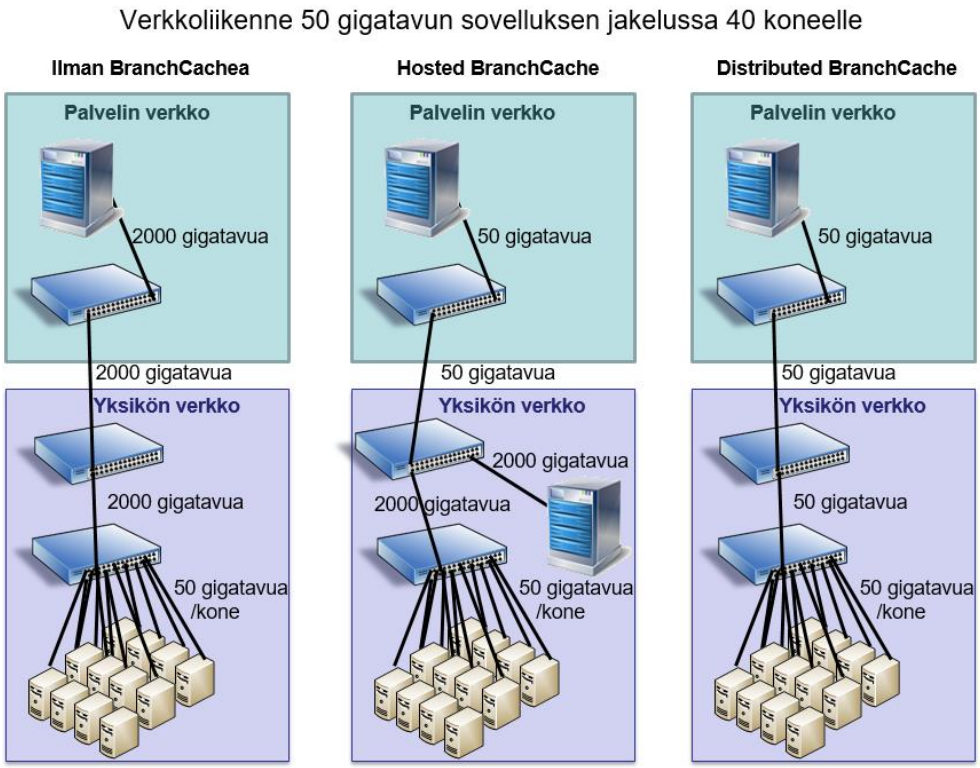
Suurissa työasemaympäristöissä työasemahallinta voi aiheuttaa suurta verkon kuormitusta, mikä voi häiritä merkittävästi työskentelyä ja liiketoimintaa. Kansallisesti näin suuria voivat olla esimerkiksi korkeakoulut ja yliopistot. Joissakin työasemaympäristöissä on jouduttu aikatauluttamaan asennuksia, jotta suuri määrä samanaikaisia työasema-asennuksia tai sovellusjakeluita ei hidastaisi verkon toimintaa. Aikatauluttaminen hidastaa muutosten toteuttamista ja aiheuttaa ylimääräistä työtä prosessiin. Työskentelyn aikana asentuvat asennukset voivat aiheuttaa koneen uudelleenkäynnistyksen, sammuttaa ohjelmia, hidastaa konetta tai estää jotain sovellusta toimimasta.

Edellä mainittuihin asioihin SCCM ei itsessään tarjoa paljoa, tai ainakaan riittävästi apua. Näiden asioiden ratkaisemiseksi otettiin käyttöön BranchCache ja suunniteltiin huoltoikkunakäytäntö. Nämä vaativat myös tietoverkkoon tehtäviä lisämuutoksia.

3.2.1 BranchCache

Microsoft BranchCache on suunniteltu laajaverkkoyhteyksien (WAN) optimointiin. Useamman työaseman pyytäessä samaa sisältöä, työasemat lataavat sisällön informaation sen sijaan että lataisivat varsinaisen sisällön. Sisällön informaatio pitää sisällään hash-tiedot, jotka on laskettu alkuperäisestä sisällöstä. Sisällön tiedot ovat erittäin pieniä verrattuna varsinaiseen sisältöön. Tämän jälkeen työasema tekee lähiverkkoon pyynnön saamallaan hash-tiedolla, ja lataa varsinaisen sisällön pyyntöön ensimmäisenä vastanneelta työasemalta tai palvelimelta. BranchCachen voi jakaa distributed cache tai hosted cache -muodossa. Hosted cache -muodossa työasemien kanssa samaan lähiverkkoon (LAN) asetetaan palvelin, joka varastoi työasemien pyytämiä tiedostoja kiintolevylle BranchCache muodossa. Distributed cache -muodossa työasemille määritetään, kuinka paljon kiintolevytilaa BranchCachella on käytettävissä. (Microsoft 2018a.)

Microsoft suosittelee tyyppiä ”distributed cache” pienille haarakonttoreille, joilla ei ole paikallista palvelinta käytettävissä. Toimistoille joilla on palvelin käytettävissä, Microsoft suosittelee hosted cache -tyyppiä. Perusteluksi hosted cache -tyypin suosimiseksi Microsoft kertoo lisääntyneen saatavuuden, koska palvelin on päällä, vaikka työasemat olisivat pois päältä. Toinen perustelu on, että toisin kuin distributed cachella, sama välimuistissa oleva sisältö voidaan jakaa useampaan aliverkkoon.



Kuva 2. 50 gigatavun kokoinen jakelu 40 koneelle eri menetelmin.

Microsoftin suosituksista huolimatta Hämeen ammattikorkeakoulun tapauksessa havaitsin distributed cachen olevan huomattavasti tehok-

kaampi vaihtoehto. Korkeakoulun lähiverkoissa on niin suuria määriä koneita, että aktiivituntien aikaan työasemia on paljon päällä. Tällöin lähes aina löytyy lähettyviltä kone, jolla on pyydetyt paketit BranchCache-välimuistissa. Hiljaisten tuntien aikaan tapahtuvaa liikennettä on puolestaan niin vähän, ettei sillä ole merkitystä muulle verkolle tai käyttäjille. Koulumaailmassa jaetaan perinteisesti päivitykset ja asennukset samaan aikaan kaikille koneille, tai kokonaiselle luokalliselle koneita. Tällöin koneiden BranchCache-välimuistissa on ajantasaiset tiedostot, joita koneet ovat samaan aikaan tarvitsemassa. Lisäksi pääsääntöisesti sovellusten ja päivitysten jakelut tehdään koneille määritetyssä huoltoikkunassa yöaikaan, jolloin kaikki koneet ovat päällä. Microsoftin suosituksesta poiketen suosittelisin distributed cachen käyttöä pienissä ja erittäin suurissa työasemaympäristöissä. Hosted cache puolestaan toimii parhaiten keskisuurissa ja suurehkoissa ympäristöissä, joissa verkko on pilkottu pieniin osiin.

Kuvassa 2 näkyy, miten liikenne poikkeaa tavallisen verkkolatauksen, hosted BrancCachen ja distributed BranchCachen välillä. Korkeakoulun tapauksessa Hosted BranchCache ruuhkauttaisi yksikön/rakennuksen pääkytkintä liikenteen kulkiessa sen kautta. Distributed BranchCachen avulla lataus haetaan pääsääntöisesti vain kerran palvelimelta, minkä jälkeen luokan työasemat vaihtelevat paketteja keskenään. Mikäli luokassa olevilla työasemilla ei ole haluttua pakettia, voivat koneet hakea paketin myös saman yksikön/rakennuksen toisen luokan koneelta, joka on samassa VLAN-verkossa.

BranchCachen käyttöönotto vaatii työasemille Group Policy asetukset, palvelimelle BranchCachen käyttöönoton, verkkopääsyt, sekä jakeluiden määrittämisen niin, että ne sallivat BranchCache jakelun. Työasemille Distributed BranchCache vaatii neljä Group Policy asetusta. Vaaditut asetukset löytyvät Administration Templates haaran alla olevassa haarassa Network/BranchCache. Asetukset ovat “Configure BranchCache for network files”, “Set BranchCache Distributed Cache mode”, “Set percentage of disk space used for client computer cache” sekä “Turn on BranchCache”. Nämä asetukset jaettiin opiskelijapuolen työasemille. Palvelimille tarvitsee puolestaan asettaa Administration Templates -haaran alla olevaan Network/Lanman Server -haaraan “Hash Publication for BranchCache” -asetus päälle. Korkeakoulussa BranchCache sisällön jakaminen sallittiin SCCM Distribution point -palvelimille, sekä unc-sovelluksia jakaville palvelimille. Opiskelijakoneiden VLAN-verkkoihin sallittiin BranchCachen käyttämä liikenne. Henkilökunnan puolelle tätä ei nähty tarpeelliseksi huomattavasti pienemmän volyymin vuoksi. Asia on kuitenkin harkinnassa HAMKin suurimman yksikön Visamäen osalta.

HAMKin tietoverkkoasiantuntija Antti Salosen kanssa tutkittiin verkkoliikenteen määrää verkkokytkimeltä, sovelluksen jakavalta palvelimelta (Distribution point) sekä työasemilta. Testeissä käytettiin 50 gigatavun Adobe Suite SCCM-jakelua suljetussa 40 työaseman laboratorioympäristössä. Aluksi monitoroitiin verkkoliikennettä ilman BrachCache-ominaisuutta.

Tuolloin oletetusti jokainen luokan kone haki sovelluksen koko median palvelimelta. Tietoverkko sekä SCCM Distribution Point -palvelimen levy IO ruuhkautuivat pahasti, minkä vuoksi asennukset kestivät pitkään. Seuraava testi tehtiin samalla kokoonpanolla ja sovellusjakelulla. Ainoana erona oli BranchCache, joka oli asetettu käyttöön. Tulokset olivat odotettua paremmat. Palvelin lähetti ainoastaan 50 gigatavua dataa eteenpäin, tietoverkko ei ruuhkautunut, eikä palvelimen suorituskyky hidastanut jakelua. Koneet vaihtelivat paketit keskenään ja sellaiset, joita ei ollut yhdelläkään työasemalla haettiin palvelimelta vain kerran. Työasemien toisilleen lähettämä datan määrä vaihteli jonkin verran, mutta jakautui kaikille koneille. Datasiirtojen nopeus ylitti oletusarvot. Oletuksesta poikkeavaa oli myös se, ettei työasemien kytkimen ulkopuolelta lataantunut dataa huomattavasti jaetun sovelluksen kokoa enempää. Samoja paketteja ei haettu palvelimelta kahta kertaa, eivätkä hash-tarkistukset näkyneet merkittävästi verkkoliikenteen määrässä.

3.2.2 Wake-On-Lan

Työaseman automaattinen hallinta edellyttää, että tietokoneita voidaan hallita myös silloin kun ne eivät ole päällä. Haluttujen koneiden herätys onnistuu verkkoon lähetetyillä herätyspaketeilla (Magic Package), joka on osa koneiden etäherätys Wake-On-Lan (WOL) standardia. (Datasynergy 2018.)

Wake-On-Lan vaatii verkon avaukset VLANien yli toimiakseen. Tätä varten broadcast-pyynnöt sallittiin HAMKin VLAN-verkkojen yli, mutta estettiin Access Control listoilla kaikki muu paitsi erikseen sallittu broadcast-liikenne. Broadcast -liikenne sallittiin admin VLAN-verkosta sekä SCCM-site -palvelimelta työasemien VLAN-verkkoihin. Liikenne sallittiin kahteen porttiin: seitsemän ja yhdeksän. Langattomiin verkkoihin pääsyjä ei laitettu, koska ei haluttu koneiden heräävän ilman kiinteää verkkoyhteyttä. Verkkopääsyjen lisäksi työasemien BIOS- sekä Windows-asetuksista täytyy asettaa Wake-On-Lan käyttöön.

Hämeen ammattikorkeakoulun koneiden BIOS-asetukset vakioitiin, jotta voitiin varmistua siitä, että WOL-asetus tulee päälle myös uusilla koneilla. BIOS-asetuksia voidaan hallita myös SCCM-sovellusjakelun kautta joidenkin tietokonemerkkien osalta, mutta ei kaikkien. Kun verkko ja BIOS-asetukset ovat kunnossa, koneet heräävät WOL-paketteihin ollessaan pois päältä.

Jotta koneet heräisivät myös syväuni -tilasta WOL-pakettiin, on varmistettava, että myös työasemien Windows-käyttöjärjestelmässä on sallittu Wake-On-Lan. Tätä varten tehtiin SCCM Application -jakelu WinWol_Settings. Jakelu koostuu neljästä tiedostosta. Asennus- ja asennuksen poistotiedostot ovat komentokehote CMD-skriptejä. Lisäksi jakelussa on Windows Task Scheduler -tehtävän XML-määritystiedosto, sekä varsinaisen

asetuksen tekevä VBS-skripti. Asennusskripti luo XML-määrityksen mukaisen tehtävän Task Scheduleriin ja kopioi koneelle WOL-asetuksen tekevän VBS-skriptin. Ajastettu tehtävä käynnistää VBS-skriptin kerran viikossa. VBS-skripti käy Windows rekisteristä for-silmukalla läpi kaikki koneen verkkokorttiyhteydet. Kaikkiin verkkokorttiyhteyksiin, joiden interface-tyyppi on kiinteä lähiverkko eli Ethernet, asetetaan WOL-asetukset päälle.

Windows WOL-asetusta ei voi jakaa Group Policyillä, koska asetus on verkkokorttikohtainen. Asetusta ei myöskään haluttu päälle muille kuin Ethernet-tyypin verkkokorttiyhteyksille. Ainoa keksitty ratkaisu asetuksen jakamiseen oli skripti. Päädyin Task Schedulerin kautta jakamiseen, jotta voidaan varmistaa jatkossakin, että asetus menee työasemille perille. Koneen kokoonpanon muuttuessa asetus astuu voimaan myös uudelle verkkokorttiajurille. Koneen kokoonpano voi muuttua esimerkiksi laitteistopäivityksen yhteydessä, mutta yleisemmin uudemman ajurin asentuessa koneelle. Uusi ajuri voi asentua koneelle joko Windows-päivitysten mukana, tai päätelaitehallinnan tietoturva- tai ominaisuus-ajuripäivityksen kautta. Kerran viikossa suoritettava ajastus on erittäin nopea ja kevyt automaattinen operaatio, joka ei näy käyttäjälle.

3.3 **Asetusten hallinta**

Windows työasemien asetuksia hallitaan perinteisesti Microsoft Group Policy (GPO) -määrityksillä. Hämeen ammattikorkeakoulun Windows-työasemien asetukset ovat myös pääosin niillä hallittuja. Valmiit GPO-määritykset eivät kuitenkaan pidä sisällään kaikkia asetuksia. Group Policy -laajennoksia on saatavilla, ja niitä on korkeakoulussa laajennettukin esimerkiksi Microsoft Office -asetusten hallinnan osalta. Laajennokset ovat XML-määritystiedostoja, joiden pääte on ADMX. Lisäksi asetukset vaativat kielikohtaisen määritystiedoston, jonka nimi on sama, mutta tiedostopääte on ADML. ADML-tiedostossa määritellään ylläpitäjälle käyttöliittymässä näkyvät asiat, ADMX-tiedostossa puolestaan varsinaiset asetukset ja työasemalle tehtävät muutokset. ADMX- ja ADML-tiedostoja voi myös itse tehdä tarvittaessa. Puuttuvia asetuksia varten luotiin HAMK määritystiedostot, ja niihin määritettiin sellaisia asetuksia, joita oli olemassa olevien lisäksi tarve hallita. Omia asetuksia luotiin esimerkiksi Windows ja Office-asetuksia varten, joita ei sovellustoimittajan laajennuksella saanut määritettyä.

Myös SCCM:n kautta voi määrittää työasemille asetuksia Compliance Settings asetusten kautta. Compliance settings sekä Group Policy -asetukset ovat pääosin pelkkiä Windows-rekisterimuutoksia. Group Policyiden heikkous on, ettei niiden voimaan astumista voida verifioida tai seurata. Toinen heikkous on, ettei niitä voi kytkeä AD:n ulkopuolisille koneille. SCCM Compliance Settings -asetuksilla puolestaan voi ratkaista nämä kummatkin ongelmat. Näiden asetusten määrittäminen ja hallitseminen ovat puolestaan työläämpää. Asetuksia ei myöskään voi jakaa koneille joilla ei ole SCCM-client -ohjelmaa, eivätkä asetukset toimi, mikäli SCCM-client ei

toimi koneella. Hyvä tapa on asettaa asetukset Group Policyillä, ja tarvittaessa varmistaa niiden voimassaolo Compliance Settings -määrityksillä. (John Devito 2015.) Hämeen ammattikorkeakoulussa jaettiin kriittisiä asetuksia SCCM Compliance Settings -määrityksillä. Myös yksi satunnainen Group Policyiden kautta tuleva asetus laitettiin tarkkailuun Compliance Settings -asetuksiin, jotta voidaan seurata miten Group Policyt asettuvat voimaan.

Usein on tarpeen jakaa myös monimutkaisempia asetuksia, jotka vaativat rekisteri muutoksen lisäksi PowerShell-skriptausta, WMI-tarkistuksia tai tiedostoja. Tällaisten asetusten jakamiseen SCCM Application, eli sovellusjakelu on mainio tapa.

3.4 **Sovellusten jakelu ja päivitykset**

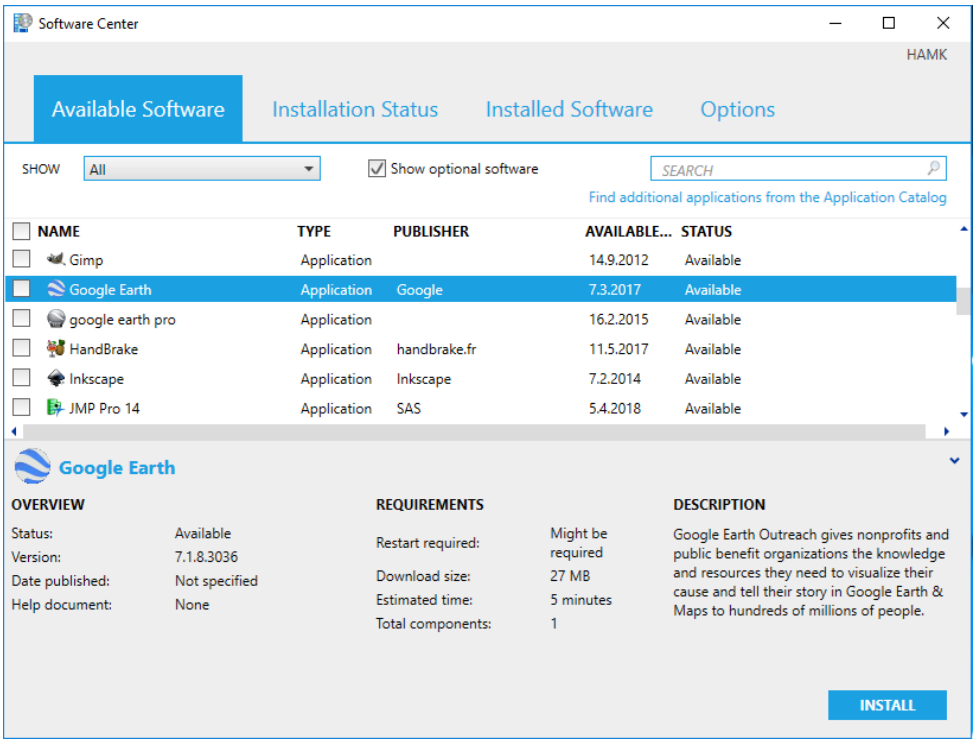
Sovellusten jakelun voi SCCM-hallittuun ympäristöön tehdä joko Package- tai Application-tyyppisenä jakeluna. Sovellusjakelu voi olla ohjelman asennus, päivitys tai koneelle tehtävä asetus. Package on aikaisempien SCCM-versioiden tapa jaella sovelluksia, ja samalla myös Application-tapaa huomattavasti rajoittuneempi ominaisuuksiltaan. Package-jakelut lähtökohtaisesti asennetaan koneille vain kerran, ja luotetaan tämän jälkeen, että asennus on mennyt onnistuneesti koneelle ja pysyy koneella. Packagen voi myös asettaa asentumaan joka kerta, kun kone esimerkiksi käynnistetään tai käyttäjä kirjautuu koneelle. Application-jakelupakettiin voi puolestaan määrittää asennuksen tunnistussääntöjä, tavan poistaa sovellus, riippuvuuksia ja monta muuta toiminnallisuutta, joita Package-jakelut eivät mahdollista. SCCM tunnistaa vapaasti määritettävien sääntöjen perusteella jakelun asennuksen tilan, eli onko sovellus jo työasemalla vai puuttuuko sovellus. Säännöt voivat pohjautua esimerkiksi tiedostojen olemassaoloon, versioihin, päivämääriin tai rekisterimerkintöihin. Sääntöjä voi olla useita ja niiden määrittämiseen voi käyttää AND- sekä OR-päättelyitä. (Microsoft 2016a.)

Päätelaitehallinnassa on tärkeää, että sovellukset voidaan myös poistaa tietokoneilta tarvittaessa. Tällaisia tilanteita voi tulla viallisen jakelun, havaitun tietoturvauhkan tai esimerkiksi lisenssisovelluksen siirron vuoksi. Hämeen ammattikorkeakoulun päätelaiteympäristöön haluttiin mahdollisuus poistaa jokainen jakelu tarvittaessa. Tahdottiin myös varmistua, että halutut muutokset menevät koneille, ja asentuvat automaattisesti uudelleen, mikäli sovellus poistuu koneelta esimerkiksi koneen uudelleenasennuksen yhteydessä. Näiden asioiden vuoksi kaikki jakelut päätettiin tehdä Application-tyyppisinä.

Sovellusten jakelut kytkettiin asentumaan pakotetusti dynaamisille koneryhmille. Tällä saavutettiin ohjelmien automaattinen asentuminen kuhunkin yksikköön, luokkaan ja yksittäiselle koneelle koneen nimen perusteella. Jakeluita on kytketty ryhmiin yli kaksi tuhatta kappaletta. HAMKin koneille on jaeltu noin 500 eri sovellusta. Käsin tehtävien asennuksien ja

työmäärän vähentämisen vuoksi, päätettiin jakaa kaikki sovellukset keskitetyn päätelaitehallinnan kautta. Sovittiin että kaikki sovellukset, joita asennetaan tai tullaan asentamaan enemmän kuin kahdeksan kertaa, paketoidaan ja jaellaan koneille keskitetysti.

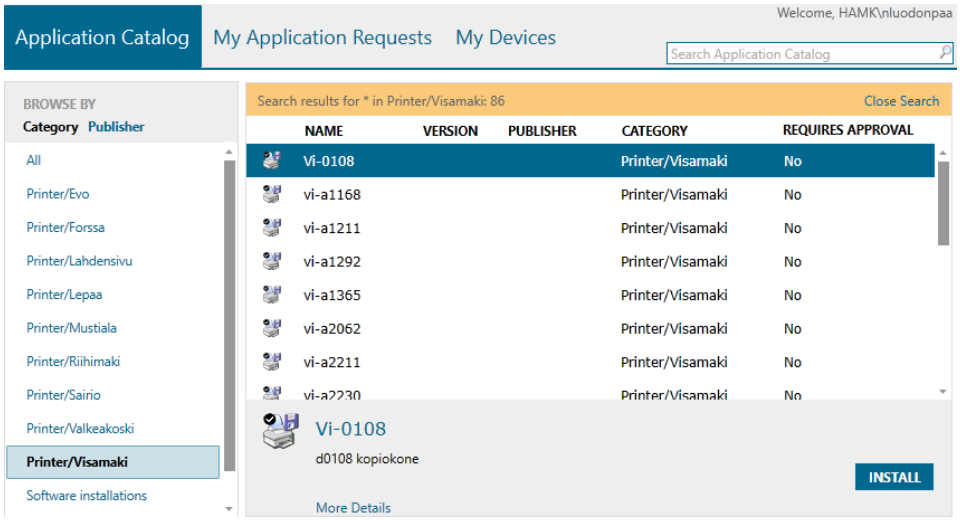
Opinnäytetyön tilaaja halusi tarjota käyttäjille myös itsepalvelumahdollisuuksia. SCCM sisältää kaksi sovelluskauppaa. Software Center kuvassa 3 on sovelluskauppa työasemille kytkettyjä sovelluksia varten, ja Application Catalog kuvassa 4 puolestaan käyttäjille kytkettyjä sovelluksia varten. Software Centerin kautta laitettiin tarjolle vapaaehtoisia sovelluksia, joita on pyydetty tai joiden on nähty helpottavan käyttäjiä. Sovellusten lisenssioikeudet täytyy tarkistaa ennen sovelluksen tarjolle laittamista. Sovelluspyynnöistä on pyritty karsimaan myös samaa tarkoitusta varten olevia sovelluksia. Jokainen sovellus aiheuttaa lisätyötä päivitysten, ylläpidon ja tietoturvan osalta.



Kuva 3. Itsepalvelusovelluskauppa Software Center.

Monet opettajat ja IT-valveutuneet työntekijät tarvitsevat kuitenkin testaamiseen, kokeilemiseen tai työhönsä sovelluksia, joita ei ole asetettu sovelluskauppaan tarjolle. Käyttäjillä ei ole koneille pääkäyttäjätason käyttöoikeuksia. Näitä tilanteita varten tehtiin sovellus, jolla käyttäjä saa perustellusta pyynnöstä pääkäyttäjätason tunnuksen koneellensa. Jaettava tunnus on kuitenkin määritetty tietoturvasyistä niin, ettei sillä pysty kirjautumaan koneelle. Koneelle jaettava tunnus sallii ainoastaan ohjelmien suorittamisen ja asennuksen korotetuin käyttöoikeuksin.

Käyttäjille kohdistettuun sovelluskauppaan, eli Application Catalogiin puolestaan kytkettiin tarjolle kaikki HAMKin tulostimet. Koska tulostimet asentuvat käyttäjän profiiliin eivätkä tietokoneelle, luontevampi ratkaisu niiden jakeluun oli Application Catalog. Application Catalogissa oli myös helppo kategorioida tulostimet yksiköittäin, jolloin käyttäjän on helppo löytää haluamansa tulostin. Käyttäjät liikkuvat paljon eri yksiköiden ja luokkien välillä, joten eri tulostinten helppo asentaminen on oleellista. Myös Active Directory mahdollistaa tulostimien asentamisen. Se koettiin kuitenkin käyttäjille turhan monimutkaiseksi ja hitaaksi tavaksi lisätä tulostimia. Kummankin sovelluskaupan pikakuvake jaettiin koneiden työpöydälle Application-jakelulla, jotta ne olisivat helposti löydettävissä.



Kuva 4. Itsepalvelusovelluskauppa Application Catalog.

3.5 Työasemien asennus

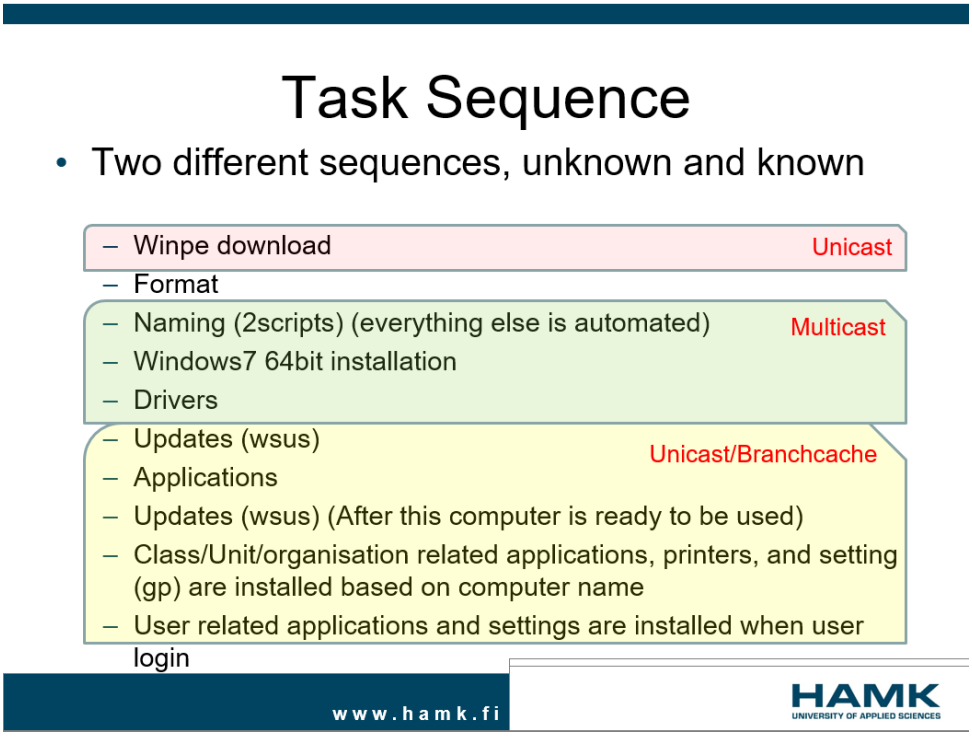
Tietokoneiden asennus tahdottiin mahdollisimman nopeaksi ja automaattiseksi toimenpiteeksi. Uusista tietokoneista ei järjestelmässä ole valmiiksi mitään tietoja. Järjestelmässä olevista, eli uudelleenasennettavista on paljon tietoa, muun muassa nimitieto. Nimikäytäntö sekä sovellusten ja asetusten jakelu suunniteltiin niin, että koneen automaattista asentamista varten ei tarvita muita tietoja. Tämän ansiosta koneiden uudelleenasennus onnistuu automaattisesti, ja uusien koneiden asennus ei vaadi muuta kuin nimitiedon syöttämisen.

SCCM suorittaa koneiden asennukset verkosta käynnistettävällä asennusrutiinilla (Task sequence). Task Sequencet sisältävät joukon sinne määritettyjä tehtäviä. Pääasialliset tehtävät ovat verkosta käynnistettävä asennusympäristön lataus (PXE), kiintolevyn formatointi, käyttöjärjestelmän lataus ja asennus sekä ajureiden, päivitysten ja ohjelmien asennukset.

Työasemien asennuksia varten luotiin kaksi erillistä asennusrutiinia, toinen uusien koneiden asennuksia varten ja toinen jo järjestelmässä oleville koneille. Erona kahdella rutiinilla on se, että uudelleenasennettavien konei-

den Task Sequencen ei tarvitse kysyä koneen nimeä. Koneet voidaan tällöin asentaa tai ajastaa asentumaan haluttuna aikana automaattisesti uudelleen. Uusien koneiden asennuksessa sen sijaan nimitieto ei ole valmiiksi tiedossa.

Uusien koneiden asennusta varten luotiin kaksi VBS skriptiä, jotka käynnistetään heti PXE käynnistyksen jälkeen. Ensimmäinen skripti pyytää koneen nimeä ja tarkistaa sen oikeellisuuden Hämeen ammattikorkeakoulun nimeämiskäytännön mukaan. Mikäli nimi ei ole nimeämiskäytännön mukainen, skripti ilmoittaa nimessä olevista virheistä ja pyytää antamaan nimen uudelleen. Mikäli nimi on käytännön mukainen, skripti tallentaa sen muuttujaan. Seuraava skripti lukee nimen muuttujasta ja asettaa sen Task Sequencen sisäiseen tietokoneen nimi -attribuuttiin (OSDComputerName). Lisäksi skripti tulkitsee nimen perusteella mihin Active Directory (AD) domainiin työaseman tulee kuulua ja asettaa AD Domain attribuutin (OSDDomainOUName). Attribuutin perusteella kone nousee AD:ssa automaattisesti oikeaan haaraan. Asentaja pääsee koneen käynnistyksestä koneen nimeämisruutuun noin kahdessa minuutissa. Koneennimen syöttämisen jälkeen loput toimenpiteet tapahtuvat automaattisesti. Koneen asennus on siis tässä kohtaa työn näkökulmasta valmis. Oikeat sovellukset asentuvat koneelle automaattisesti annetun nimen perusteella. Loin Task Sequenceen myös skriptin, joka asettaa BranchCachen päälle käyttöjärjestelmä- ja ajuriasennusten jälkeen, jotta loput toimenpiteet kuten ohjelma- ja päivitys-asennukset hyödyntävät BranchCachea tiedon siirrossa. Lähiverkkoteknisesti Task Sequencen voi jakaa kolmeen vaiheeseen, jotka on kuvattu kuvassa 5.



Kuva 5. Task Sequencen vaiheet kuvattuna päätasolla ja jaettuna verkkoteknillisesti eroaviin vaiheisiin.

Ensimmäinen vaihe on PXE:n kautta käynnistyvä asennusympäristön (WinPE) lataus. Tämä vaihe onnistuu ainoastaan unicast-protokollalla. Unicast-datasiirto tarkoittaa, että jokainen työasema hakee tarvittavat paketit erikseen palvelimelta. Tässä vaiheessa siirrettävän datan määrä on vain noin 1,3 gigatavua.

Toinen vaihe on käyttöjärjestelmän lataus, jossa voi käyttää joko unicast- tai multicast-tiedonsiirtomenetelmää. Tämän latausvaiheen datamäärä on noin 15 gigatavua. Multicast-datasiirrossa VLAN-verkon lähikytkimelle perustetaan multicast-ryhmä, kun ensimmäinen tietokone pyytää median latausta. Median lähetys alkaa multicast-ryhmälle. Tietokoneet, jotka tarvitsevat saman latauksen liittyvät tähän multicast-ryhmään. Kun tietokone on ladannut kokonaan tarvitsemansa median, se lähtee pois ryhmästä. Lähetys pyörii alusta loppuun ympyrää, kunnes ryhmässä ei ole enää yhtään jäsentä. Ryhmään voi liittyä lähetyksen missä vaiheessa tahansa. Työasemat voivat siis aloittaa latauksen keskeltä mediaa. Tämä siirtotapa on unicastia huomattavasti tehokkaampi, sillä dataa siirtyy palvelimen ja VLAN-verkon välissä vain yhden lähetyksen verran, eikä unicastin tapaan jokaiselle koneelle erikseen.

Hämeen ammattikorkeakoulussa tämä vaihe laitettiin käyttämään multicast-menetelmää. Multicastin ongelmaksi havaittiin hitaat koneet, jotka aiheuttivat kaikkien koneiden asennusten hidastumisen hitaimman tasolle. Lähetys odottaa mukana olevien koneiden kuittausta saadusta paketista. Tätä varten palvelimelle luotiin kolme erillistä multicast-ryhmää Fast, Medium ja Slow. Koneet aloittavat nopeassa ryhmässä. Mikäli kone ei pysy vauhdissa mukana, se alennetaan hitaampaan Medium-ryhmään, ja niin edelleen. Tällöin muutama hidas kone ei hidasta muiden samaan aikaan asennettavien koneiden asennuksia.

Verkkoteknisesti kolmas vaihe on päivitysten ja ohjelmien asennukset. Tässä vaiheessa siirtyy suurin osa asennuksen datamäärästä. Määrä vaihtelee erittäin paljon koneen nimestä, eli asennettavista ohjelmista riippuen. Siirrettävän datan määrä vaihtelee noin 40 ja 300 gigatavun välillä. Oletuksena tämä vaihe asentuu unicast-menetelmällä, mutta unicast aiheuttaisi erittäin suurta kuormitusta lähiverkkoon. Tämän vuoksi Hämeen ammattikorkeakoulun Task Sequenceen luotiin skripti, joka ennen vaiheen aloittamista asettaa BranchCachen päälle. Luokkatilakäytössä olevat koneet asennetaan tavanomaisesti kaikki uudelleen samaan aikaan. Tällöin BrachCache toimii erittäin tehokkaasti, kun luokan koneet ovat päällä ja vaihtavat keskenään tarvittavia tiedostoja, eikä data siirry koko verkon läpi.

4 TYÖASEMIEN HUOLTOIKKUNA

Tietokoneen käytön aikana asentuvat päivitykset ja ohjelmat hidastavat koneen käyttöä. Asennukset voivat myös häiritä käyttöä ilmoituksilla tai ohjelmia sammuttamalla. Pahimmassa tapauksessa päivitykset voivat aiheuttaa koneelle pakollisen uudelleenkäynnistyksen, jolloin käyttäjä menettää tallentamattomat työnsä. Ilman hyvin suunniteltua huoltoikkunakäytäntöä pitkään käyttämättömänä olleiden koneiden tietoturva vaarantuu. Lisäksi päivityksiä on voinut kertyä hyvinkin paljon jonoon, jolloin päivitysten asentuminen kestää huomattavan kauan. Jonossa olevat päivitykset saattavat lisäksi estää käyttäjää asentamasta Software Centeristä uusia sovelluksia itsepalveluna. SCCM ei suostu tekemään muutoksia, mikäli koneelta puuttuu vaadittuja kriittisiä Windows-päivityksiä. Configuration Managerin oma huoltoikkuna sisältää tavan rajoittaa ohjelmia ja päivityksiä asentumasta haluttuun aikaan, jotteivat ne häiritse tuottavaa työtä (Microsoft 2017). Tämä ei kuitenkaan riitä toimivaan huoltoikkunaan.

Huoltoikkuna voidaan jakaa neljään osaan. Ensimmäinen on SCCM-huoltoikkuna, jolla rajoitetaan muutokset asentumaan haluttuina aikoina. Toinen on koneiden herätykset, joka onnistuu Wake-On-Lan automatisoinnilla. Kolmas on työaseman tietojen päivittäminen puuttuvien asennusten ja päivitysten osalta. Neljäs osa huoltoikkunaa on jakelukäytäntöjen suunnittelu siten, että lähes kaikki asennukset tapahtuvat huoltoikkunassa. Myös koneiden uudelleenkäynnistyskäytännöt auttavat huoltoikkunan toimintaa merkittävästi.

4.1 SCCM-huoltoikkuna

Microsoftin SCCM käsitteen mukaan huoltoikkuna pitää sisällään ainoastaan päivitysten ja ohjelmien asentumisaikojen rajoittamisen (Microsoft 2017). Tämä on yksi osa huoltoikkunaa, mutta ei kuitenkaan riittävä kokonaisvaltaisen huoltoikkunan määrittämiseksi.

SCCM-huoltoikkuna-asetus määritettiin HAMKissa Windows Workstations-non-vdi -Collectionille. Collection pitää sisällään kaikki Windows-työasemat VMware VDI Client -virtuaalikoneita lukuun ottamatta. Huoltoikkuna asetettiin joka päiväksi aikavälille 00:00-05:00.

4.2 Työasemien herätykset

Työasemien tulee olla päällä huoltoikkunan aikaan, jotta ne voivat asentaa muutoksia. Koneiden herätys voidaan automatisoida huoltoikkunan alkamisaikaan automaattisesti lähetettävillä WOL-paketeilla.

HAMKissa koneiden herätykset automatisoitiin samalla WOL-skriptillä, joka tehtiin koneiden reaaliaikaista hallintaa varten. Skripti kopioitiin

SCCM-pääpalvelimelle (SCCM Site-Server). Kyseiselle palvelimelle oli jo aikaisemmin määritetty pääsyt työasemien VLAN-verkkoihin WOL-pakettien lähettämiseen käytettyyn porttiin. Komento muutettiin lähettämään automaattisesti herätyspaketit samalle Collectionille, jolle SCCM-huoltoikkunakin määritettiin. Skripti ajastettiin Windows Task Scheduleriin ajettavaksi jokaisen viikon keskiviikkona ja lauantaina ennen huoltoikkunan alkua kello 23:47.

WOL-paketit eivät lähde samalla hetkellä kaikille työasemille, vaan yksi kerrallaan. Tämä tasoittaa SCCM-palvelimille tulevaa kuormaa, ja mahdollisesti säästää sulakkeitakin. Skriptin ajo kestää noin 20 minuuttia, minkä jälkeen kaikille 2300 koneelle on lähetetty herätyspaketti.

4.3 **Työasemien tietojen päivitys**

SCCM ei automaattisesti käynnistä asennuksia koneiden käynnistyessä. Asennukset alkavat, kun tietojen päivitysajot (Cycle) havaitsevat puuttuvia ohjelmia tai päivityksiä. Ohjelmien asennuksille on oma Cycle ja Windows-päivityksille (WSUS) omansa. SCCM-hallintakonsolilla määritellään Default Client Settings -asetuksilla, kuinka usein nämä tietojen päivitysajot työasemilla ajetaan. Oletusasetuksilla molemmat tarkistukset tehdään seitsemän päivän välein. (Microsoft 2018b.) Tämä ei ole riittävä nopeus sovellusmuutoksille Hämeen ammattikorkeakoulussa. Ohjelmien päivitysajo määritettiin tunnin välein, ja WSUS-päivitysajo kerran vuorokaudessa ajettavaksi.

Tästä huolimatta koneen herätessä huoltoikkunaan voisi kestää tunnin ennen kuin puuttuvien ohjelmien asennukset alkaisivat. Puuttuvien WSUS-päivityksien asennukset eivät puolestaan alkaisi välttämättä ollenkaan. Tämän lisäksi työaseman SCCM-clientin tiedossa olevat puuttuvat WSUS-päivitykset voivat estää ohjelmia asentumasta. SCCM ei asenna muita sovelluksia, mikäli koneelta puuttuu kriittisiä WSUS-päivityksiä. Tällöin huoltoikkunassa ei välttämättä asentuisi mitään. Edellä mainittujen seikkojen vuoksi tein ja jaoin työasemille sovellusjakelun kautta Windowsin ajastetun tehtävän, joka käynnistää tietojen päivitysajot PowerShell-skriptillä. Ajastus käynnistyy torstaisin ja sunnuntaisin viisitoista minuuttia yli puolenyön. Aika on noin puoli tuntia koneiden herätysajastuksen jälkeen. Tässä ajassa koneet ovat ehtineet käynnistyä, tehdä uudelleen käynnistyksen tarvittaessa ja ladata SCCM-clientin käyntiin.

4.4 **Käytännöt huoltoikkunaa varten**

Mikäli SCCM-sovellusjakelu tai WSUS-päivitys kytketään Collectioniin oletusasetuksilla ilman aikamäärityksiä, jakelu asentuu työaseman ajaessa sitä vastaavan ajastetun Cyclen. Tämä voi tapahtua milloin vain, ja mahdollisesti haitata käyttäjien työskentelyä. Jakeluun voidaan määrittää kaksi eri aikarajaa. Ensimmäinen on saatavilla-aikaraja, eli milloin sovellus on

asennettavissa, mutta asennetaan automaattisesti vain SCCM huoltoikkunan aikana. Toinen aikaraja on deadline, jolloin sovellus asennetaan myös huoltoikkunan ulkopuolella.

Sovimme Hämeen ammattikorkeakoulun päätelaitehallintaryhmän kesken, että sovellus jakeluiden ja WSUS-päivitysten saatavilla-ajaksi laitetaan jakelun aloittamishetki, joka on yleensä heti. Isompien päivitysten ja ohjelmajakeluiden asentamisesta voidaan sopia jokin tietty käyttöönottopäivä. Tällöin saatavilla-aika asetetaan käyttöönottopäivälle. Deadline-määritystä varten kysyimme tietoturvaryhmän näkemystä ja seurasimme jakeluiden edistymistä. Jakelut menevät suurimmalle osalle koneista jo ensimmäisessä deadlinen jälkeisessä huoltoikkunassa. Koneilla voi kuitenkin olla paljon päivityksiä jonossa eivätkä kannettavat ole aina paikalla, joten jakelun asentaneiden koneiden määrä lisääntyy myös seuraavissa huoltoikkunoissa. Kahdessa viikossa koneet herätetään neljä kertaa yölliseen HAMK-huoltoikkunaan. Tämä päätettiin sopivaksi ajaksi, ottaen huomioon tietoturvan, käyttäjille tulevien häiriöiden minimoinnin ja riittävän nopean muutosvauhdin.

5 TYÖASEMIEN ITSESTÄÄN KORJAANTUVUUS

Microsoft System Center Configuration Manager pitää sisällään itsestään korjaantuvuus -ominaisuuden. Työasemalle asennettaessa SCCM-client luo Windows Task Scheduleriin ajastetun tehtävän nimeltä Configuration Manager Health Evaluation. Tehtävän käynnistyessä se suorittaa ccmeval.exe -ohjelman. Ohjelma suorittaa tausta-ajona SCCM-toimintakunnon tarkistuksia. Tarkastuksia tehdään esimerkiksi esivaatimuksien täyttymistä, vaadittujen palvelujen toimivuutta ja WMI-rajapinnan eheyttä koskien. Vikoja tai puutteita löytäessään ccmeval.exe pyrkii tekemään vaaditut toimenpiteet asian korjaamiseksi, joskus siinä kuitenkaan onnistumatta.

Windows-käyttöjärjestelmä vaatii säännöllisesti uudelleenkäynnistyksiä täysin toimiakseen. SCCM sisältää ominaisuuksia tietokoneiden uudelleenkäynnistämiseksi tarvittaessa. Näiden ominaisuuksien säätämiseen on kuitenkin erittäin vähän vaihtoehtoja. Käytännössä säätövara rajoittuu siihen, käynnistetäänkö tietokone pakotetusti uudelleen, mikäli SCCM-clientin tekemä asennus sitä vaatii. Toiminnallisuus rajoittuu ainoastaan SCCM:n tekemiin asennuksiin. Niidenkin tekemistä uudelleenkäynnistystarpeista SCCM huomioi vain osan. Koneita ei myöskään voi käynnistää uudelleen pakotetusti, mikäli koneelle on käyttäjä kirjautuneena.

5.1 Automaattinen uudelleenkäynnistys

Windows-päivitykset, Windows-palvelut ja ohjelmat voivat vaatia koneelle muutoksia, joita ei voida asettaa käyttöön käyttöjärjestelmän ollessa käynnissä. Tällöin muutos- ja uudelleenkäynnistyspyyntö lisätään Windows-rekisteriin. Jotkin ohjelmat tarkistavat ennen asennuksen aloittamista, ettei rekisteristä löydy uudelleenkäynnistyspyyntöjä. SCCM-client myös tarkistaa ennen työasemalle muutoksien tekemistä, ettei koneella ole muutoksia haittaavia uudelleenkäynnistyspyyntöjä. SCCM-client ei aloita muutosten tekemistä, jos se tällaisia havaitsee. Mikäli tarkistusta ei tehtäisi, käynnistyksen yhteydessä käyttöönotettavissa muutospyynnöissä voisi olla ristiriitaisia pyyntöjä. Sieltä voisi myös puuttua tai olla vääriä pyyntöjä, jos tilanne on muuttunut asennushetkestä merkittävästi. Tämä aiheuttaisi epävakautta ohjelmien tai jopa käyttöjärjestelmän toimintaan.

Uudelleenkäynnistyspyynnöt voivat hidastaa tai käytännössä estää muutoksien menemisen työasemalle. Kokemus on osoittanut, että useat käyttäjät eivät uudelleenkäynnistä tai sammuta työasemaa. Tällöin muutoksia alkaa kertyä jonoon ja niitä voi kertyä hyvinkin paljon. Tällöin uudelleenkäynnistyksiä tarvitaan niin useita, kun uudelleenkäynnistyksen vaativia muutoksia on jonossa. Ennen jokaista uudelleenkäynnistystä tarvitsee myös odottaa, että seuraavat muutokset asentuvat koneelle. Tietoturvan vaarantumisen lisäksi tästä aiheutuu ongelmia käyttäjälle. Käyttäjä ei saa uusia ominaisuuksia ja ohjelmia käyttöönsä, mikä voi olla turhauttavaa.

Ongelman korjaus on käytännössä SCCM-tietojen päivittämistä, odottamista, uudelleenkäynnistystarpeen tarkastamista ja työaseman uudelleenkäynnistämistä. Korjaus vie sitä enemmän työaikaa, mitä enemmän muutoksia on ehtinyt kertyä jonoon.

Koska käyttäjät eivät ole innokkaita käynnistämään koneita uudestaan ja Windows niitä kuitenkin tarvitsee, on hyödyllistä suunnitella automaattisia koneen uudelleenkäynnistysmenetelmiä. Hyvin suunnitellut uudelleenkäynnistystavat vähentävät ongelmia, säästävät työaikaa ja lisäävät tietoturvaa.

5.1.1 Pakotettu uudelleenkäynnistys

Uudelleenkäynnistyksen automatisoimiseksi tein PowerShell-skriptin, jonka jaoin työasemille Windows Task Schedulerin ajastetuksi tehtäväksi SCCM-sovellusjakelun kautta. Skripti tarkistaa aluksi onko käyttäjää kirjautuneena koneelle, jos on ei tehdä mitään. Mikäli käyttäjää ei ole, tarkistetaan uudelleenkäynnistyksen tarve kolmesta eri Windows-rekisterihaarasta. Asiaa siis tutkitaan WSUS, Windows-palvelujen ja ohjelmien osalta. Ohjelmien osalta löytyneiden uudelleenkäynnistyspyyntöjen sisältö tarkistetaan, ja ne tekstirivit jätetään huomioimatta, joista löytyy tiettyjä merkkijonoja. Nämä rivit jätetään huomioimatta viallisten sovellusten ja ajureiden vuoksi. Jotkin ohjelmistot lisäävät virheellisen merkinnän uudelleenkäynnistystarpeesta jokaisella käynnistyskerralla. Mikäli skripti havaitsee uudelleenkäynnistystarpeen, se kirjoittaa lokitiedostoon päivämäärän, kellonajan, tiedon että kone on uudelleenkäynnistetty järjestelmän toimesta ja kaikki rivit mitkä vaativat uudelleenkäynnistystä. Riveistä selviää asennukset, päivitykset ja palvelut, mitkä uudelleenkäynnistyksen tarvitsi. Lokitiedostoa käytetään ongelmien selvitykseen, sekä asennushistorian selvittämiseen.

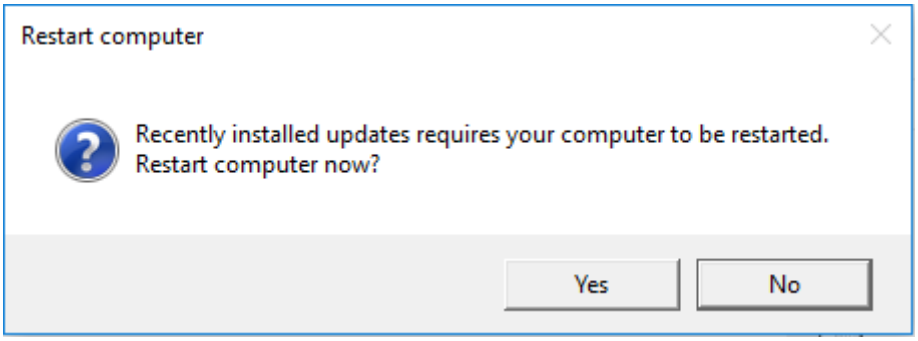
Skriptin ansiosta koneet saadaan uudelleenkäynnistämään itsensä automaattisesti, kun käyttäjä ei ole kirjautuneena koneelle. Tämä tehostaa merkittävästi etenkin huoltoikkunan toimintaa, kun asennukset eivät pysähdy odottamaan uudelleenkäynnistystä. Tarkistus on ajastettu tehtäväksi tunnin välein, joten tarvittaessa se kerkeää käynnistämään konetta uudelleen useamman kerran huoltoikkunan aikana.

5.1.2 Uudelleenkäynnistyspyyntö

Suurimmalla osalla henkilökunnasta on kannettavat tietokoneet. Tietokoneet ovat monesti kotona mukana. Sammutuksen tai uloskirjautumisen sijaan moni työntekijä vain lukitsee työasemansa. Tällöin koneen automaattisesta uudelleenkäynnistysskriptistä ei ole apua.

Tällaisia tietokoneita varten tein toisen PowerShell-skriptin, joka pohjautuu aikaisempaan skriptiin. Erona on, että tämä skripti ajetaan vain, jos

käyttäjä on kirjautuneena. Mikäli uudelleenkäynnistystarve havaitaan, kirjautuneelle käyttäjälle kerrotaan asiasta, ja häneltä kysytään käynnistetäänkö tietokone uudelleen (kuva 6). Aluksi skriptin oletusvastauksena oli ”Yes”. Käyttöönoton jälkeen kävi kuitenkin useampi tapaus, joissa käyttäjä oli painanut Enter-painiketta ja menettänyt tallentamattomat työnsä. Kokemuksen pohjalta oletusvastaukseksi muutettiin ”No”. Skripti on ajastettu suoritettavaksi joka toinen tunti, jottei se häiritsisi liian usein käyttäjää. Kaksi tuntia nähtiin kuitenkin tarpeeksi tiheäksi, jotta uudelleenkäynnistystarve tulisi ilmi. Skripti kirjoittaa samaan lokitiedostoon päivämäärän, kellonajan, uudelleenkäynnistystarpeen tiedot sekä käyttäjän vastauksen.



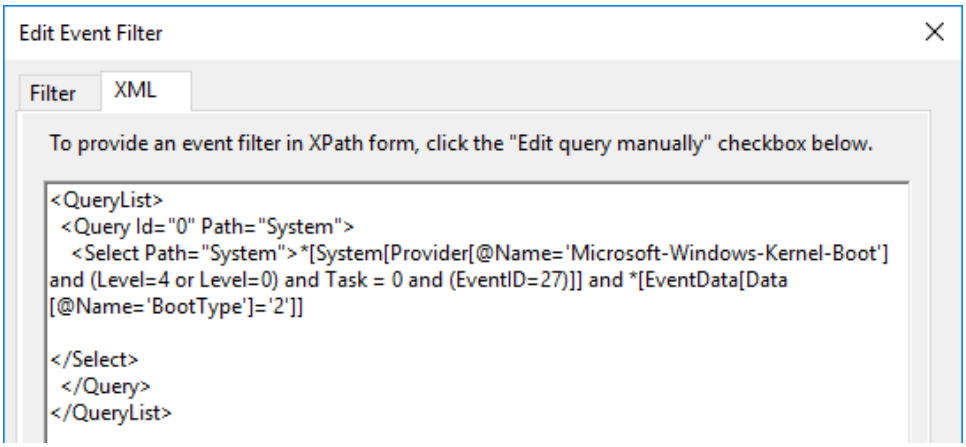
Kuva 6. Käyttäjältä kysytään tietokoneen uudelleenkäynnistystä.

5.1.3 Syväunitilasta heräävien koneiden uudelleenkäynnistys

Havaitsimme uudelleenkäynnistyskäytäntöjen ja huoltoikkunan käyttöönoton jälkeen, että muutokset eivät asennu osalle koneista huoltoikkunan aikana. Työasemien lokeja ja SCCM-raportteja seuraamalla havaitsimme ongelman johtuvan siitä, että koneet menevät syväunitilaan kahden minuutin päästä herättyään WOL-pakettiin. Normaalisti koneet menevät syväunitilaan kahden tunnin päästä. Windowsin oman toiminnallisuuden vuoksi koneet menevät syväunitilaan hyvin nopeasti, mikäli ne heräävät syväunitilasta, ja niiden hiireen tai näppäimistöön ei kosketa tuona aikana. Koneet eivät kerkeä asentamaan vaadittuja päivityksiä ja ohjelmia tuossa ajassa.

Tätä varten tein vielä kolmannen PowerShell-skiptin. Scripti tarkistaa onko kello yö yhdentoista ja aamu kuuden välillä, onko kone henkilökunta- vai opiskelijakäytössä ja onko koneella kirjautunutta käyttäjää. Mikäli on yö ja koneella ei ole käyttäjää kirjautuneena se uudelleenkäynnistetään. Opiskelijapuolen kone uudelleenkäynnistetään, vaikka koneella olisikin käyttäjä kirjautuneena. Skripti käynnistetään Task Schedulerin kautta, kun Windows-lokiin tulee merkintä, että kone on käynnistynyt syväunitilasta. Ajastuksen tein Task Scheduleriin Custom Trigger -kohtaan XML-määrityksenä, joka näkyy kuvassa 7. Task Schedulerissa on valmiina vain yksinkertaisia ajastukseen tai tapahtumaan, esimerkiksi koneen käynnistykseen viittaavia triggereitä. Tekemällä itse triggerin XML:n avulla Task Schedulerin saa suorittamaan toivotut toimenpiteet käytännössä minkä

tahansa tapahtuman yhteydessä. Tämän skriptin ansiosta koneet, jotka heräävät syväunitilasta käynnistävät itsensä heti uudelleen, eivätkä mene kahden minuutin päästä takaisin syväunitilaan.



Kuva 7. Task Scheduleriin määritetty Custom triggeri koneen herätessä syväunitilasta.

Kaikki kolme uudelleenkäynnistysskriptiä olisi voinut rakentaa yhteen ja samaan skriptiinkin. Jakelumäärityksiä, asetuksia ja ajastuksia on kuitenkin helpompi määrittää kullekin skriptille erikseen, kun ne eivät ole samassa skriptissä ja jakelupaketissa. Tämän vuoksi ne haluttiin pitää erillään.

5.2 WMI-seuranta ja korjaus

WMI on Microsoftin Windows -käyttöjärjestelmätietojen hakemiseen ja käyttöjärjestelmän hallintaan tarkoitettu standardi. WMI sisältää rajapinnat tietojen hakemiseen ja syöttämiseen, sekä tietovaraston tietojen säilömiseen. WMI on kriittinen osa nykypäivän Windows-käyttöjärjestelmien toimintaa ja hallintaa. (Microsoft 2018c.)

SCCMn oma itsestään korjaantuvuus Ccmeval.exe ei aina onnistu korjaamaan toimimattomia tai vajaasti toimivia työasemia. Isommissa työasemaympäristöissä, kuten HAMKn tuhansien koneiden ympäristössä tällaiset työasemat aiheuttavat paljon työtä. Vaikka tapauksia tulee prosentuaalisesti harvakseltaan, niin ajan myötä niitä kertyy useita satoja. WMI-ongelmat eivät näy selvästi työasemalla, vaan kaikki näyttävät päällepäin toimivan normaaliin tapaan. Käyttäjälle ei myöskään tule virheilmoituksia. Ongelma ilmenee etenkin järjestelmän WMI-rajapintatasosta riippuvaisten sovellusten vajaana toimintana. Tällaisia sovelluksia ovat esimerkiksi virustorjunnat ja SCCM-client. Viallisessa koneessa virustorjunta ei toimi, ja SCCM-client ei esimerkiksi suorita uusien sovellusten asennuksia. Koneella voi esiintyä muidenkin ohjelmien ja palveluiden kanssa mitä erikoi-

sempia ongelmia. Vaarantunut tietoturva ja viallisten koneiden havaitsemishaaste tekevät asiasta erityisen vaikean. Ongelma selvisi tutkimalla koneita, joille kytketyt sovellusjakelut eivät asentuneet.

5.2.1 Ongelmien seuranta

Ongelman havaitsemisen jälkeen tutkin, mikä Windows-lokimerkintä viittaa kyseiseen virheeseen. Tämän jälkeen tein CMD-skriptin, joka lokittaa WMI-errors -verkkojakokansioon koneennimen mukaiseen tiedostoon päivämäärän ja kellonajan. Skriptiä varten tein Task Scheduler -ajastuksen. Määritin ajastukselle XML:llä Custom triggerin, joka käynnistää skriptin kun Windows Event -lokiin tulee WMI:tä koskeva virhemerkintä. Verkkolevylle kertyvien tiedostojen nimestä näkee, millä koneilla virheitä on ollut. Sisällöstä selviää virheen esiintymisajat ja lukumäärät. Tiedostojen lukumäärästä puolestaan voi seurata kuinka monella koneella virhettä on havaittu. Jaoin ajastuksen ja skriptin työasemille SCCM-sovellusjakelun kautta. Virheitä esiintyi odotettua enemmän, ja myös sellaisilta koneilla, jotka toimivat normaalisti. Asian tutkimisessa selvisi, että Microsoft on jättänyt Windows-käyttöjärjestelmään WMI false positive -virheen. Ohjelmistokehittäjät ovat käyttäneet virhettä Windows-kehitysvaiheessa debuggaus-tarkoituksessa. False postive -virheilmoitusten poistamiseen löytyi Microsoftilla korjausohjeet. (Microsoft 2016b.)

Teimme skriptin ohjeen mukaan ja jaoimme sen SCCM-sovellusjakelun kautta koneille. Tämän korjauksen jälkeen lokit alkoivat pitää paikkansa. WMI-virheitä kuitenkin tuli edelleen satunnaisesti myös ehjiltä koneilta. Tämä johtuu ilmeisesti siitä, että kaksi eri sovellusta tai ohjelmaa yrittävät käyttää samaa tietovaraston kohtaa samanaikaisesti. Nämä tapaukset pystytään huomaamaan lokeista siitä, että virhe esiintyy vain kerran eikä uusia rivejä kerry lokiin. Havaitsimme lokeja seuraamalla, että viallisia koneita oli HAMKin ympäristössä yli kolmesataa. Lisää viallisia työasemia tuli noin yksi kone päivässä.

5.2.2 Ongelmien automaattinen korjaus

Saadun tutkimustiedon perusteella aloin selvittämään tapaa korjata WMI-vialliset koneet automaattisesti. Usein pelkkä WMI-tietovaraston korjausajo ei riittänyt, vaan se täytyi nollata kokonaan. Tietovaraston uudelleenrakentaminen vie Windowsilta paljon aikaa. Kesto riippuu työaseman ja etenkin sen kiintolevyn nopeudesta.

Tein tietovaraston uudelleenrakentamista varten PowerShell-skriptin. Myös tämä skripti käynnistyy Task Schedulerin kautta WMI-virheen sattuessa. Se tarkistaa verkkolevypalvelimella olevasta WMI-Errors -kansiosta löytyykö sieltä koneen nimellä olevaa tiedostoa. Mikäli tiedosto löytyy, tiedoston viimeiset kolme riviä tallennetaan muuttujaan. Mikäli rivejä on alle kolme, tai viimeiset kolme riviä sisältävät tiedon tehdystä WMI-korjauksesta, kirjoitetaan vain lokimerkintä tiedostoon. Jos rivejä on kolme eikä niiden aikana ole nollattu WMI-tietovarastoa, se nollataan. WMI-Errors lokiin kirjoitetaan ajan lisäksi tieto WMI-nollauksesta. Tämä skripti jaettiin koneille SCCM Application -jakeluna. Se korvasi aiemmin luomani WMI-virheiden seurantaskriptin.

SCCM Distribution point -palvelimelle tehtiin ajastus, joka poistaa WMI-Errors -kansiosta tiedostot, joita ei ole muokattu yli kahteen kuukauteen. Tällä saatiin karsittua pois satunnaisista virheistä aiheutuvat turhat tietovaraston tyhjennykset. Skripti laitettiin ajettavaksi Task Schedulerin kautta samalla XML-triggerillä, jonka olin tarkistusta varten luonut. Task Schedulerin kautta ajettavan skriptin ansiosta työasemat korjaavat automaattisesti WMI-tietovaraston, mikäli siinä on vikaa. WMI-ongelmaa esiintyy vähemmän Windows 10 kuin Windows 7 -käyttöjärjestelmässä. Tarkkoja määriä on vaikea sanoa, koska lokitiedostot poistuvat nykyisin automaattisesti.

5.3 **Toimintavarmuuden parantaminen**

Sccm-client menee koneen asennusvaiheessa provisiointitilaan. Provisiointitila suojaa, ettei Task Sequence -vaiheessa koneelle asennu Sequencen ulkopuolisia asennuksia. Jostain syystä työasemat kuitenkin menevät joskus provisiointitilaan myös Task Sequencen ulkopuolella. SCCM-client ei suostu tekemään asennuksia, mikäli kone on tuossa tilassa. Myöskään SCCM-asetukset eivät päivity, kone ei myöskään päivitä SCCM-tietokantaan tietojaan. Työasemat eivät poistu itsestään tuosta tilasta, vaan ne pitää määrittää normaalitilaan kahdella rekisterimerkinnällä. (Gary Blok 2018.)

Määritimme kahdella Group Policy -asetuksella provisiointitilan pois päältä. Kyseiset Group Policyt eivät saa kuitenkaan mennä päälle kesken Task Sequencen. Asetimme Group Policy -asetuksiin rajoituksen, että koneella pitää olla VDI-client asennettuna. Se asennetaan HAMKn Task Sequencessä viimeisenä. Tällä estettiin, ettei kone poistu provisiointivaiheesta liian aikaisin.

Aika ajoin esiintyi myös ongelmaa, jossa työaseman Active Directory -luottosuhteet olivat rikkoutuneet. Luottosuhteiden rikkoutuessa koneelle ei

pääse kirjautumaan. Ongelma poistuu, kun koneen poistaa AD:sta ja nostaa sen sinne takaisin. Tutkiessamme syytä ongelmaan työasemien lokeista, havaitsimme kahdenlaisia tapauksia. Mikäli kone on nimetty samalla nimellä, kun järjestelmässä jo oleva kone, kummankin luottosuhteet menevät rikki. Tämän ongelman korjaamiseksi opastimme ylläpitäjiä tarkistamaan konetta nimetessään, ettei järjestelmässä ole saman nimisiä koneita.

Toisenlaisissa tapauksissa kone oli palauttanut varmuuskopion. Varmuuskopiossa oli vanha työaseman salasana, jolla työasema ei voinut autentikoitua AD-palvelimelle. Poistimme System Restoren käytöstä GPO-asetuksilla, mutta tämä ei kuitenkaan poistanut vielä kokonaan näitä tapauksia. Teimme vielä CMD-skriptin joka poistaa shadow copies -varmuuskopiot koneelta. Jaoimme skriptin SCCM-sovellusjakeluna koneille. Tämän jälkeen ongelmia ei ole ilmennyt.

6 SCCM-TIETOKANTADATAN HYÖDYNTÄMINEN HAMKISSA

SCCM tietokanta pitää sisällään erittäin paljon tietoa työasemista, työasemaympäristöstä, ohjelmista ja niiden käytöstä. SCCM-raportointi sisältää lähes 500 erilaista valmista raporttia, joista saa paljon hyödyllistä tietoa ympäristöstä ja sen käytöstä. Tietokannassa on kuitenkin paljon myös sellaista tietoa, jonka hyödyntämiseen ei ole valmiita raportteja tai tapaa. Vain mielikuvitus ja työn hyötysuhde ovat rajana, mihin kaikkeen tietoa voi hyödyntää.

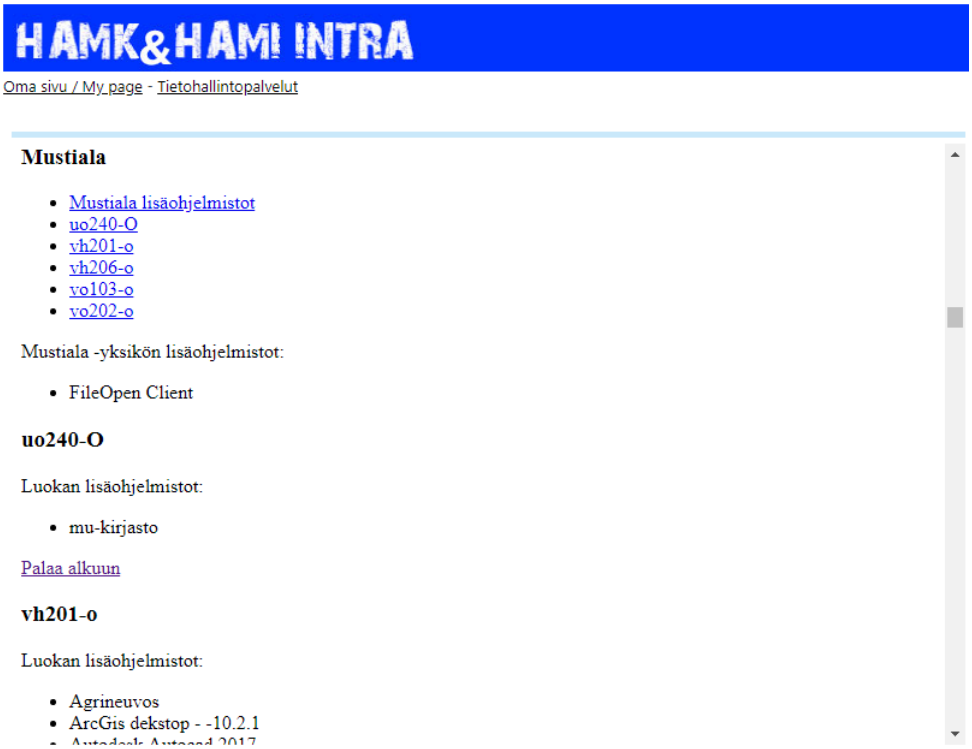
Hämeen ammattikorkeakoulussa on enenevässä määrin alettu hyödyntämään olemassa olevaa tietoa. Myös päätelaitehallinnan osalta etsittiin tapoja saada dataa hyödyntämällä lisäarvoa käyttäjille, säästöjä ja helpotusta työmäärään. Kävin Sovelton SQL Server Reporting Services -kurssin, josta sai hyvän perusymmärryksen SQL-tietokannoista, sekä raportoinnista (Sovelto 2015).

6.1 Sovelluslistaus

Tampereen teknilliseltä yliopistolta saatiin järjestelmäasiantuntija Jaakko Luodon tekemä PowerShell-skripti, joka tekee sovelluslistauksen SCCM-jakelukytkentöjen perusteella. Skripti ei suoraan sellaisenaan ollut käyttökelpoinen, johtuen eri tavalla suunnitellusta ympäristöstä ja hierarkiasta. Käytin Jaakon tekemää scriptiä pohjana ja tein HAMKin päätelaiteympäristöön sopivan skriptin. Pohjana ollut noin 170-rivinen skripti kasvoi noin 350-riviseksi. Rivimäärien kasvu johtui siitä, että HAMK-päätelaiteympäristössä SCCM-Collection -hierarkia on useampi tasoinen, kuin Tampereen teknillisessä yliopistossa. Useampaa tasoa varten skriptiin täytyi rakentaa lisää logiikkaa.

Skripti käy SCCM-tietokannasta läpi kaikki HAMKn yksikkö-, rakennus- ja luokkakohtaiset Collectionit, sekä Collectionit, joihin kaikki koneet kuuluvat. Skripti katsoo näille kytkettyjen sovellusjakeluiden nimet, ja rakentaa tämän pohjalta kullekin luokalle sovelluslistauksen asennetuista sovelluksista. Sovelluslistaukset tulevat loppukäyttäjien käyttöön, joten kaikkia jakeluita ei haluta esittää sovelluslistauksessa (esimerkiksi korjauksia, asetuksia ja päivityksiä, jotka eivät ole itsenäisiä ohjelmistoja). Jakelut joiden lisätietokentässä on merkkijono #private, updates, settings, fix tai uninstall suodatetaan pois listauksesta. Jakeluiden nimissä voi myös olla merkkijonoja, jotka halutaan suodattaa pois. Skripti suodattaa tällaiset merkkijonot pois nimestä, mutta ei poista sovellusta kokonaan listauksesta. Tämän jälkeen skripti muodostaa kuvassa 8 esitetyn HTML-sivun. Sivulle on listattu kussakin luokassa olevat sovellukset, ja se sisältää ankkurit ja sisällysluettelon navigoimisen helpottamiseksi. Lopuksi skripti julkaisee HTML-sivun HAMKn sisäisille sivuille, joista se on opiskelijoiden ja henkilökunnan luettavissa. Skripti on ajastettu SCCM Distribution Point -palvelimelle ajetta-

vaksi joka perjantai-iltana. Ajo kestää yli puoli tuntia. Ajastuksen olisi voinut laittaa joka päivälle, mutta kerran viikossa nähtiin riittävän ajantasaiseksi tiedoksi käyttäjille. Sovellusjakelukytkentöihin ei tule merkittävän paljon muutoksia viikossa. HTML-sivu antaa käyttäjille lisäarvoa, kun hän pääsee helposti katsomaan tarvitsemiensa sovellusten sijainnin.



Kuva 8. PowerShell-skriptin luoma HTML-sivu luokkien sovelluksista.

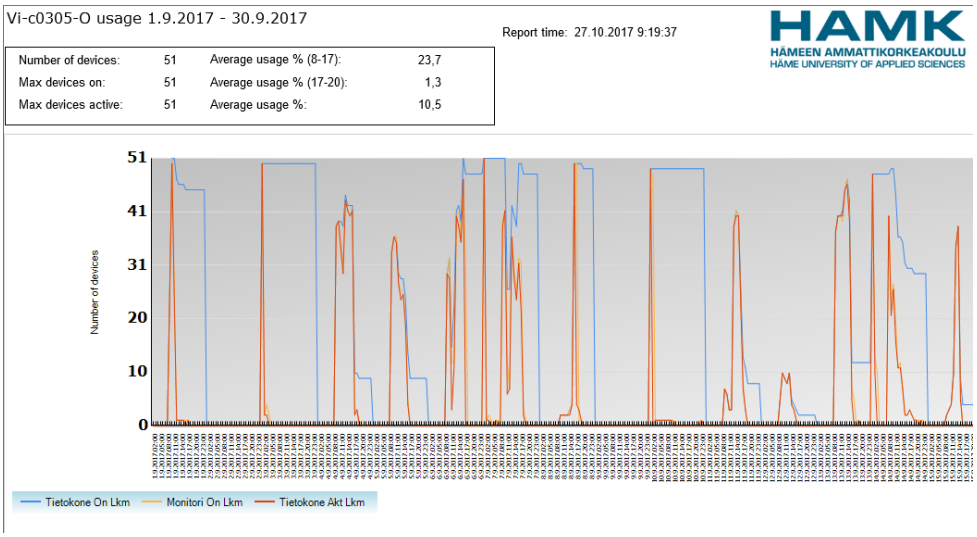
6.2 **Käyttöasteseuranta**

Hämeen ammattikorkeakoulussa tietokonehankinnat ovat aikaisemmin perustuneet enemmän tai vähemmän arvioon ja kokemukseen. Päätöksenteon tukena ollut tieto on rajoittunut aikaisempiin kokemuksiin ja tuleviin koulutuksen muutoksiin, kuten koulutusohjelmiin sisään otettavien opiskelijoiden määriin. Päätöksenteon tueksi tarvittiin tietoa koneiden käytön määristä, mutta tähän ei ollut mitään valmista ratkaisua.

6.2.1 Raportointi SCCM-tietokannasta

SCCM-tietokannan sisältämiä SQL-tietokantatauluja tutkimalla havaitsin niiden sisältävän tietoa koneiden käynnissä olo- sekä käyttöajoista. Tämän tiedon hyödyntämiseen ei SCCM tarjonnut valmiita raportteja. Rakensin oman raportin SQL Reporting Services -työkalulla. Suunnittelin raportin siten, että se listaa valitun luokan tai tilan työasemien käyttömäärät valitulta ajanjaksolta (kuva 9). Käyttäjä voi ottaa raportin mistä tahansa Collectionista valitsemallaan aikavälillä. Raportissa ilmenee tilan nimi, valittu aikaväli, raportin ajoaika, tilassa olevien työasemien lukumäärä, maksimi määrät päällä ja aktiivisena olleista koneista, käyttöasteet prosenttilukuina

sekä tilastografiikka koneiden toiminnasta valitulla ajanjaksolla tunnin tarkkuudella. Prosentuaaliset käyttöasteluvut ovat erikseen päivä-, ilta- ja kokonaiskäytöstä.



Kuva 9. Vi-c0305-O luokan käyttöasteraportti syyskuulta 2017.

Raportista selviää, kuinka montaa konetta luokassa yleensä käytetään yhtä aikaa, kuinka usein luokkaa käytetään ja kuinka suurella käyttömäärällä luokka on. Grafiikasta voi myös seurata, millaista luokan käyttö tavallisesti on, eli kuinka monta tuntia koneita käytetään yhtämittaisesti, ja minkä verran tila on vapaana. Grafiikassa Y-akselilla on koneiden määrä ja X-akselilla on valittu aikajakso tunneittain. Sininen viiva kuvaa päällä olevien koneiden määrää. Punainen viiva kuvaa aktiivisten koneiden määrää. Aktiivinen kone tarkoittaa konetta, jota käyttäjä on käyttänyt kyseisen tunnin aikana. Keltainen kuvaa monitorin päällä oloaikaa, joka tiedoista on vähiten kiinnostava. Grafiikasta voi seurata koneiden toimintaa, ja poikkeamia tunnistamalla havaita viallisia tai jopa haittaohjelman saastuttamia koneita. Tein PowerShell-skriptin, joka päivittää koneiden käyttöastetiedot kannassa ajan tasalle. Ajastin työasemien Task Scheduleriin skriptin ajamisen jokaisen kuukauden viimeisenä päivänä, jotta tiedot olisivat tietokannassa kuukauden alussa ajan tasalla. Ajastus jaettiin koneille SCCM-sovellusjakelun kautta.

6.2.2 Datan ja raportoinnin siirto tietovarastoon

SCCM-tietokanta taltioi koneiden käyttödataa vain kuukauden ajalta. Monen SCCM-datan säilytysaikaa voi muuttaa asetuksilla, mutta käyttödataa ei voinut. Sen vuoksi tein aluksi SQL Reporting Services tilauksen jokaisen luokan käyttöasteraportista kuukauden ensimmäiselle päivälle. Lisäksi tilasin kunkin toimipaikan opiskelijapuolen koneiden raportit, jotta yksiköiden kokonaiskuvaa voidaan tarkkailla. Rajoittavaksi tekijäksi nähtiin, että jälkikäteen dataa ei enää ollut olemassa, kuin ainoastaan tilattujen Collectioneiden osalta staattisessa MHTML-muodossa.

Päätimme siirtää datan tietovarastoomme, josta sitä voisi jälkikäteen hyödyntää. Datan talteenottoa varten SCCM-kantaan rakennettiin SQL-proseduuri, joka tarjoaa kantaan tätä varten tehdylle näkymälle datan oikeassa muodossa. Tietovarastoon teimme ajastuksen tietojen hakemiselle päivittäin SCCM-kannasta pysyvään talteen. Tämän jälkeen siirsin SCCM-kantaan tekemäni raportit käytettäväksi myös tietovarastopalvelimelle.

6.2.3 Raportointi päätöksenteon tukena

Nykyisen raportoinnin lukeminen vaatii hyvän ymmärryksen ympäristöstä ja raportista. Lukeminen on melko työlästä. Kokonaan käyttämättömät koneet on helppo havaita numeroista. Pelkät numerot eivät kuitenkaan kerro tilan käytöstä todellista kuvaa. Sen lisäksi tulee tarkkailla grafiikasta, miten luokkaa on käytetty, jotta havaitaan harvoin käytössä olevien koneiden määrä, sekä tilan yleinen käyttötapa. Raportteja joudutaan myös vertailemaan keskenään, jotta saadaan käsitys miten viereiset luokat ovat olleet samaan aikaan käytössä. Työmäärään vaikuttaa raporttien suuri määrä. Esimerkiksi vuoden 2017 raportteja on yhteensä 624 kappaletta. Väärintulkintojen ja suuren työmäärän vuoksi johdolle tulee laatia raportoinnista yhteenveto päätöksenteon tueksi. Kuvassa 10 on esimerkki yhden luokan vuoden 2017 yhteenvedosta.

vi-c0305
Koneita: 51
Käyttöaste: (13,4%)
Käytössä:
51 = 4 tuntia vuodessa
42 = 45 tuntia vuodessa
38 = 102 tuntia vuodessa
24 = 421 tuntia vuodessa
Ehdotus: Koneiden määrää voisi pienentää 43kpl:n. Tuo käyttömäärä ylitetään harvoin (30 tuntia vuodessa). Maltillinen vähennys olisi 47 koneeseen.

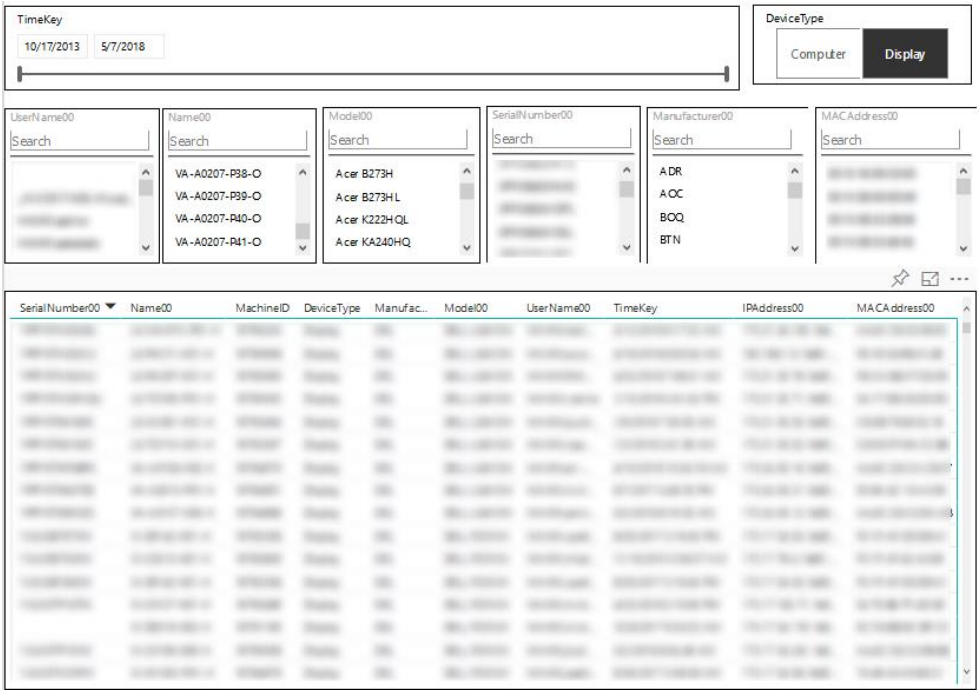
Kuva 10. Vi-c0305 luokan vuoden 2017 käyttömäärän yhteenveto investointeja varten.

Raportoinnin hyödyntämisellä on saavutettu laiteinvestoinneista useiden kymmenien tuhansien eurojen säästöt vuosittain. Raportoinnin jatkokehittämisestä on alkamassa Power-BI-projekti. Projektin tarkoitus on rakentaa raportointi helpommin luettavaksi, jotta raporttiin vähemmän tutustunut saisi työasemien käytöstä hyvän käsityksen. Ajatuksena on rakentaa Dash Board -tyylinen raportti, josta selviää tieto oleellisista asioista. Raportin tietoja klikkaamalla pääsee kyseisen asian tarkempaan raporttiin.

6.3 **Laiterekisteri**

Työasemamäärällisesti isoissa ympäristöissä on joskus vaikea seurata etenkin kannettavien tietokoneiden sijaintia. Inhimillisten syiden ja koneiden siirtojen vuoksi välillä on työlästä etsiä laitteita, joiden leasingaika on päättymässä. Asiaa joudutaan kysymään useilta henkilöiltä, ja tarkistamaan useammasta tietojärjestelmästä. Pahimmillaan tämä on erittäin paljon työaikaa vievää, ja leasing-aikaa saatetaan joutua pidentämään myöhästyneen palautuksen vuoksi.

Asian helpottamiseksi suunnittelin tietokantataulun, jossa olisi kaikki mahdollinen tieto, mikä voi helpottaa laitteen paikantamista. Tauluun tallennetaan laitteen sarjanumero, nimi, SCCM-ID, laitteentyyppi, valmistaja, malli, koneelle viimeksi kirjautunut käyttäjä, viimeisen havainnon aika, IP-osoite ja MAC-osoite. Loin SCCM-tietokantaan näkymän, joka sisältää nämä tiedot. Tietovarasto käy päivittäin hakemassa tiedot, jotta tieto saadaan pysyvään tietovarastoon. SCCM poistaa omasta tietokannastaan koneen tiedot, mikäli kone poistuu järjestelmästä. Laajensimme Active Directoryn SCCM-schemaa, jotta saimme myös näyttöjen tiedot tallentumaan SCCM-tietokantaan. Työasemille on jaettu skripti, joka päivittää siihen kytkettyjen näyttöjen tiedot SCCM-tietokantaan.



Kuva 11. Power-BI:llä toteutettu käyttöliittymä koneiden sijainnin selvittämiseksi.

Kuvassa 11 on esitetty Power-BI:llä tehty raportti, jolla koneiden sijaintia voi jäljittää. Raportilla voi etsiä koneita kaikilla tietovarastossa olevilla tiedoilla. Yleensä tiedossa on sarjanumero. Tämän tiedon avulla saadaan selville koneen IP-osoite, joka kertoo missä VLAN-verkossa kone on viimeksi havaittu ja milloin. Myös viime käyttäjä selviää, sekä koneen nykyinen

nimi. MAC-osoitteen perusteella on myös mahdollista jäljittää koneen sijainti verkosta. Raportti helpottaa koneiden sijainnin selvitystyötä ja säästää siten työaikaa.

7 LOPPUTULOS

Työasemaympäristön kehittämiselle oli asetettu paljon tavoitteita. Projekti onnistui täyttämään projektille asetetut tavoitteet erittäin hyvin. Kaikki oleelliset tavoitteet saavutettiin heikentämättä mitään palveluja. Palvelun taso nousi monelta osin toimintavarmemman ympäristön ja paremmin suunniteltujen käytäntöjen ansiosta.

Työasemaympäristön tavanomaista toimintaa onnistuttiin rakentamaan automaattisemmaksi sekä entistä vakaammaksi itsestään korjaantuvuudella. Kattavalla työasemaympäristön suunnittelulla saatiin automatisoitua koneiden ja sovellusten asennukset sekä asetukset erittäin pitkälle. Automatisoinnissa merkittävässä roolissa toimi koneiden nimeämiskäytäntö. Työasemat vaativat vain vähän manuaalista työtä, josta suurin osa aiheutuu viallisesta laitteistosta. Esimerkiksi ohjelmia ei ole tarpeen asentaa koneille käsityönä käytännössä ollenkaan. Työasemilla esiintyy vain vähän ongelmia useiden automatisoitujen itsekorjaantuvuus toimien ansiosta. Myös automatiikan ylläpito vie minimaalisesti työaikaa hyvin suunnitellun ympäristön ansiosta. Näiden toimenpiteiden ansiosta ylläpitoon vaadittu työmäärä on vähentynyt, ja ylläpitäjillä on jäänyt enemmän aikaa loppukäyttöopastuksen kasvaneeseen tarpeeseen.

Käyttäjille pystyttiin tarjoamaan itsepalvelumahdollisuuksia tarjoamalla heidän tarvitsemansa ohjelmat HAMK-sovelluskaupan kautta suoraan työpöydälle. SCCM-jakeluita ei kuitenkaan tehdä sovelluksista joita asennetaan alle kahdeksan kertaa. Joustavuuden vuoksi käyttäjille tarjottiin myös mahdollisuus suorittaa asennuksia ja komentoja korotetuin käyttöoikeuksin. Tähän käytetyllä tunnuksella käyttäjä ei kuitenkaan pysty kirjautumaan koneelle. Tämän ansiosta se on huomattavasti tietoturvallisempi ratkaisu kuin paikallisen pääkäyttäjätunnuksen luovuttaminen käyttäjälle. Hyvin suunniteltujen käytäntöjen ja huoltoikkunan ansiosta voitiin tarjota parempi käyttäjäkokemus. Sovellukset ja päivitykset kun asentuvat pääosin huoltoikkunoissa yöaikaan käyttäjiä häiritsemättä.

Ympäristön datasta saatiin luotua huomattavaa lisäarvoa loppukäyttäjille, ylläpitäjille sekä päättäjille. Lisäarvoa saatiin luomalla uusia tapoja rikastuttaa, laajentaa ja käyttää dataa. Työasemien käyttöseurannalla on saavutettu tuntuvia vuosittaisia säästöjä tehostamalla työasemien käyttöä. Palvelun laatuun säästöt eivät käytännössä ole vaikuttaneet ollenkaan.

Työasemaympäristö elää jatkuvassa muutoksessa sovellusten ja niiden versioiden suhteen. Aika ajoin ilmenee uusia ongelmia, jotka vaativat ongelman syyn ja mahdollisen korjauksen selvittämistä. Lopullisesti valmiiksi ympäristöä ei tämän vuoksi voida saada. Tällainen tilanne tuli esimerkiksi viimeisen SCCM-päivityksen jälkeen. SCCM ei enää asenna automaattisesti saatavilla-määrityksellä jaettuja sovelluksia huoltoikkunassa. Vaikka tieto-

kone heräisi HAMK-huoltoikkunoihin saatavilla-määrityksen jälkeen, asennus tapahtuu vasta deadline-ajan täytyttyä. Ongelma havaittiin SCCM-versio 1710 -päivityksen jälkeen. Ongelma aiheuttaa lisääntyneen määrän työaseman käytönaikaisia sovellus- ja päivitysasennuksia, jotka voivat hidastaa koneita. Käyttäjille voi myös tulla normaalia enemmän uudelleenkäynnistyspyyntöjä. Ongelman syystä tai korjauksesta ei vielä löytynyt enempää tietoa.

Työasemien käyttöastedatan hyödyntämisestä on alkamassa jatkokehitysprojekti. Projektin tavoite on luoda tietovaraston käyttöasteseurannan raportointi Microsoft Power-BI -alustalle. Raportoinnista on tarkoitus luoda helposti tulkittava Dash Board -tyylinen näkymä, josta ylläpitäjät sekä päättäjät pääsevät itse näkemään tarvitsemansa tiedon. Dash Board -päänäkymästä näkisi merkittävimmät asiat koskien ympäristön käyttöasteita. Dash Board -mittareita painamalla pääsisi katsomaan tarkemman raportin valitsemastaan asiasta. Tällaisia mittareita voisi olla esimerkiksi pienimmällä käytöllä olevat tietokoneluokat, luokat jossa eniten käyttämättömiä koneita ja luokat joissa vähiten päällekkäisiä tunteja viereisten luokkien kanssa. Projekti on kuitenkin vasta aluillaan ja suunnittelutyö on kesken. SCCM-tietokannasta löytyy myös sovelluksista samankaltaista käyttöasteseurantadataa kuin työasemista. Myös tämän tiedon hyödyntämisen etuja on pohdittu.

LÄHTEET

Datasynergy (2018). Wake-on-LAN Explained. Luettavissa: http://www.datasynergy.co.uk/products/wakeman/pdfs/Wake-on-LANExplained.pdf

Gartner (2015). Gartner Magic Quadrant for Client Management Tools. Luettavissa: https://www.gartner.com/doc/3073718/magic-quadrant-client-management-tools

Gary Blok (2018). ConfigMgr Client Provisioning Mode. Luettavissa: https://garytown.com/configmgr-client-provisioning-mode

John Devit (2015). AD GPOs or ConfigMgr 2012 Compliance and Settings?. Luettavissa: https://www.1e.com/blogs/2013/08/02/ad-gpos-or-configmgr-2012-compliance-and-settings/

Microsoft (2015a). Microsoft TechNet, System Center Configuration Manager TechCenter, Documentation Library for System Center 2012 Configuration Manager, Getting Started with System Center 2012 Configuration Manager, Introduction to Configuration Manager. Luettavissa: https://technet.microsoft.com/en-us/library/gg682140.aspx

Microsoft (2015b). Microsoft TechNet, Library, System Center, System Center 2012 R2 and System Center 2012, Configuration Manager, Technical Reference for Ports Used in Configuration Manager. Luettavissa: https://technet.microsoft.com/en-us/library/hh427328.aspx

Microsoft (2016a). Microsoft Docs, System Center 2012 R2 and 2012, Configuration Manager, Introduction to Application Management in Configuration Manager. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg682125%28v%3dtechnet.10%29

Microsoft (2016b). Microsoft Support, Event ID 10 is logged in the Application log after you install Service Pack 1 for Windows 7 or Windows Server 2008 R2. Luettavissa: https://support.microsoft.com/en-us/help/2545227/event-id-10-is-logged-in-the-application-log-after-you-install-service

Microsoft (2017). Microsoft Docs, Enterprise Mobility + Security, Configuration Manager, Core infrastructure, Manage clients, Collections, How to use maintenance windows in System Center Configuration Manager. Luettavissa: https://docs.microsoft.com/en-us/sccm/core/clients/manage/collections/use-maintenance-windows

Microsoft (2018a). Microsoft Docs, Windows Server, Networking, BranchCache. Luettavissa: https://docs.microsoft.com/en-us/windows-server/networking/branchcache/branchcache

Microsoft (2018b) Microsoft Docs, Enterprise Mobility + Security, Configuration Manager, Core infrastructure, Deploy clients, Client deployment tasks, About client settings. Luettavissa: https://docs.microsoft.com/en-us/sccm/core/clients/deploy/about-client-settings

Microsoft (2018c). Microsoft Developer Network, Windows Desktop App Development, Develop, Server Technologies, System Administration, Windows Management Instrumentation. Luettavissa: https://msdn.microsoft.com/en-us/library/aa394582(v=vs.85).aspx

Sovelto (2015). SQL Server Reporting Services -koulutus.