Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2025

Lumi Kosonen

Active Directoryn alas ajaminen

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2025 | 31 sivua

Lumi Kosonen

Active Directoryn alas ajaminen

Microsoft Active Directory on jo vuosia toiminut keskeisenä järjestelmänä käyttäjätunnusten ja laitteiden hallinnassa. Nykyään pilvipalveluiden tarjoamat edut ovat korostuneet entisestään. Pilvipohjaiset ratkaisut mahdollistavat resurssien hallinnan entistä tehokkaammin ja joustavammin.

Tämä opinnäytetyö toteutettiin merenkulkualan yrityksessä osana organisaation IT-järjestelmien kehittämistä. Tavoitteena oli päivittää kaikkien työntekijöiden ja alusten tietokoneet sekä siirtää käyttäjätunnukset Microsoft Active Directorysta pilvipohjaiseen Microsoft Entra ID -palveluun. Päivityksen tarkoituksena oli yksinkertaistaa laite- ja tunnushallintaa sekä parantaa etätyöskentelyn sujuvuutta ja tietoturvaa.

Työ eteni projektiluonteisesti useassa vaiheessa, joista osa toteutettiin rinnakkain. Tietokoneet päivitettiin sitä mukaa, kun ne saatiin käyttöön. Jokaiselle laitteelle asennettiin Windows 11 -käyttöjärjestelmä, ja varmistettiin, että keskusmuistia oli vähintään 16 gigatavua.

Projektin tuloksena organisaation IT-infrastruktuuri on teknisesti valmis pilvisiirtymää varten, ja siirtymän kannalta keskeiset toimenpiteet ovat hyvässä vauhdissa. Työ jatkuu suunnitelman mukaisesti kohti täyttä pilvipohjaista hallintamallia, jonka odotetaan tuovan merkittäviä parannuksia tietoturvaan, hallittavuuteen ja etätyöskentelyn toimivuuteen.

Asiasanat:

Active Directory, Entra ID, Okta, laitehallinta, pilvipalvelut

Bachelor’s | Abstract

Turku University of Applied Sciences

Information and communication technologies

2025 | 31 pages

Lumi Kosonen

Active directory termination

Microsoft Active Directory has for many years been a key system for managing user IDs and devices. Today, the benefits of cloud computing have become even more pronounced. Cloud-based solutions enable more efficient and flexible resource management.

This thesis was carried out in a maritime company as part of the development of the organisation's IT systems. The objective was to upgrade the computers of all employees and vessels and to migrate user IDs from Microsoft Active Directory to the cloud-based Microsoft Entra ID service. The purpose of the upgrade was to simplify device and password management and to improve remote working and security.

The project was carried out in several phases, some of which were implemented in parallel. The computers were upgraded as they became available. Windows 11 was installed on each machine, and it was ensured that the machines had at least 16 GB of RAM.

As a result of the project, the organisation's IT infrastructure is technically ready for the cloud migration, and key migration activities are well underway. Work continues as planned towards a full cloud-based management model, which is expected to bring significant improvements in security, manageability, and remote working functionality.

Keywords:

Active Directory, Entra ID, Okta, Device management, Cloud services

Sisältö

Kuvat

Käytetyt lyhenteet ja sanasto

AD DS	Active Directory Domain Services. AD:n osa, joka, hallitsee verkkotunnuksia ja käyttäjätilejä.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuntaa verkkotunnukset IP-osoitteiksi.
Global Catalog	Active Directory -palvelimen rooli, joka mahdollistaa käyttäjätietojen nopean haun koko metsästä.
Group Policy	Windows-ympäristössä käytettävä hallintatyökalu, jolla voi määrittää asetuksia keskitetysti.
IAM	Identity and Access Management. Identiteetin ja pääsynhallinta on prosessien, datan ja teknologian yhteensovittamista.
Kerberos	Verkkotodennusprotokolla, jota käytetään käyttäjän ja palveluiden turvalliseen tunnistamiseen.
LCM	Lifecycle management. IT-järjestelmien ja sovellusten elinkaaren hallinta.
LDAP	Lightweight Directory Access Protocol. Protokolla hakemistopalvelujen käyttöön ja hallintaan.
M365	Microsoft 365. Microsoftin pilvipohjainen tuottavuus- ja yhteistyöalusta.
MDM	Mobile Device Management. Järjestelmä, jonka avulla yritykset voi turvata, hallita ja ohjailla työntekijöiden mobiililaitteita.
MFA	Multi-Factor Authentication. Monivaiheinen todennusmenetelmä, joka parantaa tietoturvaa.
OTP	One-Time Password. Kertakäyttösalasana, jota käytetään usein osana MFA:ta.
RBAC	Role-Based Access Control. Roolipohjainen pääsynhallinta, jossa oikeudet määritellään roolien mukaan.

SaaS	Software as a Service. Ohjelmistopalvelumalli, jossa sovellukset tarjotaan pilvestä.
SCIM	System for Cross-domain Identity Management. Automatisoi käyttäjätietojen kulkua tunnistetietojen tai IAM-järjestelmän ja pilvipohjaisten sovellusten tai palveluiden välillä.
SSO	Single Sign-On. Kertakirjautuminen, joka mahdollistaa pääsyn useisiin palveluihin yhdellä kirjautumisella.

1 Johdanto

Tässä opinnäytetyössä tutkitaan käyttäjätunnus- ja laitehallinnan siirtymistä Microsoft Active Directorysta pilvipohjaiseen Microsoft Entra ID -palveluun merenkulkualan yrityksen IT-infrastruktuurissa. Tutkimuksen tarkoituksena on selvittää, miten siirtymä voidaan toteuttaa teknisesti ja hallinnollisesti, ja miksi muutos on tarpeen parantamaan tietoturvaa, etätyöskentelyä sekä hallintaprosessien sujuvuutta.

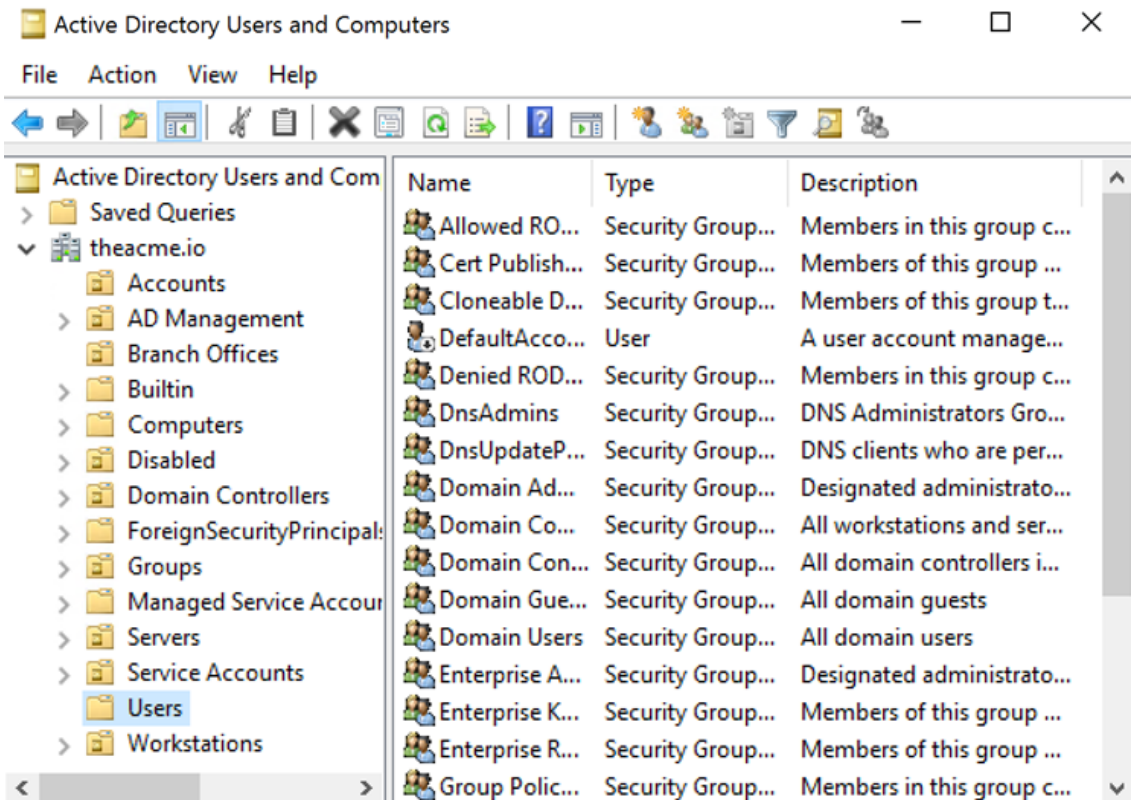
Tutkimus toteutettiin projektiluonteisesti. Työssä päivitettiin noin 130 laitetta Windows 11 -käyttöjärjestelmään, suunniteltiin käyttäjätunnusten siirto Microsoft Entra ID:hin sekä otettiin käyttöön synkronointimenetelmiä, kuten Okta-palvelu. Rajauksena oli keskittyä ensisijaisesti teknisiin päivityksiin ja pilvisiirtymän valmisteluun yrityksen olemassa olevassa ympäristössä.

Aiempaa tutkimusta ja käytäntöjä kartoitettiin liittyen pilvipalveluiden hyödyntämiseen käyttäjähallinnassa ja tietoturvassa, joista nousi esiin pilvipohjaisten ratkaisujen etuja joustavuudessa ja hallittavuudessa.

Raportissa käsitellään projektin toteutusvaiheet, käytetyt työkalut ja teknologiat, haasteet sekä vaikutukset organisaation IT-toimintoihin. Tuloksena organisaation IT-infrastruktuuri on valmisteltu pilvisiirtymää varten, ja siirtymän odotetaan parantavan merkittävästi tietoturvaa, hallittavuutta ja etätyöskentelyn sujuvuutta.

2 Microsoft Active Directory -käyttäjähakemistopalvelu

Microsoft Active Directory (AD) on käyttäjähakemistopalvelu, joka on suunniteltu Windows-toimialueympäristöön. Se julkaistiin ensimmäisen kerran vuonna 1999 Windows Server 2000 -käyttöjärjestelmässä (Advania n.d.). AD tallentaa käyttäjien, laitteiden ja muiden resurssien tiedot sekä asetukset keskitettyyn tietokantaan. Sen avulla on helpompi hallita ja suojata organisaation resursseja. AD käyttää Kerberos-protokollaa turvalliseen kirjautumiseen ja LDAP-protokollaa tiedon hakemiseen hakemistosta (Auxility 2024). Käyttöliittymä (kuva 1.) on selkeä ja helppokäyttöinen.

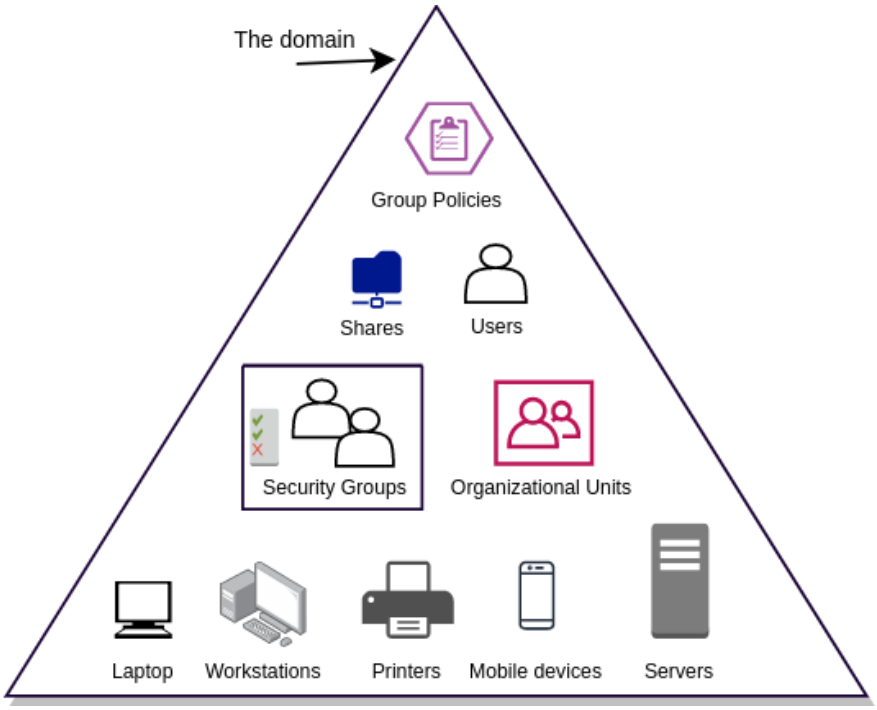


Kuva 1. Active Directoryn käyttöliittymä.

Active Directory koostuu viidestä erilaisesta hakemistopalvelusta, joista Active Directory Domain Services (AD DS) on yleisimmin käytetty ja keskeisin. Tiedot kaikista laitteista ja käyttäjistä sekä hakemistotietojen tallentaminen löytyvät AD DS -palvelusta (Microsoft 2025c). AD DS käyttää DNS-protokollaa domainien tunnistamiseen sekä laitteiden väliseen kommunikointiin (Microsoft 2024b).

Tietorakenteeltaan AD DS perustuu hierarkkiseen malliin, joka koostuu metsistä (engl. forests), puista (engl. trees) ja toimialueista (engl. domains) (kuva 2.). Skeemassa (engl. Schema) määritellään objektiluokat, jotka voidaan luoda AD-metsään. Skeemassa määritellään myös objektiluokkien attribuutit, jotka voivat olla joko pakollisia tai valinnaisia kullekin objektityypille (Microsoft 2025c).

Yleisimpiä AD:n objektityyppejä ovat käyttäjät, tietokoneet, tulostimet, jaetut kansiot ja sovellukset. Osa objekteista voi olla laajempia kokonaisuuksia, jotka sisältävät toisia objekteja. Siitä syystä AD:tä kuvataan hierarkkiseksi. Globaali luettelo (engl. Global Catalog), josta löytyvät tiedot kaikista hakemiston objekteista, on tärkeä ominaisuus AD:ssä. Sen avulla tiedot on helppo löytää mistä tahansa toimialueesta (Microsoft 2025c).



Kuva 2. Active Directory Domain Services -hierarkia. (RootDSE 2021.)

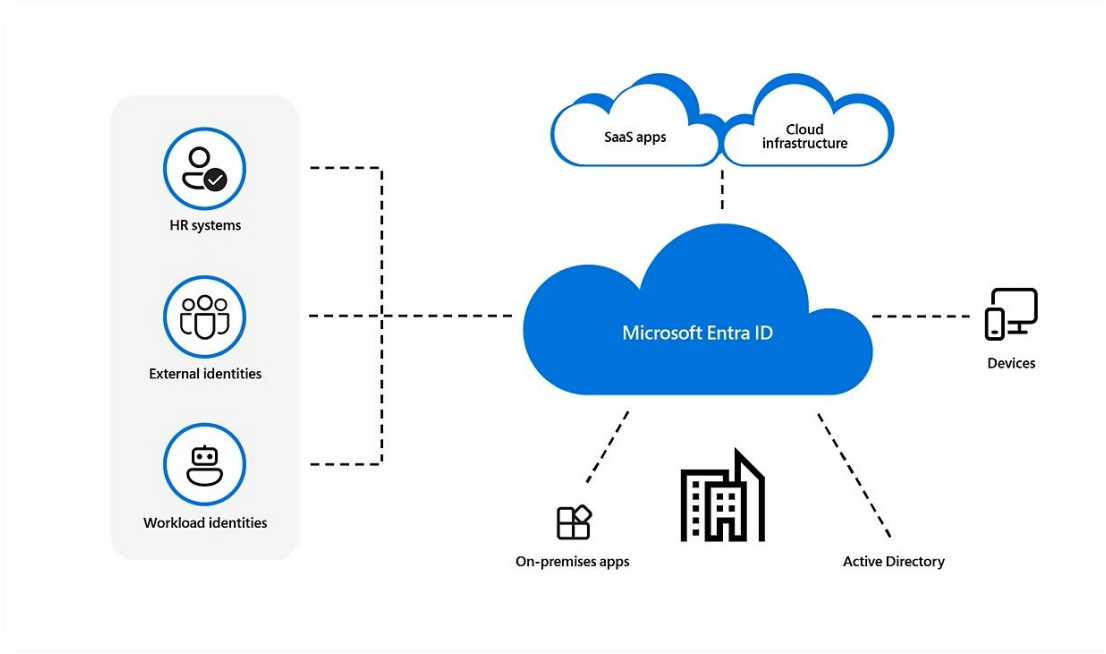
Turvallisuus on integroitu kirjautumistodennuksen ja objektien käyttöoikeuksien hallintaan. Ylläpitäjät voivat yhden kirjautumisen kautta hallita hakemistotietoja ja organisaatiota verkossaan. Politiikkapohjainen hallinta, kuten ryhmäkäytännöt (Group Policy), tekee verkkojen hallinnasta helpompaa ja mahdollistaa keskitetyn käyttäjähallinnan ja turvallisuuden hallinnan (Microsoft 2025c).

AD:n suurimmat edut, kuten keskitetty hallinta, käyttäjähallinnan tehokkuus ja turvallisuuspolitiikkojen noudattaminen, ovat syitä sen pitkään suosioon. Keskitetty hallinta yksinkertaistaa turvallisuuspolitiikkojen noudattamista, käyttäjien sekä käyttöoikeuksien hallintaa. Pilvipalveluiden käytössä monet organisaatiot käyttävät AD:ta, jotta todennus ja valtuutus olisi mahdollisimman helppoa eri ympäristöjen välillä (Microsoft n.d.).

3 Microsoft Entra ID -pilvipalvelu

Microsoft Entra ID on pilvipohjainen identiteetin- ja pääsynhallintaratkaisu, joka tarjoaa monipuoliset työkalut käyttäjien, ryhmien ja käyttöoikeuksien hallintaan. Sen avulla voidaan hallita käyttäjiä, ryhmiä ja käyttöoikeuksia sekä ottaa käyttöön monivaiheinen tunnistautuminen (MFA) ja kertakirjautuminen (SSO). Jos organisaatiolla on käytössä sekä Entra ID että perinteinen AD, niiden välillä voidaan synkronoida identiteetit. Tämä mahdollistaa saumattoman kirjautumisen eri ympäristöjen ja palvelujen välillä (Microsoft 2025a.).

Koska Entra ID on täysin pilvipohjainen, sen avulla voidaan hallita pääsyä erilaisiin pilvisovelluksiin ja -palveluihin, kuten Microsoft 365:een ja muihin SaaS-ratkaisuihin. (Kuva 3.) Sen hallintakonsoli on moderni, helppokäyttöinen ja se saa säännöllisesti automaattisia päivityksiä, mikä tekee siitä vaivattoman käyttää verrattuna perinteiseen Active Directoryyn, joka vaatii manuaalisia päivityksiä ja ylläpitoa (Microsoft 2025b.).



Kuva 3. Entra ID -arkkitehtuuri (Microsoft n.d.).

Tietoturvaominaisuudet

Tietoturva on yksi Entra ID:n keskeisimmistä ominaisuuksista. Palvelu hyödyntää tekoälyä ja koneoppimista analysoidessaan kirjautumisia ja havaitakseen mahdollisia uhkia. Riskipohjainen todennus voi esimerkiksi tunnistaa epäilyttävät kirjautumisyritykset ja vaatia lisävahvistusta, kuten monivaiheista tunnistautumista. Ehdollinen pääsy mahdollistaa käyttöoikeuksien rajoittamisen tietyissä tilanteissa – esimerkiksi jos käyttäjä yrittää kirjautua tuntemattomalta laitteelta tai poikkeuksellisesta sijainnista, pääsy voidaan estää. Identiteetin suojaus toimii reaaliaikaisesti ja auttaa ennaltaehkäisemään identiteettivarkauksia ja muita tietoturvauhkia (Microsoft n.d.).

Automaatio ja hallinta

Entra ID tukee automatisointia, jonka avulla vähennetään manuaalisia työtehtäviä. Power Automate on Microsoftin työkalu, jonka avulla työnkulkuja voidaan automatisoida. Sinne luodaan säännönmukaisia prosesseja, jotka laukaisevat automaattisia toimia, kuten esimerkiksi lisenssien myöntäminen uusille käyttäjille tai käyttäjien lisääminen eri ryhmiin.

Lisenssit ja ominaisuudet

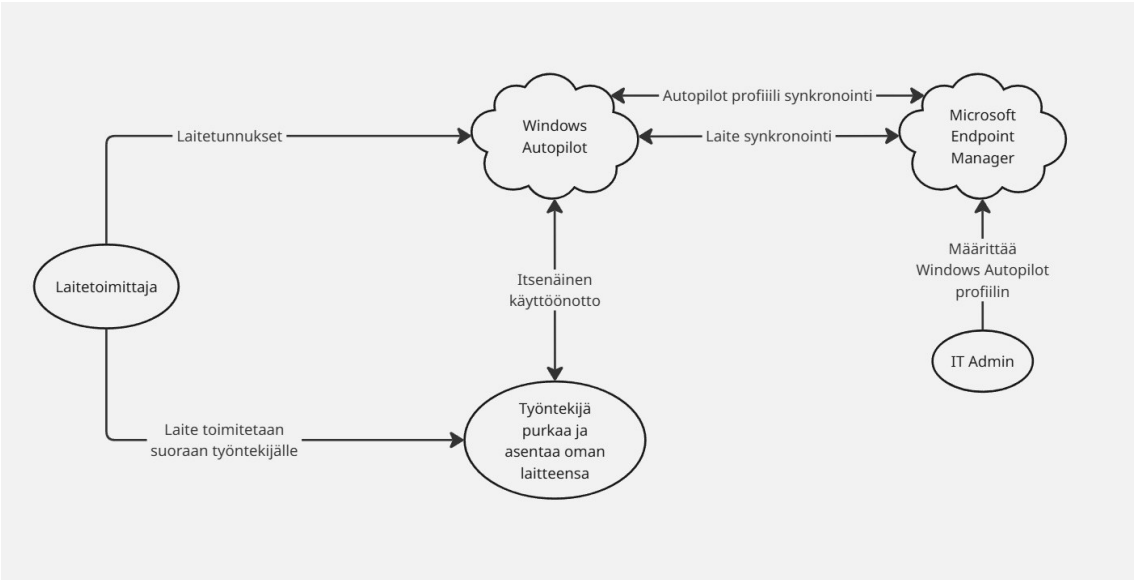
Entra ID:stä on saatavilla useita eri lisenssiversioita. Ilmainen versio sisältää perusominaisuuksia, kuten monivaiheisen tunnistautumisen, kertakirjautumisen SaaS-sovelluksiin, perusraportit ja itsepalvelusalasanan vaihdon. P1-lisenssi maksaa 6 $ per käyttäjä kuukaudessa ja tarjoaa lisäominaisuuksia, kuten ehdollisen pääsyn, roolipohjaisen pääsynhallinnan ja dynaamiset ryhmät. P2-lisenssi, joka maksaa 9 $ per käyttäjä kuukaudessa, tuo mukanaan kehittyneemmät tietoturvaominaisuudet, kuten identiteetin suojauksen ja riskipohjaisen todennuksen. Peruslisenssien lisäksi on saatavilla Entra Suite -paketti, joka maksaa 12 $ per käyttäjä kuukaudessa ja sisältää laajan valikoiman Microsoft Entra -tuotteita (Quest n.d.).

4 Windows Autopilot -laitteiden käyttöönottopalvelu

Windows Autopilot on kokoelma teknologioita, joiden avulla uusien Windows-laitteiden käyttöönotto voidaan automatisoida ja yksinkertaistaa. Se on suunniteltu moderniin työympäristöön, jossa työntekijät saavat uudet laitteensa suoraan valmistajalta tai jälleenmyyjältä – ilman että IT-osaston tarvitsee käsitellä niitä fyysisesti. Autopilotin avulla laitteet konfiguroidaan automaattisesti pilvipalveluiden, kuten Microsoft Intunen ja Microsoft Entra IDn, avulla heti ensimmäisen kirjautumisen yhteydessä (Microsoft 2024a.).

Laitteen rekisteröinti ja käyttöönotto

Prosessi lähtee liikkeelle siitä, että laitteen valmistaja tai yrityksen IT-osasto rekisteröi laitteen Autopilot-palveluun sen laitteistotunnisteen perusteella. Kun käyttäjä käynnistää laitteen ja yhdistää sen internetiin, Windows tunnistaa laitteen rekisteröidyksi ja hakee sille automaattisesti oikean käyttöönotto- ja konfiguraatioprofiilin. (Kuva 4.) Nämä profiilit sisältävät mm. organisaation määritykset, kuten sovellukset, suojausasetukset, verkkoyhteydet ja käyttäjäpolitiikat. Käyttäjän tarvitsee vain kirjautua sisään omilla tunnuksillaan, kaikki muu hoituu automaattisesti taustalla. Autopilotin avulla laitteet liittyvät suoraan Entra ID -ympäristöön ja rekisteröityvät hallintaratkaisuihin, ilman erillistä manuaalista asennusta. Tämä mahdollistaa laitteiden keskitetyn hallinnan ensimmäisestä käynnistyksestä lähtien (Microsoft n.d.).



Kuva 4. Windows Autopilot -arkkitehtuuri.

Käyttökokemuksen personointi ja ylläpito

Autopilotin avulla käyttöönottoa voidaan personoida esimerkiksi näyttämällä organisaation logo tai piilottamalla tietyt käyttöjärjestelmän valintaikkunat, jolloin käyttökokemus pysyy selkeänä ja yhdenmukaisena (Javed 2023.).

Yksi Autopilotin hyödyllisimmistä ominaisuuksista on "Autopilot Reset" -toiminto, jolla käytössä oleva laite voidaan palauttaa alkuperäiseen, organisaation määrittelemään tilaan. Tämä on hyödyllistä esimerkiksi henkilövaihdosten yhteydessä, jolloin sama laite voidaan ottaa nopeasti uudelleen käyttöön ilman, että asennusta tarvitsee aloittaa alusta alkaen uudelleen (Microsoft 2024a.).

Hyödyt organisaatiolle

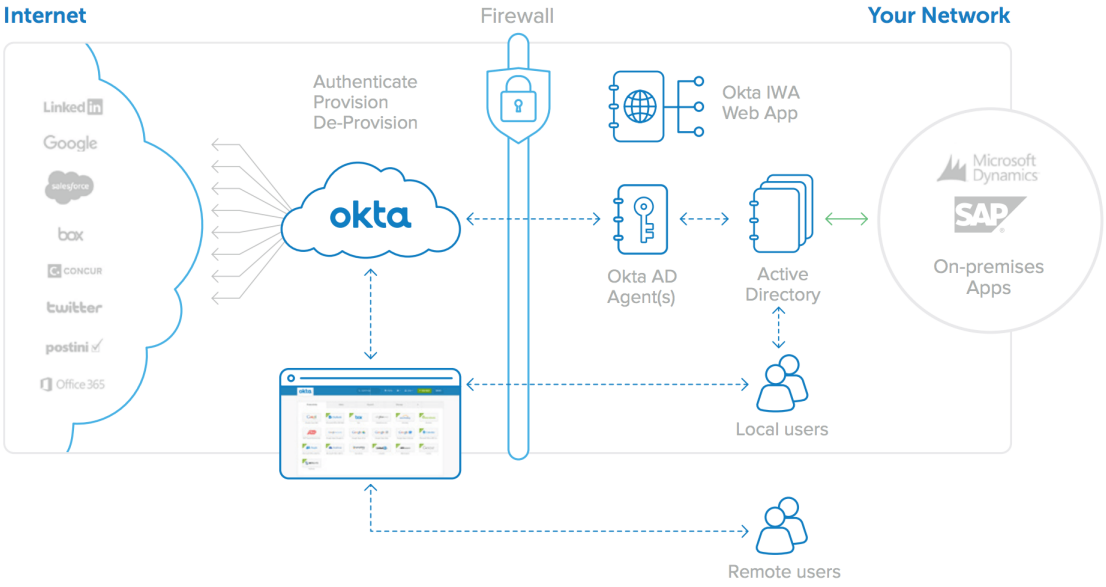
Organisaatioille tästä on konkreettisia hyötyjä. Esimerkiksi IT-osaston aikaa ja resursseja säästyy, tietoturva paranee, kun laitteet noudattavat automaattisesti yhteisiä suojauskäytäntöjä, ja loppukäyttäjien käyttöönotto on huomattavasti sujuvampaa. Käytännössä Autopilot mahdollistaa laitteiden "zero-touch provisioningin", jossa monia laitteita voidaan ottaa käyttöön yhtä aikaa ilman, että IT joutuu käsittelemään niitä (Softlanding 2024.).

5 Okta -identiteettien hallinta-alusta

Okta on pilvipohjainen järjestelmä, joka tekee käyttäjien tunnistautumisesta ja käyttöoikeuksien hallinnasta sujuvampaa ja turvallisempaa. Se on suunniteltu yrityksille, organisaatioille ja yksityishenkilöille, jotka haluavat yksinkertaistaa kirjautumisprosesseja ja suojata käyttäjätilejään. Okta sisältää monia eri ominaisuuksia esimerkiksi yhdistetyn hakemiston kaikista käyttäjistä ja ryhmistä, kertakirjautumisen, vahvan tunnistautumisen ja identiteettien elinkaaren automatisoinnin (Kuva 5.) (Secure Cloud n.d.).

Kuva 5. Oktan tarjoamat palvelut. (Identity Classes n.d.)

Perinteisesti eri sovelluksiin on pitänyt luoda omat käyttäjätunnukset ja salasanat, mutta Okta kokoaa kaiken yhteen niin, että yhdellä kirjautumisella saa pääsyn kaikkiin tarvittaviin palveluihin. Se tukee laajasti eri sovelluksia, kuten Microsoft 365:tä, Google Workspacea ja Salesforcea, mutta sen voi integroida myös muihin järjestelmiin tarpeen mukaan (Kuva 6.) (Okta 2025a.).



Kuva 6. Okta Active Directoryssa -arkkitehtuuri (Okta n.d.).

Tietoturva ja todennus

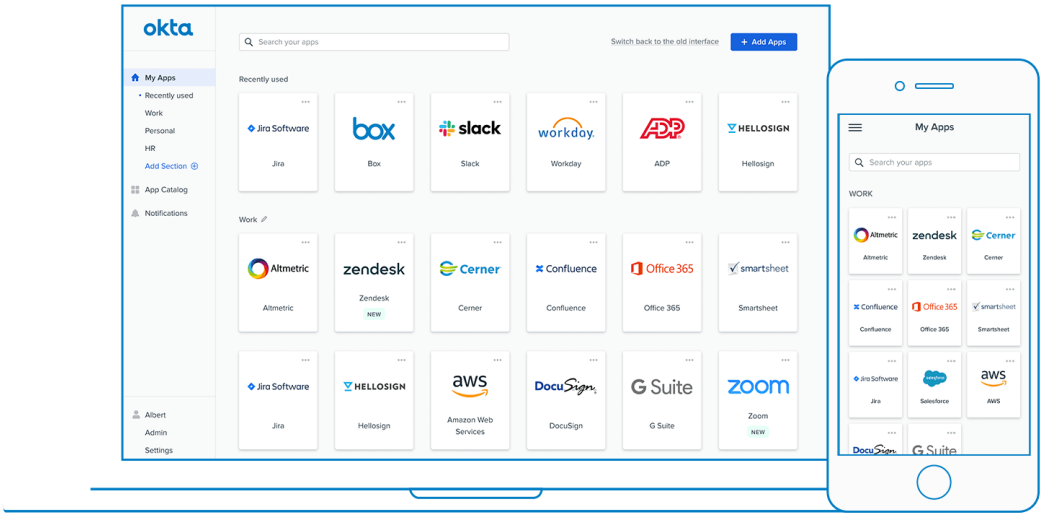
Turvallisuus on yksi Oktan tärkeimmistä ominaisuuksista. Okta hyödyntää monivaiheista tunnistautumista (MFA). Käytännössä tämä tarkoittaa, että pelkän salasanan lisäksi kirjautumisen yhteydessä vahvistetaan henkilöllisyys toisella menetelmällä, kuten sormenjäljellä, kertakäyttöisellä varmistuskoodilla (OTP) tai push-ilmoituksella, joka hyväksytään puhelimesta. Tämä tekee tilien kaappaamisesta huomattavasti vaikeampaa ja parantaa tietoturvaa merkittävästi (Okta 2025b.).

Käyttäjähallinnan automaatio

Okta tarjoaa tehokkaita työkaluja käyttäjähallintaan. Uuden työntekijän aloittaessa, hänen käyttöoikeutensa voidaan määrittää automaattisesti ilman, että IT-osaston tarvitsee tehdä kaikkea manuaalisesti. Vastaavasti, kun työntekijä lähtee, hänen pääsynsä eri järjestelmiin voidaan poistaa yhdellä kertaa, mikä vähentää tietoturvariskejä (Okta 2024.).

Laiteriippumattomuus ja käytettävyys

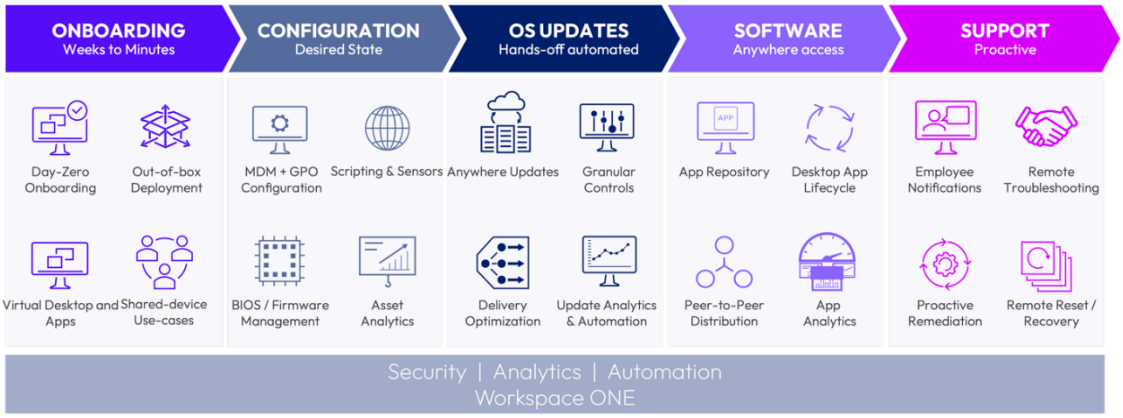
Okta toimii kaikilla laitteilla, joten se ei ole sidottu mihinkään tiettyyn käyttöjärjestelmään tai verkkoympäristöön (Kuva 7.). Käyttäjä voi kirjautua tietokoneella, tabletilla tai puhelimella, ja järjestelmä toimii saumattomasti eri sovellusten ja palveluiden välillä (Okta n.d.).



Kuva 7. Oktan käyttöliittymä tietokoneella ja puhelimessa (Okta n.d.).

6 Workspace ONE -työympäristöratkaisu

Workspace ONE on digitaalinen työympäristöratkaisu, joka auttaa yrityksiä hallitsemaan ja suojaamaan työntekijöidensä laitteita, sovelluksia ja tietoja. Se yhdistää identiteetinhallinnan, laitehallinnan ja sovellusten hallinnan yhdeksi kokonaisuudeksi, jolloin IT-osasto voi hallita kaikkia yrityksen laitteita yhdestä paikasta (Kuva 8.) (Omnissa n.d.).



Kuva 8. Pilvessä toimivien työasemien moderni ylläpito (Omnissa n.d.).

Tietoturva ja pääsynhallinta

Tietoturva on yksi Workspace ONEn keskeisimmistä ominaisuuksista. Se varmistaa, että vain valtuutetut käyttäjät pääsevät käsiksi yrityksen järjestelmiin ja tietoihin. Sen avulla yritys voi asettaa erilaisia käyttöoikeussääntöjä, kuten monivaiheisen tunnistautumisen, ja estää luvattoman pääsyn yrityksen resursseihin. Lisäksi Workspace ONE mahdollistaa laitteiden ja sovellusten keskitetyn hallinnan, jolloin IT-osasto voi esimerkiksi asentaa päivityksiä ja määrittää tietoturva-asetuksia ilman, että käyttäjän tarvitsee tehdä mitään (Omnissa n.d.).

Laitteiden elinkaarenhallinta

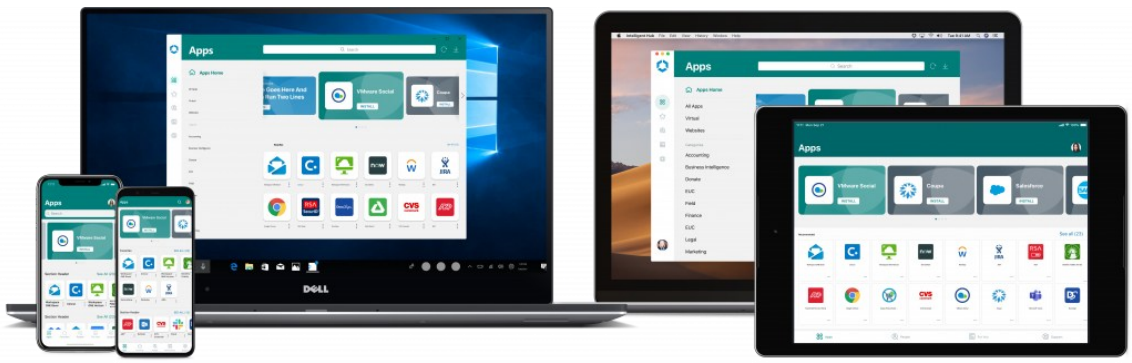
Workspace ONE tukee laitteiden elinkaarenhallintaa, mikä tarkoittaa, että yritys voi hallita laitteita niiden koko käyttöiän ajan. Kun uusi työntekijä aloittaa, hänen työvälineensä voidaan ottaa käyttöön automaattisesti esiasennetuilla sovelluksilla ja asetuksilla. Jos työntekijä vaihtaa laitetta tai poistuu yrityksestä, kaikki tarvittavat muutokset voidaan tehdä etänä ilman manuaalista työtä (Omnissa n.d.).

Hallintakonsoli ja käyttäjän käyttöliittymä

Workspace ONE tarjoaa kaksi erillistä käyttöliittymää eri käyttäjäryhmille: selainpohjaisen hallintakonsolin IT-osastolle ja Workspace ONE Hub -sovelluksen loppukäyttäjille.

Hallintakonsolin avulla IT-henkilöstö voi hallita koko organisaation laitekantaa keskitetysti. Konsolista voidaan mm. seurata laitteiden tilaa, hallinnoida sovellusten jakelua ja soveltaa tietoturvakäytäntöjä eri laitteille. Tämä keskitetty hallinta parantaa reagointikykyä ja vähentää manuaalista työtä.

Loppukäyttäjän näkökulmasta Workspace ONE Hub toimii yhtenäisenä pääsyportaalina yrityksen sovelluksiin ja resursseihin. Käyttäjä voi kirjautua sovellukseen miltä tahansa laitteelta – olipa kyseessä kannettava tietokone, tabletti tai älypuhelin. Hub-sovellus mahdollistamaa sujuvan siirtymisen eri palveluiden välillä (Kuva 9.) (Omnissa, n.d.).



Kuva 9. Workspace ONE Hub -käyttöliittymä (Marshall 2021.).

Hyödyt organisaatioille

Workspace ONE tekee työskentelystä sujuvampaa ja turvallisempaa sekä työntekijöille että IT-osastolle. Se poistaa tarpeen monimutkaisille kirjautumisprosesseille, automatisoi laitehallinnan ja varmistaa, että yrityksen tiedot pysyvät turvassa riippumatta siitä, millä laitteella niitä käytetään. Se sopii kaikenkokoisille yrityksille, jotka haluavat parantaa työntekijöidensä käyttökokemusta ja samalla varmistaa tietoturvan korkealla tasolla (Omnissa 2023.).

7 Syyt muutokseen

Ennen projektia uusien käyttäjätunnusten luominen ja hallinta vaati huomattavan määrän manuaalisia työvaiheita. Aamuisin saatiin sähköpostitse listat tunnusmuutoksista, jotka käytiin läpi yksi kerrallaan. Tämän jälkeen tehtiin tarvittavat päivitykset käyttäjätunnuksiin. Jos työntekijän sopimus päättyi, tieto ei aina kulkenut ajallaan, ja tunnukset saattoivat jäädä turhaan auki.

Prosessien automatisointi helpotti huomattavasti IT-osaston työtaakkaa ja paransi yrityksen kykyä hallita tietoja avatuista ja suljetuista tileistä. Tiedonsiirron parantaminen mahdollisti entistä tehokkaamman seurannan ja automaattiset toimenpiteet.

Työntekijöiden pääsy tiedostoihin ja sovelluksiin oli erityisen tärkeää aluksilla, joissa käytettiin mobiilidataa. Tämä mahdollisti sen, että työntekijät pystyivät työskentelemään sujuvasti koko työvuoron ajan.

Salasanojen nollauspyynnöt kuormittivat aiemmin IT-osastoa. Muutoksen myötä työntekijät pystyivät itse vaihtamaan salasanansa ilman IT-tukea, mikä vähensi IT-osaston työkuormaa ja paransi työntekijöiden käyttökokemusta.

Etätyöskentelyn verkko-ongelmat olivat myös haaste, erityisesti kun yhteydet kulkivat tunnelin kautta ja pätkivät usein. Kun kaikki tieto siirtyi pilvipalveluihin, verkkoyhteyksien luotettavuus parani huomattavasti ja ongelmat vähenivät.

8 Työn suorittaminen

8.1 Tietokoneiden tyhjentäminen ja uudelleen asennus

Projekti alkoi toimiston tietokoneiden uusimisella ja päivittämisellä. Uudet laitteet tilattiin työntekijöille, joilla oli vanhat laitteet käytössä. Tietokoneisiin asennettiin tarvittavat sovellukset ja päivitykset Workspace One Hubin kautta. M365-sovellukset ladattiin selaimen kautta, koska se oli nopein ja tehokkain tapa.

Kun kaikilla toimiston työntekijöillä oli uudet laitteet käytössä, siirryttiin vanhojen tietokoneiden käsittelyyn. Varmistettiin, että koneissa oli vähintään 16 gigatavua muistia ja asennettiin niihin Windows 11. Laitteet tyhjennettiin ja niihin määritettiin aluksen tunnukset. Asennetut laitteet lähetettiin aluksille, ja vanhat koneet palautettiin toimistolle jatkokäsittelyä varten. Tätä prosessia toistettiin, kunnes kaikilla aluksilla ja käyttäjillä oli päivitetyt, Entra ID:hen liitetyt koneet käytössä.

Haasteet ja ratkaisut

Uusien koneiden asennusta hidasti käytössä olevien laitteiden vähäisyys. Ennen kuin uudet koneet olivat saapuneet, niin koneita oli rajoitettu määrä mikä hidasti työn etenemistä.

Windows 11:n asentaminen toi mukanaan useita haasteita. Joissakin koneissa ei ollut tarvittavia vaatimuksia käyttöjärjestelmän asennukseen, joten asennus piti tehdä pakotettuna näille laitteille. Asennusaika vaihteli 15 minuutista muutamaan tuntiin. Käyttäjillä oli haasteita uusien koneiden käytössä, esimerkiksi joidenkin verkkosivustojen käyttäjätunnukset ja salasanat eivät olleet siirtyneet uudelle laitteelle. Myös tiettyjen sovellusten ja asetusten poistaminen aiheutti ongelmia.

Laitteiden liittäminen Autopilot-järjestelmään oli tärkeä osa prosessia. Muutamat koneet jouduttiin liittämään Autopilottiin PowerShellin-komentojen avulla kesken

Entra ID-rekisteröinnin. Laitteiden nollauksen jälkeen laitetilit poistettiin Active Directorysta.

Tietokoneiden päivityksissä ilmeni myös ongelmia, kun eräs Windowsin kumulatiivinen päivitys ei suostunut asentumaan osalle laitteista. Windowsin korjauspäivityksen asentamisen jälkeen asennus onnistui useimmissa tapauksissa. Uusia sovelluksia ei voitu asentaa ennen päivityksen valmistumista.

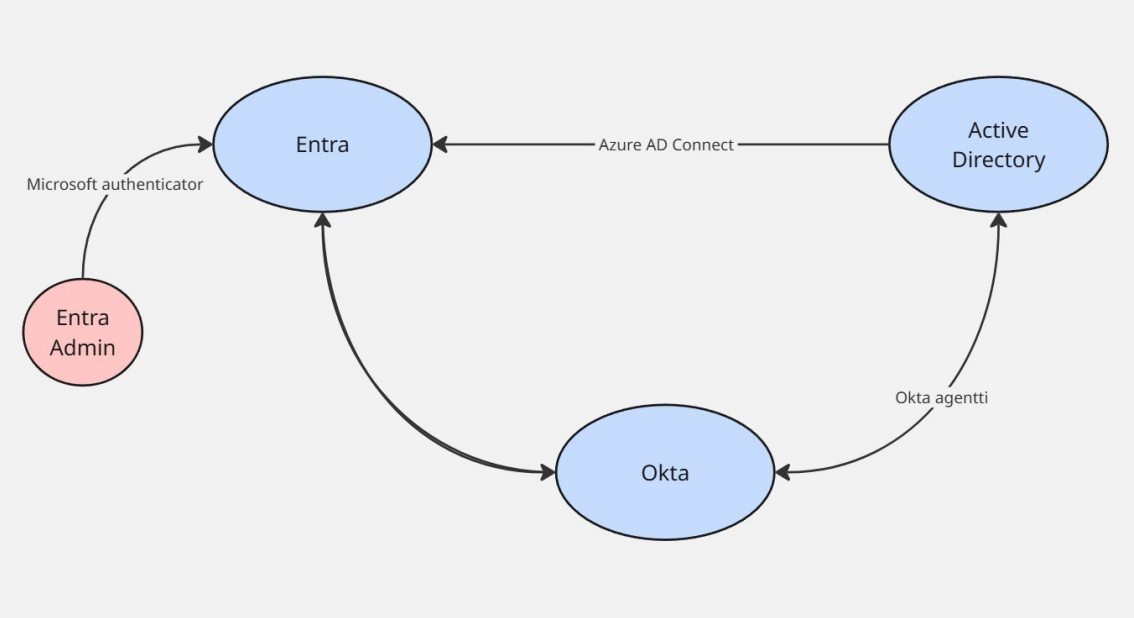
Telakalla huollossa oleviin aluksiin käytiin paikan päällä asentamassa tietokoneet ja verkot.

8.2 Käyttäjähakemiston synkronointi

Ennen käyttäjätunnukset synkronoitiin ADsta sekä Oktaan että Entraan. Jos käyttäjään tehtiin muutoksia Oktassa, ne synkronoituivat takaisin AD:n puolelle. (Kuva 10.)

Käyttäjähakemiston synkronoinnissa Entraan käytettiin Azure AD Connect -työkalua, joka on Entra Connectin keskeinen komponentti.

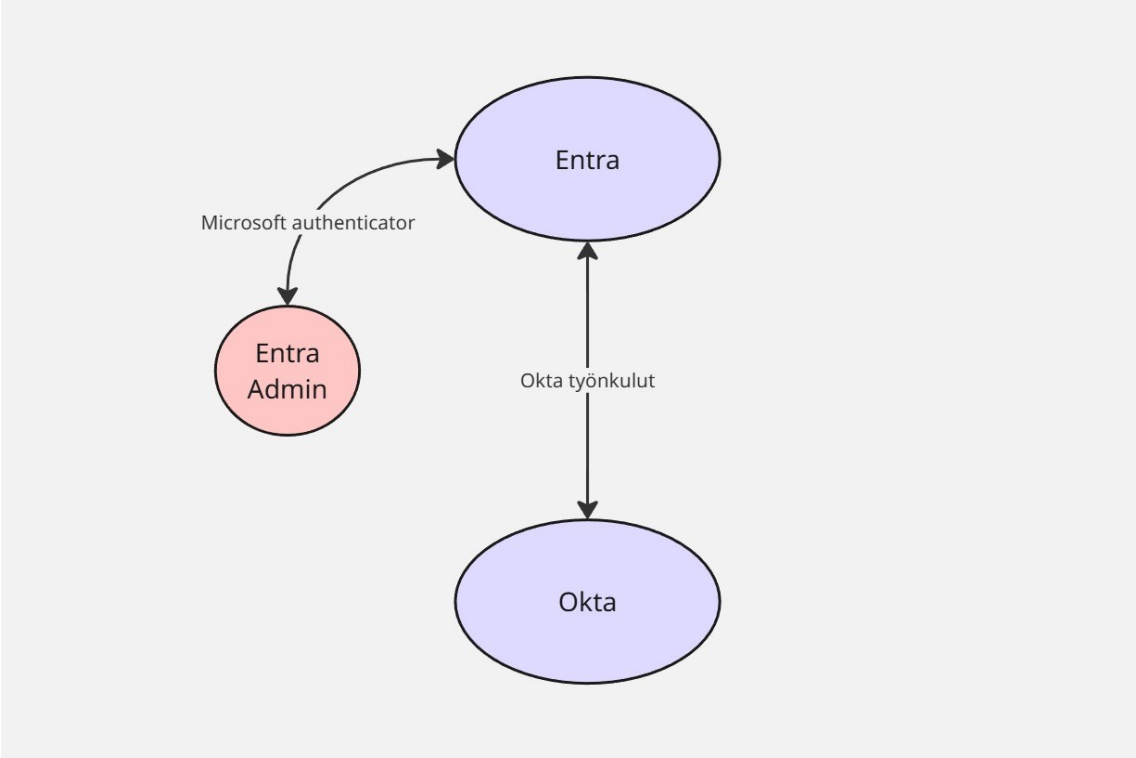
Vanhan synkronoinnin heikkous oli viiveet Entrassa. Esimerkiksi ryhmämuutosten, uusien käyttäjien luomisen tai vanhojen käyttäjien poistojen jälkeen tiedot päivittyivät Entraan vain noin 30 minuutin välein. Sen sijaan salasanamuutokset siirtyivät välittömästi ilman viivettä.



Kuva 10. Tietojen synkronointikaavio ennen.

Kun AD-palvelin suljetaan, niin Azure AD Connect -yhteys on katkaistava, koska synkronointi AD:n ja Entra ID:n välillä ei enää toimi ilman tätä yhteyttä. Tämän jälkeen kaikki käyttäjät, jotka olivat aiemmin AD:ssä, siirtyvät pilvikäyttäjiksi Entra ID:ssa.

Tässä tilanteessa muutos täytyy tehdä tenantti kerrallaan, sillä yksittäistä käyttäjätunnusta ei voi suoraan muuttaa AD-käyttäjästä pilvikäyttäjäksi. Suoraa synkronointia ei ole tarjolla, mutta muutokset voidaan hallita Okta-järjestelmän työnkulkujen avulla (Kuva 11.). Tämä tarkoittaa, että AD:n hallinta jää taakse, ja pilvipalveluiden välinen synkronointi ja hallinta ottavat paikan.



Kuva 11. Synkronointikaavio muutoksen jälkeen.

8.3 Käyttäjä- ja laitehallinnan muutokset

Ennen muutosta käyttäjätunnusten, laitteiden, ryhmien ja sääntöjen hallinta tapahtui pääasiassa AD:n kautta. Entra ja Okta eivät tukeneet suoria muutoksia käyttäjätunnuksiin tai ryhmiin.

Muutoksen jälkeen käyttäjätunnusten hallinta siirtyi Okta-järjestelmään, jossa oli mahdollista luoda, poistaa ja muokata käyttäjätunnuksia. Oktan toiminnallisuudet muistuttivat paljon AD:n toimintaa, mikä teki siirtymästä sujuvamman.

Oktan työnkulkujen automatisointi teki prosesseista tehokkaita. Työnkulut pystyivät hakemaan tarvittavat tiedot pilvipalveluista, kuten työntekijän työsopimuksen alkamis- ja loppumispäivämäärän sekä aluksen tiedot, johon työntekijä oli menossa. Näiden tietojen perusteella työnkulku käynnisti käyttäjätunnusten luomisen ja aktivoinnin lähellä sopimuksen alkua. Lisäksi työnkulku lähetti työntekijälle ohjeet kirjautumiseen ja salasanan vaihtamiseen,

ja tunnukset lisättiin automaattisesti oikeisiin ryhmiin ja sähköpostiketjuihin. Kun työntekijän sopimus päättyi, työnkulku poisti käyttäjätunnukset ryhmistä ja sulki ne.

Haasteena automaation toteutuksessa oli kuitenkin se, että osa työntekijöistä työskenteli usealla aluksella samanaikaisesti tai vuorotteli alusten välillä. Tämä edellytti, että heidät lisättiin automaattisesti useampaan aluksen ryhmään yhtä aikaa.

8.4 Active Directoryn tyhjentäminen

Siirtymävaiheessa AD:n tyhjentäminen ja poistaminen ei toteutunut alkuperäisen aikataulun mukaisesti. Viivästystä aiheuttivat erityisesti laitteiden saatavuusrajoitteet sekä odotus seuraavan MDM-järjestelmäversion julkaisusta. MDM:n uusi versio oli välttämätön, sillä se toi mukanaan tuen SCIM-protokollalle, joka mahdollisti laitekäyttäjien synkronoinnin Entran ID:stä ja käyttäjähallinnan siirtämiseksi pois AD-ympäristöstä.

SCIM oli erityisen tärkeä protokolla, sillä osa organisaation kriittisistä järjestelmistä käytti LDAP-protokollaa, joka on vahvasti sidoksissa AD:hen. Vasta SCIM:n käyttöönoton jälkeen oli teknisesti mahdollista alkaa siirtää näitä järjestelmiä pois LDAP-riippuvuudesta.

SCIM helpotti huomattavasti käyttäjätietojen hallintaa eri järjestelmien välillä. Sen ansiosta tietoja voitiin synkronoida automaattisesti ilman manuaalista työtä tai erikseen rakennettuja integraatioita. Tämä vähensi virheiden riskiä ja kevensi IT-osaston työtaakkaa. Käyttäjätiedot pysyivät ajan tasalla, ja koko järjestelmäympäristön tietoturva parani.

SCIM toi lisää selkeyttä ja läpinäkyvyyttä käyttäjähallintaan. Kun käyttäjätietoihin tehtiin muutoksia, niistä jäi lokiin jäljet, mikä helpotti esimerkiksi tietoturvatarkastuksia.

9 Lopuksi

Opinnäytetyössä saavutettiin useita tärkeitä tavoitteita, vaikka kaikki suunnitellut toimenpiteet eivät toteutuneet alkuperäisten odotusten mukaisesti. Yrityksen tietokoneet päivitettiin onnistuneesti Windows 11 -käyttöjärjestelmään, ja samalla laitteiden hallinta siirrettiin Entra ID -palveluun. Tämä onnistui hyvin, vaikka päivitysprosessi eteni hitaasti ja joidenkin laitteiden kohdalla tarvittiin lisätoimenpiteitä, kuten pakotettua asennusta.

Tekniset haasteet, kuten Windowsin kumulatiivisten päivitysten asennusongelmat sekä tiettyjen automaatioiden luominen käyttäjätunnusten ja ryhmien hallintaan, aiheuttivat lisätyötä. Erityisesti työntekijöiden työskentely useilla aluksilla samanaikaisesti vaati monimutkaisempia ratkaisuja ryhmäjäsenyyksien hallintaan.

Active Directory -palvelimen sulkeminen ja siirtyminen täysin pilvipohjaiseen käyttäjähallintaan edellyttivät suunnittelua ja vaiheittaista toteutusta. SCIM-protokollan käyttöönotto osoittautui ratkaisevaksi, sillä sen avulla pystyttiin lopulta siirtämään käyttäjätiedot järjestelmien välillä ilman AD:n ja LDAP:n riippuvuutta.

Vaikka projekti toi esiin muutamia ongelmakohtia ja kehityskohteita, tuloksia voidaan hyödyntää jatkossa organisaation IT-prosessien parantamisessa, erityisesti automaation ja pilvialustojen tehokkaassa käytössä. Projektin tuloksia voidaan soveltaa myös muissa yrityksissä, joissa on tarpeita käyttäjähallinnan ja laitehallinnan tehostamiseksi.

Jatkokehityksessä olisi tärkeää tarkastella pilvipalveluiden ja käyttäjähallinnan tulevaisuutta. Myös tietoturvariskien hallinta ja automaation parantaminen ovat alueita, jotka vaativat jatkuvaa seurantaa ja kehitystä.

Lähteet

Advania n.d. Identiteetin- ja pääsynhallinta (IAM). Viitattu: 21.3.2025. https://www.advania.fi/palvelumme/tietoturva/iam

Auxility 2024 25 Years of Active Directory. Viitattu: 5.3.2025. https://auxility.be/25-years-of-active-directory/

Finferries n.d. FinFerries työnantajana. Viitattu: 21.3.2025 https://www.finferries.fi/meille-toihin/finferries-tyonantajana.html

Hassan Javed 2023 A Beginner's Guide to Windows Autopilot- A Streamlined Device Provisioning. Viitattu: 12.5.2025. https://techbullion.com/a-beginners-guide-to-windows-autopilot-a-streamlined-device-provisioning/

Identity Classes n.d. Ultimate OKTA Essential Training for Beginners. Viitattu: 15.4.2025. https://www.identityclasses.com/okta-training/

Marshall Anne Busbee 2021 What is Workspace ONE Intelligent Hub? Viitattu: 18.4.2025. https://blogs.vmware.com/euc/2021/04/what-is-workspace-one-intelligent-hub.html

Microsoft 2024a DNS and AD DS. Viitattu: 12.5.2025. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/dns-and-ad-ds

Microsoft 2024b Overview of Windows Autopilot. Viitattu: 12.2.2025. https://learn.microsoft.com/en-us/autopilot/overview

Microsoft 2025a Compare self-managed Active Directory Domain Services, Microsoft Entra ID, and managed Microsoft Entra Domain Services. Viitattu: 17.3.2025. https://learn.microsoft.com/en-us/entra/identity/domain-services/compare-identity-solutions

Microsoft 2025b What is Microsoft Entra ID? Viitattu: 15.3.2025. https://learn.microsoft.com/en-us/entra/fundamentals/whatis

Microsoft 2025c Active Directory Domain Services overview. Viitattu: 10.3.2025. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft n.d. Microsoft Entra ID. Viitattu: 15.3.2025. https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id

Microsoft n.d. Microsoft Entra plans and pricing. Viitattu: 17.3.2025. https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing

Microsoft n.d. Windows Autopilot. Viitattu: 12.5.2025. https://www.microsoft.com/fi-fi/microsoft-365/windows/windows-autopilot

Okta n.d. Okta Directory Integration – An Architecture Overview. Viitattu: 24.4.2025. https://www.okta.com/resources/whitepaper/ad-architecture/

Okta, 2025a. What is Okta and What Does Okta Do, Viitattu: 15.4.2025. https://support.okta.com/help/s/article/what-is-okta?language=en_US

Okta 2025b Multi-Factor Authentication (MFA) on the Okta Help Center. Viitattu: 15.4.2025. https://support.okta.com/help/s/article/multi-factor-authentication-mfa-on-the-okta-help-center?language=en_US

Okta 2024 Understanding user access management (UAM). Viitattu: 15.4.2025. https://www.okta.com/identity-101/user-access-management/

Okta n.d. User Management. Viitattu: 15.4.2025. https://www.okta.com/products/user-management/

Okta n.d. Get access to Okta’s Demo library. Viitattu: 15.4.2025. https://www.okta.com/uk/resources/demo-library/

Omnissa n.d. Workspace ONE UEM. Viitattu: 17.4.2025. https://www.omnissa.com/products/workspace-one-unified-endpoint-management/

Omnissa n.d. Workspace ONE Cloud Services Security. Viitattu: 17.4.2025. https://techzone.omnissa.com/resource/workspace-one-cloud-services-security

Omnissa 2023 What is Omnissa Workspace ONE: Key Features and Benefits. Viitattu: 17.4.2025.

https://www.wwt.com/article/what-is-omnissa-workspace-one-key-features-and-benefits

Omnissa n.d. What Is Workspace ONE Unified Endpoint Management (UEM). Viitattu: 19.4.2025. https://techzone.omnissa.com/resource/what-workspace-one-unified-endpoint-management-uem

Quest n.d. What is Active Directory and how does it work? Viitattu: 17.3.2025. https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx

RootDSE 2021 Active Directory Fundamentals (Part 1)- Basic Concepts. Viitattu: 18.4.2025. https://rootdse.org/posts/active-directory-basics-1/

Secure Cloud n.d. Okta – Identity Platform. Viitattu: 21.5.2025 https://securecloud.fi/okta/

Softlanding 2024 Windows Autopilot: What Is It and How to Use It to Deploy New Devices Securely. Viitattu: 12.5.2025. https://www.softlanding.ca/blog/windows-autopilot-what-is-it-and-how-to-use-it/

Vijay Kanade 2025 What Is Active Directory? Working, Importance, and Alternatives. Viitattu: 5.3.2025. https://www.spiceworks.com/tech/networking/articles/what-is-active-directory/