

**MICROSOFT-AKTIIVIHAKEMISTO MONIASIAKASYMPÄRISTÖSSÄ
CASE: CALPRO**



Ammattikorkeakoulututkinnon opinnäytetyö

Visamäki, Tietojenkäsittelyn koulutusohjelma

Syksy, 2017

Mika Laakso

Tietojenkäsittelyn koulutusohjelma
Visamäki

Tekijä	Mika Laakso	Vuosi 2017
Työn nimi	Microsoft-aktiivihakemisto moniasiakasympäristössä case: Calpro	
Työn valvoja	Erkki Laine	

TIIVISTELMÄ

Työn toimenksiantajana toimi Calpro Oy. Calpro tuottaa ICT-palveluja omistaja-asiakkailleen, suurimpana Lahden kaupunki ja Päijät-Hämeen Hyvinvointiyhtymä. Sote-uudistuksen ja kunnallisen yhtiöittämisen seurauksena on tullut tarve tarjota asiakaskohtaisia palveluja omistaja-asiakkaille mahdollisimman kustannustehokkaasti. Useamman tietotekniikkapalveluja tarjoavan organisaation yhdistämisellä Calpro Oy:hyn tietojärjestelmien segmentointi ja asiakaskohtainen hallinta on noussut tärkeään rooliin ylläpidon kannalta. Opinnäytetyössä keskityttiin Microsoftin aktiivihakemistopalveluun: miten se pystytään tarjoamaan asiakaskohtaisena toteutuksena nykyisille asiakkaille ja mahdollisesti laajentamaan tulevaisuudessa koskemaan useampia asiakkaita.

Työ oli toiminnallinen opinnäytetyö, jossa keskeisenä ideana on kuvata modulaarinen malli asiakaskohtaisesta aktiivihakemisto toteutuksesta moniasiakasympäristössä, jota on helppo laajentaa. Työssä sovellettiin tekijän omaa tietämystä Microsoftin aktiivihakemistosta, sekä Microsoftin parhaita käytäntöjä aktiivihakemistoympäristön suunnittelusta. Teoriaosuudessa tutustuttiin Microsoft-aktiivihakemistopalveluihin yleisesti. Teoriaosuutta ja käytännön tietämystä yhdistämällä luotiin modulaarinen malli segmentoidusta aktiivihakemistoympäristöstä.

Avainsanat Microsoft Active Directory, Microsoft Azure, pilvipalvelut, asiakkuudenhallinta, segmentointi

Sivut 39 sivua, joista liitteitä 1 sivua

Degree program in Business Information Technology
Visamäki

Author	Mika Laakso	Year 2017
Subject	Microsoft Active Directory in Multi-Customer Environment Case: Calpro	
Supervisor	Erkki Laine	

ABSTRACT

The commissioner of this thesis was Calpro Oy. Calpro Oy provides ICT-services for owners. Renewal process of Finnish healthcare sector and incorporation of municipal owned ICT have arisen a need to provide both common and customer dedicated ICT services to Calpro Oy owners in a cost-efficient way. Combining ICT-functions of both city of Lahti and Päijät-Häme Central Hospital to Calpro Oy created a company that will take care of providing these ICT-functions for existing customers in a combined environment.

The study was a functional thesis, where the main idea was how to provide Microsoft Active Directory services and Microsoft Azure Active Directory services in common platform in a cost-efficient and secure way. Thesis explained how to create a model for customer segmented AD-solution in multi-customer environment that can easily be applied for existing and new customers.

In this thesis, the author applied his own knowledge of AD and Microsoft best-practices scenarios for Active Directory design. In the theory part, the author has deepened his knowledge of Active Directory design and services. The theory was combined with practical experience and know-how and segmented model for modular Active Directory design was created for Calpro Oy.

Keywords Microsoft Active Directory, Microsoft Azure, Cloud services, Customer relationship management, Segmentation

Pages 39 pages including appendices 1 pages

SISÄLLYS

1	JOHDANTO.....	1
2	ICT-YMPÄRISTÖN LÄHTÖTILANNE.....	2
3	WINDOWS SERVER AKTIIVIHAKEMISTO	4
3.1	Metsän looginen ja fyysinen rakenne	4
3.2	Toimialueen palvelimet.....	5
4	AKTIIVIHAKEMISTON VERKKOPALVELUT DNS JA DHCP	8
5	RYHMÄKÄYTÄNNÖT	10
6	TIEDOSTO- JA LEVYPALVELUT.....	11
7	KÄYTTÄJÄTUNNUSPROSESSI JA VOLUMEACTIVATION/KMS -PALVELU.....	13
8	RADIUS JA AVAINTENHALLINTA	14
9	BITLOCKER-SALAUSPALVELU	15
10	MOBIILILAITTEHALLINTA (MDM).....	17
11	PUBLIC KEY INFRASTRUCTURE (PKI)	19
12	AKTIIVIHAKEMISTON FEDERAATIOPALVELUT	20
13	PILVIPALVELUNA MICROSOFT AZURE	22
14	TIETOKONEIDEN HALLINTAAN SYSTEM CENTER CONFIGURATION MANAGER.....	25
15	ICT-YMPÄRISTÖN VALVONTAAN SYSTEM CENTER OPERATIONS MANAGER	27
16	PALVELUIDEN MODULAARISET TOTEUTUKSET	28
17	YHTEENVETO JA POHDINTA.....	29
	LÄHTEET	30

KÄSITELUETTELO

AD	AD (engl. Active Directory) Microsoftin hakemistopalvelu.
AZURE	Microsoftin pilvipalvelu alusta.
AD FS	AD FS (engl. Active Directory Federation Services) Microsoftin ratkaisu käyttäjien kertakirjautumiseen.
DFS	DFS (engl. Distributed File System) Tiedostojakojen esitysmuoto, jolla voidaan esittää redundanttisesti useampia jaettu hakemistoja eri lähteistä asiakkaalle.
DNS	DNS (engl. Domain Name System) Internetin nimipalvelujärjestelmä, jolla muutetaan verkkotunnukset IP-osoitteiksi.
DHCP	DHCP (engl. Dynamic Host Configuration Protocol) Verkko-protokolla, jolla jaetaan IP-osoitteita verkkoon liittyville laitteille.
FQDN	FQDN (engl. Fully Qualified Domain Name) Täydellinen toimialueenimi.
FSMO	FSMO (engl. Flexible Single Master Operation) roolit ovat Aktiivihakemiston ohjauspalvelimia.
GPO	GPO (engl. Group Policy Object) on ominaisuus, jolla hallitaan käyttäjän ja tietokoneen työskentely ympäristöä.
IDM	IDM (engl. Identity Management) identiteetin hallintapalvelu.
KMS	KMS (engl. Key Management Service) Microsoftin palvelu vo-luumi käyttöoikeuksien aktivoimiseen.
MDM	MDM (engl. Mobile Device Management) Mobiililaitteiden hallintapalvelu.
PKI	PKI (engl. Public Key Infrastructure) on julkisten avainten hallintajärjestelmä, tietoturva sertifikaatteja varten.
RADIUS	RADIUS (engl. Remote Authentication Dial In User Service) on standardi, jolla on määritelty tekniikka käyttäjien ja laitteiden tietoverkkoon todennetaan.
SCCM	SCCM (engl. System Center Configuration Manager) Microsoftin järjestelmä hallinnan työkaluohjelmisto.
SCOM	SCOM (engl. System Center Operations Manager)

Microsoftin järjestelmävalvonnan työkaluohjelmisto.

UPN

UPN (engl. User Principal Name) Kirjautumistapa, jonka esitysmuoto on määritelty muotoon "käyttäjätunnus@toimialue".

1 JOHDANTO

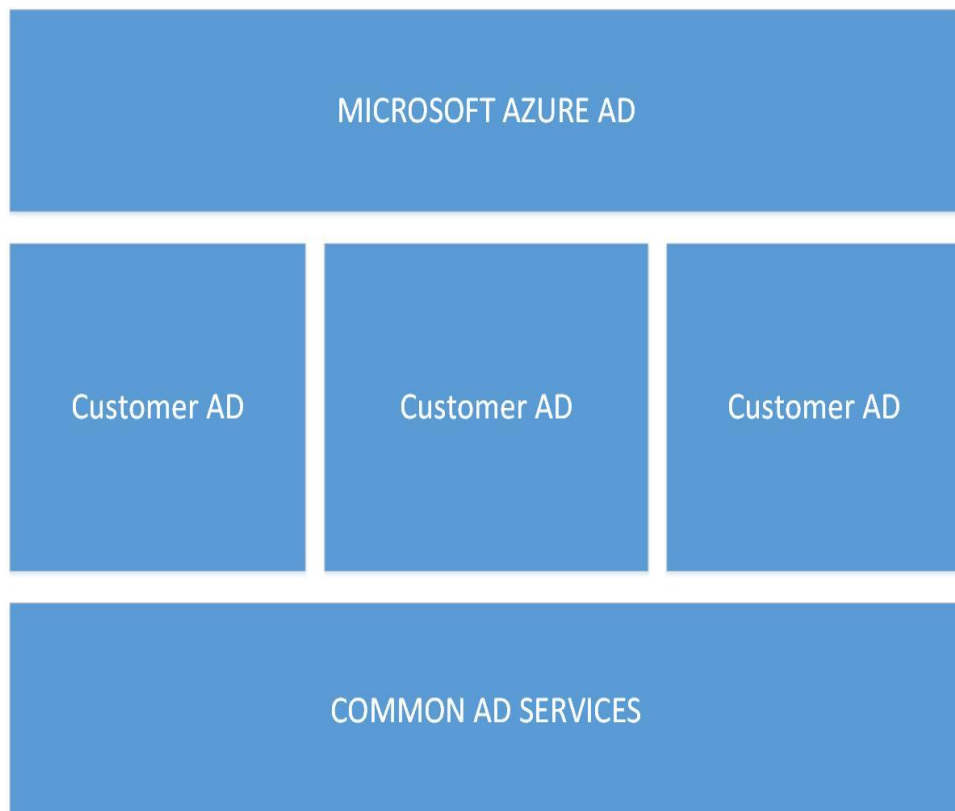
Opinnäytetyön toimeksiantaja on Calpro Oy ICT-Palvelut. Calpron ICT-Palvelujen tehtävänä on tuottaa omistaja-asiakkailleen ICT-palveluja. Calpro Oy toimii asiakkailleen sisäisenä palveluntarjoajana. Työ on hyvin ajan-kohtainen, sillä se liittyy sote-uudistukseen. Lahden kaupungissa, ympäristökunnissa ja Päijät-Hämeen hyvinvointiyhtymässä yhtiöittämisen seurauksena tapahtuneiden liikkeenluovutusten johdosta ICT-palvelujen keskittetty tuottaminen on siirretty Calpro Oy:n tehtäväksi. Tavoitteena on yhdistää eri toimintaympäristöjä kunnallisen palveluyhtion toimialueeseen. Suurimpina asiakkaina uudella palveluyhtiöllä ovat Lahden kaupunki, Päijät-Hämeen hyvinvointiyhtymä ja peruspalvelukeskus Oiva. Sote-palvelujen keskittäminen Päijät-Hämeen hyvinvointiyhtymään tarkoittaa henkilöstön ja palvelujen siirtämistä Lahden kaupungilta ja Hollolan kunnalta Päijät-Hämeen hyvinvointiyhtymään. Mittavat ICT-muutokset ovat luo- neet tarpeen arkkitehtuurillisille muutosmalleille, joiden avulla maakunta- mallin vaativat käytännön toteutukset ovat mahdollisia toteuttaa. Opin- näytetyön idea syntyi Calpron tarpeista tuottaa asiakkailleen palveluja, joista osa tuotettaisiin asiakaskohtaisina ja osa yhteisinä palveluina. Ta- voitteena olisi saada kustannussäästöjä ICT-kuluissa. Näihin pyritään yllä- pitotehtävien automatisoinnilla ja palveluiden yhdistämisellä yhteisiin alustoihin mahdollisuuksien mukaan.

Opinnäytetyössä keskitytään Microsoftin aktiivihakemistoon ja siihen liit- tyihin palveluihin sekä Microsoft Azure –pilvipalvelutuotteen AD-osaan. Työssä kuvataan AD-ympäristöä ja palveluja ylätasoon topologia kuvilla, joi- den tarkoituksena on havainnoillistaa, miten asiakaskohtainen segmen- tointi on tarkoitus toteuttaa ja miten palveluiden tuottaminen on mahdol- lista yhteisiltä osin kustannustehokkaasti ja tietoturvallisesti. Työssä pyri- tään vastaamaan kysymyksiin: Miten asiakaskohtainen ympäristö on tar- koitus rakentaa? Mistä palveluista AD-ympäristö koostuu? Miten saadaan rakennettua liitteen 1. kaltainen modulaarinen malli, jota on helppo laa- jentaa, mikäli asiakasmäärä lisääntyy?

2 ICT-YMPÄRISTÖN LÄHTÖTILANNE

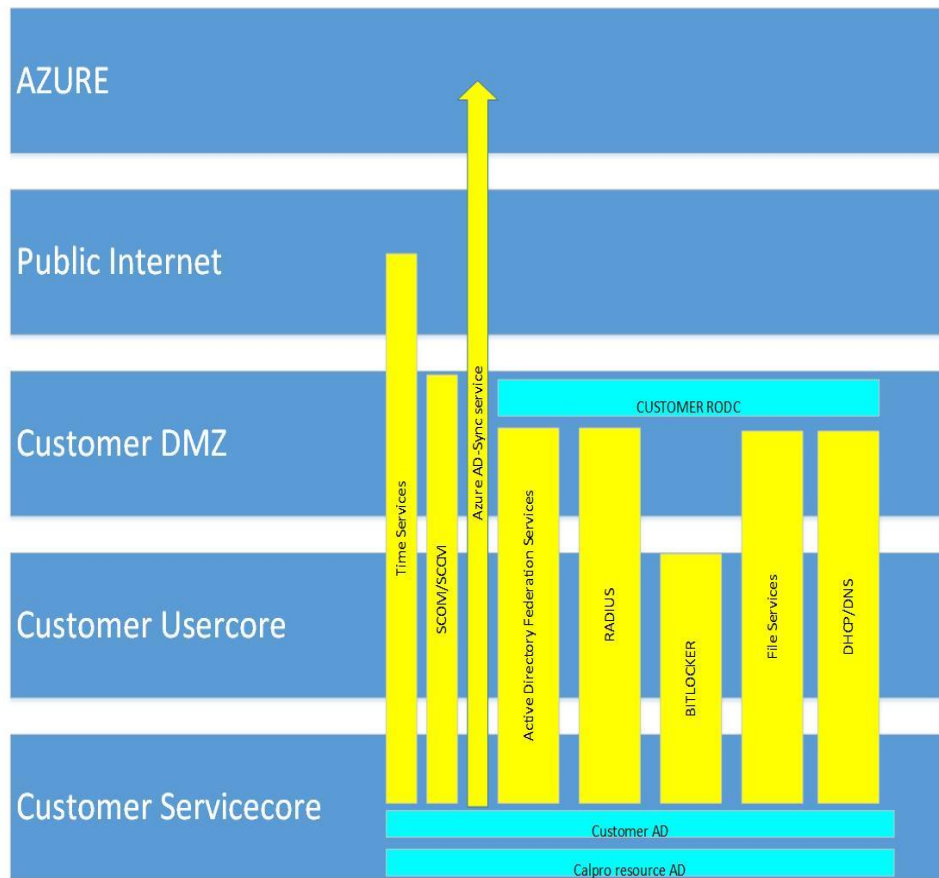
Ympäristön valmistelut aloitettiin luomalla ylemmän tason arkkitehtuurimalli, johon otettiin huomioon Microsoft Azure AD -liitäntä, asiakaskohtaiset AD toteutukset asiakkaan vaatimusten mukaan, sekä yhteinen resurssi-AD, josta on tarkoitus tuottaa yhteiset palvelut. Yhteisten palveluiden käyttö on suositeltavaa kustannustehokkuuden takia: erillistä palvelukoh- taista serveriympäristöä ei tarvitse rakentaa.

Arkkitehtuurillisesti palvelut jaettiin yhteisiin AD-palveluihin, joita käytetään kaksisuuntaisen luottosuhteen avulla, sekä asiakaskohtaisiin palveluihin. Kuvassa 1 on esitetty, miten asiakaskohtaiset AD-palvelut segmentoidaan omiksi kokonaisuuksikseen ja miten yhteiset ja Azure-palvelut näihin liittyvät. Yhteisten palvelujen vaatimat luottosuhteet luodaan asiakas-AD:n ja resurssi-AD:n väliin kaksisuuntaisena. Azure-AD toteutetaan yhteisenä tenanttina, jolloin saavutettavat kustannushyödyt ovat merkittäviä lisenssikustannusten ja ylläpitokulujen osalta.



Kuva 1: AD-arkkitehtuuri

Palvelujen sijoittaminen verkkoarkkitehtuuriin toteutettiin seuraavasti:



Kuva 2: Palveluarkkitehtuuri verkkokuva

Verkkoarkkitehtuuri on jaettu konesalissa kolmeen osaan. DMZ-verkossa toteutetaan julkiseen internettiin päin tarjottavat palvelut. Usercore-verkoon sijoitetaan työasemat, tulostimet ja muut käyttäjien tarvitsemat verkkoyhteykselliset laitteet. Servicecore on palvelin vlan-verkko, jossa on sijoitettuna usercoreen tarjottavat palvelut. Kuvasta 2 nähdään miten palvelut jakautuvat eri verkkoalueille.

Microsoft Azure -pilvipalvelut tarjotaan julkisen internetin yli joko VPN- tai IPsec -tunneloinnilla suojattuna. Tietoliikenteellisesti asiakasverkot on segmentoitu asiakaskohtaiseksi toteutukseksi ja palomuuureilla suojattu. Pääsy yhteisiin palveluihin on rajattu palomuuureissa IP- ja porttikohtaisin avauksin, jolloin saadaan toteutettua tietoturallinen asiakaskohtainen malli. Tietoturvan kannalta kaikki asiakasverkot segmentoidaan omiksi ympäristöikseen niin, että pääsy servicecoren palveluihin rajataan palomuuureilla ja yhteydet reititetään kuormantasaajan kautta. DMZ- ja Servicecore-verkot levitetään useamman konesalin ratkaisuksi, jolloin palveluiden 24/7 käytettävyys pystytään takaamaan. Jatkokehityksenä konesalien verkot tullaan toteuttamaan SDN-ratkaisulla.

3 WINDOWS SERVER AKTIIVIHAKEMISTO

Opinnäytetyötä käytetään Calpron AD-projektin pohjana. Seuraavissa kappaleissa käydään läpi ympäristön nykytilaa ja yksittäisten palvelujen ominaisuuksia ja rooleja. Seuraavat kappaleet esittävät miten konfiguraation muutoksen on tarkoitus toteuttaa Microsoftin parhaiden käytäntöjen mukaan. Osa muutoksista perustuu myös opinnäytetyön tekijän parhaisiin käytännön kokemuksiin Microsoft ympäristön suunnittelusta ja ylläpidosta.

3.1 Metsän looginen ja fyysinen rakenne

Looginen rakenne perustuu asiakaskohtaiseen AD-metsä malliin, johon asetetaan yksi toimialue ja yksi toimipiste. Fyysiseltä rakenteelta Domain Controller -palvelimia sijoitetaan 1 fyysinen palvelin / konesali ja virtuaalipalvelimia myös 1 / konesali. Palvelimien resurssit mitoitetaan asiakkaan AD-tunnusten ja työasema määrän mukaan. Tarvittavat laajennukset pyritään toteuttamaan virtuaalipalvelimilla, tavoitteena saada palvelin kustannukset pidettyä mahdollisimman alhaisena ja fyysisten palvelimien määrä minimoituna. Kahden konesalin ratkaisuna saadaan vikasietoisuusvaatimukset täytettyä. Aktiivihakemiston FQDN nimenä käytetään ”asiakas”.local nimeä. NetBIOS-nimenä käytetään ”asiakas”. (Microsoft 2013). Nykytilan muutos pelkästä asiakaskohtaisesta toteutuksesta modulaariseen toimintamallin pyritään toteuttamaan käyttämällä olemassa olevaa infrastruktuuria mahdollisimman paljon.

Tämä haluttu ratkaisumalli pyritään toteuttamaan mahdollisimman joustavasti ja asiakkaiden näkökulmasta mahdollisimman pienillä tuotantokatkoksilla. Käytännössä rakennetaan rinnalle uusi ympäristö, jolloin toiminnallisuus- testaus on helpompaa ja migraatio uuteen ympäristöön voidaan toteuttaa parhaalla mahdollisella tavalla jakamalla migratoitavat tunnukset ja konetilit asiakkaan kriittisyysmäärittelyn mukaisesti ja infrastuktuurin kannalta järkevän pieniin kokonaisuuksiin. Uuden ympäristön metsä ja toimialue toteutukset tehdään Windows 2012 R2 tai Windows 2016 servereillä ja aktiivihakemiston toiminnallisuustaso asetetaan 2012 tasolle. Tasonnosto 2016 tasolle tehdään myöhemmin, kun taustajärjestelmät mahdollistavat Windows Server 2016 version käytön. UPN-suffiksit asetetaan vastaamaan sähköpostiosoitetta. UPN-suffiksien suunnittelussa on huomioitava myös siirtymä paikallisen sähköpostin ja pikaviestinnän käytöstä O365 pilvipalvelun käyttöön. Luottosuhteiden rakennetaan asiakas-AD:n ja Calpron resurssi-AD:n välille kaksisuuntaisena. Sovellusten toimintavaa-

timukset vaikuttavat myös luottosuhteen määrittelyyn. Ensisijaisena toteutustapana sovelluksille on ADFS-federaatio, mikäli sovellus ei tätä tue on toteutustapa luottosuhteen yli.

3.2 Toimialueen palvelimet

Taulukkoon 1 on listattu asiakaskohtaisen AD-ympäristön tarvittavat palvelimet ja palvelut.

Taulukko 1. AD-ympäristön palvelimet ja palvelut.

Nimi	Si-jainti	Palvelin	Virtuaali-nen	Palvelut
DC1	Calpro	Win-dows Server 2012 R2		AD, DNS, Global Catalog
DC2	Calpro	Win-dows Server 2012 R2		AD, DNS, Global Catalog
DC3	Calpro	Win-dows Server 2012 R2	x	AD, DNS, Global Catalog
DC4	Calpro	Win-dows Server 2012 R2	x	AD, DNS, Global Catalog
DHCP1	Calpro	Win-dows Server 2012 R2	x	DHCP
DHCP2	Calpro	Win-dows Server 2012 R2	x	DHCP
DA1	Calpro	Win-dows Server 2012 R2	x	Direct Access
DA2	Calpro	Win-dows Server 2012 R2	x	Direct Access
ADFS1	Calpro	Win-dows Server 2012 R2	x	AD Federation services 1

ADFS2	Calpro	Windows Server 2012 R2	x	AD Federation services 2
ADFS-Proxy1	Calpro	Windows Server 2012 R2	x	Web Application Proxy 1
ADFS-proxy2	Calpro	Windows Server 2012 R2	x	Web Application Proxy 2
NPS1	Calpro	Windows Server 2012 R2	x	NPS 1
NPS2	Calpro	Windows Server 2012 R2	x	NPS 2

Suurin osa palvelimista toteutetaan virtuaalisina, Domain Controller koneista toteutetaan 1 Domain Controller konesalia kohti fyysisenä palvelimena, muut kapasiteettivaatimusten mukaan virtuaalisena.

Schema Master on vastuussa kaikista muutoksista ja päivityksistä koko metsän alueella Aktiivihakemiston schemaan. Vain schema administrators –ryhmän jäsenet voivat tehdä muutoksia schemaan (Microsoft 2015). Domain Controller -kone, jolla on Domain Naming Master –rooli, huolehtii myös siitä, että uusia toimialueita voidaan lisätä ja poistaa metsän alueella. Relative Identifier Master (RID) –roolia tarvitaan luotaessa uusia security principal objekteja. Kaikilla toimialueen Domain Controller -koneella on oma RID-pooli, jotta käyttäjätunnuksia, tietokonetilejä jne. voidaan luoda. Kun pooli tyhjenee, Domain Controller -kone pyytää uuden poolin RID-masterilta. Primary Domain Controller Emulator (PDC Emulator) vastaa vanhempien clienttien sisäänkirjautumisten vastaanottamisesta sekä salasanojen varmentamisesta. Se toimii myös Domain Master Browserina sekä Windows Time palvelimena. Infrastructure Master vastaa toimialueiden välisten käyttäjien ja käyttäjäryhmien välisten sidosten toimivuudesta.

Global Catalog on hajautettu tietovarasto, joka sisältää näkymän kaikkiin AD-metsässä oleviin objekteihin. Global Catalog -palvelu asetetaan päälle kaikkiin metsän Domain Controller –palvelimiin, myös tulevaisuudessa mahdollisille uusille palvelimille. KCC-palvelu määrittää replikointi topologian Site Link arvojen mukaan ja luo yhteyden palvelimien välille. Replikointitopologian muutosasetukset pidetään oletusasetuksissa, jolloin ne toimivat automaattisesti. Hierarkian mukaisesti PDC -palvelin metsän juuressa päättää käytettävän kellonajan. PDC-palvelin hakee kellon ajan julkisessa internetissä olevilta NTP-palvelimilta: time1.mikes.fi ja time2.mikes.fi

Active directory recycle bin -ominaisuus mahdollistaa poistettujen AD-objektien palautuksen, tällä saavutetaan nopean palautuksen etu erillisestä backup järjestelmästä tehtävään palautukseen verrattuna.

Poistettuja objekteja ja palautuksia voidaan tehdä Active Directory Administrative Center -työkalulla. Windows Server 2012 R2 Active Directory Recycle Bin -ominaisuus tullaan ottamaan käyttöön. Oletusasetuksena poistettu objekti on palautettavissa 180 päivän ajan.

4 AKTIIVIHAKEMISTON VERKKOPALVELUT DNS JA DHCP

DNS-palvelun tarkoituksena on tarjota asiakkaille nimipalvelut, joilla verkotunnusten muunto IP-osoitteiksi on käytännöllisempää.

Kaikki Windows Server domain controller -palvelimet määritellään toimimaan DNS -palvelimina. DNS-zonet määritellään Windows 2012 R2 Active Directory integroiduiksi DNS-zoneiksi. Nimen selvitystä voidaan keskittää Calpron resurssiympäristöön ja tuottaa sitä palveluna kaikille asiakkaille. Hallinnan helpottamiseksi otetaan myös käyttöön Microsoftin IPAM -palvelin, jolla pystytään hallitsemaan kyseiset palvelut ja pitämään helposti yllä monimutkaista infrastruktuuria. DNS juuri domainin nimi on "asiakas".local, jossa kaikki palvelimet ja työasemat sijaitsevat.

Forwarder palvelimien tarkoitus on ohjata nimipalvelukyselyt ulkopuoliselle nimipalvelimelle. Modulaarisessa toteutuksessa nimipalvelukyselyiden ohjaukset voidaan toteuttaa asiakkaan tarpeiden mukaisesti, joko yhteisenä palveluna tai asiakaskohtaisesti segmentointuna. Ehdolliset ohjaukset toimivat samalla tavalla kuin forwarder palvelimet. Erona edellä mainittuun on nimipalvelukyselyjen ohjaukseen käytettävien ehtojen käyttö, jolloin voidaan määritellä tarkemmin, mitkä kyselyt ohjataan eteenpäin.

Dynaaminen päivitys: Dynamic Updates -asetuksella sallitaan vain autentikoitujen asiakkaiden päivittää DNS-tiedot.

Asetetaan arvoon Secure Only.

SOA replikointi:

SOA-tietueen replikointiin liittyvät oletusarvot:

- Refresh interval 15 min.
- Retry interval 10 min.
- Expires after 1 day.

Cache pollution: Secure cache against pollution –asetus estää sellaisten tietueiden kirjoittamisen cacheen, jotka on lähetetty palvelimelta ja joka ei ole auktoritatiivinen kyseiselle zonelle. Asetus on oletuksena päällä Windows Server 2012 ja 2016 DNS -palvelimissa (Microsoft 2016).

Scavenging: Domain Controller asetetaan poistamaan vanhat DNS tiedut.

Asetukset Scavenging palvelua varten:

- No-Refresh interval: 4 days.
- Refresh interval: 4 days.
- Scavenging period: 7 days.

Forward lookup zonen toiminnallisuus on tarkoituksenmukaista jakaa asiakaskohtaisiksi alueiksi, jolloin zone määritykset toteutetaan toimialuekohtaisiksi. Nimenselvityksen kannalta yhteisen DNS -palvelimen käyttö helpottaa zonejen hallintaa. Reverse lookup -palvelun toiminta on päinvastoin, kun forward lookup zone:n kohdalla, tässä DNS-kyselyllä haetaan IP-osoitteet nimeksi. Konfiguraatio toteutetaan vastaavasti DNS -serverille kun forward lookup zonet.

DHCP -palvelu asennetaan erillisille palvelimille. Tähän tarkoitukseen käytetään kahta Windows Server 2016 palvelinta, jotka klusteroidaan. Calpron DHCP:lle tulee useita DHCP-scopeja, joista osoitteet haetaan IP helper -osoitteiden avulla. Asiakkaan vaatimusten tai verkkototeutuksen mukaan voidaan käyttää, joko yhteistä DHCP-palvelinta tai asiakaskohtaista ratkaisua. DHCP:n avulla jaetaan työasemille IP-osoite, aliverkon maski, oletus yhteyskäytävä, DNS-palvelimien osoitteet ja IP toimialueen nimi. DHCP-leasing aika on määritelty 8 päiväksi. Palvelimille ei DHCP:llä jaeta osoitteita vaan käytetään aina kiinteitä IP-osoitteita. DHCP-scope asetetaan Load Balanced toimintatilaan.

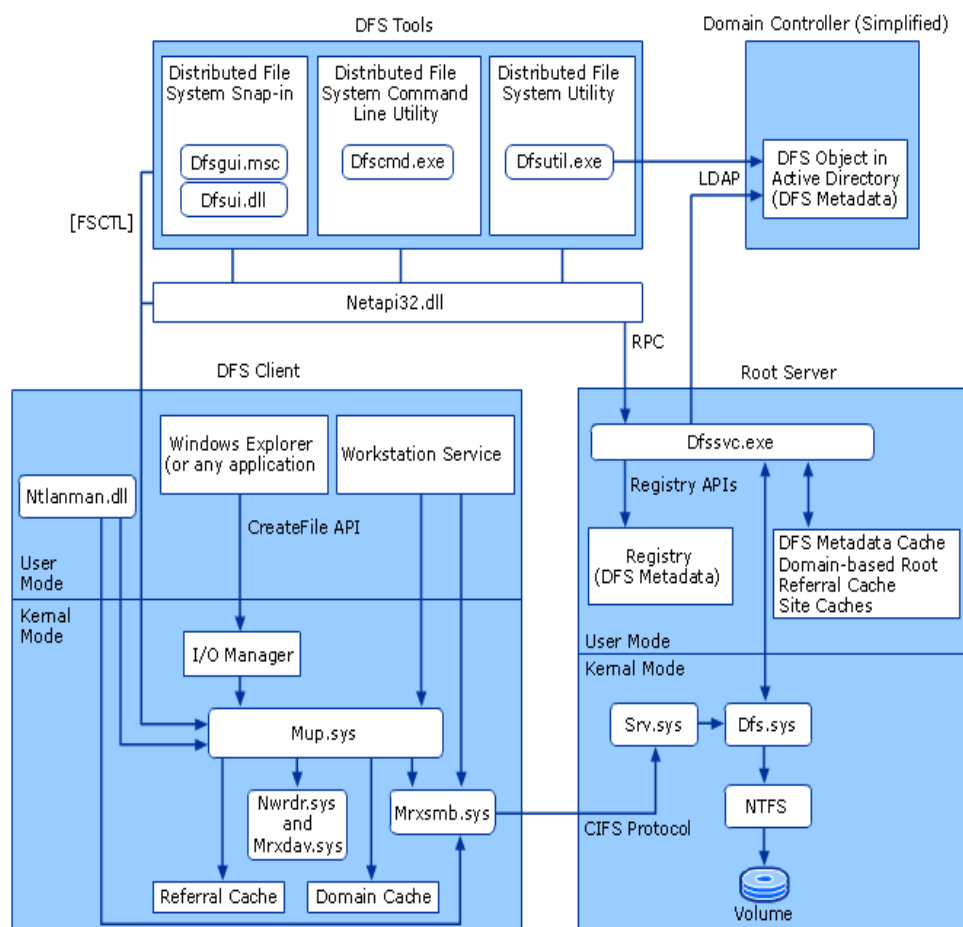
5 RYHMÄKÄYTÄNNÖT

Toimialueen ryhmäkäytännöissä otetaan käyttöön Central Store malli. Ryhmäkäytäntöjen pohjana olevat adm(x) tiedostot sijaitsevat keskitetysti aktiivihakemistossa eivätkä paikallisessa koneessa kuten oletuksena. Microsoft AD Policy templatet kopoidaan palvelimen `\\%systemroot%\PolicyDefinitions` kansioista saman toimialueen `\\”asiakas”.local\Policies` -kansioon juureen PolicyDefinitions nimiseen kansioon. Microsoft Office adm(x) tiedostot kopioidaan myös samaan hakemistoon (Microsoft 2016).

Default domain policyyn ja default domain controller policyyn ei tehdä muita asetuksia kuin salasana määritykset. Muut muutokset tehdään Custom Domain Settings- ja Custom Domain Controllers policyyn. Ryhmäkäytännöt ovat asiakaskohtaisia toteutuksia, tarvittavat määritykset pyritään tekemään mahdollisimman pitkälle Microsoftin parhaita käytäntöjä noudattaen ja asiakkaan tarpeet huomioon ottaen. Aktiivihakemiston hallinnassa pyritään automatisointiin mahdollisimman pitkälle. IDM tulee huolehtimaan käyttäjätunnusten luonnista, poistosta ja oikeuksista mahdollisimman paljon. Tietyt erityistapaukset joudutaan luomaan edelleen ilman automatiikkaa. Helpdeskillle otetaan käyttöön ManageEnginen ADManager tuote, jolla pystytään antamaan rajoitettuja oikeuksia haluttuihin AD -objekteihin. Myös asiakkaan itsepalvelua kehitetään IDM:n mahdollisuuksien pohjalta, eli salasanojen resetointi ja web-shop pohjaisia palveluja voidaan tuottaa IDM-palvelun ohella.

6 TIEDOSTO- JA LEVYPALVELUT

Tiedostopalvelut tuotetaan tiedostopalvelimelta ja sharepoint ympäristön työtiloista. Oikeuksien hallinta ja käytettävyys ovat asiakkaan näkökohdasta kriittisiä vaatimuksia. DFS-palvelulla voidaan toteuttaa SMB-jakojen näkyvyys asiakkaille läpinäkyvästi ja redundanttisesti. DFS-palvelun avulla asiakkaalle on mahdollista näyttää useampi levyjako saman hakemiston alle. Käytettävyyden kannalta helpointa on määrittellä levyjärjestelmästä asiakaskohtaisesti segmentoidut levyalueet tiedostopalvelimelle, josta ne jaetaan DFS:n avulla loppukäyttäjälle.



Kuva 3: Client/Server DFS-arkkitehtuuri (Microsoft 2013).

Kuvassa on esitetty Microsoftin DFS -toimintamalli ja komponentit Client/Server ympäristössä. Käyttäjälle toteutus näkyy CIFS jakona yhteisessä levypalvelussa. Käytännöllisintä on myös uudelleen nimetä näytettävät DSF-jaot uudelleen, jolloin ne vastaavat paremmin asiakkaan tarpeita.

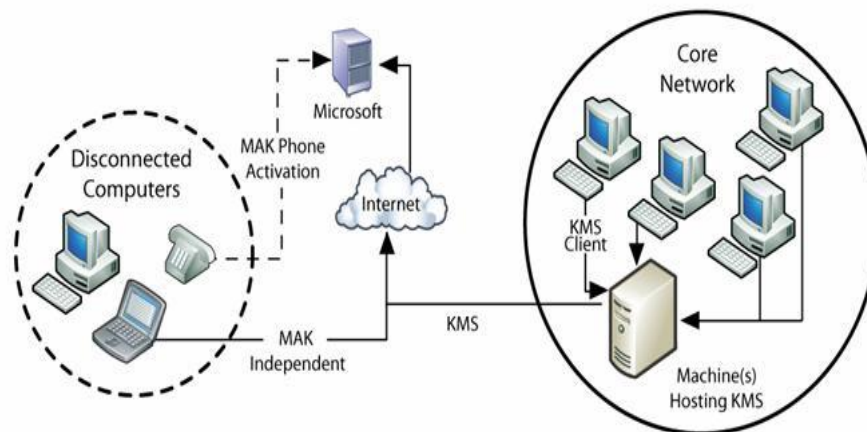
Tiedostopalvelujen toteutus sharepointin työtiloissa toteutetaan sharepointin omien suojausten avulla, joihin annetaan työtilakohtaiset oikeudet. Työtilojen omistajilla on oikeus määrittää kenelle tiedostojen käyttöoikeudet annetaan. AD-ryhmillä annetaan oikeudet ainoastaan sharepointin käyttöön. Sharepointin käytön etuna on mahdollisuus jakaa tiedostopalveluja myös ulkopuolisten henkilöiden käyttöön extranetin avulla, mitä ei voida tietoturvasyistä toteuttaa perinteisillä levypalveluilla. Lähinnä vastaava ominaisuus on käytössä O365 palveluun saatavana OneDrive for Business toiminnallisuudella.

Tiedostopalvelut on tarkoitus tuottaa yhteisenä palveluna. Tarkoitusta varten rakennetaan neljän palvelimen klusteri Calpron resurssi-AD:n alle ja otetaan käyttöön DFS-palvelu. Osa tiedostopalveluista on myös tarkoitus siirtää sharepoint alustalle, jolloin pystytään tarjoamaan myös ulkopuolisille mahdollisuus päästä käsittelemään extranetin kautta julkaistua aineistoa. Tiedostopalvelinta hyödynnetään myös SCCM-sovelluskirjaston kanssa. O365-pilvipalveluun siirtymisen ohella on tarkoitus ottaa käyttöön myös Microsoft OneDrive for Business palvelu ja mahdollisesti siirtää käyttäjien kotihakemistot pilvipalveluun. Tietoturvan takia on erittäin tärkeää huolehtia, että käyttäjillä on oikeudet tarvittaviin aineistoihin, ja on myös tiedettävä kuka tiedon omistaa ja kenelle siihen voidaan antaa oikeudet. Tiedostopalvelimella tämä on toteutettu AD-ryhmä ja käyttöjärjestelmä tason suojauksella. Käyttöjärjestelmä tasolla oletussuojauksena SYSTEM ja Administrators -ryhmille annetaan Full Control -oikeudet levyille, jolloin ne periytyvät hakemistopuussa alemmille tasoille. Share ja NTFS -oikeudet määritellään sovellus- ja käyttäjätarpeen mukaan (Microsoft 2013). AD -ryhmillä annetaan ylemmän tason oikeudet, jotka on vielä jaettu AD -tasolla globaaleihin ja palvelintasolla lokaaleihin ryhmiin.

IDM:n on tarkoitus huolehtia näiden oikeuksien jakamisesta käyttäjille tarkoitusta varten luodun hyväksymiskäytännön mukaan. IDM myös huolehtii oikeuksien poistosta tarvittaessa, ennalta määriteltyjen prosessien mukaan, jolloin käyttäjille ei jää tarpeettomia oikeuksia.

7 KÄYTTÄJÄTUNNUSPROSESSI JA VOLUMEACTIVATION/KMS -PALVELU

Käyttäjätunnusten muoto on asiakaskohtaisesti päätetty. Asiakkaan tietohallinto määrittelee käytettävät tunnusformaatit. Tunnusprosessi hoidetaan yhteisenä IDM-palveluna, johon saadaan toteutettua asiakaskohtaiset työkulut asiakkaan vaatimusten mukaan. Nimeämisessä pyritään käyttämään Englantia, jolloin ei tarvita ääkkösiä, mikä helpottaa tunnusprosessia. Myös UPN suffix formaatti on sovittu käytettäväksi samanlaisena kuin sähköpostiosoite, jolloin tunnusten synkronointi Azure aktiivihakemistoon on helpompaa. Nimeämiskäytännössä noudatetaan asiakkaan vaatimuksia, niin että käyttäjätunnusprosessissa noudatetut vaatimukset tulee huomioida. Suurimpana haasteena on huolehtia eri organisaatiosta migratoitavien tunnusten nimeämiskäytäntöjen tiedotuksesta asiakkaille ja mahdollisten duplikaattitunnusten uudelleen nimeämisen käytännöistä. Näiden käytäntöjen sopiminen tehdään yhteistyössä Calpron ja asiakkaan tietohallinnon ja HR-osaston kanssa. KMS-palvelu asennetaan omalle palvelimelle. KMS-palvelu kaikkia Calpron asiakkaiden koneita ja Microsoft-ohjelmistoja. Samaa palvelinta hyödynetään myös RDS licensing roolin kanssa.

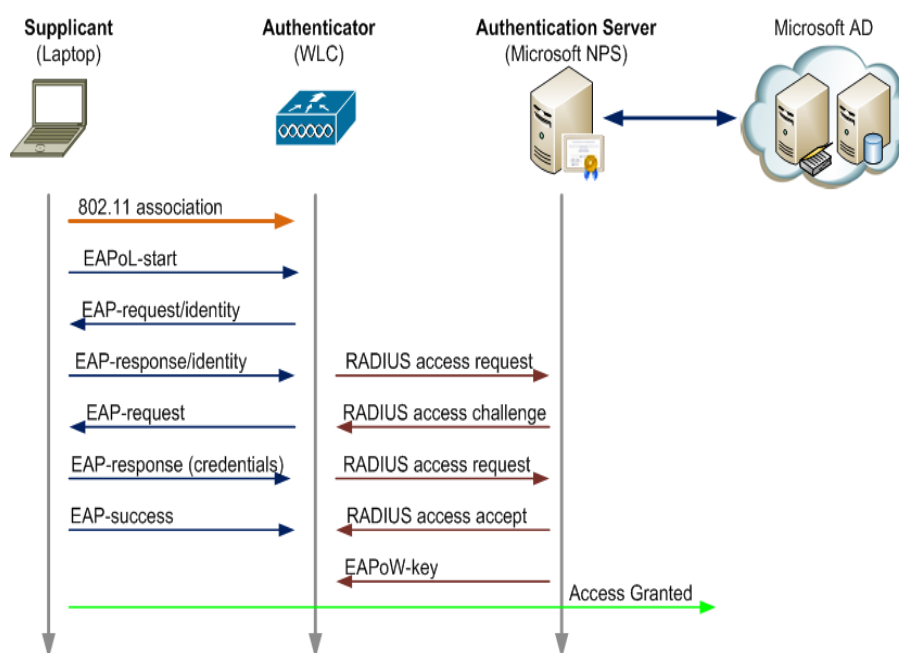


Kuva 4: KMS arkkitehtuurikuva (Microsoft 2016).

Kuvan 4. mukainen Microsoftin referenssi arkkitehtuuri on suoraan sovellettavissa Calpron ympäristöön. Keskitetyn KMS-palvelun vaatimuksena on myös käytössä oleva Microsoftin lisenssimalli, jolloin kaikki lisenssit ovat samalla sopimusnumerolla.

8 RADIUS JA AVAINTENHALLINTA

Radius palvelu on IEEE:n 802.1x standardin mukainen palvelu, jota tarjotaan LAN ja WLAN verkkoihin, estämään luvattoman laitteen kommunikointi usercore tai servicecore verkkoon. Kuvassa 5 on esitetty RADIUS 802.1x autentikointi proseduuri.



Kuva 5: Radius-autentikointi proseduuri (WifiNigel 2016).

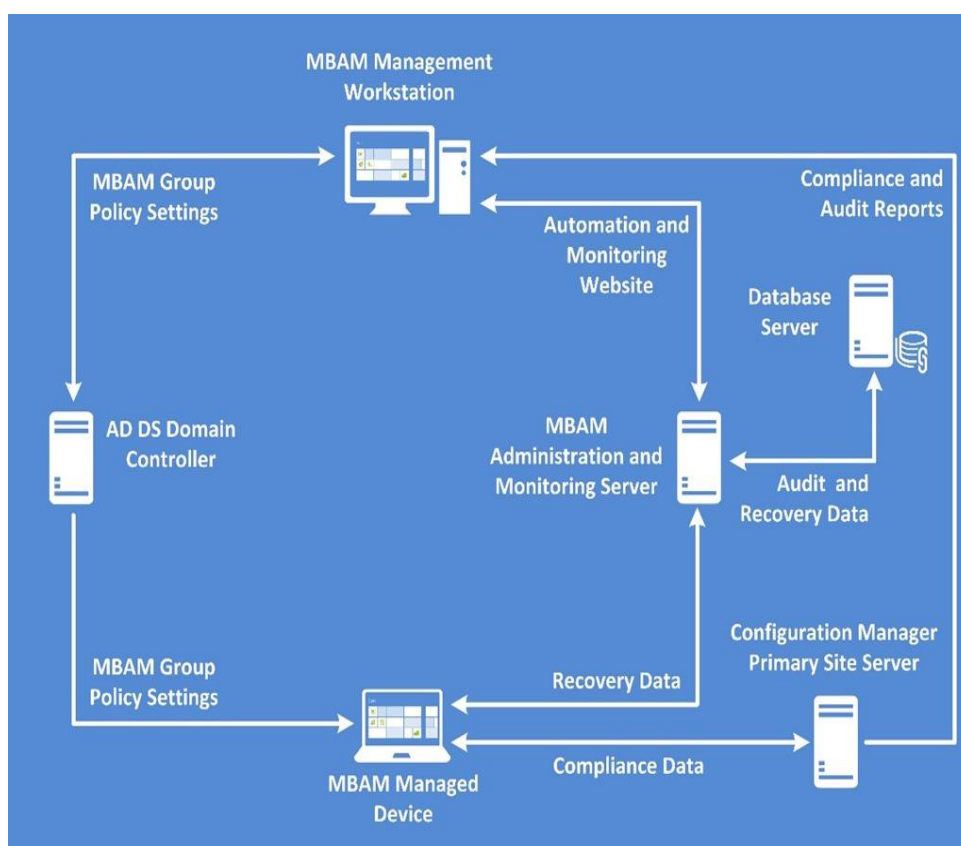
Tietoturvan kannalta radius palvelun käytöllä pystytään rajaamaan vain haluttujen työasemien pääsy usercore verkkoon. Muut työasemat, jotka eivät läpäise radius autentikointia pudotetaan automaattisesti vierailija vlaniin, josta on pääsy ainoastaan internetiin. Käytännöllisintä tämän kaltaisessa toteutuksessa on verkkoympäristö, missä on paljon sisään tulevia autentikointipyyntöjä ja ulkopuolisia käyttäjiä.

BOYD toiminnallisuutta ei toteuteta tässä tapuksessa, vain Calpron hankkimat ja hallitsevat laitteet päästetään läpi radius autentikoinnista usercore verkkoon. Radius palvelut tuotetaan yhteisenä palveluna, jota tarjotaan open-source pohjaisella sovelluksella. Tällä palvelulla tarjotaan WLAN/Wired 802.1x –autentikointi kaikille asiakkaille.

9 BITLOCKER-SALAUSPALVELU

Laitteet sisältävät tietoa, jonka päätyminen ulkopuoliselle on pyrittävä estämään parhaalla mahdollisella tavalla. Erityisesti laitteiden katoamis- tai varkaustapauksissa on kiintolevyn sisältämä tieto salattava, jolloin sen lukeminen on huomattavasti hankalampaa.

Kannettavien ja työasemien kohdalla kustannustehokkain ratkaisu on Microsoftin Bitlocker ominaisuuden käyttö. Tämä kuuluu Microsoftin lisenssimalliin, eikä tuo ylimääräisiä kustannuksia. Bitlocker on Microsoftin salausohjelma, jolla on mahdollista salata kiintolevyn tai ulkoisen muistilaitteen tiedot. Tämä tuotetaan asiakkaille keskitettynä palveluna, jolloin MDOP-palvelin asennetaan ja keskitetty salausavainten hallinta on mahdollista. Tavoitteena on kaikkien työasemien levysalauksen käyttöönotto, johon päästään, kun kaikki työasemat tulevat sisältämään TPM piirin.

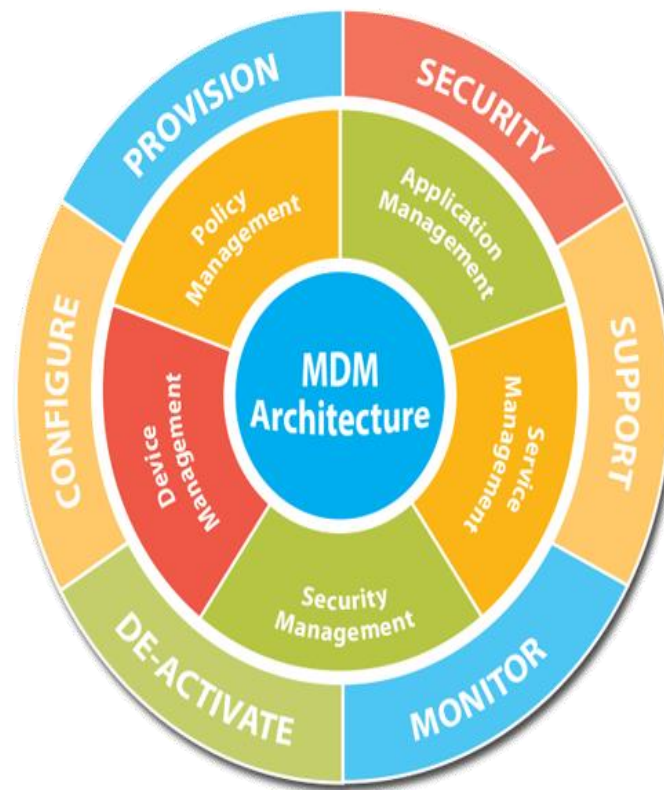


Kuva 6: Bitlocker MDOP arkkitehtuurikuva (Microsoft 2016).

Microsoftin suosituksen mukainen kuvassa 6 esitetty referenssi arkkitehtuuri voidaan toteuttaa yhteisenä palveluna, jolloin helpdesk pystyy huolehtimaan keskitetysti asiakkaiden salausavaintenhallinnasta. Bitlockerin keskitetyn hallinan avulla on mahdollista vaihtaa asiakkaan levysalauksen avain, joka muussa tapauksessa on käyttäjän itse huolehdittava.

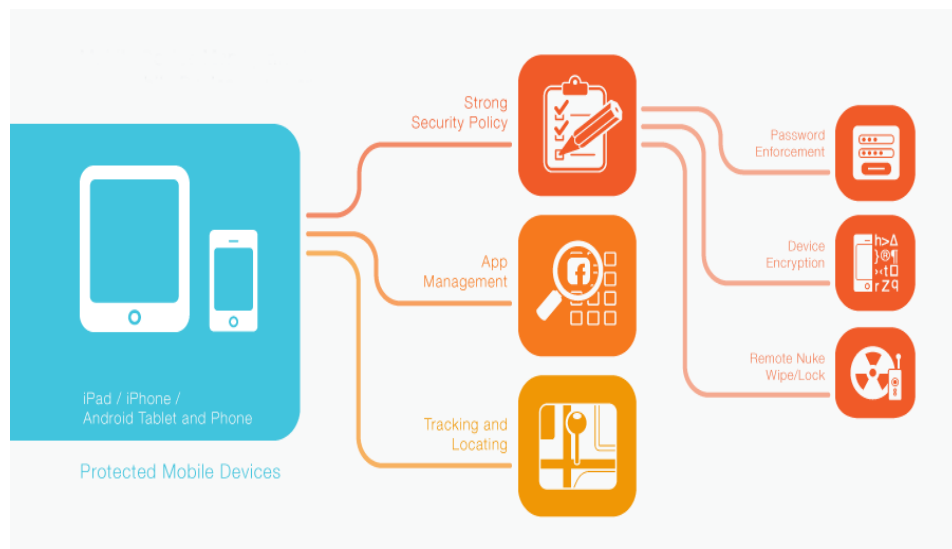
10 MOBIILILAITTEHALLINTA (MDM)

MDM, eli Mobile Device Management tarjoaa mobiililaitteille laajemmat tietoturva- ja hallintaominaisuudet kuin bitlocker tai sccm.



Kuva 7: MDM palveluarkkitehtuuri (Mobilemacsters 2017).

Mobiililaitteiden hallinnan tarpeen osuus tulee tulevaisuudessa kasvamaan, jolloin näiden laitteiden tietoturvaan, hallintaan ja käytettävyyteen on kiinnitettävä erityistä huomiota. Kokonaisarkkitehtuurikuvasta (Kuva 7) on pilottivaiheessa olevien ohjelmistojen testauksessa keskitytty laitehallinnasta security ja service management osioihin (Kuva 8). Käytettävyyden kannalta asiakkaiden laitteiden konfigurointi keskitetysti pienentää helpdeskin työmäärää ja tietoturvaosio mahdollistaa laitteiden tyhjennyksen etänä, jolloin katoamis- ja varkaustapauksissa luottamuksellisen tiedon päätyminen väärin käsiin pienenee.

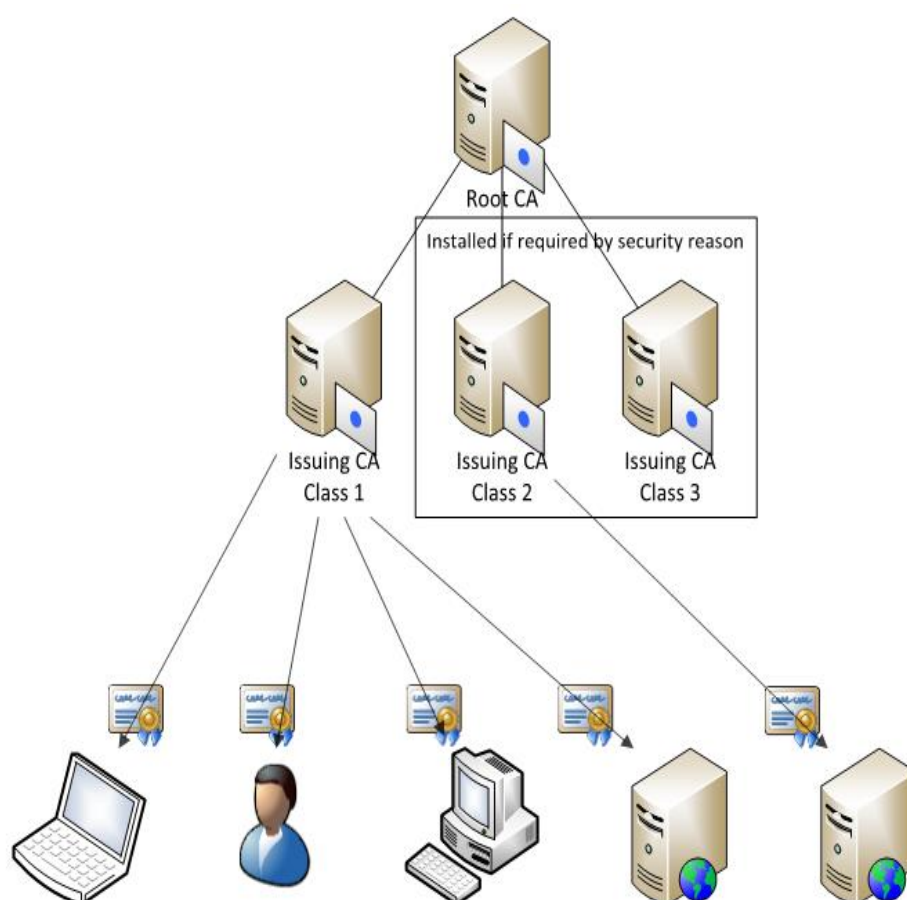


Kuva 8: MDM ominaisuudet (Mobilemacsters 2017).

Kehityskohteena on myös mobiiliapplikaatioiden kehittyessä erilaiset sovelluskohtaiset vpn-tunneloinnit taustajärjestelmiin. Mobiililaitteiden konfigurointi keskitetysti pienentää merkittävästi servicedeskin työmäärää ja kustannuksia. Suurimpina säästökohteina on mobiililaitteiden automaattinen sähköpostitilien konfigurointi, verkkolevyjen ja sharepoint sisällön pääsynhallinta. Tavoitteena on kokonaispalveluna tuotettu MDM-järjestelmä, jolla pystytään hallitsemaan kaikki Calpron ylläpidossa olevat mobiililaitteet.

11 PUBLIC KEY INFRASTRUCTURE (PKI)

PKI eli julkisten avainten hallintajärjestelmä, jolla saadaan tietoturvajärjestelmiin varmentajan (CA, Certificate authority) ja varmenteen (Certificate) avulla varmistettua käytettävän avaimen tekninen oikeellisuus ja allekirjoittavan osapuolen luotettavuuden perusteella varmistettua avaimen tunnistetiedot. Yleisimmin käytetyistä tietoturvajärjestelmistä SSL/TLS salaukset ja S/MIME käyttävät X.509 standardiin perustuvia varmenteita. Tavoitteena on käyttää tunnettujen valmistajien varmennepalveluja ja Calpron tapauksessa tähän on valittu Entrust ja Väestörekisterikeskus.



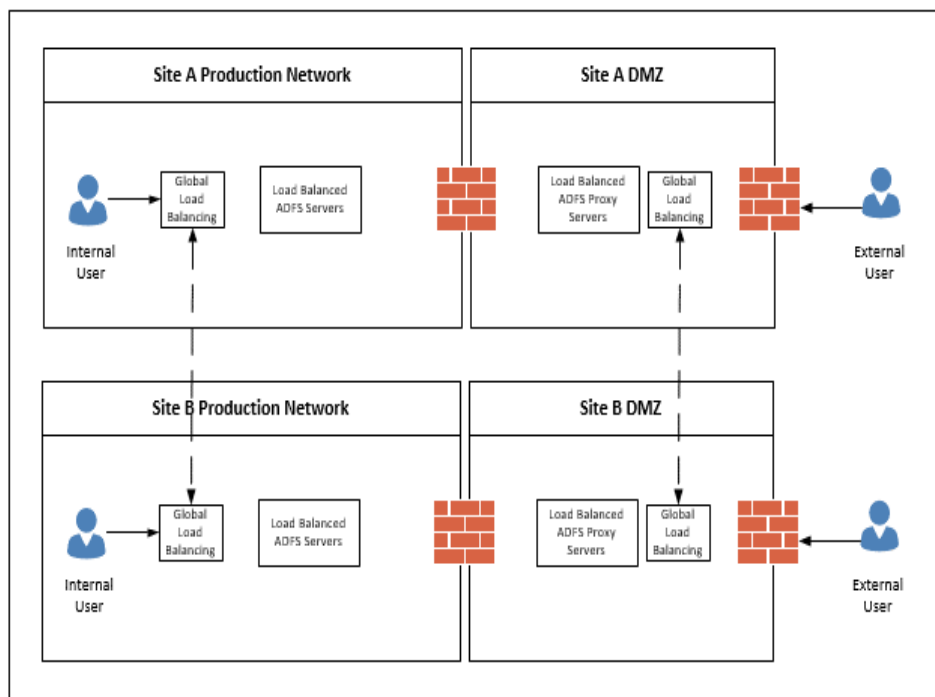
Kuva 9: PKI-arkkitehtuurikuva (Microsoft 2016).

Kuvan 9. mukainen toteutus tehdään modulaarisena toteutuksena. Issuing palvelin tuotetaan yhteisenä palveluna kaikille asiakkaille. Useamman CA palvelimen käyttö ei ole tarpeellista.

12 AKTIIVIHAKEMISTON FEDERAATIOPALVELUT

Adfs -palvelulla tuotetaan identiteetin federointi organisaation ulkopuolisiin palveluihin. Samalla saadaan varmistettua käyttäjän identiteetti ja oikeus käyttää palveluja palvelun tuottajan puolelta. Suurin palvelu, johon federaatiota käytetään on Microsoftin O365. Myös muiden saas -palvelujen käytön tietoturvan ja käyttökokemuksen kannalta on palvelun tuki adfs:lle. Käyttäjän kannalta parhaan käyttökokemuksen tarjoaa adfs:n kautta tapahtuva kertakirjautuminen, jolloin perinteisiä sovelluskohtaisia tunnus/salasana yhdistelmiä ei tarvita. Palvelu voidaan tuottaa keskiteytysti, mikäli asiakkaalla ei ole erityisvaatimuksia, missä tapauksessa on tarpeellista tehdä asiakaskohtainen ADFS-ympäristö.

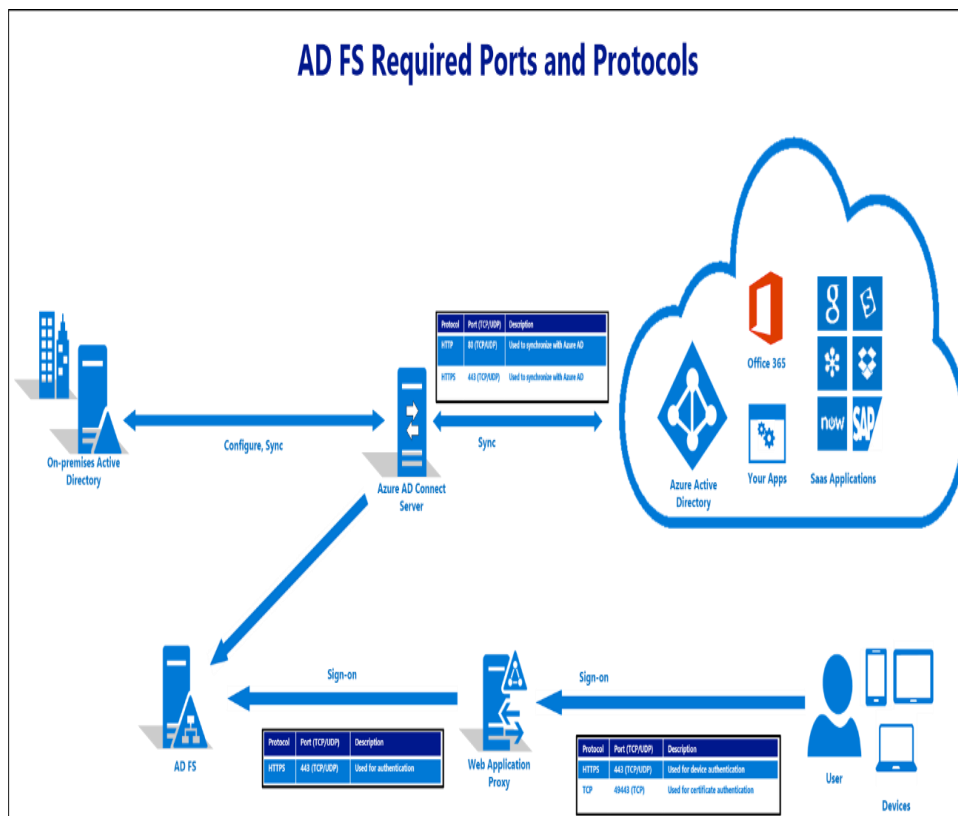
Palvelun toteutuksen ja kriittisyyden kannalta on klusteroitu ratkaisu perusteltua, jolloin servicecoreen sijoitetaan kahdennettu ADFS-palvelin ratkaisu ja DMZ-verkkoon kahdennettu ADFS-Proxy ratkaisu. Ulkopuolinen liikenne ohjataan proxy -palvelimille, joista kyselyt edelleen Servicecoren palvelimille. Molemmissa tapauksissa kuormantasaajan käyttö liikenteen ohjaukseen on tarpeellista. Calpron toteutuksena tähän käytetään F5 Big-IP ratkaisua, jonka avulla saadaan sisä- ja ulkoverkon kuormantasaus toteutettua tietoturvallisesti.



Kuva 10: ADFS-palvelun sijoittaminen sisäiseen verkkoon (Microsoft 2016).

ADFS -palvelimet sijoitetaan kuvan 10. mukaisesti. ADFS-serverit kahdennettuna Servicecore-verkkoon ja ADFS Proxy -serverit DMZ-verkkoon. Yhteydet näiden välille rajataan palomuuressa ip ja porttikohtaisilla avauksilla kuvan 11. mukaisesti.

Pilvipalveluiden käytön lisääntyessä federaatiopalvelujen käyttö kasvaa ja esimerkkinä näistä on tähän työhön valittu O365 palvelu, joka toteutetaan E3 lisenssi mallilla. Arkkitehtuurina käytetään kuvan 11 mukaista Microsoftin referenssitoteutusta.

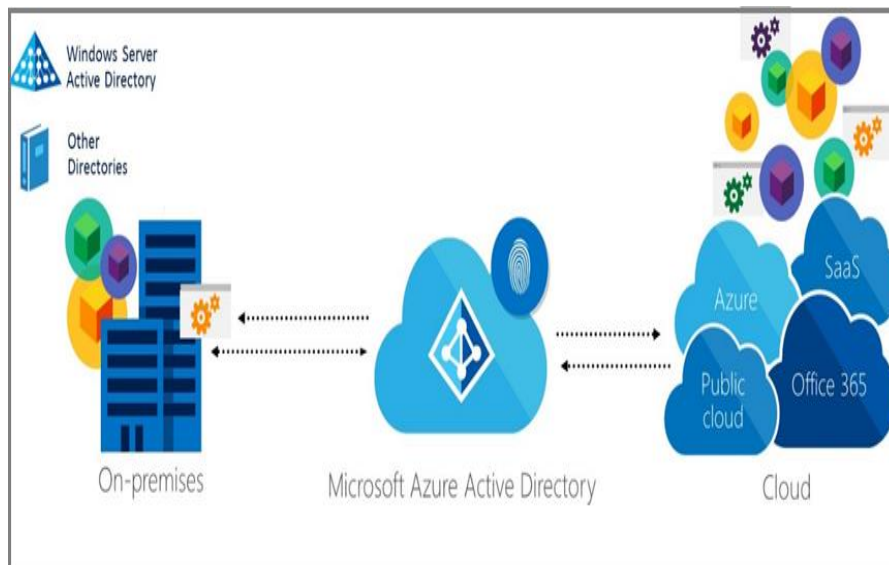


Kuva 11: ADFS O365 arkkitehtuurikuva (Microsoft 2016).

Asiakkaalle O365-palveluun siirtyvät sähköposti, pikaviestintäpalvelut ja Microsoft Office -tuoteperheen ohjelmat. Federaatiopalveluiden avulla nämä toimivat kertakirjautumisella selaimella käytettäessä. Tavoitetilana on saada mahdollisimman moni palveluista ADFS pääsynhallinnan piiriin. Tämä on otettava huomioon myös uusien palveluiden vaatimusmäärittelyissä, erityisesti pilvipalveluina tarjottavien saas palveluiden osalta.

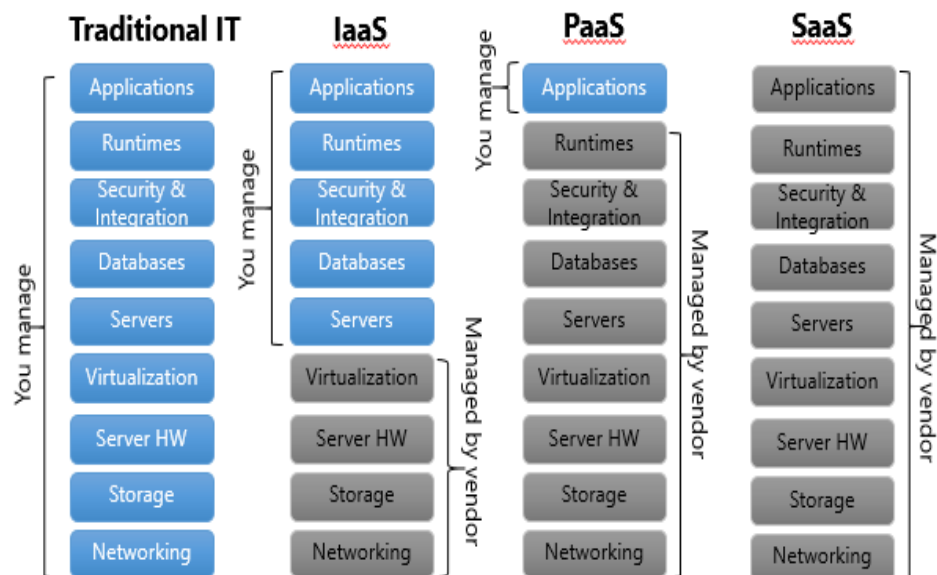
13 PILVIPALVELUNA MICROSOFT AZURE

Azure on Microsoftin tapa tuottaa ICT-palveluja ja kehittää liiketoimintaratkaisuja asiakkaiden tarpeisiin. Näitä voidaan toteuttaa Azuren avulla, joko puhtaasti pilvipalveluna tai hybridimallina, jossa olemassa olevaa infrastruktuuria laajennetaan pilvipalveluun.



Kuva 12: Microsoft Azure (Microsoft 2016).

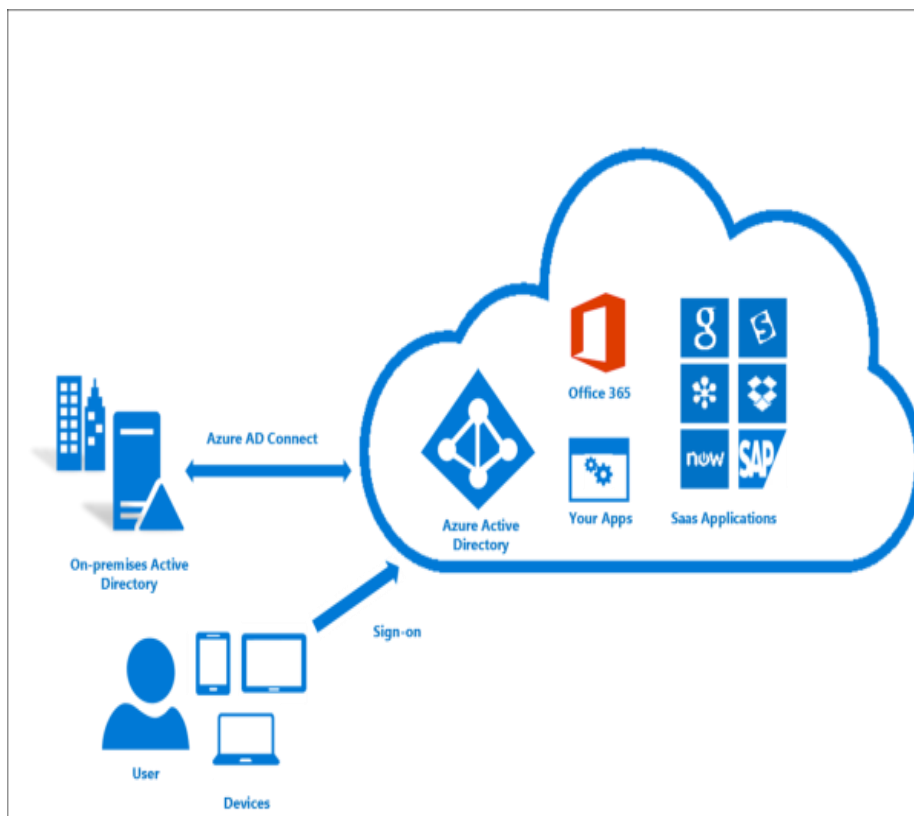
Kuvan 12. mukainen hybriditoteutus on tarkoitus toteuttaa kaikille Calpron asiakkaille. Ensimmäisenä palveluna Microsoftin pilvipalveluista otetaan käyttöön Office 365, jonka yhteydessä asiakaskohtaiset on-premises Exchange ja Skype -palvelut siirretään pilvipalveluiksi. Tähän on valittu Microsoftin lisenssimalleista E3, joka katsottiin kustannuksiltaan riittäväksi vastaamaan palvelutarvetta.



Kuva 13: Pilvipalvelumallit (Mazikglobal 2017).

Kuvasta 13. Pilvipalvelumallien vertailuna voidaan todeta siirtymä perinteisestä palvelinkeskusmallista pilvipalveluihin. Oikealle siirryttäessä ylläpidon siirtyminen kasvavassa määrin palveluntarjoajalle. Calpron pilvipalvelustrategiana on, että käyttämällä erilaisia SaaS palveluja, joiden käyttö toteutetaan asiakaskohtaisten tarpeiden mukaan ja näin saavutetaan tällä hetkellä paras ja kustannustehokkain pilvipalvelumalli. Palvelukustannukset, käytettävyys- ja laajennustarpeet määrittelevät sen otetaanko palvelu pilvipalveluna, paikallisena palveluna vai mahdollisesti hybridipalveluna. PaaS tai IaaS palvelujen käyttöön ei ole vielä tässä vaiheessa tarvetta siirtä. Tulevaisuudessa näiden käyttö on myös mahdollista.

Azure AD -connect palvelulla integroidaan paikalliset AD -identiteetit Microsoftin Azure AD:hen. Tällä saavutetaan yhteinen identiteetti käyttäjille paikallisessa AD:ssä ja Microsoftin Azure palveluissa. Käyttäjätunnusten hallinta ja oikeudet pysyvät IDM:n hallinnassa, joka toimii koko AD-tunnusten master datana. Tunnusten luonnit ja poistot tapahtuvat IDM:n kautta paikalliseen AD:hen, josta ne synkronoidaan Azureen AD-connect palvelimen kautta. Kokonaisuutena palvelu tuotetaan keskitettynä palveluna kaikille asiakkaille, Microsoftin tukiessa useamman AD:n synkronointia yhteen tenanttiin. Palvelun kriittisyyden kannalta tämä toteutetaan klusteroituna palveluna.



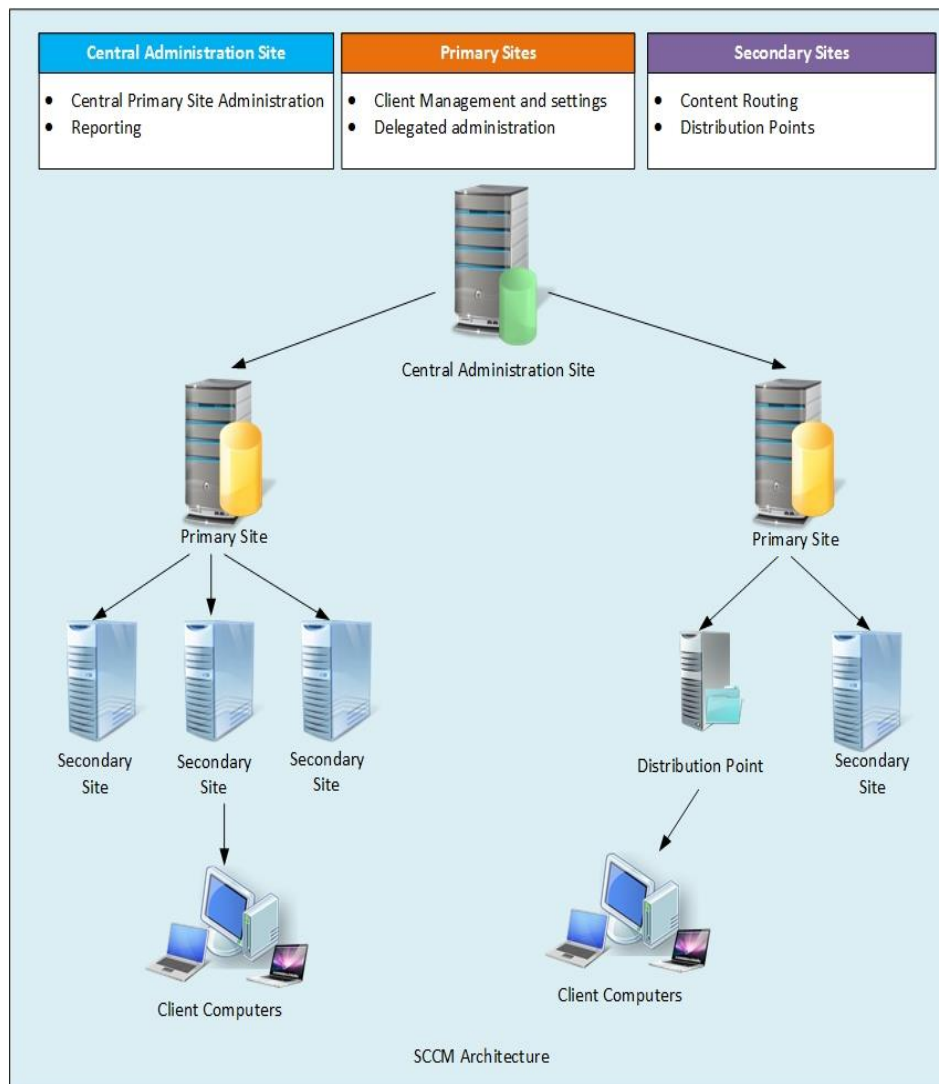
Kuva 14: Azure AD-connect palvelu arkkitehtuurikuva (Microsoft 2016).

Kuvan 14. mukainen käyttäjätietojen synkronointipalvelu on edellytys O365 migraatiolle ja muiden Azure pohjeisten SaaS palvelujen käyttöön- otolle.

14 TIETOKONEIDEN HALLINTAAN SYSTEM CENTER CONFIGURATION MANAGER

System Center Configuration Manager on Windows pohjaisten tietokoneiden hallintajärjestelmä, joka sisältää työasemien etähallinnan, Windows päivityksienhallinnan, keskitetyn ohjelmistojakelun, käyttöjärjestelmä jakelun, sekä laitteisto- ja ohjelmistoinventaarion. SCCM inventaario tiedot linkitetään Calpron ERP -järjestelmään asset management moduuliin.

Kokonaisarkkitehtuuri kuvana käytetään kuvassa 15. näkyvää Microsoftin referenssi arkkitehtuuria, jossa yhteisenä palveluna toteutetaan Central administration Site-server. Distribution pointtien määrän ja sijoittelun ratkaisevat asiakkaan verkkoinfrastruktuuri ja työasemien määrä. Sijoituspaikkoina käytetään myös asennustiloja, joiden pääasiallisena käyttönä pidetään image -asennusta. Image asennuksen kannalta tätä ei voida suurissa määrissä toteuttaa usercore verkon yli verkkoinfrastruktuurista ja sen kriittisyydestä johtuen. Management pointit asennetaan DMZ -verkkoon, jolloin päivitysten jakaminen myös tähän verkkoon ja usercore verkon ulkopuolisiin koneisiin saadaan toteutettua keskitetysti.

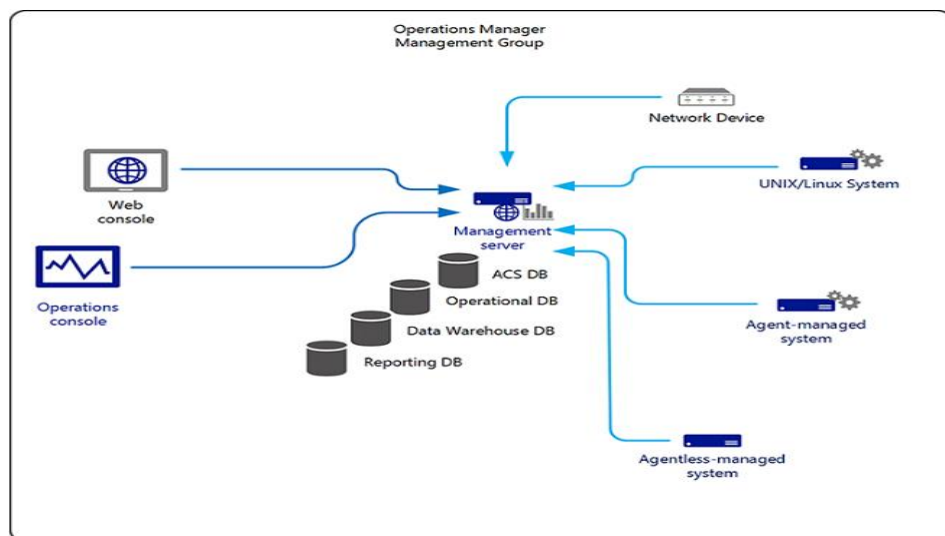


Kuva 15: SCCM Arkkitehtuurikuva (Microsoft 2016).

Oikeudet SCCM palvelun käyttöön toteutetaan AD-ryhmillä, tämä on keskitettyyn toteutukseen mahdollista toteuttaa AD-federaation avulla. Haasteina SCCM työasemaimage jakelussa on radius autentikointi. Käytännön kannalta tämän helpottamiseksi on asennustilat rajattu radius palvelun ulkopuolelle. Pääsy noihin tiloihin on rajoitettu henkilöstön osalta kulkuoikeuksilla ja ulkopuolisten henkilöiden pääsy näihin on myös hyvin rajoitettua.

15 ICT-YMPÄRISTÖN VALVONTAAN SYSTEM CENTER OPERATIONS MANAGER

Microsoft SCOM on ICT-ympäristön valvontaan tarkoitettu SC-tuoteperheen tuote. Valvonnan tarve on lisääntynyt asiakkaiden käytettävyyssvaatimusten mukaan ja nämä on kirjattu SLA-sopimukseen. Ylläpidon valvontasovelluksen tehokkuus ja monipuolisuus ovat ensisijaisen tärkeää SLA-vaatimusten täyttämisen kannalta. Raportointi asiakasympäristön tilasta on proaktiivisen kapasiteettitarpeen seurannan takia myös olennaista.



Kuva 16: SCOM Arkkitehtuurikuva (Microsoft 2016).

Kuvan 16. mukaista referenssiarkkitehtuuria käytetään järjestelmä- ja verkonvalvontaan. Laajenuksena tähän tulee myöhemmässä vaiheessa olevien Azure palvelujen käyttöönotto, johon SCOM tarjoaa valmiin ratkaisumallin. Tämä tuotetaan kaikille asiakkaille yhteisenä palveluna, joka voidaan järjestelmän sisällä segmentoida asiakaskohtaiseksi ja antaa asiakkaalle tietyt näkymät ja raportit, jolloin tarjottavien palvelujen seuranta helpottuu. SCOM on helposti laajennettavissa monitoroimaan käytössä olevia laitteita ja palveluja, sillä monet toimittajat tuottavat SCOM:ia varten omat management packit, jotka ovat valmiiksi tehtyjä templateja valvontaa varten.

16 PALVELUIDEN MODULAARISET TOTEUTUKSET

Palveluiden modulaariset toteutukset voidaan jakaa kahteen ryhmään asiakaskohtaiset toteutukset ja yhteisten palveluiden asiakaskohtaiset segmentoinnit. Osa yhteisistä palveluista voidaan toteuttaa ilman segmentointia. Segmentoitujen toteutusten osalta pyritään asennusten automatisointiin mahdollisimman suuressa määrin. Asiakaskohtaisten vaatimusten konfigurointi varsinkin AD-palvelujen osalta on edelleen manuaalista työtä, eikä näiden automatisointi olisi kustannustehokasta, vaikka osa taustajärjestelmien tarjoamista työkaluohjelmista antaisi tähän osittaisen mahdollisuuden.

Taulukko 2. Kooste modulaarisista toteutusmalleista.

MODULAARISET TOTEUTUKSET			
PALVELU	ASIAKASKOHTAINEN TOTEUTUS	SEGMENTOITU TOTEUTUS	YHTEINEN PALVELU
AD	X		
DNS	X		X
DHCP	X		X
DFS		X	
IDM			X
KMS			X
RADIUS	X		X
BITLOCKER			X
MDM		X	X
PKI			X
ADFS	X	X	X
AZURE	X		X
AZURE AD-CONNECT	X		X
SCCM		X	X
SCOM		X	X

Taulukossa 2 on koostettu yhteenveto mahdollisista toteutusmalleista. Osa toteutuksista sisältää vaihtoehtoisia toteutustapoja, jotka ovat asiakkaan vaatimuksesta mahdollisia. Suosituksena on kuitenkin käyttää mahdollisimman paljon yhteisiä palveluja tai niiden segmentoituja toteutuksia. Dedikoitu asiakaskohtainen toteutus on aina kallein vaihtoehto ja työmäärältään suurin ylläpidettävä.

17 YHTEENVETO JA POHDINTA

Opinnäytetyössä esitetyjä asioita on käytetty pohjana uuden AD-ympäristön ja siihen liittyvien palvelujen suunnittelussa ja projekti aikaisen toteutuksen mallina. Työssä oli keskitytty palvelujen modulaaristen toteutusten suunnitteluun, jolloin nykyinen asiakasympäristö saadaan korvattua hybridimallilla, jossa yhteisten modulaaristen palvelujen käyttöönotto toteutuu kustannustehokkaasti ja tietoturvallisesti. Erityistä huomiota kiinnitettiin myös alustapalvelujen laajennettavuuteen ja käyttöönoton helppouteen.

Yhtenä suunnittelun lähtökohtana oli sote- ja maakuntauudistus. Tarkoituksena on saada AD infrastruktuuri kestäväälle pohjalle vuoden 2018 loppuun mennessä, jotta tarvittavien muutosten suunnittelu ja toteutus olisi helpompaa ja aikataulullisesti mahdollista. Tietoturvan kannalta tärkeimpänä asiana työssä oli otettu huomioon EU tietoturva-asetus GDPR. Palvelujen tietoturvaa parannettiin keskittymällä moniasiakasympäristön vaatimuksiin, erityisesti verkko- ja palvelininfrastruktuurin segmentoinnin osalta. Työssä haasteena oli myös työn julkisuus. Tietoliikenteen ja palvelininfrastruktuurin osalta pitäydyttiin pelkästään kokonaisarkkitehtuurin osalla, sillä paljon asioita kuuluu luottamuksellisen tai salassapidettävän tiedon piiriin. Tarkemmat tekniset dokumentaatiot jäävät vain Calpron käyttöön.

Calpron AD-projekti on tällä hetkellä toteutusvaiheessa. Opinnäytetyötä on käytetty pohjana kokonaisarkkitehtuurisuunnittelussa, josta saatiin perusteet suunnitteluun, resurssointiin, toteutusmalleihin ja kustannuslaskentaan. Osana projektia on myös siirtyminen uuteen ympäristöön, jonka testausvaihe on myös juuri alkamassa. Siirtymistä uuteen ympäristöön hankaloittaa myös suuri asiakas- ja työasema määrä, jonka vuoksi resurssointi ja dokumentointi tulevat nousemaan tarkeään osaan. Palvelutuotannon keskeytymätön toiminta ja toimintakatkosten minimointi tämän muutosprojektin osalta on resursoinnin kannalta suurin haaste, koska sairaalaympäristö vaatii järjestelmien katkeamatonta toimintaa.

Opinnäytetyön tuloksena saatiin muodostettua helposti laajennettava ja kustannustehokas modulaarinen malli, jossa on eriteltyä eri AD:hen liittyvät palvelukomponentit. Tätä mallia voidaan käytännössä soveltaa eri asiakasympäristöjen rakentamiseen asiakkaan ICT-ympäristölle asetettujen vaatimusten mukaan ja eri komponentteja ottaa käyttöön tarpeen mukaan.

LÄHTEET

Centero (2017). PKI yleisesti blogi julkaisu. Haettu 10.5.2017 osoitteesta <http://www.centero.fi/blogi/pki-for-dummies/>

Jackson, S. (2015). Active Directory Federation Service (ADFS) Design Considerations and Deployment Options blogi julkaisu. Haettu 20.3.2017 osoitteesta <https://shanejacksonitpro.wordpress.com/2015/08/31/active-directory-federation-service-adfs-design-considerations-and-deployment-options/comment-page-1/>

Mazikglobal (2017). What is Cloud Computing Stack (SaaS, PaaS, IaaS).

Haettu 10.5.2017 osoitteesta <http://www.mazikglobal.com/blog/cloud-computing-stack-saas-paas-iaas/>

Microsoft (2016) Active Directory: Best Practices for Internal Domain and Network Names. Haettu 15.2.2017 osoitteesta <https://social.technet.microsoft.com/wiki/contents/articles/34981.active-directory-best-practices-for-internal-domain-and-network-names.aspx>

Microsoft (2016). AD DS Design Guide. Haettu 15.2.2017 osoitteesta [https://technet.microsoft.com/en-us/library/cc754678\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc754678(v=ws.10).aspx)

Microsoft (2017). Azure Active Directory Documentation. Haettu 5.3.2017 osoitteesta <https://docs.microsoft.com/en-us/azure/active-directory/>

Microsoft (2017). Azure Active Directory Hybrid Identity Design Considerations. Haettu 4.4.2017 osoitteesta <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-hybrid-identity-design-considerations-overview>

Microsoft (2017). Best practices for securing Active Directory Federation services. Haettu 22.4.2017 osoitteesta <https://technet.microsoft.com/en->

us/windows-server-docs/identity/ad-fs/deployment/best-practices-securing-ad-fs

Microsoft (2016). BitLocker Drive Encryption Overview. Haettu 1.5.2017 osoitteesta [https://technet.microsoft.com/en-us/library/cc732774\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx)

Microsoft (2016). Capacity Planning for Active Directory Domain Services. Haettu 15.2.2017 osoitteesta <https://social.technet.microsoft.com/wiki/contents/articles/14355.capacity-planning-for-active-directory-domain-services.aspx>

Microsoft (2017). How DFS Works. Haettu 22.3.2017 osoitteesta [https://technet.microsoft.com/en-us/library/cc782417\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc782417(v=ws.10).aspx)

Microsoft (2017). Integrate your on-premises directories with Azure Active Directory. Haettu 25.4.2017 osoitteesta <https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect>

Microsoft (2017). Microsoft BitLocker Administration and Monitoring. Haettu 15.5.2017 osoitteesta <https://technet.microsoft.com/en-us/windows/hh826072.aspx>

Microsoft (2016). Planning a Management Group Design. Haettu 4.4.2017 osoitteesta <https://docs.microsoft.com/en-us/system-center/scom/plan-mgmt-group-design>

Microsoft (2017). Understanding KMS. Haettu 2.5.2017 osoitteesta <https://technet.microsoft.com/en-us/library/ff793434.aspx>

Microsoft (2017). Volume Activation in Disconnected Environments.

Haettu 2.5.2017 osoitteesta <https://technet.microsoft.com/en-us/library/dd981010.aspx>

Mobilemacsters (2017). MDM. Haettu 10.5.2017 osoitteesta <http://mobilemacsters.com/mdm/>

Shintaku, K. (2013). Bitlocker Administration & Management 2.0 blogi julkaisu. Haettu 1.5.2017 osoitteesta <https://kurtsh.com/2013/04/10/release-bitlocker-administration-management-2-0-mbam2/>

Terminalworks (2015). SCCM 2012 R2 Installing and Configuring blogi julkaisu. Haettu 4.4.2017 osoitteesta <http://www.terminalworks.com/blog/post/2015/10/03/sccm-2012-r2-installing-and-configuring-part-01-overview>

WifiNigel (2014). Microsoft NPS as a RADIUS Server for Wi-Fi Networks: SSID Filtering. Haettu 22.4.2017 osoitteesta <http://wifinigel.blogspot.fi/2014/03/>

Modulaarinen palvelutarjoama

