



Ilpo Hautala

# VDI-MALLIN TUOTTAMINEN JA TESTAUS MICROSOFT AZURE -YMPÄRISTÖSSÄ OPETUKSEN TUEKSI

Raportti, Moottori-hanke 2023

MOOTTORI

centria  
ammattikorkeakoulu



kpedu



Vipuvoimaa  
EU:lta  
2014–2020



# SISÄLLYSLUETTELO

YLEISTÄ.....	3
HALLINTA.....	3
VDI-YMPÄRISTÖN RAKENTAMINEN.....	4
AZURE VDI -YMPÄRISTÖN TEKNINEN RAKENNE.....	6
YHDISTÄMINEN VDI-YMPÄRISTÖÖN.....	7
KOKEMUKSIA HYVISTÄ JA HUONOISTA PUOLISTA.....	8
LOPPUTULOS .....	9

## YLEISTÄ

Moottori-hankkeessa yhtenä osa-alueena oli VDI-ympäristön (Virtual Desktop Infrastructure) luominen testikäyttöön sekä jatkokehittäminen opetuksen tueksi. Alustaksi valikoitui Microsoftin (MS) Azure Virtual Desktop -ympäristö. Centria-ammattikorkeakoululla oli olemassa jo tiettyjä palveluita MS Azuressa, ja siitä syystä MS Azure alustana tuntui sopivalta ratkaisulta.

Lähdimme kartoittamaan, kuinka VDI-ympäristö luodaan, ja mitä se vaatii teknisesti, taloudellisesti ja ajallisesti. Valitsimme testausmalleiksi kahden erilaisen lähestymistavan mallin: ns. perusopetusmallin (esim. Linux-ympäristön opettaminen ja perusohjelmistot, jotka eivät vaadi grafiikkakiihdytintä) ja grafiikka kiihdytetty -mallin (3D-suunnittelu). Lisäksi halusimme saada ymmärrystä ja kokemusta skaalautuvuudesta, kloonauksesta ja varmistamisesta.

Perusopetusmallin VDI-ratkaisu toteutettiin MS Azuressa kahdella virtuaalityöasemalla. Niihin valittiin perustason virtuaalinen tietokone (Standard D2s v3). Laitteessa on Intelin prosessori 2 ytimellä, ja 8 Gib muistia. Levyksi valittiin standardin mukainen SSD, jossa 127 GiB tallennuskapasiteetti (Standard SSD LRS, 127 GiB). Kustannus tälle virtuaalikoneelle oli 62,85 €/kk.

Grafiikka kiihdytetty -mallin VDI-ratkaisu otettiin kokeeksi NV-sarjasta NV4as-V4. Kyseinen malli on optimoitu perustason grafiikkakiihdytystä vaativaan työhön, esim. grafiikkatyökalut. Kyseinen malli on AMD-prosessoreilla toteutettu, ja sisältää 4 ydintä sekä 14 GiB muistia. Virtuaalikoneeseen saa neljä SSD-levyä sekä kaksi 1 Gib verkkokorttia. Kustannus tälle virtuaalikoneelle oli 153,84 €/kk.

VDI-käyttöön on mahdollista saada hyvin laaja skaala eri tason virtuaalikoneita ja -palveluita. Hintahaitari on 50-5000 €/kk. Hinta onkin optimoinnin kannalta oleellinen, koska kustannuksia syntyy herkästi. Käyttö tulee miettiä tarkkaan ja mitoittaa palvelu juuri oikeanlaiseksi. Samoin käyttöajan automatisointi ja automaattinen käynnistys/sammutus-toiminto säästää rahaa. Esimerkiksi yöaika on syytä rajata pois. Toinen merkittävä seikka on, kuinka opettaja/hallinnoija saa reaaliaikaista tietoa kustannuksista. Tähän ratkaisuna on budjetointi ja ilmoitusten hallinta. Esimerkiksi tietyille kurssille luodaan budjettiarvo ja sen mukaan sääntö, joka lähettää tiedon opettajalle/hallinnoijalle kustannuksista.

## HALLINTA

Hallintamallilla on merkitystä kokonaiskuvan määrittelyssä: kuinka MS Azure -kapasiteettiamme käytetään, ja millä ehdoilla? Pääsyhallinnan miettiminen sekä tietoturvalliset yhteystavat ovat oleellisia osia määrittelyssä. Tilauksia (Subscriptions) voidaan käyttää erittelemään VDI omaksi kokonaisuudekseen, ja tarvittaessa myös erittelemään VDI-ratkaisut toisistaan. Ns. Landing Zone -ajattelumallissa on valmiiksi määritellyt VM-mallit (Virtuaalikoneet), lo-kaatio-asetukset ja oikeudet valmiina, mikä on hyvä käytäntö. Joten kun tarve ilmenee, voidaan ympäristö toteuttaa nopeasti, turvallisesti ja organisaation ohjeiden mukaan.

# VDI-YMPÄRISTÖN RAKENTAMINEN

VDI-ympäristön rakentaminen alkaa uuden MS Azure Virtual Desktop -resurssin luomisella. Tässä resurssissa on mahdollisuus luoda ensimmäinen VDI-ympäristö ohjatulla toiminnolla.

## Ohjattu toiminto luo VDI-ympäristön seuraavasti:

- Host pool – tietty ryhmä virtuaalikoneita, joihin voidaan kohdistaa asetuksia
- Applikaatioryhmä – ohjelmien ja appien ryhmä
- Yksi käyttäjä – järjestelmänvalvoja, jolla voidaan asentaa halutut ohjelmat virtuaalikoneelle.

## Toinen vaihtoehto on luoda ympäristö juuri omaan tarpeeseen:

- Host pool – alue valituille virtuaalikoneille
- Applikaatioryhmä – valitut ohjelmistot
- Useampi käyttäjä – esim. Role Based Access Control (RBAC) -malli, joka määrittää käyttäjien oikeudet ryhmien mukaan (esim. opettaja, oppilas).

Home > Azure Virtual Desktop

### Azure Virtual Desktop | Host pools

Search

+ Create Manage view Refresh Export to CSV Open query Assign tags Delete

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 2 of 2 records. No grouping List view

<input type="checkbox"/>	Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓	Host po... ↑↓	Load bal... ↑↓	Applicati... ↑↓	
<input type="checkbox"/>	MotorVDIpool	MoottoriResurssit	West Europe	KKP-MoottoriVDI-400...	Pooled	Depth-first	3	***

KUVA 1.

## Perusasetuksissa määritellään tilaus, identiteetin hallinta (Azure Active Directory tai esim. Lokaalitunnukset) ja tyyppi:

- Resurssiryhmä – kaikki resurssit
- Lokaatio – missä palvelut sijaitsevat
- Virtuaaliverkko topologia – esim. kaikki virtuaalikoneet liitetään (Verkkoasetukset)
- MS Azure -hallintatunnukset
- Domain Admin -tunnusten määrittely.

Virtuaalikoneiden asetuksissa määritellään, käytetäänkö virtuaalikonetta per käyttäjä vai useampi käyttäjä yhtä aikaa. Virtuaalikoneissa voidaan käyttää valmiita levykuvia Microsoftin kirjastosta tai vaihtoehtoisesti omasta tallennuspaikasta. Virtuaalikoneen resurssit määritellään myös, eli edellä mainitut valmiit konetyypit. Nimeämiskäytäntö voidaan valita, sekä kuinka monta virtuaalikonetta luodaan.

**Basic**

Resource ID  
/subscriptions/3fca8fe8-433b-4626-a23e-06e04d7223d9/resourceGroups/MoottoniResurssit/providers/Microsoft...

Resource group  
MoottoniResurssit  
[Change resource group](#)

Subscription  
3fca8fe8-433b-4626-a23e-06e04d7223d9  
[Change subscription](#)

Location  
West Europe

Name  
MotorVDIpool

**Configuration**

Personal desktop  Yes  No

Preferred app group type

Start VM on connect  No  Yes

Validation environment  No  Yes

Friendly name

Description  
Created through the Azure Virtual Desktop extension

Load balancing algorithm

Max session limit

KUVA 2.

Käyttäjämäärittely tapahtuu seuraavaksi. Määritellään testikäyttäjätili, joka saa ryhmäoikeuden MS Azure Virtual Desktop Users -ryhmään. Jos tiedossa on jo käyttäjäryhmä tai käyttäjät, voidaan heidätkin nimetä jo tässä vaiheessa, mutta se onnistuu myös myöhemmin. Valitsimme RBAC-vaihtoehdon, eli käyttäjiä hallitaan ryhmäperusteisesti.



KUVA 3.

Seuraavaksi on VDI-ympäristön luonti ja testausvaihe. MS Azuren automatiikka valmistelee ympäristön annettujen reunaehtojen mukaan. Vaihtoehtona on luoda rinnalle koeympäristö, jolloin vain Host pool -valinnoissa valitaan Validation Environment ja lisätään käyttäjät MS Azure Virtual Desktop Validation -ryhmään. Tällä toiminnot voidaan testata ja siirtää myöhemmin tuotantoon.

Validation environment ⓘ  No  Yes

KUVA 4.

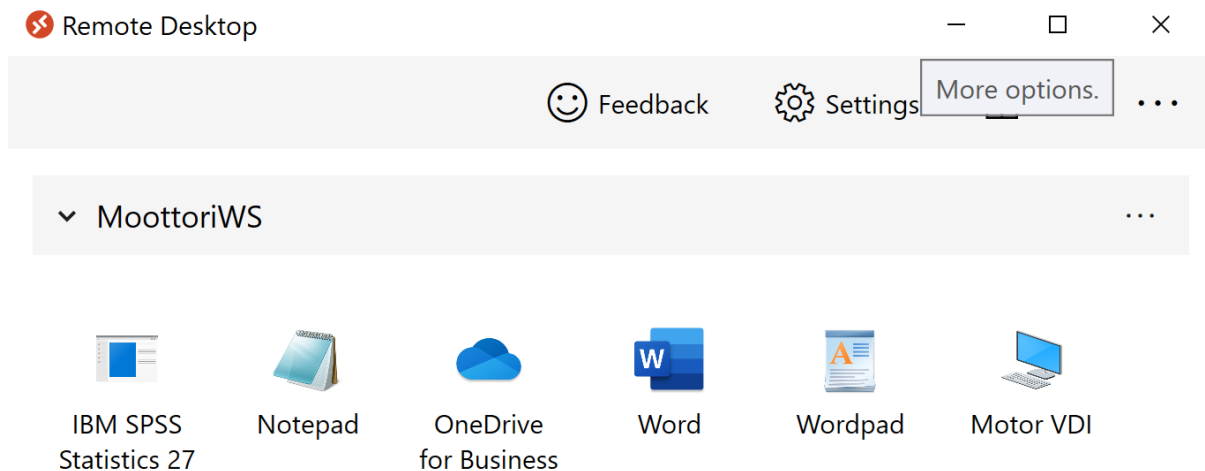
## AZURE VDI -YMPÄRISTÖN TEKNINEN RAKENNE

Azure VDI -ympäristölle vaaditaan Subscription, jonka alle tulee resurssiryhmä. Resurssiryhmä sisältää kaiken tarvittavan: virtuaaliverkot, virtuaalikoneet, VPN-putket, Host poolit, App poolit jne. Rakenne mahdollistaa skaalautuvuuden joko manuaalisesti tai automatisoituna esim. käyttäjämääriin pohjautuen. Käyttäjähallinta tapahtuu Azure AD -ympäristössä ryhmien avulla. Tämäkin voi tapahtua automaattisesti pohjautuen käyttäjätietoihin, esim. opiskelijaryhmään.

Tietoturvaa varten on olemassa Microsoft Defender -tuoteperhe. Myös kolmannen osapuolen tietoturvatkaisuja voidaan käyttää virtuaalikoneissa (esim. F-secure). Kokonaisuuden kannalta on kuitenkin hyvä tukeutua Microsoftin tuotteisiin, jolloin saadaan kokonaiskuva tilanteesta ns. komentokeskukseen (lokit, haavoittuvuudet, päivitykset jne.).

# YHDISTÄMINEN VDI-YMPÄRISTÖÖN

Kokeilimme yhdistämistä Windows Remote Desktop Clientin (Kuva 5.) avulla sekä selaimen kautta (Kuva 6.). Molemmat tavat olivat toimivia ja nopeita ottaa käyttöön, ja käyttökokemus oli hyvä. Jaoimme käyttäjille erilaisia paketoituja olemassa olevista resursseista: jokaiselle käyttäjälle voidaan määrittää eri ohjelmat, virtuaalikoneet ja pääsyoikeudet.



KUVA 5.



KUVA 6.

Kokeilimme kuvien mukaisesti virtuaalikoneympäristöä sekä ohjelmien jakamista. Ohjelmistona oli Windowsin sisään rakennettuja ohjelmia sekä erikseen asennettavia ja lisensoitavia ohjelmia. Lisenssipalvelut tuotettiin OnPremise-ym- päristöstä VPN-putkea käyttäen virtuaaliympäristöön. Tämän konfiguroiminen vaatii ymmärrystä sekä MS Azuresta, että käytössä olevasta VPN-ratkaisusta.

Muita mahdollisuuksia käyttää VDI-ympäristöä löytyy IOS, OS X ja Android -käyttöjärjestelmiin. Microsoftin Store Clientin ja Thin Clientin käyttö on myös mahdollista. Mahdollisuus tietoturvalliseen työskentelyyn löytyy Bastion-yhteydestä. Huomioitavaa on, että Bastion suojaa vain yhteyden, eli työaseman täytyy olla myös kovetettu. Tämä on hyvä huomioida esim. opinnäytetöissä, joissa käsitellään sensitiivistä materiaalia.

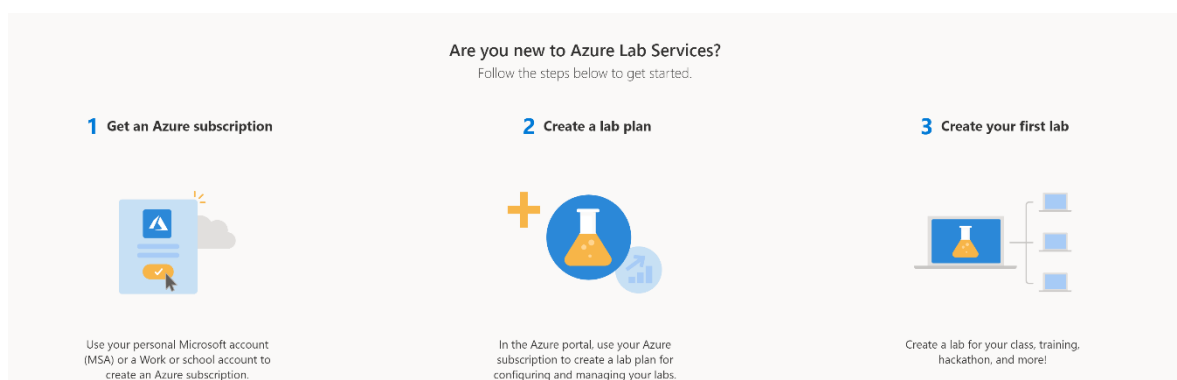
## KOKEMUKSIA HYVISTÄ JA HUONOISTA PUOLISTA

Kokemuksiemme perusteella Azure VDI -ympäristö soveltuu hyvin opetuksen tueksi teknisessä mielessä sekä toimivuudeltaan. VDI-ympäristössä voidaan tuottaa erilaisia turvallisia ympäristöjä oppilaiden käyttöön ja se mahdollistaa ns. hands on -opetuksen.

Hyviä puolia ovat turvallisuus, skaalautuvuus sekä ajasta ja paikasta riippumaton opetus ja oppiminen. Oppilas voi esim. tehdä harjoitustyön edullisemmalla tietokoneella käyttäen koulun resursseja kotoa käsin. Tällaisia voivat olla erilaiset tietotekniikkaan tai suunnitteluun liittyvät opetusjaksot. Esimerkkinä WordPress Multisite -ympäristö, jota opettaja hallinnoi ja opiskelijoilla oli omat alustat tehtäviä varten.

Huono puoli ovat kustannukset, jotka kasvavat herkästi suuriksi. Kustannukset voivat olla tuhansia euroja kuussa. Oikeastaan tämä on ainoa huono puoli MS Azuren -palveluiden käytössä. Tätä voidaan kompensoida pudottamalla fyysisiä luokkia pois, eli vähentämällä konemäärää. MS Azure VDI -ympäristössä ei tule ns. rautahankintoja lainkaan, eli ympäristön vanheneminen on hitaampaa, jos oppilaat toimivat omilla laitteillaan. Kuitenkin on huomioitava oppilaiden laitteiden tietoturvan taso esim. käyttämällä pääsynhallinnassa ns. Conditional Access Policyja (Ehdollinen pääsy), joilla voidaan vaatia tietty päivitystaso liittymisen ehtona.

Perusasioiden opetuksessa tulisi jatkossa käyttää mieluiten MS Azure Lab Services -palvelua. Opettajalle luodaan oma laboratorio, johon hän voi asentaa halutun määrän virtuaalikoneita halutulla käyttöjärjestelmällä ja ohjelmilla. Tätä olemme testanneet Linux-kursseilla. Tässä palvelussa opettaja voi määrittää opetustunnit sekä niiden päälle tulevat harjoitusajat. Opettaja voi muuttaa asetuksia tilanteen mukaan, ja hän näkee mitä kyseinen skenaario maksaa maksimissaan. Tämä helpottaa resurssointia ja suunnittelua merkittävästi.



KUVA 7.



## LOPPUTULOS

Lopputuloksena koeajasta meille jäi käsitys siitä, mitä MS Azure VDI -ympäristön käyttöönotto, ylläpito sekä varmistaminen vaatii. Saimme mallin, millä voimme jatkaa tutkimista, ja luoda ympäristöjä opettajien ja oppilaiden käyttöön.

Osaamisen laajentaminen MS Azuren VDI -ympäristön suhteen on tärkeässä roolissa, jotta tulevaisuudessa saamme kaiken irti lisensseistämme. Opetuksen tukeminen teknisesti vaatii myös osaamisen laajentamista kokonaisuutena. Samoin on syytä rajata, mitä tehdään MS Azure Lab Services -palvelussa ja mitä varsinaisessa VDI-ympäristössä, joka on monipuolisempi.

Tekniikoiden kehittyessä ja tämän kokeilun pohjalta voimme jatkaa kehitystyötä yhdessä opetuksen kanssa. Se vaatii koulutusta niin opettajille kuin tietohallinnolle, jotta käytöstä saadaan paras hyöty.