Jarkko Tolonen

Lokitiedon merkitys käyttöjärjestelmän asennuksessa SCCM-ympäristössä

Tietojenkäsittely

Kevät 2017

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

TIIVISTELMÄ

Tekijä: Jarkko Tolonen

Työn nimi: Lokitiedon merkitys käyttöjärjestelmän asennuksessa SCCM-ympäristössä

Tutkintonimike: Tietojenkäsittelyn koulutusohjelma

Asiasanat: lokitiedot, SCCM

Lokien avulla kerätään tietoa systeemin prosesseista. Lokitietoa kerätään sekä laitteistosta kuin myös ohjelmistoista. Loki sisältää usein aikaleiman, käyttäjätiedon, systeemin käyttötarkoituksen, virheilmoituksia ja varoituksia. Lokeja hyödynnetään järjestelmän käytön analysoimiseen jälkikäteen tai lähes reaaliajassa. Lokitietoa voidaan käyttää hyväksi, kun tutkitaan ulkopuolisen käyttäjän tunkeutumista järjestelmään. Lokeja voidaan käyttää myös järjestelmän käyttäjän tukena, jos epäillään väärinkäytöksiä organisaation sisällä. Lokien tulisi sisältää merkityksellistä tietoa, eikä niiden tulisi haitata työntekoa.

Miksi lokeja kerätään? Usein lokitieto on ainoa paikka, johon tunkeutuja jättää jälkiä. Järjestelmän ylläpitäjän tulee tiedostaa, ettei lokeja synny aina automaattisesti. Lokitieto tulisi tallentaa niille tarkoitettuun palvelimeen salatun linjan avulla. Lokien lähettämiseen koneelta toiselle tulisi käyttää mahdollisimman vähän verkkolaitteita. Joissain tapauksissa tunkeutuja voi aiheuttaa lokitiedoston merkittävän koon kasvun, joten lokeja varten tulee olla varattuna tarpeeksi tilaa.

Organisaatiossa lokeja varten tulisi olla eri ylläpitäjä kuin varsinaisella systeemillä. Lokitieto voi sisältää henkilökohtaista tietoa käyttäjistä, mikä tulee ottaa huomioon lokien käsittelyssä. Kaikilla lokitiedoilla tulee olla sama aikaleima, jotta lokeja voidaan verrata toisiinsa. Usein organisaatio keskittyy epäonnistuneisiin kirjautumisiin, mutta myös onnistuneet kirjautumiset lokeissa tulisi ottaa huomioon. On mahdollista, että tunkeutujalla on tarvittava tieto kirjautua järjestelmään, mikä näkyy normaalina käytöksenä järjestelmässä.

Tämä opinnäytteen tavoite on tutkia SCCM:n avulla toteutetun käyttöjärjestelmäasennuksen synnyttämiä lokitietoja ja niiden hyödynnettävyyttä. SCCM on ohjelmistokokonaisuus, jota organisaatio voi käyttää ohjelmistojen keskitettyyn hallintaan. SCCM kerää automaattisesti lokeja, myös käyttöjärjestelmien asentamisesta, ja tässä työssä pyritään selvittämään kyseisten lokien hyöty lähinnä ongelmatilanteissa. Käyttöjärjestelmä asennetaan Zero Touch asennuksena siten, että käyttöjärjestelmän lisäksi SCCM:n avulla asennetaan samalla halutut ohjelmistot. Zero Touch asennus tarkoittaa, ettei käyttäjä ole interaktiossa asennukseen. Zero Touch asennus on hyödyllinen suurissa organisaatioissa, mutta helpottaa IT-osaston ylläpitotöitä pienemmässäkin mittakaavassa.

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Author: Jarkko Tolonen

Title of the Publication: Relevance of Log Files in Installing Operating System in SCCM

Degree Title: Business Information Technology

Keywords: logs, SCCM

Log is a part of the system that collects information about system's processes. Logs are collected from hardware and software. Log in a computer world includes a timestamp, a user information, purposes the system was used, errors and warnings. Log files can be used for analyzing a data usage afterwards. Log file is also used as an evidence in a case where some unwanted outsider has been intruded into the system. Also, log can be an evidence for a normal user that has done nothing wrong. Logs should include only information that matter for an organization and they should not produce any harm for normal users.

Why to record events? In many cases logs are only places where hacker leaves track behind. Administrator also should remember that logs are not always automatically been recorded. It is best practice to put log files into a dedicated server trough a secure line. When sending logs to another computer administrator should use as little as possible number of hardware. And in some cases, hacker can cause an increase of log file sizes, so there must be enough space to handle the attack.

In an organization, there should be a different administrator for analyzing log files than the system administrator. Log files can include some personal data of users so it must be considered. Log files should be synchronized so that the timestamp do not differ from another. Typically, organization focus on failed login attempts but not succeed logins which are at least equally important. If a hacker already knows the specific password and the username then administrator can't see it from failed logins.

In this thesis the main point is to investigate correlation between installing operating system with SCCM and log files. SCCM is a system that organization's IT-management can use for centralized software deployments. SCCM gathers automatically many logs from installing operating system and this work tries to give good sight what logs are beneficial for a user. Installing operating system, Windows 10 in this work, has been accomplished with Zero touch installation with multiple software integrated into the installation. Installing operating system with Zero touch installation means that installer don't need to interact in any way. Zero touch installation is also called High-Volume Deployment, but in this work number of target computers is below 50.

SISÄLLYS

SYMBOLILUETTELO

Active Directory(AD): on Microsoftin luoma suojattu, strukturoitu, hierarkkinen tiedon tallennuspaikka verkon objekteille, joita voivat olla käyttäjät, tietokoneet, tulostimet ja palvelut. (Microsoft 2017a).

Asennusmedia: on joko fyysinen tai virtuaalinen media, jonka avulla voidaan asentaa käyttöjärjestelmä tai jokin ohjelmisto.

Asiakaskone(client): on kone, johon on asennettu asiakaskoneohjelmisto, jonka avulla asiakaskone on yhteydessä palvelua ylläpitävään kokonaisuuteen, tässä työssä SCCM:ään. (Microsoft 2007; Microsoft 2017e.)

Deployment: tarkoittaa ohjelmiston käyttöönottoa. Käyttöönotto voidaan suorittaa joko paikallisesti tai verkon välityksellä esimerkiksi Microsoft Deployment Toolkitin avulla. (Microsoft 2013e.)

DHCP: on asiakaskoneen ja palvelimen välinen protokolla, jonka avulla asiakaskone saa automaattisesti verkkoasetukset, kuten IP-osoitteen, aliverkonpeitteen sekä yhdyskäytävän. (Microsoft 2013f.)

Group Policy Object(GPO): on asetuskokonaisuus, jonka avulla asetus voidaan kohdistaa useaan AD-ympäristön objektiin samanaikaisesti. GPO:n avulla voidaan esimerkiksi säätää AD-ympäristössä käyttäjien käyttöoikeuksia ryhmittäin. (Microsoft 2011.)

Levykuva: on tietokoneen kiintolevyn, levyosion tai muun levyn sisällöstä ja rakenteesta tehty tiedosto. Levykuvaa voidaan käyttää hyödyksi esimerkiksi käyttöjärjestelmän asennuksessa. Levykuva voidaan muuntaa fyysiseksi asennusmediaksi tai käyttää sellaisenaan virtuaaliympäristössä. (TSK, 2016.)

Loki: Sähköinen loki on tiedosto, johon tallentuu aikajärjestyksessä merkinnät tietojärjestelmän tapahtumista ja niiden aiheuttajista. Loki kertoo, kuka järjestelmää käytti, mihin tarkoitukseen ja mihin aikaan. (Andreasson & Koivisto 2013, 127; Männikkö 2008b.)

MAC-osoite: on laitteen yksiselitteinen verkko-osoite. (VAHTI 2009b.)

NTP-palvelin: on palvelin, jolla synkronoidaan verkon laitteiden aika. (VAHTI 2010, 72.)

Organization Unit (OU): on AD-ympäristön säilö, johon voidaan laittaa käyttäjiä, ryhmiä, tietokoneita ja toisia Organization Unitteja. OU on pienin AD-ympäristön yksikkö, johon voidaan kohdistaa GPO. (Microsoft 2008a.)

PXE-käynnistys: on Intelin kehittämä protokolla, joka on johdettu DHCP protokollasta. PXE-käynnistys on yhteydessä tietokoneen verkkokorttiin. PXE-käynnistyksen avulla voidaan asentaa käyttöjärjestelmä verkon kautta. (Microsoft 2008b.)

Powershell: on automaatioalusta ja skriptikieli Windows koneisiin ympäristön hallintaa varten. (Microsoft 2017h.)

Proxy: eli välityspalvelin on tietoverkon ja paikallisen järjestelmän välissä. Välityspalvelin voi toimia toimintaa nopeuttavana välivarastona tai turvapalvelimena. (VAHTI 2009b.)

SCCM: Microsoft System Center Configuration Manager on ohjelmistokokonaisuus, jonka avulla voidaan keskitetysti ylläpitää organisaation työpöytäympäristön ohjelmistopuolta. (Martinez & Daalmans & Bennett 2014, 1.)

SQL: tarkoittaa tietokantaa. Tietokanta on kokoelma yhteen liittyvää tietoa, joka on koottu yhtenäiseksi merkitykselliseksi kokoelmaksi, esimerkiksi opiskelijarekisteriksi. Tietokantoja käytetään suuren tietomäärän hallintaan. (Heikkinen, 2015.)

Task Sequence: tarkoittaa usea vaiheista tai usean tehtävän sisältävää asennusta komentokehoitetasolla ilman käyttäjän interaktiota. (Microsoft 2010b.)

UNIX: on käyttöjärjestelmä, jota alettiin kehitellä AT&T:n Bell laboratorioissa 1960-luvun lopussa. UNIX:n suosio on johtanut moniin eri versioihin. (Opengroup 2004.)

Zero-Touch Installation (ZTI): on termi, jota käytetään käyttöjärjestelmien asentamisesta ilman käyttäjän interaktiota asentamisen välivaiheisiin. (Microsoft, 2014a.)

1 JOHDANTO

Tutkimuksen aiheen valinta on prosessi ja aihe syntyy monien neuvottelu- ja harkintavaiheiden jälkeen. Yleensä tutkimuksen tekijällä ei ole liiaksi aikaa määrittää tutkimuksen aihetta, mutta toisaalta, tutkimuksen aihe ei yleensä ole myöskään ensimmäinen mieleen tullut aihe. Aiheen valinnassa voidaan käyttää seitsemää perusohjetta: työ tehdään kohtuullisessa ajassa, työstä ei tehdä elinikäistä projektia, työksi soveltumaton aihe vaihdetaan, mikään tutkimus ei ole virheetön, elämä jatkuu tutkimustyön jälkeenkin, tutkimuksesta voi viritä uusia mielenkiintoisia aiheita ja tutkimus on vain yksi näkökulma aiheeseen. Aiheeksi ei tulisi valita aihetta, joka on liian laaja tai sellainen, josta ei löydy lähdekirjallisuutta. Aihe ei myöskään saisi olla sellainen, joka ei avaudu tutkijalle, tai joka on liian emotionaalinen. Tutkimusaihe tulisi olla myös joltain osin tutkijalle tuttu entuudestaan, ettei tutkimusta tehdessä jouduta opettelemaan paljon uusia taitoja. (Hirsjärvi & Remes & Sajavaara 2004, 60 – 61, 74.)

Ajatus opinnäytteestä syntyi osittain jo vuoden 2015 keväällä Windows kurssin aikana Kajaanin ammattikorkeakoulussa. Windows kurssilla saimme tehtäväksi asentaa Windows 7 käyttöjärjestelmän mahdollisimman automatisoidusti. Windows kurssin aikana onnistuin asentamaan käyttöjärjestelmän verkon kautta kohdekoneeseen ilman interaktiota. Windows kurssissa on täten osittain perusta tämän työn SCCM osioon. Tutkin SCCM omalla ajalla koulun ohessa ja asensinkin SCCM Kajaanin ammattikorkeakoulun laboratorioon. SCCM mahdollistaa käyttöjärjestelmän asennuksen verkon kautta automatisoidusti ja auttaa hallitsemaan työasemia keskitetysti.

Ajatus lokien käsittelemistä syntyi ennen kesää 2016 valitessani lopullista aihetta opinnäytteelle. 2016 kesän jälkeen opintoihin kuului Ajankohtaisseminaari ja asiakirjoittaminen kurssi, johon tein seminaarityön lokitiedoista. Alun perin jo seminaarityön oli tarkoitus käsitellä SCCM ja lokitiedon välistä yhteyttä, mutta pelkästään lokitiedot aiheena oli laaja ja SCCM osio jäi seminaarityöstä pois. Seminaarityön teksti toimii lähes sellaisenaan tämän opinnäytteen teoriaosana lokitiedon suhteen. Työn aihe siis on pyörinyt ajatuksen tasolla jossain määrin opintojen alusta

asti. Työn aihepiiri oli entuudestaan tuttu ja siihen tarttuminen luonnollista. Aloittaessani harjoittelun tammikuussa 2017 pääsin asentamaan SCCM:n oikeaan tuotantoympäristöön ja pystyin samalla tekemään opinnäytetyn käytännön osan. Lokitietojen käsittely SCCM:n yhteydessä tuli lähes täysin uutena asiana, joten työn kautta oppi myös uutta.

Tekstillä on ainakin yksi otsikko, joka on työn nimi. Otsikon täytyy herättää lukijan mielenkiinto, sekä kertoa työn sisällöstä. Pääotsikoinnin lisäksi teksteissä usein käytetään myös useatasoisia väliotsikoita. Hyvä otsikointi auttaa lukijaa muodostamaan ennakkokäsityksen kyseisestä tekstistä. Otsikointiin ja niiden muotoiluun tulee käyttää riittävästi aikaa, koska se vaikuttaa erittäin paljon tekstin luettavuuteen. Sisällysluettelosta selviää hyvin tekstin johdonmukaisuus, tarkkuus ja kiinnostavuus, sekä sen sisällön eritasoiset suhteet. (Hirsjärvi & Remes & Sajavaara 2004, 287.)

Etukäteen tietämykseni tietojärjestelmän lokeista oli melko vähäistä. Olemme sivunneet useilla kursseilla lokien merkitystä IT-ympäristöissä, muttemme ole opinnoissa syventyneet aiheeseen. Kirjoitustyön aikana lokien ja lokitiedon laajuus osana tietojärjestelmää alkoi hahmottua. Lokit tulisi ottaa huomioon organisaatioissa jo järjestelmien suunnitteluvaiheessa. Lokeja voidaan myös kerätä järjestelmissä lähes kaikesta, niin itse laitteista kuin myös ohjelmistoista. Lokit ovat myös osa organisaation tietoturvaa, joten niiden merkitystä ei voi väheksyä missään tilanteessa. Työn aihe ja samalla nimi tarkentui lopulta koskemaan lokitietojen merkitystä käyttöjärjestelmän asennuksessa, tässä tapauksessa SCCM:ää käyttäen. Käyttöjärjestelmän, tässä työssä Windows 10 käyttöjärjestelmä, asennetaan mahdollisimman automaattisesti SCCM:ää käyttäen. Työn nimi viittaa lokitiedon hyödyntämiseen käyttöjärjestelmän asennuksessa ja työn päätavoitteista on auttaa lukijaa ymmärtämään, mitä lokeja SCCM:n yhteydessä kannattaa tutkia käyttöjärjestelmäasennuksissa.

2 LOKITIETO

Lokien käytöllä on merkittävä osa organisaation tietojärjestelmien ja tietoverkkojen ylläpidossa, tietosuojan varmistamisessa ja tietoturvallisuuden valvonnassa. Lokeja käytetään työvälineenä järjestelmän eheyden tarkistamiseen, häiriöiden ja väärinkäytösten havaitsemiseen ja korjaamiseen. Lokeja käytetään myös tapahtumaketjujen kirjaamiseen ja toteamiseen. (VAHTI 2009a, 3; Männikkö 2008b.)

Organisaatioissa johto tekee päätöksen yritystoimintaan liittyvien lokien riittävyydestä ja kattavuudesta. Johdon vastuulla on myös integroida lokit yritystoimiin ja hankkeisiin. Yrityksen tulee tunnistaa lokien vaatimukset, määritellä lokien suojaustarve, laatia rekisteriselosteet, määritellä lokien käsittelyyn liittyvät vastuut ja arvioida lokien turvallisuus ja suojaus säännöllisin väliajoin. Lokitietojen hallinnan tulee olla suunnitelmallista ja sen tulee toimia koko lokien elinkaaren. (VAHTI 2009a, 3; Männikkö 2008.)

Lokien käsittely vaatii laitteisto- ja henkilöstöresursseja, ja tästä syystä lokit on otettava huomioon osana yrityksen budjettia. Lokeja tulee käsitellä kustannustehokkaasti, jottei niiden keräämisestä synny turhaan kuluja ja ylimääräistä tiedonkeruuta. Jottei tietoturva vaarannu liiallisen alhaisten resurssien ansiosta, on lokien suhteen oltava tietoturvasuunnitelma siitä, mitä lokeja kerätään ja miten. (VAHTI 2009a, 3.)

2.1 Lokitiedon määritelmä

Loki on vanha sana, jota on aiemmin historiassa käytetty purjehduksessa. Alun perin lokiin kirjoitettiin manuaalisesti tasaisin väliajoin laivan nopeus, jotta voitiin arvioida kuljettu matka. Tässä työssä loki yhdistetään organisaation sähköisiin tietojärjestelmiin. Tietojärjestelmissä lokiin kerätään tietoa tapahtumista organisaation järjestelmissä, verkoissa tai muussa tämän kaltaisessa ympäristössä. Lokeja kerätään usein automaattisesti järjestelmien tekemistä merkinnöistä. Lokitiedot voidaan luokitella monin eri tavoin. Kuitenkin voidaan yleistää lokit käyttölokiin, yl-

läpitolokiin, luovutuslokiin, muutoslokiin ja virhelokiin. Lokien avulla tietojärjestelmissä voidaan selvittää, mitä ja milloin on tapahtunut ja kenen toimesta. (Andreasson & Koivisto 2013, 23-24; VAHTI 2012, 13-14.)

Sähköinen loki on tiedosto, johon tallentuu aikajärjestyksessä merkinnät tietojärjestelmän tapahtumista ja niiden aiheuttajista. Loki kertoo, kuka järjestelmää käytti, miten ja mihin aikaan. Loki sisältää usein myös tietoa virhetilanteista. Yleisesti voidaan olettaa jokaisen järjestelmän keräävän yksilöllistä lokia. (Andreasson & Koivisto 2013, 127; Männikkö 2008b.)

Lokien tarkoitus on se, että jälkikäteen voidaan seurata ja valvoa tietojen käyttöä. Lokeihin on tallennettava tieto, jonka perusteella seurantaa ja valvontaa voidaan tehdä luotettavasti, ja jotta lokeja voitaisiin käyttää todisteena tapahtuneesta. Jälkikäteisellä seurannalla asiakas luottaa organisaatioon ja samalla annetaan viesti väärinkäytöstä harkitsevalle. Lokien tarkoitus ei ole estää asiallista toimintaa järjestelmässä. (Andreasson & Koivisto 2013, 127.)

2.2 Yleiset lokityypit

Lokityyppejä on hyvin paljon, mutta tässä esitellään yleisimpiä lokityyppejä. Kuten edellä tuotu esiin voidaan lokit luokitella yleisellä tasolla ylläpito-, käyttö-, muutos- ja virhelokiin. On yleistä, että lokia ei voi selkeästi laittaa yhteen edellä mainituista tyypeistä, vaan se sijoittuu useaan eri lokityyppiin. Lokeja syntyy käyttöjärjestelmien varusohjelmistoista, sovelluksista, tietokannoista ja verkkolaitteista. Lokit voidaan jakaa tyypin, sisällön tai käytön mukaan. Järjestelmälokin tavoite on ilmoittaa toimintahäiriöistä ja -virheistä. Järjestelmäloki voidaan luokitella virhe tai käyttölokiin. Haltijaloki ilmoittaa esimerkiksi IP-osoitteen perusteella tietyn asian haltijan tietyllä ajanhetkellä. Haltijaloki voidaan sijoittaa käyttölokiin. Pääsynvalvontaloki on keskeinen osa turvallisuutta. Pääsynvalvontaloki ilmoittaa onnistuneet ja epäonnistuneet kirjautumiset, ja siksi se voidaan sijoittaa käyttölokiin. Toisaalta pääsynvalvontaloki voitaisiin sijoittaa myös virhelokiin sen ilmoittamien virheiden vuoksi. (VAHTI 2009a, 29.)

Ylläpitoloki sisältää tietoja käyttöoikeuksien muutoksista, poistosta ja lisäyksistä. Ylläpitolokiin kirjoitetaan tieto myös rekistereiden käyttöön liittyvistä virhetilanteista sekä järjestelmään tehdyistä muutoksista. Käyttöloki sisältää kirjautumiset käyttäjä-, ryhmä- ja sovellustietotasolla sekä epäonnistuneet kirjautumiset. Käyttölokiin kirjataan myös käyttöoikeuksien kasvattamiset, tietokannan lukutapahtumat ja kyselyt sekä tiedot tulostuksista ja tallennuksista. Muutoslokiin kirjoitetaan tieto järjestelmän tietosisällön poistot ja lisäykset sekä järjestelmäparametrien ja asetusten muutokset. Virhelokiin talletetaan tieto seurattavien järjestelmien tai tapahtumien virheet sekä rekisterissä havaitut virheet. (VAHTI 2009a, 30; Andreasson & Koivisto 2013, 127-128; Allen 2002, 94-95)

2.2.1 Lokityypit käytön mukaan

Neljän yleisen lokityypin lisäksi voidaan nimetä lokeja käytön mukaan kuten viestinnänloki, haltijaloki, sovellustason pääsynvalvontaloki, tarjotut julkisten verkkopalveluiden sovelluslokit, käyttöjärjestelmä- ja sovelluslokit sekä verkkotason pääsynvalvontaloki. Viestinnän loki sisältää tietoja viestintätapahtumista, ja sen avulla pyritään selvittämään vikatilanteita ja tietoturvapoikkeamatilanteita. Viestinnänlokeja ovat sähköpostilokit ja keskustelujärjestelmän lokit. Kuvaan 1 sivulle 6 on koottu lokitiedot käytön mukaan. (VAHTI 2009a, 31.)

2.2.1.1 Haltijaloki

Haltijalokin avulla voidaan tunnistaa kenen hallussa jokin verkkotunnista, kuten IP- tai MAC-osoite, on ollut käytössä tiettynä ajankohtana. Haltijalokin perusidea on saada selville liittymän haltija ja selvittää tapahtumien kulku ja osapuolet. Organisaation sisällä voidaan verrata laitekirjanpidon tietoja lokitiedon MAC-osoitteisiin. Tietoturva mielessä voidaan selvittää esimerkiksi ylimääräiset WLAN-tukiasemat vertailemalla lokitietoja kirjanpitoon MAC-osoitteiden suhteen. Tarpeellisia haltijalokeja ovat DHCP-loki, kun organisaatiossa ei käytetä staattisia verkko-osoitteita

työasemilla tai verkkolaitteilla. Proxy-lokit ovat tarpeen, jos käytetään hyväksi välityspalvelinta liikennöitäessä HTTP-protokollalla. Myös kirjautumisloki työasemille voidaan luokitella tarpeelliseksi haltijalokiksi. (VAHTI 2009a, 32.)

Lokityypit käytön mukaan	Sisältö
Viestinnänloki	Viestintätapahtumat, joiden avulla selvitetään vikatilanteita ja tietoturvapoikkeamia.
Haltijaloki	Haltijalokin avulla selvitetään, kenen hallussa jokin verkkotunniste, kuten IP- tai MAC-osoite, on ollut käytössä tiettynä ajankohtana
Sovellustason pääsynvalvontaloki	Sovellustason pääsynvalvontaloki kertoo, mistä IP-osoitteesta yhteys on muodostettu suojattuun kohteeseen ja millä tunnuksella
Tarjotut julkisten verkkopalveluiden sovelluslokit	Verkkopalveluiden sovelluslokista käy ilmi, mistä osoitteesta palveluun otettiin yhteys sekä mahdollinen käyttäjätunnus, jos palvelu vaatii tunnistautumisen.
Käyttöjärjestelmä- ja sovelluslokit	Käyttöjärjestelmästä ja ohjelmista kerätyt lokit. Sovellusloki sisältää tietoa käynnistetyistä ohjelmista, käynnistysvirheistä, käynnistyksen ajankohdasta ja käynnistäjästä.
Verkkotason pääsynvalvontaloki	Verkkotason pääsynvalvonta- ja yhteyslokeilla tarkoitetaan verkon aktiivilaitteiden, kuten reitittimien ja palomuurien, keräämiä lokitietoja

KUVA 1. Lokityypit käytön mukaan.

2.2.1.2 Sovellustason pääsynvalvontaloki

Sovellustason pääsynvalvontaloki kertoo, mistä IP-osoitteesta yhteys on muodostettu suojattuun kohteeseen ja millä tunnuksella. Sovellukset pitävät usein kirjaa epäonnistuneista yhteisyrityksistä sekä yrityksistä ylittää omat käyttövaltuudet. Pääsynvalvontalokeja ovat esimerkiksi shell access-lokit ja erilaisten sovellusten lokit. Sovelluksia voivat olla taloushallinnon järjestelmä tai toiminnanohjausjärjestelmä. Shell access-lokeja voidaan luoda Secure Shellilla, joka tarkoittaa salattua

etäkäyttöprotokollaa, sekä TCP wrapperilla, joka on pääsynvalvontatoteutus. (VAHTI 2009a, 32-33.)

2.2.1.3 Tarjotut julkisten verkkopalveluiden sovelluslokit

Tarjotuilla julkisilla verkkopalveluiden sovelluslokeilla tarkoitetaan lokeja, jonka käyttäjäjoukko ei ole rajattu tai ennalta tiedossa. Verkkopalveluiden sovelluslokista käy ilmi, mistä osoitteesta palveluun otettiin yhteys sekä mahdollinen käyttäjätunnus, jos palvelu vaatii tunnistautumisen. Perusperiaate verkkopalveluiden sovelluslokilla on yhdistää palvelutapahtuma ja lähdeosoite vikatilanteiden ja tietoturvapoikkeaman selvittämiseksi. Esimerkkeinä voidaan todeta WWW-lokit, joihin kuuluvat tapahtumaloki, virheloki, selaintyyppiloki ja viittausloki. Tapahtumaloki luo WWW-palvelimelta haetusta tiedosta lokimerkinnän. Virhelokiin kirjoitetaan sovellusten virheet selityksineen. Selaintyyppiloki kerää tietoa käyttäjien selaintyypeistä ja viittausloki, johon kerätään HTTP-yhteyteen liittyviä tietoja. (VAHTI 2009a, 33-34.)

2.2.1.4 Käyttöjärjestelmä- ja sovelluslokit

Käyttöjärjestelmälokeihin kerätään tietoa monista järjestelmän tapahtumista, ellei tätä ominaisuutta ole erikseen kytketty pois päältä. Myös muut ohjelmistot voivat kerätä moninaisesti lokeja. Windows-käyttöjärjestelmä tuottaa sovellus-, suojaus- ja järjestelmälokeja. Sovellusloki sisältää tietoa käynnistetyistä ohjelmista, käynnistysvirheistä, käynnistyksen ajankohdasta ja käynnistäjästä. Suojausloki sisältä tietoa onnistuneista ja epäonnistuneista tapahtumista, niiden toteuttajasta ja toteutusajasta. Järjestelmäloki sisältää tietoa sisäisistä prosessista ja virheistä. Windows-sovellusten lokien tuottaminen riippuu sovelluksesta itsestään. (Puolustusministeriö 2015, 47; VAHTI 2009a, 34-35.)

UNIX-järjestelmissä lokit sijaitsevat tyypillisesti /var/log tai /var/adm-hakemistoissa, ja niihin tallennetaan järjestelmän sisäisiä tapahtumia sekä käyttäjän teke-

misiä. Lokien sisältö ei välttämättä vastaa kaikissa ympäristöissä tarpeellisia tietoja, joten ne on varmistettava sisällön suhteen tapauskohtaisesti. Käyttöjärjestelmälokeja käytetään järjestelmän käytön ja toiminnan valvontaan, mahdollisten vikojen paikallistamiseen tai järjestelmän turvallisuuden valvontaan. Yleensä käyttöjärjestelmissä on mahdollisuus säätää lokien sisältö, säilytysaika ja toin, kun loki on saavuttanut tietyn koon. Organisaation kannalta käyttöjärjestelmän lokit eivät aina ole tarkoituksenmukaisia, joten ne on syytä säätää ja dokumentoida tehdyt asetukset lokimäärityksiin. (Puolustusministeriö 2015, 47; VAHTI 2009a, 34-35.)

2.2.1.5 Verkkotason pääsynvalvonta- ja yhteyslokit

Verkkotason pääsynvalvonta- ja yhteyslokeilla tarkoitetaan verkon aktiivilaitteiden, kuten reitittimien ja palomuurien, keräämiä lokitietoja. Verkkotason lokiin kirjataan, mistä osoitteesta on mennyt liikenne mihinkin osoitteeseen. Korkeamman tietoliikenneprotokollatason lokista näkyy myös mihin tietoliikenneportteihin liikenne on kohdistunut. Palomuuri- ja reititinlokeista käy ilmi hyökkäyksen kulkureitit, mutta tämä ei kerro sitä, mitä itse järjestelmässä on tehty. Verkkotason pääsynvalvonta- ja yhteyslokeja käytetään vikatilanteiden selvittämiseen, mutta niitä voidaan käyttää myös tietoturvapoikkeamien dokumentointiin ja selvittämiseen. Verkkotason pääsynvalvonta- ja yhteyslokeja ovat reititinloki, palomuuriloki ja reitittimen tuottama flow-data. Tyypillisesti flow-data sisältää esimerkiksi tiedon versionumeroista, sekvenssinumerot, SNMP liittymätiedot, aikatiedot verkkoliikenteen kestoista, siirretyn datan määrän sekä lähde- ja kohde-IP-osoitteet. (VAHTI 2009a, 36.)

2.2.1.6 Transaktiolokit

Transaktiolokia muodostavat tietokantaan tapahtuvat kirjoitus-, muutos-, poisto- ja lukuoperaatiot. Tietomurroissa tietokannat ovat yleinen kohde, sillä niissä säilytetään rahanarvoista tietoa. Siksi tietokannat tulisi salata ja suojata erityisen hyvin,

ja niiden käyttöä tulisi valvoa. Transaktioloki on tiedosto, joka on tehty tietokantaan ja sitä säilytetään erillään tietokannasta. Virhetapauksissa transaktiolokia voidaan käyttää palauttamaan tietokanta virhetilannetta edeltävään tilaan. Transaktioloki sisältää lokimerkinnän uniikin numeron, tiedon edellisestä lokimerkinnän numerosta keskinäisen järjestyksen takaamiseksi sekä tietokantapahtuman tunnistetiedon, joka kertoo tietokantapahtuman aiheuttajan. Transaktioloki sisältää myös tiedon tallennustyypistä ja tiedon tietokannan muutoksesta, joka tietokantaan tehtiin. Tietokannat voivat pitää lokia myös kirjautumisista, tietokannan käynnistyksestä, järjestelmävirheistä, käyttöoikeuksien muutoksesta, tietokannan rakenteen muutoksesta, ylläpitäjän toimista ja tietokannan tietojen luvusta ja muutoksista. Usein tietokannan tietoturvaan liittyvät lokiasetukset ovat oletuksena pois päältä. (VAHTI 2009a, 37-38.)

2.2.1.7 Lokien käsittelylokit

On myös olemassa muiden lokien käsittelyä koskevia lokeja. Muiden lokien käsittelyloki kirjaa, kuka on lukenut, muuttanut, poistanut tai käsitellyt tiettyä lokitietoa tai lokitiedostoa. Hyvin rakennetussa ympäristössä kaikesta lokien käsittelystä pidetään kirjaa. Yleensä organisaation tulee itse rakentaa järjestelmä lokienkäsittelyn seurantaa varten. (VAHTI 2009a, 39.)

Sähköisen viestinnän tunnistamistietojen käsittelyloki tulisi tehdä siihen tarkoitetulla käyttäjätunnuksella, joka on henkilökohtainen. On myös suotavaa, että organisaatiossa erotettaisiin järjestelmän ylläpito lokivalvonnasta erilleen. On myös suotavaa, että kriittiset toimet hoidetaan kahden tai useamman henkilön toimesta, niin sanotun ”kahden miehen säännön” avulla. Lokien sisältämää tietoa voidaan luovuttaa Tietoyhteiskuntakaaren momentin 316 tapauksissa ohjaus- ja valvontaviranomaiselle. (Finlex 2014; VAHTI 2009a, 39; Puolustusministeriö 2015, 39.)

3 LOKIEN HALLINTA

Kaikkia lokitietoja tulee käyttää rekisterien säädösten ja ohjeiden mukaisesti käytön valvonnassa, tietoturva- ja tietosuojarikkeiden esitutkinnassa. Lokitietoja käytetään myös rekisterien tietosisällön oikeellisuuden tarkistamisessa. Lokien avulla tapahtuvassa valvonnassa on kyse asiakkaan tietojen turvaamisen lisäksi myös työntekijän oikeusturvasta. Lokitietojen avulla voidaan todentaa työntekijän oikeutetut toimet. (Andreasson & Koivisto 2013, 128.)

3.1 Lokien kerääminen

Lokitiedostot ovat usein ainoa paikka, johon epäilyttävästä toiminnasta jää jälki. Lokien keräämispalvelut eivät aina ole automaattisesti järjestelmissä käytössä, vaan ne tulee ottaa manuaalisesti käyttöön. Ilman keräysmekanismeja ja niiden tuottamia automaattisia varoituksia heikkenee järjestelmän kyky puolustautua tunkeutumisyrityksiä vastaan. (Allen 2002, 94.)

Lokeja kerätessä on syytä ottaa huomioon keräysmekanismien toimintatapa. Jossain tilanteissa järjestelmän lokien keräys tulee käynnistää joka kerta järjestelmää käynnistäessä. On myös syytä tiedostaa, minne lokitiedot kerätään. Yleensä ylläpitäjä voi määrittää itse paikan lokitiedostoille. Lokitiedoston sijaintiin tulee kohdistaa yrityksen tietoturvan kannalta käyttöoikeusrajoituksia ja samalla varmistaa, ettei lokien kerääminen lopu tilanpuutteeseen. (Allen 2002, 217.)

On tärkeää, ettei tunkeutuja pääse käsiksi lokitiedostoihin ja kykene muokkaamaan tai poistamaan niitä. Lokitiedot tulisi kerätä palvelimelle, joka on tehty niiden keruuta varten. Organisaation johtaja tai tukihenkilö voi erillisen palvelimen avulla tutkia lokeja lähes reaaliajassa. Palvelimen tulisi sijaita fyysisesti turvallisessa paikassa ja siihen ei tule päästä helposti käsiksi verkon kautta. Lokien siirtyminen palvelimelle tulisi toteuttaa dedikoitua linjaa pitkin, eikä lokitietoja tulisi säilyttää samalla koneella, millä ne tuotetaan. Lokit olisi myös syytä tallentaa levylle, jolla

niitä ei pystytä muuttamaan. Olisi myös suotavaa, että tiedosto, johon lokia kirjoitetaan, olisi sellainen, ettei siihen voi kuin lisätä uusia rivejä. Lokitiedot tulisi myös salata. (Järvinen 2002, 138; Allen 2002, 217-218.)

Jos lokitietoja tuottava palvelin on eri kuin se, johon tieto tallennetaan, on palvelimien välinen yhteys oltava turvallinen. Jos palvelimet sijaitsevat lähekkäin, voi niissä olla lyhyt point-to-point-kaapeliyhteys. Jos taas ympäristö ei salli palvelimien lähekkäisyyttä, on lokitietojen siirrossa käytettävä mahdollisimman vähän verkkoja ja reitittimiä. On myös varmistettava, ettei lokien keruu esty DoS-hyökkäyksen aikana. UNIX-ympäristöissä on huomioitava, ettei hyökkääjä pääse täyttämään syslog-tietostoja, jolloin lokien keruu lakkaisi lokiosion tullessa täyteen. NT-ympäristöjen ongelmana on lokitiedon päällekirjoitus, mihin syntyy mahdollisuus, kun käytettävissä oleva tila loppuu. (Allen 2002, 218.)

3.1.1 Lokitiedostojen hallintasuunnitelma

Lokitietoja olisi syytä kerätä niin paljon kuin mahdollista, vaikka ne veisivätkin tilaa ja samalla resursseja. On vaikeaa ennustaa, milloin lokitietoja tarvitaan tutkittaessa organisaatioon kohdistunutta uhkaa tai väärinkäytöstä. Lokitietoja voi kierrättää, arkistoida, salata ja poistaa. (Allen 2002, 219.)

Lokitietoja kierrättäessä tulisi ottaa säännöllisesti kopio ja nimetä samalla uudelleen, ettei niiden päälle vahingossa kirjoiteta. Lokitiedostot voi myös välillä tyhjentää samalla varmistaen, että lokien keruu toimii vieläkin. Kierrättämällä voidaan rajata ajanjakso tapahtunut väärinkäytöstä silmällä pitäen. Näin lokitiedoista saadaan koottua kokoelma ajanjaksoittain. (Allen 2002, 219.)

Lokitietojen arkistoinnissa tiedostot siirretään pysyvään säilytyspaikkaan. Arkistoinnista tulisi olla dokumentaatio siitä, miten ja mitä on arkistoitu. Dokumentaatio on tärkeää varsinkin, jos kaikkea lokien tietoa ei haluta säilyttää, vaan lokeista valikoidaan haluttu tieto. Lokit voidaan myös salata samalla kun niitä tallennetaan. Salattaessa avain tulisi tallettaa varmaan paikkaan, siten, että ilman avainta lokeja

ei voida tutkia. Jos käytetään julkisen avaimen salausta, tulee salaukseen tarvittavaa yksityistä avainta säilyttää offline-tilassa. Kun lokeja aletaan hävittää, tulee varmistua siitä, että kaikki kopiot lokeista on myös hävitetty. (Allen 2002, 220.)

3.2 Lokien käsitteleminen

Lokien käsittely sisältää viisi eri vaihetta: lokien kerääminen, lokien analysointi, lokien säilyttäminen, lokien luovuttaminen ja lokien poistaminen tai arkistointi. Yleisesti lokien käsittely ymmärretään erotetun lokien keräämisestä ja säilyttämisestä. Lokitietojen suuresta määrästä johtuen on keskityttävä olennaisiin kohteisiin, tapahtumiin, raportointitapoihin ja valittava tarkastuksen suorittaja. Lokeja voidaan käsitellä niihin tarkoitetuilla analysointityökaluilla ja välittää haluttu tieto analyysin tekevälle henkilölle. Lopulta ylläpitäjä on se, joka tekee päätökset automatisoidun ja manuaalisen tiedonkeruun perusteella. (VAHTI 2009a, 14.)

Lokien käsittely on osa tietojärjestelmien ja tietoverkkojen ylläpitoa sekä tietoturvaa. Lokit ovat työväline järjestelmän eheyden tarkistamisessa, häiriöiden havaitsemisessa ja niiden korjaamisessa. Lokien avulla pyritään jäljittämään järjestelmän tapahtumia, virheitä, väärinkäyttöä ja tietomurtotilanteita. Lokeja voidaan käyttää hyväksi rikosprosesseissa. Lokien käsittelyllä saavutetaan ja varmistetaan tapahtuman osapuolet, kiistämättömyys, tapahtumien kulku, tunkeutuminen ja poikkeaminen havaitseminen, suorituskykyongelmien havaitseminen ja käyttäjien oikeusturvan varmistaminen. (VAHTI 2009a, 15.)

Lokien suhteen osapuolilla tarkoitetaan sitä, kuka tai ketkä osallistuivat tiettyyn tapahtumaan. Kiistämättömyydellä pyritään siihen, ettei mikään osapuoli voi kiistää osallisuutta tapahtumaan. Esimerkiksi pankkijärjestelmässä on lokiin syytä merkitä niin sallitut onnistuneet toimet kuin myös ei-sallitut toimet. Kululla tarkoitetaan lokitietojen järjestämistä kronologiseen järjestykseen. Tunkeutumisen ja poikkeaman havaitsemisella tarkoitetaan poikkeavaan kellonaikaan tapahtuvat toimet, valtuuttamaton käyttö, resurssien väärinkäyttö, murtautumisyritykset, epäonnistuneet kirjautumiset ja murtautumisesta edeltävät tiedustelut. Suorituskykyongel-

mien havaitsemisessa on kyse järjestelmän vika- ja ongelmatilanteiden lokiin kirjaamisesta. Käyttäjien ja rekisteröityjen oikeusturva on taattu, kun lokitiedoilla voidaan osoittaa mitä kukin on tehnyt järjestelmässä. Asianmukaisella lokien keräämisellä parannetaan järjestelmien ylläpitoa ja siihen osallistuvien oikeusturvaa. (VAHTI 2009a, 15.)

3.2.1 Huomioitavia asioita lokien käsittelyssä

Viestinnän lokissa on huomioitava, että ne sisältävät tunnistamistietoja sekä henkilötietoja. Tunnistetietojen takia viestinnän lokeissa on huomioitava viestinnän tietosuojalain, henkilötietolain sekä työelämän tietosuojalain velvoitteet. Myös haltijalokeja koskevat samat tunnistetietoihin liittyvät lait kuin viestinnän lokeihin. Haltijalokeissa on otettava myös huomioon, että lokeja tuottavat laitteet ovat ajan suhteen synkronoituja, ja että ylläpitäjä on tietoinen mille aikavyöhykkeelle lokeja kirjataan. Ajan synkronoiminen lokien suhteen on yleistettävissä kaikkiin lokityyppeihin. (VAHTI 2009a, 31-32.)

Julkisten verkkopalveluiden sovelluslokeissa ja sovellustason lokeissa tulee ottaa myös huomioon henkilön tunnistamiseen liittyvät lait. Jos sovelluslokeissa käsitellään henkilötietoja, tietoturvaluokiteltuja tai suojattavaa aineisto, pääsynvalvontalokeista on otettava kopio erilliseen lokipalvelimeen, johon ulkopuolinen taho ei pääse käsiksi. Jos henkilö voidaan tunnistaa lokista, on loki käytännössä henkilörekisteri ja siihen on huomioitava henkilötietolain vaatimukset. Henkilöllisen tiedon tallentaminen lokiin on syytä harkita tarkoin. (VAHTI 2009a, 33-34; Männikkö 2008.)

Käyttöjärjestelmä- ja sovelluslokeissa on otettava huomioon, että lokitiedostojen koko riittää lokien keräämiseen, ja niille on tietty kierrätysrutiini. Käyttöjärjestelmälokeja tulisi siirtää keskitettyyn palvelimeen, jotta taataan riittävä tallennustila. Sovellukset tuottavat usein epästandardeja lokitietoja, joten järjestelmää rakennettaessa on otettava huomioon, että lokitiedot saadaan talteen keskitettyyn lokijärjestelmään. (Puolustusministeriö 2015, 46; VAHTI 2009a, 35.)

Verkkotason pääsynvalvontalokeissa palvelimen suojana olevan palomuurin tulee kirjata sekä onnistuneet että epäonnistuneet yhteydet. Yleisesti palomuurin oletusasetuksissa painotetaan liikaa epäonnistuneita yhteyksiä. Verkkolaitteiden lokit tulisi myös keskittää lokipalvelimelle. (VAHTI 2009a, 36.)

Transaktiolokien lokeista tulisi myös ottaa automaattiset kopiot talteen suojattuun lokipalvelimeen, jos järjestelmässä käsitellään salassa pidettävää aineistoa. Tietokannoissa tapahtuvasta kirjaamisesta lokiin voi olla vaikutusta järjestelmän suorituskykyyn, mikä tulee ottaa huomioon järjestelmän suunnittelussa. Lokien käsittelyn loki voidaan tuottaa ohjaamalla tärkeät lokit erilliseen palvelimeen, jonne vain tietyillä henkilöillä on henkilökohtainen kirjautumisoikeus. (Puolustusministeriö 2015, 65; VAHTI 2009a, 39-40.)

3.2.2 Lokien käsittelyn perusperiaatteet

Lokien prosessointi tulee ottaa huomioon laitteisto- ja henkilöresursseissa. Lokien käsittelyssä ja suunnittelussa tulee huomioida lokien tarkoitus, tarve ja suunnitelmallisuus. Lokien käsittely pitäisi optimoida siten, ettei lokien käsittelyyn kulu turhaan resursseja liiallisen tiedon keräämisen ja analysoinnin tuloksena. Neljä perusperiaatetta ovat:

a) Lokien käsittely perustuu tarpeeseen.

b) Lokien käsittely tapahtuu määriteltyjen järjestelmien ja toimintatapojen mukaisesti.

c) Lokien analysoinnin tulosten perusteella tehtävät toimet ovat ennalta määriteltyjä.

d) Rekisteröityjen, järjestelmän käyttäjien sekä ylläpitäjien tietosuoja ja oikeusturva huomioidaan lokien käsittelyssä. (VAHTI 2009a, 19; Männikkö 2008.)

Teknillisestä näkökulmasta tietojärjestelmien ja ympäristön turvallisuutta tukevien järjestelmien tulee kerätä lokitietoja. Yleensä lokeja luodaan automaattisesti,

mutta myös manuaalisesti voidaan kerätä merkintöjä esimerkiksi konesalin kävijälokiin. Lokien tulee kerätä riittävästi tietoa valvottavista tapahtumista. Riittävä tieto määritellään jo järjestelmän rakennusvaiheessa. Tyypillisesti lokitiedosta pitäisi selvitä tapahtuman onnistuminen tai epäonnistuminen, tapahtuminen luotettavasti yksilöitävä suorittaja ja ajankohta. Lokit pitäisi turvata niin, ettei niitä voida muuttaa tietomurron yhteydessä. Lokien asiatonta käsittelyä varten tulee olla oma lokinsa. Vain pienemmissä organisaatioissa riittää manuaalinen lokien valvonta, mutta yleensä lokimassan tarkasteluun vaaditaan automaattista havainnointi- ja hälytystyökaluja. (Puolustusministeriö 2015, 48; VAHTI 2009a, 23.)

3.3 Lokitiedot murretussa järjestelmässä

Tietojärjestelmästä tulisi ottaa varmuuskopioita. Jos järjestelmään on murtauduttu ja varmistusta halutaan käyttää todisteena, on varmistusta säilytettävä turvallisessa paikassa. Varmistuksen aikana levyjen käyttö on korkeaa, mikä voi paljastaa murtautujalle, että hänet on huomattu. On myös mahdollista, että tunkeutuja on asentanut järjestelmään lokit poistavan ohjelman. Lokitiedot tulisi varmuuskopioida säännöllisin väliajoin. (Puolustusministeriö 2015, 46; Allen 2002, 274.)

Usein tunkeutuja tekee järjestelmään useita sisäänmenokohtia. Hyökkäykset järjestelmiä kohtaan voi tapahtua skannaamalla laajoja IP-osoitealueita. Hyökkäys kohdistuu usein DNS, FTP, HTTP ja SMTP palveluja kohtaan. Hyökkäyksen yhteydessä tulisi tutkia lokit, koska hyökkäyksestä jää usein jälkiä. Jäljet voivat löytyä lokeista tai tiedostoista, joita hyökkääjä on jättänyt jälkeensä. Palomuurit, verkon valvontajärjestelmät ja reitittimen lokit sisältävät tietoa, mikä usein pysyy muuttumattomana, vaikka tunkeutuja pääsisikin paikalliseen järjestelmään kiinni ja tuhoaisi sen lokitiedot. Palomuuri voidaan asettaa tallentamaan lokeja siirretyn tiedon määrän mukaan. On myös syytä huomioida tallennustilan suhteen, että hyökkäyksen yhteydessä lokimäärä voi kasvaa merkittävästi. (Puolustusministeriö 2015, 47; Allen 2002, 274-275.)

Päivämäärän, kellonajan ja hyökkäyksen kohteena olevien järjestelmien perusteella pystytään paikallistamaan lokeista toisiinsa liittyviä tietueita, joiden avulla

tunkeutujasta saadaan lisätietoa. Tunkeutumista tutkittaessa tulisi selvittää yhteyksiä, jotka ovat samasta lähteestä kotoisin tai menossa samaan kohteeseen. Kaikkien järjestelmien lokiformaatit eivät ole yhteensopivia, eikä ole saatavilla systeemiä joka yhdistäisi kaikkien järjestelmän osien tuottamat lokitiedot kronologiseen järjestykseen. On myös huomioitava, etteivät kaikki järjestelmän lokitiedot ole samassa ajassa, vaan ne tulee synkronoida käyttäen hyväksi NTP-protokollaa. (Allen 2002, 276; VAHTI 2009a, 23.)

Palomuurien, reitittimien ja verkon valvontajärjestelmien tuottamien lokien lisäksi tulisi käyttää hyväksi paikallisia lokitietoja selvittääkseen sitä, minkä tyyppistä hyökkäystä tunkeutuja on käyttänyt. Yleensä verkkolaitteiden lokit pysyvät tunkeutujan ulottumattomissa, jos tunkeutuja ei erikseen ole murtautunut itse verkkolaitteeseen. On kuitenkin suositeltavaa siirtää lokitiedot talteen myös verkkolaitteista. Järjestelmä- ja verkkolokien tiedoista tulisi etsiä:

a) Pääsyn kieltoa koskevat ilmoitukset, joita syntyy jos tunkeutuja yrittää arvata salasanoja (access denied).

b) Viestit, jotka viittaavat vanhoihin tietoturva-aukkoihin.

c) Asennettuja ohjelmia, kuten TCP wrapper, joka kerää yhteydenottopyyntöjä.

Lokeista voidaan löytää päivämäärät, kellonajat ja lähdeosoitteet. Itse verkkolaitteiden lokit pysyvät tunkeutujan ulottumattomissa, jos tunkeutuja ei erikseen ole murtautunut itse verkkolaitteeseen. On kuitenkin suositeltavaa siirtää lokitiedot talteen myös verkkolaitteista. (Allen 2002, 276-277; VAHTI 2009a, 36.)

Pelkän tunkeutumisen tiedostaminen ei riitä selvittämään tunkeutumisen vakavuutta. On helppoa havaita, jos tiedostoja on yritetty muokata, mutta arkaluontoisten tiedostojen lukemista ei. On siis varauduttava aina siihen, että tunkeutuja on päässyt käsiksi kaikkeen järjestelmässä. Tunkeutumista tutkittaessa on turvauduttava lokitietoihin, verrata luotettavien tiedostojen tarkistussummia murretun koneen tiedostojen tarkistussummiin ja käyttää mahdollisia analysointityökaluja. On tärkeää tutkia tarkistussummia käyttöjärjestelmän ytimen suhteen. Yleensä tunkeutumisesta jää jälki lokitietoihin, tunkeutuja muuttaa järjestelmää peittääkseen

jälkensä ja asentaa Troijan hevosia, takaovia tai järjestelmäkomentojen uusia versioita. (Allen 2002, 277.)

3.4 Lokien säilytys

Jotta organisaatio pystyy vastamaan tietojen säilytys- ja luovutusketjujen todentamisvaatimuksiin, joutuu organisaatio usein säilyttämään lokitietoja pidempään kuin tuottajasovelluksen tuki kestää. Organisaatiossa voi syntyä tarve lokitietojen arkistoinnille ja käytänteille, joiden mukaan lokeja arkistoidaan. Lokeihin on syytä jättää kirjoittamatta tietoja, joita ei haluta arkistoida. Kuitenkin lokien arkistoinnissa tulee ottaa huomioon tiedon luottamuksellisuus ja eheys. On myös syytä kiinnittää huomiota lokitiedon suojaamiseen arkistoinnin ja siirron yhteydessä, ettei lokitiedon suhteen tule ulkopuolisen tahon tekemiä muutoksia. Lokien säilyttämiseen liittyvät lokien arkistoiminen, supistaminen, lokimuunnokset, lokien normalisointi ja lokien säilytysaika. (VAHTI 2009a, 57-58.)

Lokien kerääminen tapahtuu lokikierron mukaan. Lokikierto tarkoittaa lokitiedoston sulkemista ja uuden luomista, kun tiedosto katsotaan olevan täynnä. Lokitiedosto on täynnä saavutettuaan tietyn koon. Kun käytetään lokikiertoa, pystytään pitämään lokitiedostot käsiteltävän kokoisina ja ne voidaan siirtää arkistoon tiivistettyinä. Tiivistys tarkoittaa tointa, jolla lokista suodatetaan talteen halutut lokimerkinnät. Suodatuksen yhteyteen voidaan myös automatisoida analyysiä lokin sisällöstä esimerkiksi rikollisen toiminnan huomaamiseksi. Lokien arkistointi tarkoittaa lokien säilyttämistä pidennetyn ajan. Lokit tulisi arkistoida irrotettavalle tallennusvälineelle, SAN-verkkoon, erilliselle palvelimelle tai muulle arkistointiin tarkoitetulle laitteelle. Usein lokeja tulee säilyttää lainsäädännöllisistä syistä tietyn aikaa. (VAHTI 2009a, 58.)

Lokien tiivistämisellä tarkoitetaan lokitiedoston koon minimoimista ilman, että lokitiedoston sisältö muuttuu. Lokeja tiivistetään yleensä lokikierron tai arkistoinnin yhteydessä. Lokitietoja voidaan pakata tehokkaasta, koska tiedostot sisältävät tyy-

pillisesti vain tekstiä. Lokien supistamisella tarkoitetaan ylimääräisten lokimerkintöjen poistamista lokista, jotta tiedoston kokoa saadaan pienennettyä. Lokista voidaan poistaa merkintöjä tai kokonaisia tietokenttiä. (VAHTI 2009a, 58-59.)

Lokimuunnos tarkoittaa lokitietojen muotoilua ja tallentamista toiseen muotoon. Esimerkiksi lokitiedosto voidaan muuttaa XML-tiedostomuotoon. Lokin muunnos voidaan usein tehdä ohjelmalla, joka tekee itse lokin, mutta myös erillisellä ohjelmalla. Lokin normalisoinnilla tarkoitetaan lokin tietokenttien muuttamista tiettyyn esitysmuotoon. Normalisointia on muuttaa esimerkiksi lokitiedoston aikatiedot tiettyyn esitysmuotoon. Lokeja tuottavat ohjelmat voivat tuottaa lokeja 12 tai 24 tunnin muodoissa, joten normalisointi on tarpeen. Normalisoinnilla tehostetaan lokien analysointia ja raportointia, kun eri lokien tuottajien lokit ovat samassa muodossa. Normalisointi voi aiheuttaa organisaation resursseihin menoja, joten jo järjestelmien hankintavaiheessa tulisi kiinnittää huomiota lokien yhtenäisyyteen. (VAHTI 2009a, 59.)

Lokien säilytysajan tulee määräytyä sen suhteen, miksi lokia ja sen sisältämää tietoa kerätään. Esimerkiksi arkistolaki edellyttää, että lokitietojen säilytysajassa otetaan huomioon asiakirjallisen tiedon alkuperä, eheys ja luotettavuuden varmistus. Lokitiedon yhteys asiankäsittelyjärjestelmään pakottaa säilyttämään lokitiedot niin kauan kuin itse järjestelmä on organisaatiossa käytössä. Kun asiakirjat hävitetään, tulee lokista käydä ilmi asiakirjan hävittäminen. (VAHTI 2009a, 60.)

Tietojärjestelmän testauksesta ja käytössäkin syntyviä lokeja ei yleensä tallenneta kovin pitkäksi aikaa. Yleensä tietojärjestelmän lokeilla tutkitaan järjestelmän virhetilanteita ja kuormaa. Tietokantojen varmistamiseksi kerätään lokia vähintään varmistusajan verran, eli niin kauan, että koko tietokannasta on tallessa varmuuskopio ja edelliseen varmistukseen asti tehdyt muutokset. Tavallinen säilytysaika tietokannalla voi olla 1-2 vuotta. Laskutustietoja varten kerätään lokiin eri hintaiset henkilökohtaiset ostotapahtumat. Laskutustietojen säilytysaika riippuu laskutusvälistä ja maksuperusteen vanhenemisesta. Myös järjestelmän tai käyttäjien käyttömäärää voidaan lokittaa, ja sen säilytysaika on normaalisti yksi kalenterivuosi. (VAHTI 2009a, 60.)

4 SCCM

SCCM eli System Center Configuration Manager on Microsoftin tekemä ohjelmisto, jonka avulla voidaan ylläpitää organisaation IT-infrastruktuuria. IT-puolen tarkoitus on ylläpitää yrityksen palveluita, joiden avulla pyritään asetettuihin tavoitteisiin. Palveluiden ylläpitoon kuuluvat esimerkiksi työpöytätuki, ohjelmistokehitys, palvelintuki ja tallennustilan hallinta. Usein ylläpidettävät palvelut eivät ole yhtenäisesti yhden organisaatioelimen hallinnassa. SCCM on alettu kehittää keskittämisen vuoksi, jotta saataisiin mahdollisimman moni ylläpidettävä osa IT-palveluista saman ohjelmistokokonaisuuden alaisuuteen. It-palveluiden ylläpidossa on tärkeää, että niitä kehitetään myös tulevaisuutta silmällä pitäen ottaen huomioon sekä liiketoiminta, että asiakkaat. It-palveluita tulisi myös kehittää laadun suhteen ja kehityksellä pitäisi pyrkiä pienentämään yrityksen kuluja palveluiden ylläpidossa. IT-ylläpito sijaitsee kaupankäynnin ja teknologian välimaastossa mahdollistamassa yrityksen liiketoiminnan. (Martinez & Daalmans & Bennett 2014, 1.)

Seuraavissa alaotsikoissa on käyty läpi SCCM-ympäristön koneiden vaatimuksia niin rautatasolla kuin myös ohjelmistojen suhteen. Microsoft on listannut SCCM:n vaatimille osakokonaisuuksille vaatimukset. Vaatimuksissa esitellään Site-palvelimen, Site-etäpalvelimen, asiakaskoneiden, Configuration Manager Consolen ja tietokantapalvelimen konevaatimuksia. Vaatimusten lopusta löytyy myös testiympäristöjä varten omat vaatimukset. Microsoft mainitsee konesuosituksissaan sen, että ne on tehty suuria ympäristöjä varten, ja niissä on huomioitu maksimimäärä asiakaskoneita ja käytössä ovat kaikki SCCM tarjoamat ominaisuudet. Mainittakoon Microsoft 2017e lähteestä, että se päivittyy ajan kanssa, ja kirjoitushetkellä se oli päivitetty viimeksi 30.3.2017, mutta lähteen linkki on kirjoituksen aikana pysynyt samana. (Microsoft 2017e.)

4.1 SCCM koneen vaatimukset

Microsoft on listannut Site-palvelimen vaatimuksiksi tietyn määrän levytilaa, muistia ja prosessoritehoa. Suosituksissa vaihtoehtona on pitää SCCM kone ja tietokantapalvelin erillään tai samassa koneessa. Jos tietokanta on Site-palvelimella, Microsoftin vaatimukset muistin määrälle ovat 96 gigatavua, suorittimessa tulee olla 16 ydintä ja tietokannan muistinkäyttöaste palvelimelta tulee olla 80 prosenttia. Jos tietokanta erotetaan Site-palvelimesta, putoaa Site-palvelimen muistivaatimus 16 gigatavuun ja suoritinvaatimus kahdeksaan ytimeen. Erillään olevan tietokannan vaatimukset ovat 64 gigatavua muistia 90 prosentin käyttöasteella ja suorittimessa tulisi olla 16 ydintä. Jos käytössä olisi isompi organisaatio, joka käyttäisi keskitettyä hallintaa usean eri Site-palvelimeen, on kyseessä Central administration Site-ratkaisu. Keskitetty Central administration site-ratkaisussa pääpalvelimelta vaaditaan 128 gigatavua muistia, 20 ydintä suorittimelta ja 80 prosentin muistin käyttöaste tietokantaa varten. Central administration sitessa ajatellaan olevan 700000 asiakaskonetta ja muussa kuin minimitapauksessakin Microsoftin suositukset on tehty 25000 asiakaskonetta varten. Ympäristö, jonka tämän työn puitteissa asennan, sisältää yhden Site-palvelimen. Ympäristöä hallitaan Configuration Manager Consolella, joka voidaan asentaa haluttuihin koneisiin. Kuvaan 2 on koottu Site-palvelimen vaatimukset. (Microsoft 2015b; Microsoft 2017e).

Site-palvelimen laitteistovaatimukset	Tietokanta Site-palvelimella	Site-palvelin erillään tietokannasta	Central administration ratkaisu
Muistin määrä	96 gigatavua	Site-palvelin 16 gigatavua ja tietokantapalvelin 64 gigatavua	128 gigatavua
Suorittimen ydinten määrä	16 ydintä	Site-palvelimessa 8 ydintä ja tietokantapalvelimessa 16 ydintä	20 ydintä
Muistin käyttöaste	80%	Tietokantapalvelimessa 90%	80% tietokannalle

KUVA 2. SCCM koneen laitteistovaatimukset isoissa organisaatioissa.

Tämän työn puitteissa kaikki SCCM:n vaatimat kokonaisuudet sijaitsevat samalla palvelimella. Microsoftin Site-etäpalvelimelle (palvelin, jossa useita rooleja samassa) olevat suositukset sisältävät kaikki osaset, joita ovat Management point, Distribution point, Application Catalog, Software update point ja muut mahdolliset asennettavat roolit. Management pointia varten suositukset ovat suorittimelle neljä ydintä, kahdeksan gigatavua muistia ja 50 gigatavua levytilaa. Distribution pointia varten suositellaan kaksi prosessoriydintä, kahdeksan gigatavua muistia ja levytilaa asennettavien ohjelmien sekä itse käyttöjärjestelmän verran. Application Catalogia varten suositellaan neljää prosessoriydintä, 16 gigatavua muistia ja 50 gigatavua levytilaa. Software update pointia varten suositellaan suorittimelle kahdeksaa ydintä, 16 gigatavua muistia ja kiintolevytilaa päivitysten vaatima tila huomioiden samalla käyttöjärjestelmän vaatimukset. Muita mahdollisia rooleja varten Microsoft suosittelee neljää ydintä suorittimelle, kahdeksan gigatavua muistia ja 50 gigatavua levytilaa. Configuration Manager Console vaatii Intel i3 suorittimen tai vastaavan, 2 gigatavua muistia sekä 2 gigatavua kiintolevytilaa. Console voidaan asentaa haluttuun koneeseen AD-ympäristössä. (Microsoft 2017e.)

Testiympäristöjä varten Microsoft suosittelee Site-palvelimelle, jossa samassa on tietokanta, suorittimelle kahdesta neljään ydintä, 7-12 gigatavua muistia sekä 100 gigatavua levytilaa. Jos Site-palvelin on erillään, suositus on yhdestä neljään ydintä suorittimelle, kahdesta neljään gigatavua muistia ja 50 gigatavua levytilaa.

Koska tämän opinnäytetyön kohdeympäristö sisältää alle 50 työasemaa, ei Microsoftin suurille ympäristöille tehtyjä suosituksia voi käyttää suoranaisesti. Lähimmäksi työn kohdeympäristöä päästään analysoimalla suosituksia Site-etäpalvelimelle, joka sisältää kaikki vaaditut osakokonaisuudet, peilaten niitä testiympäristöä varten oleviin suosituksiin. Microsoft ilmoittaa, että minimivaatimus Configuration manageria varten on 25 gigatavua levytilaa ja 100 gigatavua jokaista 25000 asiakasta kohden tietokannan tiedostoja varten. Testiympäristön vaatimuksissa mainitaan sen soveltuvan aina 100 asiakaskoneeseen asti. Kohdeympäristöä ajatellen voidaan säätää palvelin muistin osalta testiympäristön vaatiman 7-12 gigatavun muistimäärään ja asettaa levytila asennettavien roolien mukaisesti vähintään 200 gigatavun suuruiseksi, mikä sisältää 50 gigatavua tilaa roolien lisäksi

asennettaville ohjelmille. Kohdeympäristössä SCCM kone on virtuaalinen, joten sen levykokoa, muistinmäärää ja suorittimen ytimiä voi tarvittaessa muuttaa asennuksen jälkeen, kunhan asennuksen vaatimukset täyttyvät. (Microsoft 2017e.)

4.1.1 SCCM ja asennettavat palvelinroolit

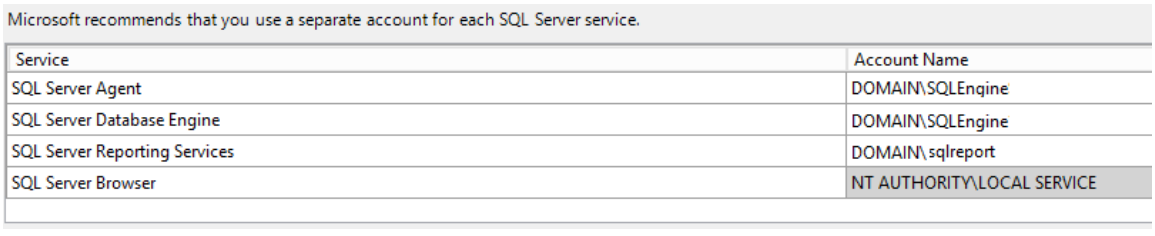
SCCM koneelle tulee asentaa Server 2016 roolit ja toiminnot osioista tarvittavat kohdat (Microsoft 2013a). Tämän opinnäytteen puitteissa roolit asennetaan Powershell-komentosarjan avulla, jotta asetukset menevät jatkossakin oikeaan ympäristöön asennettaessa täysin samalla tavalla. Powershell-skripti on liitteessä 1. Tein skriptin Microsoftin vaatimusten pohjalta hyödyntäen Powershellia etsien vaadittujen roolien nimet Powershell ympäristössä. Testasin skriptin testiympäristössä. Powershell täytyy olla 64-bittinen, jotta Windows Serverin ominaisuuksia voidaan asentaa komentosarjan avulla. Microsoftin sivuilla on perusteluja, miksi mikäkin skriptin rooli asennetaan (Microsoft 2017b). 64-bittinen versio käynnistyy automaattisesti, jos ei erikseen valitse x86-versiota. Jotkin moduulit voivat vaatia x86-version Powershellista. Skriptissä WSUS ominaisuus ei ole pakollinen SCCM toimivuuden kannalta, mutta sen kautta voidaan asentaa keskitetystä päivityksiä asiakaskoneisiin. (Microsoft 2013a; Microsoft 2013c; Microsoft 2016c.)

4.2 SQL koneen vaatimukset

Primary Site-palvelimien ollessa kyseessä tietokanta voidaan asentaa erikseen, mutta jos kyseessä on Seconday Site-palvelin, niin tietokanta tulee olla samalla koneella kuin Sitekin. Tässä työssä SQL Server 2016 asennetaan New SQL Server stand-alone asennuksena. SQL-serveriin ei asenneta kuin pakolliset ominaisuudet, joita ovat Database Engine Services ja Reportin Services–Native. Tietokantaserveriin voisi asentaa enemmänkin ominaisuuksia, mutta niitä ei tarvita SCCM:ää varten. Tietokantaserveri tukee perusasennusta tai asennusta, jossa tietokantapalvelimelle on asetettu nimetty instanssi (named instance). SCCM tukee myös usean palvelimen tietokantaklustereita. SCCM ei tue Network Load Ba-

lancing klusteria, eikä myöskään suoraa tietokantakoneelta tietokantakoneelle tapahtuvaa kahdennusta. Kahdennus tulee toteuttaa käyttäen hyväksi Management pointtia. SQL Serverien versioista pääsääntöisesti Standard ja Enterprise versiota voi käyttää kaikissa eri asennusvariaatioissa. SQL Express versiota voi käyttää vain Secondary Site-palvelimissa. Eri versioista tuki löytyy aina SQL Server 2008 asti Standard, Enterprise ja Datacenter versoissa. SQL Expressissä tuki on vain 2012 versioon saakka. Edellä mainitut versiot toimivat, jos SCCM on vähintään 1511 versio. (Microsoft 2013b; Microsoft 2017f.)

SCCM vaatii tietokannalta 64-bittistä versiota, jos sillä hallitaan Site-palvelimen tietokantaa. Tietokannan kollaatio (collation) tulee olla SQL_Latin1_General_CP1_CI_AS muotoa, vain Kiinaa varten tuetaan kahta muuta kollaatioasetusta. Database Engine Service on vaatimus kaikille Site-palvelimille. Tietokanta tulee asettaa Windows authentication asetuksella. Tietokannasta tulee löytyä dedikoitu instanssi jokaiselle Sitelle tai perusasetuksin asennettu instanssi. Tietokannan muistikäyttö tulee asettaa minimissään 50 ja maksimissaan 80 prosenttiin koneen muistinkäytöstä, jos tietokanta on samassa koneessa kuin Site. Muistia SQL-palvelinta varten tulee olla minimissään 8 gigatavua Central Administrator site ja Primary Sitea varten. Secondary Site ei vaadi kuin 4 gigatavua muistia. Tietokantaa voidaan käyttää sekä paikallisella, että domaintason käyttäjällä. Tätä työtä varten määriteltiin jokaista tietokannan palvelua varten oma tunnus, kuten kuvasta 3 käy ilmi. (Microsoft 2017f.)


Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name
SQL Server Agent	DOMAIN\SQLEngine
SQL Server Database Engine	DOMAIN\SQLEngine
SQL Server Reporting Services	DOMAIN\sqlreport
SQL Server Browser	NT AUTHORITY\LOCAL SERVICE

KUVA 3. SQL-servicekäyttäjät.

Micorosoft suositteleekin asennuksen aikana tekemään jokaiselle palvelulle omat käyttäjät. SQL Server käyttää Sitejen väliseen kommunikointiin SQL Server Service Brokeria, joka käyttää oletuksena 4022 porttia. SQL server kommunikoi Management Pointin, SMS Providerin, Reporting servicen ja Site-palvelimen kanssa portin 1433 kautta. Configuration Manager ei salli dynaamisten porttien käyttöä. Porttien avaaminen on oleellista, jos SCCM on hajautettu usealle eri koneelle. (Microsoft 2017f.)

4.3 Windows asiakaskoneen vaatimukset

Configuration Managerin asiakaskoneille on olemassa minimivaatimukset ja ne on määritelty käyttöjärjestelmän mukaan. Windows käyttöjärjestelmän suhteen asiakaskoneella tulee olla 500MB tyhjää tilaa ja suositellaan 5 gigatavua tyhjää tilaa asiakkaan välimuistia varten. RAM-muistia asiakaskoneessa tarvitsee olla vähintään 384 megatavua ja Software Center vaatii prosessorin olevan 500MHz nopea. 384 megatavun RAM-muistivaatimus koskee käyttöjärjestelmän deploymenttia ja ohjelmistoille mahdollisesti riittää pienempikin määrä. Jos asiakaskonetta ohjataan etänä, tulee koneen suorittimen olla Pentium 4 HT 3GHz tai nopeampi ja koneessa tulee olla 1 GB RAM-muistia. Vaatimuksissa voidaan alentaa, jos asiakaskoneeseen toimivuudelle ei aseteta optimaalista tavoitetta. Toisin sanoen, järjestelmä toimii pienemmilläkin muistimäärillä, mutta asennuksissa voi ilmetä hidastumista. (Martinez & Daalmans & Bennett 2014, 25; Microsoft 2017e.)

4.3.1 Linux ja Mac asiakaskoneen vaatimukset rautatasolla

Tässä työssä päätavoite on Windows-käyttöjärjestelmän asennuksessa, mutta SCCM:llä voi hallita myös Linux- ja Mac-koneita asiakasohjelmiston avulla. Suorittimen ja muistin suhteen ohjeistus on sama kuin minkä itse käyttöjärjestelmä vaatii. Levytilaa suositellaan olevan 500 megatavua tyhjää tilaa sekä 5 gigatavua välimuistia varten. Mac-konetta varten ei ole määritelty tarkkoja vaatimuksia, mutta asiakasohjelmiston voi asentaa Mac OS X 10.6 versiosta 10.12 versioon saakka. Linux-käyttöjärjestelmäksi soveltuu AIX, CentOS, Debian, HP-UX, Oracle Linux,

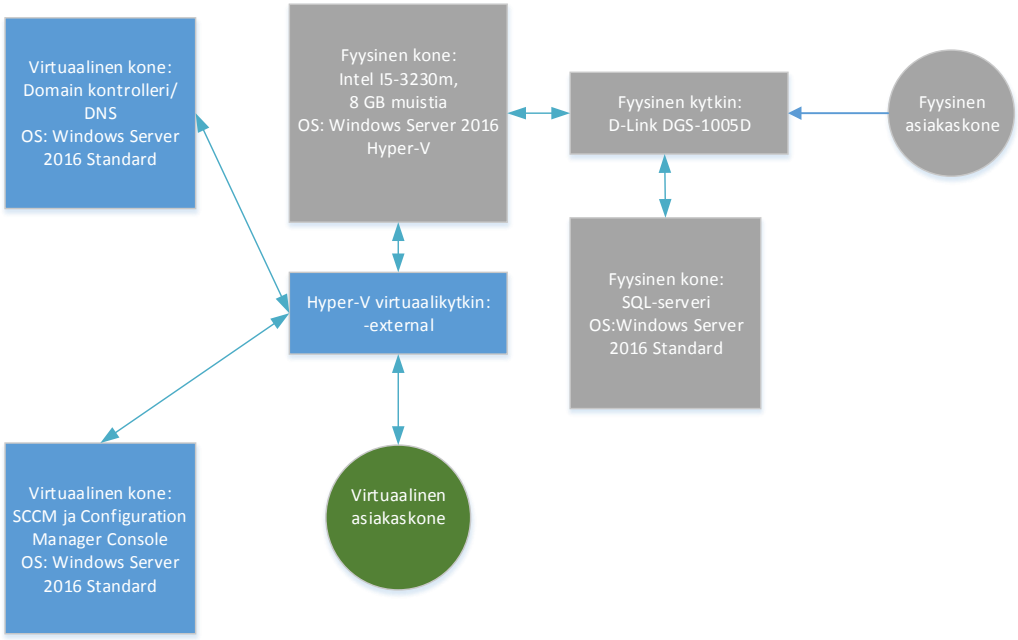
Red Hat Enterprise Linux, Solaris, Suse Linux Enterprise Server ja Ubuntu. Tarkemmat versionumerot Linux-käyttöjärjestelmille löytyvät lähteen Microsoft 2017d alta. Melko usein Linux-käyttöjärjestelmiä varten asennetaan universaali asiakasohjelmisto (ccm-Universalx64.<build>.tar niminen paketti) joko 32- tai 64-bittisenä. (Microsoft 2017e; Microsoft 2017d.)

4.4 SCCM ympäristön asentamisesta

Tämän opinnäytetyön keskiössä ei ole kertoa tarkkaan, miten SCCM on asennettu, mutta tässä kappaleessa käydään läpi asennuksen vaatimaa ympäristöä ja asennuksen joitain vaiheita pääpiirteissään. Käyttöjärjestelmät asennettiin käyttäen joko ilmaista Rufus ohjelmistoa, jonka avulla voidaan luoda muistitikuista käynnistysmedia, tai virtuaaliympäristössä suoraan käyttöjärjestelmän levykuvasta. Microsoftin omilla wikisivuillakin mainitaan yhtenä vaihtoehtona tehdä asennusmedia Rufuksen avulla (De Costa, 2015). Koneita asennettaessa testiympäristöönkin pyritään asennukset tekemään, kuten niitä asennettaisiin oikeaan tuotantoympäristöön. Tuotantoympäristöön asennettaessa palvelinkoneessa ei ole käytössä usein yhteyttä Internettiin, ja päivitykset tulee asentaa esimerkiksi usb-tikulta, verkkoasemalta sisäverkosta tai keskitetyltä palvelimelta.

Tätä opinnäytetyötä varten tehtiin testiympäristö ja varsinainen tuotantoympäristö. Testiympäristö ja tuotantoympäristö eivät eronneet tavoitteiden osalta, vaan kummassakin Windows 10 käyttöjärjestelmän asennus oli tarkoitus toteuttaa Zero-touch-asennuksella (ZTI) SCCM:n avulla. Testiympäristö rakennettiin fyysisten koneiden päälle, mutta itse ympäristö asennetaan sekä virtuaalisesti Microsoftin Hyper-V:n avulla, sekä asentamalla SQL-palvelin täysin yksittäiselle fyysiselle koneelle. Hyper-V on Microsoftin virtuaaliympäristö. Kuvasta 4 käy ilmi testiympäristön rakenne. SQL-palvelin sijaitsee yhdellä fyysisellä koneella ja AD/DNS kone sekä SCCM kone on luotu Hyper-V:n avulla virtuaalisesti. Virtuaalikoneet on yhdistetty virtuaaliseen kytkimeen ja fyysiset koneet toisiinsa fyysisellä D-linkin kytkimellä. Hyper-V:tä pyörittävä kone käyttää omaa verkkokorttia virtuaalikytkimenä. Kaikki ympäristön koneet ovat kytketty samaan Active Directoryyn. Sillä, onko ym-

päristö fyysinen tai virtuaalinen, ei ole lokitietojen sisällön suhteen merkitystä. Tosin jos ympäristöä testattaisiin täysin virtuaalisesti, voisi muodostua eri ongelmia, kuin tilanteessa, jossa esimerkiksi kohdekoneet ovat fyysisiä. Tässä opinnäytteessä lopulliset tuotantoympäristön kohdekoneet ovat fyysisiä.



KUVA 4. Testiympäristön rakenne.

Testiympäristössä käytetyt Windows serverit sisälsivät Windows Server 2016 Standard version ja SCCM on 1606 versio eli melko uusi. Versionumerossa alkuosa 16 viittaa vuoteen 2016 ja loppuosa 06 kesäkuuhun (Microsoft 2016a). Olen aiemmin asentanut 15xx versioita SCCM:stä, joten pystyn ympäristöä asentaessa tekemään huomioita eroista aiempaan. Windows Server 2016 standardi sekä datacenter versio tukevat SCCM 1606 versiota päivityksen KB3186654 jälkeen tai lokakuun 2016 jälkeen ilmestyneen version kanssa (Microsoft 2016b).

4.5 Vaatimuksia AD-ympäristölle

AD-ympäristöön asennettaan ADSI Edit ohjelmalla container, johon SCCM tallentaa tarvittavia tietoja. SCCM koneelle annetaan Full Control oikeudet – eli täydet

oikeudet – containeriin. SCCM-asennusmedialta kopioidaan extadsch.exe tiedosta AD/DNS koneelle ja ajetaan se. Extadsch.exe-tiedosto laajentaa AD-ympäristön scheman, mikä vaatii käyttäjältä Schema Admin oikeudet. Kuvassa 5 näkyy AD-ympäristön scheman laajennuksen lokitieto. Lokitiedosta voi havaita, että schemaa laajennettiin sekä atribuuttien että luokkien muodossa. Kuvassa 5 huomioitava kohta on 11:02:28 aikaan oleva onnistunut scheman laajennus tieto.

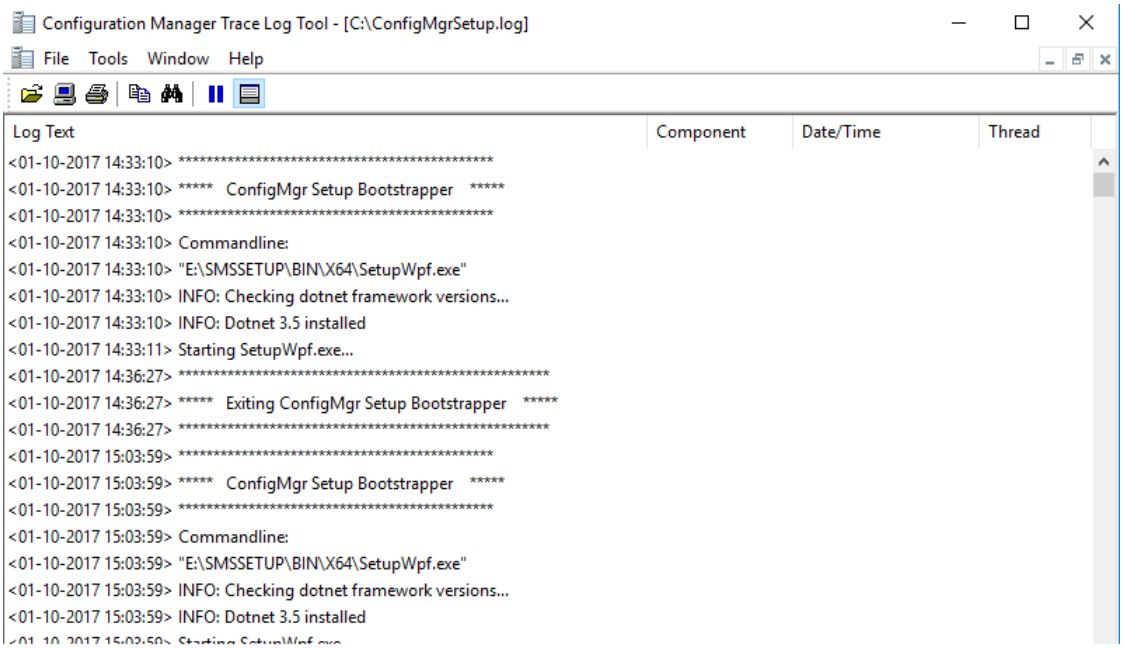
```
<01-10-2017 11:02:24> Modifying Active Directory Schema - with SMS extensions.
<01-10-2017 11:02:24> DS Root:CN=Schema,CN=Configuration,DC=testi,DC=local
<01-10-2017 11:02:25> Defined attribute cn=MS-SMS-Site-Code.
<01-10-2017 11:02:25> Defined attribute cn=mS-SMS-Assignment-Site-Code.
<01-10-2017 11:02:25> Defined attribute cn=MS-SMS-Site-Boundaries.
<01-10-2017 11:02:25> Defined attribute cn=MS-SMS-Roaming-Boundaries.
<01-10-2017 11:02:25> Defined attribute cn=MS-SMS-Default-MP.
<01-10-2017 11:02:26> Defined attribute cn=mS-SMS-Device-Management-Point.
<01-10-2017 11:02:26> Defined attribute cn=MS-SMS-MP-Name.
<01-10-2017 11:02:26> Defined attribute cn=MS-SMS-MP-Address.
<01-10-2017 11:02:26> Defined attribute cn=mS-SMS-Health-State.
<01-10-2017 11:02:26> Defined attribute cn=mS-SMS-Source-Forest.
<01-10-2017 11:02:26> Defined attribute cn=MS-SMS-Ranged-IP-Low.
<01-10-2017 11:02:26> Defined attribute cn=MS-SMS-Ranged-IP-High.
<01-10-2017 11:02:26> Defined attribute cn=mS-SMS-Version.
<01-10-2017 11:02:26> Defined attribute cn=mS-SMS-Capabilities.
<01-10-2017 11:02:27> Defined class cn=MS-SMS-Management-Point.
<01-10-2017 11:02:27> Defined class cn=MS-SMS-Server-Locator-Point.
<01-10-2017 11:02:27> Defined class cn=MS-SMS-Site.
<01-10-2017 11:02:28> Defined class cn=MS-SMS-Roaming-Boundary-Range.
<01-10-2017 11:02:28> Successfully extended the Active Directory schema.

<01-10-2017 11:02:28> Please refer to the ConfigMgr documentation for instructions on the manual
<01-10-2017 11:02:28> configuration of access rights in active directory which may still
<01-10-2017 11:02:28> need to be performed.  (Although the AD schema has now be extended,
<01-10-2017 11:02:28> AD must be configured to allow each ConfigMgr Site security rights to
<01-10-2017 11:02:28> publish in each of their domains.)
```

KUVA 5. AD-ympäristön scheman laajentamisen loki.

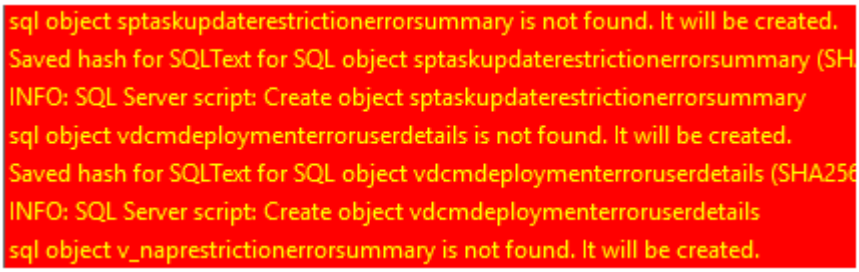
SCCM koneeseen asennetaan Windows 10 ADK, joka on tuettu Configuration Manager 1602 versiota lähtien. Asiakaskoneita varten asennetaan AD-ympäristöön Group Policy Object, jonka avulla asiakaskoneet saavat tietynlaiset palomuuri asetukset. (Microsoft 2010a; Microsoft 2012; Microsoft 2013a; Microsoft 2013d; Microsoft 2016d.)

Itse SCCM:n asentamisesta syntyy myös loki. SCCM asennuksen lopussa on lista onnistuneista ja epäonnistuneista asennusosioista, kaiken tulee olla tässä vaiheessa onnistuneita asennuksia. SCCM asennuksen jälkeen asennusohjelma luo

C:-aseman juureen ConfigMgrSetup.log nimisen lokitiedoston, josta voi katsoa tarkemmin asennuksen onnistumisen. Lokitiedostojen katseleminen onnistuu melkeinpä millä tahansa tekstinkäsittelyohjelmalla, mutta CMTrace.exe nimisellä ohjelmalla, joka löytyy SCCM-asennusmedialta \SMSTOOLS\TOOLS kansion alta, voi lokitiedostoa tutkia reaaliajassa. Esimerkiksi asennuksen aikana esiintyneitä lokeja voi lukea reaaliajassa, kuten kuvasta 6 käy ilmi. Yleensä punaisella värillä CMTrace korostaa virheitä, mutta joissain tapauksissa punainen korostusväri ei tarkoita virhettä, kuten kuvasta 7 käy ilmi. Punainen korostusväri tulee CMTracessa sanojen perusteella, esimerkiksi fail-sanan perusteella. Kuvassa 7 asennus kertoo, ettei tietokannasta löydy tietynlaista tietokantaobjektia ja luo sellaisen. (Microsoft 2015).



KUVA 6. SCCM asennus-loki avattuna CMTrace ohjelmalla.



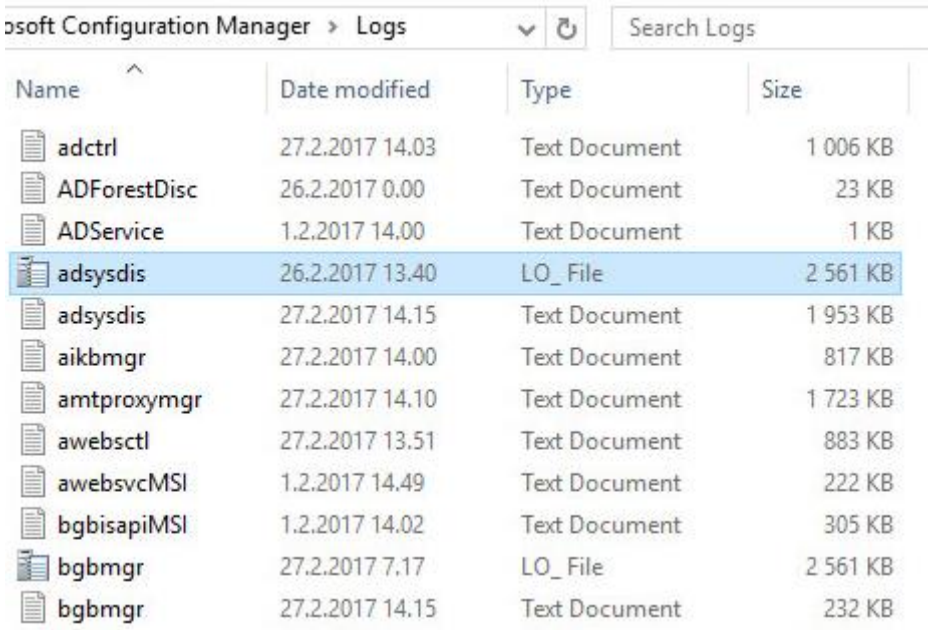
KUVA 7. ConfigMgrSetup.log tiedoston lokitietoja CMTrace ohjelmalla asennuksen aikana.

5 SCCM JA LOKIT

SCCM kerää perusasetuksilla lokitietoa niin palvelinten kuin myös asiakaskoneen prosesseista. SCCM kerää lokitietoja prosessikohtaisesti eri tiedostoihin. Lokitiedot voidaan lajitella Configuration Manager asiakas- (Configuration Manager Client), Site-palvelin- (Configuration Manager Site Server) ja toiminnallisuuslokeihin (Configuration Manager Functionality). (Microsoft 2017c; Microsoft 2015a.)

Asiakaskoneita varten olevat lokit koskevat asiakaskoneiden toimintoja ja asiakasasennuksia. Asiakaslokit löytyvät asiakaskoneesta. Site-palvelimen lokit koskevat Site-palvelimen rooleja ja ne löytyvät Site-palvelimelta. Toiminnallisuuteen liittyvät lokitiedot löytyvät sekä asiakaskoneista tai Site-palvelimelta riippuen toiminnallisuuden tyypistä. Esimerkiksi execmgr.log tiedosto sijaitsee asiakaskoneesta, ja se kertoo asiakaskoneessa suoritettavat paketit ja tehtävät. Toisaalta ADForestDisc.log sijaitsee Site-palvelimella ja se kertoo AD-ympäristössä tapahtuvista objektien etsinnöistä. Käsittelen SCCM:n tuottamia lokeja yleisesti seuraavissa kappaleissa, minkä jälkeen siirryn tämän työn pääaiheeseen eli lokitietoihin Windows-käyttöjärjestelmän asennuksen yhteydessä. Tässä työssä kaikki muut paitsi asiakaslokit löytyvät samalta SCCM-koneelta, koska kaikki SCCM vaatimat toiminnot on asennettu samaan koneeseen – katso kuva 4. (Microsoft 2017c; Microsoft 2015a.)

SCCM kirjoittaa lokeja prosessien perusteella, joita varten on varattu omat lokitiedostot. Lokitiedostot SCCM:ssä erotellaan Windows-koneissa LOG- ja LO_-päätteisiin tiedostoihin. SCCM kirjoittaa tietoa LOG-tiedostoon, kunnes tiedosto saavuttaa maksimikoon, joka on 2,5 megatavua. Kun Windows-koneen LOG-päätteinen tiedosto on saavuttanut maksimikoon, SCCM kopioi sen sisällön LO_-päätteiseen tiedostoon ja alkaa jälleen kirjoittaa prosessille varattua lokia LOG-tiedostoon. Toisin sanoen, jos tiedostoja ei kopioida talteen, niin aikaisemmat lokitiedot menetetään. Jos lokitiedostojen kokoa haluaan Windows-koneissa muuttaa, tulee tehdä muutoksia rekisteritasolla. Kuvassa 8 on nähtävissä, miten lokitietojen Windows-koneissa kierrätyksessä käytetään kahta eri päätettä edellä kuvatulla tavalla. (Desai 2016; Microsoft 2017c; Microsoft 2017d.)



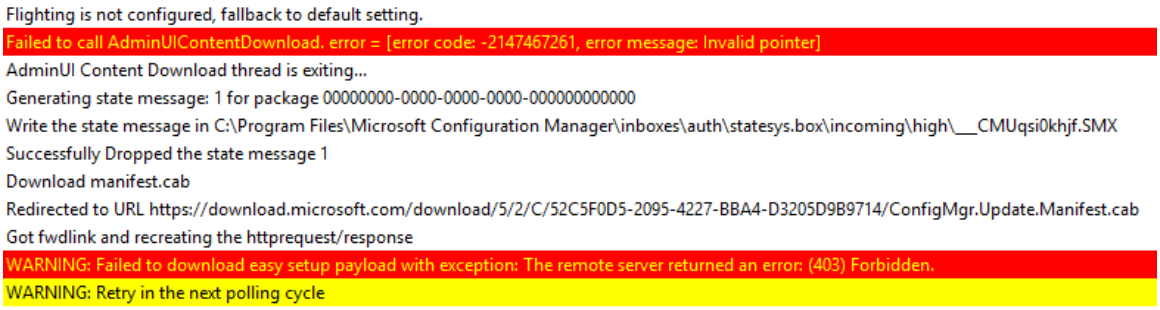
KUVA 8. SCCM tallentaa lokitietoja LOG- ja LO_-päätteisiin tiedostoihin. Kuvassa LOG-päätteiset tiedostot näkyvät Text Document tyyppisinä.

Linux-koneissa ei ole säädetty lokitiedostoilla maksimikokoa. Linux-koneille Microsoft suosittelee käyttämään logrotate-ohjelmaa lokitiedostojen koon ja kierrätyksen hallintaan. Mac-koneille SCCM kirjoittaa neljää eri lokitiedostoa. Mac-koneilla lokitiedot on jaettu asiakas-, agentti-, ilmoitus- ja PrefPane-lokiin (Preference Pane). Tässä opinnäytteessä käsitellään lähinnä Windows-koneiden lokitiedoissa, mutta käsittelen myös lyhyesti Linux-lokitietoja Debianiin perustuvan Ubuntu-koneen avulla. Linux-versiolla ei ole merkitystä lokien sisältöön, kunhan käytössä oleva versio on tuettu SCCM:ssä. (Microsoft 2017c; Microsoft 2017d.)

5.1 SCCM päivitys ennen käyttöä

Oikeassa tuotantoympäristössä SCCM kone ei ole suoraan yhteydessä Internetiin, vaan kaikki sen päivitykset haetaan proxy-palvelimen kautta. Microsoftin dokumentaation mukaan dmpdownloader.log tiedosto sisältäisi vain Microsoft Intunen kautta tulevat lataukset ja siten päivitykset. SCCM Site-palvelimeen asetetaan proxy, josta päivitykset ladataan, ja päivitysten lokitieto löytyy dmpdownloader.log

tiedostosta. SCCM on syytä päivittää ennen käyttöä. Kuvassa 9 näkyy lokitietoa päivityslatauksista. Kuvan 9 tilanteessa proxy-palvelin ei ole vielä sallinut SCCM:n ladata päivityksiä ja SCCM ilmoittaa estosta. Tämän työn lopullisessa käyttöympäristössä SCCM kone on yhteydessä ulkopuolisiin verkkoihin proxy-palvelimen kautta. SCCM päivitettiin ennen käyttöönottoa 1610 versioon ja siihen asennettiin kaikki saatavilla olevat päivitykset. (Microsoft 2017c.)



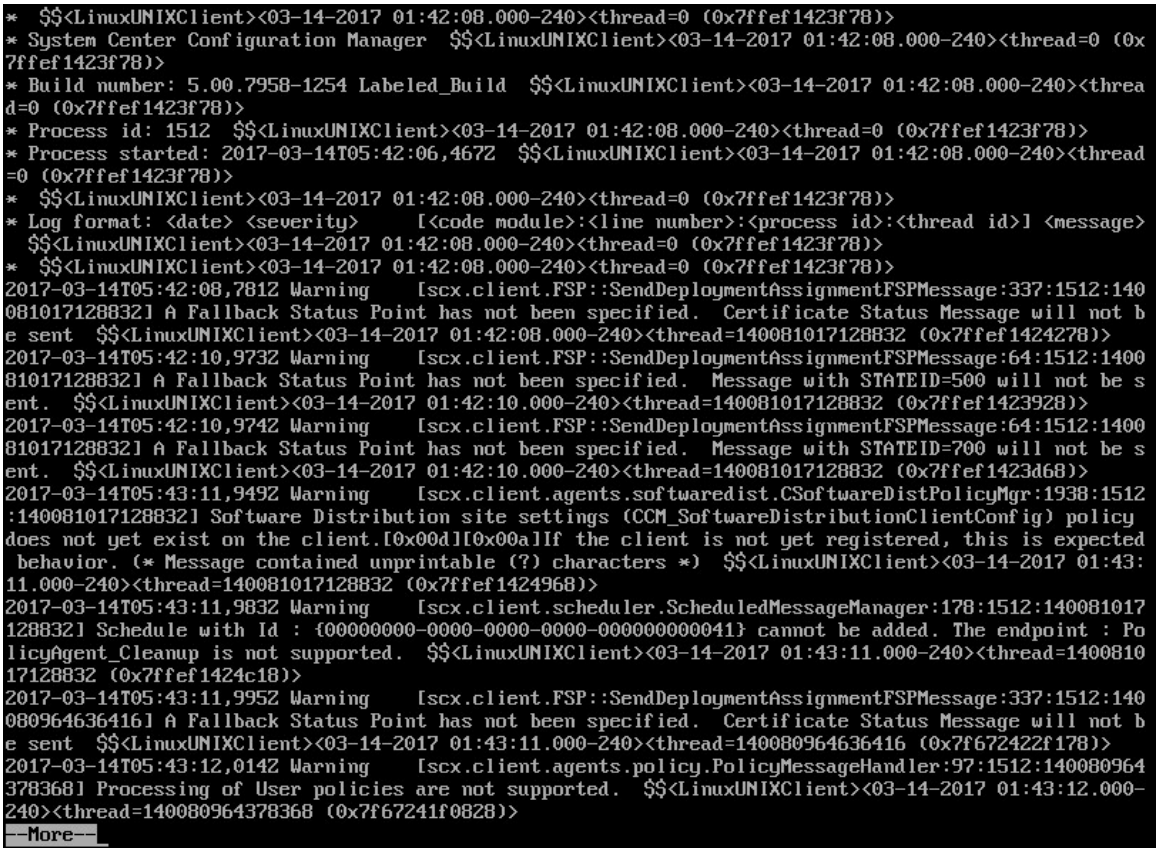
Kuva 9. Dmpdownloader.log tiedoston lokitietoa.

5.2 Asiakaskoneiden lokitiedostojen sijainnit

Asiakaskoneen lokit sijaitsevat Windows-koneilla asiakasohjelmiston asennuksen jälkeen kansiossa \\Windows\CCM\Logs. Testiympäristössä käytössä oli 1606 ja tuotantoympäristössä 1610 versio – uusin kirjoitushetkellä – Configuration Managerista. Microsoft jaottelee asiakaslokit neljään eri luokkaan, joita ovat asiakastoiminnotloki, asiakasasennusloki, asiakkuusloki Linuxia tai UNIX:ia varten sekä asiakkuusloki Mac-tietokoneita varten. (Microsoft 2017c; Microsoft 2015c.)

Linux koneissa lokitietoja kerätään kahteen eri tiedostoon, joita ovat Scxcm.log ja Scxcmprovider.log tiedostot. Scxcm.log tiedosto sijaitsee /var/opt/microsoft/ kansiossa ja Scxcprovider.log tiedosto /opt/microsoft/omi/ kansiossa. Scxcmm.log tiedosto sisältää tietoja ccmexec.bin tiedoston operaatioista ja Scxcmprovider.log tiedosto nwserver.bin tiedoston tietoja. Linuxissa SCCM:n lokitiedostojen asetuksia voi vaihtaa /opt/microsoft/configmgr/etc/scxcm.conf tai /opt/microsoft/omi/etc/scxcmprovider.conf tiedostosta. Kumpaakin Linuxin conf-tiedostoon

voidaan asettaa tasoksi joko ERROR, WARNING, INFO tai TRACE. Microsoft ohjeistaa käyttämään ERROR tasoa normaaleissa käyttöolosuhteissa. ERROR taso kertoo ongelmista, joihin tulee reagoida, WARNING kertoo mahdollisista ongelmista ja INFO kertoo enemmän tietoa eri prosesseista kuin ERROR sekä WARNING. TRACE taso kerää kaikkein eniten tietoa asiakaskoneen toiminnoista. Testasin TRACE tasoa, ja muutamassa minuutissa lokitiedoston koko oli saavuttanut 2,7 megatavun suuruuden, joten Microsoftin suosituksia on syytä noudattaa. Kuvassa 10 WARNING tasolla syntynyttä lokitietoa Ubuntu koneesta. (Microsoft 2017c.)



Kuva 10. Ubuntu koneen scxcm.log tiedoston sisältöä WARNING tasolla.

5.3 SCCM ja lokit käyttöjärjestelmän asennuksessa

Tämän kappaleen ja sen alikappaleiden alle tulen selvittämään lokitietojen yhteyttä SCCM:n avulla tapahtuvaan Windows 10 käyttöjärjestelmän asennukseen. Aluksi käyn läpi joitain verkon kautta tapahtuvaan käyttöjärjestelmän asennukseen liittyviä asioita.

Työn tavoite on asentaa Windows 10 käyttöjärjestelmä asiakaskoneeseen. Tavoite on saavuttaa käyttöjärjestelmäasennus, jossa asentajan ei asennuksen aikana tarvitse osallistua asennukseen, eli ZTI asennuksena. Asennus koostuu käyttöjärjestelmän levykuvasta sekä halutuista ohjelmistoista. Ohjelmat sekä laitteiston ajurit asentuvat käyttöjärjestelmäasennuksen yhteydessä. Asennuksen jälkeen käyttäjällä on käytössään käyttövalmis käyttöjärjestelmä ohjelmistoineen. Ohjelmistot voitaisiin laittaa käyttöjärjestelmän levykuvan sisään, mutta SCCM mahdollistaa ohjelmistojen asentamisen erillään käyttöjärjestelmästä. Ohjelmiston erottaminen käyttöjärjestelmän levykuvasta helpottaa laitteiden ylläpitoa. Kun halutaan asentaa uudempi versio käyttöjärjestelmästä, ei täydy päivittää kuin käyttöjärjestelmän levykuva. Myös käyttöjärjestelmäasennus erilaisiin konekokoonpanoihin helpottuu, koska eri kokoonpanoja varten täytyy tehdä vain konekohtaiset ajuripaketit.

Seuraavissa luvuissa on käsitelty ZTI-asennuksen vaatimia asioita. Lokien suhteen tähän työhön valitsin lokitiedostoja, joita olen käyttänyt hyödyksi ratkaistaessa erinäisiä ongelmia käyttöjärjestelmää asennettaessa. Tällainen valinta lokien suhteen ei ole tieteellisesti täysin objektiivinen, mutta jonkinlainen valinta oli tehtävä. Liitteessä 2 esitellyt Microsoftin listaamat lokit, jotka liittyvät käyttöjärjestelmän asentamiseen, mitkä tosin eivät kattaneet kaikkia lokitiedostoja, joita seuraavassa esitellään. Jokaisen lokitiedoston yhteydessä on valintaperustelu.

5.3.1 PXE-boot

Käyttöjärjestelmä asennetaan verkon kautta käyttäen PXE-käynnistystä. SCCM:stä tulee asettaa PXE-käynnistys päälle haluttuun Distribution pointiin. Kun

PXE-käynnistys asetetaan päälle SCCM koneeseen, WDS-rooli (Windows Deployment Service) asentuu automaattisesti. Windows Serverissä voitaisiin käyttää pelkkää WDS-rooliakin käyttöjärjestelmien asentamiseen verkon kautta, mutta SCCM hoitaa lähes kaiken automatisoinnin, mitä pelkkä WDS ei tee. WDS-roolin automaattinen asennus tarkoittaa myös sitä, ettei sen asetuksia muuteta. Itse asiassa SCCM ei aseta WDS-rooliin WDS-asennuksen kannalta tärkeitä asetuksia. Eli SCCM konetta ei voida käyttää suoranaisesti pelkkien WDS-asennusten yhteydessä, jos sen asetuksia ei muuteta. SCCM käyttää WDS-roolia PXE:n kautta tapahtuvissa asennuksissa. (Microsoft 2016e; Microsoft, 2014b; Microsoft 2008b.)

5.3.2 Wake on Lan

Jotta sammutettu tietokone voidaan avata verkon kautta, tulee asetuksien tukea verkon kautta herättämistä. Verkon kautta koneen käynnistämistä kutsutaan Wake on Laniksi (WOL). SCCM:stä tulee asettaa Sitelle WOL ominaisuus päälle. Vaihtoehtona on valita *Subnet Directed Broadcast* tai *Unicast asetus. Subnet Directed Broadast* lähettää aliverkkokohtaisesti broadcast lähetyksen ja käyttää hyväksi koneen MAC-osoitetta käynnistääkseen halutun koneen. *Unicast* asetus taas lähettää IP-kohtaisesti herätyskäskyn käyttäen hyväksi koneen MAC-osoitetta. Unicast asetus ei siis osaa käynnistää konetta, jos kone on saanut DHCP:ltä eri ip-osoitteet kuin minkä SCCM kone näkee juuri herätyksen aikaan. Perusasetuksilla SCCM:ssä on asetettu koneen tietojen hakuun 7 päivää, joten asetuksia testatessa päivityksen aikaväli kannattaa asettaa pienemmäksi. WOL:n avulla voidaan siis asentaa ohjelmistoja koneisiin, jotka ovat asennuksen alkamisajankohtana kiinni. (Allen 2016.)

Tässä työssä verkon kautta tapahtuva laitteiden käynnistys ei ollut keskiössä. Testasin WOL-käynnistystä testiympäristössä ja sen käyttöönotossa ei ilmennyt ongelmia. Hyper-V ei tue WOL:ia virtuaalikoneiden suhteen, mutta kohdekoneen ollessa fyysinen ei testiympäristössä esiintynyt ongelmia. SCCM:n käynnistyslevykuviin kannattaa asentaa kohdekoneen verkkokortin ajurit, jotta WOL toimii ongelmitta. Kohdekoneen asetuksista tulee myös asettaa päälle WOL-käynnistyksen vaatimat asetukset. Site-palvelimella sijaitsee wolcmgr.log ja wolmgr.log tiedostot.

Wolcmgr.log tiedosto sisältää tiedot asiakaskoneista, joihin tulee lähettää WOL-herätepaketti sekä tiedot lähetettyjen pakettien määrästä. Wolmgr.log tiedosto sisältää tietoja ajankohdista, jolloin WOL-asennuksia on asetettu. (Allen 2016; Microsoft 2017c; Microsoft 2015a.)

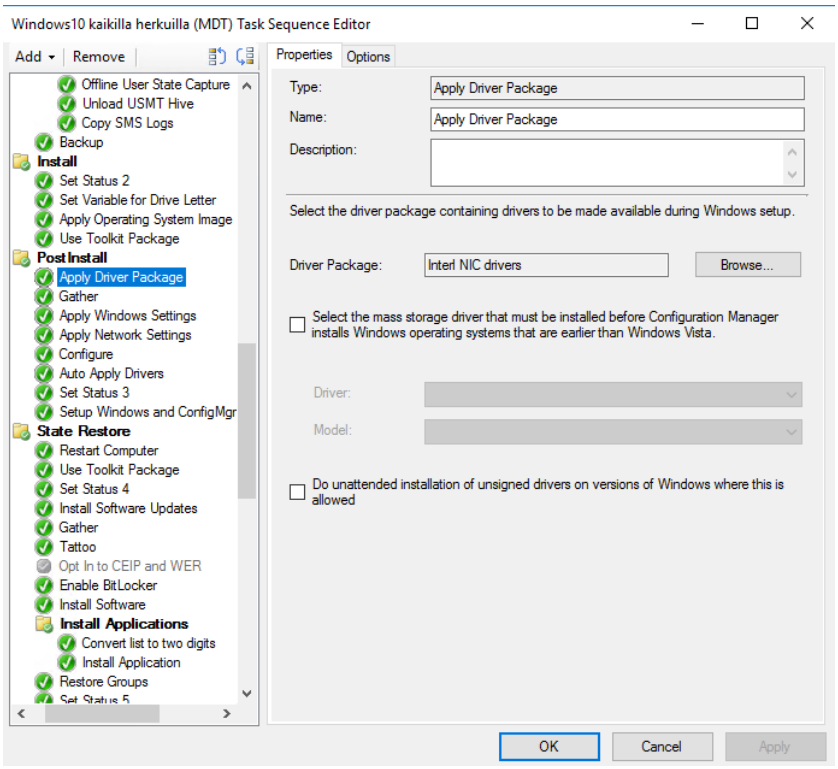
Täytyy myös huomioida, että verkon kautta tapahtuva käyttöjärjestelmän asennus vaatii sen, että koneen käynnistysasetuksista on asetettu verkon kautta tapahtuva käynnistys prioriteeteissa ensimmäiseksi. Verkon kautta tapahtuvan käynnistyksen asettaminen ensimmäiseksi aiheuttaa sen, että kone joka käynnistyksellä olisi halukas ottamaan vastaan verkon kautta tulevan asennuksen. On siis tärkeää, että SCCM:n asetuksissa ei ole turhia käyttöjärjestelmäasennuksia, jottei synny edes mahdollisuutta, että ei haluttuun koneeseen asentuisi väärä käyttöjärjestelmä verkon kautta tapahtuvan käynnistyksen ollessa käytössä. Tämän työn puitteissa tuotantoympäristön lopullisissa kohdekoneissa joudutaan kone käynnistämään asentajan toimesta verkon kautta. Jos käyttöjärjestelmäasennuksessa kyseessä olisi suuri määrä uusia koneita, olisi verkon kautta tapahtuvan käynnistyksen priorisoiminen ensimmäiseksi perusteltua. (Allen 2016.)

5.4 Käyttöjärjestelmäasennuksen automatisointi

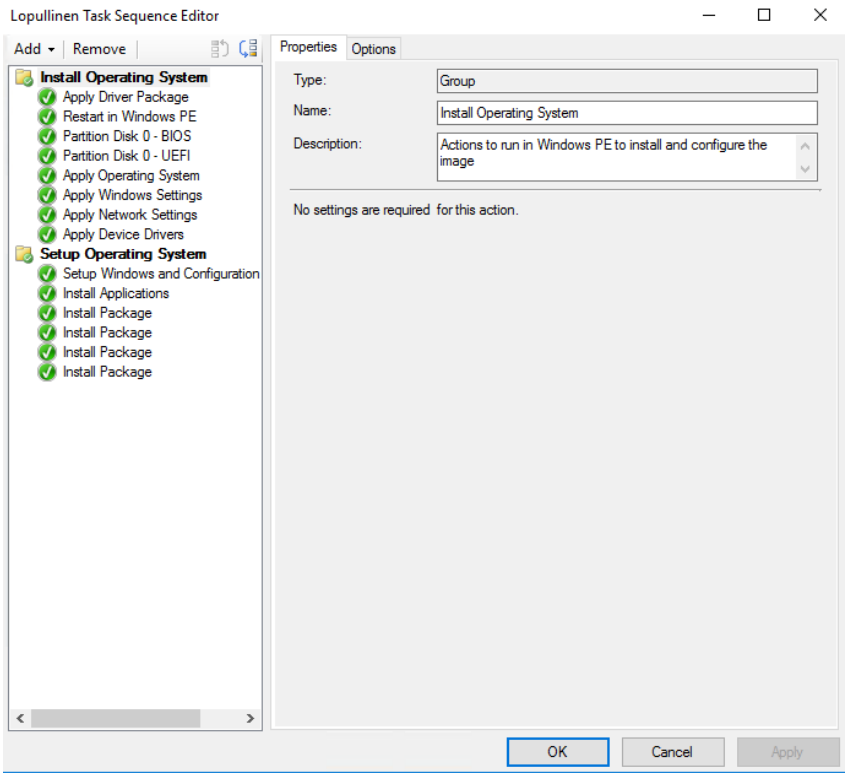
Kuten edellä on mainittu käyttöjärjestelmäasennukset kohdistuvat Windows koneisiin. Käyttöjärjestelmän asennusta varten Microsoft listaa liitteen 2 mukaiset lokitiedostot. Osa käyttöjärjestelmän asennukseen liittyvistä lokeista sijaitsevat asiakaskoneessa, Configuration Manager Consolen sisältävässä koneessa tai Site-palvelimella. Tässä työssä Consolea käytetään pääsääntöisesti Site-koneelta, joten lokit sijaitsevat kahdessa eri paikassa – varsinkin testatessa asennuksia. Konsoli voidaan asentaa mihin koneeseen halutaan, kunhan käyttäjällä on vaadittavat oikeudet SCCM:ään. Windows asiakaskoneella tiedostot sijaitsevat c:\Windows\CCM\Logs kansiossa ja Site-palvelimella C:\Program Files\Microsoft Configuration Manager\Logs sekä c:\Program Files\SMS_CMM\Logs\ kansiossa. (Microsoft 2017c; Microsoft 2015a.)

Käyttöjärjestelmä voidaan asentaa SCCM:n avulla kahdella eri tavalla. Käyttöjärjestelmän voi asentaa suoraan luomalla asennusta varten tavallisen Task Sequencen, johon määritellään halutut ohjelmistot ja ajurit laitteistolle. Käyttöjärjestelmä voidaan asentaa ilman ohjelmistoja ja ajureitakin, mutta se ei ole järkevää, jos halutaan tuottaa käyttövalmis asennus. Toinen tapa on asentaa SCCM:ään MDT (Microsoft Deployment Toolkit) työkalu. MDT:tä voi käyttää ilman SCCM:äkin käyttöjärjestelmien asentamiseen, mutta SCCM ja MDT yhdistelmällä voidaan saavuttaa asennus ilman käyttäjän interaktiota asennuksen aikana, ns. Zero Touch Installation (ZTI). Tässä työssä on keskitytty luomaan ns. tavallinen Task Seuence, joka hoitaa asennuksen ilman käyttäjän interaktiota. Tässä vaiheessa voidaan todeta, että ZTI-asennus onnistuu hyvin ilman MDT:ä. (Microsoft 2013e.)

MDT:n yhdistäminen SCCM:ään tuo käyttöjärjestelmäasennuksiin muokattavuutta. Asennettaville paketeille voidaan määritellä ehtoja, esim. ohjelmistopaketti asennetaan vain, jos kone täyttää tietyt ehdot. Ehtona voi olla esimerkiksi tietyn merkkinen kone. AD-ympäristöä varten voidaan määritellä, että työpöytäkoneet asennetaan tiettyyn Organization Unittiin (OU) ja kannettavat koneet omaansa. MDT:n avulla voidaan myös testata asennusten onnistumista simulaation avulla, ilman että asennus jouduttaisiin asentamaan kokonaan testin vuoksi. MDT:n avulla voidaan myös valvoa asennuksia reaaliajassa. Microsoft suosittelee käyttämään MDT:ä myös käyttöjärjestelmälevykuvan tekoon. MDT nopeuttaa levykuvan tekoa sekä mahdollistaa levykuvan käytön eri yhteyksissä, kuten WDS tai VDI käytössä. Kuvissa 11 ja 12 nähdään MDT:n avulla luotu Task Sequencen ja ns. tavallisen Task Sequencen eroja. MDT tuo automaattisesti enemmän muokattavuutta asennukseen. Kuitenkin on huomioitavaa, että tavallista Task Sequenceakin voidaan räätälöidä MDT-asennuksen kaltaiseksi, kuten tässä työssä onkin tehty. (Microsoft 2017g.)



Kuva 11. MDT:n asetuskuva SCCM:ssä käyttöjärjestelmäasennuksissa.



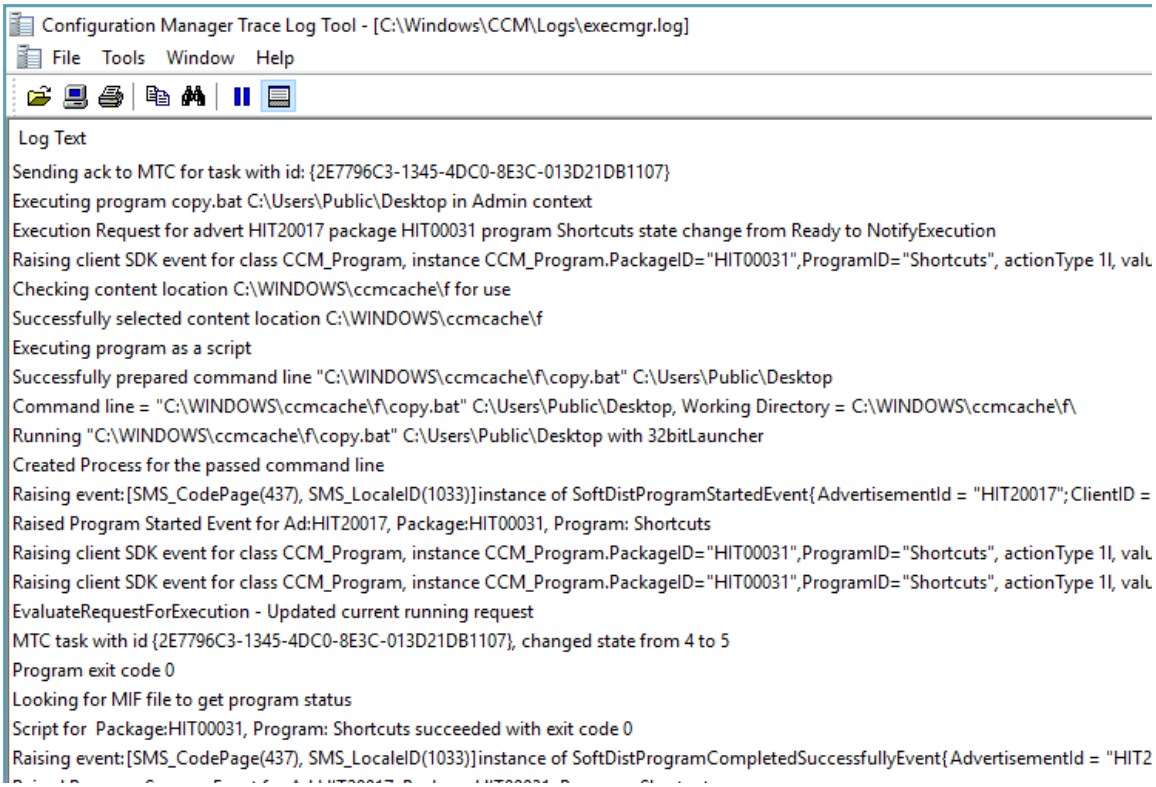
Kuva 12. Tavallinen Task Sequence käyttöjärjestelmäasennusta varten.

5.4.1 Asiakaskoneiden lokit

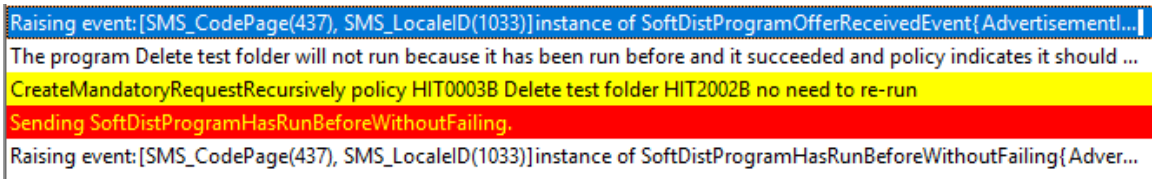
Asiakaskoneiden lokit löytyvät kansiosta c:\Windows\CCM\Logs, kuten edellä on tullut ilmi. Hyödyllisiä lokeja ohjelmien ja käyttöjärjestelmän asennuksessa ovat AppEnforce.log, execmgr.log ja smsts.log. Kolmesta lokitiedosta, jotka esittelen, vain smsts.log on Microsoftin luokittelussa käyttöjärjestelmäasennuksiin liittyvä loki. Asiakaskoneen ccmsetup.log tiedosto, joka mainitaan liitteessä 2 liittyen käyttöjärjestelmä asennuksiin, on tärkeä loki, jos asiakkuus lisätään jälkikäteen. Tämän työn kohdekoneista ei edes löydy ccmsetup.log tiedostoa, koska asiakkuus on lisätty käyttöjärjestelmäasennuksen yhteydessä. On myös huomioitava, että ccmsetup.log luokitellaan myös asiakasasennuslokiksi. Liitteessä 2 oleva TSAgent.log kerää Microsoftin mukaan tietoja Task Sequencejen riippuvuuksista ennen asennuksia. Kuitenkaan TSAgent.log tiedostoa ei löytynyt asiakaskoneelta. (Microsoft 2017c; Microsoft 2015a.)

5.4.1.1 Exemgr.log

Exemgr.log tiedosto sisältää tietoa asiakaskoneessa käynnissä olevista tai suoritetuista Task Sequenceista tai asennettavista paketeista. Kuvissa 13 ja 14 on nähtävissä exemgr.log tiedoston sisältöä. Exemgr.log tiedoston tieto oli hyödyllistä testatessa paketein (Package) asennettavia ohjelmia. Esimerkiksi jotkin ohjelmat ovat sellaisia, että niiden asennus koostuu vain tiedostojen kopioinnista kohdekoneeseen, kuten kuvasta 13 näkyy. Exemgr.log tiedoston mukaan asennukset onnistuivat, vaikka tiedostot eivät olleet kopioituneet oikeaan kansioon. Selvisi, että komennosta puuttui lainausmerkit kohdekansion suhteen ja tiedostot olivat kopioituneet hieman väärän nimiseen kansioon. Ilman lainausmerkkejä kansion useampisanaiset kansiot toimivat vain ensimmäisen sanan suhteen. Kuvassa 14 näkyy testiympäristössä usein eteen tullut ongelma. Jos deployment asetukset ovat tietynlaiset, ei deployment asennu enää uudestaan, jos se on onnistuneesti asennettu SCCM:n näkökulmasta. Deployment asetuksista voidaan asettaa deployment sellaiseksi, että se asentuu aina riippumatta edellisen asennuksen tilasta. (Microsoft 2017c.)



Kuva 13. Exemgr.log tiedoston sisältöä.

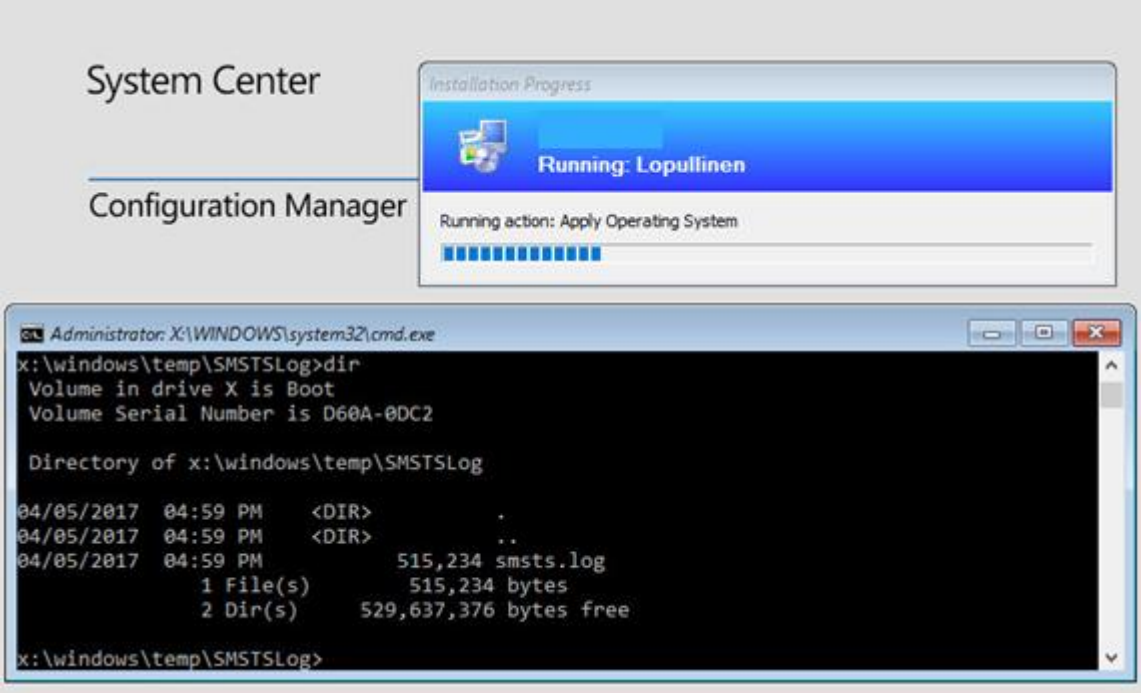


Kuva 14. Execmgr.log tiedosto kertoo, että ohjelma on jo asennettu, eikä sitä siksi asenneta uudestaan.

5.4.1.2 Smsts.log ja Appenforce.log

Smsts.log kerää tietoa Task Sequencien aktiivisuudesta. Smsts.log on myös paikka, josta voi käyttöjärjestelmän asennuksen aikana tutkia ongelmaa, jos jokin Task Sequence jää suoriutumatta. Painamalla F8-näppäintä käyttöjärjestelmän asennuksen aikana pääsee komentokehotteen kautta käsiksi smsts.log tiedos-

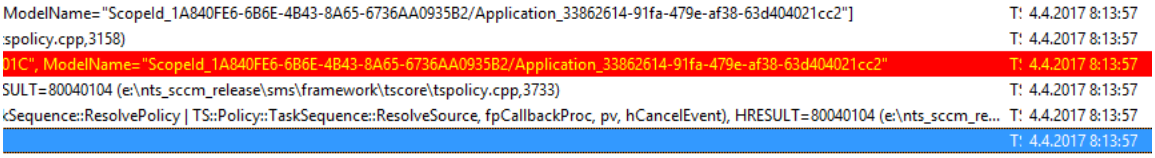
toon. Smsts.log tiedosto sijaitsee käyttöjärjestelmän asennuksen aikana x:\windows\temp\smstslog\ kansiossa ja siirtyy asennuksen jälkeen kansioon c:\Windows\CCM\logs asiakasohjelmiston asennuksen jälkeen. Asennuksen aikana smsts.log tiedoston voi kopioida palvelimelle tutkittavaksi net use ja copy komentojen avulla. AppEnforce.log kerää tietoa asennetuista ohjelmistopaketeista. AppEnforce.log tiedostosta näkyy komentotasolla, miten ohjelma on asennettu. Kuvassa 15 nähtävissä smsts.log tiedoston sijainti käyttöjärjestelmäasennuksen aikana. Näin jälkikäteen voi sanoa, että smsts.log tiedosto on hyvin tärkeä käyttöjärjestelmäasennuksia tehdessä ja sitä tulikin tutkittua eniten kaikista lokeista. (Microsoft 2017c; Microsoft 2015c.)



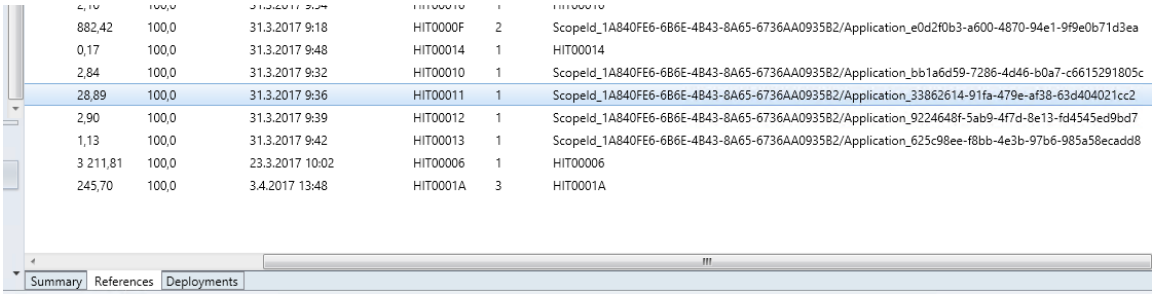
Kuva 15. smsts.log tiedoston sijainti käyttöjärjestelmäasennuksen aikana asiakaskoneella.

Kuvissa 16 ja 17 nähtävissä käyttöjärjestelmän asennuksen aikana ilmennyt ongelma ohjelman asennuksessa. Smsts.log tiedosto kopioitiin virheilmoituksen aikaan asiakaskoneelta SCCM-palvelimelle. Smsts.log tiedosto sisältää tiedon oh-

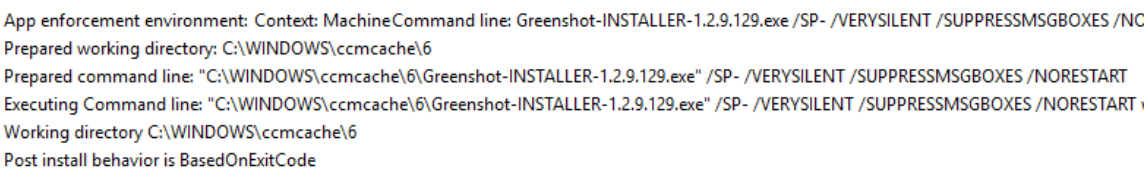
jelmasta, jonka asennus aiheutti. Kuvassa 16 punaisella pohjalla näkyy kohta Application_33862614 alkuinen tieto. Kyseisen tiedon avulla voidaan SCCM konsolista nähdä kuvan 17 mukaisesti käyttöjärjestelmän Task Sequencen alta, mihin ohjelmaan smsts.log tiedoston tieto voidaan yhdistää. Tämän opinnäytteen asennusten aikana muutama ohjelma aiheutti kyseisen virheilmoituksen ja ongelma korjaantui tekemällä virheilmoituksen aiheuttaneesta ohjelmasta uusi asennuspaketti SCCM:ää varten. Kuvassa 18 ja 19 nähdään AppEnforce.log tiedostosta Greenshot nimisen ohjelman asennus ja poistaminen. Kuvissa 18 ja 19 näkyy, mitä komentoa ohjelman asentamiseen ja poistamiseen on käytetty.



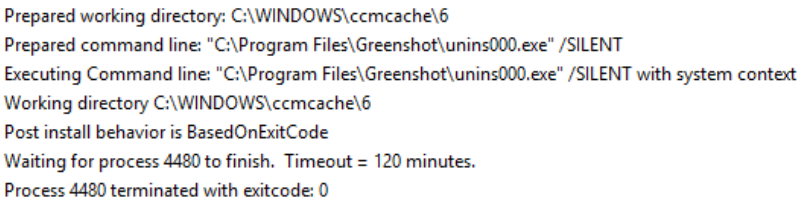
Kuva 16. Asiakaskoneen smsts.log tiedoston sisältöä käyttöjärjestelmäasennuksen aikana.



Kuva 17. Näkymä Task Sequenceen liitetyistä ohjelmista SCCM Consolessa.



Kuva 18. AppEnforce.log tiedoston lokitietoa ohjelman asennuksesta.



Kuva 19. AppEnforce.log tiedoston lokitietoa ohjelman poistamisesta.

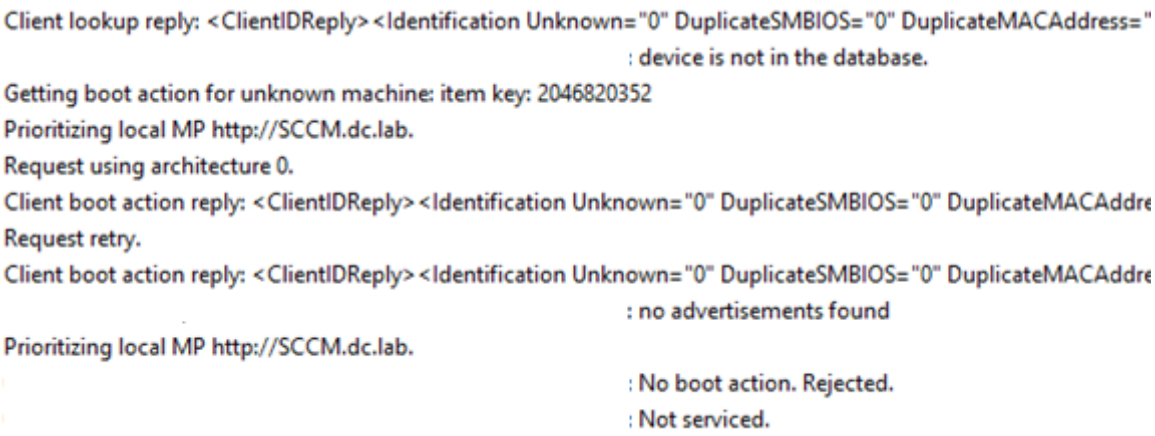
5.4.2 Site-palvelimen lokit

Site-palvelimella sijaitsevia hyödyllisiä lokitiedostoja ovat distmgr.log, smspxe.log, DriverCatalog.log ja pfirewall.log. Distmgr.log tiedosto kertoo tiedon pakettien valmistumisesta, PXE:n asettamisen Distrbution pointiin sekä kertoo Distribution pointille tulevista sisältökyselyistä. Smspxe.log tiedostoon kerätään tietoa asiakaskoneiden PXE-käynnistyksistä tietyin käynnistyskuvin. DriverGatalog.log tiedosto kertoo katalogiin tallennetut ajurit. Ajureiden asentaminen käyttöjärjestelmän yhteydessä tekee laitteiston käyttövalmiiksi heti asennuksen jälkeen. Pfirewall.log tiedosto on Windows Serverin palomuurin lokitiedosto, johon kerätään tietoa palomuurin tekemistä estoista sekä sallituista toimenpiteistä. Esittelen myös lopussa MP_Hinv.log tiedoston sisältämät tiedot, vaikka eivät tiedot suoranaisesti liity käyttöjärjestelmäasennukseen, vaan asiakaskoneen laitteiston tietoihin. Mainitaan vielä, että useita liitteessä 2 olevia lokeja ei löytynyt Site-palvelimelta. SCCM luo lokitiedoston, kun jotain ominaisuutta käytetään ensimmäisen kerran, joten lokitietojen puuttuminen johtui todennäköisesti ominaisuuden käyttämättömyydestä. (Microsoft 2017c; Microsoft 2015a.)

5.4.2.1 Smspxe.log

Kuvassa 20 nähtävissä epäonnistunut asennuksen käynnistyminen smspxe.log tiedoston kertomana. Hyvin usein tämän työn aikana epäonnistuneet käynnistymiset johtuivat siitä, että PXE-käynnistys oli kohdistettu tuntemattomiin tietokoneisiin (Unknown Computers) SCCM-koneesta. Jos SCCM-koneesta halutaan asentaa käyttöjärjestelmä uusiin eli tuntemattomiin koneisiin, ei asennettavana oleva

kone saa esiintyä SCCM:n listoissa lainkaan, eikä näin myöskään tietokannassa. Jos asennus on edes käynnistetty uudessa koneessa, niin kyseinen kone ilmestyy tuntemattomana koneena SCCM:n konelistaan, tietyllä viiveellä. Ongelma häviää poistamalla kone SCCM:n konelistasta ja käynnistämällä PXE-käynnistys uudelleen. Kohdekoneet voidaan lisätä SCCM:ään etukäteen MAC-osoitteilla, joten niistä tieto on tietokannassa ja smspxe.log kertoo tiedon asennuksen alkaessa. Etukäteen koneen lisääminen SCCM:ään parantaa tietoturvaa ja asennuksen onnistumista, koska asennus kohdistuu yksiselitteisiin MAC-osoitteisiin, eikä kaikkiin mahdollisiin uusiin koneisiin, myös ei haluttuihin. Toki SCCM:stä voidaan säätää asennuksen alkaminen salasanan taakse, jotta ei haluttuja koneita ei ilmesty organisaation verkkoon, jos käytetään Unknown Computers valintaa.

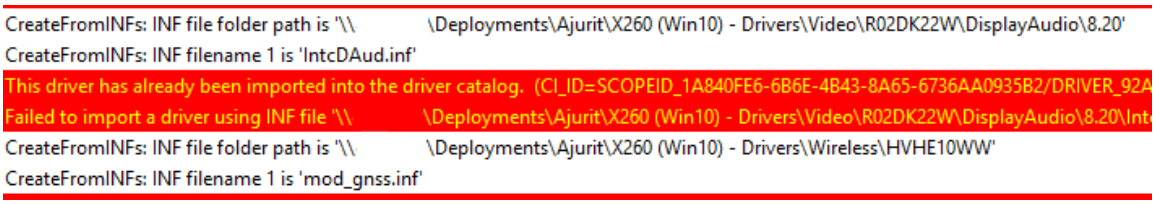


Kuva 20. Smspxe.log tiedoston tieto epäonnistuneesta PXE-asennuksen käynnistymisestä.

5.4.2.2 DriverCatalog.log

Tässä työssä lopullinen kone haluttiin mahdollisimman käyttövalmiiksi, joten koneen ajurit asennettiin käyttöjärjestelmäasennuksen yhteydessä. DriverCatalogista voi katsoa, mitkä ajurit on lisätty katalogiin. Kohdekoneiden ollessa hyvin samankaltaisia voi ilmetä DriverCatalogista kuvan 21 mukainen asia. Kuvasta 21 huomataan, että tiettyjen konepakettien SCCM-ajuripaketit sisältävät samoja ajureita, eikä niitä asenneta uudelleen katalogiin. SCCM:n puolella ajureiden päällekkäisyys näkyy siten, ettei listoihin ilmestyä uusia ajureita, vaan ajureiden kohdalle

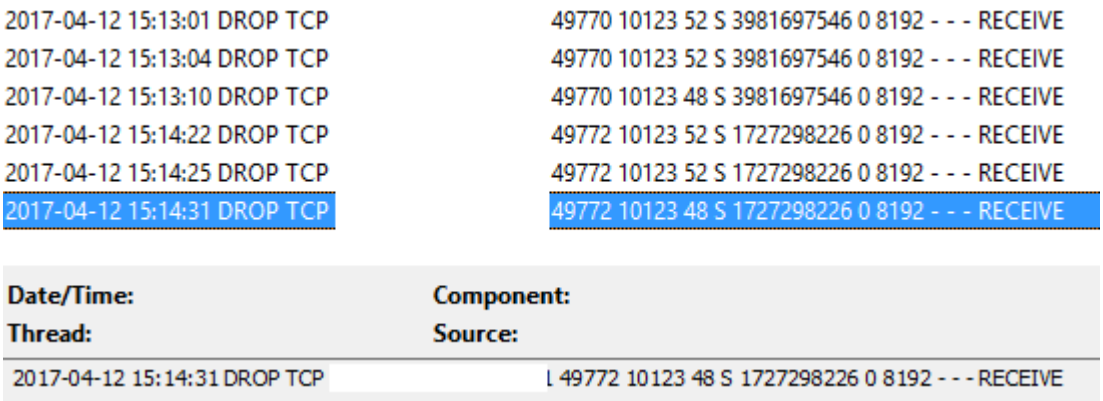
ilmestyy usea konekategoria. Jos koneita ei kategorioi SCCM:ssä voi ajureiden ilmestymättömyys listaan tai konekohtaisiin kansioihin olla odottamatonta. (Microsoft 2015a.)



Kuva 21. Ajurien katalogiointia DriverCatalog.log tiedostosta.

5.4.2.3 Pfirewall.log

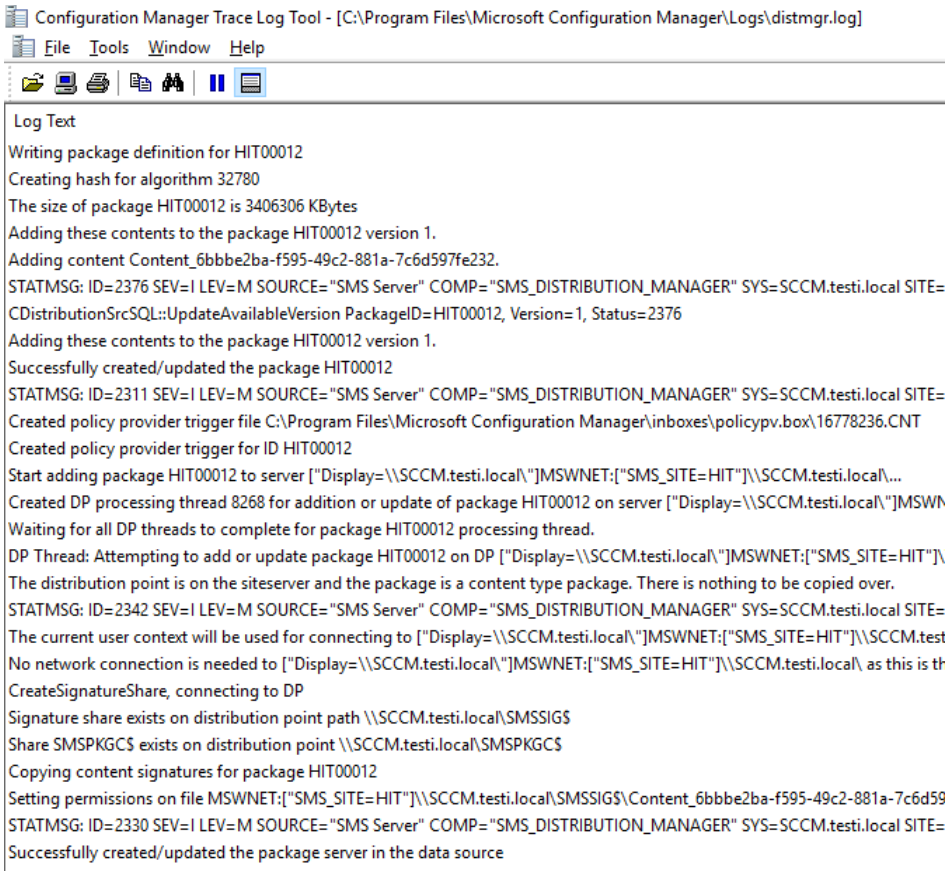
Windows Firewallin tuottamat lokitiedot menevät perusasetuksilla %systemroot%\system32\LogFiles\Firewall\pfirewall.log tiedostoon. Palomuurin lokin sijainnin voi muuttaa haluamakseen ja kannattaa tarkistaa onko lokien kirjaaminen yleensäkään päällä palomuurin suhteen. Palomuurin lokitiedoista ei sinänsä ollut tämän työn suhteen suurta hyötyä, koska kaikki SCCM:n vaatimat osat sijaitsevat samalla koneella. Jos SCCM hajautettaisiin usealle eri koneelle, voisi palomuurin lokitiedoista olla hyötyä. Eräässä työn vaiheessa oli epäilys, että palomuuri voisi estää onnistuneen asennuksen, mutta palomuurin lokin mukaan mitään ei oltu estetty. Lokin tutkiminen auttoi poissulkemaan palomuuriasetukset. Kuvassa 22 on nähtävissä Windows palomuurin lokitietoja – kuvasta 22 poistettu IP-osoitteet.



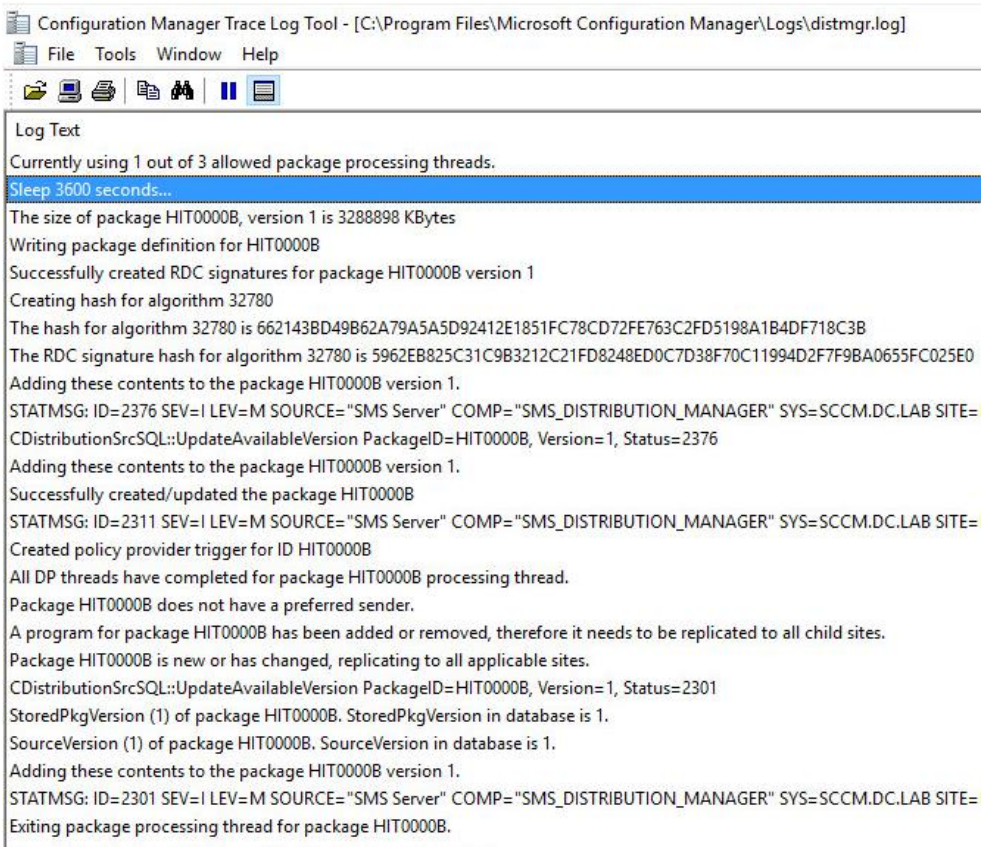
Kuva 22. Windows Firewall lokitietoa.

5.4.2.4 Distmgr.log

SCCM:ssä kaikista asennettavista ohjelmista tehdään ensin paketti tai Task Sequence, joka asennetaan kohdekoneeseen verkon kautta. Distmgr.log tiedosto sisältää tiedon tehdyista paketeista ja niihin kohdistuneista päivityksistä. Distmgr-lokitiedosto sisältää tietoa asennettavista paketeista, lähinnä sen, onko paketti valmis asennettavaksi. Distmgr-lokitiedosto kertoo paketin ID-numeron, koon ja sijainnin, mihin paketti on tallennettu. Kuvassa 23 on näkyvissä Chrome-selainta varten tehdyn paketin loki. Samaan tapaan Windows 10 imagea varten tehdyn Task Sequencen tiedot kuvassa 24. Windows-käyttöjärjestelmän levykuvasta tehty Task Sequence ja ohjelmistoista tehdyt paketit mahdollistavat käyttöjärjestelmän asennuksen verkon kautta. (Microsoft 2015a; Microsoft 2017c.)



Kuva 23. Distmgr-lokin tietoa Chrome-selainpaketin asennuksesta. Paketin nimi kuvassa HIT00012.

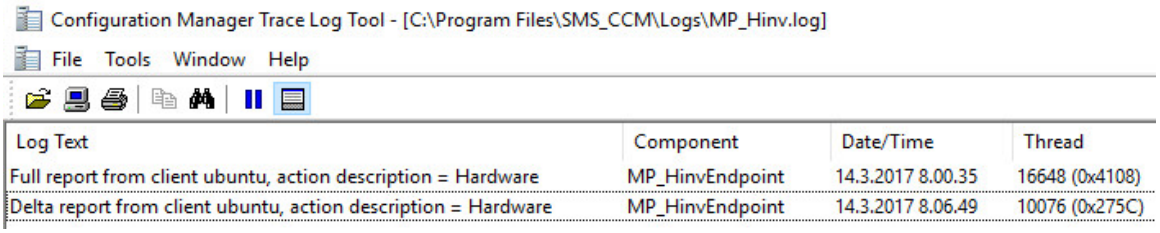


Kuva 24. Windows 10 image-paketin luomisloki. Paketin nimi kuvassa HIT0000B.

5.4.2.5 MP_Hinv.log

MP_Hinv lokitiedosto sijaitsee c:\Program Files\SMS_CMM\Logs\ kansiossa Site-palvelimella. MP_Hinv lokitiedosto kertoo, kun asiakaskoneiden tiedot niin ohjelmiston kuin myös rautatason suhteen on lähetetty Site-palvelimelle. Kuvassa 25 näkyy Ubuntu-jakelun lokitieto lähetetyistä tiedoista Site-palvelimelle. Samalla tavalla Windows-koneet lähettävät tietoa omasta raudastaan ja asennetuista ohjelmista. Kuvassa 25 kummallakin rivillä näkyy asiakaskoneen nimi ja toimenpiteen selvitys eli Hardware, laitteiston tiedot. MP_Hinv.log tiedostoon tallentuu XML-tiedostomuodossa oleva tieto asiakaskoneen ohjelmistoista ja käytössä olevasta laitteistosta ja tieto kopioidaan Site-palvelimelle. MP_Hinv lokitieto oli hyödyllinen, kun SCCM:ään lisättiin Linux-koneita. SCCM:llä voi asentaa paketteja Linux-koneisiin, mutta niitä ei tämän työn puitteissa keretty testata. MP_Hinv.log oli ainut

kosketuspinta Linuxin ja SCCM:m välillä SCCM:n näkökulmasta. Linuxista on nähtävissä SCCM:n konsolin puolelta laitteistokokoonpano sekä asennetut ohjelmat. (Microsoft 2017c; Microsoft 2015a.)



Kuva 25. Ubuntu-koneen lähettämä tieto SCCM-koneelle MP_Hinv-lokitiedostosta. Lokitiedoston tieto filtteröity koneen nimellä ”ubuntu”.

5.4.3 Lokitiedon merkitys käyttöjärjestelmän asennuksessa

Työtä aloittaessa oli epäselvää, miten lokitiedot palvelevat käyttöjärjestelmän asentamisessa SCCM:n avulla. Kuitenkin pian kävi selväksi, että ilman lokitietoja käyttöjärjestelmän ja yleensäkin ohjelmistojen asentaminen olisi hankalampaa. Varsinkin ohjelmistojen asennusta testatessa lokitiedoista oli suuri apu, koska ei tarvinnut odotella jotain tapahtuvaksi, vaan lokitiedostosta pystyi näkemään heti, asentuiko ohjelma vai ei. SCCM:ssä on graafinen näkymä asennusten tilalle, mutta SCCM:n graafinen käyttöliittymä ei ole reaaliaikainen, kuten lokitiedot ovat. Muutaman kerran lokin perusteella paketti näytti asentuneen, mutta haluttuja tiedostoja ei näkynyt siellä, missä niiden piti olla. Selkisikin, että paketti toimi oikein, mutta sen komento oli vajavainen kohdekansion suhteen. Kohdekansion vajavuus johti siihen, että tiedostot kyllä kopioituivat kohdekoneeseen, mutta väärään kansioon. Selkisi, että Windows-ympäristössä etänä tapahtuvassa tiedostojen kopioinnissa kohde kansio kannattaa laittaa lainausmerkkien sisään, jotta kopiointikäsky toimii oikein kansioihin, joiden nimi koostuu useasta eri sanasta.

Toinen suuri hyöty lokitiedoista oli käyttöjärjestelmän asennuksessa ohjelmien kera. Testiasennusta tehdessä tuotantoympäristössä oli odottamatonta, että oh-

jelmistojen asetusten siirtäminen testiympäristöstä tuotantoympäristöön toisi mukanaan ongelmia. Jostain syystä osa ohjelmapaketeista ei asentunut tuotantoympäristössä ja niiden selvittäminen oli lokitiedoista helppoa ja nopeaa. Tosin on aikaa vievää testata asennusta, joka jää kesken kohdatessaan ongelmallisen paketin. SCCM:stä voi säätää asetuksen, että käyttöjärjestelmän asennus jatkuu, vaikka jokin paketeista ei onnistuisikaan. Jälkeenpäin voi käydä läpi testiasennuksen jälkeen, mitkä ohjelmat jäivät asentumatta. Virtuaalinen testiympäristö on asennuksia testatessa hyvä olla olemassa. Virtuaalinen ympäristö antaa paljon mahdollisuuksia asennuksia testatessa. Tosin virtuaalinen asennusympäristö voi tuoda mukanaan eri ongelmia kuin lopullinen fyysinen ympäristö. Esimerkiksi lopullisten kohdekoneiden kiintolevyt salattiin Bitlockerilla, mutta virtuaalikoneet eivät tukeneet levyn salausta. Salausta ei voinut testata kuin lopullisen ympäristön testiasennuksissa.

Lokitietojen jakaantuminen Site-palvelimelle ja asiakaskoneelle tuo mukanaan lokitietojen hajanaisuuden. Tätä työtä tehdessä tuli selväksi, että on tärkeää tarkkailla sekä asiakaskoneen että Site-palvelimen lokitietoja. Asiakaskoneen lokitiedot olivat tärkeitä asennuksen aikana ilmenneissä ongelmissa ja Site-pavelimen lokitiedot asennuspaketteja tehdessä. Ongelman selvittäminen asennuksen aikana ei ole SCCM toteutettu kovin käyttäjäystävällisesti. Asennuksen aikana ilmenneet ongelmat voi ratkaista kopioimalla lokitiedot asiakaskoneista Site-palvelimelle ja tutkimalla. Jos asennukseen on asetettu valinta, että asennus etenee vaikka ongelmia syntyisi, täytyy lokitietoja tutkia jälkikäteen. Tämän vuoksi onkin tärkeää tehdä vähintään yksi testiasennus kohdekoneeseen, ennen kuin asennuksia alkaa tehdä suurelle määrällä koneita. On myös huomioitavaa, että tämän työn kohdekoneiden määrä on suhteellisen pieni, mutta suuremmissa organisaatioissa asentaja ei näe asennusprosessinsa tulosta, vaan palaute voi tulla vasta loppukäyttäjiltä.

Tietoturvamielessä lokitietoja varten voisi tehdä jonkinlaisen automatisoinnin, joka tutkii esimerkiksi MAC-osoitteen perusteella koneita, jotka tekevät kyselyn SCCM-koneelle halusta asentaa käyttöjärjestelmä. SCCM:ssä voidaan kohdistaa käyttöjärjestelmän asennus PXE-käynnistyksen kautta joko tuntemattomiin (Unknown Computers) tai tunnettuihin koneisiin. Tunnetut koneet ovat joko ennestään AD-

ympäristössä tai ne voidaan syöttää käsin SCCM:ään MAC-osoitteen ja halutun nimen kera. Järkevintä on lisätä uudetkin koneet oikeilla AD-nimillä SCCM:ään, jotta niiden nimiä ei tarvitse enää AD:seen liittämisen jälkeen nimetä uudelleen. Koneen lisäämisellä etukäteen SCCM:ään vältytään myös siltä, että jokin ei haluttu laite alkaisi asentaa itseensä käyttöjärjestelmää. On myös tietoturvan kannalta parempi, ettei asennukset kohdistu kaikkiin SCCM:n näkökulmasta uusiin laitteisiin, vaan sellaisiin, joihin asennus halutaankin asentaa.

6 JOHTOPÄÄTÖKSET

Lokitieto on tärkeä osa organisaation tietoturvaa. Lokitieto pitäisi ottaa huomioon jo järjestelmän suunnitteluvaiheessa, koska lokitiedon oikeanlainen käsittely vie tietyn määrän organisaation tietojärjestelmän resursseista. Lokitietojen käsittelyssä on myös otettava huomioon lokitiedon sisältämä tieto, joka koskee käyttäjien yksityisyyttä. Lokitiedot pitäisi pitää erillään muusta tietojärjestelmän ylläpitotoimesta. Lokitietoa kerättäessä on myös huomioitava tietyt määräykset, mitä lokien tiedoille tehdään arkistoinnin yhteydessä.

Työ onnistui hyvin. Ennakkokäsitykset lokitietojen suhteen olivat vajavaiset ja lokien hyödyntäminen SCCM:n yhteydessä lisäsi tietoutta. Seminaarityön teoriaosan päälle oli hyvä lähteä rakentamaan käytännön osaa. Työn tavoite oli asentaa Windows 10 käyttöjärjestelmä täysin automatisoidusti ja tavoite saavutettiin. Työn päätavoite oli tutkia lokitietojen merkitystä käyttöjärjestelmän asennuksessa ja tämäkin tavoite saavutettiin. Etukäteen tiesin, että SCCM kerää paljon lokitietoa, mutta ennen työtä oli vaikea nähdä täysin SCCM:n lokitietojen suhdetta käyttöjärjestelmän asennuksessa. Pienoinen yllätys oli, ettei SCCM kerää verkon kautta asiakaskoneiden lokitietoja itsellään, vaan niitä tuli tutkia joko asiakaskoneella tai siirtämällä ne halutulle koneelle. On ymmärrettävää, että tuhansien koneiden organisaatiossa asiakaskoneiden lokien keskitetty hallinta veisi paljon tilaa. Asennustestaukseen SCCM:n lokitiedot ovat tärkeitä. Lopullisten kohdekoneiden suhteen lokitiedoista ei ole suurta hyötyä muuten, kuin ongelmatilanteissa. Kaiken pitäisi loppuasennusten suhteen olla jo testausvaiheen jälkeen kunnossa.

Mielestäni saavutin tutkimukselle vaaditun määrän lähteitä. Työssä keskeisenä lähteenä teoriaosassa toimi Valtionvarainministeriön VAHTI-ohje ”Lokiohje”, joka on suunnattu ministeriölle ja hallinnonalojen organisaatioille. Käytännön osassa on paljon Microsoftin tai Microsoftin nimen alla julkaistuja digitaalisia lähteitä. VAHTI-ohjeen tiedoille etsin tietopohjaa myös muista lähteistä, ja löysin sitä hyvin. Vastaavuudet muissa lähteissä kertovat VAHTI-ohjeen paikkansapitävyydestä. Mukana lähteissä on myös useita painettuja lähteitä, joten työn lähdeaineisto ei ole vain digitaalisten lähteiden varassa. Painettujen lähteiden tuoreus ei ole digi-

taalisten lähteiden tasolla, mutta lokitieto käsitteenä ei ole kovin uusi, joten lähteiden uutuudella ei ole niin suurta merkitystä. Lähteitä löytyi kohtuullisen hyvin tutkimalla aiemmin tehtyjen opinnäytetöiden lähdeluetteloja ja käyttämällä Kajaanin ammattikorkeakoulun kirjaston palveluja. Suoranaisesti lokeista ei ole paljoa tehty opinnäytetöitä, vaan ne ovat olleet pienissä rooleissa. Käytännön osaan oli helpompi löytää uusia lähteitä verkosta.

SCCM kehittyy ohjelmistona kaiken aikaa ja myös siihen liittyvä dokumentaatio. Kirjoituksen aikana SCCM:ään tuli useita päivityksiä, joista uusin 1702 versio kerkesi tulla tämän työn loppuvaiheessa. Työn aikana jotkin digitaaliset lähteet muuttuivat, vaikka niihin osoittava linkki ei. Lähteiden muutos kertoo jatkuvasta ohjelmiston kehittymisestä, mutta myös siitä positiivisesta seikasta, että dokumentaatio pidetään ajan tasalla. On vaikeaa tehdä täysin objektiivista katsausta omasta työstä, mutta olen tyytyväinen työn lähteisiin ja työn luotettavuuteen yleisesti.

Työtä tehdessä huomasi lokitietojen laajuuden niin teoriassa kuin käytännössä SCCM:n kautta. Teoriaosan ja käytännön osan välille olisi voinut saada enemmän peilausta, mutta teoriaosa toi näkökulmaa käytännön tekemiseen hyvänä pohjana. Moni loki jäi käytännön osassa tutkimatta johtuen työlle asettamista rajoitteista sekä tavoitteista. Esimerkiksi lokien säilytys voisi olla hyvä tutkimisen aihe. Työn aikana huomasin esimerkiksi 300 megatavun edestä lokitiedostoja pakkautuvan alle kymmenesosaan alkuperäisesti.

Tämä työ voi toimia pohjana jatkotutkimuksille, jossa keskitytään SCCM:n tuottamiin lokitietoihin jostain eri näkökulmasta tai lokeista eri ohjelmistokokonaisuuden yhteydessä. Keskitetyn järjestelmän kautta asennetun käyttöjärjestelmän ylläpitäminen lokien avulla voisi olla myös hyvä aihe jatkotutkimuksille. Tämä työ toimii jatkotutkimuksille hyvänä pohjana sekä ohjeena siihen, miten SCCM:n käytöstä saa tehokkaamman lokien avulla.

LÄHTEET

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tallinna: AS Pakett.

Allen, J. Cert. 2002. Verkkotietoturvan hallinta. Helsinki.

Allen, C. 2016. Configuration Manager – Wake on LAN, one stop shop. https://blogs.technet.microsoft.com/charlesa_us/2016/03/21/configuration-manager-wake-on-lan-one-stop-shop/. Luettu 19.1.2017.

Da Costa, A. 2015. How to: Create a bootable ISO file from your Windows 10 Download for reinstallation. https://answers.microsoft.com/en-us/windows/wiki/windows_10/how-to-create-a-bootable-iso-file-from-your/07590098-90a9-4c7e-b6fe-5ce1632daf4b. Luettu 5.1.2017.

Desai, P. 2016. How to Increase SCCM Site Server Log Files Size. https://prajwaldesai.com/how-to-increase-sccm-site-server-log-files-size/. Luettu 10.3.2017.

Finlex, 2014. Tietoyhteiskuntakaari. 7.11.2014/917. http://www.finlex.fi/fi/laki/ajantasa/2014/20140917. Luettu 6.11.2016.

Heikkinen, L. 2015. Tietokantojen perusteet. Tietojenkäsittelyn luento 16.3.2015. Kajaanin ammattikorkeakoulussa.

Hirsjärvi, S. & Remes, P. & Sajavaara, P. 2004. Tutki ja kirjoita.

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä.

Martinez, S. & Daalmans, S. & Bennett, B. 2014. Mastering System Center 2012 R2 Configuration Manager. Indianapolis, Indiana, Canada.

Microsoft. 2017a. Active Directory Domain Sevices. https://msdn.microsoft.com/en-us/library/aa362244(v=vs.85).aspx. Luettu 5.1.2017.

Microsoft. 2017b. Supported Configurations for Configuration Manager. https://technet.microsoft.com/en-us/library/gg682077.aspx. Luettu 9.1.2017.

Microsoft. 2017c. Log files in System Center Configuration Manager. https://docs.microsoft.com/en-us/sccm/core/plan-design/hierarchy/log-files. Luettu 7.2.2017.

Mirosoft. 2017d. Supported operating systems for clients and devices for System Center Configuration Manager. https://docs.microsoft.com/en-us/sccm/core/plan-design/configs/supported-operating-systems-for-clients-and-devices. Luettu 2.3.2017.

Microsoft. 2017e. Recommended hardware for System Center Configuration Manager. https://docs.microsoft.com/en-us/sccm/core/plan-design/configs/recommended-hardware. Luettu 8.3.2017.

Microsoft. 2017f. Supported SQL Server versions for System Center Configuration Manager. https://docs.microsoft.com/en-us/sccm/core/plan-design/configs/support-for-sql-server-versions. Luettu 8.3.2017.

Microsoft. 2017g. Integrate Configuration Manager with MDT. https://technet.microsoft.com/en-us/itpro/windows/deploy/integrate-configuration-manager-with-mdt. Luettu 9.4.2017.

Microsoft. 2017h. Microsoft Powershell. https://msdn.microsoft.com/en-us/powershell/mt173057.aspx. Luettu 23.4.2017.

Microsoft, 2016a. What’s new in System Center Configuration Manager incremental versions. https://docs.microsoft.com/en-us/sccm/core/plan-design/changes/whats-new-incremental-versions. Luettu 16.12.2016.

Microsoft. 2016b. Supported operating systems for System Center Configuration Manager site system servers https://docs.microsoft.com/en-us/sccm/core/plan-design/configs/supported-operating-systems-for-site-system-servers. Luettu 16.12.2016.

Microsoft. 2016c. Starting the 32-Bit Version of Windows PoerShell.https://msdn.microsoft.com/en-us/powershell/scripting/setup/starting-the-32-bit-version-of-windows-powershell. Luettu 9.1.2017.

Microsoft. 2016d. Configuration Manager and the Windows ADK for Windows 10, version 1607. https://blogs.technet.microsoft.com/enterprisemobility/2016/09/09/configuration-manager-and-the-windows-adk-for-windows-10-version-1607/. Luettu 10.1.2017.

Microsoft. 2016e. Prerequisites For Deploying Operating Systems in Configuration Manager. https://technet.microsoft.com/en-us/library/gg682187.aspx. Luettu 4.4.2016.

Microsoft. 2015a. Techinal Reference for Log Files in Configuration Manager. https://technet.microsoft.com/en-us/library/hh427342.aspx. Luettu 11.1.2017.

Microsoft. 2015b. Planning for Sites and Hierarchies in Configuration Manager. https://technet.microsoft.com/en-us/library/gg712681.aspx. Luettu 8.3.2017.

Microsoft. 2015c. How to copy SMSTS.log when a Task Sequence fails. https://social.technet.microsoft.com/wiki/contents/articles/30109.sccm-how-to-copy-smsts-log-when-a-task-sequence-fails.aspx. Luettu 3.4.2017.

Microsoft. 2014a. Zero-Touch, High-Volume Deployment for Education. https://technet.microsoft.com/en-us/library/dn645480(v=ws.11).aspx. Luettu 4.1.2017.

Microsoft. 2014b. Boot images and Distribution Point Configuration In SCCM 2012 R2. https://gallery.technet.microsoft.com/Boot-and-Distribution-a3241b51. Luettu 17.1.2017.

Microsoft. 2013a. Installing Prerequisites for Configuration Manager 2012 R2. https://gallery.technet.microsoft.com/Installing-Prerequisites-0867f36b. Luettu 10.1.2017.

Microsoft. 2013b. Installing SQL Server For Configuration Manager 2012 R2. https://gallery.technet.microsoft.com/Installing-SQL-Server-For-220ed264. Luettu 10.1.2017.

Microsoft. 2013c. Installing WSUS for Configuration Manager 2012 R2. https://gallery.technet.microsoft.com/Installing-WSUS-for-9b0039c2. Luettu 10.1.2017.

Microsoft. 2013d. Firewall Settings For Configuration Manager 2012 R2. https://gallery.technet.microsoft.com/Firewall-Settings-For-383b5ca6. Luettu 10.1.2017.

Microsoft. 2013e. Using the Microsot Deployment Toolkit. https://technet.microsoft.com/en-us/library/dn759415.aspx. Luettu 9.4.2017.

Microsoft. 2013f. What is DHCP?. https://technet.microsoft.com/en-us/library/cc781008(v=ws.10).aspx. Luettu 23.4.2017.

Microsoft. 2012. System Center: Configuration Manager – Extending the Schema in System Center 2012 Configutration Manager. https://blogs.technet.microsoft.com/configurationmgr/2012/10/30/extending-the-schema-in-system-center-2012-configuration-manager/. Luettu 10.1.2017.

Microsoft. 2011. Group Policy for Beginners. https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx. Luettu 23.3.2017.

Microsoft. 2010a. How to Create the System Management Container in Active Directory Domain Services. https://technet.microsoft.com/en-us/library/bb632591.aspx. Luettu 10.1.2017.

Microsoft. 2010b. About Task Sequences. https://technet.microsoft.com/en-us/library/bb693631.aspx. Luettu 5.4.2017.

Microsoft. 2008a. Understanding Organizational Units. https://technet.microsoft.com/en-us/library/cc771811(v=ws.11).aspx. Luettu 9.4.2017.

Microsoft. 2008b. Using PXE Boot Technologies to Install Windows over a Network. https://technet.microsoft.com/en-us/library/2008.07.desktopfiles.aspx. Luettu 23.4.2017.

Microsoft. 2007. Understanding Configuration Manager Clients. https://technet.microsoft.com/en-us/library/bb680749.aspx. Luettu 9.3.2017.

Männikkö, P. 2008a. Tietosuojalehti 4/2008. Tietosuoja: Loki jättää jäljen. https://www.tietosuoja-lehti.fi/index.php?mid=2&pid=32&aid=2587. Luettu 22.11.2016.

Männikkö, P. 2008b. Tietosuojalehti 4/2008. Tietosuoja: Mikä loki? https://www.tietosuoja-lehti.fi/index.php?mid=2&pid=32&aid=3176. Luettu 22.11.2016.

Opengroup. 2004. History and Timeline. http://www.unix.org/what_is_unix/history_timeline.html. Luettu 23.4.2017.

Puolustusministeriö, 2015. Katakri: Tietoturvallisuuden audiointityökalu viranomaisille. Helsinki.

Radwan, M. 2013. Installing System Center Configuration Manager 2012 SP1 on Windows Server 2012. http://mohamedradwan.com/2013/03/11/installing-system-center-configuration-manager-2012-sp1-on-windows-server-2012/

TSK. 2016. Tietotekniikan termitalkoot. http://www.tsk.fi/tsk/termitalkoot/. Luettu 4.1.2017.

VAHTI. 2010. Sisä-verkko-ohje. https://www.vahtiohje.fi/c/document_library/get_file?uuid=5084ce47-32bf-4025-bcc1-73fc2de4edad&groupId=10128. L

VAHTI. 2009a. Lokiohje. https://www.vahtiohje.fi/web/guest/3/2009-lokiohje. Luettu 26.9.2016.

VAHTI. 2009b. Lyhenteitä ja teknisiä termejä. https://www.vahtiohje.fi/web/guest/312. Luettu 5.4.2017.

Powershell-skripti SCCM-koneen vaatimista rooleista ja ominaisuuksista. Skriptissä #-merkillä kommentit asennettavista osista.

```
Get-Module servermanager

#IIS
Install-WindowsFeature Web-Server -IncludeManagementTools

#NET Framework 3.5 Features, lähde on Win-imagen polku \sources\sxs kansioon
Install-WindowsFeature NET-Framework-Features -IncludeAllSubFeature -Source D:\sources\sxs

#NET Framework 4.6 Features
Install-WindowsFeature NET-Framework-45-Features -IncludeAllSubFeature -Source D:\sources\sxs

#Background Intelligent Transfer Service
Install-WindowsFeature BITS -IncludeManagementTools

#Remote Differential Compression
Install-WindowsFeature RDC

#Basic authentication
Install-WindowsFeature Web-Basic-Auth

#IP and Domain Restrictions
Install-WindowsFeature Web-IP-Security

#URL Authorization
Install-WindowsFeature Web-Url-Auth

#Windows Authentication
Install-WindowsFeature Web-Windows-Auth

#ASP.NET 2.0, ASP.net 3.5 ja ASP.NET 4.6 (Server 2016ssa)
Install-WindowsFeature Web-ASP
Install-WindowsFeature Web-Asp-Net
Install-WindowsFeature Web-Asp-Net45

#Management tools ja IIS 6 MAnagement Compatibility
Install-WindowsFeature Web-Mgmt-Tools
Install-WindowsFeature Web-Mgmt-Compat

#IIS 6 Metabase Compatibility ja IIS 6 WMI Compatibility
Install-WindowsFeature Web-Metabase
Install-WindowsFeature Web-WMI
```

```
#IIS MangementScripts and Tools
Install-WindowsFeature Web-Scripting-Tools

#Management Service
Install-WindowsFeature Web-Mgmt-Service

#Custom IIS configuraatiota varten
Install-WindowsFeature Web-ISAPI-Ext

#Application Catalog web service pointia varten nama featuret
Install-WindowsFeature NET-HTTP-Activation
Install-WindowsFeature NET-Non-HTTP-Activ
```

Operating system deployment		
Log name	Description	Computer with log file
CAS.log	Records details when distribution points are found for referenced content.	Client
ccmsetup.log	Records ccmsetup tasks for client setup, client upgrade, and client removal. Can be used to troubleshoot client installation problems.	Client
CreateTSMedia.log	Records details for task sequence media creation.	Computer that runs the Configuration Manager console
DeployToVhd.log	Records details about the Virtual Hard Disk (VHD) creation and modification process.	Computer that runs the Configuration Manager console
Dism.log	Records driver installation actions or update application actions for offline servicing.	Site system server
Distmgr.log	Records details about the configuration of enabling a distribution point for Preboot Execution Environment (PXE).	Site system server
DriverCatalog.log	Records details about device drivers that have been imported into the driver catalog.	Site system server
mcsisapi.log	Records information for multicast package transfer and client request responses.	Site system server
mcsexec.log	Records health check, namespace, session creation, and certificate check actions.	Site system server
mcsmgr.log	Records changes to configuration, security mode, and availability.	Site system server
mcsprv.log	Records multicast provider interaction with Windows Deployment Services (WDS).	Site system server
MCSSetup.log	Records details about multicast server role installation.	Site system server
MCSMSI.log	Records details about multicast server role installation.	Site system server
Mcsperf.log	Records details about multicast performance counter updates.	Site system server
MP_ClientIDManager.log	Records management point responses to the client ID requests task sequences initiated from PXE or boot media.	Site system server
MP_DriverManager.log	Records management point responses to Auto Apply Driver task sequence action requests.	Site system server
OfflineServicingMgr.log	Records details of offline servicing schedules and update apply actions on operating system Windows Imaging Format (WIM) files.	Site system server
Setupact.log	Records details about Windows Sysprep and setup logs.	Client
Setupapi.log	Records details about Windows Sysprep and setup logs.	Client
Setuperr.log	Records details about Windows Sysprep and setup logs.	Client
smpisapi.log	Records details about the client state capture and restore actions, and threshold information.	Client
Smpmgr.log	Records details about the results of state migration point health checks and configuration changes.	Site system server
smpmsi.log	Records installation and configuration details about the state migration point.	Site system server
smpperf.log	Records the state migration point performance counter updates.	Site system server
smspxe.log	Records details about the responses to clients that use PXE boot, and details about the expansion of boot images and boot files.	Site system server
smssmpsetup.log	Records installation and configuration details about the state migration point.	Site system server
Smsts.log	Records task sequence activities.	Client
TSAgent.log	Records the outcome of task sequence dependencies before starting a task sequence.	Client
TaskSequenceProvider.log	Records details about task sequences when they are imported, exported, or edited.	Site system server
loadstate.log	Records details about the User State Migration Tool (USMT) and restoring user state data.	Client
scanstate.log	Records details about the User State Migration Tool (USMT) and capturing user state data.	Client