jamk

Sovellusten jakaminen Jyväskylän Nova-sairaalaan

Pauli Hokkanen

Opinnäytetyö, AMK
Huhtikuu 2021
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Hokkanen, Pauli

Sovellusten jakaminen Jyväskylän Nova-sairaalaan

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2021, 34 sivua.

Tekniikan ala. Tieto- ja viestintätekniikan koulutusohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Jyväskylään rakennettiin vuosina 2016–2020 uutta sairaalaa, joka nimettiin sairaala Novaksi. Uuteen sairaalaan siirrettiin vanhan sairaalan puolelta palvelimia. Novan tietokoneille tuli asentaa tarvittavia sovelluksia henkilökunnan käyttöön eri osastoille. Tavoitteena oli rakentaa hallittu ympäristö, jossa sovellusten jakaminen, päivitys, ja ylläpito olisivat järjestelmänvalvojien tehtävänä.

Opiskeltiin Microsoft Endpoint Configuration Managerin ja batch-skriptien käyttöä testikoneilla. Selvitettiin asennettavien sovellusten määrä, tietokoneiden määrä, johon ne asennettaisiin, ja vaadittavat metodit, joilla sovellukset saataisiin asennettua etänä. Paketoitiin sovelluksia niin, että ne asentuisivat koneille ilman asennusikkunoita tai muita häiritseviä tekijöitä. Kartoitettiin eri koneiden sovellustarpeita ja luotiin jakeluryhmiä sovelluksille. Tehtiin jakelut ryhmille, ja tarkkailtiin niiden tilannetta Endpoint Configuration Managerin monitorointityökalujen kautta. Vikatilanteissa selvitettiin, mikä jakelussa meni vialle ja korjattiin ongelma, joko asennusskriptistä, tai sovelluksen tunnistustavassa.

Sovellusten jakelut saatiin tehtyä onnistuneesti käyttäjille. Valmiiksi tehdyt jakeluryhmät jätettiin tulevia päivityksiä ja muutoksia varten järjestelmään. Järjestelmä saattaa tulevaisuudessa olla muutosten kohteena, jos lisäksi otetaan käyttöön esimerkiksi Microsoft Intune.

Valmis kaikki verkon tietokoneet kattava järjestelmä toteutettuna Microsoft Endpoint Configuration Managerilla oli erittäin toimiva keinoa hallita sovellusten asennuksia ja päivityksiä isossa sairaalaympäristössä. Luodut ryhmät, paketoinnit, ja monitorointitekniikat nopeuttivat sovellusasennustyötä, joka muuten olisi ollut pitkä ja hidas prosessi. Yksittäisten koneiden käsin asennus olisi hidastanut sairaala Novan käyttöönottoa merkittävästi.

Avainsanat (asiasanat)

Active Directory, Microsoft Endpoint Configuration Manager, MECM, MEMCM, tietoverkko, tietoliikenne, valvonta, ylläpito, sovellusohjelmat, paketoiminen,

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Hokkanen, Pauli

Deployment of applications in Jyväskylä's Nova-hospital

Jyväskylä: JAMK University of Applied Sciences, May 2020, 34 pages.

Engineering and technology. Degree Programme in Information and Communications Technology. Bachelor's thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

A new hospital was under construction in Jyväskylä in 2016-2020. Servers were being transferred from the old hospital to the new hospital. Needed programs had to be installed for the staff on the computers in the Nova-hospital. The objective was to build a controlled environment, where deployment, upgrading, and maintenance of applications would be the task assigned to administrators.

Usage of Microsoft Endpoint Configuration Manager and batch-scripts were learnt on test-machines. Information was gathered about the number of applications to be installed, amount of computers and where they would be installed, and the required methods to install applications remotely. Applications were packaged so that their installation windows and other disruptive features weren't present. Different application needs were mapped, and deployment groups were created. Applications were deployed to groups and the process was observed through Endpoint Configuration Manager's monitoring tools. In error situations the problem was resolved through modifying the install script or the application's detection method.

The deployment of applications for users was successful. Created deployment groups were left in the system for future updates and changes. The system might be as a target for change in the future, if Microsoft Intune is brought into use.

A complete all computers including system implemented by Microsoft Endpoint Configuration Manager was a very effective way to manage the installations of applications and updates in a big hospital environment. Created groups, packages, and monitoring techniques sped up work required for installation of applications, which would have otherwise been a long and slow process. Individually installing every machine would have slowed the deployment of the Nova-hospital substantially.

Keywords/tags (subjects)

Active Directory, Microsoft Endpoint Configuration Manager, MECM, MEMCM, network, computer network, communication, maintenance, applications, packing

Miscellaneous (Confidential information)

Lyhenne- ja termiluettelo

AD	Active Directory
ADDS	Active Directory Domain Services
CAS	Central Administration Site
DC	Domain Controller
DS	Domain Services
DP	Distribution Point
GPO	Group Policy
KSSHP	Keski-Suomen sairaanhoitopiiri
LDAP	Lightweight Directory Access Protocol
LOB	Line-of-business
MDM	Mobile Device Management
MECM	Microsoft Endpoint Configuration Manager
SCCM	System Center Configuration Manager
SSH	Secure Shell
SSRS	SQL Server Reporting Services
SQL	Structured Query Language
WMI	Windows Management Instrumentation
WQL	WMI Query Language

Sisältö

Kuviot

Taulukot

1 Työn lähtökohdat

1.1 Taustaa

Kaikki maailman tietokoneet ovat jonkun henkilön hallinnassa. Tällä henkilöllä on oikeus asentaa ja muokata sovelluksia ja käyttää laitetta omiin tarkoituksiinsa. Suurimmalla osalla maailman ihmisistä on jokin elektroninen laite jonka henkilökohtaiset tiedot halutaan pitää turvassa. Tällaisten laitteiden suojaus onnistuu kohtuullisen helposti, koska yhdellä ihmisellä on yleensä hyvin rajallinen määrä laitteita. Yritysmaailmassa tilanne on paljon laajempi ja monimutkaisempi. Laitteiden hallintaa ei voida tietoturva-, tuotteliaisuus- ja toimintasyistä jättää käyttäjän vastuulle. On myös mahdotonta olettaa jokaisen yrityksen työntekijän ymmärtävän täysin tietoturvallisuutta. Tämän takia laitteiden hallinta jätetään niiden vastuulle, jotka ymmärtävät tietoturvallisen laitteen ylläpitämisestä. Koska laitteiden määrä yrityksissä on niiden haltijoita suurempi, tarvitaan keino valvoa ja hallita tätä massaa tehokkaasti. Näihin ongelmiin yritysmaailmassa on rakennettu useita erilaisia keskitetyn hallinnan ohjelmistoja.

Keskitetyn hallinnan järjestelmät on luotu helpottamaan heidän töitä, joiden vastuulla on pitää yrityksen tietoturva kunnossa. Nimi keskitetty hallinta tulee siitä, että verkon toiminnan hallinta on keskitetty yhden henkilön tai ryhmän alle, joka vastaa kaikkien verkon käyttäjien oikeuksista toimia määritetyillä alueilla. Oikeanlainen järjestelmä auttaa järjestelmänvalvojaa luomaan tarkkoja sääntöjä, joilla estää yritykselle haitallinen toiminta verkossa. Näihin sisältyy mm. kielletyillä sivustoille vieraileminen, pääsy salattuihin tietoihin, ja yrityksen tietoturvan heikentäminen. Toinen ominaisuus hyvässä hallintaratkaisussa on sen tuoma tehokkuus, joka vähentää ylläpitämiseen tarvittavaa aikaa. Eri prosessien automatisointi säästää järjestelmänvalvojan aikaa keskittyä muihin tärkeisiin töihin. Ylivoimaisesti kaikista käytetyimmät ovat Microsoftin kehittämät active directory ja system center configuration manager (SCCM), nykyiseltä muodoltaan Microsoft endpoint configuration manager (MECM). Molemmat keskittyvät pääosin tietoturvapuoleen käyttäjä- ja laitehallinnan kautta, mutta endpoint configuration managerin tehokkuus tulee esille, kun isolle määrälle laitteita pitää jakaa sovelluksia. Muitakin vastaavia sovelluksia hyvine puolineen on markkinoilla, mutta ne on tarkoitettu hieman erilaisiin ympäristöihin ja käyttötarkoituksiin.

Vuonna 2021 suurin osa maailman tietokoneista käytti järjestelmänä Microsoft Windowsia. Moni on jo siirtynyt uusimman Windows 10:n käyttöön, mutta valtava osa ihmisistä käyttää vielä Windows 7:ää, ja jopa Windows XP:tä käyttöjärjestelmänä. Microsoftin osuus käyttöjärjestelmien markkinaosuudesta on eri lähteistä riippuen 75-90%, joka vastaa suurinta osaa käytössä olevista tietokoneista. Kaikille nykyisille versioille yhteistä on, että ne käyttävät Active Directoryä (AD) ja niitä voidaan hallita työympäristössä sen kautta. (The world's second-most popular desktop operating system isn't macOC anymore 2021)

1.2 Toimeksiantaja

Vuonna 2016 Jyväskylään aloitettiin uuden sairaalan rakentaminen, joka nimettiin sairaala Novaksi. Uutta sairaalaa päädyttiin rakentamaan, koska se tuli halvemmaksi, kuin vanhan sairaalan jatkuva korjaaminen. Samalla voitiin rakentaa sellaiset tilat, joissa voitiin tarjota laajat erikoissairaanhoidon palvelut Keski-Suomen 22:lle kunnalle. Osana tätä muutosta päätettiin siirtää vanhan sairaalan tietojärjestelmät uuden sairaalan tiloihin. (Arola, 2010, Jyväskylään mahdollisesti uusi keskussairaala; Laiho & Penttilä & Salomaa, 2020, Sairaala Nova)

Kaikki sairaala Novan tietokoneet ovat Windows-pohjaisia ja niitä varten tarvittiin toimiva hallintaratkaisu. Tässä päädyttiin Microsoft Endpoint Configuration Manageriin. Järjestelmä on yksi maailman suosituimpiin kuuluvista, johtuen sen erinomaisesta toimivuudesta Windows-käyttöjärjestelmien kanssa ja osittain, koska markkinat nojaavat yritysmaailmassa Microsoftin tuotteisiin päin. Sovellus on erittäin skaalautuva ja sen opettelussa on paljon jyrkempi oppimiskäyrä, kuin muilla vastaavilla sovelluksilla, mutta moni yritys on kokenut, että se on tarpeeksi tehokas ja varma omaan käyttöön. Sen yksi haittapuoli on, että se toimii vain Windows-laitteilla. Tämä ei kuitenkaan ollut haittana Novan projektissa. Toinen sovellus, jota harkittiin oli Microsoft Intune, joka on pilvipohjainen hallintaratkaisu pääosin mobiililaitteille. Tämä jätettiin kuitenkin tulevaisuuden mahdollisiin lisäyksiin.

Keskitetty sovellusten hallinta on avainasemassa, kun Keski-Suomen keskussairaalan palvelimet siirretään uuden Nova-sairaalan puolelle ja sovelluksia asennetaan uusille

koneille. Jokaista sovellusta ei voitu asentaa käsin rajallisen ajan ja henkilökunnalle aiheutuvien keskeytysten vuoksi. Hyvin valmisteltu ohjelmistokirjasto auttaa myös tulevaisuudessa ohjelmistojen asennuksen ja poiston yhteydessä, kuten myös tarvittavien ohjelmistojen valvonnassa.

Sovellusten paketoinnit ja asennukset hoiti Istekki Oy, joka on vuonna 2009 perustettu julkisomisteinen osakeyhtiö tietoteknologian alalla. Yritys on keskittynyt julkishallinnon ja terveydenhuollon teknologiaratkaisuihin, minkä takia se oli erinomainen tekijä Nova-sairaalan projektissa. Paketoinnit tehtiin käyttäen Istekin ja Keski-Suomen keskussairaalan verkkoja, tietokoneita, ja järjestelmiä.

2 Vaatimukset ja tavoitteet käyttöönotettavalle järjestelmälle

Tässä opinnäytetyössä keskityttiin tarkastelemaan Microsoft endpoint configuration managerin tehokkuutta sairaalaympäristössä. Ratkaistavina ongelmina olivat kuinka suuren ohjelmistomäärän tehokas keskitetty asennus, valvonta ja hallinta voidaan toteuttaa turvallisella tavalla ilman että siitä on haittaa henkilökunnan päivittäisessä työssä. Resursseina tähän oli käytössä Istekin Nova-projektiin varatut henkilöt ja KSSHP:n tietohallinnon henkilöstö. Selvitimme järjestelmien tilan vanhan sairaalan puolelta ja mietimme sekä varsinaiseen siirtotyöhön liittyvät mahdolliset ongelmatilanteet että parannuskeinoja tulevan järjestelmän vakaana pysymiseen. Vaatimuksena oli, että kaikki toimisi vielä vuosien päästä ilman suurta muutosta hallintaratkaisussa. Sairaalan käyttöönoton jälkeen Istekki hoiti vielä viimeisten järjestelmien siirtoa uuteen konesaliin Novan tiloihin. Sairaalan henkilökunnan järjestelmiin liittyvissä ongelmatilanteissa oltiin yhteydessä Istekin asiakaspalveluun, jossa asiasta luotiin vikatiketti. Järjestelmäasiantuntijat ottivat vianselvitykseen liittyvät asiat hoidettavakseen, jotta vikaantuneet järjestelmät saatiin palautettua toimintakuntoon.
Sovellusten jakelut tuli osoittaa ryhmille ja koneille, eikä käyttäjille. Tällä pyrittiin välttämään sovellusten asennusta useampaan kertaan samalle koneelle eri käyttäjätilin alle ja ylläpitämään hyvää tietoturvaa. Osastotyöntekijät käyttivät pääosin yhteisiä koneita, joilla oli heidän tarvitsemat ohjelmat. Laiteryhmille sovellusten asentaminen täytti vaadittavat tietoturvakriteerit.

Asennuksia varten olevat skriptit tulivat olla selkeästi kommentoituja, jotta niiden tulkitseminen olisi selkeää. Jos tiedostoa piti muokata myöhemmin, kommentoitu skripti auttoi ymmärtämään mitä osaa piti muuttaa. Erityisen tärkeää oli muuttaa vanhasta sairaalasta siirtyvien ohjelmien tietokannan IP-osoite skriptiin, jotta yhteys luotaisiin uuden konesalin palvelinkantaan.

Jokaisen sovellusjakelun metatiedot tuli olla selkeästi täytetyt, jotta järjestelmänvalvojat ja sairaalan työntekijät ymmärtäisivät asennettavan paketin sisällön ja löytäisivät lisäapua tarvittaessa. Tarkat tiedot olivat tärkeitä varsinkin vapaaehtoisesti ladattavissa sovelluksissa. Ohjelmakirjaston sovellusikkunassa tuli myös olla linkki käyttöohjeisiin, josta kävisi ilmi kaikki sovelluksen vaatimat yhteydet, tietokannat, ja käyttöoikeudet. Sovelluksille joiden käyttö vaati pääsyä erilliselle verkkolevylle, luotiin oma käyttäjäryhmä. Näiden ryhmien tavoitteena olisi jakaa oikeus salassa pidettäviin tietoihin vain niitä tarvitseville henkilöille. Pääsyoikeudet jaettiin Group Policyllä (GPO).
Kaikki asennettavat sovellukset tuli järjestää selkeään hierarkiaan Endpoint Configuration Managerin sovelluskirjastoon helppoa hallintaa ja mahdollisia tulevaisuuden muutoksia varten.

Sairaalaympäristöön luotiin useampi jakelupiste verkon suunnitelman mukaan. Sovellukset ja päivitykset jaettiin alueittain sairaalassa, jottei verkossa päässyt syntymään ruuhkaa vilkkaampina aikoina.

3 Hallintaratkaisujen vertailu

Windows-pohjaisille laitteille on olemassa useita eri hallintasovelluksia, joista muutamana esimerkkinä ovat Microsoft Endpoint Configuration Manager, Microsoft Intune, ja Ansible. MECM on näistä ehkäpä kaikista helpointa käyttää pienen opiskelun jälkeen. Intune keskittyy enemmän mobiilipuolen hallintaan ja Ansible sijoittuu johonkin näiden välimaastoon. On kuitenkin hyvä huomioida, että vaikka Intunessa laitteiden hallinnasta vastaa Mobile Device Management (MDM), sillä voi kuitenkin hallita myös tietokoneita. MECM on myös kaikista selkein käyttää sen graafisen käyttöjärjestelmän kautta. Intune on lähellä sen helppoutta, mutta nykyversio tuntuu vielä hyvin suppealta ja vaikeaselkoiselta. Valikoiman suppeus tulee esiin muun muassa verrattaessa

Group Policyn ja Mobile Device Managementin eroja. Windows 10:n hallintavaihtoehtoja on noin 3300 vähemmän Intunessa. Joidenkin asetusten muuttaminen Intunen avulla on myös vaikeampaa, koska säännöistä ei ole valmiita malleja ja ne tulee luoda itse. Myös monet asetukset käyttävät mielummin GPO:ta, jos sekä Intunen että Group Policy ovat käytössä. Tässä tapauksessa menetettyjen hallintavaihtoehtojen määrä kasvaa noin 10 000:n. (Policies in Policy CSP supported by Group Policy 2019, Policy CSP – ControlPolicyConflict 2021, ADMX-backed policies in Policy CSP 2020, Understanding ADMX-backed policies 2020)

Ansiblessa sen sijaan kaikki säännöt ajetaan osana *playbookkia*, joka on sääntökirja asetuksista ja oikeuksista. Näitä voidaan laatia useampia eri käyttötarkoituksille ja ryhmille. Playbookin hyvä puoli on, että siihen voidaan sisällyttää myös vastaavia Group Policyn sääntöjä. (Intro to Playbooks 2020, Best Practices 2020)

Ansible vaatii komentorivin käyttöä ja ohjelmointitaitoa, toisin kuin MECM ja Intune. Kehitteillä on kuitenkin Ansible AWX, joka on visuaalinen käyttöliittymä nettiselaimeen. Ansible on kuitenkin monipuolisempi joissain sen ominaisuuksissa, esimerkiksi sen kuljetustason protokollissa ja salauksissa. MECM:ssä on myös komentoja, joita voidaan ajaa vain Powershellillä, mutta suurin osa käytettävistä toiminnoista on graafisen käyttöliittymän takana. Ansible on agentiton ohjelma, joka ottaa yhteyden SSH:lla ja ajaa tarvittavat komennot laitteille. Jos laite tukee SSH-yhteyttä ja ymmärtää Pythonia, se erittäin todennäköisesti tukee myös Ansiblea (ks. Taulukko 1.) Sekä MECM että Ansible tukevat autentikointitekniikkana Kerberosta, mutta niiden lisäksi Ansiblella on käytössä mm. NTLM, CredSSP, basic authentication, ja sertifikaattiautentikointi. Yksi Ansiblen aikaa säästävistä ominaisuuksista on kyky ajaa skriptin täysin automatisoidusti päätelaitteille. Jos tietokone vaatii uudelleenkäynnistyksen ohjelmiston asennuksen päätteeksi, Ansible osaa jatkaa skriptiä automaattisesti sen jälkeen. (winrm - Run tasks over Microsoft’s WinRM 2020)

Sovellusten jakamisessa Intune jää MECM:n ja Ansiblen jalkoihin, koska sillä voi jakaa vain hyväksyttyjä sovelluksia Microsoftin, Google Playn ja Androidin kaupasta. Se ei siis salli omien sovellusten jakamista, muuta kuin siinä tapauksessa, että ne on luotu yrityksen sisällä. Näitä kutsutaan line-of-business (LOB) sovelluksiksi.

Koska yritysmaailma on pääosin tottunut Microsoftin graafisiin käyttöjärjestelmiin, on Microsoft Endpoint Configuration Manager saanut suuren jalansijan muiden hallintasovellusten joukosta. Tuotteen jatkuva kehitys tekee siitä myös monipuolisemman ja toimivamman ratkaisun kaikenkokoisten ympäristön hallintaan. Jatkuva kehitys näkyy myös MECM:n tuetuissa Windows 10 versioissa. Tietoturva-aukkoja löytyy tasaisin väliajoin ja ne pyritään korjaamaan aikataululla, joka määräytyy riskin tasosta. Vanhin Windows 10 versio, jota tuetaan on vuoden 2018 huhtikuussa julkaistu versio ja sitä voidaan käyttää Configuration Managerin versiolla 1910 eteenpäin. Uudemmat versiot vaativat myös uudemman Configuration Managerin, ja päivittäminen vaatii lisätyötä järjestelmänvalvojilta (ks. Liite 3.) Uudemmat versiot myös poistavat tuen joiltain käyttöjärjestelmiltä (ks. Liite 4.) (Supported OS versions for clients and devices for Configuration Manager 2021, Supported operating systems and browsers in Intune 2021) Microsoft Intune on vielä hieman alkuvaiheessa käyttömukavuudessaan ja laajuudessaan. Sen toiminta mobiililaitteille pilvipalvelussa toteutettuna on erittäin toimiva ratkaisu nykymaailmassa, jossa langattomat yhteydet ovat saavuttaneet riittävät nopeudet suuren laitekannan ylläpitämiseksi. Järjestelmä toimii yhdessä Azure AD:n kanssa, jotka sijaitsevat Microsoft Azure-pilvessä. Esimerkiksi Office 365:n toteutus pilven kautta on erittäin toimiva ratkaisu asennusten ja autentikoinnin kannalta (Kts. Liite 5.) Sen suppeat asetukset ryhmäkäytäntöjen hienosäätöön jättävät sen kuitenkin selvästi sekä MECM:n että Ansiblen taakse. (Microsoft Intune is an MDM and MAM provider for your devices 2020, Support for Windows 10 in Configuration Manager 2021, What is Microsoft Intune app management? 2021)

Taulukko 1 Hallintasovellusten vertailu

	MECM	**Intune**	**Ansible**
Hinta	$1323-$3607	$8/käyttäjä/kk	Ilmainen
Käyttöjärjestelmä	Graafinen	Graafinen	CLI

Markkinaosuus	75-90%	5-10%	-
Linux-tuki	Tuki poistettu versiossa 1902	-	RHEL7 ja 8, CentOS, Fedora, Ubuntu, Debian, Gentoo FreeBSD, Solaris, Arch Linux, Slackware Linux, Clear Linux
Microsoft	Windows 10, Windows 8.1 (x86, x64): Professional & Enterprise, Windows 10 IoT Enterprise (x86, x64), Windows 10 IoT Mobile Enterprise, Windows 10 Team for Surface Hub, Windows 10 Mobile, Windows 10 Mobile Enterprise	Surface Hub, Windows 10 (Home, S, Pro, Education, ja Enterprise), Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise (x86, x64), Windows Holographic for Business, Windows 10 Teams (Surface Hub), Windows 10 1709 (RS3)+, Windows 8.1 RT, Windows 8.1 (Sustaining mode)	Windows 7, 8.1, ja 10
Apple-tuki	macOS 10.13-10.15	Apple iOS 12.0+, Apple iPadOS 13.0+, Mac OS X 10.13+	macOS 10.12+

Taulukko jatkuu seuraavalla sivulla.

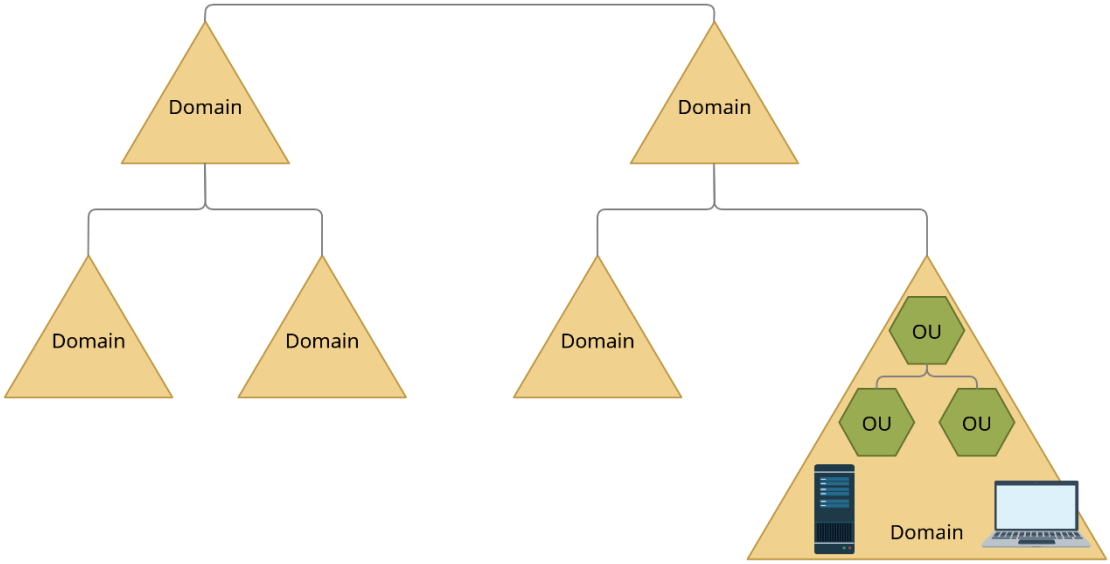
Taulukko jatkuu.

Google-tuki	-	Android 5.0+ w/ Samsung KNOX Standard 2.4+	On
UNIX-tuki	Tuki poistettu versiossa 1902	-	On

4 Active Directory

Active Directory on Microsoftin vuonna 1999 luoma keskitetyn hallinnan järjestelmä, joka sisältyy Windows Server-käyttöjärjestelmään. AD koostuu vähintään yhdestä pääpalvelimesta, Domain Controllerista (DC) ja sen alla olevista päätelaitteista. Suurissa verkoissa se voi koostua useista verkossa olevista DC:ista, jotka keräävät tiedon kaikista päätelaitteista ja käyttäjistä, joita määritellyssä verkossa on olemassa. Kaikki tieto kerätään yhteen hierarkkiseen tietokantaan, josta se voidaan jakaa muille verkon käyttäjille ja tietokoneille. AD-verkko koostuu metsästä (*forest*), joka sisältää toimialueita (*domain*), jotka voivat sisältää pienempiä hallinnollisia yksiköitä (*organizational unit*). Kaikki samassa metsässä sijaitsevat laitteet ovat samassa nimiavaruudessa (ks. Kuvio 1.) (What Are Domains and Forests? 2014)

AD käyttää avointa Microsoftin kehittämää Lightweight Directory Access Protocolia (LDAP), joka mahdollistaa hakemistotietoihin pääsyn ja hallinnan IP-verkoissa. Keskeinen osa Active Directorya on sen Domain Services -osio (ADDS), josta hallitaan käyttäjiä ja laitteita keskitetysti. ADDS:ssä määritetään tietokoneiden ja käyttäjien asetukset koko domainin alueelle. Tietokoneet keskustelevat toistensa kanssa käyttäen DNS-nimipalvelimia, jonka avulla ne löytävät DC:t. Myös kirjautumiset suoritetaan verkon avulla, sillä todennusprotokollana käytetään Kerberosta. (Active Directory Domain Services Overview 2017)



Kuvio 1 Esimerkki Active Directoryn rakenteesta

Group policy eli ryhmäkäytäntö on ADDS:n osa, jolla määritetään sääntöjä ja konfiguraatioita käyttäjille ja tietokoneille. Käyttäjä voi kirjautua mille tahansa koneelle toimialueessa ja saa aina samat asetukset. Asetusten sidonnaisuus käyttäjiin luo sekä tietoturvallisen ympäristön, että mahdollistaa käyttäjien työskentelyn useammalla koneella. (Group Police overview 2016) Jos kaksi tai useampi sääntö on ristiriidassa keskenään, oikea sääntö päätetään arvolla nimeltä *precedence*, joka tarkoittaa ristiriitaisten sääntöjen prioriteettijärjestystä. Korkeamman prioriteetin säännöt valitaan ensin ristiriidan tullessa vastaan. Jos laitteelle tai käyttäjälle tulee useampi samaa asetusta koskeva sääntö, oikea sääntö valitaan seuraavien sääntöjen perusteella: 1. Vaadittavat asetukset ovat tärkeämpiä, kuin profiiliasetukset, 2. Jos kaksi samaa vaadittavaa asetusta ovat ristiriidassa, niin rajoittavampi sääntö on tärkeämpi, ja 3. Jos asetuskäytännöt ovat ristiriidassa toisen asetuskäytännön kanssa, ongelma tuodaan esille Intunessa ja ongelma tulee ratkaista käsin. (Common questions and answers with device policies and profiles in Microsoft Intune 2021)

Novassa Group Policyä (GPO) eli ryhmäkäytäntöä käytetään pääsyoikeuksien rajoittamiseen, verkkotulostinten yhdistämiseen tileihin sekä verkkolevyjen jakamisessa niitä tarvitseville henkilöille. GPO:n käyttäminen vaati hallinnollisia yksiköitä ja ne jaettiin pääosin osastoittain. Monet ohjelmat käyttivät salassapidettäviä potilastietoja, eikä

niitä voitu säilyttää paikallisella levyllä kaikkien saatavilla. Näissä tapauksissa ryhmäkäytännöllä jaettiin verkkolevyjen oikeudet niille, jotka niitä tarvitsivat ja kaikki muut suljetaan tietojen ulkopuolelle.

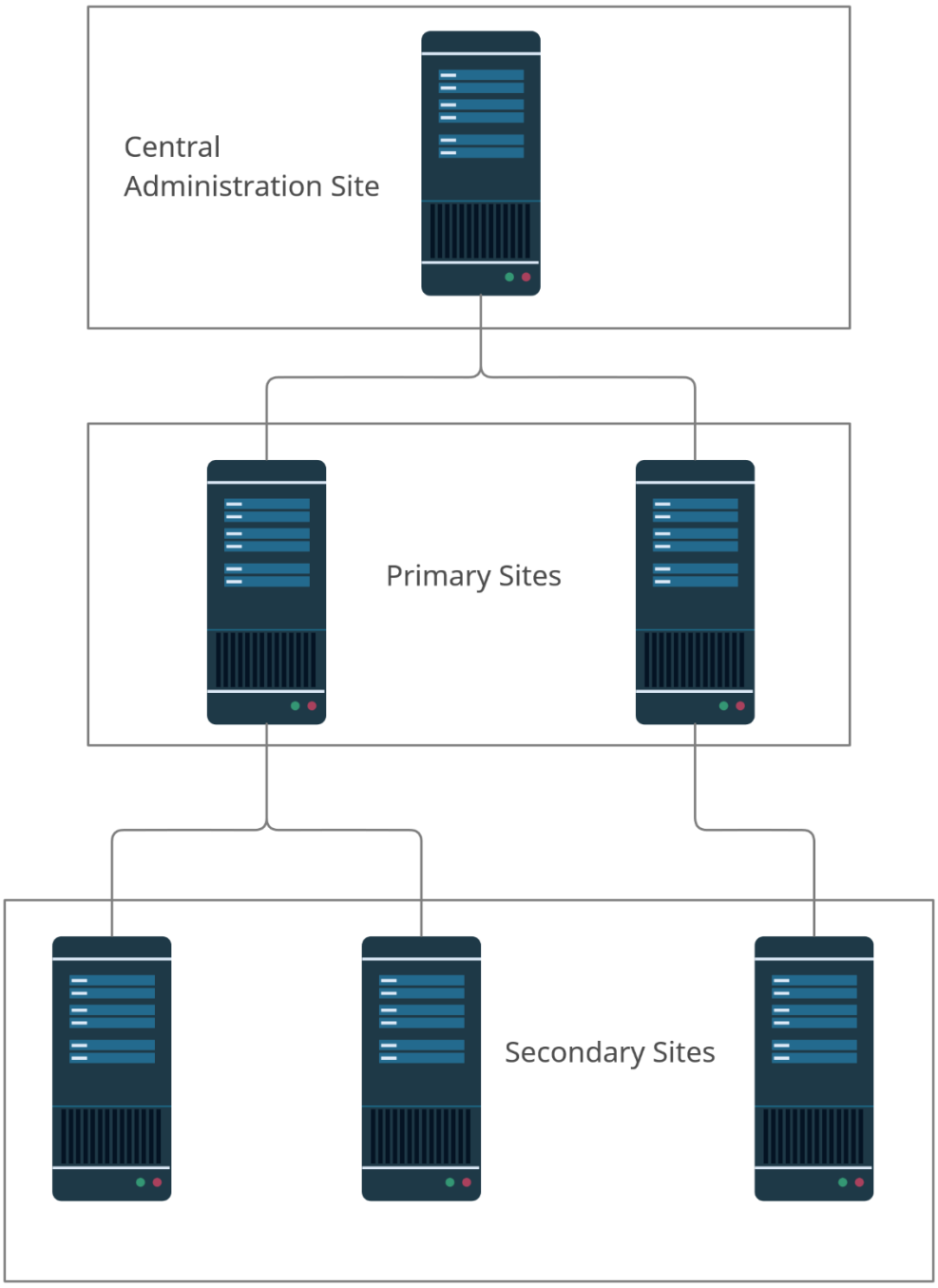
5 Microsoft Endpoint Configuration Manager

5.1 Toimintamalli

Endpoint configuration managerin pääasiallinen tarkoitus on hallita, mitä sovelluksia päätelaitteille asennetaan. Tämä toteutetaan poistamalla käyttäjien oikeudet asennuksiin ja keskittämällä sovellusten jakaminen MECM:n alle, jota vain pieni ryhmä ihmisiä hallitsee. Kaikista Novaan tulevista sovelluksista tehtiin lista, määriteltiin mille koneille ne kuuluvat ja sovellusten asennukset toteutettiin massajakeluina. (Microsoft Endpoint Manager overview 2020)

5.2 Palvelimet ja roolit

Microsoft Endpoint Configuration Manager saa tietonsa Active Directory Domain Servicesiltä, joka noudattaa hierarkiarakennetta. Perinteisessä mallissa tämä tarkoittaa, että kaikki tieto verkon objekteista ja säännöistä kerätään yhdelle pääpalvelimelle (*Central Administration Site*; CAS), josta se jaetaan alaspäin seuraavaksi tärkeimmille laitteille. Tässä tapauksessa seuraavana olisi domainin Distribution Point (DP) eli jakelupiste, joka jakaa tarvittavat tiedot päätelaitteille. Kaikki asennettavien sovellusten tarvitsemat tiedot lähetetään jakelupisteelle, josta ne ladataan päätelaitteille, kun asennus käynnistyy. Hierarkiarakenne on tärkeä verkon yhtenäisyyden ja toiminnan kannalta. Suurissa yli 100000 laitteen verkoissa täytyy olla yksi päätietokanta, joka kerää ja jakaa muutokset eteenpäin ensisijaisille hallinta-alueille, jotka tekevät varsinaiset muutokset alemman tason verkon laitteille. Kaikki tämä tieto verkon käyttäjistä ja laitteista on oleellinen pohja Endpoint configuration managerin toiminnan kannalta (ks. Kuvio 2.) (Install and configure distribution points in Configuration Manager 2021)



Kuvio 2 Hierarkiarakenne

Nykyisin Microsoft suosittelee jättämään CAS:n pois, mikäli verkossa on alle 100000 laitetta, koska se ei juuri tuo hyötyä pienille verkoille. Tietokantojen replikointi useiden eri palvelimien välillä tuo ylimääräistä työtä ja hankaloittaa hallintaa, jos niille ei ole pakottavaa tarvetta. Yksi ensisijainen hallinta-alue pystyy palvelemaan 250:tä toissijaista aluetta, mutta Novan tapauksessa oli suositeltavaa käyttää niiden sijaan jakelupisteitä.

(Fundamentals of sites and hierarchies for Configuration Manager 2016, Size and scale numbers for Configuration Manager 2021))
Novan verkko sisältää yhden toimialueen, jonka sisällä kaikki verkon laitteet toimivat. Koska Novassa ei ole hallinnan alla kuin muutama tuhat konetta, jakelupisteiden 4000:n koneen rajoitus oli riittävä. Paremman kaistankäytön vuoksi jakelupisteitä luotiin 4 ja ne rajattiin eri osiin rakennusta, jotta kaistankäyttö sovellusten lataamisen aikana pysyisi kohtuullisissa mitoissa kovankin rasituksen aikana. Lisäksi yksi jakelupiste luotiin Istekin testikoneita varten.

5.3 Kokoelmat

Laitteista voidaan luoda kokoelmia eri tarkoituksiin. Ne helpottavat sovellusten jakamista merkittävästi, koska sovelluksen asennuspyyntö voidaan lähettää yhdelle ryhmälle, josta se jakautuu kaikille ryhmässä oleville laitteille. Kokoelmia voidaan luoda myös päätelaitteiden kuntoa tarkastellen. Tällä tavalla voidaan tarkkailla laitteiden kuntoa ja ennaltaehkäisevästi vaihtaa vanhat tai rikkinäiset laitteet, ennen kuin ne aiheuttavat haittaa työskentelylle.

Endpoint Configuration Manageriin on sisäänrakennettu seitsemän oletusryhmää: Kaikki käyttäjäryhmät, kaikki käyttäjät, kaikki käyttäjät ja käyttäjäryhmät, kaikki tietokoneet ja palvelimet, kaikki mobiililaitteet, kaikki järjestelmät ja kaikki tuntemattomat tietokoneet. Näitä oletusryhmiä käytettiin luomaan tarkemmin rajattuja ryhmiä Novan infrastruktuurista eri osastoille ja sovellustarpeille. Pienemmät ryhmät helpottavat havainnollistamaan, miten laitekanta jakautuu ja helpottamaan sen hallinnassa. Ryhmiä käytettiin paljon mm. sovellusten jakamisessa päätelaitteille. Pienempien ryhmien luonti oli myös välttämätöntä nopeuttamaan sovelluskyselyiden käyttöä, koska niiden ajaminen isolle määrälle laitteita on hidasta ja erittäin raskasta verkolle. (Introduction to collections in Configuration Manager 2019)

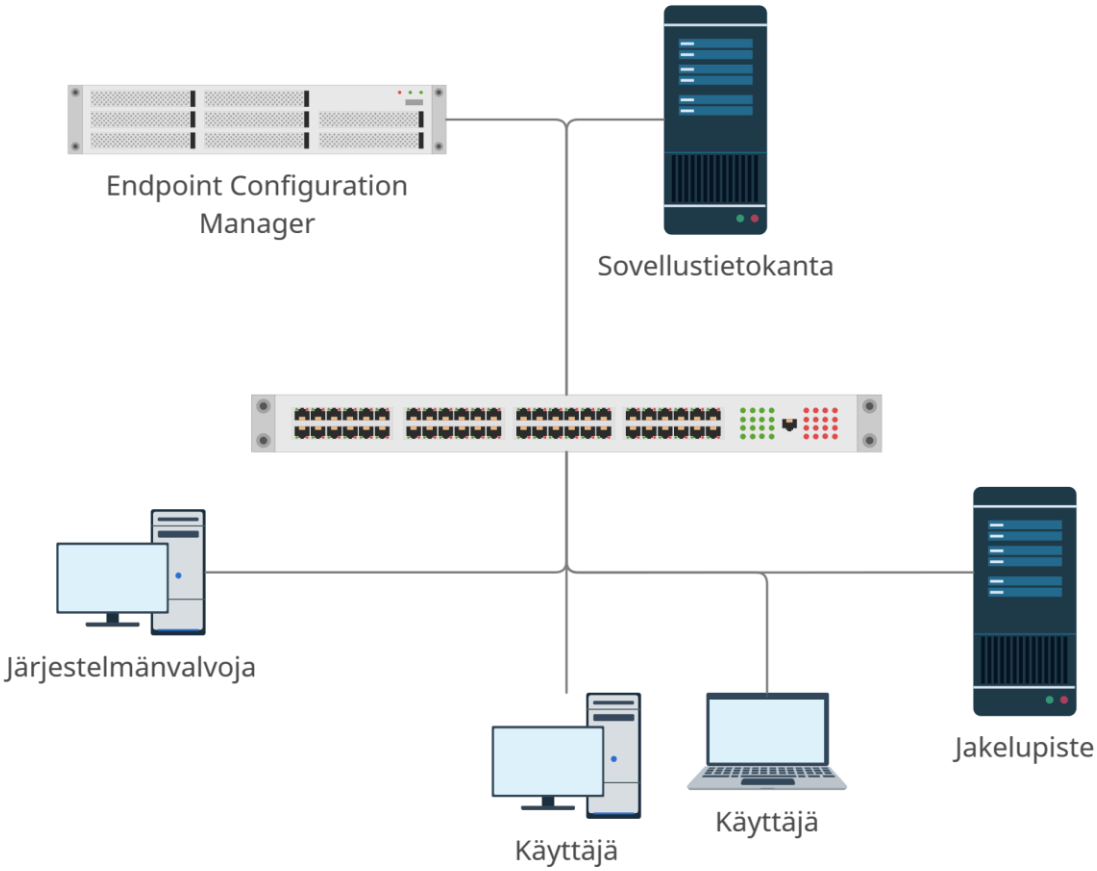
5.4 Palvelut

Itse ohjelman sisältä löytyy erilliset osiot käyttäjille, laitteille ja niiden ryhmille, ohjelmakirjastoille, monitoroinnille ja hallinnalle. Jokainen näistä rooleista tehostaa

verkon valvontaa ja hallintaa eri tavoilla, ja hyvässä hallintajärjestelmässä jokaista myös käytetään.

5.4.1 Ohjelmakirjasto

MECM saa AD:n kautta listan laitteista, jotka ovat hallinnan piirissä. Jotta sovellus voidaan jakaa verkossa olevalle koneelle, tulee sovelluksen asennustiedostot olla saatavilla sellaisessa tallennussijainnissa, jonne MECM:llä on pääsy. Yksi toimintamalli tähän on luoda erillinen verkkolevy toiselle palvelimelle, jotta hallintapalvelimen levy ja liikenne eivät ruuhkaudu ylimääräisistä pyynnöistä. Nämä pääsyoikeudet asetetaan sille koneelle, johon MECM on asennettu. Verkonvalvoja kopioi tarvittavat tiedostot jaettuun sijaintiin, jonka jälkeen voidaan luoda jakelutapa Endpoint Configuration Managerissa. Kun sovelluksesta lähetetään asennuspyyntö koneelle tai ryhmälle, asennuksen tiedot ja mediat lähetetään sovellustietokannasta jakelupisteelle, josta ne kopioidaan käyttäjille asennusta varten (ks. Kuvio 3.) Tarvittavista sovelluksista tehtiin tietoturvaselvitykset Keski-Suomen sairaanhoitopiirin muutoshallinnassa, jotta verkkoon ei asennettu sitä haavoittavia osia.



Kuvio 3 Jakeluverkon perusrakenne

KSSHP:n tapauksessa sovellukset asennettiin pääosin tietokoneiden järjestelmätilin alle, jotta tarvittavat sovellukset olivat näkyvissä kaikille käyttäjille. Koneet asennettiin eri osastoille niin, että kaikilla henkilöillä oli tiedossa millä koneilla on heidän tarvitsemansa sovellukset. Muussa tapauksessa ohjelmat olisivat asentuneet aina uusille koneille, joihin he kirjautuisivat ja näin sovellukset olisivat olleet kaikkien saatavilla. Tämä ei olisi ollut ongelma kaikkien sovellusten kohdalla, koska suurin osa vaati erilliset käyttäjätunnukset, mutta se olisi antanut mahdollisuuden yrittää murtautua suojattuihin tietoihin.

Ohjelmakirjasto-välilehdeltä löytyy osio nimeltä sovellukset, jonne luodaan jokaiselle jaettavalle sovellukselle oma jakelutapa. Tähän jakelutapaan määritetään kaikki tiedot, joita MECM tarvitsee asentaakseen ohjelman ja jotka käyttäjä näkee etsiessään sovellusta. Ohjelman sisään on rakennettu ominaisuus, joka tunnistaa asennettavan sovelluksen tiedot asennuspaketista automaattisesti, mutta tämä on rajattu vain tiettyihin

tiedostomuotoihin, joista yleisimpänä on Windowsin yleinen asennuspaketti .msi. (ks. Liite 1.) Toisena vaihtoehtona on syöttää sovelluksen tiedot manuaalisesti, jolloin ainoa pakollinen kenttä on nimi. Muita mahdollisia tietoja ovat julkaisija, kommentit, versio, järjestelmänvalvojan kommentit ja päivä jona sovellus on julkaistu. Seuraavassa osassa jakelun luomista määritetään, mille ryhmälle sovellus näkyy valinnaisesti asennettavien sovellusten listalla ja mitä tietoja käyttäjälle näkyy sovelluksesta. Näkyviksi tiedoiksi voidaan määrittää nimi, linkki sovelluksen dokumentointiin/käyttöohjeeseen ja sen otsikko, tietosuojaselosteen linkki, sovelluksen kuvaus, avainsanoja hakua varten ja ikoni sovellukselle sovelluskauppaan.

Osa sovelluksista jaettiin käyttäjien saataville, mutta ei pakotetusti. Nämä sovellukset näkyivät käyttäjien omassa ohjelmakirjastossa nimeltä *Software Center*. Ohjelmakirjasto sisältää kaikki MECM:n kautta koneelle pakotetut sovellukset, saatavilla olevat sovellukset ja niiden asennuksen tilat. Osaa sovelluksista tarvittiin vain tietyillä osastoilla ja nämä jaettiin vain niiden osastojen saataville. Osa yleisistä sovelluksista, esim. Notepad++, jaettiin kaikkien saataville. Edellisessä kappaleessa mainitut sovelluksen tiedot tuli täyttää tarkasti, koska ne tulevat näkyville käyttäjille Software Centeriin. Tämän vuoksi myös erillisten ohjeiden tekeminen oli tärkeää. Niistä löytyvillä ongelmaratkaisuilla voitiin säästää lähituen ja asentajien aikaa muihin tehtäviin. (Software Center user guide 2020)

Ohjelmiston jakelutyyppiin ei tarvitse määritellä sovelluksen sisältöä ja tunnistusmenetelmää, mikäli sovellustietojen tunnistukseen on käytetty automaattista tunnistusmenetelmää. Muussa tapauksessa nämä tiedot tulee syöttää käsin. Jakelutyypille määritetään asennusmedioiden sijainti, josta tulee löytyä asennusohjelma tai skripti asennukseen ja sovelluksen poistoon. Jakelutyyppiin määritetään tieto, asennetaanko vai poistetaanko kyseinen sovellus kohdekoneelta. Asennetaviin sovelluksiin pyrittiin aina tekemään batch-skripti, joka sisälsi tarvittavat komennot asennussovelluksen ajamiseen järjestelmän taustalla. Msi-pakettien hiljaiseen asennukseen käytettiin vipua */q* ja uudelleenkäynnistyksen estoon */norestart*. Skripti vaadittiin kolmannen osapuolen sovelluksiin, jotta ne voitiin ajaa käyttäjältä piilossa häiriön välttämiseksi ja asennusten lisäparametrien antamista varten. Sekä asennusta, että poistoa varten tehtiin erilliset

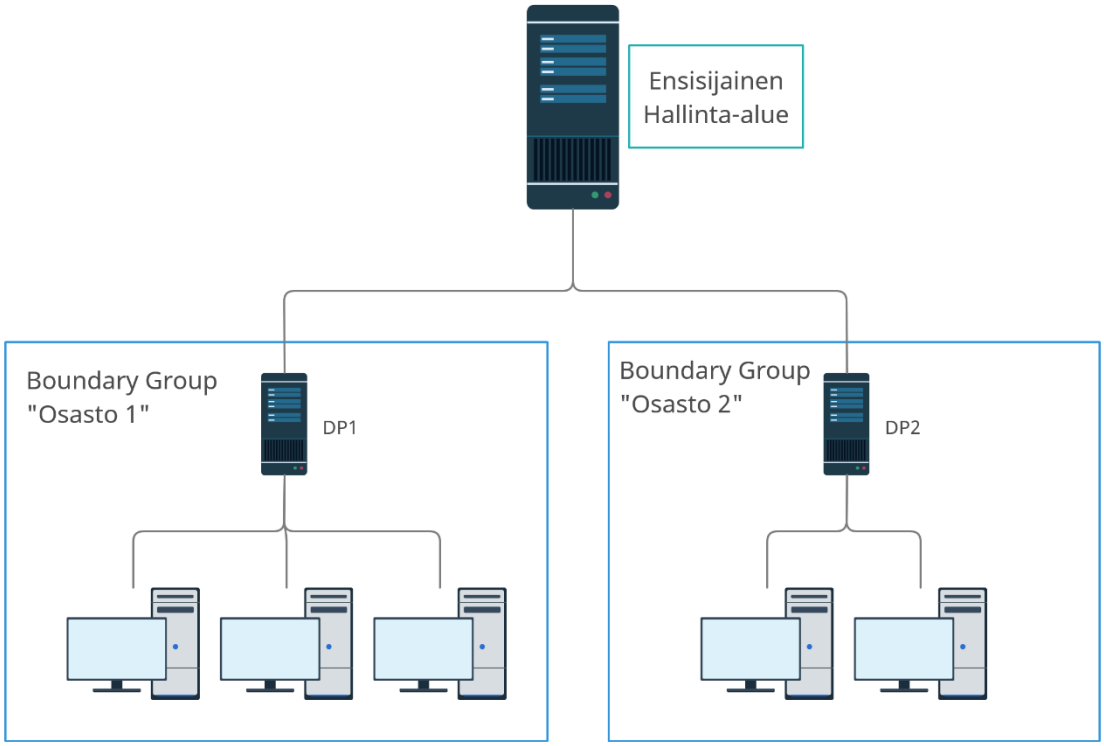
skriptit. Osaa sovelluksista ei voitu asentaa skriptillä, jos niissä ei ollut sisäänrakennettuja komentoja tausta-ajoa varten. Tällaiset sovellukset joko vaihdettiin toisiin, jossa oli oikeanlaiset komennot massa-ajoa varten, tai pienempien ryhmien tapauksissa asennettiin tietokoneille käsin.

Keino, jolla MECM tunnistaa onko sovellus asennettu koneelle, voidaan syöttää joko rekisteriavaimena tai polkuna tiedostoon, joka tulee löytyä koneelta ohjelman jo ollessa asentuneena. Varmempi keino tunnistukseen on käyttää rekisteriavainta, joka on yksilöllinen jokaiselle sovellukselle ja joka poistuu rekisteristä sovelluksen poiston yhteydessä. Vaihtoehtoisesti tunnistustavaksi voidaan luoda PowerShell tai VBScript-skripti, joka syötetään jakelutyyppiin.

Sovellus voidaan asentaa *yhdelle käyttäjälle*, *järjestelmälle* tai *järjestelmälle jos asennuskohde on laite, muussa tapauksessa käyttäjälle*. Sovellukset asennettiin aina järjestelmälle, koska tietyt sovellukset asennettiin aina osastoittain sairaalaan. Toisena syynä oli turhien asennusten välttäminen yksittäisille käyttäjille, jos useampi henkilö käyttäisi sovellusta samalla koneella. Asennukselle kerrotaan, voidaanko sovellus asentaa, jos käyttäjä on kirjautuneena. Vaihtoehtoina ovat *käyttäjä on kirjautuneena*, *ei väliä onko käyttäjä kirjautuneena*, ja *vain kun käyttäjä ei ole kirjautuneena*. Suurin osa Novan asennuksista voitiin toteuttaa, vaikka käyttäjä oli kirjautuneena, koska sovellukset pyrittiin asentamaan käyttäjältä piilossa järjestelmän taustalla. Sovelluksia ei asennettu koneelle, jos käyttäjä oli kirjautuneena vain niissä tapauksissa, joissa asennettava ohjelma vaati muiden ohjelmien sulkemista tai se näkyi käyttäjälle. Asennus voidaan suorittaa taustalla, normaalisti tai koko ruudulla ja vaihtoehtoisesti käyttäjälle voidaan antaa oikeus olla vuorovaikutuksessa asennusohjelman kanssa. Nämä vaihtoehdot eivät tulleet käyttöön aikaisemmin mainituista syistä. Jotkin sovellukset vaativat koneen uudelleenkäynnistämistä ja tämä voidaan joko sallia tai estää. Uudelleenkäynnistäminen estettiin oletuksena, jottei käyttäjien työt keskeydy yllättävästi. Jos asennettava sovellus vaatii muita sovelluksia asennettavaksi tai poistettavaksi ennen asennusta, ne voidaan määrittää myös jakelutyyppiin. Viimeisenä on mahdollisuus asettaa hälytyksiä sovelluksen jakeluun liittyen, esimerkiksi niissä tapauksissa, kun sovellus ei ole tietyn

määräajan sisällä löydettävissä koneilta. Tällöin MECM lähettää viestin järjestelmänvalvojille, jotta he voivat korjata ongelman jakelussa. (Create applications in Configuration Manager 2020)

Kun jakelutyyppi on luotu, voidaan asennuksen sisältämät tiedostot lähettää ohjelman avulla jakelupisteille, jotka jakavat ne edelleen päätelaitteille, kun ne niitä tarvitsevat. Jokaisen jakelupisteen tulee kuulua rajaryhmään (*boundary group*), joka on rajattu osa verkossa toimiville laitteille. Verkon alueita voidaan yhdistää yhdeksi rajaryhmäksi esimerkiksi valitsemalla tietyn IP-avaruuden osat. Tällaisen osion tarkoitus on pitää osa laitteista erillään esimerkiksi hallinnan helpottamista varten. Sovellusten jakamisen näkökulmasta jakelupisteitä tulee olla kaikissa rajaryhmissä, jotta jokaisessa verkon osassa on paikka, josta päätelaitteet voivat saada päivityksiä ja sovelluksia. Jos rajaryhmiä ei määritettäisi, kaikki verkon koneiden kyselyt ohjautuisivat yhdelle oletusarvoiselle koneelle, joka kuormittuisi turhan paljon (ks. Kuvio 4.)



Kuvio 4 Hallinta-alueet

Windows-päivityksiä ei jaettu automaattisesti koneille, vaan niillä oli aluksi tarkastusjakso. Päivityksistä luettiin tietoa mahdollisista ongelmatilanteista järjestelmän ja sovellusten kannalta ja selvitettiin mahdollisten tietoturva-aukkojen riski. Jos kaikki oli kunnossa, päivitykset jaettiin normaalisti koneille. Muussa tapauksessa odotettiin korjaavaa päivitystä.

Joissain tapauksissa jaettavan sovelluksen mukana on välttämättömiä tiedostoja, joita ei voitu tai haluttu jakaa koneille MECM:llä. Esimerkkinä pikakuvakkeet, jotka viittasivat erilliseltä palvelimelta ajettavaan sovellukseen. Tällaisen pikakuvakkeen olisi voinut jakaa sovelluspakettina, mutta se olisi jouduttu jakamaan julkisille työpöydille kaikille koneille, jossa sitä käytettäisiin. Tämä olisi ollut sekä tietoturvariski, että epäkäytännöllistä. Käyttäjä tarvitsi myös pääsyoikeudet palvelimelle. Paras käytäntö tähän oli jakaa sekä pikakuvake että oikeudet GPO:lla, jotta käyttäjällä on aina tarvittava pikakuvake tietokoneella, jonne hän kirjautuu.

5.4.2 Monitorointi ja raportointi

Sovellusten käytön valvonta on oleellinen osa sairaalan kulunhallintaa. Mikäli jotain sovellusta ei käytetä tarpeeksi, voidaan se vaihtaa toiseen tuotteeseen tai poistaa käytöstä kokonaan. Sairaalaympäristön laitesovellukset ovat kallis ylläpitokulu, jos niistä ei saada hyötyä. Samalla tavalla voidaan valvoa sovelluksia, joiden lisenssit ovat käytetty ja näyttää, että niitä voisi tarvita jatkossa lisää. Kaikki tämä on aktiivisen valvonnan tehtävä ja se kuuluu ympäristön elinkaarivalvontaan.

Novan siirtyvien järjestelmien projektissa selvitettiin eri sovellusten käyttöasteita. Tällä pyrittiin saamaan laajempi käsitys siitä, mitkä sovellukset ovat käytössä, jotta turhat sovellukset voitaisiin poistaa tai tarvittavia hankkia lisää. Osa sovelluksista löytyi aikaisemmin luotujen ryhmien perusteella ja osa jouduttiin etsimään WQL-kyselyiden (*Queries*) avulla. Kyselyt etsivät tutkittavan ryhmän tietokoneiden tietokannasta haettuja avaintietoja, jotka määritetään jokaiseen kyselyyn erikseen. Näillä voidaan etsiä tietoa koneen laitteistosta ja ohjelmistosta erittäin tarkasti ja siksi ne ovat hyvä keino kartoittaa sekä rauta- että ohjelmistotason tilannetta. Kyselyt luotiin joko käsin kirjoittamalla

tai käyttämällä selkeää graafista työkalua, joka antoi hakukriteerivaihtoehtoja. (Create queries in Configuration Manager 2020, WQL (SQL for WMI) 2018)

Raportointi liittyy oleellisesti valvontaan. Siinä missä monitoroinnilla voidaan manuaalisesti etsiä tietoa verkon laitteista, raportointi on automaattinen tapa saada päivityksiä oman järjestelmän tilanteesta. MECM:iin on sisäänrakennettu ominaisuus, joka on täysin järjestelmänvalvojan määriteltävissä. Sen pohjana toimii SQL Server Reporting Services (SSRS), joka mahdollistaa monimutkaistenkin kyselyiden luomisen. Raportteja voidaan luoda tarkastelemaan esimerkiksi uusimpien Windows-päivitysten tilannetta ja lähettämään niistä päivän päätteeksi tiivistelmä määritetyn henkilön sähköpostiin. Samalla tavalla voidaan luoda automatisoituja viestejä muista halutuista tilanteista, joita verkossa ilmenee. Raporttien tehtävänä on siirtää valvontaan ja tilannekatsauksiin liittyvät manuaaliset työt automaattisen järjestelmän tehtäväksi. (Introduction to reporting in Configuration Manager 2021)

6 Pohdinta

Työn tavoitteena oli rakentaa ja kuvata sairaala Novan työasema- ja käyttäjähallintaa sovellusjakelun näkökulmasta. Iso sairaala koostui isosta infrastruktuurista, johon sisältyi paljon eri osa-alueita, joista vain murto-osaa on käsitelty tässä työssä. Sovellusten jakaminen isossa hallitussa verkossa oli itselleni uusi aluevaltaus ja sen kautta pääsin osallistumaan ison maamerkin pystytykseen. Monet projektin osa alueet olivat itselleni jo tuttuja koulun puolesta, esim. Active Directory, ja se helpotti suurelta osin kokonaisuuden hahmottamista. Vaikka uusia asioita tuli paljon, ne oli helppo ymmärtää pienten opiskelupäivien jälkeen ja käytännön harjoittelulla testikoneilla.
Henkilökohtaisena tavoitteena oli oppia ymmärtämään kuinka Active Directory ja MECM toimivat isossa organisaatiossa ja kuinka jo tuotannossa olevia järjestelmiä siirretään yhdestä palvelinsalista toiseen.

Lopputuloksena Endpoint Configuration Manager toimi todella kiitettävästi sovellusten jaossa. Jakeluiden luominen oli helppoa, ja niiden osoittaminen jakeluryhmille ei vaatinut juurikaan lisävaivaa. Sovellusten asennuksen seuranta monitoroinnin kautta auttoi

näkemään jakeluiden tilanteet, samalla kun loin uusia sovellusjakeluita. Niissä tilanteissa, joissa jakelu antoi virhekoodin ongelma saatiin ratkaistua nopean googletuksen avulla. Skriptien ei tarvinnut olla pitkiä tai vaikeita ja tämä nopeutti omalta osaltani niiden ymmärryksessä ja luonnissa.

Novan nykytilanne näyttää ohjelmiston hallinnan kannalta erittäin hyvältä, tosin se ei ole täydellinen. Vaikka Endpoint Configuration Manager on laaja ja toimiva ohjelmisto, sen tehokkuus itsekseen ei yllä vielä esimerkiksi mobiililaitteiden puolelle. Laajempi mobiililaitteiden hallinta tarvitsisi rinnalleen esimerkiksi Microsoft Intunen, joka on erikoistunut mobiilipuoleen.
Yksi toteutusmahdollisuus Intunen kanssa olisi ottaa käyttöön nk. *Co-management*, jossa käytössä olisi sekä MECM että Intune. Tässä mallissa työjako voidaan määrittää laitekohtaisesti. MECM:iinn ja Intuneen kirjatut laitteet saavat molempien palveluiden ominaisuudet käyttöön. Yhdistetyssä hallintatilassa voidaan määrittää mitkä työt ohjataan MECM:lle ja Intunelle. Näin voidaan saada molempien palveluiden edut ilman ristiriitoja. Näiden kahden yhdistäminen vaatisi enemmän rahaa, aikaa ja työtä. MECM:n ja Intunen välillä on myös prioriteettiongelmia osan Group Policyn sääntöjen kanssa. Osalla säännöistä on preferenssi kumman ohjelmiston antamat asetukset ovat etusijalla ja tärkeämmäksi luokiteltu asetus voittaa. Tällaiset tapaukset vaatisivat lisää selvitys- ja suunnittelutyötä sääntöjen luomista varten, jotteivat loppukäyttäjien laitteet saa vääränlaisia asetuksia. Tämä on kuitenkin vain pieni osa kokonaislaitemäärästä Novassa.
Tulevaisuudessa on mielenkiintoista nähdä pitääkö Microsoft-yhtiö Endpoint Configuration Managerin ja Intunen erillään vai voisivatko ne yhdistyä yhdeksi kaiken kattavaksi ohjelmistoksi. Taka-ajatuksena tässä on jatkuvasti kasvava mobiililaitteiden osuus käyttäjien laitteistossa. SCCM ja MECM on luotu pääosin silloin, kun mobiililaitteiden osuus ja käyttötarkoitukset ovat olleet suhteellisen pienessä roolissa. Koska molemmat ohjelmistot ajavat samanlaista takaa hallintamallia hieman eri näkökulmasta, olisi mielestäni looginen seuraava askel pyrkiä yhdistämään nämä yhdeksi kokonaisuudeksi.

Henkilökohtaisen raporttini kirjoittaminen on ollut hieman haasteellista, johtuen omista työajoistani ja osittain myös globaalista pandemiasta. Loppujen lopuksi projekti

oli erittäin mielenkiintoinen ja opettava isojen organisaatioverkkojen ymmärtämisessä ja hallitsemisessa.

Lähteet

ADMX-backed policies in Policy CS. 2020. Microsoftin dokumenttisivusto. Viitattu 18.4.2021. https://docs.microsoft.com/en-us/windows/client-management/mdm/policies-in-policy-csp-admx-backed

Axon, S. 2021. The world's second-most popular desktop operating system isn't macOC anymore. Arstechnican artikkeli verkossa. Viitattu 17.4.2021. https://arstechnica.com/gadgets/2021/02/the-worlds-second-most-popular-desktop-operating-system-isnt-macos-anymore/

Active Directory Domain Services Overview. 2017. Microsoftin dokumenttisivusto. Viitattu 14.4.2021. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Best Practices. 2020. Ansiblen dokumenttisivusto. Viitattu 24.4.2021. https://docs.ansible.com/ansible/2.5/user_guide/playbooks_best_practices.html

Common questions and answers with device policies and profiles in Microsoft Intune. 2021. Microsoftin dokumenttisivusto. Viitattu 21.4.2021. https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot

Create applications in Configuration Manager. 2020. Microsoftin dokumenttisivusto. Viitattu 5.4.2021. https://docs.microsoft.com/en-us/mem/configmgr/apps/deploy-use/create-applications

Create queries in Configuration Manager. 2020. Microsoftin dokumenttisivusto. Viitattu 19.4.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/servers/manage/create-queries

Fundamentals of sites and hierarchies for Configuration Manager. 2016. -Microsoftin dokumenttisivusto. Viitattu 19.4.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/understand/fundamentals-of-sites-and-hierarchies

Group Police overview. 2016. Microsoftin dokumenttisivusto. Viitattu 15.4.2021. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11)

Install and configure distribution points in Configuration Manager. 2021. Microsoftin dokumenttisivusto. Viitattu 15.4.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/servers/deploy/configure/install-and-configure-distribution-points

Intro to Playbooks. 2020. Ansiblen dokumenttisivusto. Viitattu 24.4.2021. https://docs.ansible.com/ansible/2.5/user_guide/playbooks_intro.html

Introduction to collections in Configuration Manager. 2019. Microsoftin dokumenttisivusto. Viitattu 19.4.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/collections/introduction-to-collections

Introduction to reporting in Configuration Manager. 2021. Microsoftin dokumenttisivusto. Viitattu 21.4.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/servers/manage/introduction-to-reporting

Arola, J. 2010. Jyväskylään mahdollisesti uusi keskussairaala. Artikkeli Keskisuomalainen-lehdessä 4.6.2010. Viitattu 28.4.2021. https://www.ksml.fi/paikalliset/2794440

Microsoft Endpoint Manager overview. 2020. Microsoftin dokumenttisivusto. Viitattu 14.4.2021. https://docs.microsoft.com/en-us/mem/endpoint-manager-overview

Microsoft Intune is an MDM and MAM provider for your devices. 2020. Microsoftin dokumenttisivusto. Viitattu 17.4.2021. https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Policies in Policy CSP supported by Group Policy. 2019. Microsoftin dokumenttisivusto. Viitattu 18.4.2021. https://docs.microsoft.com/en-us/windows/client-management/mdm/policies-in-policy-csp-supported-by-group-policy

Policy CSP – ControlPolicyConflict. 2021. Microsoftin dokumenttisivusto. Viitattu 18.4.2021. https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict

Laiho, M., Penttilä, S. & Salomaa J. 2020. Sairaala Nova. Jyväskylä-lehden liite 25.11.2020. Viitattu 28.4.2021. https://online.fliphtml5.com/enxld/qstv/#p=1

Size and scale numbers for Configuration Manager. 2021. Microsoftin dokumenttisivusto. Viitattu 19.4.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/size-and-scale-numbers

Software Center user guide. 2020. Microsoftin dokumenttisivusto. Viitattu 15.4.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/understand/software-center

Support for Windows 10 in Configuration Manager. 2021. Microsoftin dokumenttisivusto. Viitattu 2.5.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/support-for-windows-10

Supported operating systems and browsers in Intune. 2021. Microsoftin dokumenttisivusto. Viitattu 2.5.2021. https://docs.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers

Supported OS versions for clients and devices for Configuration Manager. 2021. Microsoftin dokumenttisivusto. Viitattu 2.5.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/supported-operating-systems-for-clients-and-devices

Understanding ADMX-backed policies. 2020. Microsoftin dokumenttisivusto. Viitattu 18.4.2021. https://docs.microsoft.com/en-us/windows/client-management/mdm/understanding-admx-backed-policies

What Are Domains and Forests? 2014. Microsoftin dokumenttisivusto. Viitattu 5.5.2021. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)

What is Microsoft Intune app management? 2021. Microsoftin dokumenttisivusto. Viitattu 17.4.2021. https://docs.microsoft.com/en-us/mem/intune/apps/app-management

winrm - Run tasks over Microsoft's WinRM. 2020. Ansible dokumenttisivusto. Viitattu 17.4.2021. https://docs.ansible.com/ansible/2.5/plugins/connection/winrm.html

WQL (SQL for WMI). 2018. Microsoftin dokumenttisivusto. Viitattu 19.4.2021. https://docs.microsoft.com/en-us/windows/win32/wmisdk/wql-sql-for-wmi

Liitteet

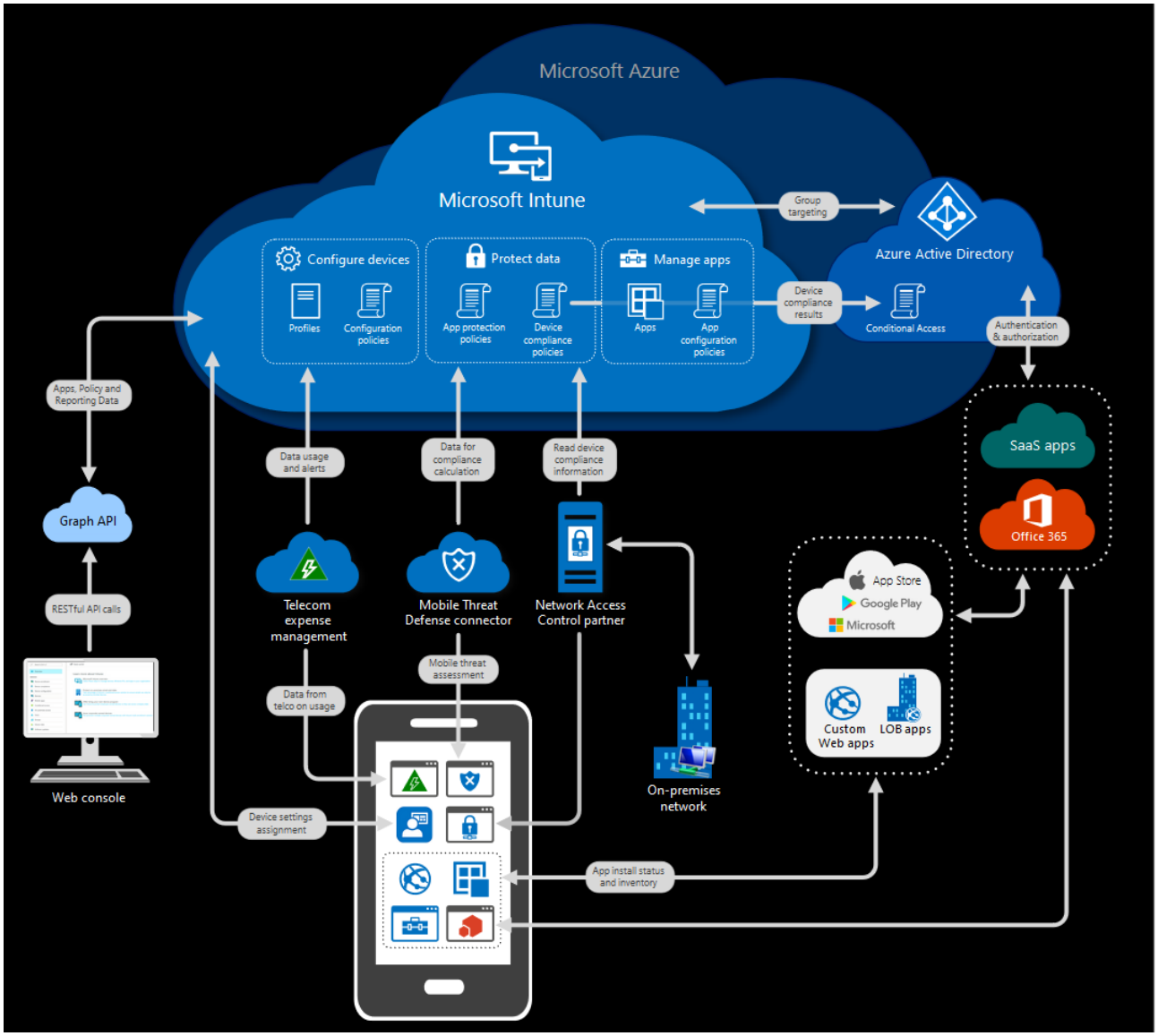
Liite 1 Tuetut jakelutavat pakettityyppeineen

Supported deployment types

Configuration Manager supports the following deployment types for applications:

Deployment type name	Description
Windows Installer (*.msi file)	A Windows Installer file.
Windows app package (*.appx, *.appxbundle, *.msix, *.msixbundle)	A Windows app package file (.appx), a Windows app bundle package (.appxbundle), a Windows 10 app package (.msix), or Windows 10 app bundle (.msixbundle).
Windows app package (in the Windows Store)	Specify a link to the app in the Windows Store, or browse the store to select the app.[Note 1]
Script Installer	Specify a script or program that runs on Windows clients to install content or to do an action. Use this deployment type for setup.exe installers or script wrappers.
Microsoft Application Virtualization 4	A Microsoft App-V v4 manifest.
Microsoft Application Virtualization 5	A Microsoft App-V v5 package file.
Windows Phone app package (*.xap file)	A Windows Phone app package file.
Windows Phone app package (in the Windows Phone Store)	Specify a link to the app in the Windows Store.
macOS X	For macOS computers running the Configuration Manager client. Create a .cmmac file with the **CMAppUtil** tool.
Web Application	Specify a link to a web application. This deployment type installs a shortcut to the web application on the user's device.
Windows Installer through MDM (*.msi)	Create and deploy Windows Installer-based apps to Windows 10 devices. For more information, see Deploy Windows Installer apps to MDM-enrolled Windows 10 devices.
Task sequence	Starting in version 2002, install or uninstall complex applications using task sequences. For more information, see Task sequence deployment type.

Liite 2 Microsoft Intune Azuren pilvessä



Liite 3 MECM:n tukemat käyttöjärjestelmät

Windows 10 version	ConfigMgr 1910	ConfigMgr 2002	ConfigMgr 2006	ConfigMgr 2010	ConfigMgr 2103
1803 (10.0.17134)	✓	✓	✓	✓	✓
1809 (10.0.17763)	✓	✓	✓	✓	✓
1909 (10.0.18363)	✓	✓	✓	✓	✓
2004 (10.0.19041)	✗	✓	✓	✓	✓
20H2 (10.0.19042)	✗	✗	✓ Note	✓ Note	✓ Note

Liite 4 Tuen piiristä poistetut käyttöjärjestelmät

OS version	Deprecation first announced	Support removed
Windows CE 7.0	July 19, 2019	Version 2006
Windows 10 Mobile	July 19, 2019	Version 2006
Windows 10 Mobile Enterprise	July 19, 2019	Version 2006
Windows 7		January 14, 2020
Windows Server 2008		January 14, 2020
Windows Server 2008 R2		January 14, 2020
Linux and UNIX	March 22, 2018	Version 1902
Windows 8: Professional, Enterprise	January 12, 2016	Version 1802
Windows Embedded 8 Pro	January 12, 2016	Version 1802
Windows Embedded 8 Industry	January 12, 2016	Version 1802
Windows XP Embedded Includes all XP-based embedded operating systems	July 10, 2015	Version 1702
Windows Vista	July 10, 2015	Version 1511
Windows Server 2003 R2	July 10, 2015	Version 1511
Windows Server 2003	July 10, 2015	Version 1511
Windows XP	July 10, 2015	Version 1511
macOS X 10.6 - 10.8	July 10, 2015	Version 1511
Windows Mobile 6.0 - 6.5	July 10, 2015	Version 1511
Nokia Symbian Belle	July 10, 2015	Version 1511
Windows CE 5.0 - 6.0	July 10, 2015	Version 1511

Liite 5 Yhteensopivuustaulukko

Platform	Configuration Manager client	On-premises MDM	Configuration Manager with Exchange	Intune
Android			Yes	Yes
iOS			Yes	Yes
macOS X	Yes		Yes	Yes
Windows 10	Yes	Yes	Yes	Yes
Windows 10 Mobile		Yes	Yes	Yes
Windows (previous versions)	Yes		Yes	
Windows Server	Yes		Yes	
Windows Embedded	Yes			