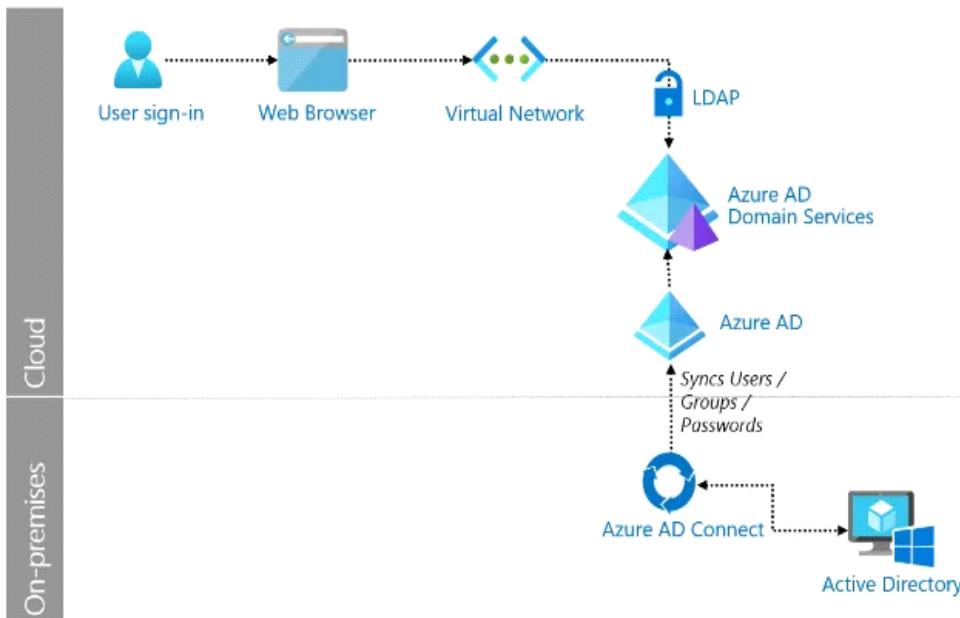


# Pilvipalvelu ja hybridimalli

Saturday, October 18, 2025 10:19

Azure AD (entra ID) + virtualisoitu Vmworkstation playeri (windows serveri) - **Hybridimalli**



## ◊ Hybridimalli

Tämä on hyvin yleinen ratkaisu yrityksissä:

1. **On-prem AD DS (VM1)**
  - Käyttäjät ja koneet liitetään tähän domainiin.
  - Perinteiset GPO:t, sisäverkon resurssit, tiedostopalvelimet jne. hallitaan täällä.
2. **Azure AD Connect (synkronointi)**
  - Asennetaan VM1:lle ( tai muulle palvelimelle).
  - Synkronoi käyttäjät ja salasanat ( tai hashit ) on-prem AD:stä Azure AD:hen.
  - Käyttäjällä on sama tunnus ja salasana sekä paikallisesti että pilvessä.
3. **Azure AD (Entra ID)**
  - Käyttäjät voivat kirjautua Microsoft 365:een, Teamsiin, pilvisovelluksiin samoilla tunnuksilla.
  - MFA, Conditional Access ja muut pilvipalveluiden turvaominaisuudet käytössä.

## ◊ Käytännön hyödyt hybridistä

- **Yksi identiteetti:** käyttäjällä sama käyttäjätunnus ja salasana kaikkialla.
- **Hallinta:** sisäverkossa GPO:t ja perinteinen AD, pilvessä modernit turvaominaisuudet.
- **Joustavuus:** voit siirtyä vähitellen kohti pilveä ilman että kaikki pitää muuttaa kerralla.

Azure Entra ID ja VM1 Windows Server AD DS, voi rakentaa **hybridimallin** Azure AD Connectin avulla. Tämä on itse asiassa Microsoftin suositteleva malli monille pk-yrityksille ja organisaatioille, jotka haluavat hyödyntää sekä pilveä että perinteistä AD:tä.

Jos yritys aikoo ottaa käyttää Entra ID:tä hybridistä, GPO-asetuksia ei tarvitse heti luovuttaa – mutta siirtymisen Intuneen ja Defenderiin on suositeltavaa pitkällä aikavälillä. Tämä vaatii oikeat lisenssit, kuten Microsoft 365 Business Premium, E3 tai E5.

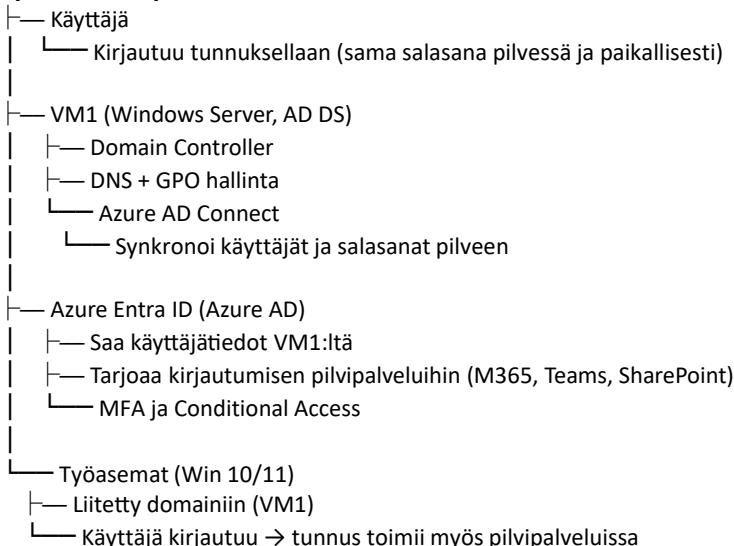
- **Johtopäätös:** Jos käytössä on **hybrid Entra ID** (eli laitteet ovat sekä AD- että Entra ID-joinattuja), voi silti **jatkaa GPO-asetusten käyttöä**, mutta **Intune tarjoaa joustavuutta ja pilvihallintaa**, erityisesti etätyössä ja mobiiliilaitteiden hallinnassa

## ✎ Hybridikäyttö: GPO + Intune

- Voi käyttää GPO:ta Intune-rekisteröinnin automatisointiin hybridilaitteilla.
- Microsoft Defender for Endpoint voidaan integroida hybridisti AD-laitteisiin Intunen kautta.
- GPP (Group Policy Preferences) ei toimi Entra ID-joinatuilla laitteilla, joten ne kannattaa korvata Intune-profileilla tai kolmannen osapuolen työkaluilla.

Jos aikoo luovuttaa GPO käytöstä, ennen sitä pitää testata Intunen käyttöä fyysisesti + hiekkaympäristön ennen kuin viede muille käyttäjille työaseminsa. Sama pätee varmistuksena on lisenssi kattaus (Intune + Defender + Entra ID premium) ja sama pätee dokumentointi siirtymisen strategia.

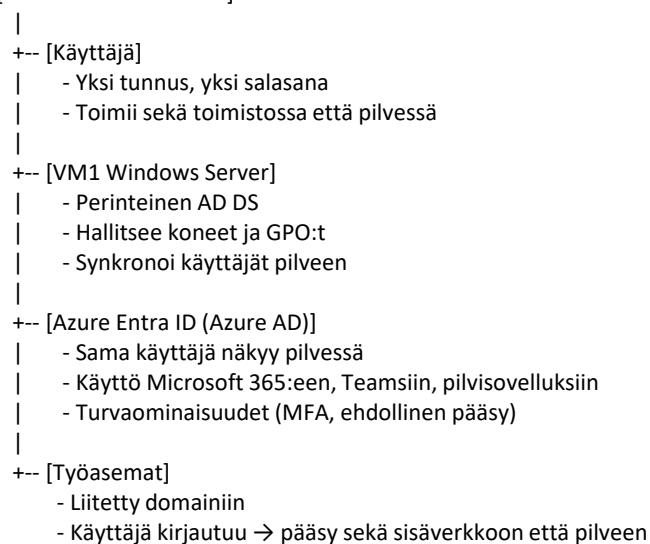
## Hybrid Identity Environment



Esim. **VM1 hallitsee paikallista domainia**, ja **Azure Entra ID** saa käyttäjätiedot synkronoituna, jolloin käyttäjällä on yksi identiteetti molemmissa.

## Mindmap tyylinen selostus:

[HYBRIDI-IDENTITEETTI]



#####

Hybridin ympäristön konfigurointi Azure AD:n ja paikallisen **Windows Serverin AD:n** välillä ei ole teknisesti mahdotonta, mutta se vaatii **huolellisuutta ja suunnittelua**. Esimerkiksi **Azure AD Connectin** käyttöönotto on verrattain suoraviivainen prosessi, mutta siinä on muutamia vaiheita ja valintoja, jotka kannattaa tehdä huolellisesti.

Hybridimallin (Azure AD + paikallinen Windows Server AD) käyttöönottoa ja mahdollisia vaikutuksia, jos malli päätetään katkaista:

## Hybridimallin käyttöönotto

### 1. Ennen käyttöönottoa:

- **DNS ja verkko:** Paikallisen AD DS:n DNS:n täytyy olla kunnossa. Työasemat käyttävät sitä nimipalveluna.
- **Azure AD Connect:** Tärkein työkalu, joka synkronoi käyttäjät, ryhmät ja salasanahashit Azure Entra ID:hen. Asennus on yksinkertainen, mutta vaatii domain admin -tunnukset ja Azure-tenantin admin-oikeudet.
- **Salasanapolitiikat ja identiteettien yhtenäisyys:** Huomioi käyttäjätunnusten ja UPN-suffiksien yhtenäisyys Azure AD:n kanssa, jotta käyttäjät voivat kirjautua sujuvasti molemmissa ympäristöissä.
- **MFA ja Conditional Access:** Suunnittele nämä etukäteen, jotta käyttäjät eivät jää jumiin kirjautumisen aikana.

### 2. Asennusprosessi:

- **Azure AD Connectin asennus:** Helposti suoritettavissa, mutta valitse huolellisesti synkronointiasetukset (koko AD, tietyt ryhmät, jne.).
- **Hybrid Azure AD Join:** Yhdistää laitteet Azure AD:hen, jolloin työasemat ja palvelimet voivat kirjautua molempien ympäristöihin.

- **Single Sign-On (SSO):** SSO parantaa käyttäjäkokemusta, sillä samat tunnukset toimivat paikallisissa ja pilvipohjisissa sovelluksissa.

### 3. Erityisvaatimukset:

- **Verkko ja yhteysvaatimukset:** Azure AD Connectin täytyy pystyä muodostamaan yhteys Azure AD:hen (internet-yhteys vaaditaan).
- **Salasanan synkronointi:** Määritä, käytetäänkö "Password Hash Sync" vai "Pass-through Authentication" salasanan synkronointiin.
- **Testaus:** Testaa ensin pienessä ympäristössä ennen laajempaa käyttöönottoa.

## Jos hybridimalli katkaistaan

### 1. Azure AD Connectin poistaminen:

- **Paikallinen AD:** Paikallinen Windows Server AD jatkaa toimintaansa normaalisti. Työasemat voivat kirjautua domainiin, GPO:t ja sisäverkon resurssit toimivat kuten ennenkin.
- **Azure Entra ID:** Käyttäjät, jotka on synkronoitu Azure AD:hen, muuttuvat "pilvikäyttäjiksi" (disconnected state). Salasanat eivät enää päivity paikallisesta AD:stä Azure AD:hen. Käyttäjä voi vaihtaa salasanan pilvessä, mutta se ei synkronoidu takaisin paikalliseen AD:hen.
- **Microsoft 365 ja muit pilvipalvelut:** Pilvipalvelut toimivat edelleen, mutta identiteetit eivät ole enää yhtenäisiä (esim. eri salasanat pilvessä ja paikallisessa AD:ssä).

### 2. Jos haluat palata hybridiin:

- Jos hybridimallin synkronointi katkaistaan, pitää suunnitella huolellisesti, miten vältetään duplikaattitilanteet tai ristiriidat käyttäjätiedoissa.

### 3. Azure Entra ID ilman synkronointia:

- Azure AD jää käyttökelpoiseksi, mutta se ei enää synkronoidu paikallisen AD:n kanssa. Paikalliset käyttäjät eivät pääse pilvipalveluihin ja pilvikäyttäjät eivät pääse paikallisiin resursseihin.

## Suoositukset ja varautuminen

- **Testaus ja suunnittelu:** Ennen kuin ottaa hybridimallin käyttöön, testaa synkronointi ja varmista, että Azure AD Connect on oikein konfiguroitu.
- **Käyttäjäpolitiikka ja tuki:** Varmista, että käyttäjillä on selkeät ohjeet kirjautumisesta ja pääsyn kaikkiin tarvittaviin järjestelmiin, erityisesti jos hybridimalli katkaistaan.
- **Varautuminen:** Tee varmuuskopioita ja testaa palautusprosessit, jotta ei menetetä tärkeitä tietoja synkronointivirheiden vuoksi.