Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VEIKKA PLAAMI

Migration of on-premises Active Directory to Entra ID

DEGREE PROGRAMME IN
BUSINESS INFORMATION SYSTEMS
2026

TIIVISTELMÄ

Plaami, Veikka: Paikallisen palvelinympäristön siirto pilveen käyttämällä Entra ID-palvelua
Opinnäytetyö, AMK
Tietojenkäsittely
Maaliskuu 2026
Sivumäärä: 29

Yhä useammat organisaatiot luottavat nykyisin pilvipohjaisiin palveluihin ja sovelluksiin, mikä lisää identiteetti- ja pääsynhallintapalvelujen tarvetta. Nämä palvelut täytyvät olla integroituvia paikallisiin palvelininfrastruktuureihin sekä pilvi-infrastruktuureihin. Tässä opinnäytetyössä käydään läpi pilvipalveluiden, pilvipalvelutarjoajien ja pilvipalveluiden käytäntömallien perusteet, sekä sitä miten paikallinen palvelinympäristö voidaan siirtää hybridipalvelimeksi Microsoftin Entra ID-palvelulla.

Tämän opinnäytteen testitoteutuksessa käytettiin virtuaalitietokoneita, jotka oli tehty Microsoft Azure-palvelulla. Testitoteutuksessa siirto toteutettiin käyttämällä Microsoftin Entra Connect palvelua. Lisäksi testitoteutuksessa analysoitiin ja selitettiin laajasti Entra Connect palvelua käytettäessä tulevia vaihtoehtoja ja asetuksia.

Testitoteutuksen tavoitteena oli osoittaa, kuinka käyttäjätilit ja käyttäjäryhmät synkronoituivat molempien ympäristöjen välillä. Lisäksi testaus osoitti, että käyttäjät pystyivät käyttämään paikallisia palveluita sekä pilvipalveluita samoilla kirjautumistunnuksilla, ja käyttäjät, jotka luotiin pilvessä, synkronoitiin myös paikalliseen palvelimeen. Tutkimuksen myötä voidaan todeta, että hybridi-identiteetti tarjoaa käytännöllisen lähestymistavan organisaatioille, jotka haluavat modernisoida käyttäjä- ja pääsynhallintansa pilveen.

Avainsanat: Aktiivihakemisto, Azure, Entra ID, Entra Connect, Cloud Sync, Hybridipalvelin, Käyttäjähallinta, Pääsynhallinta

ABSTRACT

Plaami, Veikka: Migration of on-premises Active Directory to Entra ID
Bachelor's thesis
Business Information Systems
March 2026
Number of pages: 29

As more organizations start relying on cloud-based services and applications, the need for identity and access management solutions that can integrate with on-premises infrastructure with cloud environments rises. This thesis explains the basics of cloud services, service providers and different cloud models, as well as how to implement a migration of a local on-premises Active Directory environment to a hybrid identity model using Microsoft Entra ID service.

The objective of this implementation was to design and implement a functional test environment that simulated a small company that wanted to move from a purely on-premises environment to a hybrid identity. The test environment was created with virtual machines hosted by Microsoft Azure and the migration was done with Microsoft's Entra Connect-services. The thesis also includes a thorough analysis and explanation of Entra Connect-wizards many options and configurations.

The implementation demonstrated how accounts, attributes and security group memberships were synchronized between both environments. Testing proved that users were able to access both on-premises and cloud-based services using same credentials, and users created withing the cloud were synchronized correctly within the on-premises environment. The study concluded that hybrid identity provides a practical approach for organizations that are seeking to modernize identity and access management, and how companies can continue to develop their cloud identity with full cloud model.

Keywords: Active Directory, Azure, Entra ID, Entra Connect, Cloud Sync Hybrid Identity, Identity management, Access management

CONTENTS

1 INTRODUCTION

In today's world, organizations are moving away from purely on-premises infrastructures in favour of hybrid and purely cloud-based environments. This transition is driven by the need for greater flexibility, scalability, security and efficiency. As more companies adopt cloud services, traditional on-premises identity management solutions, such as Active Directory, are gradually complemented or fully replaced by cloud-native platforms like Microsoft Entra ID. The purpose of this thesis is to analyse and examine what are the pros and cons of hybrid and pure cloud Active Directories versus an on-premises Active Directory, as well as going over commonly used terminology, strategies and cloud service providers that are used in cloud computing environments. The research will also include a migration from on-premises active directory to a hybrid active directory in a sandbox environment, as well as an exploration of identity and access management tools provided by Entra ID. The purpose of this research is to provide a practical framework and set of best practices for organizations planning to transition from a traditional Active Directory infrastructure to Microsoft Entra ID, and to help IT professionals seeking to modernize their identity and end-of-life cycle management in a cloud driven future.

2 CLOUD SERVICES

Cloud services are modern computing resources, like servers, storage, software, databases, that are delivered over the internet via a cloud service provider, instead of being stored and managed on your own computer or server. It enables access to files, applications and other data from almost anywhere, because the data and computing for cloud data takes place in servers in a data centre and not locally on the user's device or servers. All you need to access the files, applications or data is a computer with internet access or access to a virtual private network. (Cloudflare, n.d.)

Cloud computing's most essential characteristics by the National Institute of Standards and Technology (NIST) were On-demand self-service, Broad network access, Resource pooling, Rapid elasticity and Measured service. On-demand self-service means that an independent user can create and manage computing resources without requiring interaction from the service provider. Broad network access means that cloud computing capabilities are available and accessible over the network with wide range of client devices, such as workstations and mobile phones. Resource pooling means that the cloud service providers computing resources are share among multiple customers and users with different physical and virtual resources, and these resources are dynamically assigned and are automatically reassigned by according to demand. Rapid elasticity means that resources can be elastically assigned to scale rapidly to be bigger or smaller according to demand, and lastly Measured service, means that cloud systems can be monitored, controlled and optimized by the cloud service provider and the cloud service consumer. (Mell & Grance 2011)

2.1 Cloud service providers

Most used cloud service providers are Amazon with Amazon Web Services, Google with Google cloud platform and Microsoft's Azure services. Amazon is the current cloud service provider leader, owning almost a third of the market

(Posey, 2024). However, there are some other smaller or more niche companies that offer cloud services, including IBM, Alibaba, Oracle, Red Hat, DigitalOcean, and Rackspace (Google, n.d.).

2.2 Cloud service models

Cloud computing has three main cloud service models, Infrastructure as a service (IaaS), Platform as a service (Paas) and Software as a service (Saas) (Google, n.d.)

Infrastructure as a service (IaaS) provides storage, networking and virtualized computing resources on demand, without the need for physical hardware. It enables rapid application deployment by simplifying the IT infrastructure and eliminating hardware management. (Microsoft, n.d. -c) IaaS implementations are usually used to replace datacentre solutions and allow for more flexibility at a reduced cost. For example, Microsoft's OneDrive is an IaaS based cloud service. (Uotila, 2023)

Platform as a service (PaaS) provides organizations database, operating system and/or development platforms and allows organizations to develop applications without having to worry about building the infrastructure needed to support the development environment. (Rountree & Castrillo 2013, pp. 6-7) For example, Microsoft SQL Server is a PaaS based cloud service. (Uotila, 2023)

Software as a service (SaaS) provides both application and data services. The service provider provides all the necessary applications, data, platforms and infrastructure, while organizations usually pay a subscription to the service provider. (Rountree & Castrillo, 2013, pp. 6-7) The SaaS-model also eliminates the need for customers to install or maintain software locally and are highly scalable, which allows the customer to adjust their subscription levels as their

needs change. (Microsoft, n.d. -c) For example, Microsoft's Office 365 is a SaaS based cloud service. (Uotila, 2023)

2.3 Multicloud

Many companies use multiple cloud service providers at once for different services. This way, they can choose the best cloud service provider for their use case. It also improves resiliency and redundancy by distributing workloads across various cloud environments and decreasing downtime from service provider outages and improves disaster recovery. The use of multiple cloud service providers is often referred to as a "multicloud strategy" (Hewlett Packard Enterprises, 2025). This strategy does have its own downsides, for example, coordinating security measures between cloud platforms may become inconsistent, like group policies, encryption and access control, as well as potential latency issues between multiple applications and services. It also may increase expenses, because pricing structures and services differ among cloud service providers. Optimizing resource costs across multiple cloud service providers requires continuous monitoring to prevent unexpected expenses. (Microsoft, n.d. -b)

2.4 Public, Private and Hybrid Cloud

The cloud environment is usually classified between Public, Private and Hybrid clouds. A private cloud is designed and dedicated to the needs of a specific organization, and the infrastructure is usually located on premises. In public cloud environments, infrastructure is facilitated and managed by a cloud service provider. (Indu ym., 2018) Hybrid cloud is a mixed computing environment that combines on-premises private cloud infrastructure with cloud infrastructure from a public cloud service provider. The primary advantage of hybrid cloud is scalability, workload management and agility, and can be used as part of a disaster recovery strategy. (F5, n.d.)

3 ACTIVE DIRECTORY AND ENTRA ID

3.1 Active Directory

The Active Directory is a service developed by Microsoft for Windows Servers. It is an essential tool for user and computer organizing and management but can also be used to manage and organize network resources, security groups and their memberships, group policy objects, and so on. (Proofpoint, n.d.) It is used by network administrators to authenticate and authorize users within the domain by organizing objects and providing a hierarchy. This hierarchy is called a domain, and they can be grouped into a tree, which can also be connected to form a forest. The central server within the forest is called a domain controller, and it is used to maintain the directory database and to replicate data to other domain controllers within the same domain. (Silverfort, n.d.)

3.2 Entra ID

Entra ID, which is formerly known as Azure Active Directory, is a cloud-based identity and access management service that provides centralized identity, authentication and authorization capabilities across on-premises, hybrid and full cloud environments to protect and secure users, devices, applications and other resources. (Microsoft, 2025c) Authentication is the process of proving that you are who you are claiming to be, and authorization is specifying what data you are allowed to access and what can you do with that data. Identity and access management (IAM) ensures that the right users and machines have secure access to the right resources at the right time and for the right reasons. Entra ID centralizes identity and access management to a single to a single platform, that simplifies authorization and authentication. Delegating authentication and authorization to Entra enables Conditional Access-policies that requires users to be in specific locations to access data, Multifactor authentication that require users to have specific devices to authenticate log in-data. (Microsoft, 2025a)

It is also possible to enable users to sign in once to access their Microsoft apps and other cloud or on-premises apps with the same credentials instead of using multiple different credentials. This streamlined sign in method is called Single Sign-on (SSO). Single Sign-on is a federated identity management tool, which works by sharing and verifying log in credentials between identity providers, like Entra ID, and service providers. Single Sign on services do not store user information but instead checks a user's authentication token from the identity providers database. When verified by the identity provider, it prompts the user to log in. The user did not need to remember log in credentials to the application, but instead only needed to remember one set of credentials, reducing password fatigue and encourages the user deploy stronger passwords as they do not need to repeat the same password in multiple places. (Fortinet, n.d.)

4 IMPLEMENTATION

The purpose of the test implementation was to simulate a realistic migration of a local on-premises Active Directory environment to a hybrid cloud server using Entra ID. The test implementation was designed to reflect a typical small organizational Active Directory environment, which included a Domain controller, few users of varying security clearances and allowances, and a Windows 11-workstation. I will also be configuring and verifying a custom web domain for Entra ID, as well as changing the user's principal name suffix (UPN) for the users in my Active Directory.

4.1 Test environment

For a test environment, I am using virtual machines In Microsoft's Azure cloud services, due to its flexibility, scalability and cost efficiency. Due to logistical and practical reasons, it was not possible for me to deploy a physical on-premises Active Directory environment for this study. Establishing and maintaining on-premises infrastructure would require dedicated hardware, networking equipment and physical space, which were outside of the scope of this research. Active Directory Domain Services does not depend on physical hardware, but rather on operating systems and network connectivity. By using virtual machines and virtual networks, a simulated and controlled environment can be created that allows testing of different kinds of authentication and synchronization methods, while still ensuring safety and isolation.

First, I created a resource group where I could store all the resources I used for the migration. Resource groups are containers that store resources, like virtual machines, databases, network security groups, disks and virtual networks. they allow role-based access control and simplifies monitoring of resources. In that resource group I created a Windows server 2022 domain controller, a Windows 11 domain-joined client device, and a virtual network with local IP address space of 10.0.50.0/24. With the creation of the domain controllers, I also had to create network security groups and virtual network

interfaces for each device, where I set static IP addresses for both devices for ease of use. Usually, static IP addresses are suitable in a modern company environment, as they must be manually assigned and tracked so that there are no conflicts or overlaps in addresses. Remote working and bring your own device (BYOD) – models are impractical with static IP addresses, as they require a fixed and trusted network location.

There are many ways to connect to virtual machines that are hosted in Azure, such as Remote desktop protocol (RDP), PowerShell with the Azure PowerShell module, Secure Shell (SSH) or Azure Bastion. Azure Bastion is a fully managed PaaS-service that provides seamless RDP and SSH connections to virtual machines directly from the user's web browser via Azure portal. Azure Bastion can also be used natively via Remote Desktop Access protocol (RDP) or a SecureShell client (SSH) that is already installed on your computer. Azure Bastion is deployed directly inside the virtualized environment, which means that no network ports are required to be opened and exposed to the public internet and no public IP-addresses must be assigned. However, you do need an Azure subscription, and the service is not free, as it bills you for data transfer. (Microsoft, 2026a)

To simulate an on-premises server, I installed Active Directory Domain Services (AD DS) to the domain controller. An Active Directory forest was created with the domain controller, with the name oppari.local. Domain name system (DNS) was applied and configured on the domain controller to support Active Directory name resolution. The Windows 11 client device was configured with a static IP address of 10.0.50.5/24 and successfully joined the oppari.local domain. Several test users were created within the Active Directory with different security clearances to represent domain users. Then, connectivity and authentication were validated by initiating Remote Desktop session with the test user accounts to the Windows 11 device. It should be noted that if you are using RDP to use your virtual machines, you need to configure and allow the RDP access via Group policy objects (GPO). The group policy object can be found in Group policy Management, and from there create a new group policy. Edit the new group policy and navigate to Computer

Configuration, then continue to Policies, Administrative Templates, Windows Components, Remote Desktop Services, Remote Desktop Session Host, Connections and enable “Allow users to connect remotely using Remote Desktop Services”-policy.

After confirming that the Windows 11-workcomputer has joined the domain successfully and can be accessed via Remote desktop, I created a second Windows server named “AADC-oppari” (Shortened from Azure Active Directory Connect), which I also added to our domain and tested access via remote desktop. The reason for this second Windows server is that I will be using it as a synchronization server between Entra ID and our domain. Microsoft states that it is preferable to run Microsoft Entra Connect-services from a domain joined server rather than your domain controllers, as domain controllers are critical infrastructure that are responsible for directory services, DNS, authentication and so forth. Entra Connect-services also add additional services, synchronization processes and database dependencies, increasing workload and complicates troubleshooting. (Microsoft, 2024a)

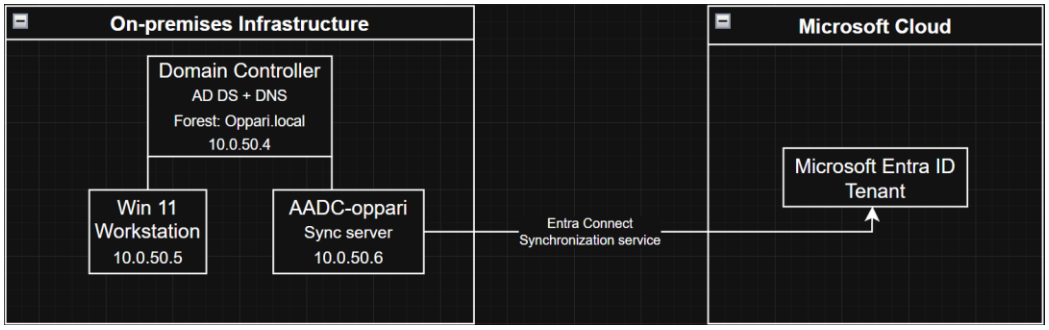


Figure 1. Hybrid identity test environment that was used in the study

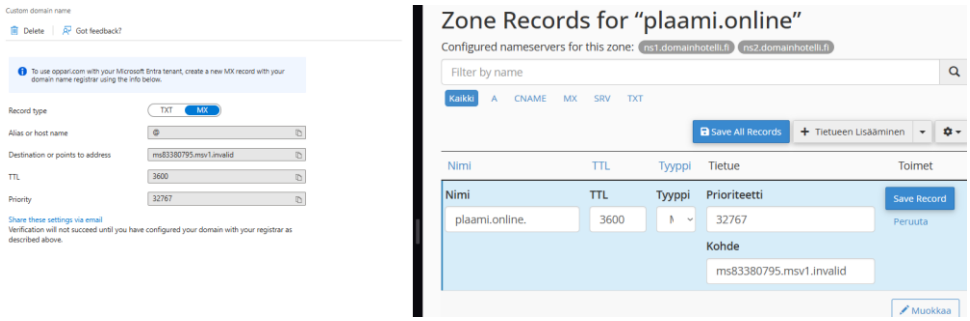
4.2 Preparing for cloud migration

Before starting the migration, the Active Directory environment should undergo a series of health checks, like deletion of disabled and stale user accounts, computer objects and security groups, as well as updating your domains UPN-suffixes (User principal name). UPN-suffixes are the part of a user’s sing-in

name that follows the @-symbol, so for example it changes from user@domain.local to user@company.com. (Microsoft, 2024b.)

A useful tool that can be used to check non-compliant attributes is Microsoft's Identity Fix-tool (IdFix). It is designed to scan on-premises Active Directory environments for attribute errors and problems that conflict with Entra ID requirements. The IdFix-tool helps users to fix most of the synchronizing errors by reporting problematic user attribute values in all domains inside the forest. However, the tool does not fix all the issues. For example, formatting errors of suggested values still need to be fixed manually by an administrator. (Microsoft, n.d. -a)

To use Entra ID, a Microsoft Entra tenant must be created. An Entra tenant is a dedicated and isolated instance of Microsoft's cloud identity and access management services. When an organization sign's up for cloud service subscription such as Azure or Microsoft Intune, a tenant is automatically created. A tenant represents an organization, and each tenant is distinct and separate from other tenants. (Microsoft, 2025a) By default, the user who creates an Entra tenant is automatically assigned the Global Administrator-role. When a tenant is created, it is also automatically assigned a default domain name, for example: organization.onmicrosoft.com. (Microsoft, 2024c) To change that, the ownership of a domain needs to be verified with either a DNS TXT-record or a DNS MX-record. From the Entra Admin center, I navigated to Domain names, and "add a custom domain". The custom domain name I own is Plaami.Online, so I added that as my domain name. From there, I was prompted to add either a TXT-record or a MX-record with pre-generated a verification value for the destination or point to address, as well as a priority number for the MX-record.



Picture 1. On the left, Entra ID's generated MX-record. On the right, Zone records for Plaami.online-domain.

After the record is added to the registrar, the custom domain name in Entra Admin center can be verified and made into the primary domain name, so the default domain name changes from company.onmicrosoft.com to company.com, so in my case from veikkaplaamioutlook.onmicrosoft.com to plaami.online.

4.3 Microsoft Entra Synchronization tools

To synchronize our Active Directory with Entra ID, either Entra Connect wizard or Cloud sync agent must be used. To download either one, the user must sign-in to The Entra ID admin center as at least a Hybrid Identity -administrator and navigate to Entra Connect and select which synchronization type you want.

Although both solutions synchronize identities to Entra ID, they differ significantly in use cases and complexity. Microsoft Entra Cloud Sync is a cloud managed option for hybrid identity, whereas Entra Connect is an on-premises tool for hybrid identity. With Cloud sync, provisioning from Active Directory to Entra ID is done with Microsoft Online Services, as organizations only need to deploy a light-weight agent in their own on-premises Active Directory environment that connects their Active Directory with Entra ID. (Microsoft, 2026b) Entra Connect on the other hand is a more customizable, but heavier, solution that takes all operations that are related to synchronize identity data between the on-premises Active Directory and Entra ID. Users and groups can be synchronized from the same domain using Entra Connect

and Cloud Sync in parallel, if the scoping filters in each synchronization are mutually exclusive and they do not have clashing attributes. (Microsoft, 2025h)

4.4 Synchronization of AD and Entra with Entra Connect

Following the preparation of the Active Directory environment and the establishment of a Entra tenant, I installed Entra Connect from the Entra Admin centre to my domain-joined server, AADC-oppari. I chose Entra Connect for my test environment, as I wanted to see how much more customizable it is compared to Cloud Sync. However, it should be noted that Microsoft states that Cloud Sync is more preferrable than Entra Connect, as it provides less latency and is more secure compared to Entra Connect. (Microsoft, 2026b)

With the installation of Entra Connect complete, I started the synchronization process. The synchronizing process can be streamlined by using the express settings from Entra Connect-wizard, and they are suitable for Windows Server's with a single forest like my Active Directory. The express settings automatically configure the synchronization of identities of the current forest and password hash's and automatically synchronizes all attributes for hybrid identity. In my test environment, I chose not to use the express settings to see how customizable the normal settings are.

During the configuration of the Entra Connect wizard, it will install some required components and drivers, like a SQL-server database instance. Alternatively, you can choose to use an already existing SQL-server. Then, choosing the sign-in method for users, as well as choosing to use Single Sign-on or not. The available options for sign-on methods are Password Hash synchronization, Pass-through authentication, Federation with Active Directory Federation Services (AD FS), Federation with PingFederate or a solution that is not managed by Entra Connect. (Microsoft, 2025b)

Password Hash synchronization is the simplest way to authenticate users for on-premises directory and Entra ID. It creates and synchronizes a hash value

representation of the user's password, which is the result of a one-way mathematical function called the hashing algorithm. There is no method to revert the hash back to text form of the user's password, and Entra and the Active Directory uses this hash to represent the user's password, allowing the user to use the same password for on-premises resources and cloud resources. (Microsoft, 2025b) Pass-through authentication provides a simple password validation service by using an agent that runs on the on-premises server. The server validates users directly in the Active Directory, which means the password validation does not happen in the cloud. It still provides the same benefits of cloud authentication for organizations, while still allows for organizations to enforce their on-premises security and password policies. (Microsoft, 2025g) Federated authentication leaves the authentication to the organizations on-premises Active Directory Federation Services (AD FS), even though the federated domain has synchronized user identities to the cloud. (Microsoft, 2025d) PingFederate on the other hand is a third-party enterprise federation server that provides user authentication and single sign-on. It integrates with many existing systems and allows for centralized control over authentication policies and credentials. (PingIdentity, n.d.) As federation services are out of scope for my study, my options are limited to either Password hash synchronization or Pass-through authentication. I chose Password hash synchronization, as I wanted to see how authentication works via Entra ID.

After, the user is required to sign in to Entra ID as at least a Hybrid Identity Administrator in the Entra ID tenant. If multi-factor authentication is enabled in the tenant, a pop-up window will appear for the verification process, which requires the user to approve the sing in request via their authentication method, like Microsoft's Authenticator app. After authenticating the sign in to Microsoft, the credentials of at least an Enterprise Administrator-account in the Active Directory must be entered. After connecting the Active Directory and Entra ID, The Entra connect wizard will retrieve the Active Directory schema. The Active Directory schema defines what type of objects can exist within the Active Directory and what attributes those objects have. (Microsoft, 2020) After retrieving the schema, the Entra Connect wizard then asks the user to enter

the connection information for your on-premises directories or forests. To configure the directory, the user needs to add an Active Directory account with sufficient permissions for synchronization. Optionally, the Entra connect wizard can be used to create a new Active Directory user but requires credentials of an Enterprise administrator or higher.

If the configured directories are connected successfully, they will be highlighted by a green check mark. Next, for users to sign in to Entra ID with the same credentials as the active directory, a matching domain name is required. If the custom domain name is already verified in Entra Admin center, it should also be automatically verified in the Entra connect wizard as well. It is possible to continue the synchronization process without matching the all UPN-suffixes to the verified domains, but the users will not be able to sign-in to Entra ID with on-premises credentials. Instead, they must use the default domain name of company.onmicrosoft.com.

In a large-scale Active Directory environment, it is advised by Microsoft to do a small-scale pilot deployment of Entra Connect or Cloud sync. For that, OU filtering can be used. With customized settings for Entra Connect, it is possible to filter which domains, Organizational Units (OU) or security groups that should be synchronized to Entra ID. An organizational unit in an Active Directory is a container that can hold users, groups and computers. (Zola, 2023) When installing Entra Connect with Express settings, every object in the on-premises Active Directory in are synchronized to Entra ID. This may include objects that you do not want to synchronize or sensitive data that cannot be synchronized for data security reasons. To minimize operational and security risk, administrators should select which directory objects should be synchronized to Entra ID. Some organizational units are necessary for Active Directory functionality, so they too should be left selected. (Microsoft, 2025f)

Next, choosing how to identify users in the domain and what attribute is used as a source anchor. To uniquely identify users in the Active Directory environment and Entra ID, an attribute must be chosen as a link to from on premises to Entra ID. This attribute is called a sourceAnchor-attribute. Either

let Azure manage the source anchor or choose a specific attribute to be as the source anchor.

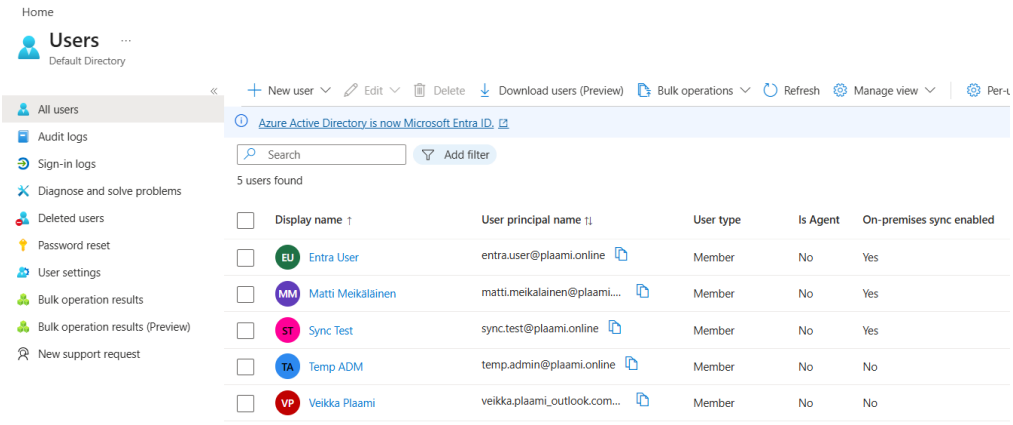
For enhanced functionality, the Entra Connect wizard has many optional features that can be activated and configured, like Exchange hybrid deployment, Exchange mail public folders, Entra app and attribute filtering, Password hash synchronization, Password-, Group- and Device writeback, and Directory extension attribute synchronization. The Exchange hybrid deployment-feature allows Microsoft 365 Exchange-service's mailboxes to exist both in the cloud and the on-premises Active Directory, while Exchange mail public folders-feature allows these mailboxes to be synchronized to Entra ID. Entra app and attribute filtering-feature allows the user to tailor set the synchronization attributes. Password hash synchronization-feature can be selected if federation was selected as the sign-in solution and enables the password hash synchronization to be used as a backup solution. Password writeback allows password changes that originate in Entra ID to be written back to the on-premises directory. Group writeback-feature allows the provision of Microsoft 365 groups directly to the on-premises Active Directory. Device writeback-feature enables conditional access-scenarios. Conditional access is a Zero Trust-policy, that grants access to resources, applications and services if the user can authenticate themselves through a multifactor authentication or denies if they cannot. Finally, the Directory extension attribute sync-feature extends the attributes that can be synchronized with your own custom attributes. (Microsoft, 2025b)

After choosing and configuring the chosen optional features, the synchronizing can begin. The ready to configure-page informs the user on what is going to happen next and what options where chosen. The user will be able to choose if they want to start the synchronization when the configuration completes, and if they want to enable staging mode. Staging mode means that the synchronization will not export any data to the Active Directory or to Entra ID but allows the user to run synchronization cycles to verify that all changes are as expected. Password synchronization and password writeback are not

enabled during staging, even if they were chosen from the optional features. (Microsoft, 2025b)

4.5 Post Synchronization verification

After the configuration, the synchronization from the Active Directory to Entra ID will begin shortly after. To verify that the synchronization is complete, the synchronization status can be viewed from the Entra ID administrator center. In the user-section, it should now be populated by the on-premises users and security groups.



Picture 2. Entra ID, that has successfully synchronized the on-premises users.

By default, Entra Connect sets up a schedule to run a synchronization cycle every 30 minutes. If the synchronization cycle has not yet ran, it can be forced to run by using the ADSync-PowerShell module in the synchronizing server. The ADSync module will install automatically during the configuration of Entra Connect but can manually be imported by using the following command: Import-Module ADSync, and to force a cycle, the following command can be used: ADSyncSyncCycle -PolicyType Delta. The default synchronization cycle can be customized with the Set-ADSyncScheduler command and viewed with Get-ADSynchScheduler command. (Microsoft, 2025e)

After successfully synchronizing with Entra Connect wizard, a monitoring tool called Entra Connect Health automatically installs on your server that was used to synchronize to Entra ID. Microsoft Entra Connect Health helps monitor on-premises identity infrastructure, enhances security and alerts administrators on systems issues, maintenance and performance loss.

5 RESULTS

With the synchronization cycle ran, the correct user profiles, attributes and security groups have been correctly synchronized between the on-premises Active Directory environment and Entra ID. Password writeback functionality was verified by changing the password of a user from Entra admin center and after the synchronization cycle, the updated credentials were applied to the user account within Active Directory. A creation of a new user account was also tested via Entra admin center, to see if it creates a new user account to the on-premises Active Directory. The new user account was synchronized to the Active Directory Users and Computers and was able to log-in to the domain joined Win 11-workstation, confirming that the users that are created from Entra admin center do not differ from users that are created from the Active Directory Users and Computers. Users within the on-premises Active Directory and Entra ID have the correct UPN-suffix and can use the same credentials across all platforms via Single Sign-on. The successful migration to hybrid-cloud has enabled unified identity management across on-premises Active Directory environment to Entra ID, expanded access control capabilities as well as increasing scalability and reliability.

5.1 Further Development

Although the migration from a purely on-premises Active Directory environment to hybrid identity has been successfully implemented, further development can be implemented by transitioning to a full cloud model. A full cloud infrastructure model means that all the applications, services and data are hosted purely in the cloud, without maintaining a on-premises server or data centre. These applications, services and computers are operated in a virtualised environment that is managed by a cloud service provider. Full cloud model offers very high availability, scalability and mobility, while automating updates and maintenance. However, full cloud model also dependant on internet connectivity, as well as reliance to a single cloud service provider.

While full cloud eliminates hardware expenses, it also increases cloud service costs drastically. (Savenet, n.d.)

6 SUMMARY

The objective of this thesis was to design and implement a migration from an on-premises Active Directory environment to hybrid cloud model using Entra ID. While designing the virtual machines and preparing for the migration, I ran into many issues with Azure and Entra ID licensing. Due to this, many services and features, like Cloud sync and Connect Health, may not have been explained or tested thoroughly. Entra ID licence requires a company e-mail address to purchase, so unfortunately, I could not purchase a licence. Nevertheless, the migration was a success. Validation and testing confirmed that it was functioning as expected, and the synchronization cycles ran correctly. The Active Directory objects were replicated to Entra Id, and newly created users were provisioned correctly within on premises across both environments.

REFERENCES

Cloudflare. (n.d.). What is the cloud? I Cloud definition.
Retrieved November 14, 2025, from
https://www.cloudflare.com/en-gb/learning/cloud/what-is-the-cloud

F5. (n.d.). What is Hybrid Cloud?
Retrieved November 29, 2025, from
https://www.f5.com/glossary/hybrid-cloud

Fortinet. (n.d.). What Is Single Sign-On (SSO)?
Retrieved March 13, 2026, from
https://www.fortinet.com/resources/cyberglossary/single-sign-on

Google Cloud. (n.d.). What is a cloud service provider?
Retrieved November 14, 2025, from
https://cloud.google.com/learn/what-is-a-cloud-service-provider

Google Cloud. (n.d.). PaaS vs IaaS vs Saas: What's the difference?
Retrieved November 21, 2025, from
https://cloud.google.com/learn/paas-vs-iaas-vs-saas

Hewlett Packard Enterprises. (October 31, 2025). What is multicloud?
Retrieved November 14, 2025, from
www.hpe.com/us/en/what-is/multi-cloud.html

Indu, I., Anand, R. Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, 21(4), pp. 488-574.
https://doi.org/10.1016/j.jestch.2018.05.010

Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Microsoft. (n.d. -a). Query and fix invalid object attributes with the IdFix tool Retrieved March 18, 2025, from https://microsoft.github.io/idfix/

Microsoft. (n.d. -b). What is multicloud? Retrieved November 14, 2025, from https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-multi-cloud

Microsoft. (n.d. -c). What is software as a service (SaaS)? Retrieved November 21, 2025, from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas

Microsoft. (August 20, 2020). Active Directory Schema (AD Schema). Retrieved February 24, 2026, from https://learn.microsoft.com/en-us/windows/win32/adschema/active-directory-schema

Microsoft. (July 16, 2024a). Set up directory synchronization for Microsoft 365. Retrieved January 12, 2026, from https://learn.microsoft.com/en-us/microsoft-365/enterprise/set-up-directory-synchronization?view=o365-worldwide

Microsoft. (October 7, 2024b). Prepare a nonroutable domain for directory synchronization. Retrieved March 11, 2026, from https://learn.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide

Microsoft. (December 19, 2024c). Managing custom domain names in your Microsoft Entra ID. Retrieved February 17, 2026, from https://learn.microsoft.com/en-us/entra/identity/users/domains-manage#set-the-primary-domain-name-for-your-microsoft-entra-organization

Microsoft. (March 22, 2025a). Authentication vs. authorization. Retrieved March 2, 2026, from https://learn.microsoft.com/en-us/entra/identity-platform/authentication-vs-authorization

Microsoft. (April 9, 2025b). Custom installation of Microsoft Entra Connect. Retrieved February 20, 2026, from https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-install-custom

Microsoft. (April 9, 2025c). Hybrid scenarios. Retrieved January 12, 2026, from https://learn.microsoft.com/en-us/entra/identity/hybrid/common-scenarios

Microsoft. (April 9, 2025d). Microsoft Entra Connect and federation. Retrieved March 4, 2026, from https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-fed-whatis?source=recommendations¨

Microsoft. (April 9, 2025e). Microsoft Entra Connect Sync: Scheduler. Retrieved February 25, 2026, from https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-feature-scheduler

Microsoft. (April 9, 2025f). Microsoft Entra Connect Sync: Configure filtering. Retrieved March 13, 2026, from https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering

Microsoft. (April 9, 2025g). User sign-in with Microsoft Entra pass-through authentication. Retrieved March 2, 2026, from https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta

Microsoft. (April 9, 2025h). What is Microsoft Entra Connect? Retrieved January 13, 2026, from https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-azure-ad-connect

Microsoft. (February 5, 2026a). What is Azure Bastion? Retrieved February 5, 2026, from https://learn.microsoft.com/en-us/azure/bastion/bastion-overview

Microsoft. (February 24, 2026b). What is Microsoft Entra Cloud sync? Retrieved March 4, 2026, from https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync

PingIdentity. (n.d.). Pingfederate. Retrieved March 13, 2026, from https://www.pingidentity.com/en/product/pingfederate.html

Posey, B. (December 30, 2024). Top public cloud service providers of 2025: How they compare. Retrieved from March 15, 2026, from https://www.techtarget.com/searchcloudcomputing/tip/Top-public-cloud-providers-A-brief-comparison

Proofpoint. (n.d.). What is Active Directory? Retrieved November 27, 2025, from https://www.proofpoint.com/us/threat-reference/active-directory

Rountree D. & Castrillo I. (2013). The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice. Newnes. (pp. 6-7).

Savenet. (n.d.). Hybrid vs. Full Cloud: Which IT Infrastructure Model Suits Your Business? Retrieved March 7, 2026, from https://savenetsolutions.ie/news/hybrid-vs-full-cloud-which-it-infrastructure-model-suits-your-business/

Silverfort. (n.d.). Active Directory.
Retrieved November 27, 2025, from
https://www.silverfort.com/glossary/active-directory/

Uotila, A. (2023). Pilvipalveluiden yleistyminen Suomessa. [Bachelor's thesis, Haaga-Helia University of applied sciences]. Theseus. https://urn.fi/URN:NBN:fi:amk-2023052614578

Zola, A. (April 10, 2023). Organizational unit (OU).
Retrieved February 20, 2026, from
https://www.techtarget.com/searchwindowsserver/definition/organizational-unit-OU