

# 1. Windows Server - eka lataus

Friday, August 9, 2024 12:02 PM

## Windows Server - koskien Active Directory - latausta - START HERE; - TÄMÄ ON LADATTU SITTEN SYKSY 2024

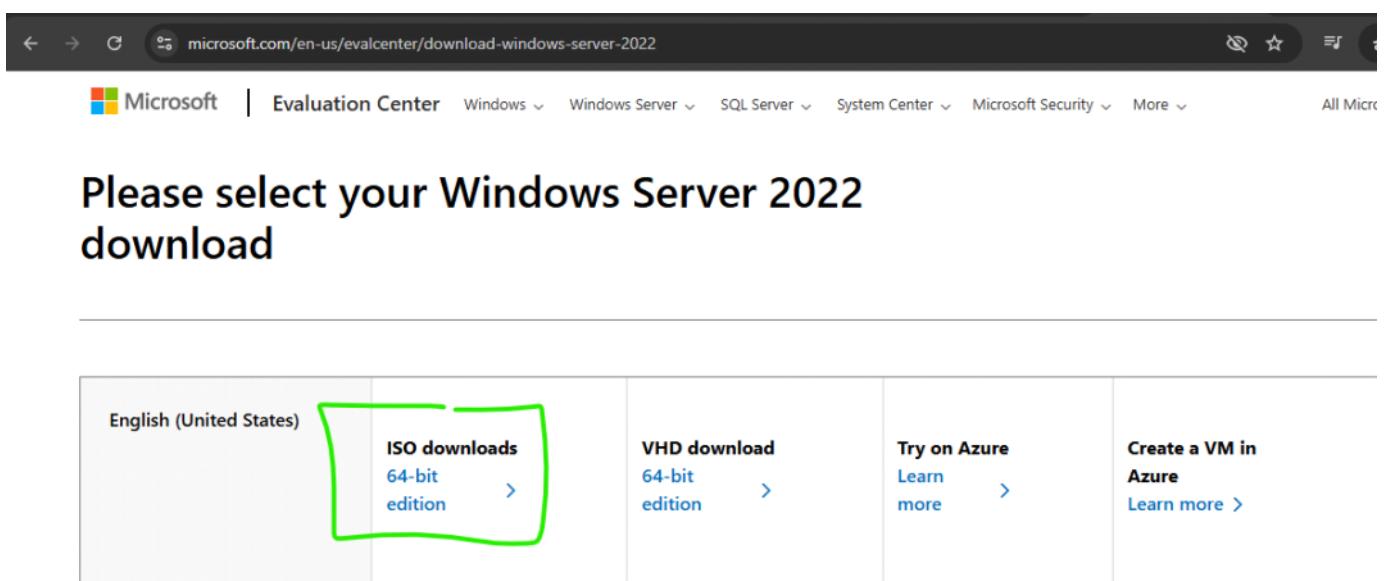
### Tarvittavat välineet ja mitkä sivustot:

Sama ohje löytyy [enkkuks](#), mutta tämä alempi menee suomeksi: <https://medium.com/@botgonbayar/part-1-setting-up-active-directory-c59677048c92>

<https://medium.com/@mohanad.hussam23/setting-up-an-active-directory-lab-for-pentesting-part-1-88f38dd3c8af>

Tarvittava materiaali löytyy tältä eli tarvittaan ISO tiedostoa:

Tämä tiedoston n. vajaa yli 4-5GB



The screenshot shows the Microsoft Evaluation Center download page for Windows Server 2022. The page has a header with the Microsoft logo and navigation links for Windows, Windows Server, SQL Server, System Center, Microsoft Security, and More. Below the header, there is a main title: "Please select your Windows Server 2022 download". Underneath the title, there are four main download options arranged in a grid:

English (United States)	ISO downloads 64-bit edition >	VHD download 64-bit edition >	Try on Azure Learn more >	Create a VM in Azure Learn more >
	ISO downloads 64-bit edition >			

Tarvitaan Vmware workstation virtualisoitu ohjelma:

Tämä on muuttunut niin kantsii tarkista mistä lataa google:sta ja vähä lisätietoa:

Pitää olla nimellä (**vmware workstation**) ja jos on virtualbox (virtualisoitu ohjelma) sekin käy, mutta pitää tarkistaa että ISO ohjelma levy tukee siihen.

Vmware workstation kannattaa ladata ainakin viimeismän versio mukaan ja tarkista ettei ole teknisiä ongelmia.



Search

Search

## Downloading VMware Workstation Pro

Article ID: 344595

Feedback Subscribe

Updated On: 06-25-2025

Products

VMware Workstation Pro

Issue/Introduction

This article provide steps to download VMware Workstation Pro.

Symptoms include,

- Unable to download VMware Workstation
- The download stops intermittently or does not complete
- An auto update to a newer version of VMware Workstation fails

**Henkilökohtaisen kone** pitää olla riittävä vahva ja ainakin minimissään:

- 8GB RAM (muisti ja jos on enemmän se on hyvä)
- 40GB muistia
- Sallii virtualisoidun BIOS.

## 2019 vs 2025 (Windows 10 vs 11)

Tämä on ainakin tärkeä olennainen tieto, koska konffauksen windows serverin jälkeen saattaa huomata miksi siinä on Windows 10 ja Windows 11 ulkonäköinen teema?

- **Windows Server 2019 Active Directory -konfigurointi menee päätärteittäin täysin samalla tavalla myös vuosina 2025 eteenpäin**, mukaan lukien uudemmat versiot kuten Windows Server 2022 ja tulevat 2025-versiot (esim. vNext).

## Miksi se menee samalla tavalla?

### Active Directoryn perusrakenne ei ole muuttunut

- Active Directory (AD DS) on **yhteensopiva taaksepäin** Windows Server 2000:sta asti
- AD:n ydinkonfigurointi (root, forest/domain, DSRM, DNS, replikointi jne.) on pysynyt **melko samanlaisena vuosikymmenien ajan**
- Uudemmissa Windows Server -versioissa tulee lisää **turvallisuusominaisuksia**, mutta **perusasennus & -konfigurointi** on lähes identtinen

**Windows Server -versio AD:n konfigurointi muuttunut? Kommentti**

Windows Server 2012 → 2019  Ei merkittäviä muutoksia Peruskonffaustäysin sama

Windows Server 2022  Ei suuria muutoksia Lisäsuojausominaisuksia, mutta konffaustäysin sama

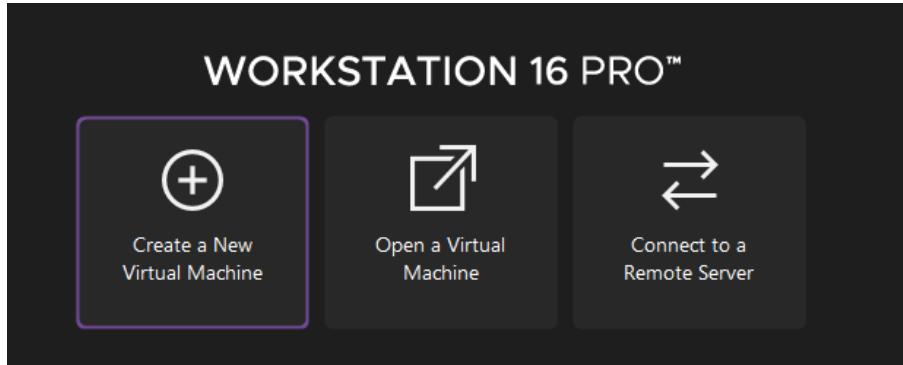
Windows Server 2025 (tuleva vNext)

Tämä ohje voi vielä toimiva seuraavan 2030 asti - mutta hyvä ohje ja hyvä alku pohja kuitenkin.

## LUO UUSI VIRTUALISOITU OHJELMA & WINDOWS SERVER KÄYTTÖÖN -

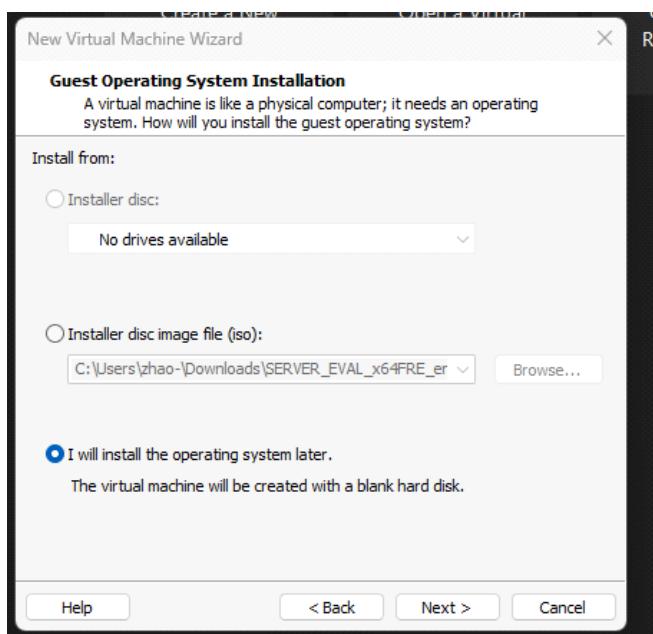
## START HERE;

TÄMÄN WINDOWS SERVERI LATAUS ALK. LOKAKUU - 2025 (10.10.2025)

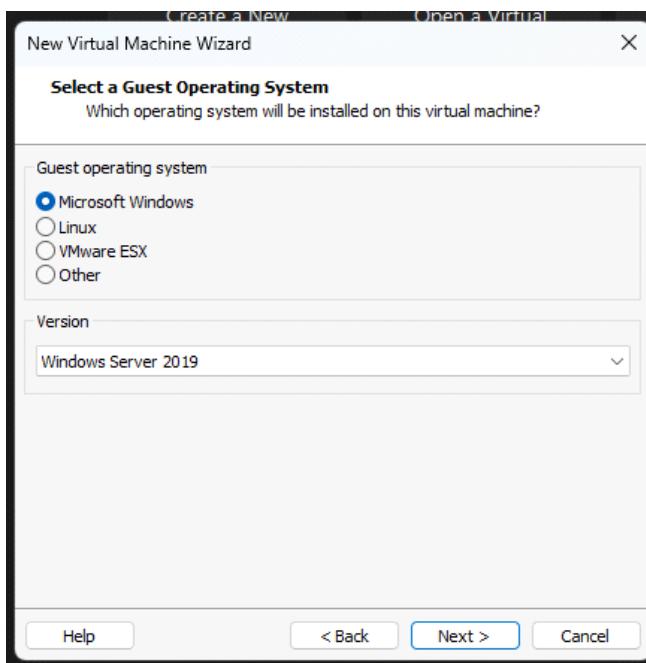


### OPTIONS:

- File >> new virtual machine

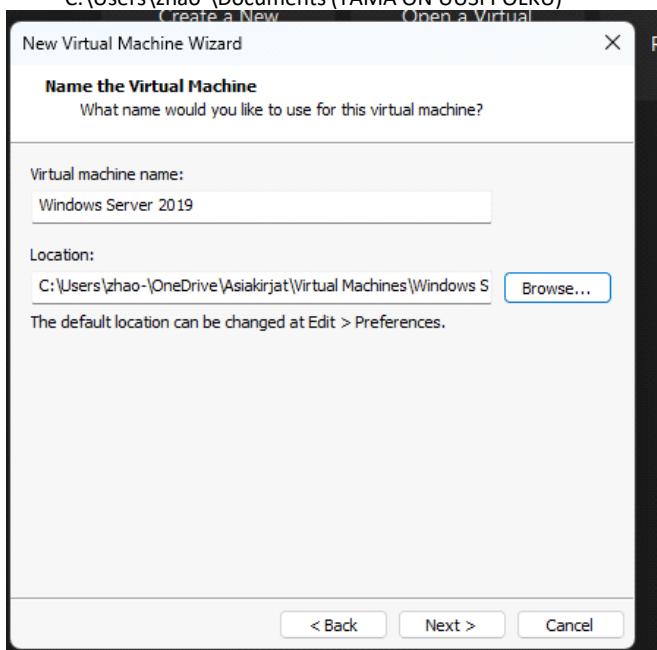


Tästä voi valita Windows Server 2025 - jos on Workstation 17 Pro tai sitä uudempi versio



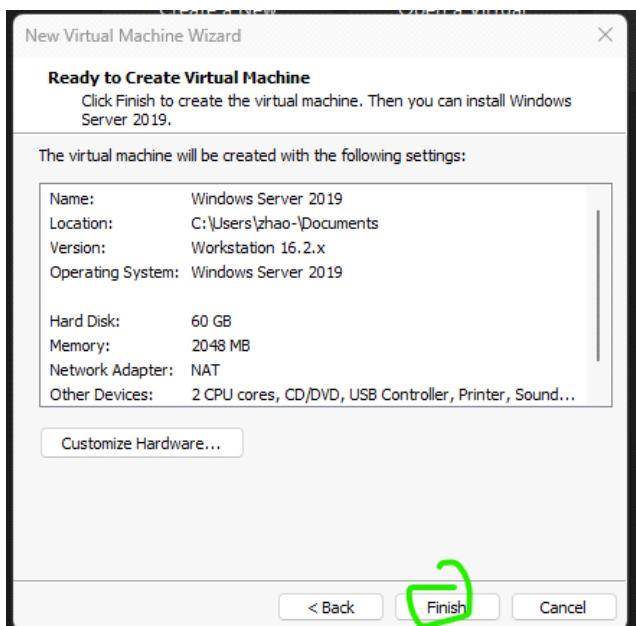
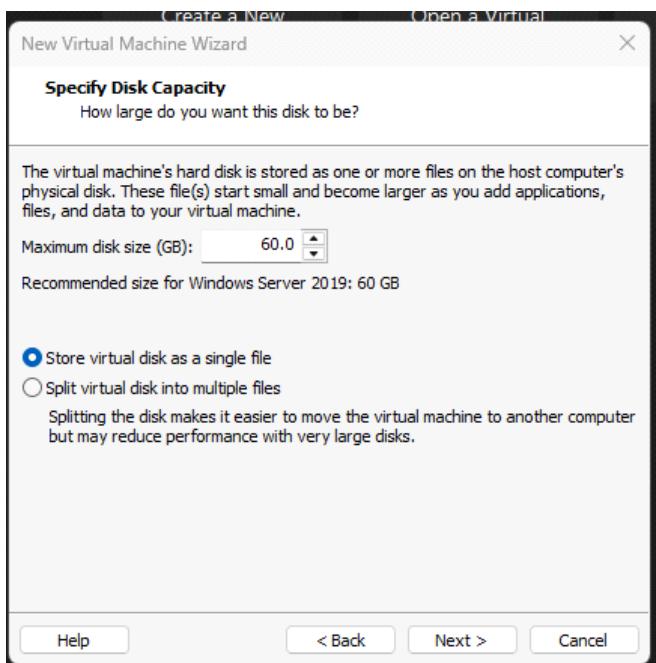
Valitse itse mihiin polkuun haluat tallentaa ja ne kaikki tarvittavat datat esim. Voi käyttää fyysisen koneen Documents tai mu ualle esim. Downloads tai johonkin kansion alle.

- Kirjoita nimellä esim. Millä itse tunnistat ja muistat
- C:\Users\zhao-\Documents (TÄMÄ ON UUSI POLKU)

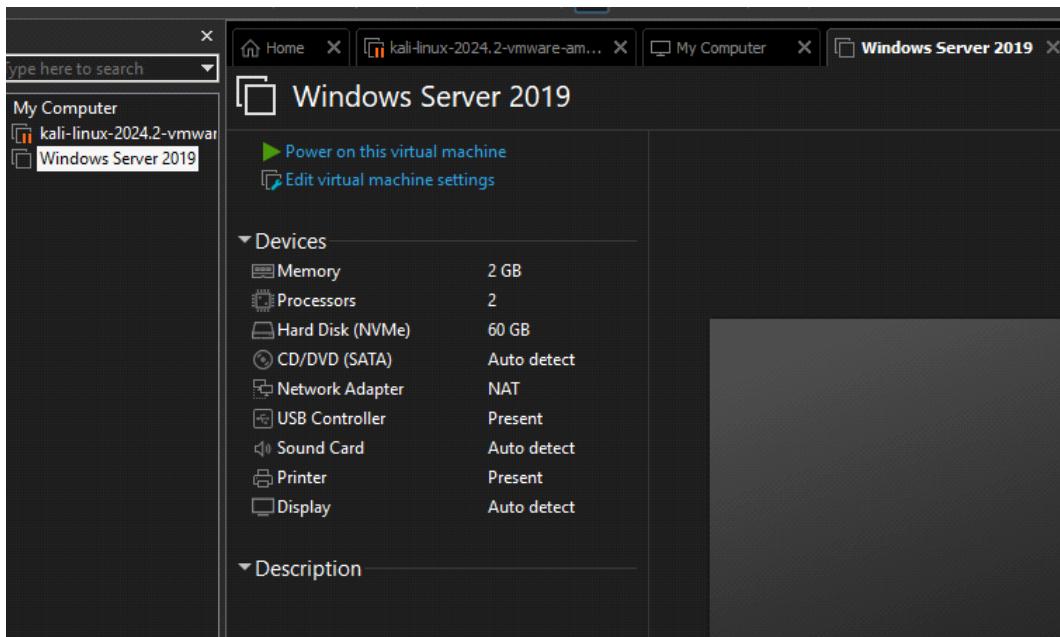


Luodaan erillinen muistielvy ja annettaan n. 60GB muistia, jos ei riittä voi erikseen lisätä muistia tälle yksittäisen virtuaalisoinnin ohjelman alle.

- Esim. Tästä 60GB voi jakaa toiseen levyn esim. D-levyn 20GB, jossa esim. Muu käyttäjät voivat jakaa yhteisen tiedoston alle muuta dataa. Ohjelman käytössä tästä 60GB oletuksena se tulee nimettyynä Windows serverin C-levyksi.



Finnish - jälkeen se ponnahtaa tänne näkyviinsä ja oletuksena saa tällaisen näkymänsä.  
Oletuksena muisti ja prosessori 2GB (2kpl) riittää hyvin alkuperäiselle mallille, ja jos fyysisen työasema antaa riittävästi muistia virtualisoinnille.



## Seuraavaksi asetettaan pieni labran IP-osoitetta - START HERE;

Jos työaseman desktop ei löydy (virtual network editor) hae Windows hausta lauseella ja suorita muutoksen IP-osoitteet näin:

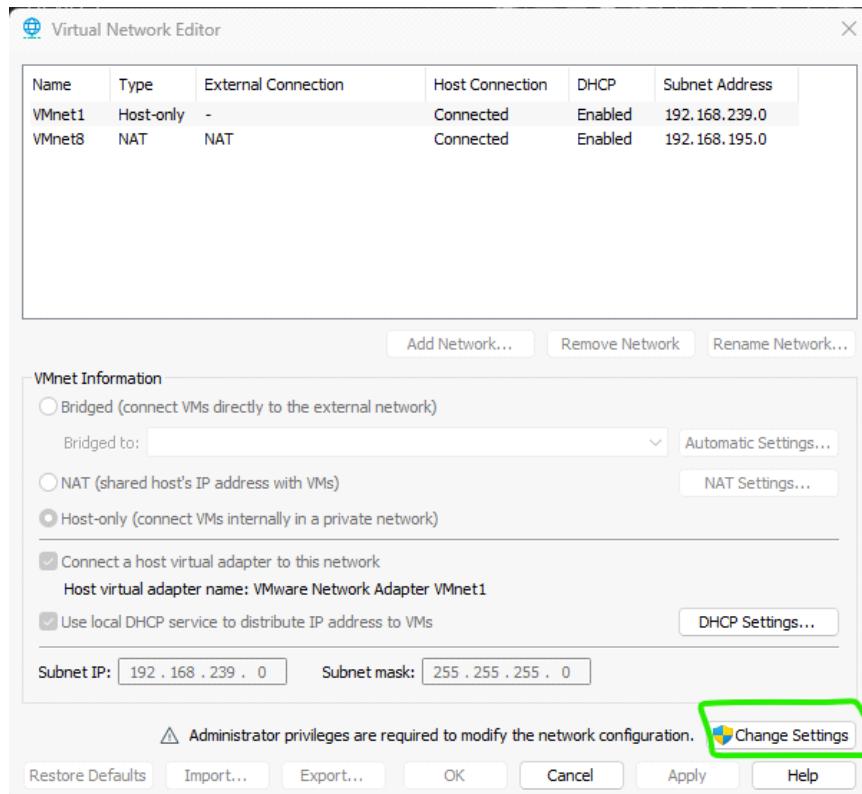
OPTIONS Vmware workstaion (Edit >> virtual network editor)

Subnet IP: 192.168.100.0/24  
 Domain Controller (Windows Server 2019): 192.168.100.10  
 Future client machines: 192.168.100.20-50  
 DHCP scope: 192.168.100.100-200

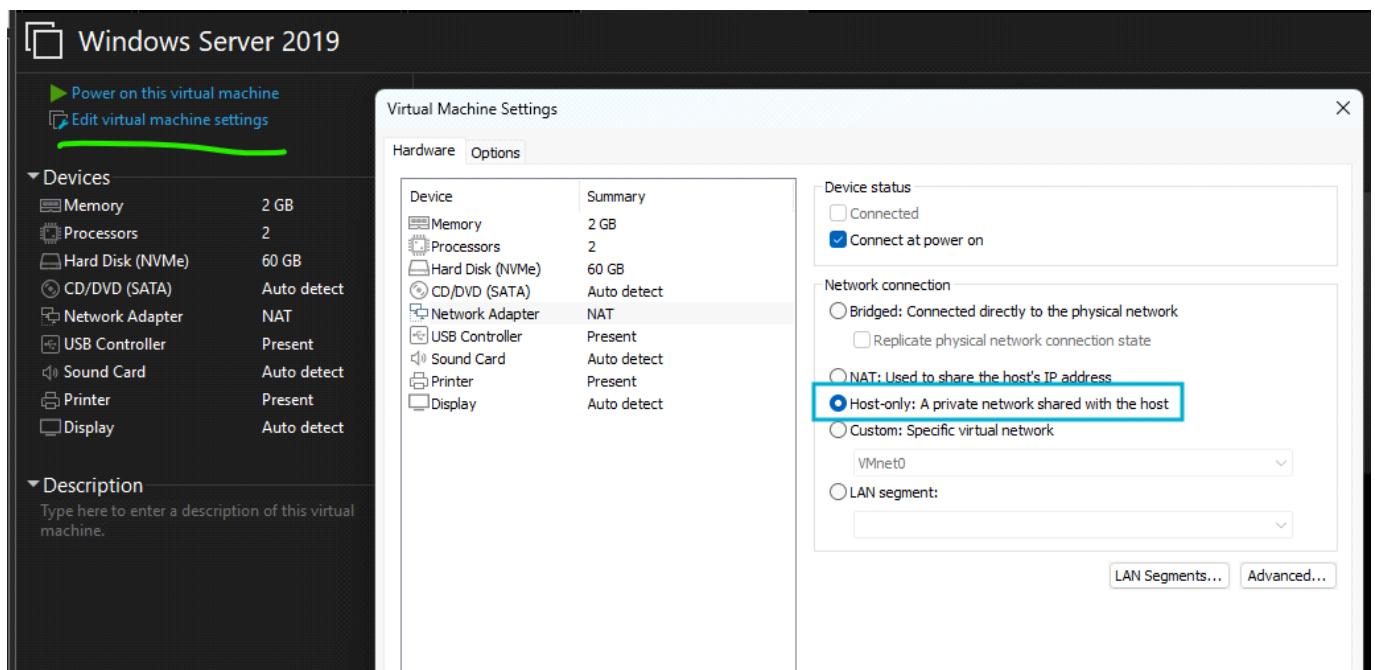
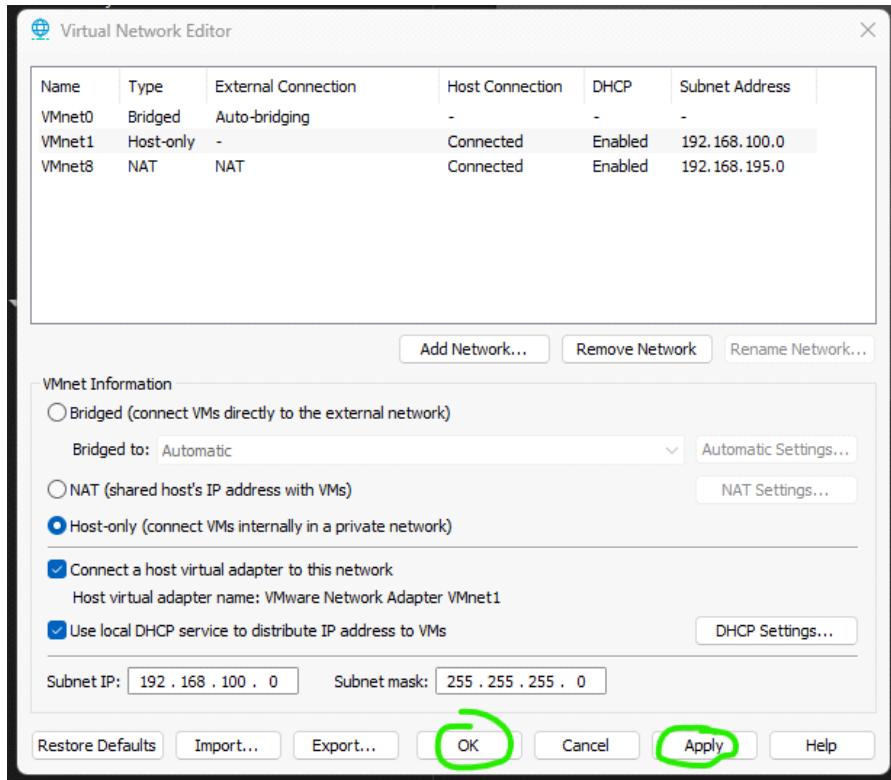
BEFORE:

Tässä vähä vaikea sanoa kumppi on mikäkin..

Paitsi toinen niistä on kali linux IP-osoite, niin se toinen on se Windows Server 2019  
 Kun klikkaa (change settings) ponnahtaa harmaa ikkuna, että sallitko tehdä muutosta



AFTER:



Mitä tämä tarkoittaa ja miksi valitsin tämän?

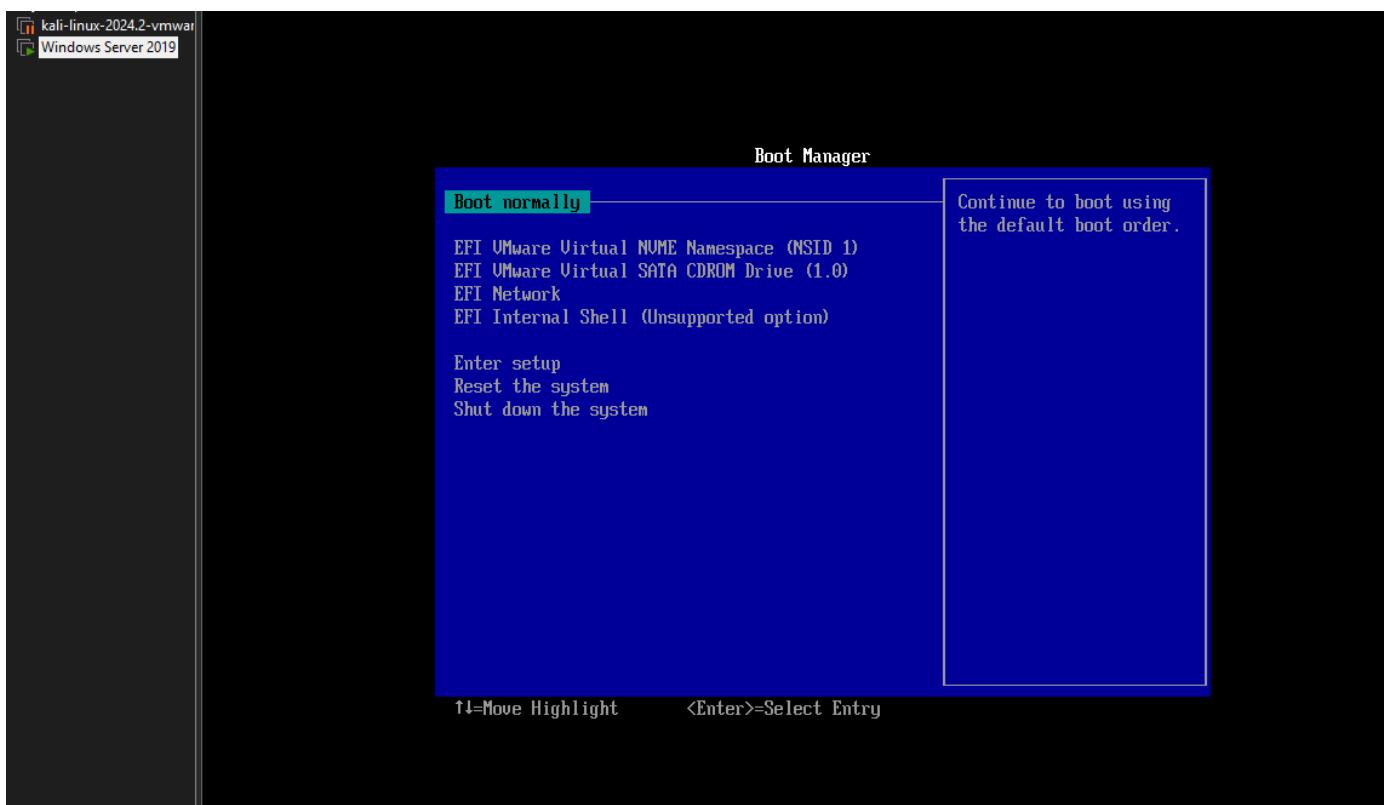
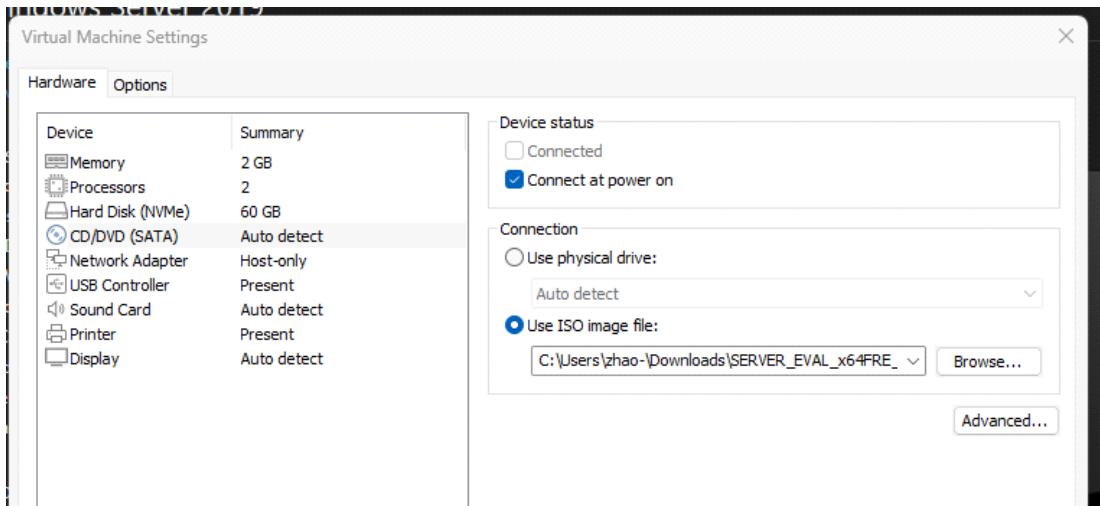
## Mitä "Host-Only" -verkko tarkoittaa VMware Workstationissa?

Host-Only = suljettu verkko, jossa:

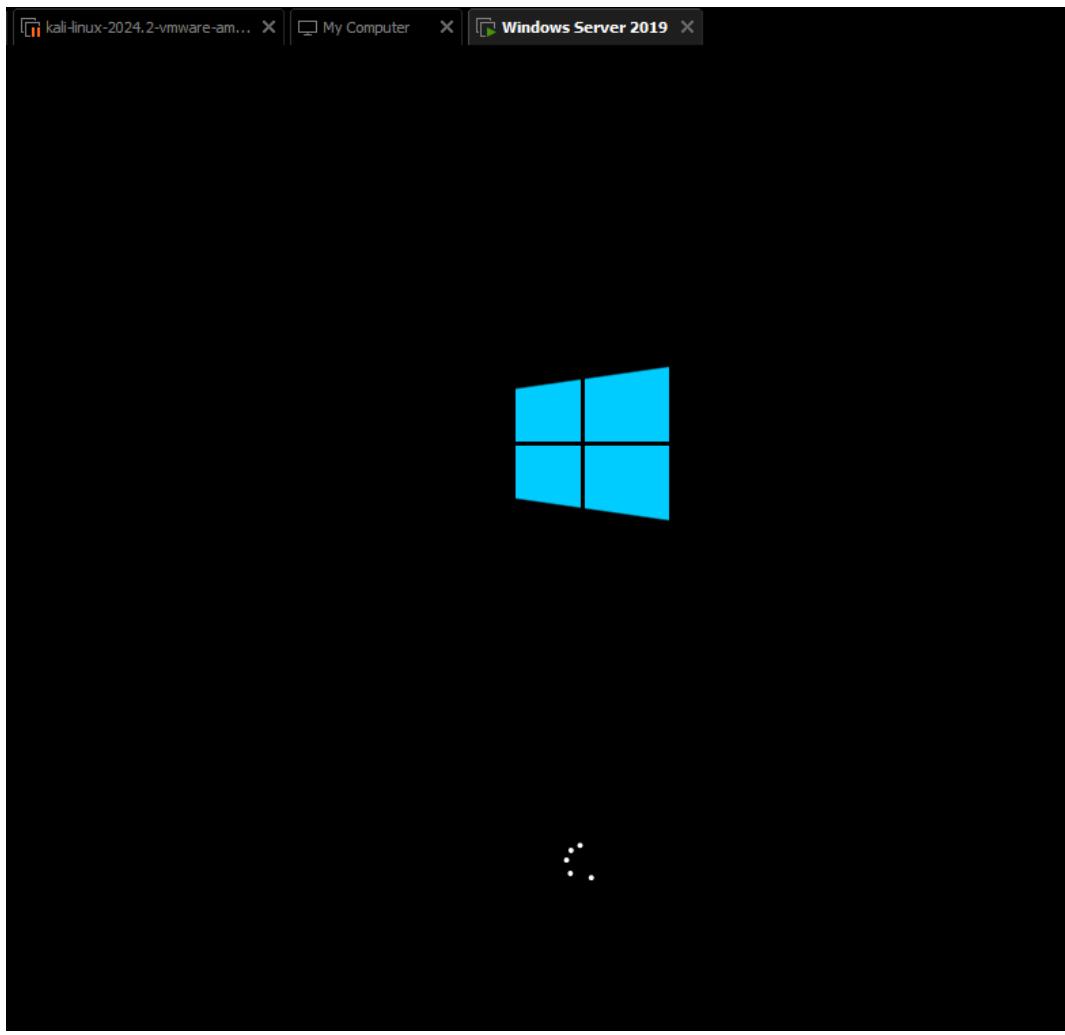
- Virtuaalikoneet voivat **keskustella keskenään**
- Virtuaalikoneet voivat **keskustella isäntäkoneen (host) kanssa**
- **Ei pääsyä internettiin**
- Fyysiset laitteet LANissa eivät näe tättä verkkoa

💡 Tämä on hyvä valinta esimerkiksi testiympäristöön, missä et halua ulkoista yhteyttä mutta haluat koneiden välisen verkon toimivan.

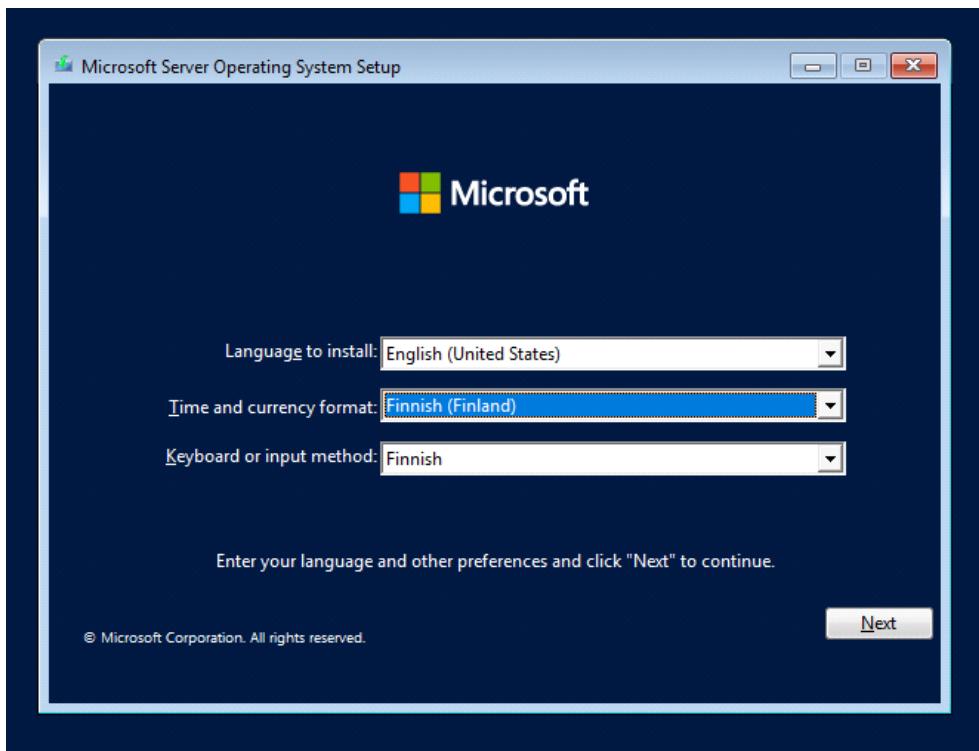
Nyt viimeisenä lisää ISO tiedosto ja tämä on se windows server tiedosto levy, ja käynnistää ohjelma!

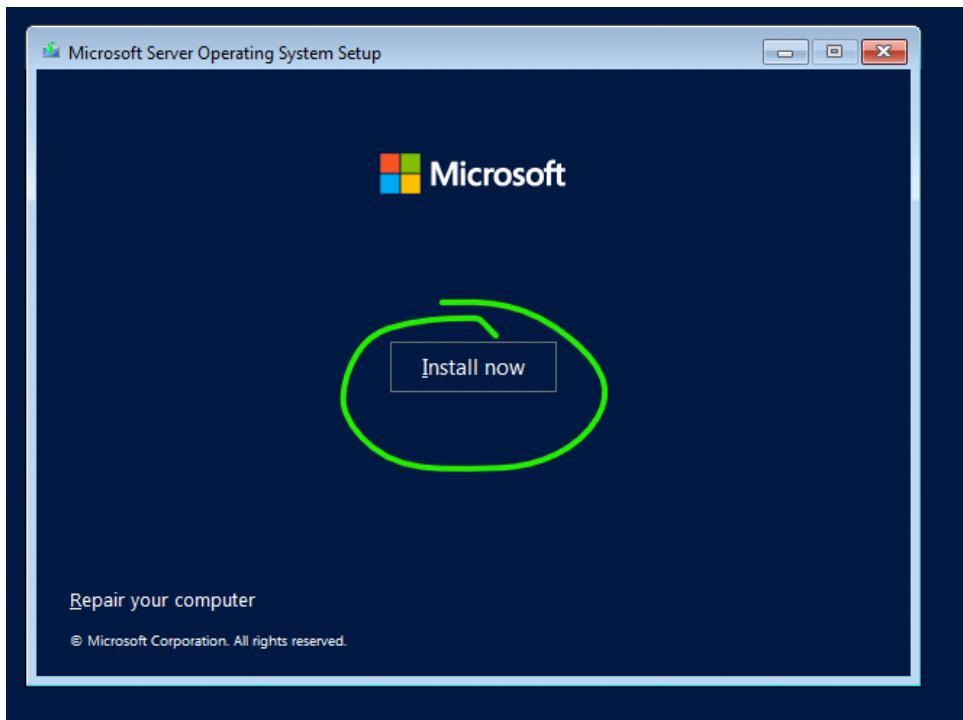


Klikkaa vaan "enter" siis näppäimistöstä ja se menee eteenpäin niin windows alkaa pelittää ja odota (kärsivällisyttä)

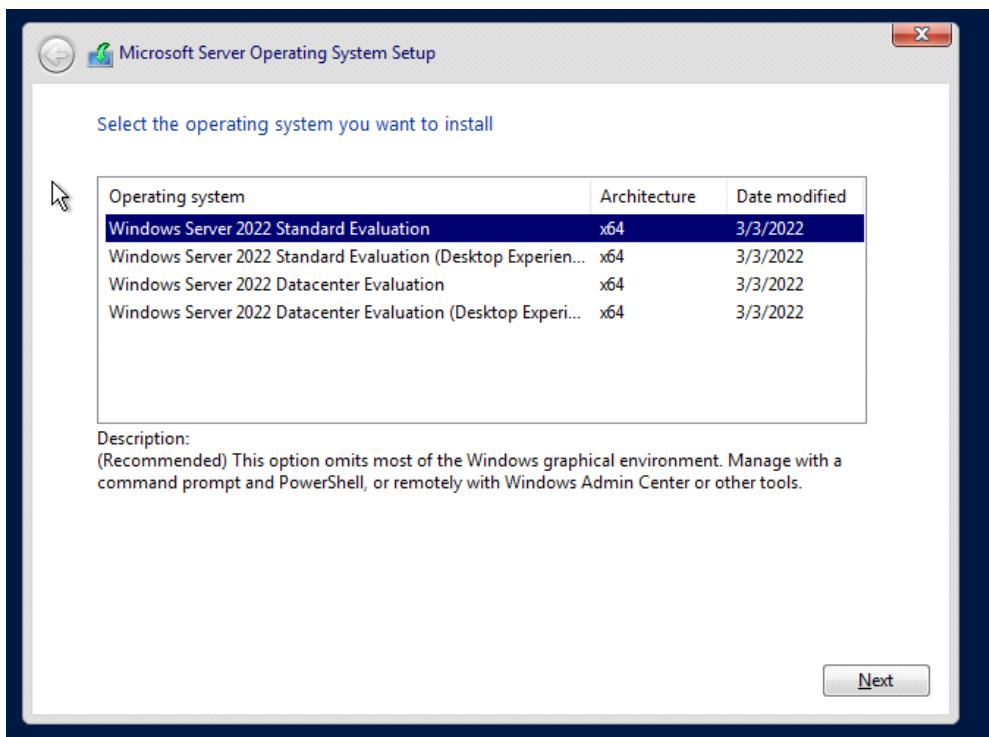


Oletuksena on yleensä English ja English - niin nyt näin vaan ja oma valinta:





Vaihtoehto	Merkitys
<b>Windows Server 2022 Standard Evaluation</b>	<b>Ilman graafista käyttöliittymää (Core-asennus).</b> Hallitaan vain komentoriviltä (PowerShell, CMD, Admin Center).
<b>Windows Server 2022 Standard Evaluation (Desktop Experience)</b>	<b>Tavallinen graafinen versio (GUI) –</b> näyttää kuin normaali Windows-työpöytä. Suositellaan, jos haluat käyttää käyttöliittymää hiirellä.
<b>Windows Server 2022 Datacenter Evaluation</b>	Sama kuin yllä, mutta sisältää lisä ominaisuuksia (kuten Hyper-V Cluster, Storage Spaces Direct jne.). Ei graafista käyttöliittymää.
<b>Windows Server 2022 Datacenter Evaluation (Desktop Experience)</b>	Sama kuin yllä, mutta sisältää <b>GUI:n</b> . Laajin vaihtoehto kaikilla ominaisuuksilla.



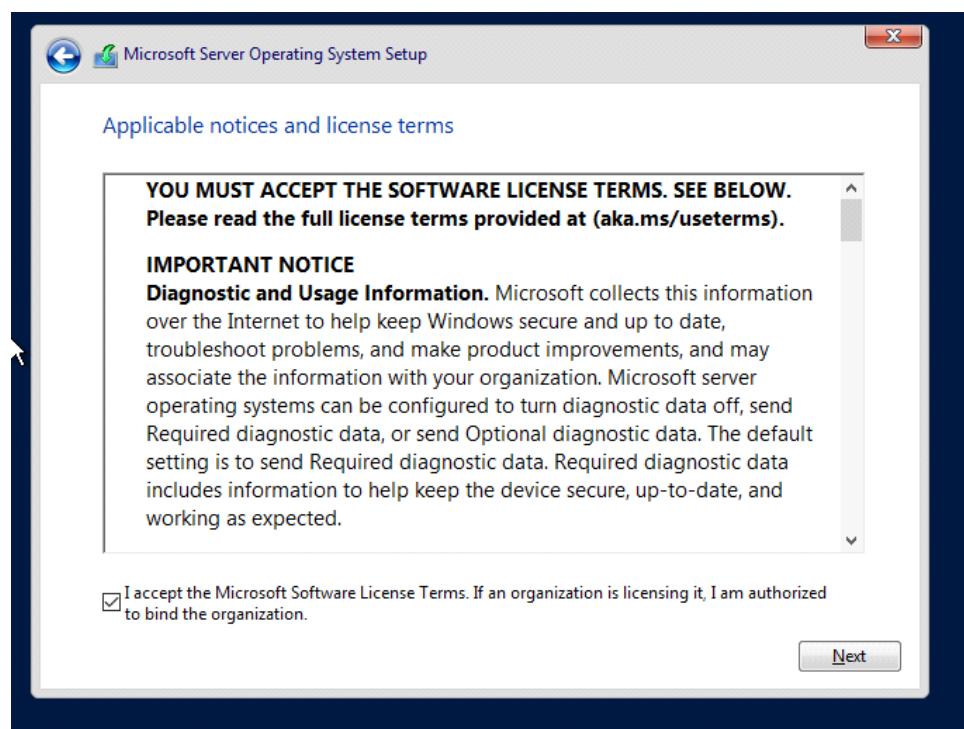
Operating system	Architecture	Date modified
Windows Server 2022 Standard Evaluation	x64	3/3/2022
<b>Windows Server 2022 Standard Evaluation (Desktop Experience)</b>	<b>x64</b>	<b>3/3/2022</b>
Windows Server 2022 Datacenter Evaluation	x64	3/3/2022
Windows Server 2022 Datacenter Evaluation (Desktop Experience)	x64	3/3/2022

Description:

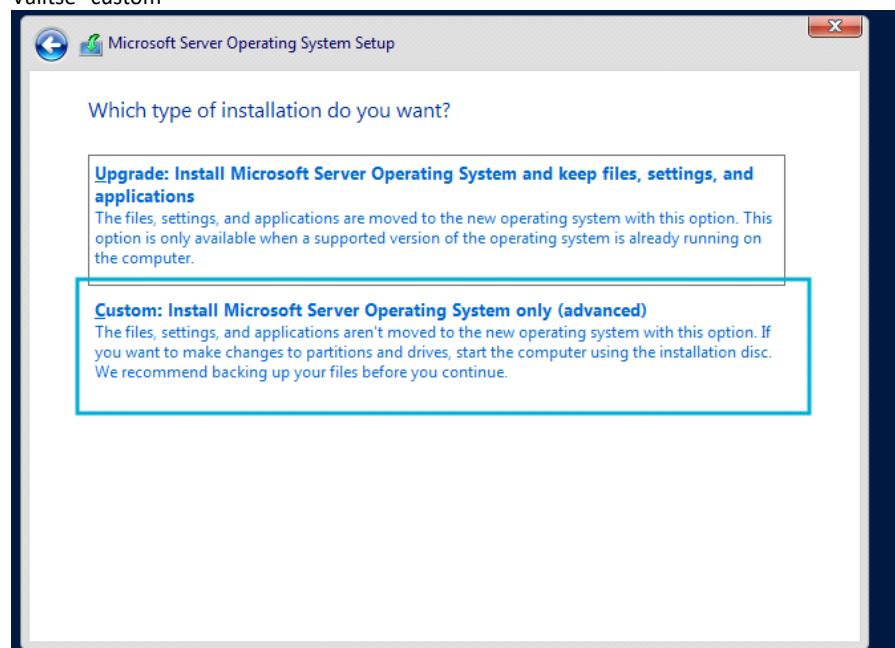
This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.

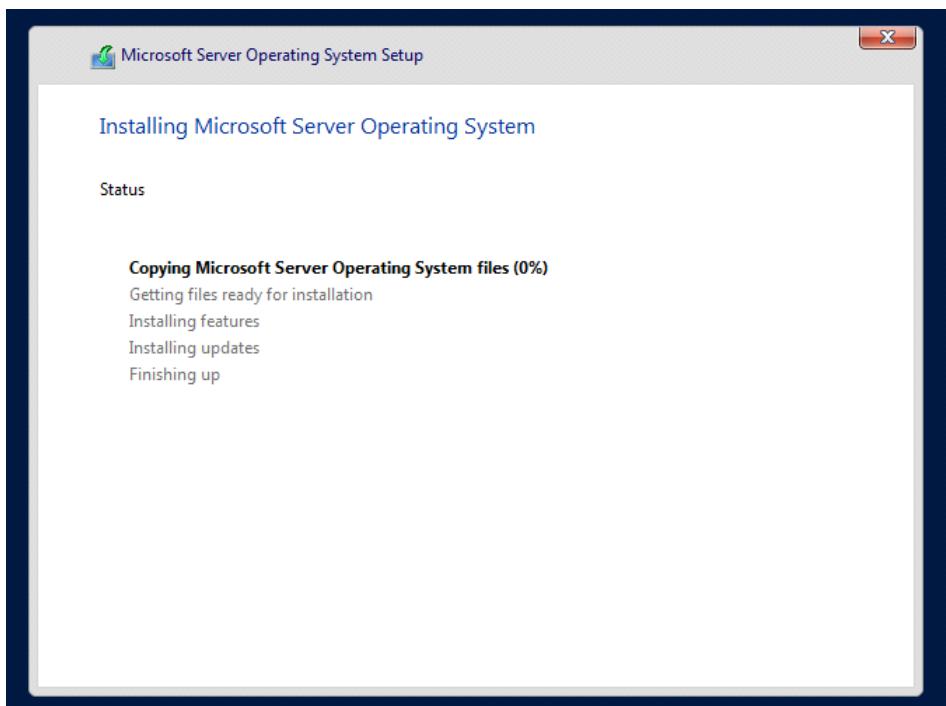
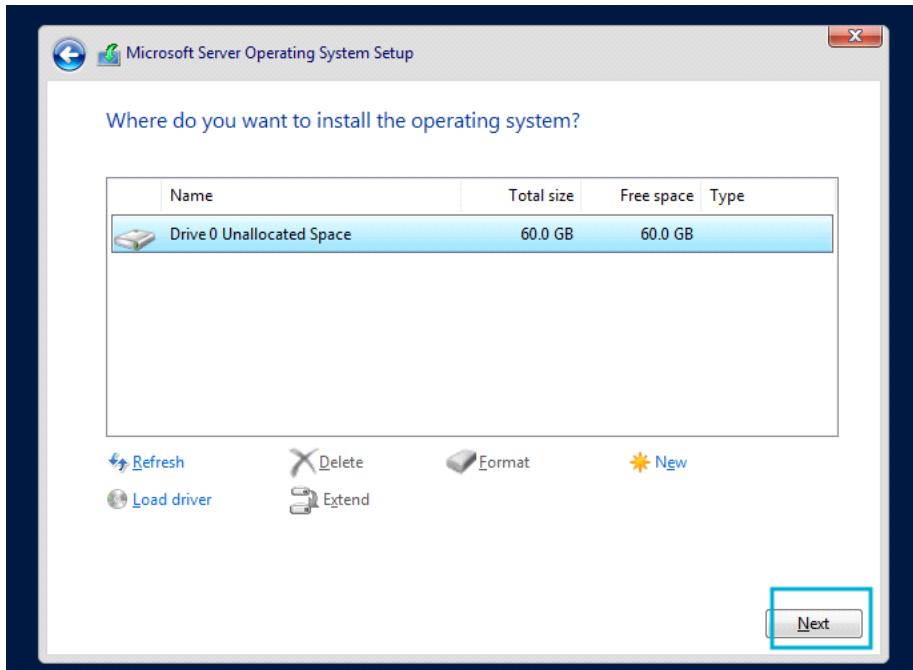
#### Windows Server 2022 Standard Evaluation (Desktop Experience)

- ✓ Sisältää graafisen käyttöliittymän
- ✓ Soveltuu Active Directory, DNS, DHCP, jne. harjoittelun
- ✓ Helpo käyttää



Valitse "custom"





Tässä väliin se alkaa itse suorittaa buuttauksen niin antaa sen suorittaa

Aseta joku salasana jonka itse muistaa ja tämä on oletus user name:

Username: administrator

Password: P@sswOrd (nolla)

## Customize settings

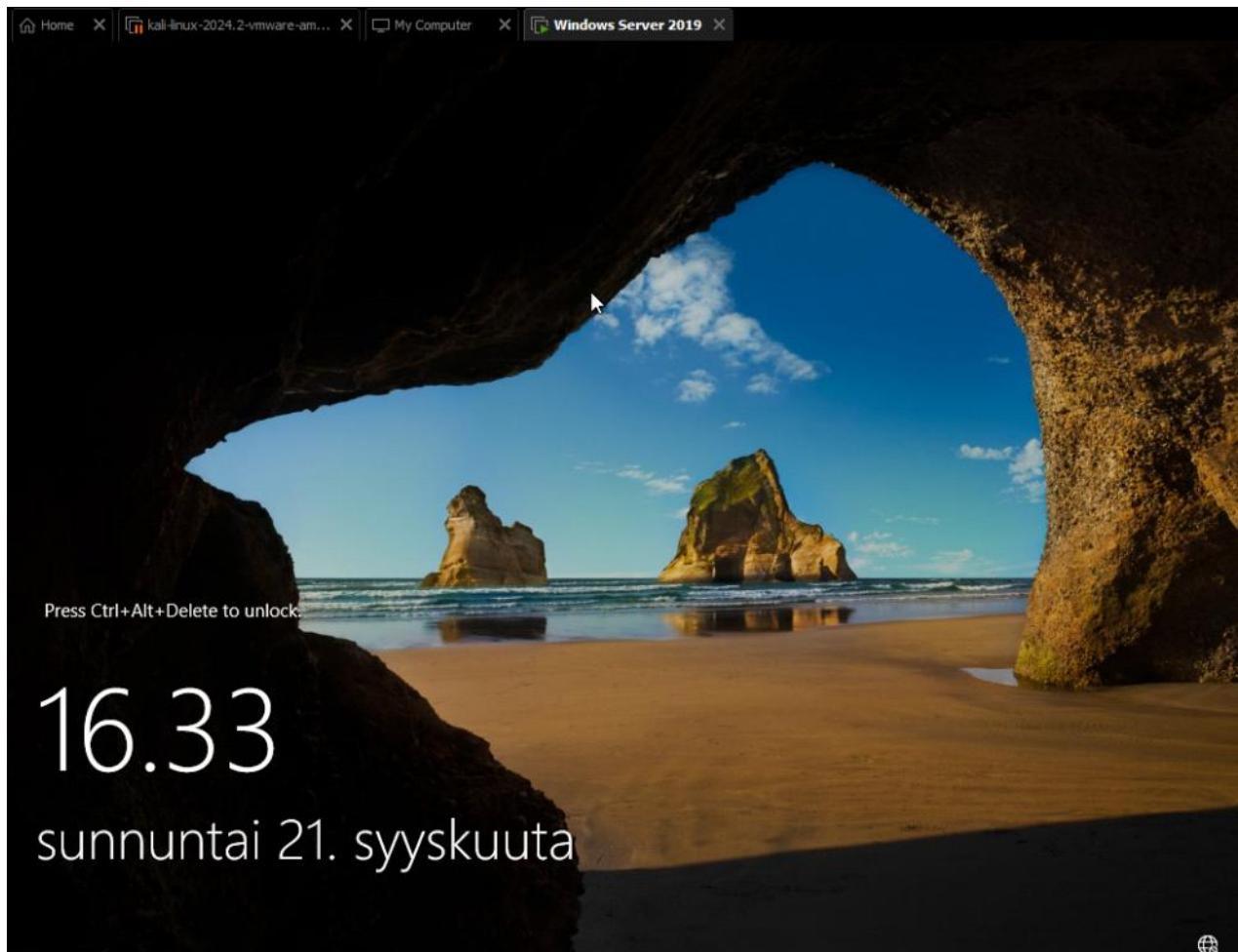
Type a password for the built-in administrator account that you can use to sign in to this computer.

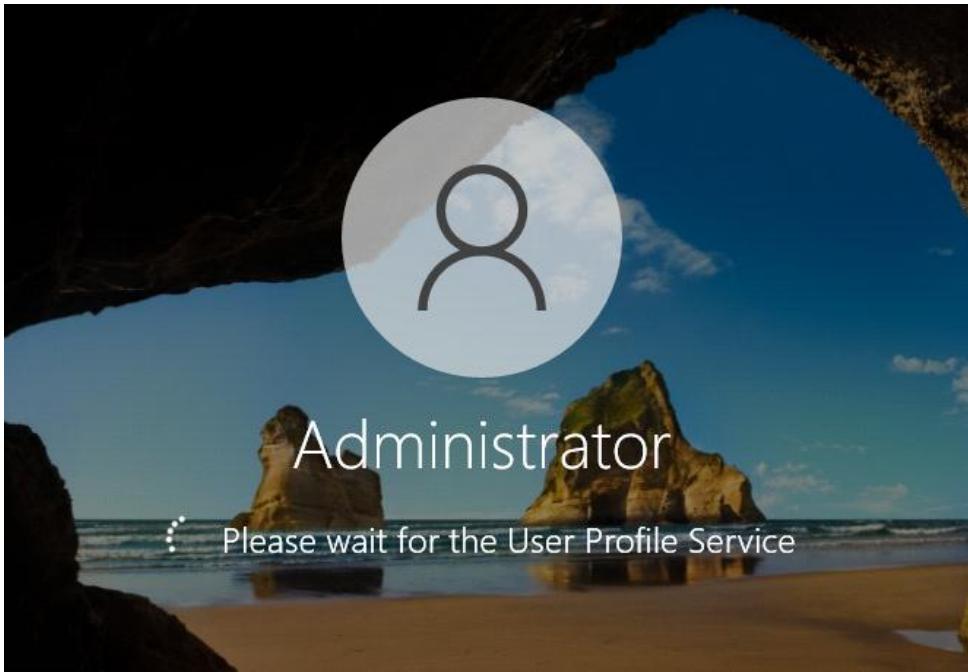
User name	Administrator
Password	•••••••
Reenter password	••••••• 



Finish

Tässä ollaan!! Tämä menisi samanlailla uusimman version (windows 11) ympäristön kauttakin, mutta ulkonäkö vähä eri näköinen vain.





Kirjauduttua sisään siinä menee pieni hetki kun "server manager" aktivoituu ja tulee näkyviinsä (hirvee buggy ja viive)

The screenshot shows the Windows Server Manager dashboard. The left sidebar has a "Dashboard" tab selected, along with "Local Server", "All Servers", and "File and Storage Services". The main area is titled "WELCOME TO SERVER MANAGER". On the left, there's a vertical stack of three orange boxes: "QUICK START", "WHAT'S NEW", and "LEARN MORE". To the right of these boxes is a numbered list: 1. Configure this local server, followed by 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this is a "Hide" link. At the bottom, there's a section titled "ROLES AND SERVER GROUPS" with a table showing one "File and Storage Services" role and one "Local Server" server group, both with a count of 1. The table includes columns for Manageability, Events, Performance, and BPA results. The bottom navigation bar includes a search bar, task icons for File Explorer, Task View, and File History, and system status indicators like battery level and network connection.

File and Storage Services	1
Manageability	
Events	
Performance	
BPA results	

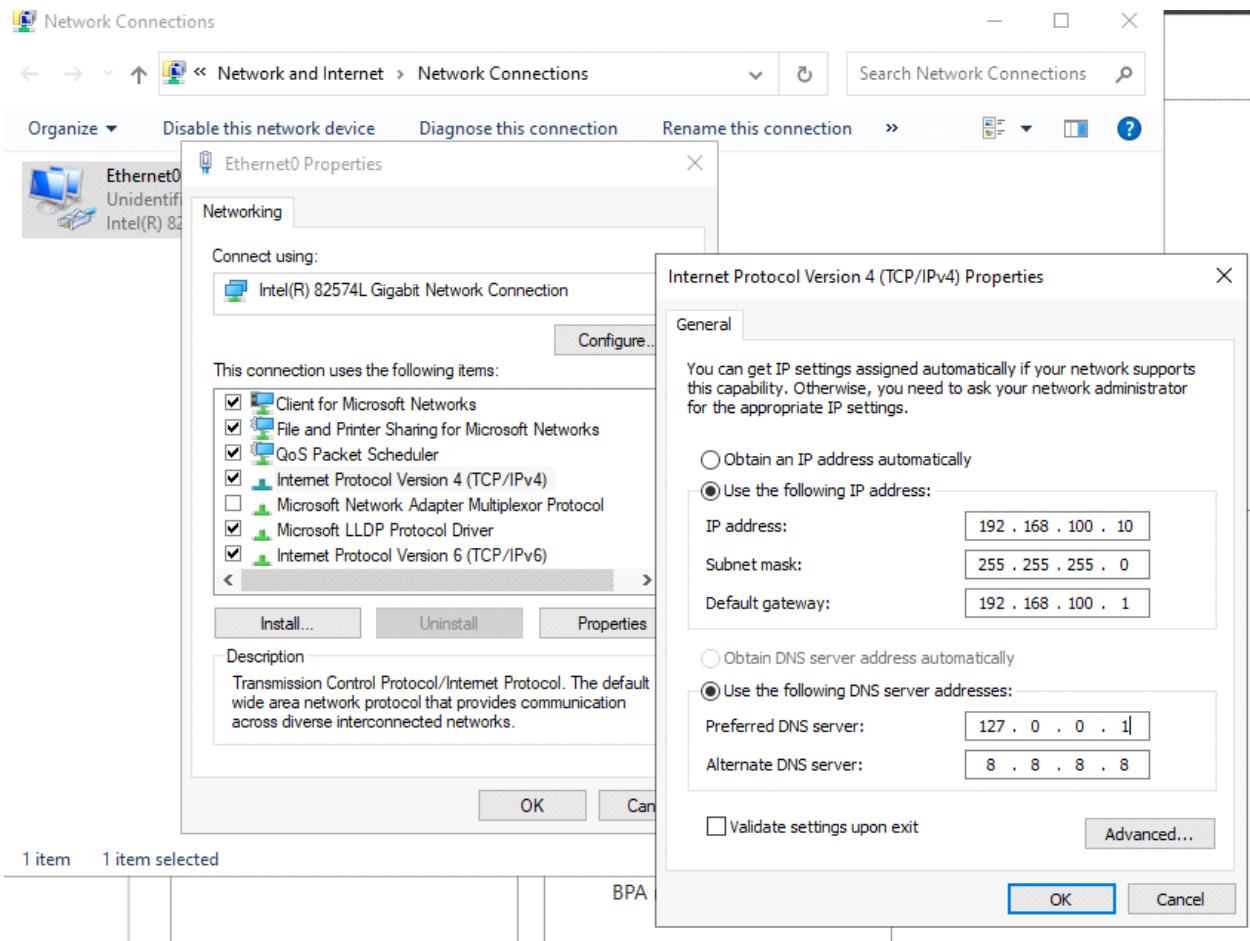
Local Server	1
Manageability	
Events	
Services	1
Performance	
BPA results	

Seuraavaksi asetettaan staattinen IP-osoite

Windows server:

- IP 192.168.100.10
- Mask 24 (255.255.255.0)
- Default gateway portti: 192.168.100.1

- DNS serverit: 127.0.0.1 & 8.8.8.8 (Google DNS)



## Ladataan Active directory domain service -START HERE;

Computer name WIN-9 jotakin - se on se Windows nimi, mutta sitä voi tarvittaessa muuttaa nimensä ja usein konffauksen pystyttämisen Windows server se antaa oletus nimensä ja näin - jos muuttaa nimen niin joutuu uudelleen käynnistää konetta.

Server Manager

Server Manager ▶ Local Server

**PROPERTIES**  
For WIN-9MD2IOQ8QRC

Computer name	WIN-9MD2IOQ8QRC	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Download updates
		Last checked for updates	Never
Microsoft Defender Firewall	Public: On	Microsoft Defender Antivirus	Real-Time Protection
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00)
Ethernet0	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	Not activate
Operating system version	Microsoft Windows Server 2022 Standard Evaluation	Processors	12th Gen Intel
Hardware information	VMware, Inc. VMware7.1	Installed memory (RAM)	2 GB
		Total disk space	59.37 GB

**EVENTS**  
All events | 28 total

Server Name	ID	Severity	Source	Log	Date and Time
WIN-9MD2IOQ8QRC	1014	Warning	Microsoft-Windows-DNS Client Events	System	21.9.2025 17.33.57
WIN-9MD2IOQ8QRC	1014	Warning	Microsoft-Windows-DNS Client Events	System	21.9.2025 17.18.32
WIN-9MD2IOQ8QRC	1014	Warning	Microsoft-Windows-DNS Client Events	System	21.9.2025 17.03.08

Tools > computer management > (storage) > Disk management

Tämä on se kovalevyn muisti (local disk C:-levyn kapasiteetti ja siksi ollan määritetty n. 60GB muistia.

Computer management kautta voi jakaa erillisenä levynä esim. Loisi toisen E - levyksi.

Computer Management

File Action View Help

Computer Management (Local)

- System Tools
  - Task Scheduler
  - Event Viewer
  - Shared Folders
  - Local Users and Groups
  - Performance
  - Device Manager
- Storage
  - Windows Server Backup
  - Disk Management
- Services and Applications

Volume

Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Basic Data)
(Disk 0 partition 1)	Simple	Basic		Healthy (EFI System Partition)
(Disk 0 partition 4)	Simple	Basic		Healthy (Recovery Partition)
SSS_X64FREE_EN-US_DV9 (D:)	Simple	Basic	UDF	Healthy (Primary Partition)

Actions

- Disk Management
- More Actions

This PC

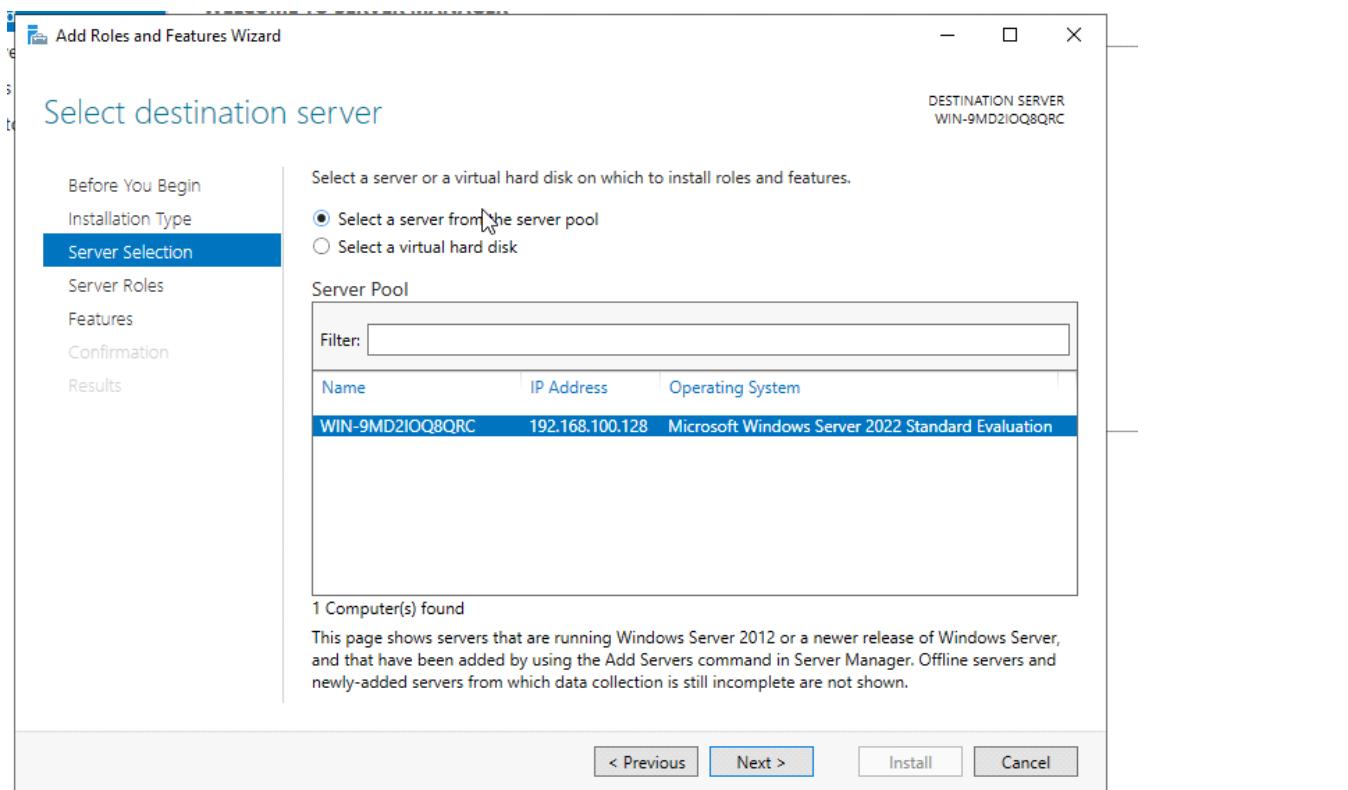
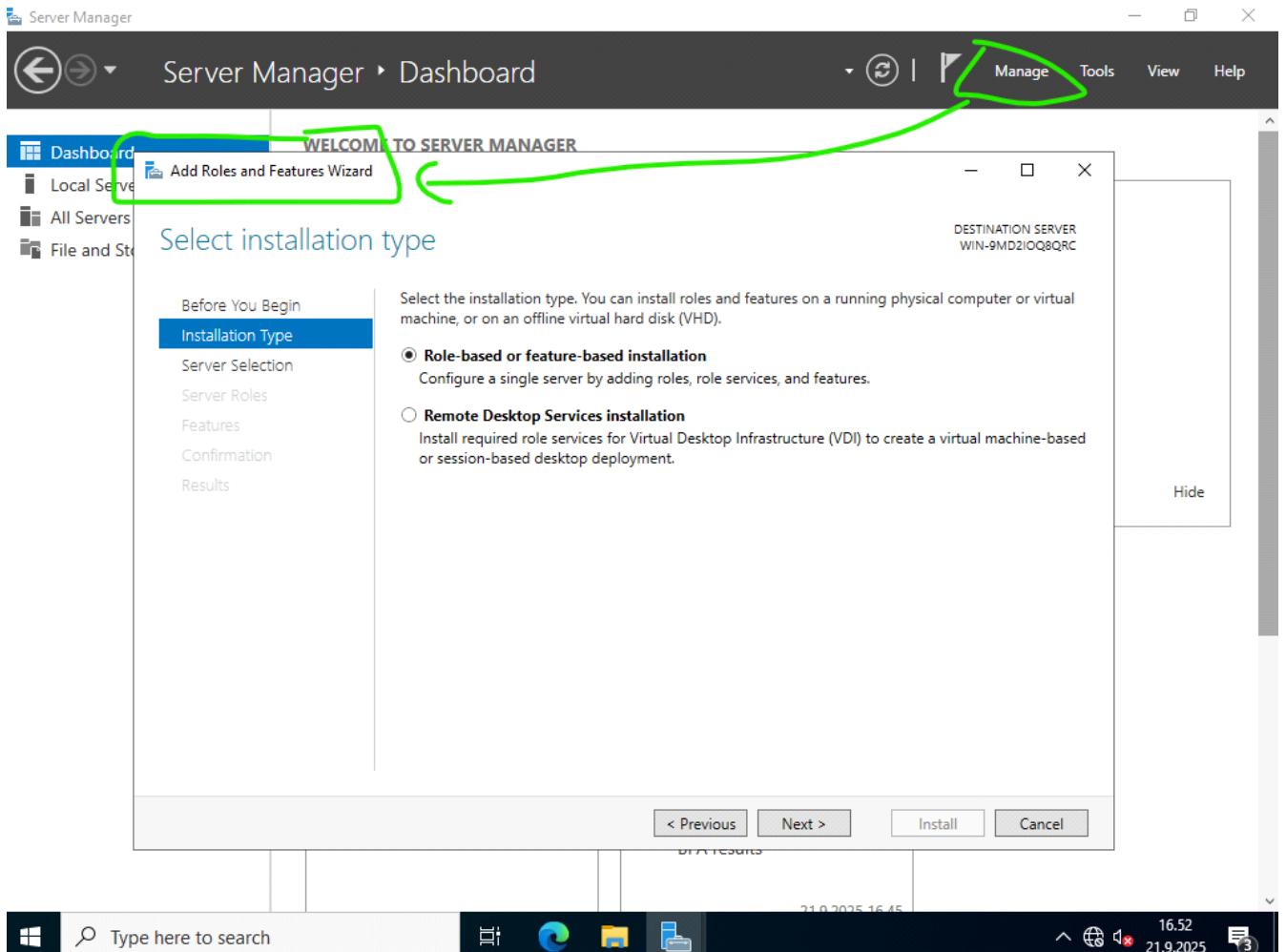
Folders (7)

- Desktop
- Downloads
- Documents
- Pictures
- Music
- Videos

Devices and drives (2)

- Local Disk (C:)
- DVD Drive (D:) SSS\_Xt

9 items



## Select server roles

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
Confirmation  
Results

Select one or more roles to install on the selected server.

**Roles**

- Active Directory Certificate Services
- Active Directory Domain Services**
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services (1 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Policy and Access Services

**Description**

Active I (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

Add Roles and Features Wizard

Select server role

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
Confirmation  
Results

Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

- [Tools] Group Policy Management
- ▲ Remote Server Administration Tools
  - ▲ Role Administration Tools
    - ▲ AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
    - ▲ AD DS Tools
      - [Tools] Active Directory Administrative Center
      - [Tools] AD DS Snap-Ins and Command-Line Tools

Include management tools (if applicable)

**DESTINATION SERVER: WIN-9MD2IOQ8QRK**

Add Features Cancel

Select server roles

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
AD DS  
Confirmation  
Results

Select one or more roles to install on the selected server.

**Roles**

- Active Directory Certificate Services
- Active Directory Domain Services**
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services (1 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services

**Description**

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous **Next >** Install Cancel

## Select features

Before You Begin

Installation Type

Server Selection

Server Roles

**Features**

AD DS

Confirmation

Results

Select one or more features to install on the selected server.

## Features

## Description

<input type="checkbox"/>	<b>.NET Framework 3.5 Features</b>	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
<input checked="" type="checkbox"/>	<b>.NET Framework 4.8 Features (2 of 7 installed)</b>	
<input type="checkbox"/>	Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/>	BitLocker Drive Encryption	
<input type="checkbox"/>	BitLocker Network Unlock	
<input type="checkbox"/>	BranchCache	
<input type="checkbox"/>	Client for NFS	
<input type="checkbox"/>	Containers	
<input type="checkbox"/>	Data Center Bridging	
<input type="checkbox"/>	Direct Play	
<input type="checkbox"/>	Enhanced Storage	
<input type="checkbox"/>	Failover Clustering	
<input checked="" type="checkbox"/>	Group Policy Management	
<input type="checkbox"/>	Host Guardian Hyper-V Support	
<input type="checkbox"/>	I/O Quality of Service	
<input type="checkbox"/>	IIS Hostable Web Core	
<input type="checkbox"/>	Internet Printing Client	
<input type="checkbox"/>	IP Address Management (IPAM) Server	
<input type="checkbox"/>	LPR Port Monitor	

&lt; Previous

Next &gt;

Install

Cancel

## Active Directory Domain Services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

**AD DS**

Confirmation

Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

## Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

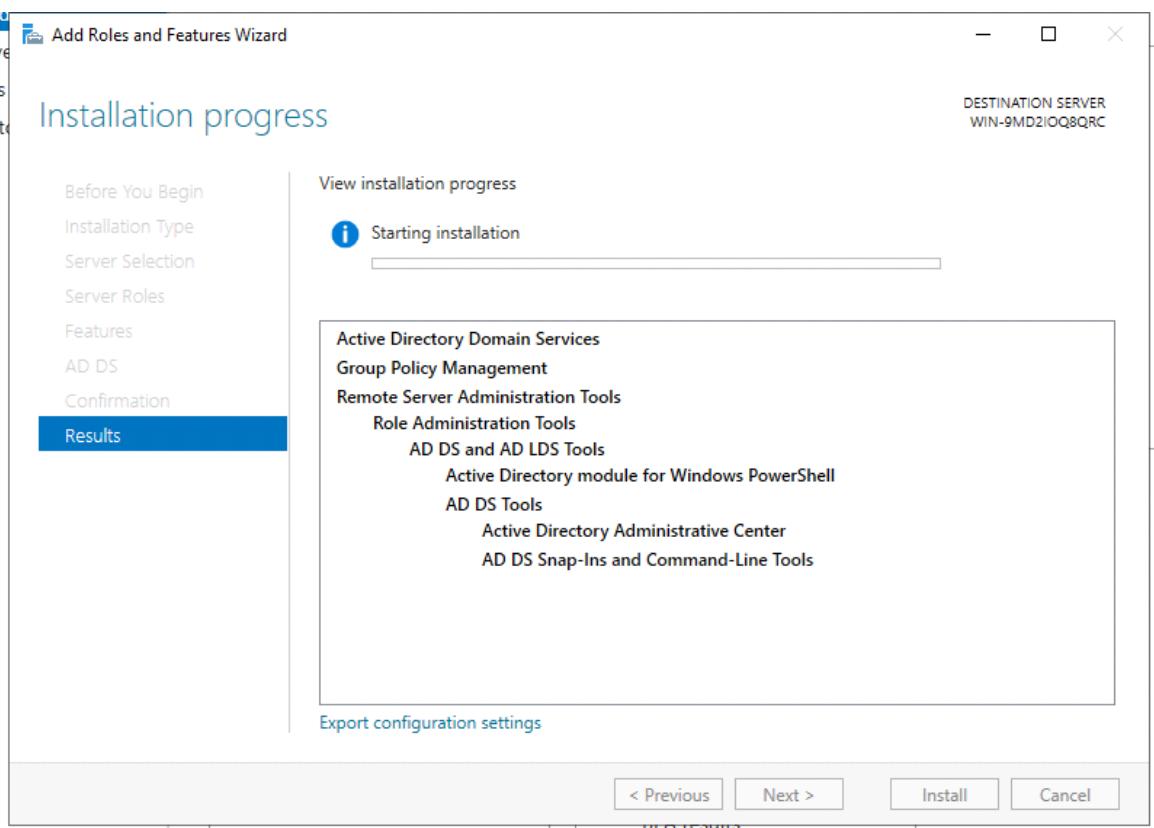
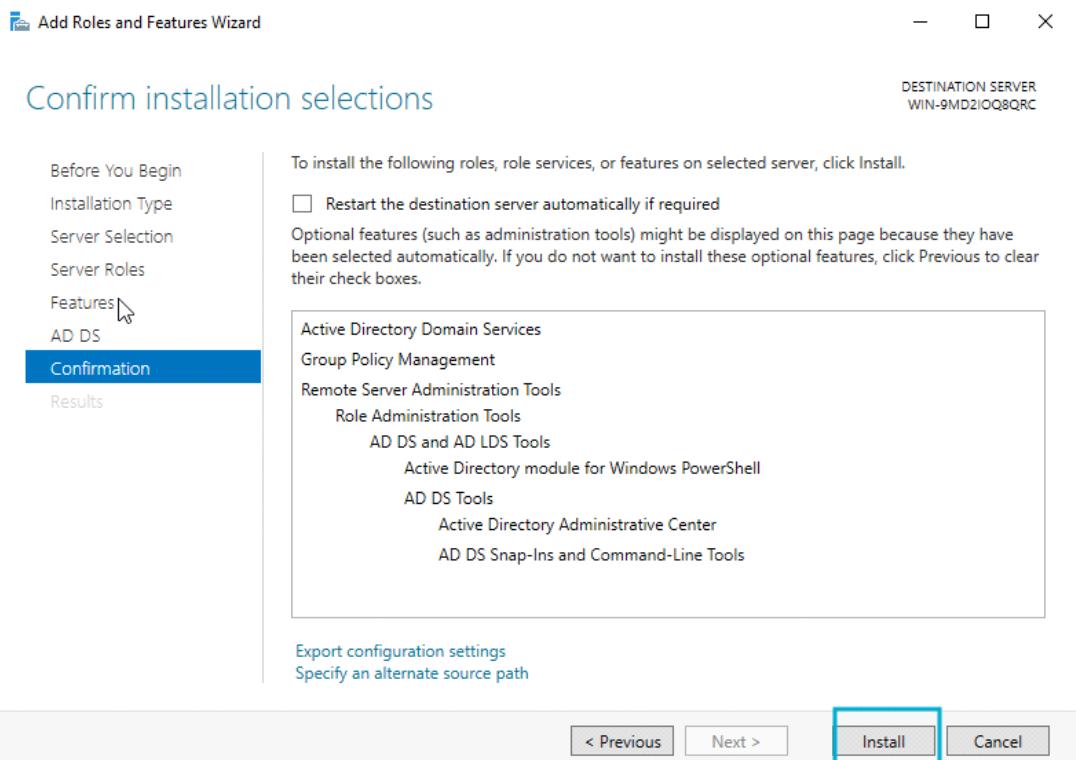
[Learn more about Azure Active Directory](#)
[Configure Office 365 with Azure Active Directory Connect](#)

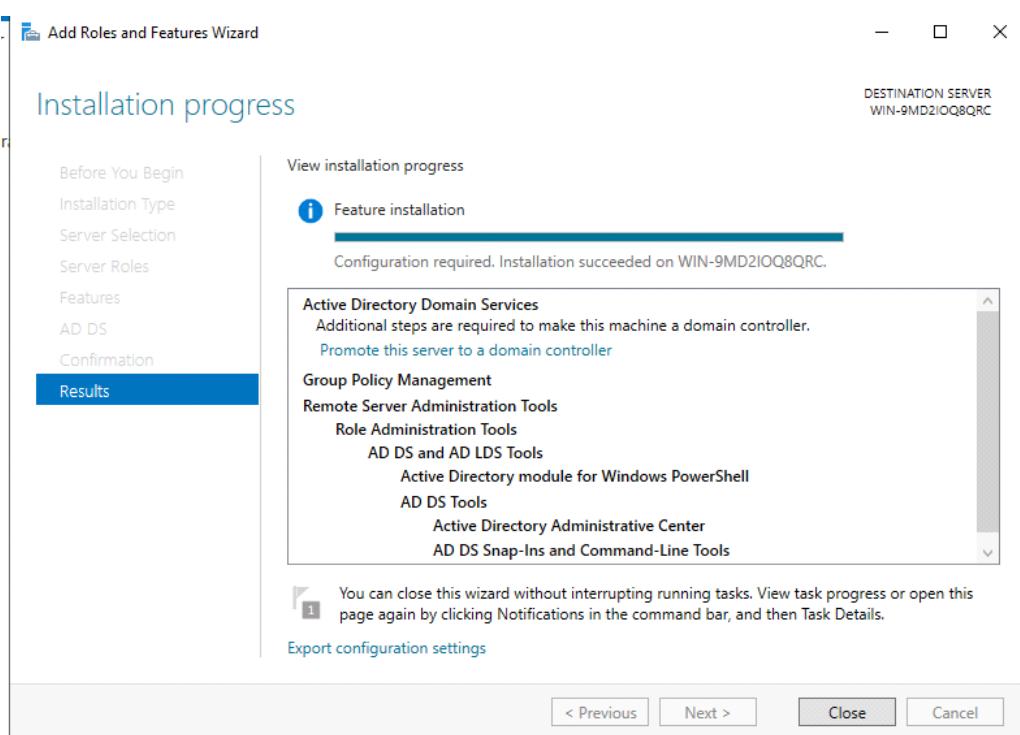
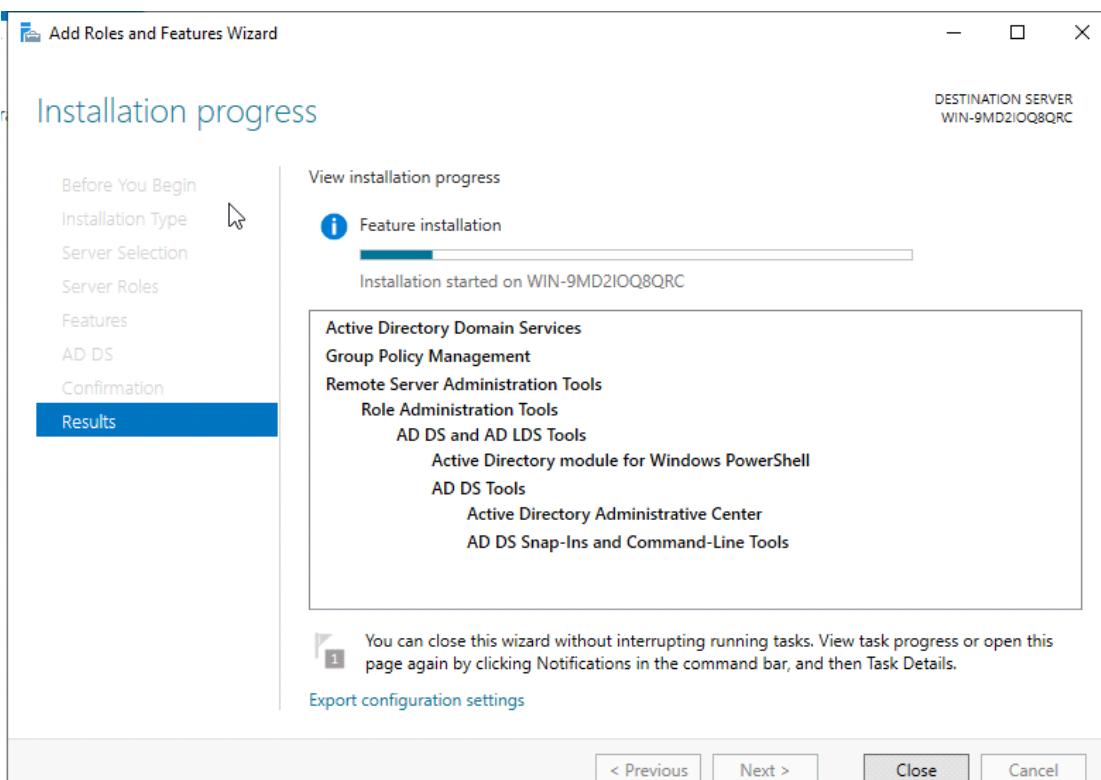
&lt; Previous

Next &gt;

Install

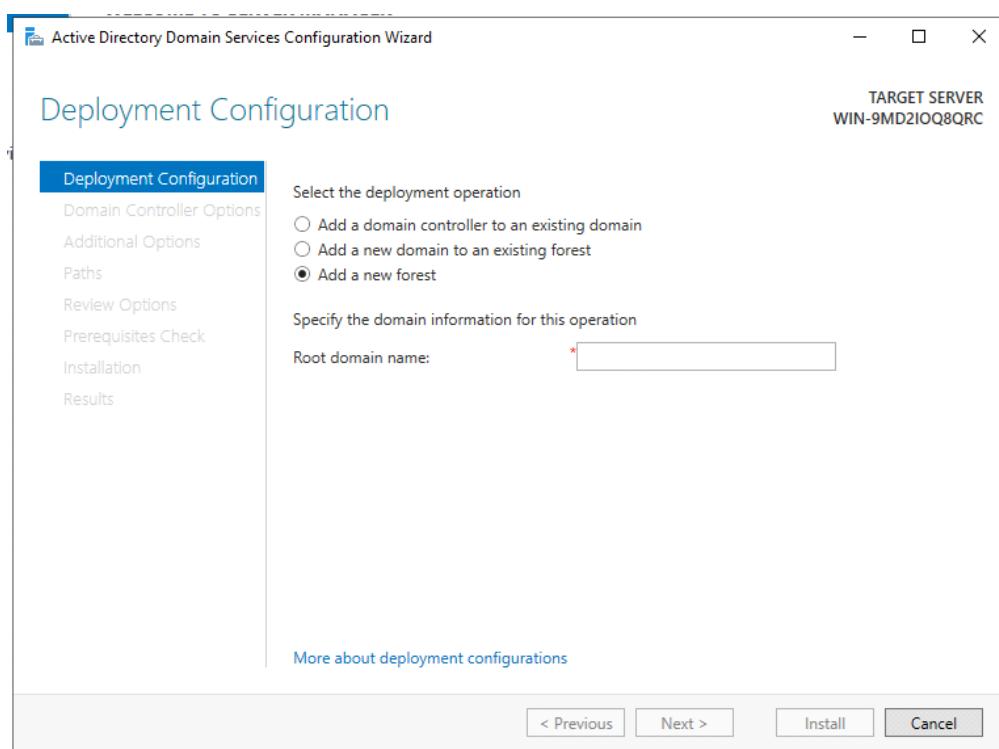
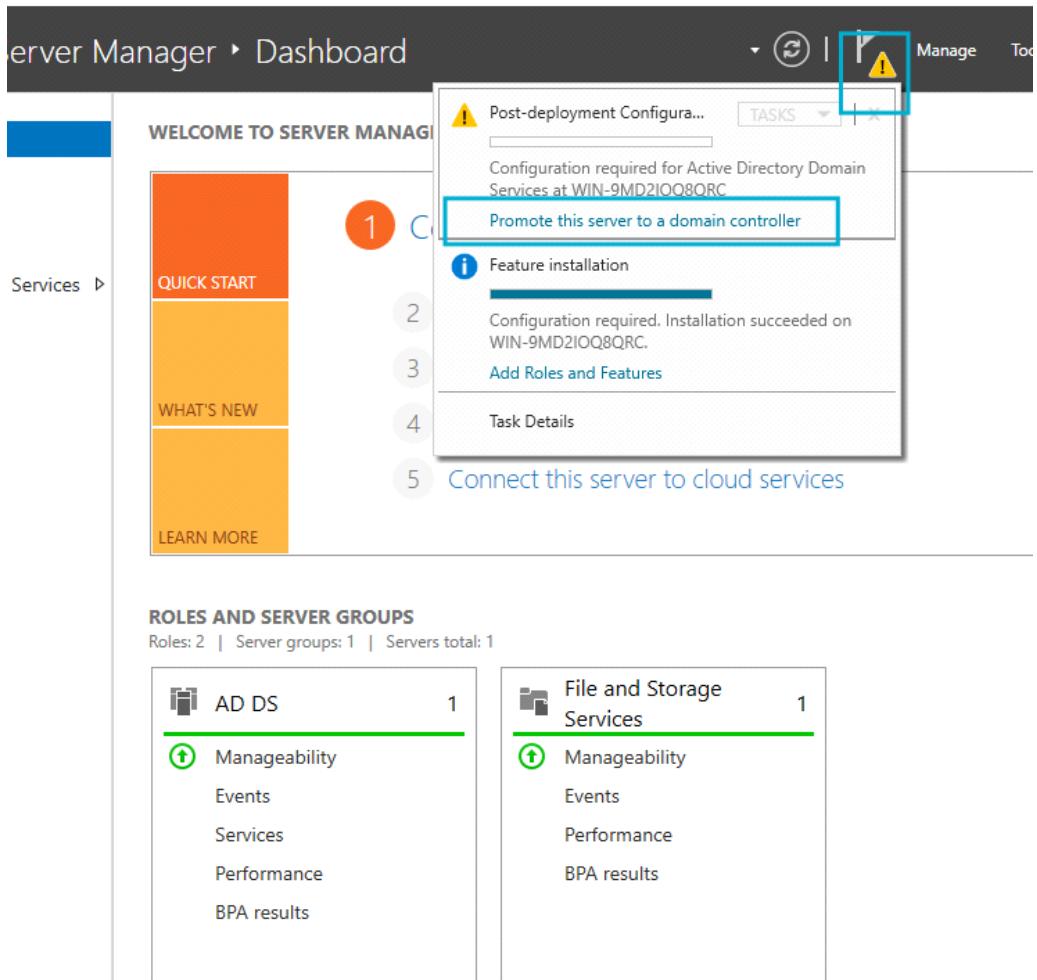
Cancel





Nyt se on valmis ja "close" vaan

Keltainen kolmio - kertoo mitä pitäisi tehdä ja pitää promottaa tätää domain controlleri asetusta.



Nyt tässä luodaan kuin uusi organisaatio, ja jos on olemassa oleva "domain" niin voi suorittaa kuin olemassa oleva metsä (forest)

**Active Directory Domain Services Configuration Wizard** – mikä rooli tämä uusi palvelin saa metsässä (forest). Tämä on kriittinen kohta, koska se määrittää koko AD-rakenteen logiikan.

- ◊ **Add a domain controller to an existing domain**
  - + Lisää uuden domain controllerin olemassa olevaan domainiin

- ✗ Ei luo uutta domainia
  - ✓ Sama domain, sama organisaatio – usein käytetään **vikasietoisuuteen, kuormantasaamiseen, tai paikalliseen DC:hen eri toimipisteessä**
  - 🔒 Vaatii pääsyn olemassa olevaan domainiin ja valtuudet liittyä siihen
- 💡 "Toinen palvelin saman domainin sisällä – jakaa saman AD-tietokannan."**
- Lisää **uuden DC:n samaan domainiin** – esimerkiksi **toiseen maahan**, toimistoon tai palvelinsaliin – osana **samaa organisaatiota**.

## ◊ Add a new domain to an existing forest

- + Luo uusi **domain**, mutta **ei uutta metsää**
  - 🏢 Tyypillinen suurissa tai jaetuissa organisaatioissa, joissa eri yksiköille halutaan oma hallinta
  - 📁 Uusi domain voi olla:
    - **Child domain**: oulu.mydomain.local
    - **Tree domain**: newdomain.fi (eri nimialue, mutta samassa metsärakenteessa)
  - 🔒 Vaatii yhteyden olemassa olevaan metsään (esim. toiseen koneeseen)
- 💡 "Eri domain, mutta silti osa samaa organisaatiokokonaisuutta – voidaan hallita erikseen."**
- **Luo uusi domain**, joka on osa **samaa AD-metsää (forest)**.  
Käytetään, kun halutaan jakaa organisaatiota **osastoittain, maittain tai tehtäväalueittain**, mutta säilyttää **yhteinen rakenteellinen luottamus**.

## ◊ Add a new forest

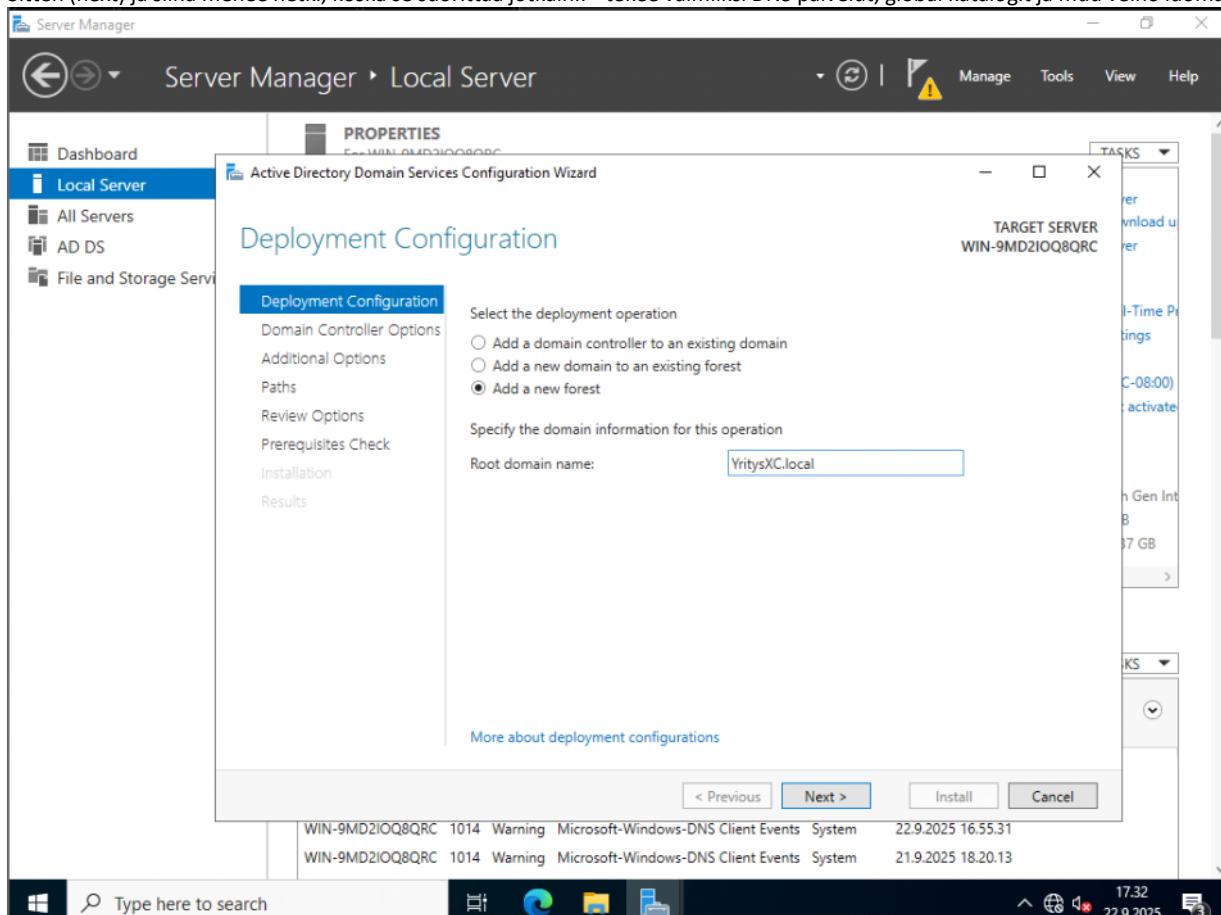
- ⚠️ Luo täysin **uuden metsän** ja samalla ensimmäisen domainin
  - ⚡ Käytetään, kun aloitetaan alusta – ei aiempaa AD:tä
  - ⚡ Esimerkiksi testikäyttöön, uuteen organisaatioon, tai täysin erilliseen järjestelmään
- 💡 "Täysin uusi organisaatio ja uusi AD-rakenne – oma hallinta, oma kokonaisuus."**

---

Nyt luodaan uusi (metsä) yritys ja perässä pitää olla ./local - koska se on vain sääntö - eli lähde on ihan normaalista tyhjästä.

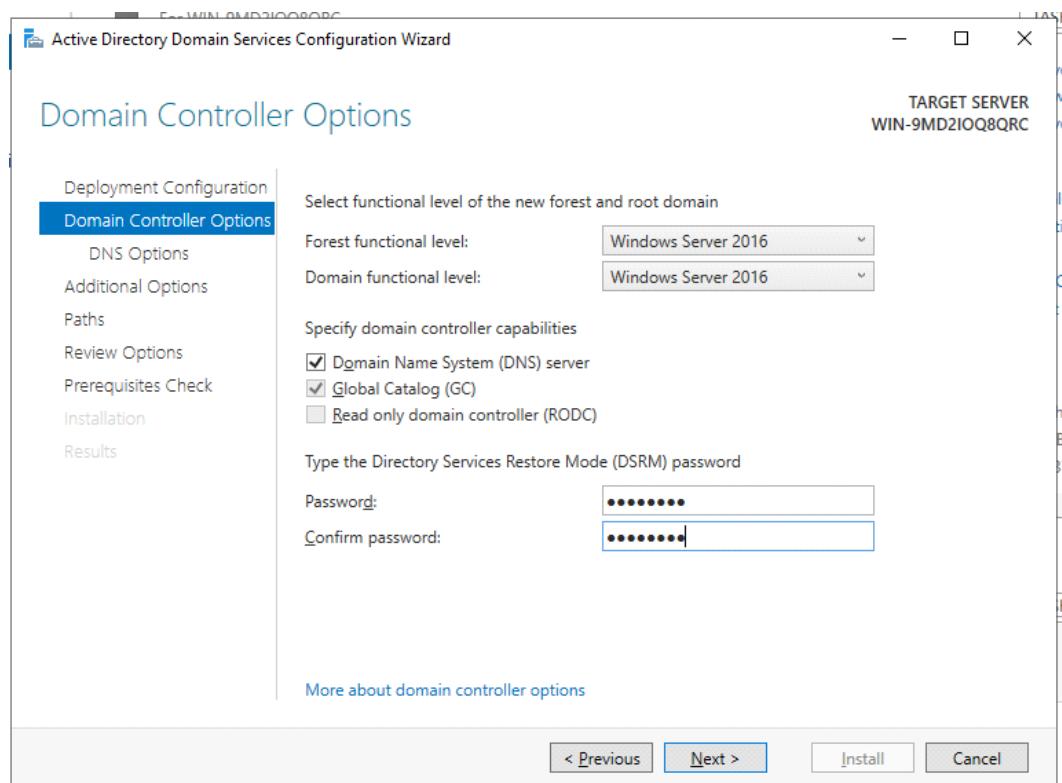
Nimetään firma: yritysXC.local (keksi ihan vapaasti nimi ja piste local pitää olla mukana).

Sitten (next) ja siinä menee hetki, koska se suorittaa jotkain.. - tekee valmiiksi DNS palvelut, global katalogit ja muu velho luomat

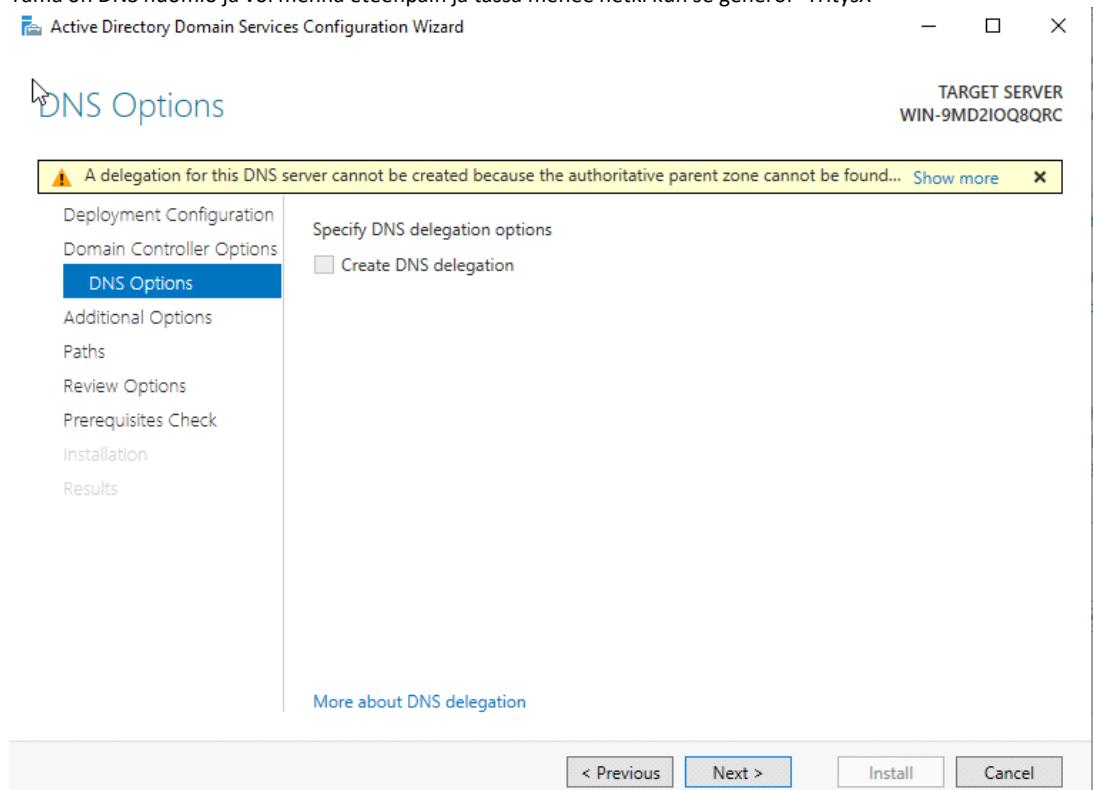


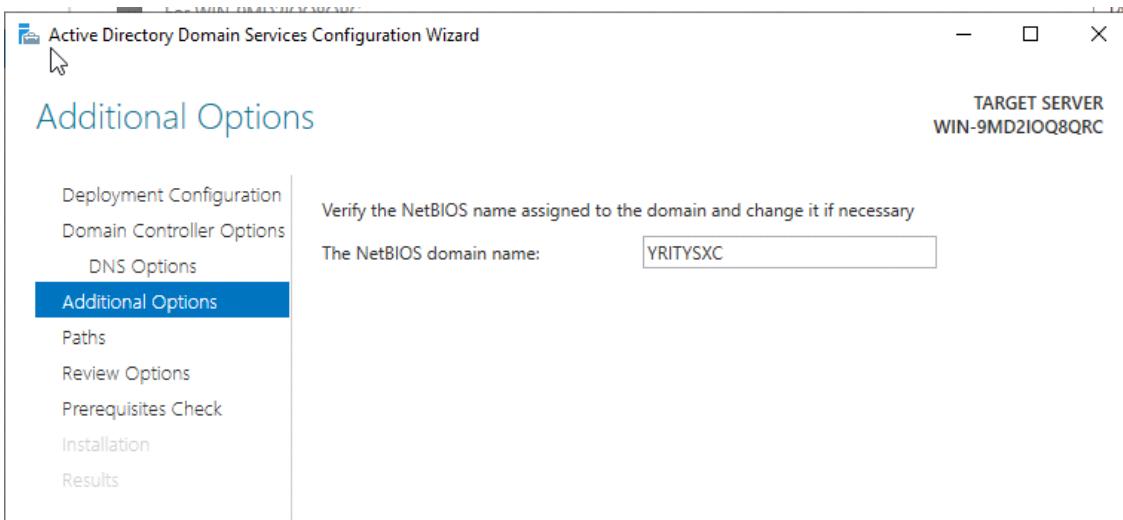
Seuraavaksi luodaan default settus ja asetetaan DSRM salsana (Directory Services Restore Mode)

- DSRM-järjestelmävalvojan tili on toimialueen ohjauskoneen ainoa paikallinen käyttäjätili. Tämä tili ei ole käytettävissä, kun ohjauskone käynnistetään normaalitilaan.
- Salasana: P@ssw0rd (nolla)

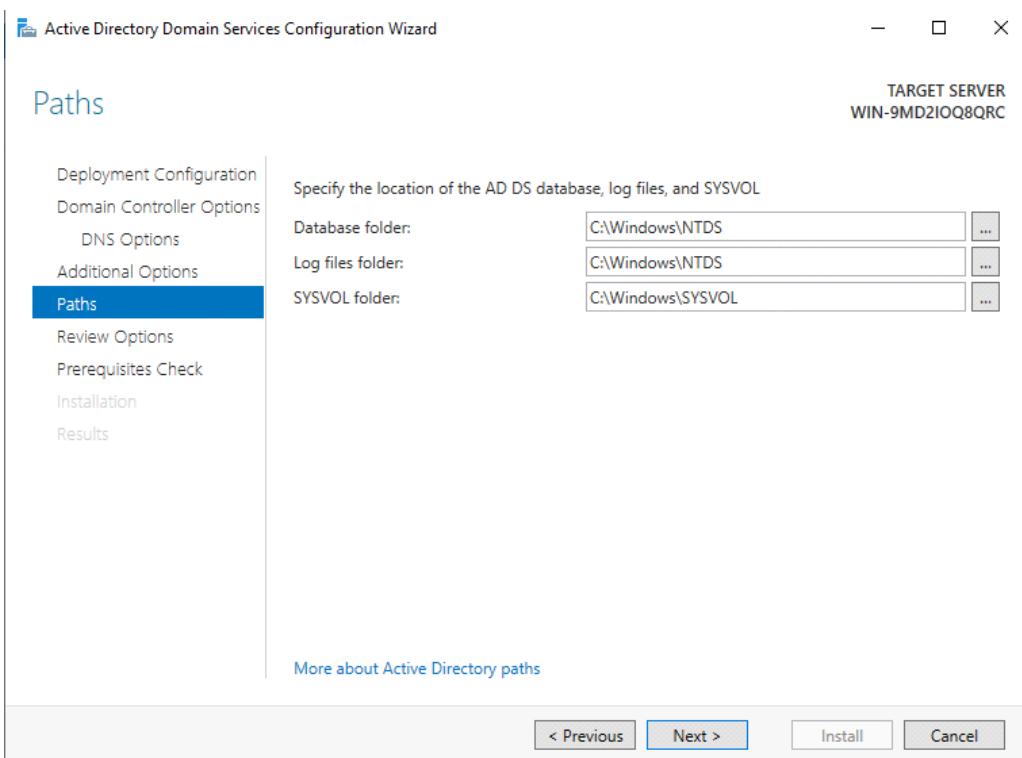


Tämä on DNS huomio ja voi mennä eteenpäin ja tässä menee hetki kun se generoi "YritysX"

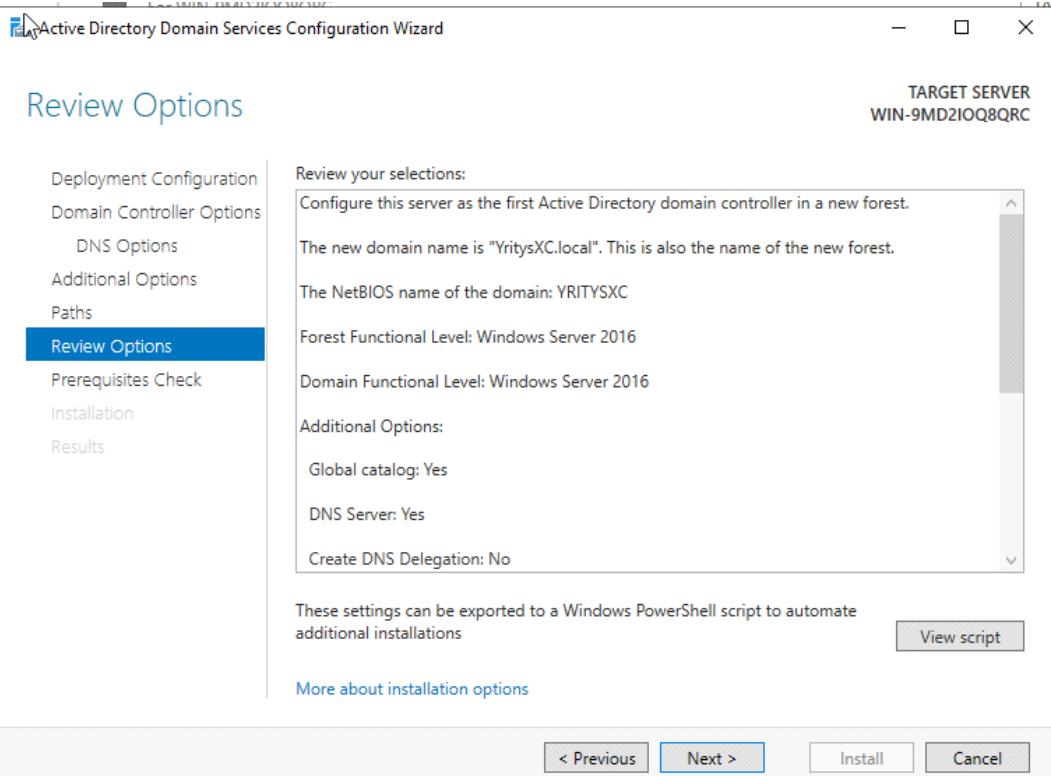




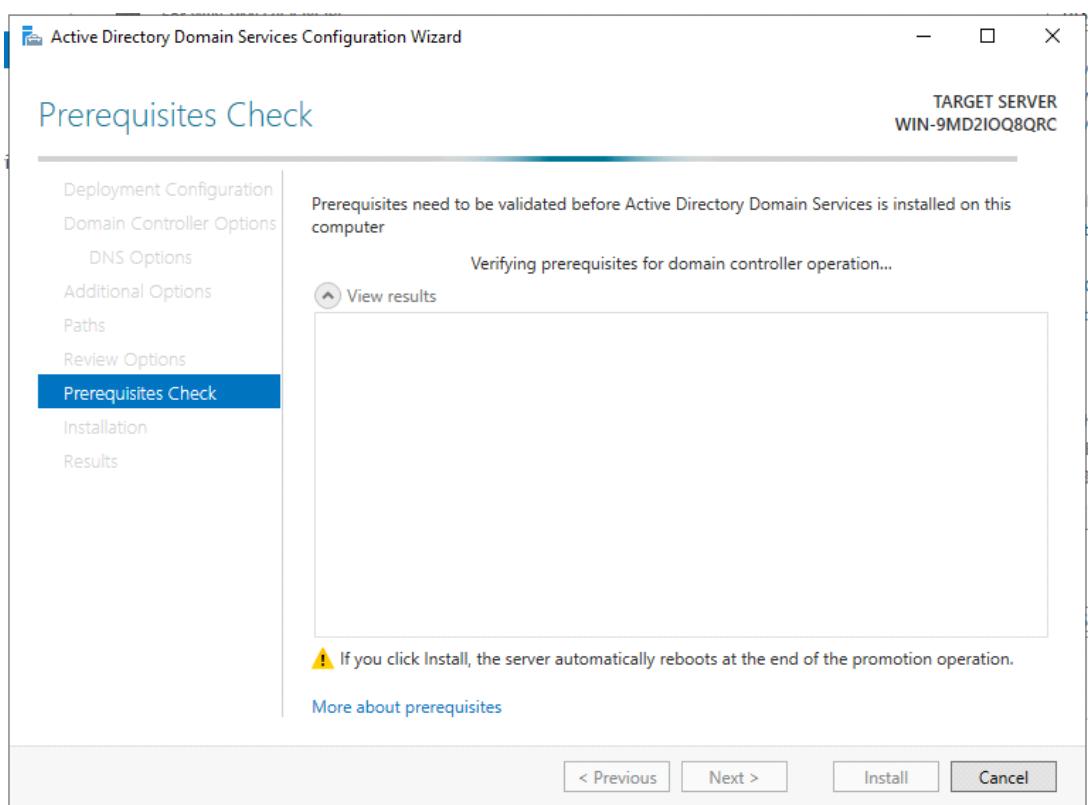
Tähän tulee tietokantoja ja jne, loki tiedostoja ja jne. Useimmin tämä on oletus



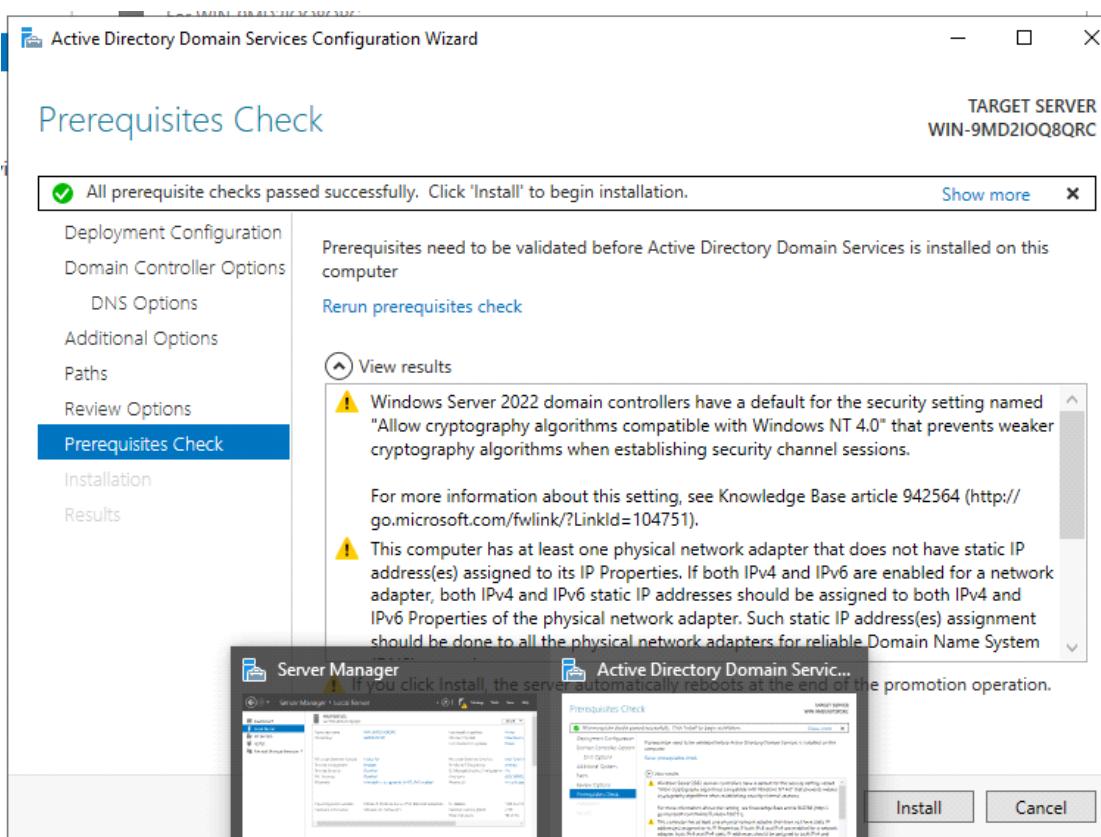
Tässä saadaan powershell skripti tarvittaessa talteen ja jne. Et vain "next"



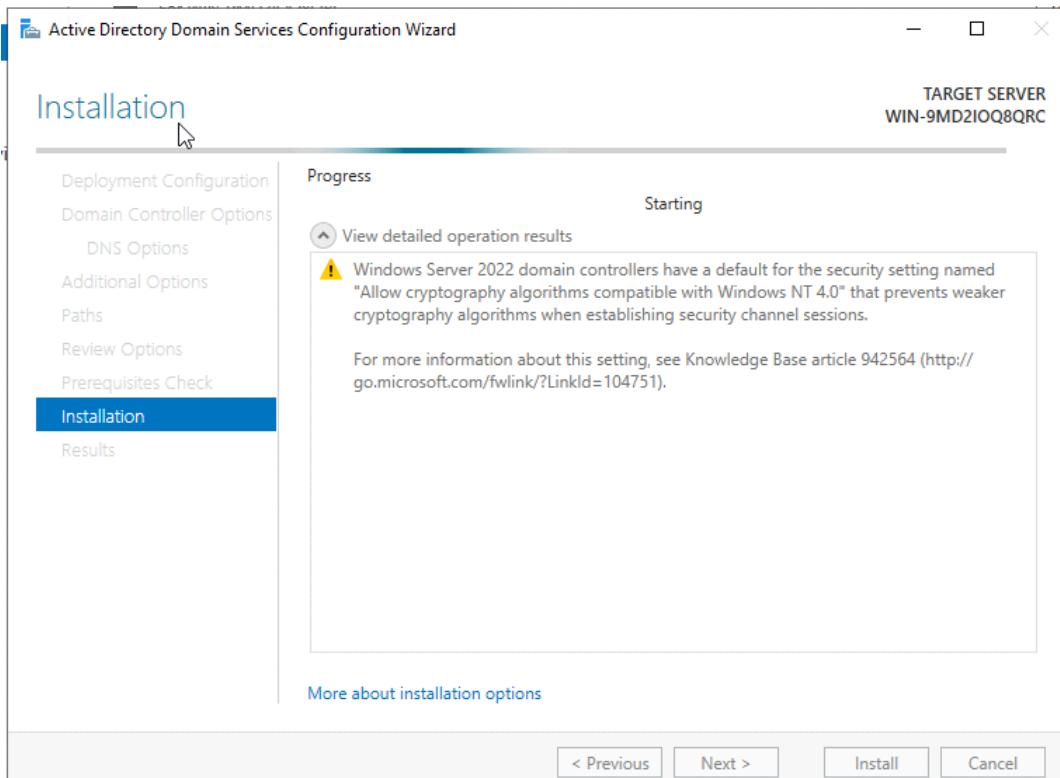
Tässä steppissä pitäisi tulla esitieto vaatimuksia ja hyväksyykö jotakin. Jotakin huomioita saattaa vilahta, mutta niitä ei tarvitse välittää.

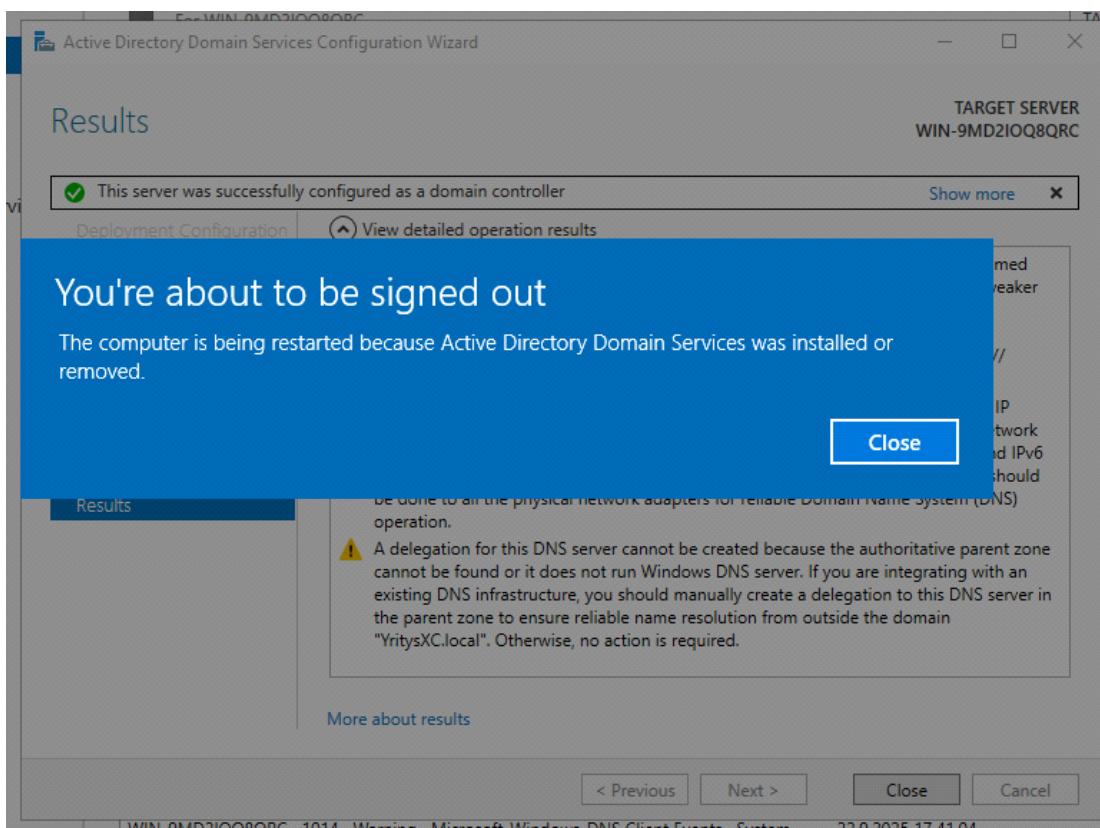


Toi vihree pallero sanoo - kaikki pitäisi olla "successfully" sitten vain "install" viimeisenä (toiseksi viimeisenä) ja antaa sen suorittaa määritykset ja tämän jälkeen uudelleen käynnistämisen



Tässä (installation) menee hetki/jonkin aikaa - että tulee ponnahdus sitten ja results ja onki ensimmäinen kerta palveluja generoidaan aktivoimaan - siis rakentaa uuden forest, asetukset ja muita juttuja päätee myös muita uudelleen käynnistystä/päivitystä.

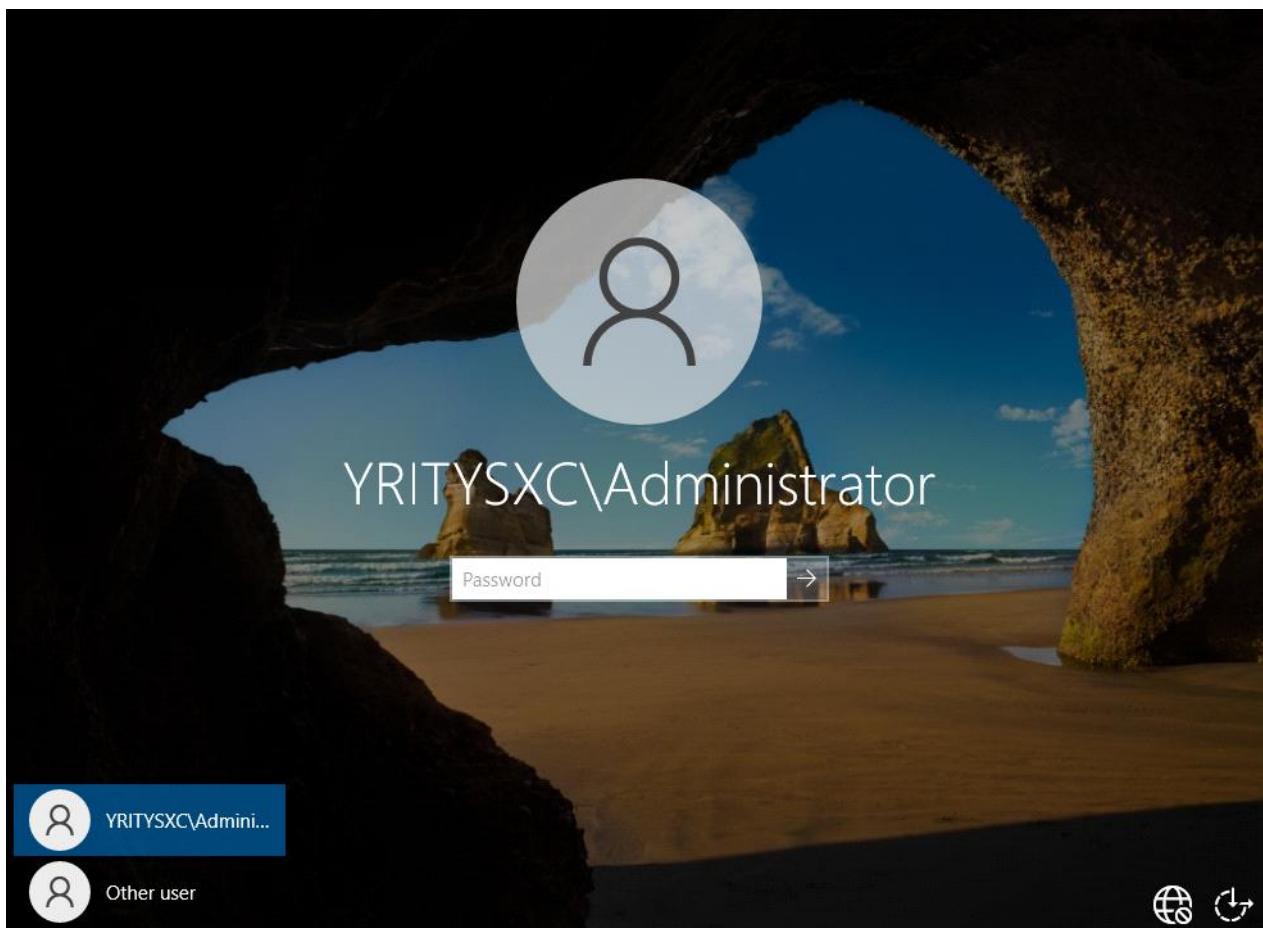




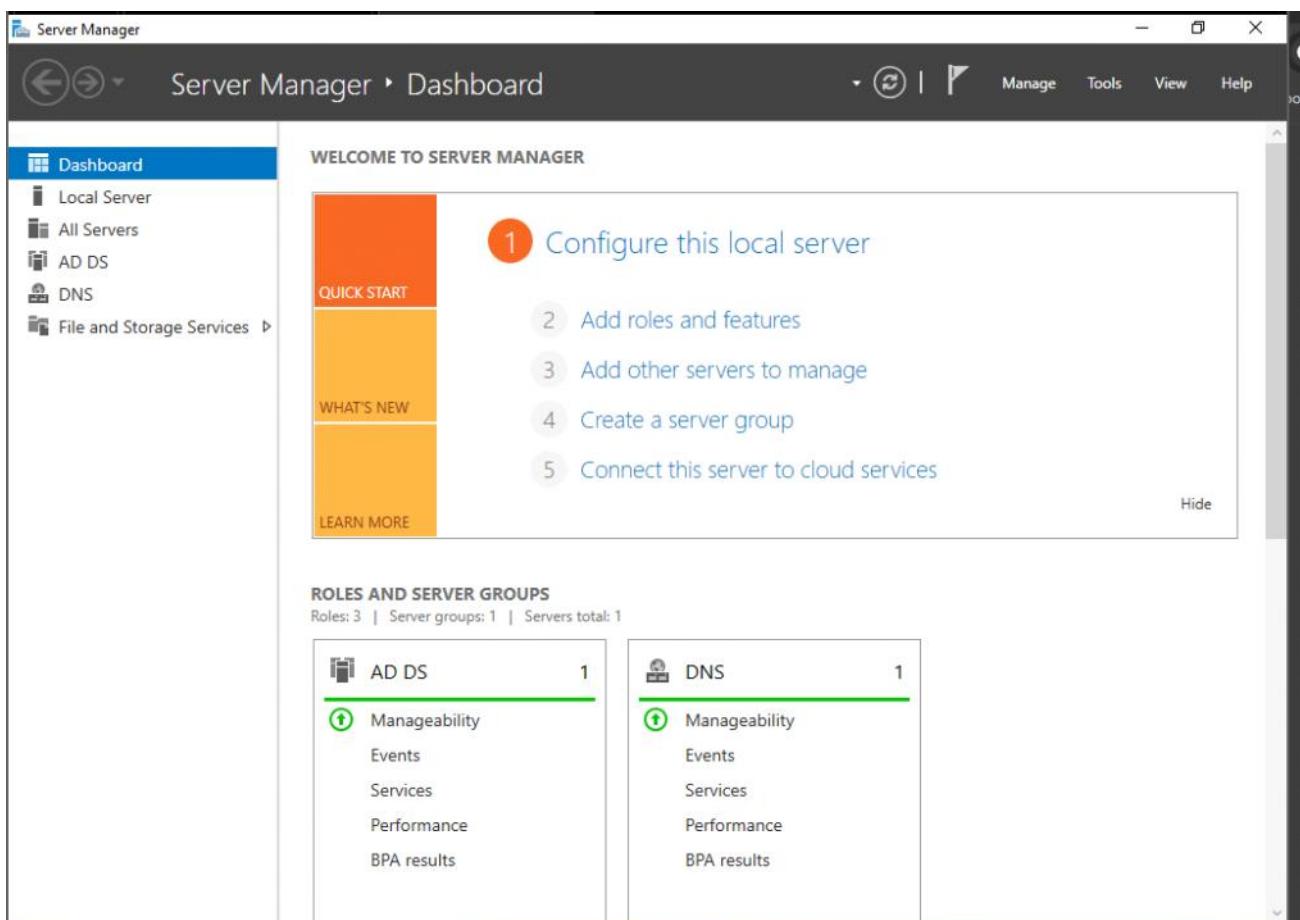
Nyt tuli tällainen ja mitä ihmettää

Nyt tässä on se yritysxc ja salasana : P@ssw0rd - jonka luottii aikaisempi

Siinä kirjauttuessa tulee sitten "Server manager" tulee näkyviinsä ja se suorittaa niitä asetuksia ja menee hetki.



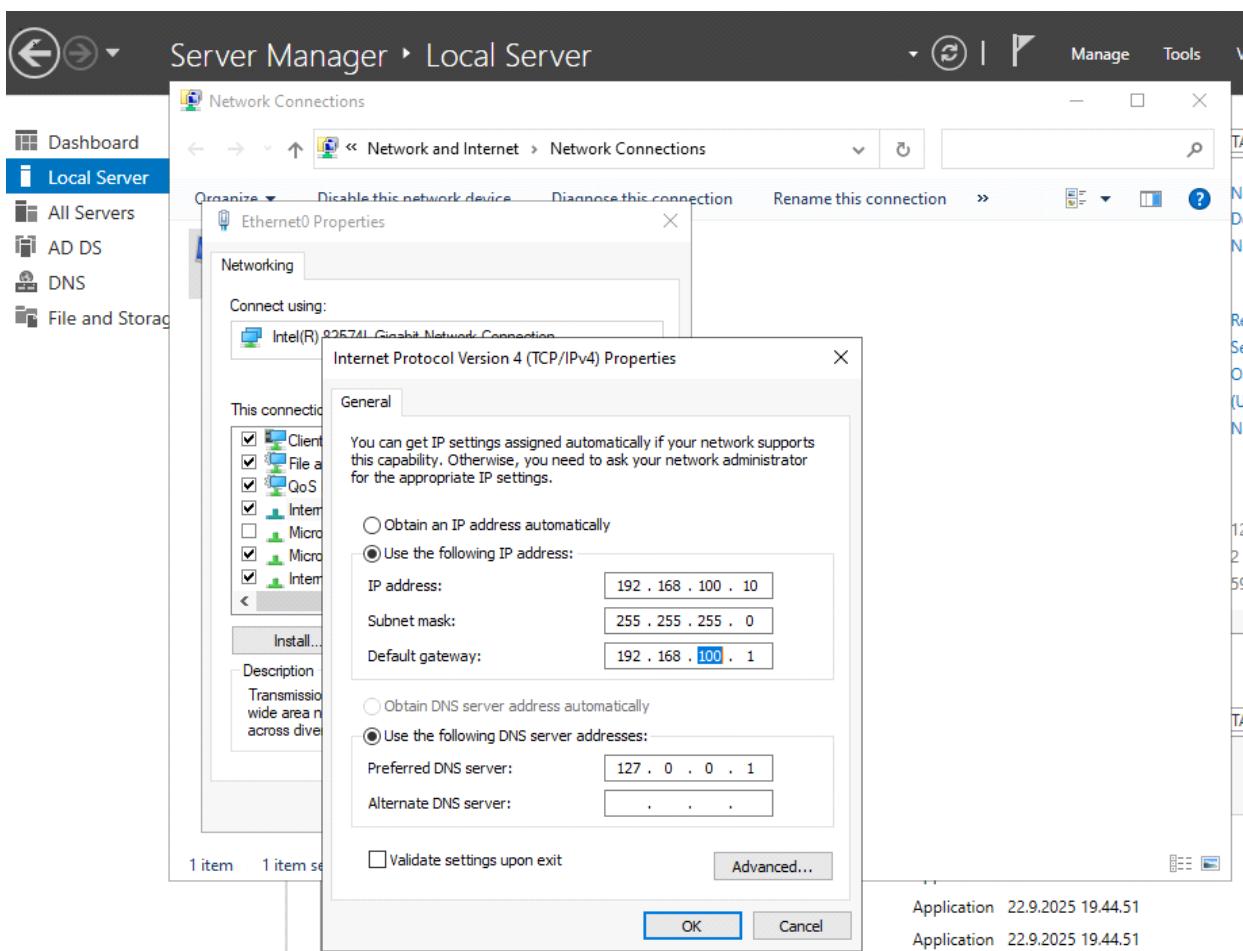
Vasemmalla (AD DS & DNS) ainakin tuli näkyviinsä ja jne. Samalla tarkistellaan muita asetuksia mm. IP osoite.



IP-osoite, josta se suorittaa promotuksensa & toimi alueensa.

Nyt tämä IP-osoite (palvelin): 192.168.100.10  
DNS localhost 127.0.0.1 tietokanta

Jossakin tilanteessa saattaa automaattisesti mennä (Obtain an IP address automatically).



Laitoin tosta "Ethernet0" dispabeld ja takaisin päälle niin tuli tällainen.

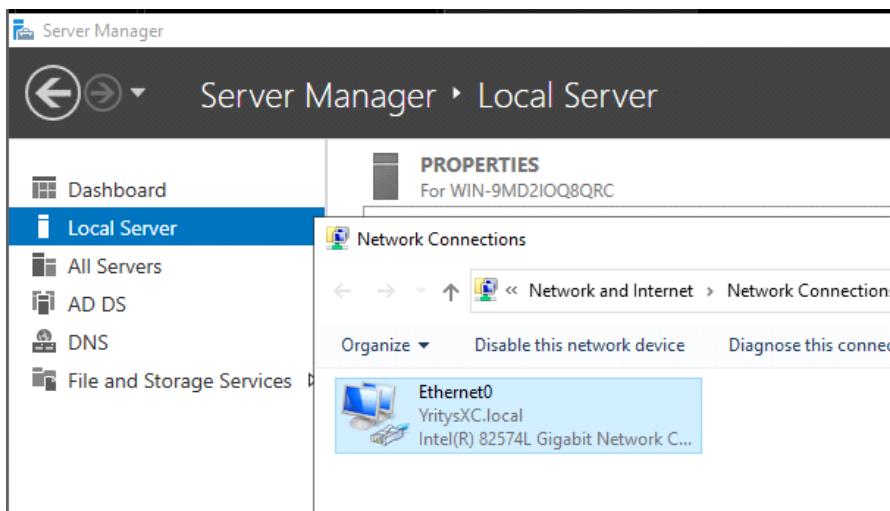
Joskus vaattii uudelleen käynnistämisen jos tää disable/enable - ei toimi ekalla/pari/muutamalla yrityksellä - älä turhaa testaa useita kertoja ja säilytä näin

**IP: 192.168.100.10**

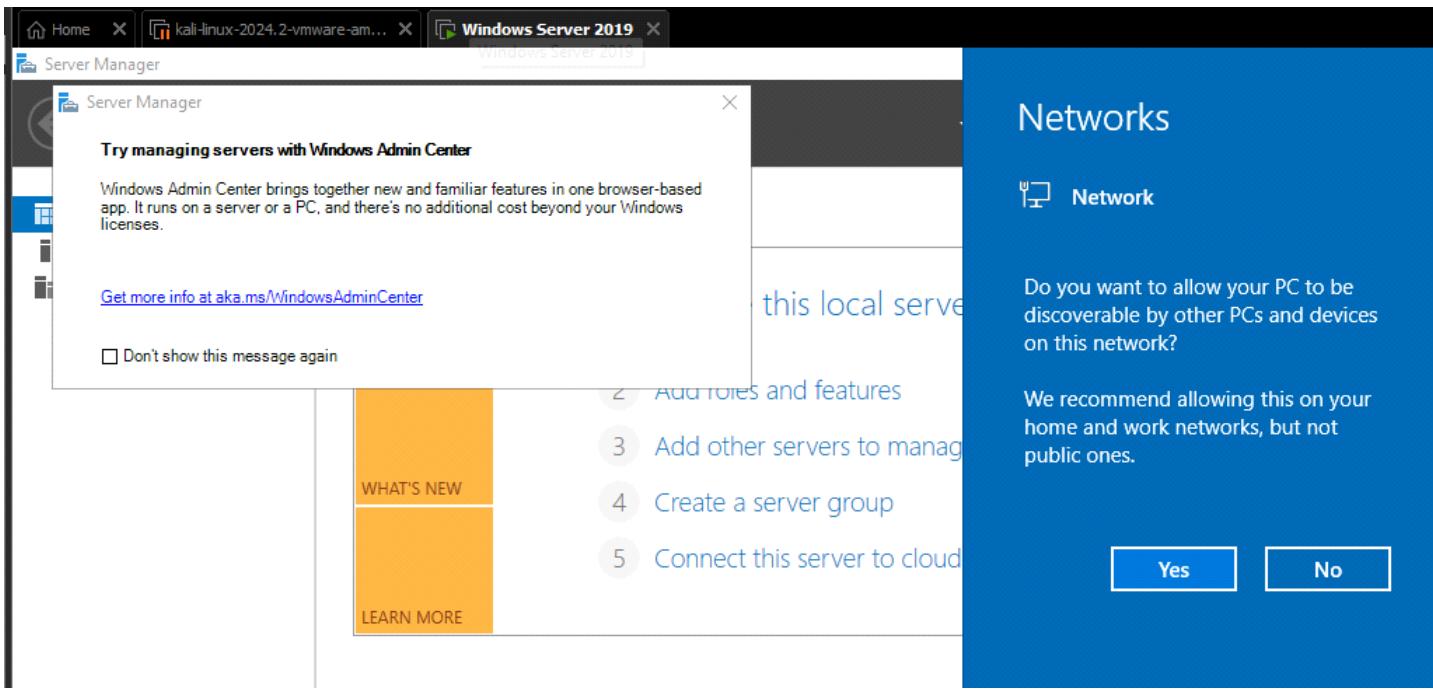
**Subnet /24 maski**

**Default gateway 192.168.100.1**

Preferred DNS server: 192.162.100.11



Buuttasin koneen varmuuden vuoksi siis tämä serveri niin ponnahti tällainen kuitenkin



Komento: \$Get-ADDomain

Tällä komennolla voi hakea tietoja AD (active directory) vekrkotunnusensa. Tämä on osa Windows PowerShellin active directory moduulia, ja sen avulla järjestelmänvalvojat voivat hallita ja automatisoida erilaisia AD-tehtäviä. Tämä konffaas on periaatteessa onnistunut ja toimii - ja toimivana tarkistuksena.

```

Administrator: Windows PowerShell
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Administrator> Get-ADDomain

AllowedDNSSuffixes : {}
ChildDomains : {}
ComputersContainer : CN=Computers,DC=YritysXC,DC=local
DeletedObjectsContainer : CN=Deleted Objects,DC=YritysXC,DC=local
DistinguishedName : DC=YritysXC,DC=local
DNSRoot : YritysXC.local
DomainControllersContainer : OU=Domain Controllers,DC=YritysXC,DC=local
DomainMode : Windows2016Domain
DomainSID : S-1-5-21-2366235558-2463432122-148030397
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=YritysXC,DC=local
Forest : YritysXC.local
InfrastructureMaster : WIN-9MD2IOQ8QRC.YritysXC.local
LastLogonReplicationInterval :
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=YritysXC,DC=local}
LostAndFoundContainer : CN=LostAndFound,DC=YritysXC,DC=local
ManagedBy :
Name : YritysXC
NetBIOSName : YRITYSXC
ObjectClass : domainDNS
ObjectGUID : fe6bebfa-8475-439c-82a2-daf97da3e644
ParentDomain :
PDCEmulator :
PublicKeyRequiredPasswordRolling :
QuotasContainer : CN=NTDS Quotas,DC=YritysXC,DC=local
ReadOnlyReplicaDirectoryServers :
ReplicaDirectoryServers :
RIDMaster :
SubordinateReferences : {DC=ForestDnsZones,DC=YritysXC,DC=local, DC=DomainDnsZones,DC=YritysXC,DC=local, CN=Configuration,DC=YritysXC,DC=local}
SystemsContainer : CN=System,DC=YritysXC,DC=local
UsersContainer : CN=Users,DC=YritysXC,DC=local

```

**PIENI YHTEENVETO TÄHÄN VÄLIIN - START HERE - 1;**

Tähän väliin konffattu windows server 2019 vois käyttää jatkossa pohjana et jos konffaan jotakin uutta esim. Organizatio UNIT jotakin niin jatkaa siitä projektia ja tai jotakin muuta testejä ilman mitään vmware workstaion snapsottia et joutuu palaa jo ka kerta taakse päin ja siitä muokkaa niitä kesken eräisiä asioita.

.vmx-tiedosto on **virtuaalikoneen asetustiedosto**, mutta **ei sisällä itse konetta**, eli käyttöjärjestelmää, levyä, dataa jne.

Tallentaa koko tiedoston 7zip tai zippi tiedostoon , ja rakentaa uuden vm pohjaisen koneensa vaan ja näin saisi suoritettu backup

### Eli: Jos haluat säilyttää koko ympäristön, tee näin:

#### 1. Tallenna koko virtuaalikoneen kansio

- Siirry kansioon, jossa virtuaalikone sijaitsee.
- Esimerkiksi:

```
D:\VMware\YritysXZ_AD\  
|   Windows Server 2019.vmx  
|   Windows Server 2019.vmdk  
|   Windows Server 2019.nvram  
|   muut tiedostot...
```

- Kopioi koko kansio esim. ulkoiselle levylle tai toiseen kansioon.
- Voit pakata sen 7-Zipillä, jos haluat säätää tilaa.

#### 2. Poista, ja palauta myöhemmin

- Jos poistat koneen VMwaresta, **älä poista levyltä tiedostoja**.
- Myöhemmin voit:
  - Avata VMware Workstationissa: **File → Open → valitse Windows Server 2019.vmx**.
  - Ja jatkaa täsmälleen siitä mihin jäit.

- Kopioi koko vanhan VM:n kansio uuteen paikkaan.
- Nimeä tiedostot uudelleen (esim. Windows Server 2019.vmx → ADLab01.vmx).
- Avaa kopio VMware Workstationissa.
- VMware kysyy: "**Did you move or copy this VM?**"
  - Vasta "I copied it" → estää SID-konflikteja jne.

## PIENI YHTEENVETO TÄHÄN VÄLIIN - START HERE - 2;

- "Forest"** on *Active Directoryn ylin rakenneyksikkö*.
- Forest = sisältää yhden tai useamman **domainin**.
- Forest syntyy vasta, kun **Active Directory Domain Services (AD DS)** on asennettu JA **DC-promootio** on tehty (eli konfiguroitu domain).

**"Forest"** = Active Directory -kokonaisuuden ylin taso, joka syntyy **AD DS -roolin promootiossa**.

- ◊ AD alkaa toimia vasta, kun olet **luonut forestin ja domainin** promootiossa – pelkkä AD DS -rooli ei vielä riitä.
- ◊ AD:n hallintatyökalut, kuten "**Users and Computers**", tulevat näkyviin vasta domain controllerin luomisen jälkeen.

"Forest" on nyt pystytetty nimellä YritysXC.local, eli olemme perustaneet ensimmäisen Active Directory -metsän ja samalla yrityksen ensimmäisen domainin. Tämä on Active Directoryn ensimmäinen varsinainen vaihe. Tästä eteenpäin voidaan luoda käyttäjiä, organisaatioyksiköitä (OU), hallita ryhmiä ja käytäntöjä (GPO), sekä määrittää käyttööikeuksia. Myös työasemia ja muita laitteita voidaan liittää domainiin ja hallita keskitetysti, kaikki samassa VMware Workstation -ympäristössä, joka toimii harjoitus- eli hiekkalaatikkoympäristöön.

## Nyt koskien tätä konffausta, mitä tässä ollaan asennettu eli "**windows server 2019**" & mini yhteenvetö ja jatko toimenpide

Tämä on koskien yhteenvetö, mitä tässä ollaan kofinguroitu, mitä tämä tarkoittaa, mitä jatkontoimenpidettä voisi tehdä ja mahdollisesti huonoa puolia.

Nyt tässä konffaussessa mitä ollaan konfiguroitu on **Windows Serveriin tämä "Active directory Domain Services (AD DS)"** ja luotu **domain (yritysXC.local)** yritysverkko - tämä kokonaisuus on "**On-premises AD**"

- Windows Server + AD DS = On-Premises AD
  - Tämä tarkoittaa "klassisen yritysverkkoa" johon liitetään fyysisesti koneet ja käyttäjät liitämiset.
  - Kokonaisuudessaan tämä toimii parhaiten oppimisen ja harjoittelun ympäristöön.

Ympäristö: **Windows Server 2019/2022 + Active Directory Domain Services (AD DS)**

Toteutustapa: **On-Premises AD** (ei Azure/Entra käytössä tässä vaiheessa)

Domain: yritysxc.local

## **⚠️ Ongelmia ja rajoituksia (ilman Azurea):**

- **Uusi käyttäjä tai uusi kone:**
  - Pitää kirjautua kerran yritysverkossa (LAN/VPN), jotta domain-profiili luodaan.
  - Utta laitetta ei voi täysin ottaa käyttöön etänä ilman yhteyttä domain controlleriin.
- **Salasanan vaihto tai palautus:**
  - Vaatii yhteyden domainiin (LAN tai VPN), muuten salasana ei päivity koneelle.
  - Jos käyttäjä vaihtaa koneen tai palaa etätöistä, profiilin pitää olla jo valmiiksi välimuistissa.
- **Kun käyttäjä poistuu:**
  - IT poistaa tunnukset AD:stä ja ottaa laitteet takaisin hallintaan.
  - Sama prosessi toistuu, kun kone otetaan uudelleen käyttöön toiselle käyttäjälle.

## **⊖ Huonot puolet (On-Prem ilman Azurea):**

- **Ei tue modernia hallintaa** (esim. Intune, Entra ID, pilvi-GPO:t)
- **Vaatii manuaalista esiasennusta:**
  - Kone pitää liittää domainiin LAN-ympäristössä
  - Käyttäjän pitää kirjautua vähintään kerran, ennen kuin voi työskennellä etänä
- **Etäkäytöönotto ei onnistu ilman VPN-ratkaisuja**
- **Salasanojen vaihdot, lukitukset yms. vaatii suoran yhteyden DC:hen**

## **On-premises (virallinen fyysisen palvelin) versus Azure AD (Entra ID) pilvipalvelu**

Tämä perinteisen AD DS (Active Directory Domain Services) vaatii todellisuudessa fyysisen tai suoran verkko - eli LAN-/VPN-yhteyden toimiakseen kunnolla.

- Tämä AD DS eli aktivoituna ja asennettuna On-premises Windows Serverin alla.

## **✓ Perinteinen AD DS (Windows Serverissä) – miten se oikeasti toimii**

- Tätä käytetään virallisesti LAN (lähiverkko) eli fyysisen yhteys
- Joka kerta uusi laite ja kone (läppäri) tarvitse liittääkseen AD:hen (yritysXY.local), joka pitääkseen tehdä verkossa, jossa saa firman tarvittavat asetukset, tunnukset ja muu oikeudet.
  - Tämä pitää suorittaa fyysisesti LAN yhteydellä tai VPN:llä.
- Tunnusten luonti ja esiasennus tehdään AD DS:n kautta
  - Käyttäjä siis saa uuden tunnuksen, käyttäjäoikeudet, ryhmäjäsenyydet mihin osastoon ja ketä siellä on nimettyvä ja GPO:n - kaikki aseteet
  - Salasanan vaihto tai päivitystä vaattii DC (domain controller)
- Koneen palautus / uudelleenkäyttö tai vaihto
  - Tämä päätee koneiden vaihto, elinkaaresta tai uudelleen käyttö esim. Uudelle omistajalle
  - IT tuki eli se administrator kuka hallitsee windows serveriä niin hän poistaa käyttäjän tunuksen AD:sta
  - Suorittaa kaikki koneen nollauksensa ja tämä pitää liittää koneen AD:n kautta käyttäen LAN yhteyttä.

## **ⓧ Eli rajoituksia tulee ilman Intunea tai Azurea:**

Tarve	On-Prem AD DS yksin	Azure / Intune
Uuden koneen käytöönotto ilman fyysisä verkko	✗ Ei onnistu	<input checked="" type="checkbox"/> Autopilot tai Azure AD Join
Salasanan vaihto etänä	✗ Vain VPN:n kautta	<input checked="" type="checkbox"/>
Etälukitus tai -puhdistus (esim. katoaminen)	✗ Ei onnistu	<input checked="" type="checkbox"/>
Sovellusten hallinta pilven kautta	✗	<input checked="" type="checkbox"/> Intune
AD/GPO:t toimivat internetin yli	✗	<input checked="" type="checkbox"/> (Pilvi-GPO:t tai Intune Policies)

Periaatteessa on rajoituksia verrattuna fyysisen windows server verrattuna pilvipalvelun Azure tarjoamaan työkaluun eli Intuneen.

- Kertauksena: Intune on pilvipalveluna toimiva etähallintatyökalu, joka mahdollistaa työasemien ja mobiililaitteiden hallinnan ilman fyysisä palvelinta. Verrattuna perinteiseen Windows Server -ympäristöön, Intune tarjoaa modernin hallintamallin, mutta joitain rajoituksia voi esiintyä esimerkiksi syvällisessä verkko- ja palvelinkonfiguroinnissa.
- AD DS perinteisessä Windows Server -ympäristössä edellyttää fyysisä LAN-verkko tai vähintään VPN-yhteyttä, jos halutaan hallita koneita, tehdä kirjautumisia, vaihtaa salasanoja tai suorittaa koneiden esiasennuksia.

## **Virallinen Windows Serveri tämä AD DS**

**AD DS vaatii palvelimen, joka on päällä silloin kun sitä tarvitaan.**

Fyysisys ei ole pakollista (VM riittää), mutta **24/7 saatavuus on tärkeää**.

Harjoitteluympäristöissä voit käyttää virtuaalikonetta vaikka työpöytäkoneella/läppärissä.

Tuotannossa DC:t sijoitetaan yleensä konesaliin tai palvelinkeskukseen, usein kahdennetusti ja UPS-sähköön taakse.

**Jos rakentaisi AD DS työpöytään ja suositeltavana testi ympäristönä, eikä tuotannossa.**

**Virallinen Windows Server, jossa ajetaan Active Directory Domain Services (AD DS), on "serveriympäristö", joka toimii käytännössä palvelimena, ja sen kuuluu olla päällä 24/7, varsinkin tuotantoympäristössä. Periaatteessa palvelin, eikä työpöytäkoneella, vaikka sisällä asetuksista on konfiguroitu on "domain controller" eli DC, johon saataviin kuuluu:**

- Käyttäjät voivat kirjautua
- DNS-resoluutiot toimivat
- GPO:t ja kirjautumispoliikit saadaan koneille
- Tunnusia voidaan hallita

Yrityskäytössä tämä tarkoittaisi 24/7, mukaan on sähköt päällä ja usein ajettuna näitä komponenteja:

- UPS-varmistus (keskeytymätön virransyöttö)
- RAID-levyt ja varmuuskopiot
- Useampi DC redundanssia varten

## Vmware workstation - Windows server - Snapshot - tärkeä osuus

Tärkeä osuus tästä on otettu yksi väliaikainen snapshot.

Tämä on muistutus ja huomio osuus: koskien omaan vmware workstation on asennettu Windwos Server ja sen alla on Active Directory Domain Services (AD DS). Tähän asti on otettu Snapshot - kertauksena snapshot on vähän kuin ottaa tallennuskohta pelissä. Jos tulee mokattua, voit ladata takaisin ja yrittää uudelleen eri tavalla.

Pelissäkin tallennetaan muistiin "**save the game**" (take a snapshot) ja jatkaisi pelaamista, jos pelissä tulee error tai epäonnistumista tilanteeseen voi tarvittaessa palata taakse pään kuin "**load the game**" (palauta snapshot).

TÄMÄ ON KUVA ON GOOGLE KUVAHAUSTA - EI OLE OMA KONE JA ESIM:

