TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Arvutisüsteemide Instituut

Sten Juhanson 093531IASB

KATALOOGITEENUSE ÜHENDAMINE PILVEKESKKONNAGA

Bakalaureusetöö

Juhendaja: Vladimir Viies
PhD

Tallinn 2019

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Sten Juhanson

20.05.2019

Bakalaureusetöö ülesanne

Üliõpilane: Sten Juhanson

Üliõpilaskood: 093531IASB

Lõputöö teema eesti keeles: Kataloogiteenuse ühendamine pilvekeskkonnaga

Lõputöö teema inglise keeles: Connecting Active Directory with Cloud

Teema päritolu: Töökohast tulenev vajadus ühendada lähitulevikus organisatsiooni identiteedid pilvega

Juhendaja (töökoht, teaduslik kraad, nimi, allkiri): Dots. Vladimir Viies, Tallinna Tehnikaülikool, Arvutisüsteemide instituut, PhD

Lahendatavad küsimused ning lähtetingimused: Anda ülevaade pilvekeskkondadest, võimalustest kataloogiteenuse identiteetide ühendamisest pilvekeskkonda. Koostada juhend identiteetide ühendamiseks ning realiseerida näidislahendus.

Eritingimused: Bakalaureusetöös käsitletakse kataloogiteenuse ühendamist Microsoft Azure'i keskkonnaga ning teiste pilveteenuse pakkujate lahendusi ei käsitleta.

Nõuded vormistamisele: Vastavalt Arvutisüsteemide instituudis kehtivatele nõuetele

Bakalaureusetöö esitamise tähtaeg: 20.05.2019

Annotatsioon

Bakalaureusetöö eesmärgiks on kohaliku kataloogiteenuse identiteetide ühendamine pilvekeskkonnaga. Antakse lühiülevaade pilvekeskkondadest, nende mudelitest ja liikidest. Töö kirjeldab erinevaid identiteetide haldamise võimalusi Microsoft Azure'i pilvekeskkonnas. Analüüsides kõiki võimalusi on koostatud juhend organisatsiooni kataloogiteenuse ühendamiseks Microsoft Azure'i pilvekeskkonna aktiivse kataloogiga.

Töö esimeses osas on ülevaade pilvekeskkondadest, nende mudelitest, turvalisusest ja teenuse hinna kujunemisest. Teises osas vaadeldakse identiteetide haldust kohalikus aktiivses kataloogis ning pilvekeskkonnas. Täpsemalt on kirjeldatud erinevaid ühendamise võimalusi aktiivse kataloogi ja pilvekeskkonna vahel. Viimases osas on teostatud organisatsiooni jaoks juhend, kuidas ühendada lokaalne identiteedihaldus Microsoft Azure'i aktiivse kataloogiga.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 38 leheküljel, 5 peatükki, 14 joonist, 2 tabelit.

Abstract

Connecting Active Directory with Cloud

Mobility and accessing to data from all over the globe is getting more and more important. Cloud computing has growing significantly fast and new applications and solutions are developed every day. The reliability of uptimes, security and price is really competitive comparing with organizations own datacenters. This is forcing organizations to abandon their own infrastructure and start moving their services into cloud. Moving to new environment brings up new situation where they have to deal the identity management in a different way.

The aim of this thesis is to connect local active directory with cloud active directory. Analyzing different solutions to integrate two environments and provide the instructions for connecting active directory with cloud environment.

This thesis describes connecting active directory with Microsoft Azure environment and not analyzing any other provider's solutions. In the first part there is an overview of cloud computing models, security and how the price develops. Introducing different cloud environments: Amazon Web Services, Microsoft Azure and Estonian Government Cloud.

The second part of this thesis gives an overview of managing identities local and in cloud environments. Detailed description and analyze on different connections methods to connect on-premises identities into Microsoft Azure. Connection models which are covered in the second part:

- Azure Cloud Only model
- Azure Synchronized model
- Azure Federated model
- Azure Pass-Through Authentication model

Third part of this thesis is describing organizational requirements, their fulfillment and realization of connecting the active directory with Azure Active Directory with suitable solution. The chosen connection method was Azure Pass-Through Authentication Model based on organization requirements. They wanted to maintain their own domain controller, get fast solution, no additional cost for infrastructure and that user passwords are not synchronized into cloud.

Based on the chosen solution the step-by-step instruction was created by fulfilling the connection model prerequisites. Manual is divided into two bigger parts. First one is installing the Microsoft Azure Active Directory Connect software and in the second part there is provided setup wizard step-by-step choices.

As a result of this thesis different organizations with their own requirements for identity management are able to make their own suitable choice to connect their active directory with Microsoft Azure. Organizations with identical requirements as used in this thesis can use the provided instruction to connect their on-premises identities with Microsoft Azure Active directory.

The thesis is in Estonian and contains 38 pages of text, 5 chapters, 14 figures, 2 tables.

Lühendite ja mõistete sõnastik

AD	Microsofti aktiivne kataloog
AD DS	Microsofti aktiivse kataloogi domeeni teenus
AD FS	Microsofti aktiivse kataloogi födereeritud teenus
AWS	*Amazon Web Services*
Cloud bursting	Hübriidpilve võimekus lokaalsel taristul nõuda ressursi puudusel avalikust pilvest lisa ressurssi
Custom domain names	Kohandatud domeeninimi
DNS TXT	Nimelahendusteenuse tekstikirje
IaaS	Infrastruktuur teenusena
ISKE	Infosüsteemide kolmeastmeline etalonturbe süsteem
Marketplace	Veebipõhine ostuplatvorm
MX kirje	E-maili vahetuse kirje nimeserveris, mis on vajalik e-mailide transpordiks
Pay-as-you-go	Maksa kasutatud teenuste eest
Reservations	Reserveeritud ressurss
SQL	Andmebaas struktuurse päringukeelega
Synchronized	Sünkroniseeritud
User administrator	Roll Azure'i keskkonnas, mis annab õiguse kasutajakontosid hallata
PaaS	Platvorm teenusena
SaaS	Tarkvara teenusena
Global administrator	Roll Azure'i keskkonnas, mis annab globaalsed haldamisõigused

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Järjest enam on olulisemaks muutumas mobiilsus ning andmetele mugav ülemaailmne ligipääs. Pilvekeskkondade areng on viimasel aastakümnel olnud väga kiire ning uusi lahendus tekib juurde igapäevaselt. Käideldavuse, turvalisuse ja hinna suhe võrreldes ettevõtete enda andmekeskustega on muutunud konkurentsivõimelisemaks. See kannustab pilvekeskkondade järk-järgulist kasutuselevõttu ning oma taristust loobumist. Selle tõttu tekib olukord, kus organisatsioon peab hakkama tegelema identiteetide haldusega uutmoodi.

Bakalaureusetöö eesmärgiks on kohaliku kataloogiteenuse identiteetide ühendamine pilvekeskkonnaga. Uuritakse erinevaid ühenduse võimalusi pilvekeskkonnaga ning koostatakse juhend kataloogiteenuse ühendamiseks pilvekeskkonnaga.

Töös kirjeldatakse kataloogiteenuse ühendamist Microsoft Azure'i keskkonnaga ning teiste pilveteenuse pakkujate lahendusi ei käsitleta. Esimeses osas on ülevaade pilvekeskkondade mudelitest, turvalisusest ja teenuse hinna kujunemisest. Tutvustatakse Amazon Web Services, Microsoft Azure'i ja Riigipilve pilvekeskkondi.

Teises osas vaadeldakse identiteetide haldust kohalikus aktiivses kataloogis ning pilvekeskkonnas. Täpsemalt on kirjeldatud erinevaid ühendamise võimalusi aktiivse kataloogi ja pilvekeskkonna vahel. Analüüsitakse nende erinevusi ning teostamise keerukust.

Viimases osas on koostatud organisatsiooni jaoks juhend, kuidas ühendada lokaalne identiteedihaldus Microsoft Azure'i aktiivse kataloogiga. Juhendi koostamisel on lähtutud konkreetse organisatsiooni lähtetingimustest.

2 Pilvandmetöötlus

Pilvandmetöötluse areng on viimasel kümnendil teinud suure sammu laialdaseks kasutuselevõtuks. Põhjusteks saab tuua kasutusmugavuse paranemise, dokumentatsiooni põhjalikkuse, kuluefektiivsuse, ligipääsetavuse. Kokkupuude pilveteenustega toimub märkamatult igapäevaselt, kasutades selleks e-posti teenuseid, failivahetuskeskkondi. Leidub üha enam ettevõtteid, kes ei näe enam otstarvet omada lokaalseid servereid ja serveriruume. Asutused saavad viidata haldusmugavusele, kokkuhoiule, mis tekib ruumide rendist, jahutamisest ja riistvara järjepideva uuendamise lõpetamisest.

Pilvandmetöötluse eelised on võimalus teha kiireid muudatusi, vaba ligipääsetavus üle maailma interneti olemasolul ning ka kõrgkäideldavuse tagamine. Süsteemidele suudetakse tagada väga kõrge käideldavus, olenevalt teenusepakkujast 99.99% ja 99.9%. Selle tagamiseks saab iga teenuse kasutaja valida omale vastava paketi. Võimalik on teenus dubleerida mitme andmekeskuse vahel ning ka geograafiliselt eraldada. [1], [2]

Järgmiseks eeliseks on hind, mis on pilvandmetöötluse puhul väga paindlik. Erinevalt füüsilistest lokaalsetest ettevõtete andmekeskustest, kus tuleb soetada riistvara täies mahus, tuleb pilvekeskkondades maksta ainult kasutatud ressursside eest. Eriti efektiivne on see suurte ja ajutiste projekti puhul, kus on lühiajaliselt vaja omada suurt arvutusjõudlust või teha andmetöötlust. Renditakse ressurss pilvest ning peale töid see vabastatakse, tasudes ainult kasutuse eest. [3]

Jagatud ressursse kasutades toetatakse energiasäästlikumat keskkonda. Tänu optimeeritud ja kalkuleeritud kasutusele ei pea iga ettevõte ehitama juurde eraldi ruume, neid jahutama ja kulutama elektrienergiat riistvara töös hoidmiseks. Üha enam toimub innovatsioon kokkuhoiu ja keskkonna vaates, kus kombineeritakse suurim arvutusjõudlus väikseima energia kuluga. Heaks näiteks on katsetused Microsofti merealustest andmekeskustest, kus kasutatakse taastuvenergiat. [3], [4]

2.1 Erinevad pilve liigid ja mudelid

Pilvandmetöötlusest ei leia ühte konkreetset pilvtöötlusmudelit, mis oleks sobilik kõigile. Selleks on kasutusel neli erinevat mudelit: privaat-, hübriid-, kommuunpilv ja avalik pilv. Lisaks erinevatele kasutatavatele pilve mudelitele saab nende kõigi peal kasutada kolme teenusemudelit: IaaS, PaaS ja SaaS. [5], [6]

Enim kasutatav on avalik pilv, sest see on kõige lihtsamini kättesaadav. See on avalikult veebilehe kaudu ligipääsetav kõigile ning peale kasutajakonto loomist on võimalik kohe teenust kasutada. Sellisel juhul jagab teenusepakkuja kõik ressursi tellijate vahel ning tarbijat maksustatakse kasutuse eest. Eelistena saab selle tüübi puhul välja tuua teenuse madala kulu, sest tellija ei osta omale riistvara, tarkvara ja makstakse ainult kasutuse eest. Puudub vajadus käsitsi uuendustele, sest platvormiomanik teeb need ise. Kõrge töökindlus ehk teenusepakkuja omab taristut mitmetes asukohtades ja on võimalik teenuseid dubleerida. Miinustena saab välja tuua oma taristu täieliku kontrolli puudumise – kõik on teenusepakkuja oma. Pakutakse ainult standardselt saadaolevat ressurssi. Andmete asukohast on teada ainult, millises andmekeskuses need on, aga täpsemat infot ei anta. Sellisteks teenusepakkujateks on näiteks Amazon Web Services ja Microsoft Azure. [5]–[7]

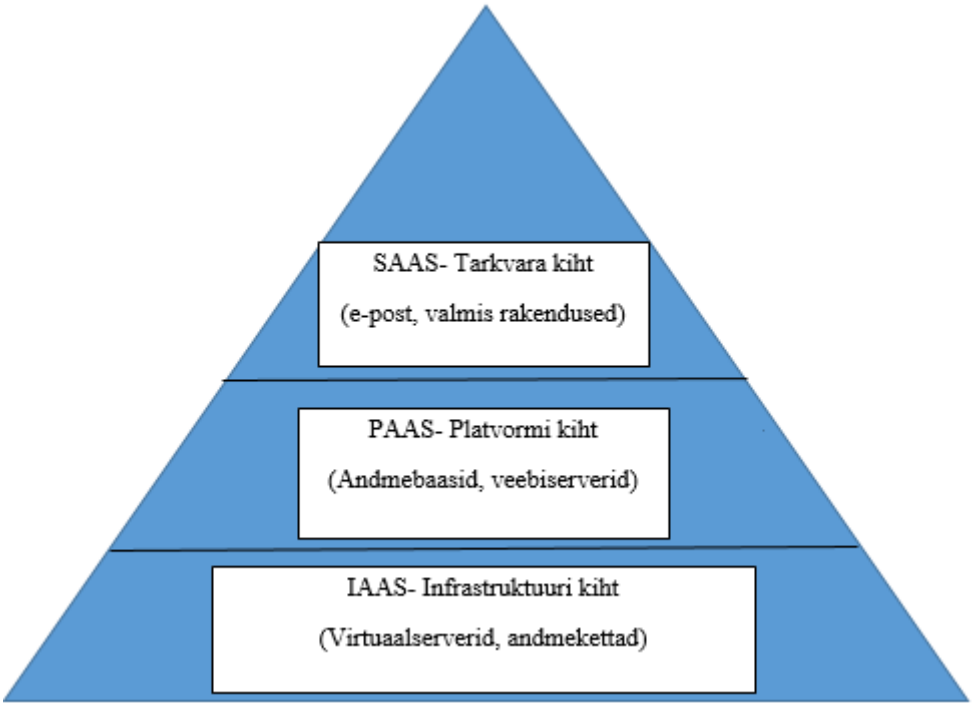
Privaatpilv on mõeldud kasutuseks kindlale organisatsioonile, mille ressursile ei ole teistel võimalik ligi pääseda. Füüsiliselt asub see ettevõtja enda juures või majutatakse kolmanda osapoole ruumides. Kuna sellisel juhul on kõik enda kontrolli all, siis on alati võimalik teha muudatusi riistvara ja ressursside tasemel, mis on aga kulukam. Võrreldes avaliku pilvega on privaatpilv turvalisem, sest kasutajate arv on piiratud ja teada on, kus andmed täpselt asuvad. [7]

Kommuunpilve infrastruktuuri jagavad ühiste huvidega, eesmärkidega organisatsioonid, kogukonnad. Sellise platvormi puhul kontrollib ja juhib kommuun seda ise. Selline mudel vähendab riske, mis võivad esineda avalikus pilves. Küll aga ei ole selline mudel nii kulukas kui privaatpilv. [6], [7]

Hübriidpilv on kombinatsioon kommuunpilvest, privaatpilvest või avalikust pilvest. Sellise lahenduse puhul on võimalik kombineerida erinevate pilvede paremaid omadusi. Näiteks hoides privaatseid andmeid ja ärikriitilisi teenuseid privaatpilves ning avalikkusele kättesaadavat avalikus pilves. Hübriidpilv võimaldab kasutada *Cloud*

Burstingut, mis tähendab, et privaatpilve ressursside limiidi korral võetakse kasutusele avalikust pilvest lisa ressurss, et rahuldada nõutud arvutusjõudlus. Sellise keskkonna näide on Eesti riigipilv, mis omab enda infrastruktuuri ning kasutusel on lisaks veel avalikke pilvi ja andmesaatkondi. [6]–[9]

Kolme teenusemudelit (Joonis 1) kasutades on kasutajal võimalus valida, kui palju soovitakse ise hallata ja milline osa jääb teenusepakkuja teha.



Joonis 1. Pilvteenuse teenusmudelid.

Kolme teenusmudelit lähemalt vaadates, moodustavad need kihilise struktuuri, mille alumine osa moodustab laiema, fundamentaalsema osa, milleks on IaaS. Keskmine osa on platvorm PaaS ja ülemine kiht on tarkvara osa SaaS, mis on kasutaja jaoks valmis toode ning toimib juba teenusepakkuja poolt eelseadistatud taristul.

IaaS (Infrastructure as a Service) ehk pilv kui infrastruktuuri mudel. Selle puhul on võimalik kasutajal luua oma vajadusele vastav konfiguratsioon taristu tasemel. Alumises kihis saab kasutaja teha virtuaalse liidese vahendusel valikuid virtuaalserverite, kõvaketaste, võrguliideste vahel, mille eest vastutab teenusepakkuja. Tellija peab paigaldama soovitud operatsioonisüsteemi ning vajalikud teenused. Selline mudel sobib kasutajale, kes soovib suurt valikuvabadust. Võimalus on konfigureerida, paigaldada tarkvara vastavalt oma soovidele valitud infrastruktuurile, kus saab teha hilisemaid

muudatusi. Selle tulemusena on IaaS mudel kasutuse ja hinna suhtes kõige paindlikum. See mudel toetab ka kõigi järgmiste mudelite rakendamist. [7]

Järgmisena on IaaS kihi peal PaaS (Platform as a Service) ehk platvorm kui teenuse mudel. Selle variandi puhul saab kasutaja lisaks riistavarale juba kasutamiseks valmis andmebaasid, arendamise keskkonnad ja teenused, mille peale saab kasutaja luua enda rakendused. Sellise mudeli kasutamise puhul vastutab teenusepakkuja nii riistvara kui ka platvormi eest. PaaS võimaldab kiirelt püsti panna tarkvaraarenduskeskkonna, mis ei nõua lisainvesteeringuid taristule ning seetõttu on see sobilik alustavatele iduettevõtetele ja tarkvaraarendajatele. Tasutakse kasutatud andmemahu, arvutusjõudluse, võrguliikluse eest. [7]

SaaS (Software as a Service) mudel põhineb ainult tarkvaral. See on püramiidi tipp, milles kasutaja saab kasutada tarkvara, mis töötab teenusepakkuja taristus. Muudatuste tegemise võimalused on piiratud rakenduse siseselt. Kasutatavad on rakendused kõikjalt ning need töötavad otse veebibrauseris. [7]

2.2 Pilvtöötluse teenusepakkujad

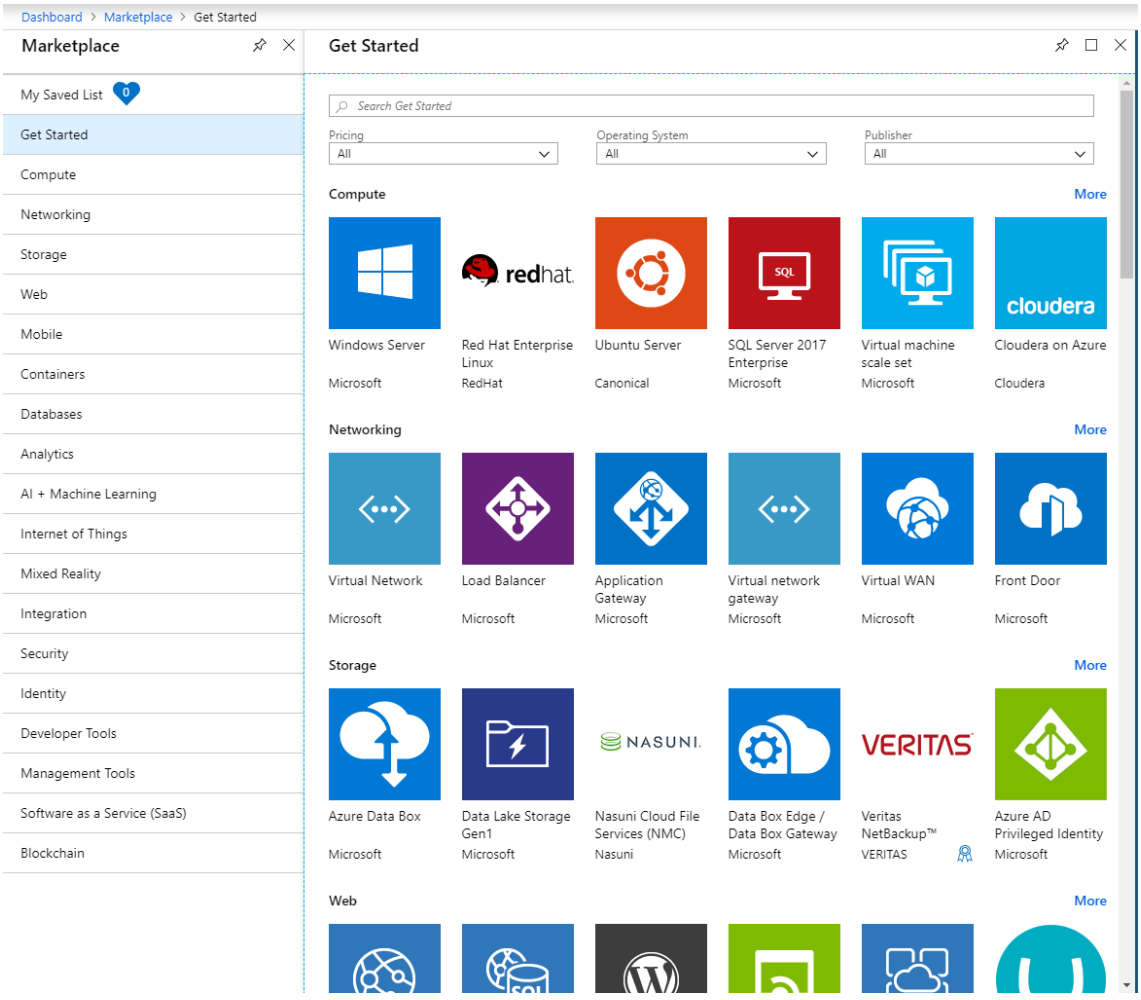
Tänu laialdasemale pilveteenuste kasutuselevõtu ja levikuga, suurenevad ka teenusepakkujate poolt pakutavad võimalused. Platvorme täiendatakse jooksvalt ning proovitakse kohaneda kasutajate soovidega ning pakkuda enda platvormil kõike, mida kasutaja soovib. Sobivaima teenusepakkuja peab valima klient, võttes arvesse vajadusi, pakutavat teenust ja hinda.

2.2.1 Microsoft Azure

Microsoft Azure on Microsofti poolt loodud pilv, keskkond avalikustati 2010. Algust tehti keskkonnaga Windows Azure, aastal 2014 sai see nimeks Microsoft Azure. Selle käigus teavitati, et see peegeldab ettevõtte uut strateegiat, kus keskendutakse avaliku pilve ja enda pilveteenuste, näiteks Office 365, Skype, Onedrive arendamisele. [10]

Microsoft Azure toetab nii IaaS, PaaS kui ka SaaS mudeleid. Tänapäevase populaarse agiilse arenduse põhjal toimib ka Azure, igapäevaselt tuleb juurde uusi võimalusi ja kõrvaldatakse teadaolevaid vigu. Nii lisatakse jooksvalt valikutesse uusi operatsioonisüsteeme, arendamise tööriistu, rakendusi ja teisi lahendusi.

Azure'iga alustamiseks on vaja ennast registreerida ning seejärel on olemas konto, millega on võimalik 30 päeva jooksul kasutada 170 eurot. Sisenedes Azure portaali *Marketplace* (Joonis 2) on võimalik saada ülevaade kõigist pakutavatest teenustest ning teha enda jaoks valik. Soovides püsti panna virtuaalserverit, on valikuvõimalusi väga palju. Näiteks tuleb seadistada regioon, millises andmekeskuses hakkab virtuaalmasin paiknema. Parameetritest mälumaht ja protsessori tuumade arv, lisaks veel andmekettad ja võrgukaart. Mõningad piirangud tulevad regioonide valikust, kuhu soovitakse virtuaalserver luua. [11]



Joonis 2. Microsoft Azure'i tootekataloog.

Kuna Azure on andmekeskustega üle maailma laiali, siis see võimaldab hoida andmeid kliendile lähemal ning sellega vähendada viiteid andmete liikumises ja päringute sooritamises. Hajutatus lisab võimaluse oma andmeid dubleerida mitte ainult mitme virtuaalserveri, vaid ka erinevate andmekeskuste vahel. Lisaks saab veel andmed eraldi regioonidesse paigutada. Sama kehtib ka andmete varundamise kohta. Sellised

lahendused on olulised neile, kes omavad kriitilise tähtsusega teenuseid, milles katkestused ei ole lubatud. Mitmes andmekeskuses andmete hoidmise eelis on, et Azure keskkonna uuendused tehakse andmekeskuste kaupa sama regiooni piires. See omakorda vähendab rakenduste katkestuse riski. Alles on jätkuvalt variant, kus varundust saab hoida samas andmekeskuses, mille eelis eelneva ees on odavam hind. [12]

2.2.2 Amazon Web Services

Amazon Web Services lühendatult AWS hakkas oma infrastruktuuri teenuseid veebiteenuste vormis pakkuma 2006. aastal, olles pilvandmetöötluse valdkonnas üks esimesi. Praeguseks on AWS kasvanud üheks suurimaks teenusepakkujaks, omades üle miljoni aktiivse kasutaja enam kui 190 riigis. Sarnaselt Azure'iga on leviku ja parima teenuse jaoks ka AWS andmekeskused erinevate maailmajagude vahel paigutatud. [13]

Ülesehitus on sarnane Microsoft Azure'i pilvekeskkonnaga, toetades kõiki pilveteenuse mudeleid. Niisamuti on ka AWS teenuste valik väga lai, igaüks leiab endale sobivaima lahenduse. Väikese erinevusena saab välja tuua, et AWS on oma loomisest alates rohkem toetanud vabavaraliste tarkvarade olemasolu enda platvormil.

2.2.3 Riigipilv

Riigipilv erineb eelnevatest selle poolest, et see on loodud Eesti riigi avaliku sektori jaoks. Riigipilve teenuse omanik on Riigi Infokommunikatsiooni Sihtasutus (RIKS) ja on arendatud koostöös eraettevõtetega Cybernetica AS, Dell EMC, Ericsson Eesti AS, OpenNode OÜ ja Telia Eesti AS. Eesmärgiks muuta avalikud teenused ühtlasemaks, kiiremaks ja mugavamaks. Selleks järgitakse kõrgeid turvanõudeid, Eesti digiühiskonna vajadusi ning soodustatakse riigiasutuste säästlikumat majandamist. [14]

Nii nagu ka kõik teised suuremad avalikud teenusepakkujad, võimaldab Riigipilv kasutada kolme pilveteenuste mudelit IaaS, PaaS ja SaaS. Läbi iseteeninduspordi saavad kliendid käivitada teenusepakkuja poolt erineva konfiguratsiooniga ettevalmistatud virtuaalservereid. Riigipilve käideldavuse tase on väga kõrge nagu eelnevalt kirjeldatud pilveteenusepakkujatel, milleks on 99.9%. PaaS teenuste pikemat loetelu ei ole avalikult kättesaadav, küll aga võib välja lugeda, et pakutakse näiteks X-tee turvaserveri teenuseid, VPN kanaleid, koormusjaotureid ja varunduse lahendusi. SaaS lahendusena on välja toodud võimalus tulevikus kasutusele võtta erinevaid raamatupidamis- ja dokumendihalduse lahendusi. [15]–[17]

Riigipilve taristu asub füüsiliselt Eesti pinnal. Nii nagu Azure ja AWS arendab ka Riigipilv oma andmekeskuseid mitmes asukohas. Üks neist asub Tallinnas ning dubleeriv keskkond on mujal Eestis. Lisaks on pikema eesmärgina plaan luua andmesaatkond väljaspool Eestit. [18]

2.3 Turvalisus

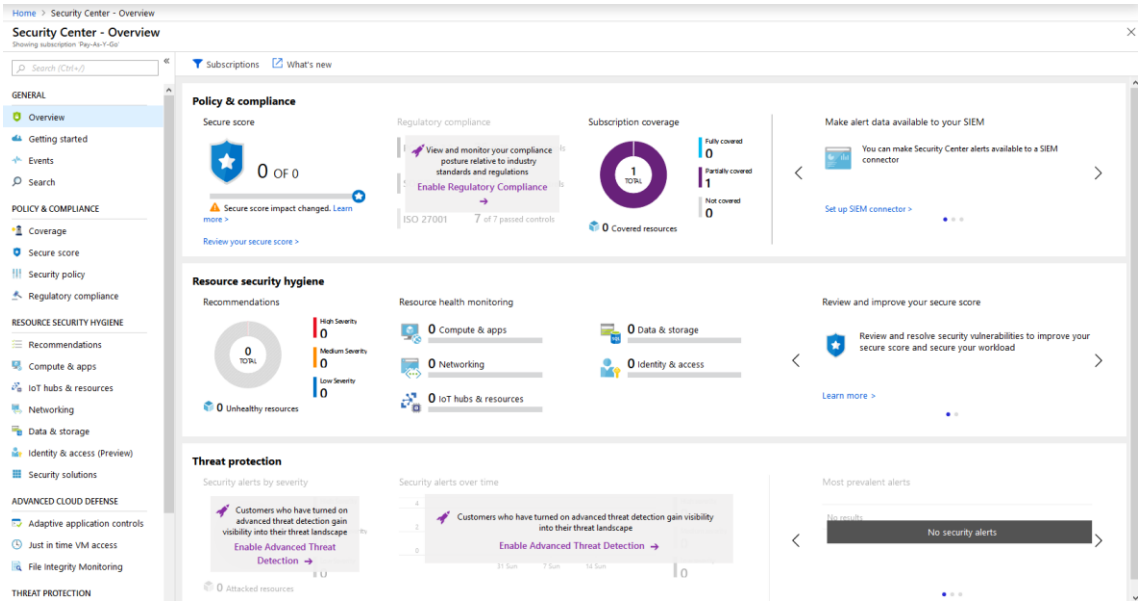
Järjepidevalt muutub olulisemaks andmete kaitse, privaatsus ja enda isiklike andmete üle kontroll. Isikuandmete kaitseks võeti 2016. aastal vastu isikuandmete kaitse üldmäärus. Sellest tulenevalt peavad ettevõtete poolt kasutatavad isikuandmed olema kontrollitavad ja vajadusel täielikult eemaldatavad oma infosüsteemidest. Kui enda taristus on andmete füüsiline asukoht teada, siis pilvekeskkondades see nii ei pruugi olla. Teada on andmekeskus, aga rohkemat teenusepakkujad ei täpsusta. [19]

Tihti jõuab avalikuse ette ka juhtumid paroolide leketest, infosüsteemidesse sissemurdmisest ja andmete vargusest. Selle vastu üritavad kõik pilvekeskkonnad pakkuda enda välja töödeldud kaitsemehhanisme. Nad sertifitseerivad ennast vastavalt rahvusvahelistelt tunnustatud sertifikaatidega, et tagada usaldusväärsus ja võimalikult turvaliste lahenduste pakkumine. Näiteks Azure'i puhul skaneeritakse internetis paroolilekkeid, kontrollitakse kahtlaseid autentimise katseid, mis ei vasta tavapärasele mustrile (Joonis 3). See omakorda vähendab tunduvalt lõppkasutaja kontode kaaperdamist. [20]

AWS pakub kasutajale lahendusena jagatud vastutust, kus teenusepakkuja vastutab pilve kui taristu turvalisuse eest. Kasutaja vastutada jääb enda loodud teenuste ja rakenduste sisene turvalisus. Riigipilv on üles ehitatud lähtudes ISKE kõrgeima klassi turvanõuetest, mis annab klientidele kindluse turvalisuse osas. Nii nagu AWS pakkus jagatud vastutust, kehtib sama ka Azure'i puhul. [20], [21]

Kõige olulisem on kasutajate ja ettevõtete jaoks nende andmed. Omades taristut, ollakse üldjuhul teadlikud, et andmeid tuleb hoida mitmes asukohas, et intsidendi korral oleks need taastatavad. Pilveteenuste puhul tuleb silmas pidada sama, sest on mitmeid variante kuidas ja kuhu varundada. Võimalus on teha koopiaid samasse pilvekeskkonda, sealt väljapoole, näiteks teise teenusepakkuja juurde või enda taristusse. Kindlasti tuleb vaadata erinevaid varundamise tingimusi. Näiteks võib endale olulise küll varundada, aga

seda tehakse samasse andmekeskussesse, mis ei pruugi tagada piisavat kaitset olulistele andmetele. [22]



Joonis 3. Microsoft Azure'i turvakeskuse ülevaade.

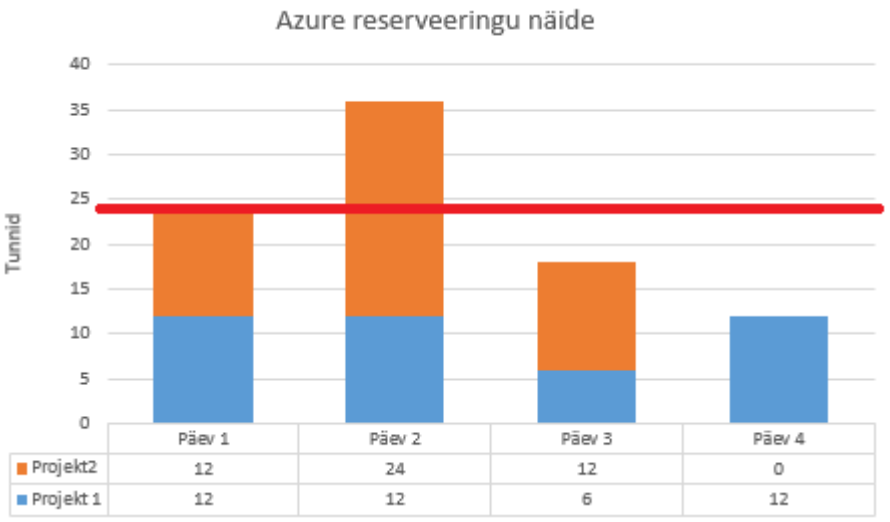
2.4 Teenuse hinnastamine

Kõik pilvandmetöötluse pakkujad rõhutavad rahalist kokkuhoidu ja keskkonna säästmist. Kliendi jaoks sõltub võimalik säästmine olemasolevast infrastruktuurist ning tulevastest vajadustest. Juhul, kui puudub olemasolev taristu, võiks kaaluda kohe kolimist väliste pilveteenusepakkujate juurde. Olenevalt kasutusvajadusest pakuvad pilveteenused erinevaid hinnastamis- ja kasutusvõimalusi.

Pay-as-you-go ehk maksa selle eest, mida oled kasutanud. Üldiselt peetakse tellitud ressursi üle arvet tunni täpsusega. Selline lahendus annab väga paindliku kasutusvõimaluse. Näiteks on vaja töös hoida virtuaalservereid 12 tundi päevas ja seda kindlatel kellaaegadel. Selle jaoks saab kasutaja luua enda automaatika, mis käivitab ja seiskab virtuaalserveri soovitud aegadel. Tänu sellele vähendatakse kulusid ning tasutakse ainult masina töötundide eest. Riigipilv hinnastab enda taristu teenust päeva täpsusega. [23]

Reservation ehk ressursi ostmine pikemaks perioodiks. Sellise variandi puhul tuleb tasuda ette terve virtuaalmasina hind aasta või enama eest, kokkuvõttes on see odavam. AWS

reklaamib seda kuni 75% ning Azure 72% odavamana kui pay-as-you-go. Näiteks Azure'i puhul on võimalik ühe reserveeritud virtuaalserveri puhul hajutada kulusid mitmete projektide vahel. Joonis 4 pealt näeme, et kasutatakse ühte virtuaalserveri reserveeringut, mida kasutab kaks projekti, need ei tööta ööpäevaringselt ning samaaegselt. Kõik, mis jääb ülespoole punast joont kuulub tasumisele pay-as-you-go järgi. [24]–[26]



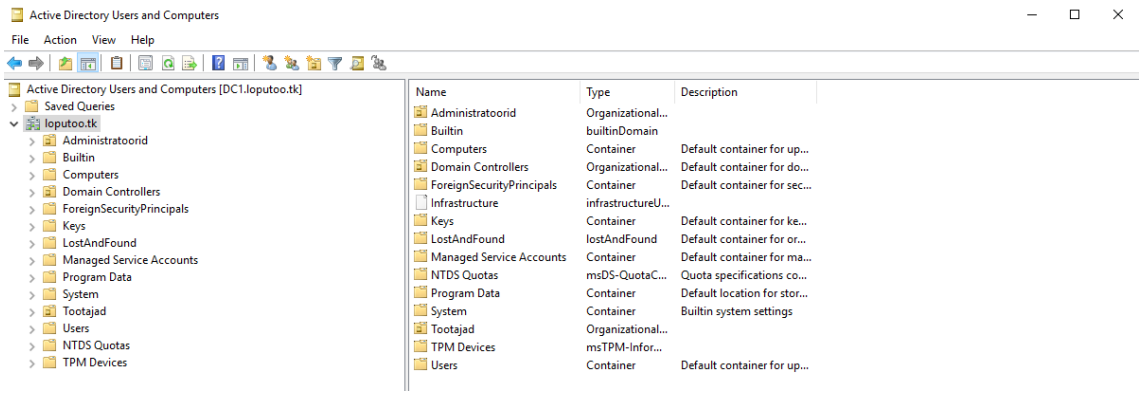
Joonis 4. Microsoft Azure ühe virtuaalserveri reserveering, mida kasutatakse kahe erineva projekti jaoks.

3 Kataloogiteenused

Infosüsteemide kasutajate ja objektide haldamiseks ning ülevaate saamise lihtsustamiseks kasutatakse eraldi kataloogiteenuseid. See võimaldab pidada arvet kasutajate üle ning hallata nende ligipääsuõiguseid. Nii nagu on kasutuses kohalikud kataloogiteenused, on need olemas ka iseseisvalt erinevates pilvekeskkondades. Seega on nad täiesti isoleeritud ning lokaalse taristu identiteetidega puudub neil seos. Kui organisatsioon otsustab kasutusele võtta pilvekeskkonna ning soovib säilitada kohaliku kataloogiteenuse kasutajate autentimist, on vaja selleks luua eraldi ühendus pilve identiteedihaldusega. Sellisele kasutusvaldkonnale vastavad enamasti SaaS mudelid

3.1 Active Directory Domain Services

Windows Active Directory Domain Services ehk aktiivse kataloogi domeeni teenus paigaldatakse lokaalselt domeeni kontrollerile. AD DS hoiab endas informatsiooni kasutajate, arvutite, gruppide, objektide kohta (Joonis 5). Selle läbi saab luua struktuurselt ja hierarhiliselt üles ehitatud organisatsiooni, mille haldamist lihtsustab turvalisusgruppide ja ressursside loomine. Ressurssideks on füüsilised seadmed nagu arvutid, printerid, serverid. Turvalisuse printsiibiks on arvutite kontod, kasutajate kontod, kasutajate grupid, millele omistatakse unikaalsed turvalisuse identifikaatorid. Läbi nende saab välja jagada ligipääsuõiguseid ja delegeerida neid teistele organisatsiooni kasutajatele. Minimeeritakse vajadus arvutis või infosüsteemis igakordsete personaalsete ligipääsude jagamine, sellega vähendatakse administraatori haldamise koormust. [27]



Joonis 5. Domeeni loputoo.tk Active Directory.

3.2 Azure Active Directory

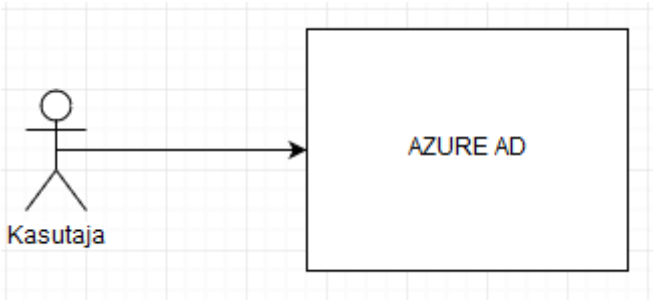
Azure Active Directory on pilvepõhine Microsoft Azure'i identiteedi ja ligipääsu haldussüsteem, milles saab luua uusi kasutajaid, gruppe, hallata ligipääsutingimusi. Kuna Azure'i keskkonnas on teenused *subscription* piires, siis saab läbi Azure AD jagada erinevaid SaaS litsentse, näiteks Office365 omasid. [28]

Azure AD Free puhul on võimalik luua kataloogi kuni 500 000 objekti ning kuni kümne rakenduse jaoks ühekordne sisse- ja väljalogimine. Lisaks tasuta tasemele on olemas veel tasulised: Basic, Premium P1 ja Premium P2, hinnavahemikuga 0.844 kuni 7.590 eurot kuus kasutaja kohta. Need võimaldavad kasutada lisa turvalahendusi, näiteks kaheastmelist autentimist, mobiilsete seadmete haldust, piiramatut objektide arvu kataloogis. [28], [29]

Organisatsioonid, kellel on kasutusel lokaalne kataloogiteenus ning soov kasutusele võtta Microsoft Azure'i pilvekeskkonna teenuseid, tuleb otsustada kuidas hallata ligipääsusid tulevikus. Variantideks on identiteet pilves ja lokaalses taristus ehk kasutajal on mitu kasutajanime ja parooli või ühendada oma kataloogiteenus Azure AD omaga ning luua hübriidne keskkond, milles on kasutusel üks identiteet.

3.2.1 *Cloud Only* ehk ainult Pilv

Cloud Only nimi viitab, et tegemist on ainult pilve identiteediga. Sellise mudeli puhul toimub kõik autentimisega seonduv pilvekeskkonnas (Joonis 6). Ühtegi kasutajat sellise mudeli puhul lokaalsest aktiivsest kataloogist ei sünkroniseerita. Kasutajaid ja gruppe loob selleks vähemalt *user administrator* rolliga Azure AD administraator. Selline mudel sobib enamasti organisatsioonidele, kes plaanivad oma taristust loobuda või ei ole veel loonud oma lokaalset kasutajate ja ressursside haldamise süsteemi. Eelistena saab välja tuua lihtsa haldamise, kõik identiteedid ühes kohas. Pole vaja luua lisa servereid ja teenuseid, säästes sellega ressursse. Juhul kui omatakse ka lokaalset kataloogiteenust ning luuakse Azure AD lisakontosid, tuleb kasutajatel pidada meeles erinevaid kasutajatunnuseid ja paroole. [30]

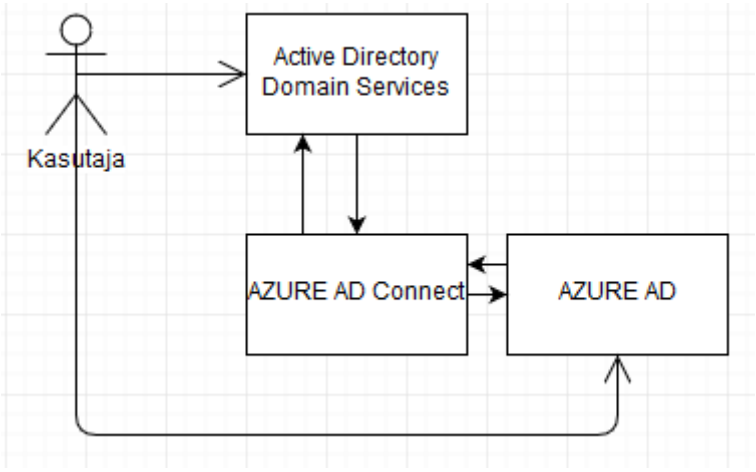


Joonis 6. Kasutaja autentimine Cloud Only mudeliga.

3.2.2 *Synchronized* ehk Sünkroniseeritud mudel

Synchronized mudeli puhul on tegemist lokaalse aktiivse kataloogi ja Azure AD identiteetide sünkroniseerimisega. Ühenduse loomiseks kasutatakse Microsofti poolt pakutavat Azure AD Connect tarkvara, mis paigaldatakse domeeni kontrollerile või eraldi serverile, millel on ligipääs aktiivsele kataloogile ja asub sellega samas domeenis. [31], [32]

Sünkroniseerimise autoriseerimiseks kasutatakse erealdi teenuskontot. See kontrollib määratud intervallidega muutusi ning regulaarselt sünkroniseerib lokaalsest kataloogiteenusest kasutajaid pilve koos nende parooli räsiga (Joonis 7). Seega sellise mudeli puhul on nii lokaalsed kui ka pilves olevad kasutajanimed ja paroolid samad. See lihtsustab kasutajate haldamist, piisab tegevustest ainult ühes keskkonnas. Kasutajatele on võimalik seadistada ühekordne sisse- ja väljalogimine. Kõrge käideldavuse tagamiseks tuleks paigaldada Azure AD Connect rohkemale kui ühele serverile. Sünkroniseeritud meetodi puhul tuleb arvestada ka organisatsioonide turvanõudeid, mõnes võib olla keelatud paroolide sünkroniseerimine. Lisaks sellele tuleb silmas pidada, et lokaalses aktiivses kataloogis suletud kasutajat ei suleta automaatselt Azure AD keskkonnas, selle jaoks tuleb luua eraldi skript või tööprotsess. [31], [32]



Joonis 7. Sünkroniseeritud mudel, kus kasutaja identiteet on nii lokaalses aktiivses kataloogis kui ka Azure AD keskkonnas sama. Sünkroniseerimine läbi Azure AD Connecti.

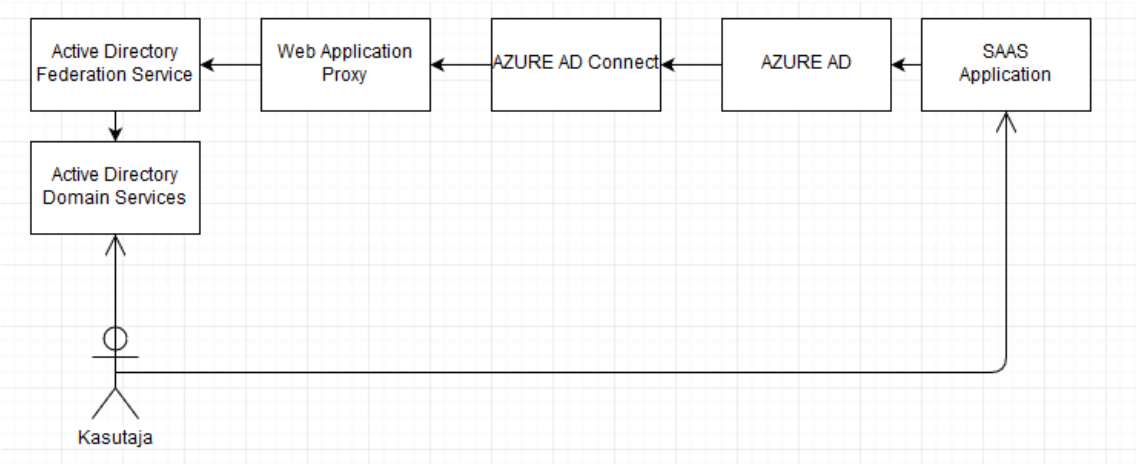
3.2.3 *Federated* ehk Födereeritud mudel

Aktiivse kataloogi födereeritud teenuse eesmärgiks on luua ühekordne sisse- ja väljalogimine ja lubada veebipõhine autentimine. Selle jaoks on vajalikud ka kolmandate osapoolte usaldatud sertifikaadid. AD FS meetodi minimaalne vajalike serverite hulk on: domeenikontroller aktiivse kataloogi domeeni teenusega, server aktiivse kataloogi födereeritud teenusega ja server veebirakenduse proksiga. Autentimisprotsess on kirjeldatud Joonis 8. Kõrge käideldavuse saavutamiseks on vaja dubleeritud servereid ja koormusjaoturit.

Alustades ühendusprotsessi läbi Azure AD Connecti, saab valida, kas kasutakse juba olemasolevaid AD FS servereid või loome need paigalduse käigus. Luues uut AD FS farmi, on meil vaja kolmanda osapoole sertifikaate ja tuleb valida kuhu teenus paigaldatakse. Paigalduse käigus on vajalik seadistada ka proksiserver, mis paistab välisvõrgust. Tuleb seadistada, millised serverid födereeritakse AD FS ja Azure AD vahel. Viimasena on vaja verifitseerida oma domeen ning selleks lisada oma välisesse nimelahendusteenusesse TXT või MX kirjed, mis on paigaldusviisardis toodud.

Liidendatud mudeli puhul on tegemist kõige kulukama ja keerukama ühendusmeetodiga. Vajalike serverite arv, omavaheliste ühenduste ja halduse keerukus on oluliselt suurem kui teiste võimalike variantide puhul. Samas tagab see võimekuse kasutada ühekordset sisse- ja väljalogimist ja lubada veebipõhist autentimist. Võimalus on integreerida erinevaid lahendusi, näiteks ID-kaardi ja SMART-ID autentimisi, teavitusi parooli

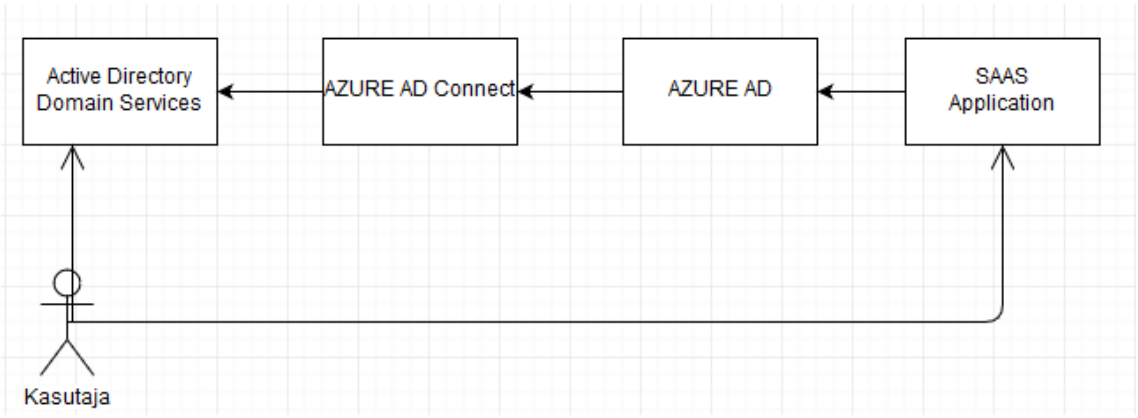
aegumisest Office365 portaalis. Selle meetodi puhul käib autentimine läbi kohaliku aktiivse kataloogi. Võimalik on seadistada paigalduse käigus paroolide räsi sünkroniseerimine. Sellega on võimalik tagada kohaliku taristu hävimise korral või ühenduse puudumisel aktiivse kataloogiga jätkuvalt kasutajate autentimine, sest paroole hoitakse ka pilves. [33]–[35]



Joonis 8. Födereeritud mudeli puhul hoitakse kasutaja identiteet kohalikus aktiivses kataloogis. Kasutaja autentimisel teenustesse või veebirakendustesse kontrollitakse läbi Azure AD Connecti, kas selline kasutaja eksisteerib lokaalses aktiivses kataloogis ning kas mandaat on olemas.

3.2.4 Pass-Through Authentication ehk läbipääsuga autentimine

Selline mudel on oma olemuselt üsna sarnane födereeritud mudeliga, võimaldades ühekordset sisse- ja väljalogimist, paroolide hoidmist ainult kohalikus aktiivses kataloogis. Kasutajatel on vaja meeles pidada ainult ühte kasutajanime ja parooli. Autentimisprotsess on näidatud Joonis 9.



Joonis 9. Pass-Through mudeli puhul hoitakse paroolid kohalikus aktiivses kataloogis ja tarkvara kui teenus kasutuse puhul käiakse küsimas paroolide õigust läbi Azure AD Connecti kohalikust aktiivsest kataloogist.

Erinevus peitub kasutuselevõtu lihtsuses. Kogu protsess on võimalik tööle panna ainult ühe domeenikontrolleri serveril, kus on ka aktiivse kataloogi domeeni teenus. Selleks on vaja Azure AD Connect tarkvara ning läbida paigaldusviisardi punktid. Selle käigus paigaldatakse serverile vajalikud sünkroniseerimise teenused ja SQL baas. Azure AD keskkonnas on vajalik oma domeeni kinnitamine, lisades TXT või MX kirje enda nimelahendusteenusesse.

Maksimaalse käideldavuse saavutamiseks peaks kasutama kahte eraldi domeenikontrollerit ja kahte eraldi serverit Azure AD Connect jaoks. Azure AD ja kohaliku aktiivse kataloogi vaheline suhtlus on turvatud sertifikaadi põhise autoriseerimisega, mida Azure AD uuendab automaatselt paari kuu tagant. Sellise lahenduse puhul on võimalik ka paroolide sünkroniseerimine Azure AD keskkonda. [36]

4 Kataloogiteenuse ühendamine pilvekeskkonnaga

Organisatsioon kuni saja töötajaga soovib kasutusele võtta Office365 tarkvara ja lubada ligipääs postkastidele üle interneti ning soov on leida parim lahendus hübriidsele identiteedihaldusele.

Organisatsioon on esitanud järgmised nõuded:

- Alles peab jääma praegune domeenikontroller
- Parooli räsisid ei hoita pilvekeskkonnas
- Kiire lahendus
- Lisakulutused taristule puuduvad

Organisatsiooni poolt on kasutusse antud vähendatud kujul testkeskkond. See koosneb ühest domeenikontrollerist, milles on olemas aktiivse kataloogi domeeni teenus ja nimelahendusteenus ning struktuur, mis vastab nende *live* keskkonnale (Tabel 1).

Tabel 1. Organisatsiooni poolt kasutusse antud testkeskkonna parameetrid.

DC (ADDS+DNS)	1x
CPU	2x CPU 3.7 GHz
RAM	4 GB

4.1 Sobiva lahenduse leidmine

Võttes arvesse organisatsiooni kriteeriumeid ja võimalikke lahendusvariante, mida käsitleti eelmises peatükis, leiame analüüsi käigus sobivaima lahenduse lokaalse aktiivse kataloogi ja pilvekeskkonna identiteetide ühendamiseks. Parima lahenduse leidmiseks on koostatud Tabel 2, milles on välja toodud olulised kriteeriumid organisatsioonile ja ühendusviiside vastavus tingimustele. Loodud Tabel 2 saab välja lugeda, et parim lahendus on kasutada Pass-Through Authentication mudelit.

Tabel 2. Võrdlustabel võimalikest lahendustest, lähtudes organisatsiooni peamistest nõuetest.

Ühenduse viis	**Kas paroole salvestatakse pilve?**	**Kas tekivad lisakulutused?**	**Kas alles jääb domeenikontroller?**	**Lahenduse kiirus**
Azure Cloud Only mudel	Jah	Ei	Võib jääda	Kiire
Azure Synchronized mudel	Jah	Ei	Jääb	Kiire
Azure Federated mudel	Ei	Jah	Jääb	Aeglane
Azure Pass-Through Authentication mudel	Ei	Ei	Jääb	Kiire

4.2 Ühenduse loomise eelnõuded Pass-Through Authentication meetodil

Selleks, et saaksime luua ühenduse lokaalse aktiivse kataloogi ja Azure Active Directory vahel, peavad olema täidetud järgmised tingimused:

- Azure Subscription
- Azure Active Directory
- Azure Active Directory *Global Administrator* rolliga kasutaja
- Verifitseeritud omanimeline domeen Azure Active Directorys
- Domeenikontroller serveril Windows Server 2008 või uuem
- Minimaalne vajalik võrguliiklus
- Lokaalne teenuskonto

Alustades esitatud nõuete täitmist algusest, tuleb esmalt minna Microsoft Azure'i portaali ning luua konto, seejärel logida sisse. Peale seda saab alustada Azure *subscription* loomist. Selleks tuleb sisestada portaali otsingulahtrisse sõna *subscriptions*, seejärel suunatakse lehele, kus kuvatakse olemasolevad lepingud. Uutel kasutajatel on nimekiri tühi, lisada on vaja uus *subscription*. Selle bakalaureusetöö lahenduse puhul on kasutatud pay-as-you-go varianti. [37]

Järgmise sammuna saab asuda Azure Active Directory eeldusi täitma. Peale uue *subscription* loomist on olemas ka kataloog kasutajate ja gruppidega. Automaatselt on tellimuse täitja Azure Active Directory kasutaja ning omistatakse roll *Global Administrator*, millega on võimalik hiljem seadistada Azure AD Connect. Hilisema haldamiskindluse tagamiseks, tuleb luua uus konto samade õigustega ehk teenuskonto, juhuks kui *subscription* tellija peaks organisatsioonist lahkuma. Vajalik on ka teenuskonto kohalikus aktiivses kataloogis, millel on õigus lugeda organisatsiooni kasutajaid ja gruppe, et jälgida võimalikke muudatusi objektide atribuutides. [38], [39]

Vaikimisi kasutab Azure Active Directory domeenina registreeritud kasutaja kasutajanime. Kuna soov on, et lokaalsed ja pilves asuvad identiteedid oleksid samad ehk domeeninimi ja parool jääksid samaks, siis selle tagamiseks tuleb lisada Azure'i keskkonda oma domeen. Selleks on Azure Active Directory's olemas menüü *Custom Domain names*. Sinna tuleb lisada soovitud domeeninimi, mille järel palutakse see kinnitada, lisades Azure'i poolt loodud TXT või MX kirje enda nimelahenduse teenussesse, mida saavad Microsofti serverid lugeda. [40]

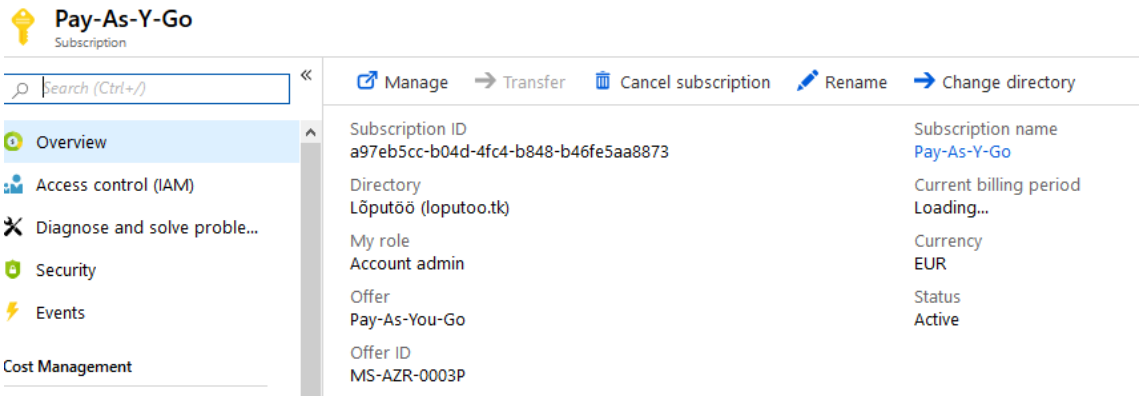
Uusima Azure AD Connecti paigaldamiseks on minimaalselt vaja ühte domeenikontrollerit või lisa serverit, mille operatsioonisüsteem on Windows server 2008 või uuem. [41]

Suhtluse Azure AD ja lokaalse aktiivse kataloogi domeeni teenuse vahel tagab Azure Active Directory Connect tarkvara. Selle jaoks on vaja lubada Azure AD Connecti paigaldatud serveris võrguliiklus väljapoole läbi tulemüüri portide 80 protokoll HTTP ja 443 protokoll HTTPS kaudu. [42]

4.3 Ühenduse Pass-Through Authentication eelnõuete täitmine

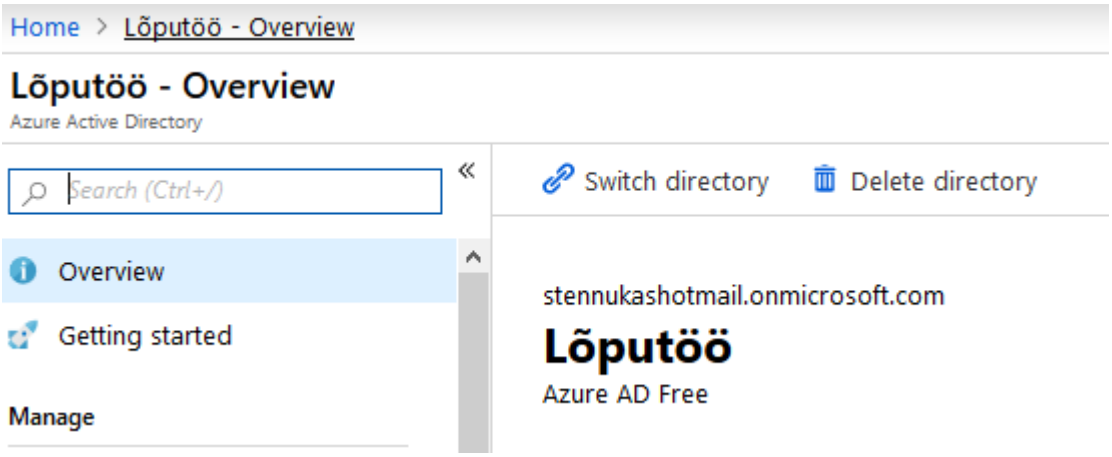
Eelmises peatükis 4.2 kirjeldatud eelnõuetest on organisatsiooni jaoks täidetud domeenikontrolleri olemasolu toetatud operatsioonisüsteemiga Windows Server 2016, millele on võimalik paigaldada Azure Active Directory Connect. Lisaks sellele on domeenikontrolleris lubatud väljapoole võrguliiklus portide 80 protokolli HTTP ja 443 protokolli HTTPS kaudu. Täidame ülejäänud vajalikud eelnõuded:

- Loome Pay-As-You-Go *subscriptioni* vastavalt peatükis 4.2 toodud kirjeldusele. Joonis 10 näeme loodud *subscriptioni* ja selle ID-d.



Joonis 10. Loodud Pay-As-You-Go *subscription.*

- Peale *subscriptioni* loomist on olemas esialgne Azure Active Directory. Domeeninimeks on stennukashotmail.onmicrosoft.com (Joonis 11), mis saadakse registreeritud konto kasutajanimest, mis on kirjeldatud peatükis 4.2.

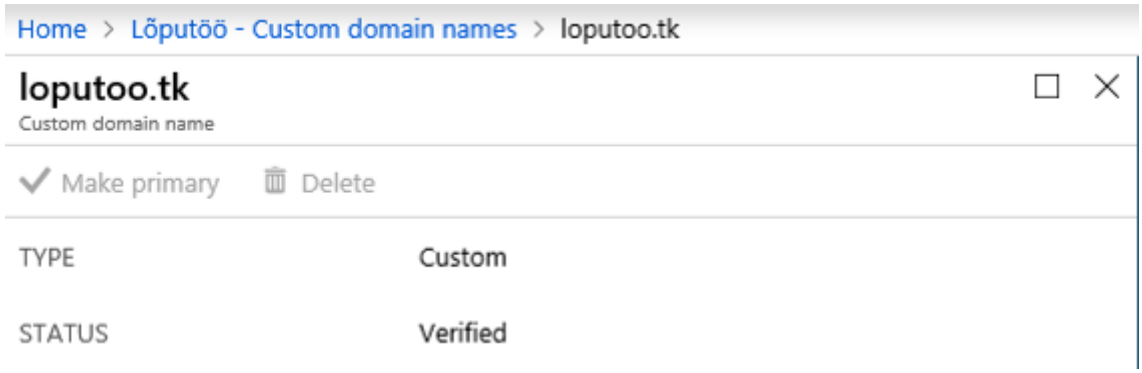


Joonis 11. Azure Active Directory domeeninimega stennukashotmail.onmicrosoft.com.

- Vajalik oli luua hilisema haldamise kindlustamiseks üks lisakonto, millel on *global administrator* õigused. Azure Active Directorys on tehtud konto „LocalAdmin“ ning omistatud *global administrator* õigused (Joonis 12).

Joonis 12. LocalAdmin konto Azure Active Directory’s.

- Kuna organisatsiooni domeeninimi on loputoo.tk, mida kasutatakse organisatsioonis kasutajate autentimisel, tuleb see registreerida ka Azure Active Directory jaoks. Selleks on lisatud vajalik TXT kirje välisesse nimelahendusteenusesse, mida saavad Microsoft serverid lugeda. Joonis 13 on näha enda lisatud domeeni loputoo.tk kinnitus.



Joonis 13. Kinnitatud lisatud domeen.

- Tekitasime domeenikontrolleris olevasse aktiivsesse kataloogi konto AzureADConnect, millel on õigus lugeda organisatsiooni kasutajaid ja gruppe. Sellega täideti peatükis 4.2 esitatud viimane eeltingimus.

4.4 Ühenduse loomine Pass-Through Authentication meetodil

Lähtudes eelnevas peatükis 4.3 täidetud eeltingimustele, koostas autor juhendi organisatsiooni kataloogiteenuse ühendamiseks pilvekeskkonnaga. See on jaotatud kahte suuremasse etappi, tarkvara paigaldamiseks ja seadistamiseviisardi läbimiseks.

Esmalt tuleb alla laadida Microsoft Azure Active Directory Connect tarkvara ja paigaldada serverile DC1.loputoo.tk. Peale esmase viisardi läbimist, mille käigus paigaldatakse mitmed eri komponendid, kontrollib tarkvara, kas on olemas varasemaid

sünkroniseerimisteenuseid. Nende puudumisel tuleb alustada paigaldamise seadistamisprotsessi.

Esimese valiku käigus tuleb määrata, millise teenuskontoga hakkab sünkroniseerimisteenus tööle. Ühenduse loomisel kasutatakse peatükis 4.3 organisatsiooni jaoks loodud teenuskontot AzureADConnect. Järgmises punktis tuleb valida, millist ühenduse meetodit kasutada soovitakse, lisaks saab kohe valida ühekordse sisse- ja väljalogimise lubamise. Kõik eeldused on Pass-Through Authentication ühenduse jaoks olemas. Küsitakse Azure AD *global administrator* õigustes kasutaja autentimist, et luua ühendus Azure Active Directory keskkonnaga. Selle jaoks loodi peatükis 4.3 Azure Active Directory kasutaja LocalAdmin, sisestame loodud kasutaja mandaadi.

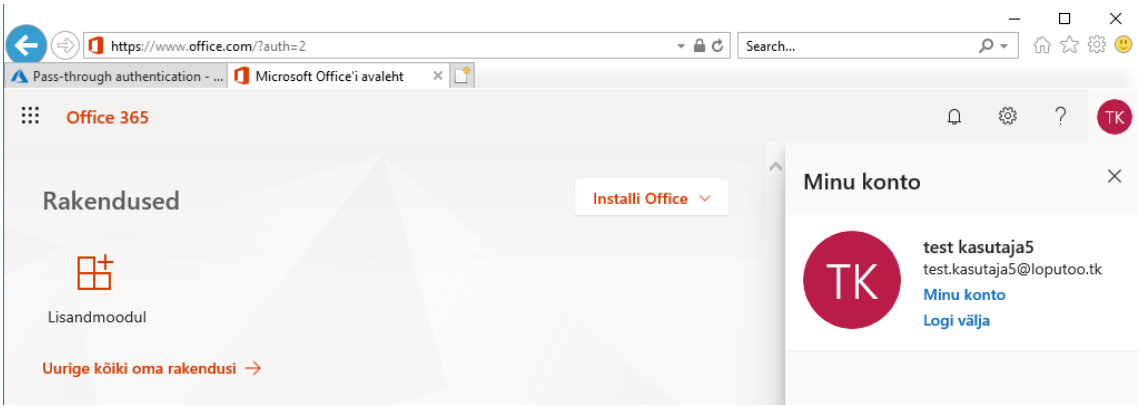
Teises etapis alustatakse seadistamise viisardis täpsema sünkroniseerimise parameetrite määramist (Lisa 1). Esimesena tuleb sisestada, millist kataloogi ja millist puud soovitakse sünkroniseerida, valitakse aktiivne kataloog ning domeeniks loputoo.tk. Vajalik on sisestada domeeni konto, millel on piisavalt õiguseid sünkroniseerimise teostamiseks. Selle jaoks loodi peatükis 4.3 organisatsiooni aktiivsesse kataloogi AzureADConnect teenuskonto, kasutatakse seda.

Seejärel kontrollitakse, kas kohaliku aktiivse kataloogi domeeni teenuse ja Azure Active Directory domeeninimed kattuvad. Kuna eelmises peatükis eeldus täideti, saab liikuda edasi. Järgmise sammuna tuleb valida, millised aktiivse kataloogi organisatsiooni üksuseid hakatakse sünkroniseerima pilve. Organisatsiooni soovidest lähtudes valitakse sünkroniseeritavaks üksuseks loputoo.tk aktiivsest kataloogist üksus nimega Tootajad.

Järgmisena on vaja määrata atribuut, mille alusel kasutajaid tuvastatakse ja lähteankur Azure AD jaoks, mille järgi kohalikus kataloogis kasutajaid eristatakse. Autor valis tuvastamise atribuudiks e-maili ning lubas Azure'l ise otsustada lähteankru üle. Vaikimisi on selleks aktiivse kataloogi kasutaja atribuut mS-DS-ConsistencyGuid. Filtrite seadistamisel lubame sünkroniseerida kõik kasutajad ja seadmed, mis asuvad aktiivse kataloogi üksuses nimega Tootajad.

Eelviimases seadistusviisardi punktis on valikus veel lisafunktsionaalsusi. Näiteks paroolide sünkroniseerimine, mis tuleb jätta lisamata, lähtudes organisatsiooni ühest nõudest, kus ei olnud lubatud paroolide salvestamine pilve. Viimse punktina viib viisard

lõpule kõik eelnevalt valitud seadistused ning alustakse sünkroniseerimist. Peale edukat ja vigadeta sünkroniseerimisprotsessi, on võimalik kasutajatel edukalt logida Microsoft Azure'i keskkonda või Office365 portaali (Joonis 14).



Joonis 14. Organisatsiooni test kasutaja5 on edukalt loginud ennast Office365 portaali.

5 Kokkuvõte

Bakalaureusetöö põhieesmärgiks oli aktiivse kataloogi identiteetide ühendamine pilvekeskkonnaga. Töös analüüsiti erinevaid pilvemudeleid. Tutvustati Amazon Web Services, Microsoft Azure'i ja Riigipilve pilvekeskkondi, käsitleti pilvekeskkondade turvalisust ja nende tasuvust. Vaadeldi erinevaid aktiivse kataloogi ühendamise meetodeid Microsoft Azure pilvekeskkonnaga:

- Azure Cloud Only mudel
- Azure Synchronized mudel
- Azure Federated mudel
- Azure Pass-Through Authentication mudel

Töö tulemusena valmis juhend Azure Pass-Through Authentication ühenduse meetodil, mis vastas organisatsiooni poolt esitatud nõuetele. Selle lahenduse puhul ei olnud vaja teha ettevõttel suuremahulisi lisatöid eeltingimuste täitmiseks ehk ühendus oli kiiresti teostatav. Alles jäid enda lokaalsed identiteedid, paroole ei sünkroniseeritud pilvekeskkonda ja autentimine käib läbi lokaalse domeenikontrolleri.

Töö viimases osas täpsustatakse organisatsiooni jaoks sobiliku lahenduse eeltingimusi, nende täitmist ja realiseerimist lõppjuhendis. Juhend on koostatud punktidest ning jagatud kaheks suuremaks etapiks. Esimeses osas paigaldatakse Microsoft Azure Active Directory Connect tarkvara ning juhendi teises pooles on toodud seadistamisviisardi punktid ja valikud.

Kuna pilvekeskkonnad on järjest kiiremini arenenud ning nende funktsionaalsus on saavutanud taseme, kus ettevõtted ei pea enam töös hoidma täiemahuliselt enda taristut, siis on väga oluline osa ka identiteetide halduse ümberkujunemisel. Töö käigus välja toodud ühendusmeetodid võimaldavad kõik identiteete pilves.

Organisatsioonidel on individuaalsed nõuded kasutajate haldusele. Vastavalt tingimustele saavad nad endale valida töös tutvustatud ühendusmeetoditest sobivaima. Ettevõtted, kelle vajadused ja kriteeriumid langevad kokku selles töös käsitletud organisatsiooni tingimustega, võivad oma identiteedid ühendada pilve bakalaureusetöös loodud juhendi järgi.

Kasutatud kirjandus

[1] Amazon Compute Service Level Agreement [Online] https://aws.amazon.com/compute/sla/ (Kasutatud 18.02.2019)

[2] SLA summary for Azure services [Online] https://azure.microsoft.com/en-us/support/legal/sla/summary/ (Kasutatud 18.02.2019)

[3] Cloud Computing, Server Utilization, & the Environment [Online] https://aws.amazon.com/blogs/aws/cloud-computing-server-utilization-the-environment/ (Kasutatud 20.03.2019)

[4] Under the sea, Microsoft tests a datacenter that's quick to deploy, could provide internet connectivity for years [Online] https://news.microsoft.com/features/under-the-sea-microsoft-tests-a-datacenter-thats-quick-to-deploy-could-provide-internet-connectivity-for-years/ (Kasutatud 20.03.2019)

[5] A Survey on Cloud Computing and Hybrid Cloud [Online] http://www.ripublication.com/ijaer19/ijaerv14n2_13.pdf (Kasutatud 20.03.2019)

[6] What are public, private, and hybrid clouds? [Online] https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/ (Kasutatud 20.03.2019)

[7] The NIST Definition of Cloud [Online] Computinghttp://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf (Kasutatud 20.03.2019)

[8] Performance Model of MapReduce Iterative Applications for Hybrid Cloud Bursting [Online] https://ieeexplore.ieee.org/abstract/document/8283575 (Kasutatud 20.03.2019)

[9] RIIGIPILVE KONTSEPTSIOON [Online] https://www.riigipilv.ee/riigipilvest/riigipilve-konseptsiooni-dokument (Kasutatud 20.03.2019)

[10] Upcoming Name Change for Windows Azure [Online] https://azure.microsoft.com/en-us/blog/upcoming-name-change-for-windows-azure/ (Kasutatud 03.04.2019)

[11] Products available by region [Online] https://azure.microsoft.com/en-us/global-infrastructure/services/?products=virtual-machines&regions=all (Kasutatud 03.04.2019)

[12] Regions and availability for virtual machines in Azure [Online] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/regions-and-availability (Kasutatud 05.04.2019)

[13] Overview of Amazon Web Services AWS Whitepaper [Online] https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/aws-overview.pdf (Kasutatud 09.04.2019)

[14] Mis on Riigipilv? [Online] https://www.riigipilv.ee/et (Kasutatud 09.04.2019)

[15] Infrastrukuur kui teenus (IaaS) [Online] https://www.riigipilv.ee/teenused/taristu-kui-teenus (Kasutatud 09.04.2019)

[16] Platvorm kui teenus (PaaS) [Online] https://www.riigipilv.ee/teenused/platvorm-kui-teenus (Kasutatud 09.04.2019)

[17] Tarkvara kui teenus (SaaS) [Online] https://www.riigipilv.ee/teenused/tarkvara-kui-teenus (Kasutatud 09.04.2019)

[18] Mis saab riigipilvest eriolukorras? [Online] https://www.riigipilv.ee/riigipilvest/riigipilvest-kkk/mis-saab-riigipilvest-eriolukorras (Kasutatud 09.04.2019)

[19] GDPR ehk isikuandmete kaitse üldmäärus - andmekäitluse kultuuri muutus [Online] https://wiki.itcollege.ee/index.php/GDPR_ehk_isikuandmete_kaitse_%C3%BCldm%C3%A4%C3%A4rus_-_andmek%C3%A4itluse_kultuuri_muutus (Kasutatud 15.04.2019)

[20] Security and Compliance [Online] https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/aws-overview.pdf (Kasutatud 15.04.2019)

[21] What Does Shared Responsibility in the Cloud Mean? [Online] https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/ (Kasutatud 15.04.2019)

[22] Other Data Related Security Issues [Online] https://pdf.sciencedirectassets.com/280203/1-s2.0-S1877050917X00239/1-s2.0-S1877050917328570/main.pdf?x-amz-security-token=AgoJb3JpZ2luX2VjECEaCXVzLWVhc3QtMSJHMEUCIQCrwnooOpPrFnJ3uhITLHdt9Dzcw4i%2BuAwLObLCpwemHgIgRU50%2BZX%2FDCZ3O5Kw2vtgmeIEkT5voT%2BYpzCiSD0DMbkq4wMI6v%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FARACGgwwNTkwMDM1NDY4NjUiDMOF0clPfOhWkG23Kiq3A7UgAYS8n%2F%2BIPYc%2B3RvQJpl4XHE2umvR0%2FmPi8sfY8kLVNSd9lRN8lmuj0uvWZZ1KNczBcTn7nfKXYB9hucfYpRvzRghBGJqasXZlKbdT7LU%2Ft%2BiVrq7Oqyf7Ww6gWugS19HFdRJTi9CDdGDs4GhIWSuzOwAsSrIbrzkc%2FJtlEw9z2aGRytX0w%2F5%2FwBxks0IZJm%2BSge2%2BUuaS9ga6tXFi6KlUii3hbAclMr1BP6WVSchoZGpt463spED33wa1vjrHAkUduC3jgb60wJT9xpZ6%2BrXkzFQU0Axedcw8MFQ%2BinvG3mUK%2BzplLf7LfA3PN23Qqb%2Bt1A0pbfRUqbVlaH%2FTkWuYPygUkdTvvpv4KDYrEe8zJJQ6Yen7qti9BL649KLTnQ6bimyCZsxmY26QqVmb9CGPp1nFq7umP6wIKR%2BTa%2FHA3zNg2LaoiZJWlwpctkNUWlW02naOUB6y3UASaVK0EJ9ex3WutljhQGsnwTf0sdPAHDeys%2ButxYwL5SfrykNAWygZCJz6WdSnsoVEcqa0YgBZjciBZT7a7ZvGDLWFPtQQ3AlMq3WP4JRHF66KZNAuQgqWR49TtgwpInR5QU6tAFowBmFwFyYSMtgtMGwJIGwvelZf0xdV%2F1j0k7B%2FS3PXyrZvgdmn%2Bqkah0EtFsI70opkJ7fQjDM8dLjAl71M8l4q3af02T3xxzZkNHULiGCRU3SVqJXxB9btGpobh%2F7XLLNKqe9zm8FcsC6wc81My6Kxi6Rsf4F45eKPkR2uRqIiCAdEVoyC%2BvCv%2BHG%2FXz4PdObOa4MIYV3mqHgxxd1KDFnJTknOtp6SLb1AThxfXWeUPBtGdM%3D&AWSAccessKeyId=ASIAQ3PHCVTYRBY3A24H&Expires=1555320903&Signature=mMvbzbtSlomLL0P7pJC9dFdn3sc%3D&hash=d638e43cf4024237ddc4cfaa9ad68546d7933291dc2b4910121430f54c6bcb04&host=68042c943591013ac2b2430a89b270f6af2c76d8dfd086a07176afe7c76c2c61&pii=S1877050917328570&tid=spdf-79c0cbc0-f288-43a9-9ae2-8ddf65ae220d&sid=0d5305ce2f3d6641e42a4ed-49f73f117ac3gxrqb&type=client (Kasutatud 10.04.2019)

[23] Hinnakiri [Online] https://www.riigipilv.ee/hinnakiri (Kasutatud 10.04.2019)

[24] Amazon EC2 Reserved Instances [Online] https://aws.amazon.com/ec2/pricing/reserved-instances/ (Kasutatud 10.04.2019)

[25] Reservations [Online] https://azure.microsoft.com/en-us/reservations/ (Kasutatud 10.04.2019)

[26] Understand how the Azure reservation discount is applied to virtual machines [Online] https://docs.microsoft.com/en-us/azure/billing/billing-understand-vm-reservation-charges (Kasutatud 10.04.2019)

[27] Active Directory: Concepts Part 1 [Online] https://social.technet.microsoft.com/wiki/contents/articles/16968.active-directory-concepts-part-1.aspx (Kasutatud 18.04.2019)

[28] Azure Active Directory pricing [Online] https://azure.microsoft.com/en-us/pricing/details/active-directory/ (Kasutatud 28.04.2019)

[29] What is Azure Active Directory? [Online] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis (Kasutatud 28.04.2019)

[30] Cloud authentication [Online] https://docs.microsoft.com/en-us/office365/enterprise/about-office-365-identity (Kasutatud 28.04.2019)

[31] What is password hash synchronization with Azure AD? [Online] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs (Kasutatud 28.04.2019)

[32] Account expiration [Online] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization (Kasutatud 28.04.2019)

[33] Step-By-Step: Setting up AD FS and Enabling Single Sign-On to Office 365 [Online] https://blogs.technet.microsoft.com/canitpro/2015/09/11/step-by-step-setting-up-ad-fs-and-enabling-single-sign-on-to-office-365/ (Kasutatud 01.05.2019)

[34] Best practices for securing Active Directory Federation Services [Online] https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs (Kasutatud 01.05.2019)

[35] What is hybrid identity? [Online] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity (Kasutatud 01.05.2019)

[36] What is Azure Active Directory Pass-through Authentication? [Online] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta (Kasutatud 01.05.2019)

[37] Create your Azure free account today [Online] https://azure.microsoft.com/en-us/free/ (Kasutatud 01.05.2019)

[38] Sign up your organization to use Azure Active Directory [Online] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/sign-up-organization (Kasutatud 01.05.2019)

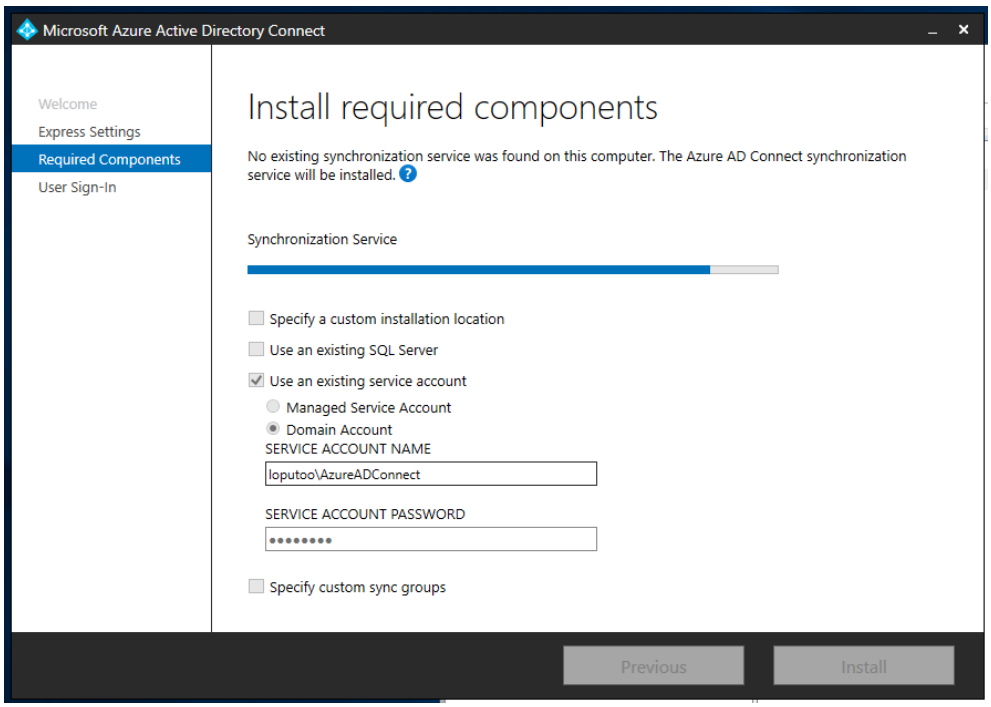
[39] Azure AD Connect: Accounts and permissions [Online] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions (Kasutatud 01.05.2019)

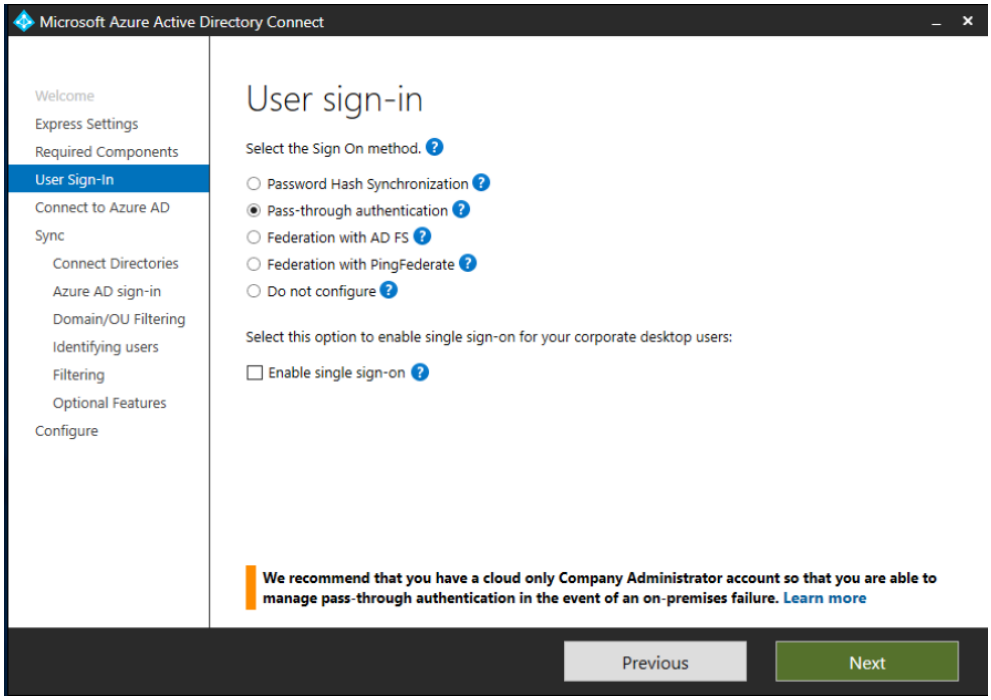
[40] Add your custom domain name using the Azure Active Directory portal [Online] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain (01.05.2019)

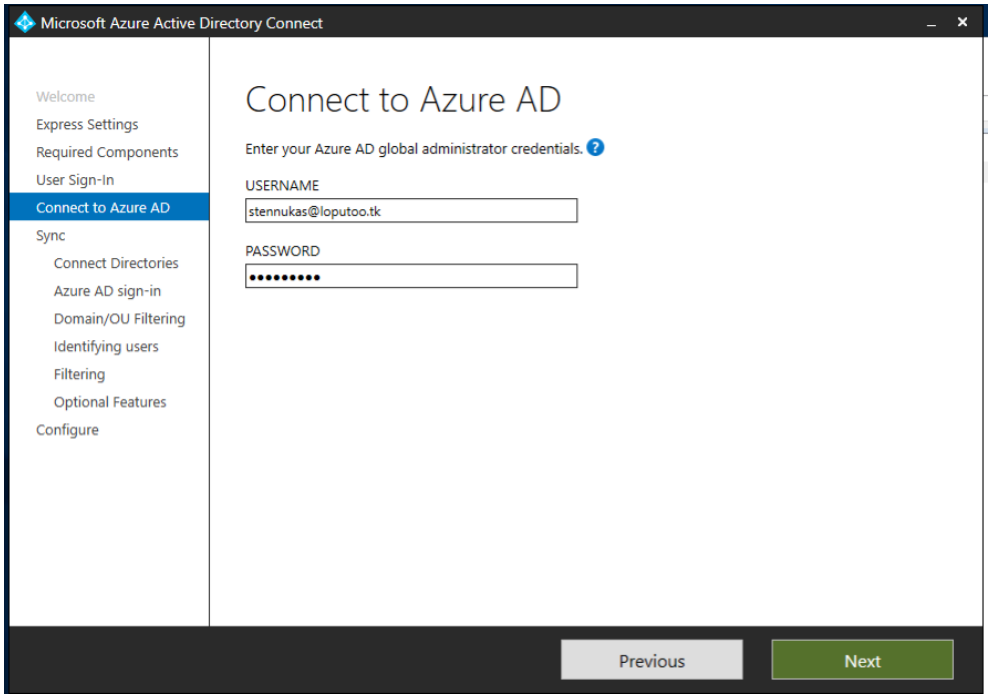
[41] Prerequisites for Azure AD Connect [Online] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites (Kasutatud 01.05.2019)

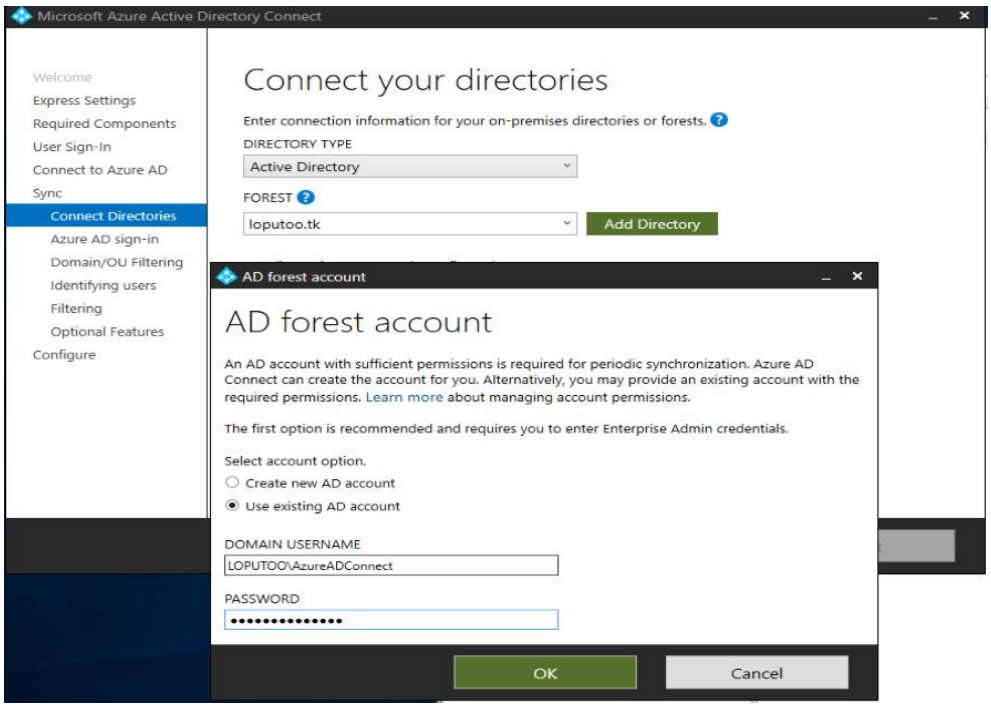
[42] Table 6a & 6b - Pass-through Authentication with Single Sign On (SSO) and Password Hash Sync with Single Sign On (SSO) [Online] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-ports (Kasutatud 01.05.2019)

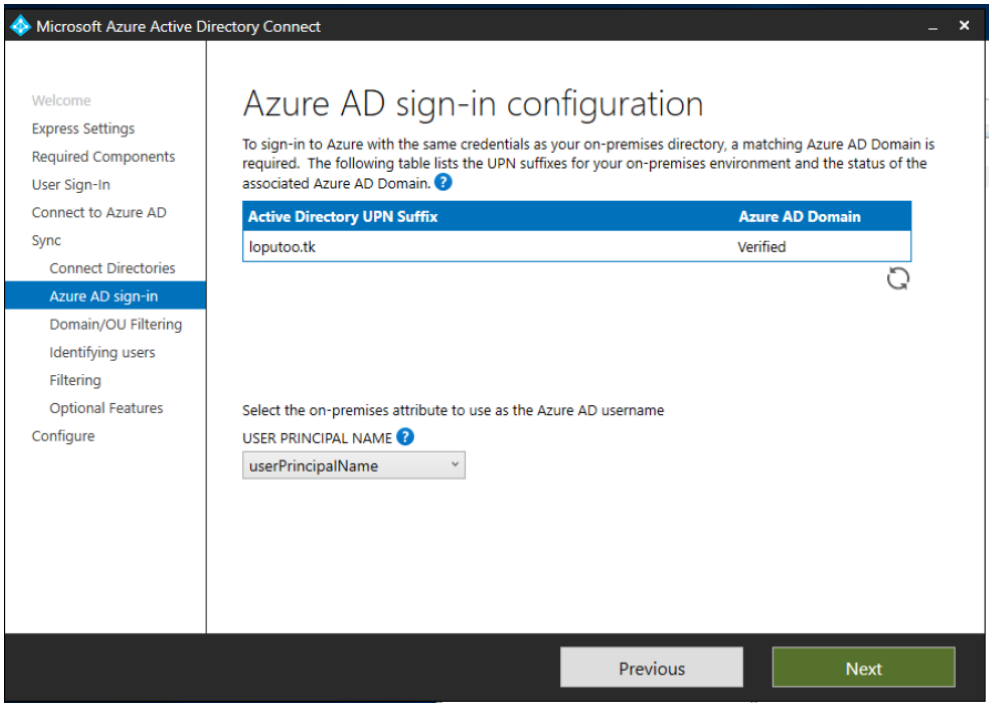
Lisa 1 – Microsoft Active Directory seadistamisviisardi pildid

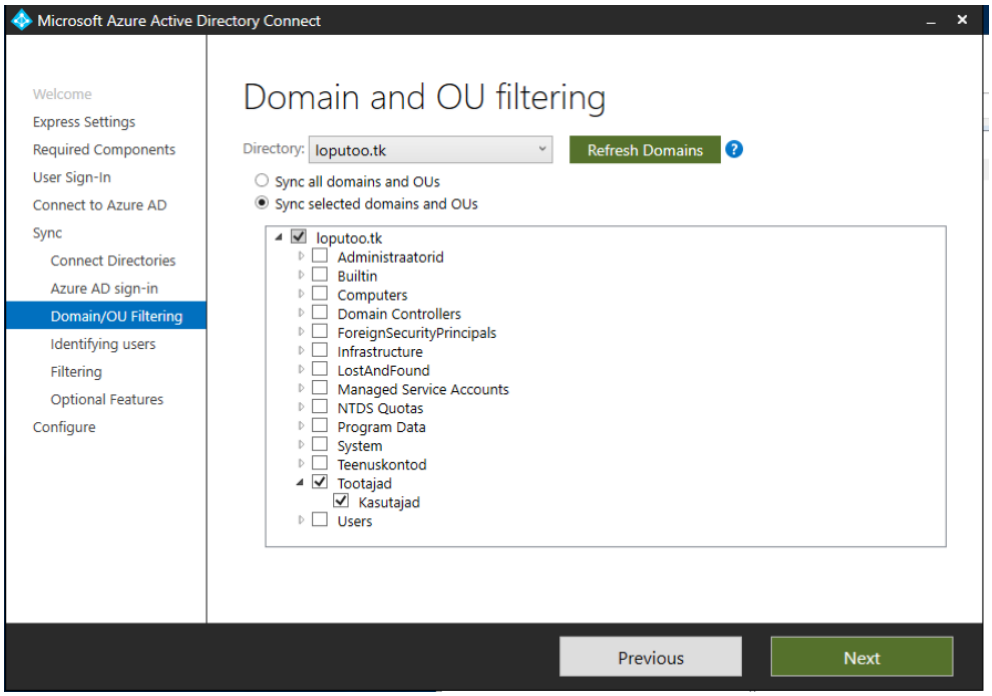


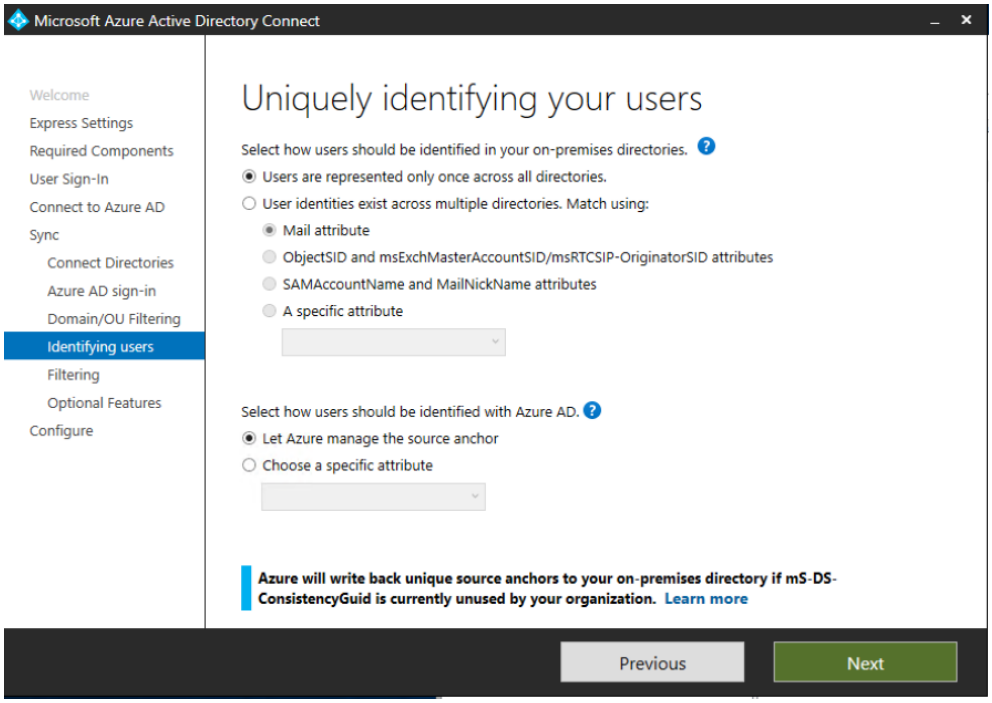


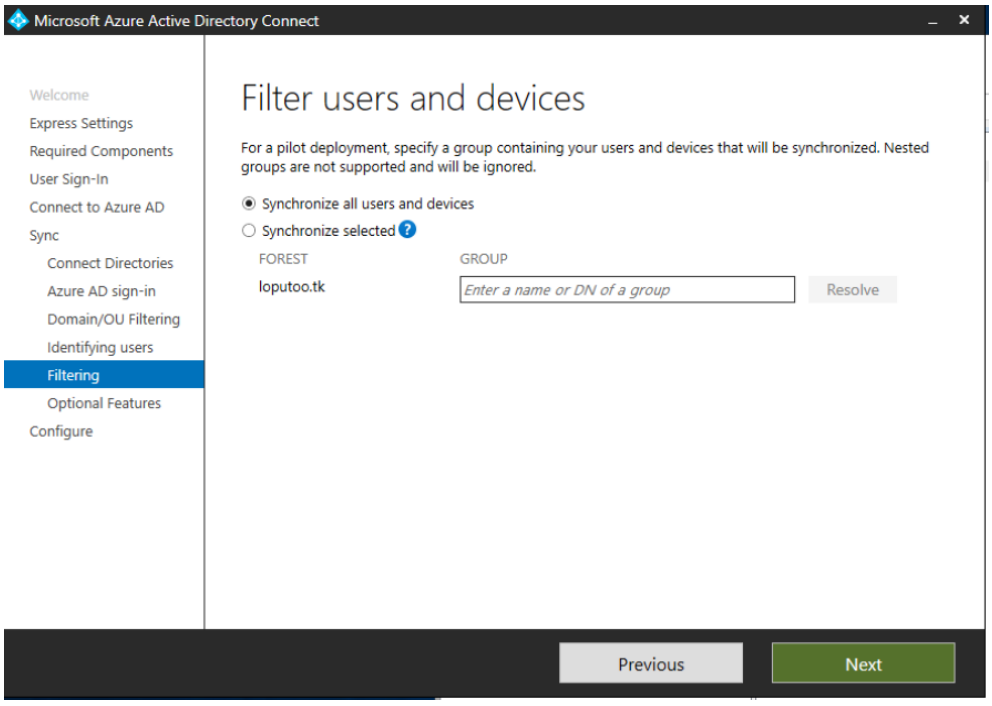

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Connect to Azure AD
Enter your Azure AD global administrator credentials.
USERNAME
stennukas@loputoo.tk
PASSWORD
Previous
Next

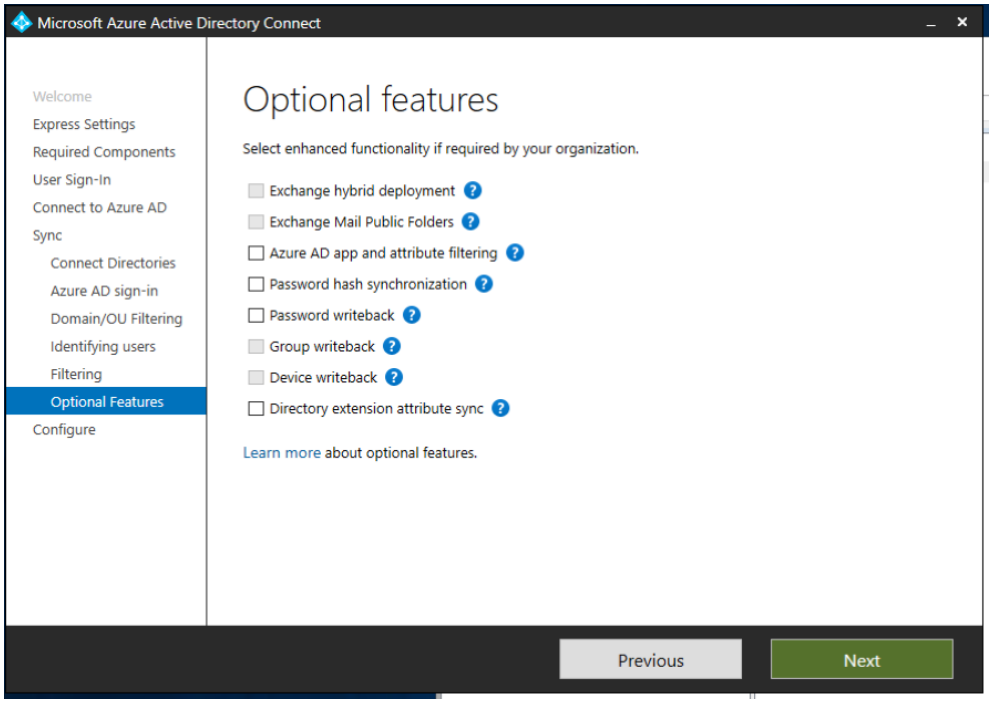

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Connect your directories
Enter connection information for your on-premises directories or forests.
DIRECTORY TYPE
Active Directory
FOREST
loputoo.tk
Add Directory
AD forest account
AD forest account
An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. Learn more about managing account permissions.
The first option is recommended and requires you to enter Enterprise Admin credentials.
Select account option.
Create new AD account
Use existing AD account
DOMAIN USERNAME
LOPUTOO\AzureADConnect
PASSWORD
OK
Cancel

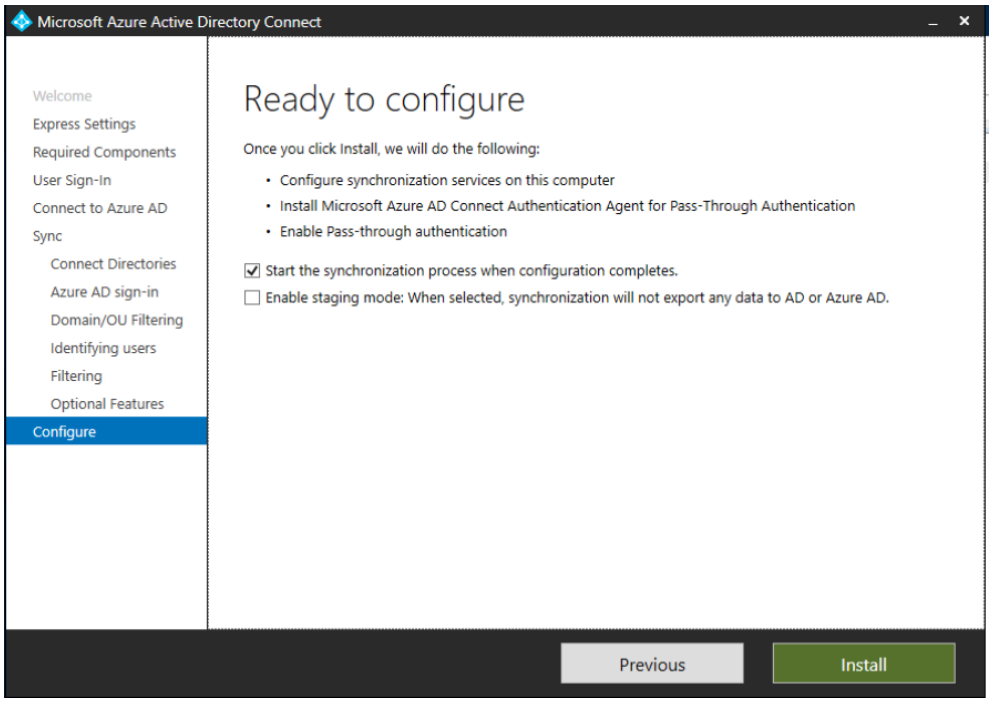

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Azure AD sign-in configuration
To sign-in to Azure with the same credentials as your on-premises directory, a matching Azure AD Domain is required. The following table lists the UPN suffixes for your on-premises environment and the status of the associated Azure AD Domain.
Active Directory UPN Suffix
Azure AD Domain
loputoo.tk
Verified
Select the on-premises attribute to use as the Azure AD username
USER PRINCIPAL NAME
userPrincipalName
Previous
Next

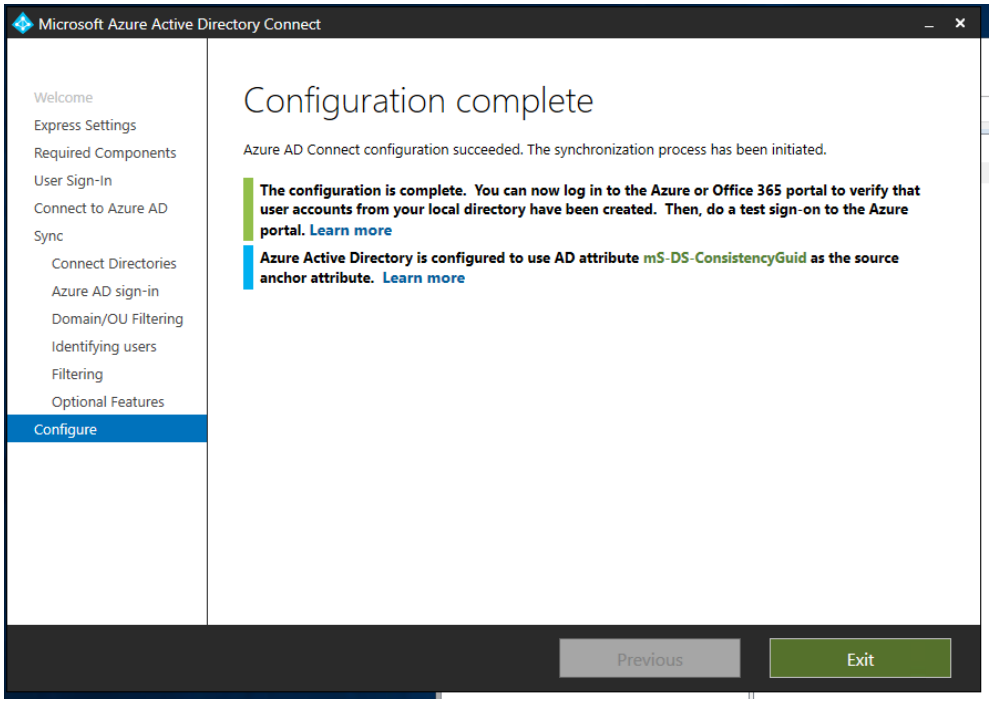

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Domain and OU filtering
Directory: loputoo.tk
Refresh Domains
Sync all domains and OUs
Sync selected domains and OUs
loputoo.tk
Administraatorid
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Infrastructure
LostAndFound
Managed Service Accounts
NTDS Quotas
Program Data
System
Teenuskontod
Tootajad
Kasutajad
Users
Previous
Next


Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Uniquely identifying your users
Select how users should be identified in your on-premises directories.
Users are represented only once across all directories.
User identities exist across multiple directories. Match using:
Mail attribute
ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
SAMAccountName and MailNickName attributes
A specific attribute
Select how users should be identified with Azure AD.
Let Azure manage the source anchor
Choose a specific attribute
Azure will write back unique source anchors to your on-premises directory if mS-DS-ConsistencyGuid is currently unused by your organization. Learn more
Previous
Next


Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Filter users and devices
For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.
Synchronize all users and devices
Synchronize selected
FOREST
GROUP
loputoo.tk
Enter a name or DN of a group
Resolve
Previous
Next


Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Optional features
Select enhanced functionality if required by your organization.
Exchange hybrid deployment
Exchange Mail Public Folders
Azure AD app and attribute filtering
Password hash synchronization
Password writeback
Group writeback
Device writeback
Directory extension attribute sync
Learn more about optional features.
Previous
Next


Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Ready to configure
Once you click Install, we will do the following:
Configure synchronization services on this computer
Install Microsoft Azure AD Connect Authentication Agent for Pass-Through Authentication
Enable Pass-through authentication
Start the synchronization process when configuration completes.
Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.
Previous
Install


Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Configuration complete
Azure AD Connect configuration succeeded. The synchronization process has been initiated.
The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. Learn more
Azure Active Directory is configured to use AD attribute mS-DS-ConsistencyGuid as the source anchor attribute. Learn more
Previous
Exit