Toimialue palvelujen perustaminen

Oheinen dokumentti kertoo fiktiivisestä Tmi. Jarno nimisestä PK -yrityksestä ja sen palvelin infrastruktuurista.

Palvelinympäristö koostuu Windows Server 2019 Core sekä Linux Ubuntu Server 18.04 palvelimista.

Server 2019 Core:en päädyin siksi, että sillä voidaan hyvin toteuttaa kaikki peruspalvelut toimialueella ja palvelimen asennus “jalanjälki” on pieni eikä se resurssointi mielessä käytä ylimääräistä palvelin kapasiteettia.

Toimialueelle tulee myös Windows 10 v1909 työasema, joka käyttää toimialueelle perustettuja palveluita.

Palvelinympäristö koostuu seuraavista palvelimista ja rooleista mitä niihin on asennettu. Tulen myös kuvaamaan tässä dokumentissa tarkemmin itse asennuksesta ja roolien asetuksista, jotta ne toimivat oikein ja palvelevat toimialueen työasemia.

Inf-dc01.jarno.local (Windows Server 2019 Core)
-Active Directory Domain Services
Tämä palvelu mahdollistaa käyttäjien kirjautumisen ja hallinnan. Tämä on perusta kaikelle
-DNS Server
Tämä palvelu mahdollistaa nimenselvityksen IP-osoitteelle, eli kun tämä muuttaa esim. 8.8.8.8 IP-osoitteen www.google.com nimeksi tai päin vastoin (ReverseDNS) www.google.com DNS nimen osoitteeksi 8.8.8.8
-DHCP Server
Tällä palvelulla voimme jakaa dynaamisia IP-osoitteita toimialueen työasemille jotta voimme käyttää verkon palveluita
-File and Storage Services
Tämä palvelu mahdollistaa tiedostojen jaon palvelimelta työasemille, esimerkiksi kotiverkkolevyn tai yhteiset verkkolevyn
-Print and Document Services
Tällä palvelulla voimme luoda jaettuja tulostimia verkkoon sekä jakaa niitä Group Policyjen / GPO avulla

Inf-ca001.jarno.local (Windows Server 2019 Core)
-Active Directory Certificate Services
Tällä palvelulla voimme luoda sertifikaatteja toimialueella erilaiselle palveluille, esim. www -palvelimelle (https)

Inf-mssql01.jarno.local(Windows Server 2019 Core)
-Microsoft SQL Server 2019 (Express)
Voimme tällä palvelulla luoda tietokantoja palveluille toimialueella

www-server.jarno.local (Ubuntu Server 18.04)
-WordPress -palvelin www -sivuja varten
Luomme tällä palvelulla toimialueelle www -palvelimen, jolla voidaan julkaista tietoa WordPress sovelluksella.

Tulen myös liittämään Ubuntu Server www -palvelimen osaksi Windows Active Directoryä, jotta toimialue käyttäjät voivat kirjauta omalla Active Directory tunnuksillaan palvelimelle ssh -protokollan avulla.
Tästä syystä ei tarvitse luoda erillisiä käyttäjiä Ubuntu palvelimelle.

Myöskin tulen käyttämään LDAP -integraatiota WordPress palvelimelle jotta käyttäjät voivat kirjautua myös omilla Active Directory tunnuksillaan WordPress hallinta sovellukseen ja tätä kautta voidaan antaa myös eritason oikeuksia itse WordPress hallinnassa käyttäen Active Directory ryhmiä

Tulen myös asentamaan Untangle nimisen Linux Debian pohjaisen palomuuri sovelluspalvelimen osaksi verkkoa, joka hoitaa liikenteen ulospäin internettiin.

Palvelimien asennus sekä verkko konfiguraatio perustiedot

Toimialueen verkkokonfiguraation on seuraava.

Gateway (Untangle palomuuri appliance)
10.0.10.1

Mask
255.0.0.0/8

DNS (INF-DC01)
10.0.10.2

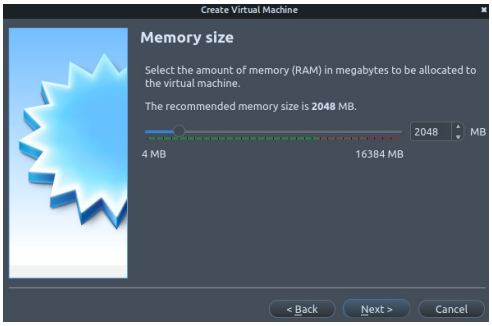
Tulen kuvaamaan perusasennuksen ensimmäisellä kerralla Windows Server 2019 Core -versiolle. Muiden palvelimen Windows Server 2019 core asennus tapahtuu samalla tavalla. Itse roolien asennus sitten tullaan kuvaamaan tarkemmin per. Toimialue palvelin tässä dokumentissa.

Myös tulen kuvaamaan Ubuntu Server 18.04 asennuksen myös aivan alusta lähtien, kun sen asennus poikkeaa Windows Server Core 2019 versiosta.

Inf-dc01 asennus

Luodaan ensin uusi Virtualbox palvelin ja käynnistetään Windows Server 2019 -iso tiedostokuvalla. Valitaan kuvaa nimi, eli tässä tapauksessa Windows Server Core

Määritellään muistin määrä, voidaan mennä oletuksella eli 2048MB

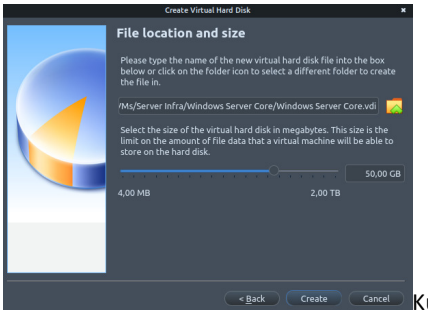


Määritellään uusi virtuaalinen kovalevy

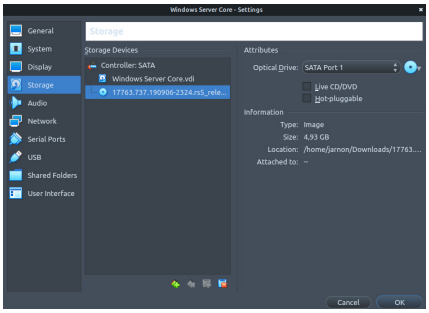
Valitaan kovalevyn tyyppi (Oletus VDI)

Määritellään tilankäyttö, eli onko levy dynaaminen (täyttyy sitä mukaan, kun tietoa kirjoitettaan) vai fixed (eli varataan maksimi tila heti kovalevyltä). Valitaan Dynamically (Oletus)

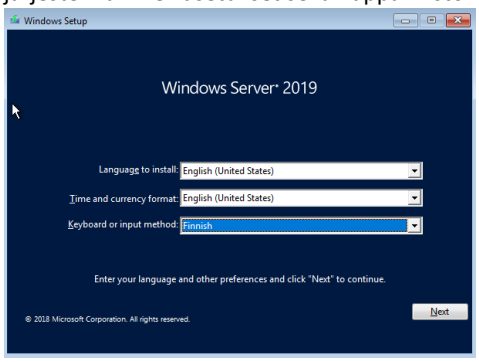
Määritellään kovalevyn paikka isäntäkoneella ja sen koko. Mennään oletuksella 50GB



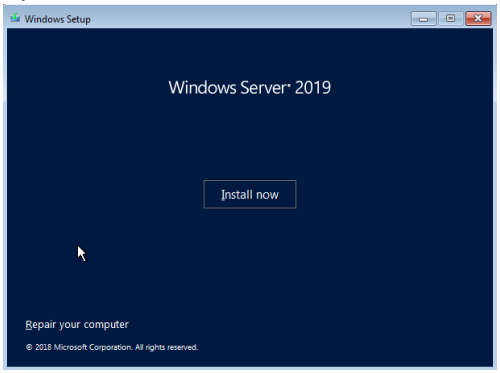
Kun olemme luoneet uuden virtuaali koneen, lisäämme Windows Server 2019 .iso levykuva -tiedoston, jolta sitten käynnistämme koneen asennusta varten.



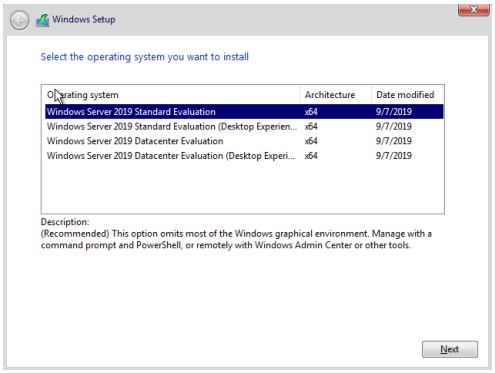
Nyt olemme käynnistäneet koneen Windows Server 2019 .iso -tiedostolta ja ensimmäiseksi valitaan järjestelmän kieli asetukset sekä näppäimistön kieli



Nyt valitsemme Install now

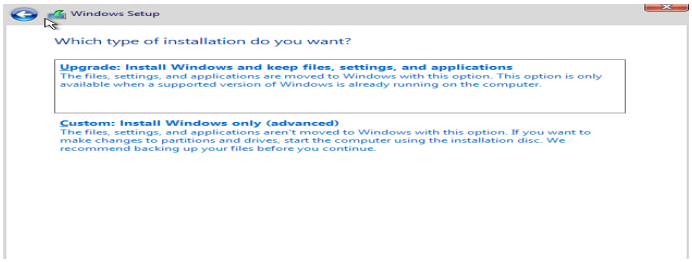


Kun haluamme asentaa Windows Server 2019 Core version ilman GUI / Desktop Expierence ominaisuutta valitsemme ylimmän vaihtoehdon (oletus)

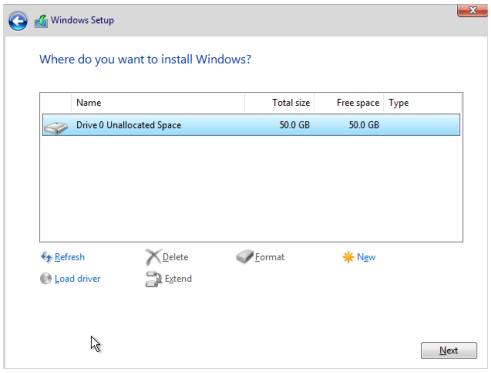


Seuraavaksi luemme loppukäyttäjäsopimuksen ja ruksaamme “I accept the license” terms” ja klikkaamme Next

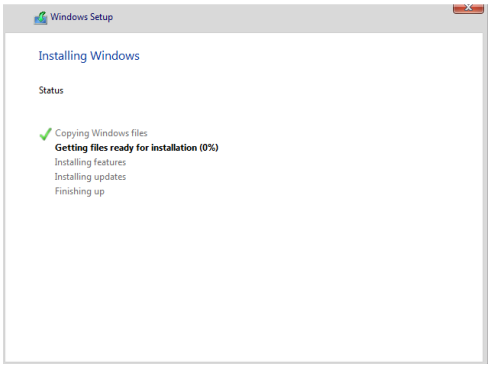
Kun kyseessä on uusi asennus, valitsemme Custom



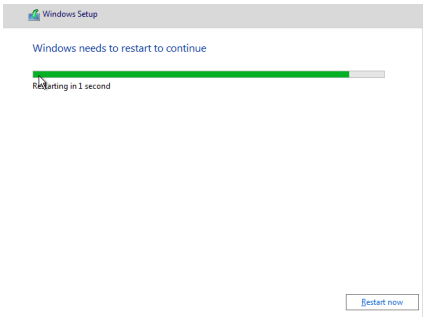
Ja kun levyllä ei ole ennestään mitään osiota, voimme Windowsin asennuksen hoitaa sen meidän puolestamme valitsemalle Next



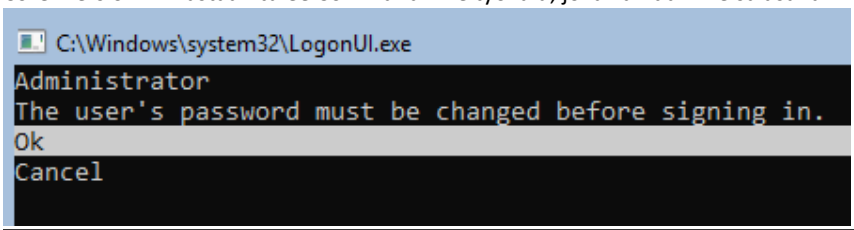
Tämän jälkeen itse asennus käynnistyy ja palvelin käynnistää itseään muutamaan kertaan uudelleen automaattisesti

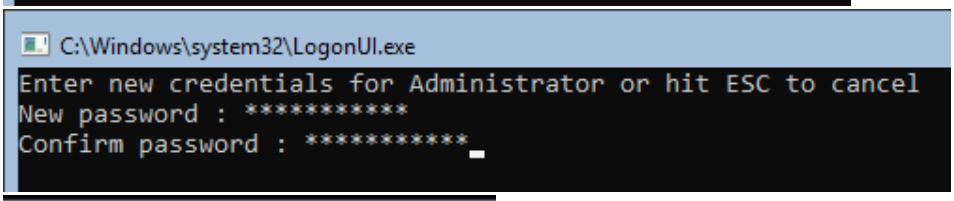


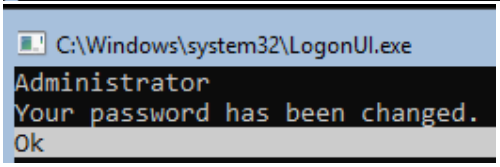
Tässä kohta kone käynnistyy uudelleen



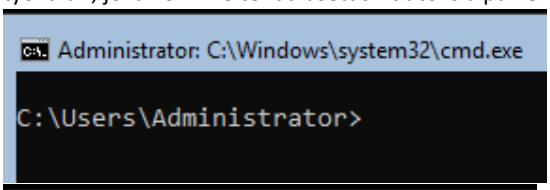
Ensimmäisellä kerralla meidän pitää määrittää Administrator käyttäjän salasana. Ja kun on kyseessä Core -versio niin vastaan tulee Command Line työkalu, jolla vaihdamme salasanan

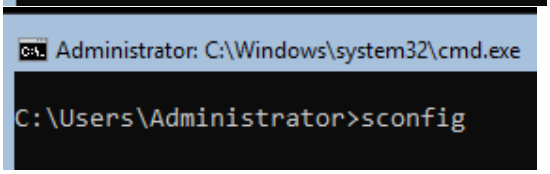






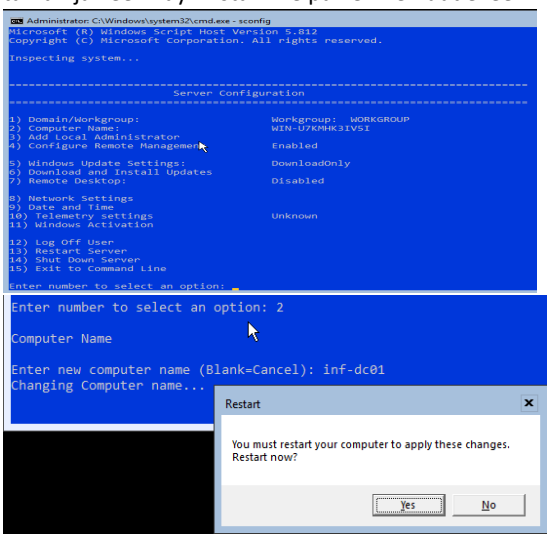
Kun olemme saaneet salasanan vaihdettua ja kirjautuneet sisään, käynnistämme sconfig nimisen työkalun, jolla voimme tehdä asetusmuutoksia palvelimelle



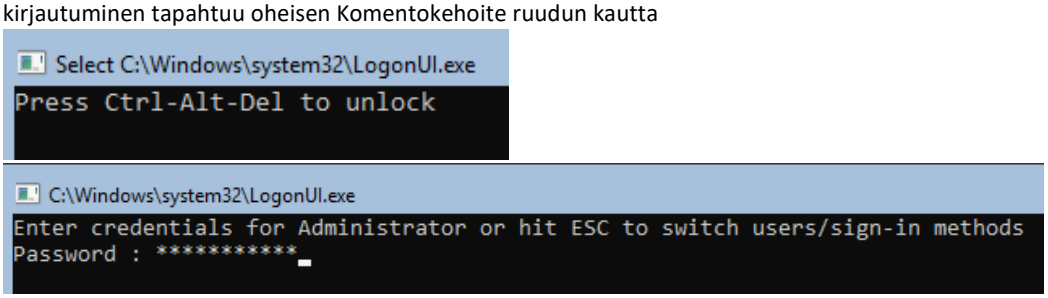


Ensiksi vaihdamme koneen nimen valitsemalle numeron 2 ja painamalla Enter

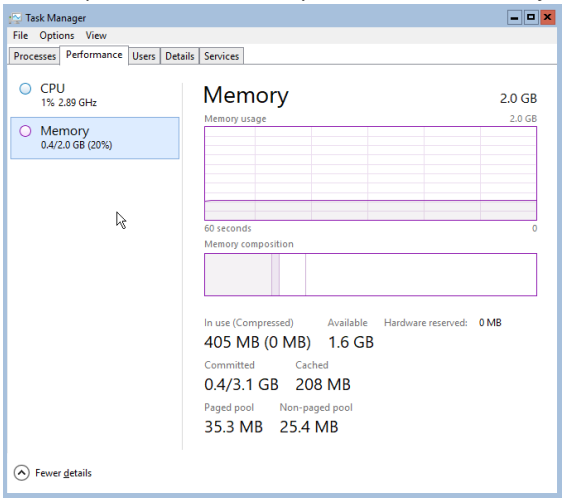
Kun kyseessä on uuden toimialueen Domain Controller palvelin niin annamme sille nimeksi inf-dc01 ja tämän jälkeen käynnistämme palvelimen uudelleen.



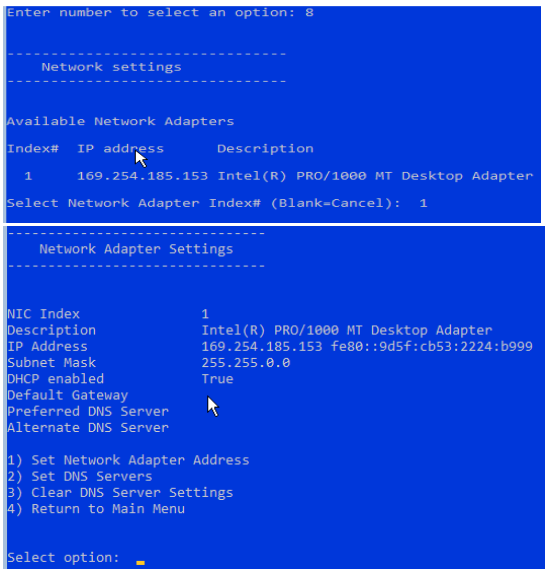
Nyt olemme käynnistäneet palvelimen uudelleen nimen muutoksen jälkeen ja kun tässä on kyseessä Windows Server Core asennus, niin mitään graaffista kirjautumisruutua ei ole tarjolla vaan kirjautuminen tapahtuu oheisen Komentokehoite ruudun kautta



Tässä vaiheessa voimme katsoa esimerkiksi mitä palvelimen muistinkäyttö on oletuksena Core -versiossa.
Tässä tapauksessa muistin käyttö on 405MB / 1.6GB joka on varsin pientä Windows palvelimen osalta.



Seuravaksi määritämme uuden IP-osoitteen palvelimelle. Kun kyseessä on palvelin, pitää IP-osoitteen olla kiinteä / Static



```
Select option:  1

Select (D)HCP, (S)tatic IP (Blank=Cancel): S

Set Static IP
Enter static IP address: 10.0.10.2
Enter subnet mask (Blank = Default 255.0.0.0):
Enter default gateway: 10.0.10.1
Setting NIC to static IP...

------------------------------
    Network Adapter Settings
------------------------------

NIC Index               1
Description             Intel(R) PRO/1000 MT Desktop Adapter
IP Address              10.0.10.2       fe80::9d5f:cb53:2224:b999
Subnet Mask             255.0.0.0
DHCP enabled            False
Default Gateway         10.0.10.1
Preferred DNS Server
Alternate DNS Server

1) Set Network Adapter Address
2) Set DNS Servers
3) Clear DNS Server Settings
4) Return to Main Menu

Select option:
```

```
1) Set Network Adapter Address
2) Set DNS Servers
3) Clear DNS Server Settings
4) Return to Main Menu

Select option:  4

================================================================================
                            Server Configuration
================================================================================

1) Domain/Workgroup:                    Workgroup:  WORKGROUP
2) Computer Name:                       INF-DC01
3) Add Local Administrator
4) Configure Remote Management          Enabled

5) Windows Update Settings:             DownloadOnly
6) Download and Install Updates
7) Remote Desktop:                      Disabled

8) Network Settings
9) Date and Time
10) Telemetry settings                  Unknown
11) Windows Activation

12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

Enter number to select an option: 15
```

Nyt kun olemme määrittäneet oikein IP-osoitteen palvelimelle, voimme käynnistää PowerShell työkalun hallintaa varten.

```
C:\Users\Administrator>powershell
```

Nyt kun haluamme asentaa tästä palvelimesta Domain Controllerin, niin lisäämme ensin palvelin ominaisuuden koneelle

```
C:\Users\Administrator>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator>
```

```
PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services, Group P...


PS C:\Users\Administrator>
```

Tämän jälkeen tuomme ADDSDeployment moduulin palvelimme ja sen jälkeen käynnistämmme Domain Controller asennuksen Install-ADDSForest komennolla

Asennuksessa määritämme uuden toimialueen nimen (jarno.local) sekä vikasietotilan salasanan jota tarvitsemme, jos meidän pitää suorittaa korjaustoimenpiteitä Active Directory tietokannalle tai palvelimelle.

Tämän jälkeen valitsemme Y, jotta ryhdymme luomaan uuden metsän Active Directory palvelinta. Asennuksen jälkeen palvelin käynnistyy automaattisesti uudelleen.

```
PS C:\Users\Administrator> Import-Module ADDSDeployment
PS C:\Users\Administrator> Install-ADDSForest

cmdlet Install-ADDSForest at command pipeline position 1
Supply values for the following parameters:
DomainName: jarno.local
SafeModeAdministratorPassword: ***********
Confirm SafeModeAdministratorPassword: ***********

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

```
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y
WARNING: Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it
 does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually
create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain
"jarno.local". Otherwise, no action is required.

WARNING: Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it
 does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually
create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain
"jarno.local". Otherwise, no action is required.


Message                      Context          RebootRequired  Status
-------                      -------          --------------  ------
Operation completed successfully DCPromo.General.3         False Success


PS C:\Users\Administrator>
```

Nyt voimme ensimmäistä kertaa kirjautua Administrator tunnuksella uudelle toimialueelle

```
Select C:\Windows\system32\LogonUI.exe
Enter credentials for JARNO\Administrator or hit ESC to switch users/sign-in methods
Password :
```

Asennuksen aikana palvelimelle asentui myös automaattisesti DNS ominaisuus, kun se on edellytys Active Directoryn toiminalle

Seuraavaksi asennamme uudelle Active Directory palvelimelle DHCP ominaisuuden

Olemme jo käynnistäneet PowerShell hallinta työkalun ja lisäämässä DHCP palvelinta sekä hallinta työkaluja

```
PS C:\Users\Administrator> Install-WindowsFeature DHCP -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {DHCP Server}


PS C:\Users\Administrator>
```

Tämän jälkeen luomme uuden Scopen tälle palvelimelle:
Add-DHCPServerv4Scope -Name “Internal” -StartRange 10.0.10.100 -EndRange 10.0.10.200 -SubnetMask 255.0.0.0 -State Active

```
PS C:\Users\Administrator> Add-DhcpServerv4Scope -Name "Internal" -StartRange 10.0.10.100 -EndRange 10.0.10.200 -SubnetM
ask 255.0.0.0 -State Active
PS C:\Users\Administrator>
```

Lisäämme uudelle scopelle Domain, DNS palvelin sekä yhdyskäytän tiedot:
Set-DHCPServerv4OptionValue -ScopeID 10.0.10.0 -DnsDomain jarno. local -DnsServer 10.0.10.2 -Router 10.0.10.1

```
PS C:\Users\Administrator> Set-DhcpServerv4OptionValue -ScopeID 10.0.10.0 -DnsDomain jarno.local -DnsServer 10.0.10.2 -R
outer 10.0.10.1
PS C:\Users\Administrator>
```

Lopuksi lisäämme DHCP palvelimen Active Directory palvelimelle, jotta se voi alkaa jakaa osoitteita:
Add-DhcpServerInDC -DnsName jarno.local -IpAddress 10.0.10.2

```
PS C:\Users\Administrator> Add-DhcpServerInDC -DnsName jarno.local -IPAddress 10.0.10.2
PS C:\Users\Administrator>
```

Tarkistamme vielä, että kaikki asetukset ovat kunnossa:
Get-DhcpServerv4Scope

```
PS C:\Users\Administrator> Get-DhcpServerv4Scope

ScopeId         SubnetMask      Name           State    StartRange      EndRange        LeaseDuration
-------         ----------      ----           -----    ----------      --------        -------------
10.0.0.0        255.0.0.0       Internal       Active   10.0.10.100     10.0.10.200     8.00:00:00

PS C:\Users\Administrator>
```

Sekä toimialueella on palvelin authorisoitu:
Get-DhcpServerInDC

```
PS C:\Users\Administrator> Get-DhcpServerInDC

IPAddress            DnsName
---------            -------
10.0.10.2            jarno.local


PS C:\Users\Administrator>
```

Nyt asennamme Tiedostopalvelin omaisuuden

```
PS C:\Users\Administrator> Install-WindowsFeature File-Services

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}


PS C:\Users\Administrator>
```

Sekä Tulostuspalvelin omaisuuden

```
Select Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrator> Install-WindowsFeature Print-Server

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Print Server, Print and Document Services}


PS C:\Users\Administrator>
```

Lopuksi myös muistamme lisätä DNS Forwarder tiedon osoittamaan meidän Untangle -palomuuriin nimenselvitys tietoja varten, jotta pääsemme ulkomaailmaan myös DNS tietoja käyttäen (esim. https:\\www.google.com)

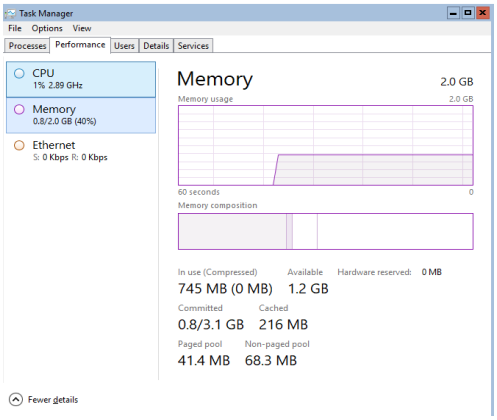
Add-DnsServerForwarder -IPAddress 172.23.90.124 -PassThru

```
PS C:\Users\Administrator> Add-DnsServerForwarder -IPAddress 10.0.10.1 -PassThru


UseRootHint        : True
Timeout(s)         : 3
EnableReordering   : True
IPAddress          : {10.0.10.1, fec0:0:0:ffff::1, fec0:0:0:ffff::2, fec0:0:0:ffff::3}
ReorderedIPAddress : {10.0.10.1, fec0:0:0:ffff::1, fec0:0:0:ffff::2, fec0:0:0:ffff::3}


PS C:\Users\Administrator>
```

Nyt voimme vielä tarkistaa mikä on palvelimen muistinkäyttö, kun olemme lisänneet

Active Directory, DNS Palvelin, DHCP Palvelin, Tiedostopalvelin sekä Tulostuspalvelin ominaisuudet

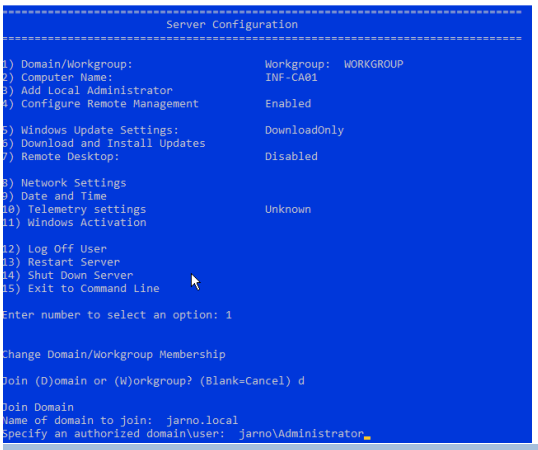
Muistia on vielä yli puolet käyttämättä 2.0GB jonka olin määritellyt asennus vaiheessa, eli muistin käyttö Corella on mielestäni todella vähäistä, kun ei tarvitse mitään “turhaa” pitää ajossa kuten graaffista liittymää

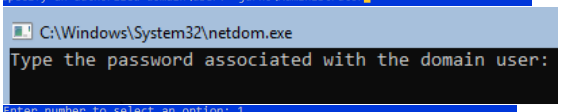


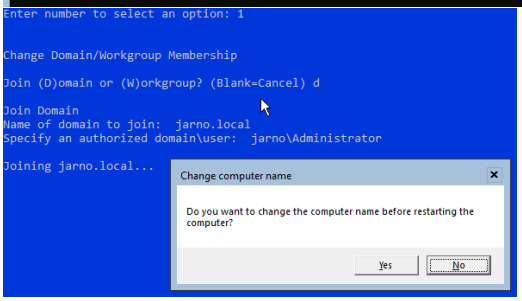
Inf-ca01 asennus

Seuraavaksi asennamme uudelle toimialueelle Active Directory Certificate Services palvelimen
Olemme luoneet jo uuden virtuaali- palvelimen valmiiksi, määritelleet sille oikein kiinteän IP
-osoitteen sekä antaneet kuvaan nimen eli inf-ca01

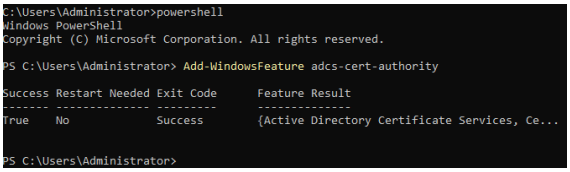
Kun kyseessä on sertifikaatti authority palvelin, nimeä ei voi enää muuttaa sen jälkeen olemme asentaneet tämän omaisuuden koneelle



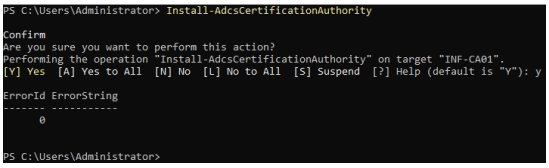




Nyt kun olemme liitteet palvelin toimialueelle, lisäämme PowerShell hallinta työkalua käyttäen Active Directory Certificate Services ominaisuuden palvelimelle:
Add-WindowsFeature adcs-cert-authority



Ja kun olemme lisänneet ominaisuuden, niin asennamme itse Active Directory Certificate Services palvelun:
Install-AdcsCertificationAuthority



Inf-mssql01 asennus

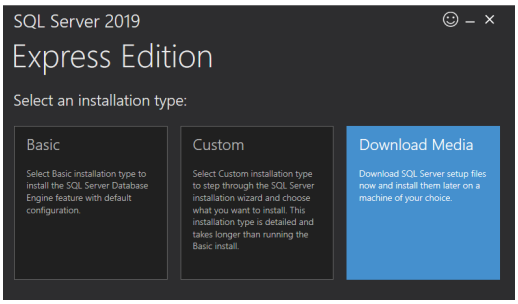
Nyt on vuorossa Microsoft SQL Server asennus.
Asennusta varten olemme taas luoneet uuden Server Core 2019 asennuksen, antaneet asennuksen jälkeen oikeat verkkoasetukset, oikean nimen (inf-mssql001) sekä liittäneet palvelimen toimialueelle

Tämän jälkeen lataamme asennusta varten tiedoston Microsoftin palvelimelta osoitteesta
https://www.microsoft.com/en-us/sql-server/sql-server-downloads

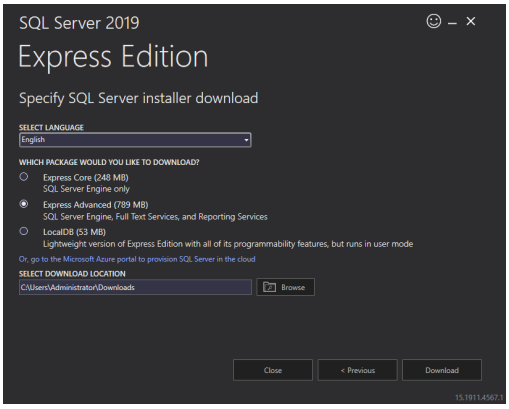
Tämän jälkeen suoritamme tiedoston komentokehoitteesta:

```
C:\Users\Administrator\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is B084-EB77

 Directory of C:\Users\Administrator\Downloads

02/07/2020  03:39 AM    <DIR>          .
02/07/2020  03:39 AM    <DIR>          ..
02/07/2020  03:37 AM         6,131,808 SQL2019-SSEI-Expr.exe
               1 File(s)      6,131,808 bytes
               2 Dir(s)  46,122,139,648 bytes free

C:\Users\Administrator\Downloads>SQL2019-SSEI-Expr.exe

C:\Users\Administrator\Downloads>_
```

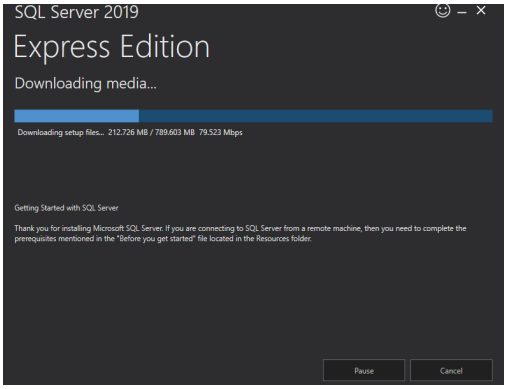
Valitsemme Download Media



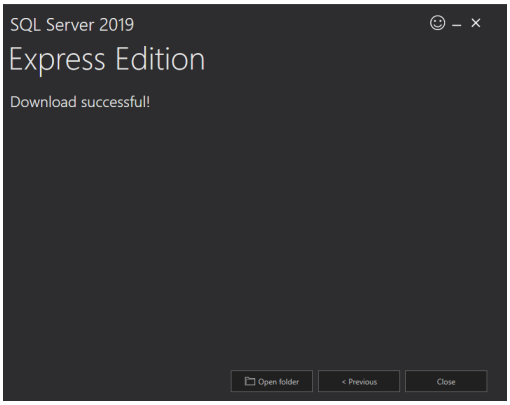
Kieleksi English, paketiksi valitsemme Express Advanced ja tallennamme tiedoston C:\Users\Administrator\Downloads (oletus) valitsemalla lopuksi Download



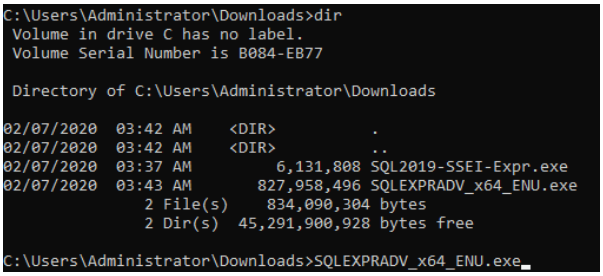
Oheinen ikkuna kertoo latauksen keston ja nopeuden:



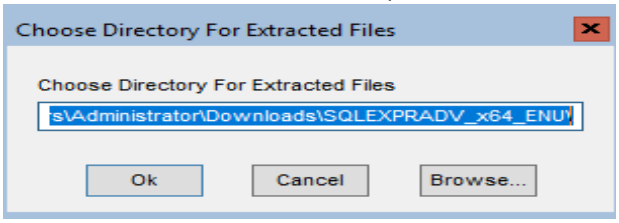
Ja lopuksi lataus velho ilmoittaa latauksen onnistuneeksi,



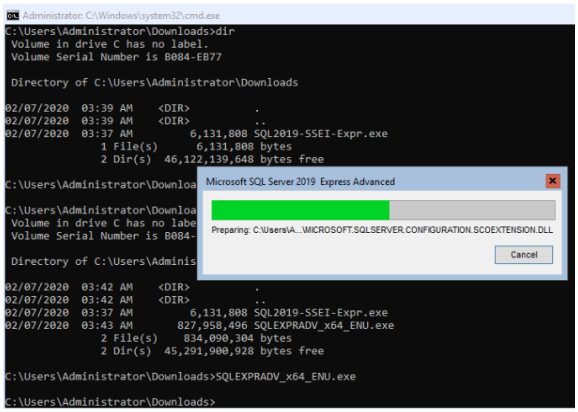
Seuraavaksi puramme ladatun tiedoston palvelimelle asennusta varten.



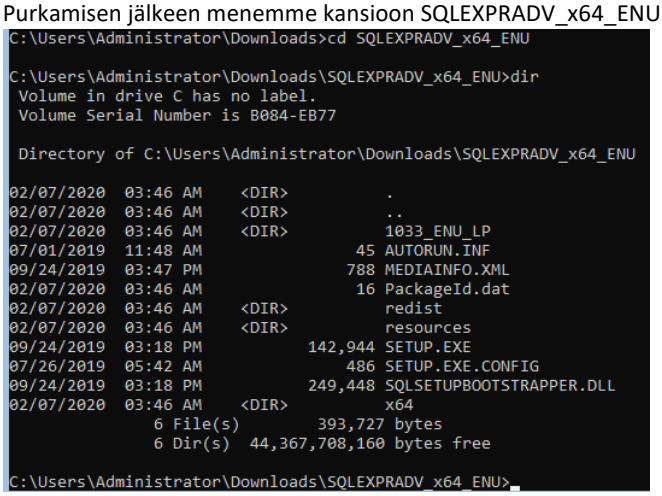
Valitsemme minne asennus tiedostot puretaan:



Nyt itse purkaminen tapahtuu



Purkamisen jälkeen menemme kansioon SQLEXPRADV_x64_ENU



Ja sieltä suoritamme oheisen komennon jolla asennamme SQL Palvelimen:

```
C:\Users\Administrator\Downloads\SQLEXPRADV_x64_ENU>SETUP.EXE /Q /IAcceptSQLServerLicenseTerms /Action=install /TCPEnabl
ed=1 /InstanceName=MSSQLSERVER /Features=SQLENGINE /Sqlsvcaccount=jarno\Administrator /Sqlsvcpassword=Password!
```

```
Microsoft (R) SQL Server 2019 15.00.2000.05
Copyright (c) 2019 Microsoft.  All rights reserved.

SQL Server 2019 transmits information about your installation experience, as well as other usage and performance data, t
o Microsoft to help improve the product. To learn more about SQL Server 2019 data processing and privacy controls, pleas
e see the Privacy Statement.

C:\Users\Administrator\Downloads\SQLEXPRADV_x64_ENU>
```

Ja asennuksen jälkeen määritämme, että SQL Browser palvelu käynnistyy automaattisesti myös, kun palvelin käynnistyy uudelleen:

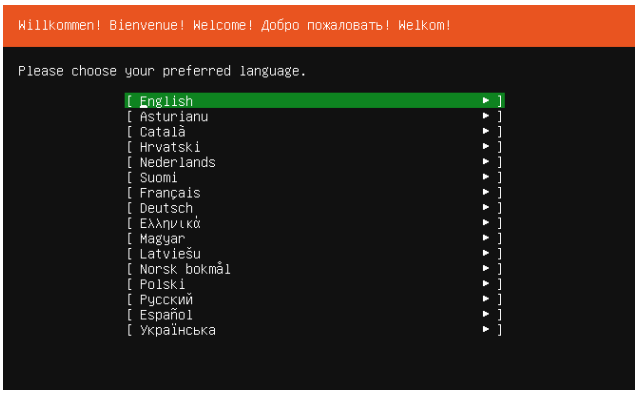
sc config sqlbrowser start=auto

```
C:\Users\Administrator\Downloads\SQLEXPRADV_x64_ENU>sc config sqlbrowser start=auto
[SC] ChangeServiceConfig SUCCESS

C:\Users\Administrator\Downloads\SQLEXPRADV_x64_ENU>
```

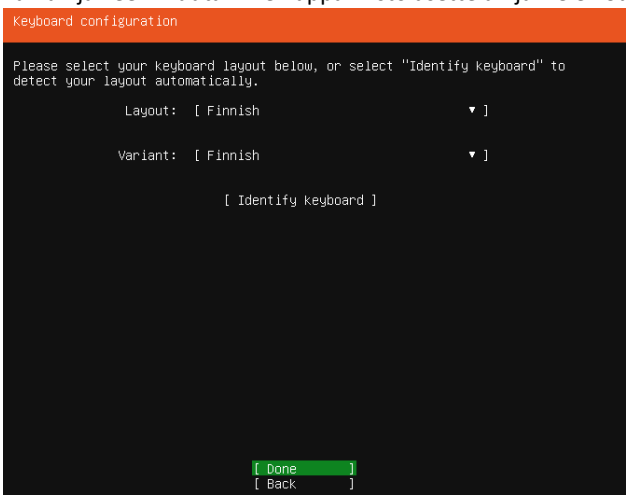
www-server01 asennus (Ubuntu Server 18.04)

Aluksi loimme virtuaalipalvelimen, kun Windows 2019 mutta .iso tiedostona käytämme Ubuntu Server 18.04 levykuvaa.

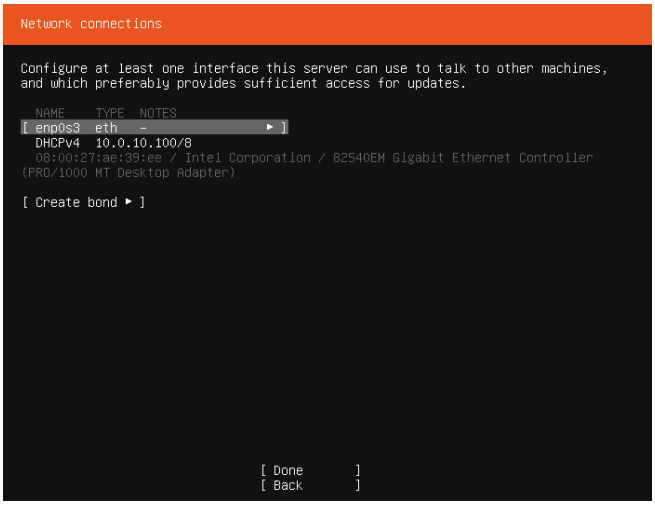
Aluksi valitsemme kielen, tässä tapauksessa English

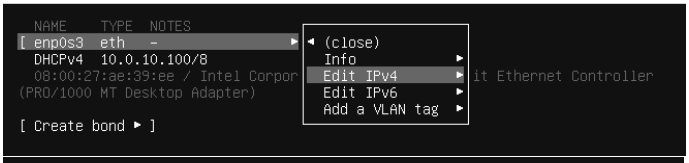


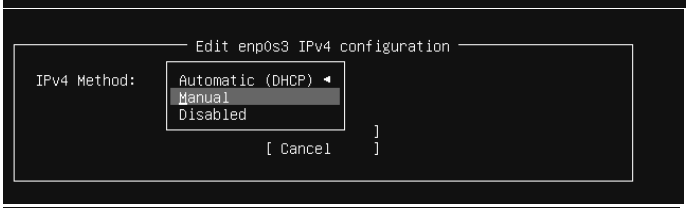
Tämän jälkeen muutamme näppäimistö asettelun ja kielen Suomeksi

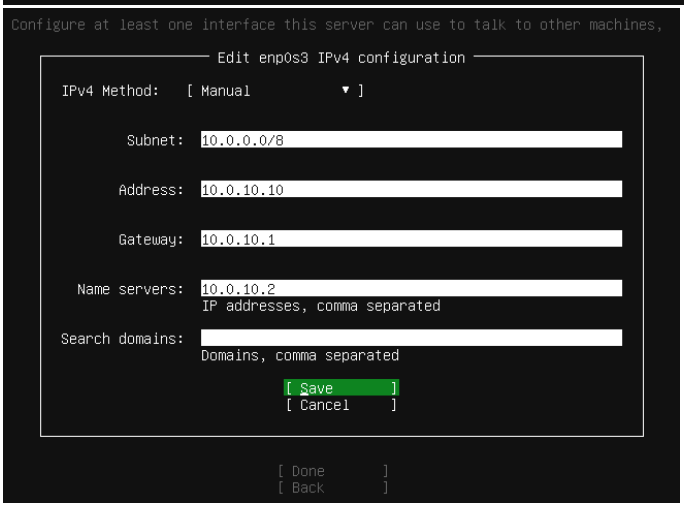


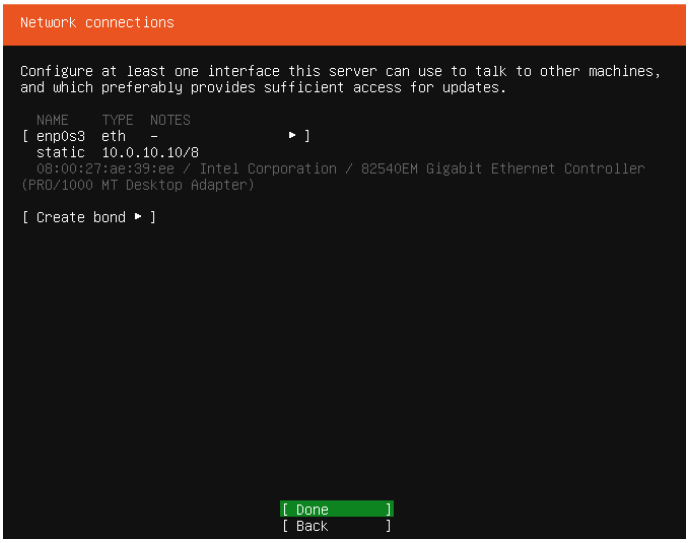
Nyt annamme verkkoasetukset, eli määrittämme staattisen IP-osoitteen



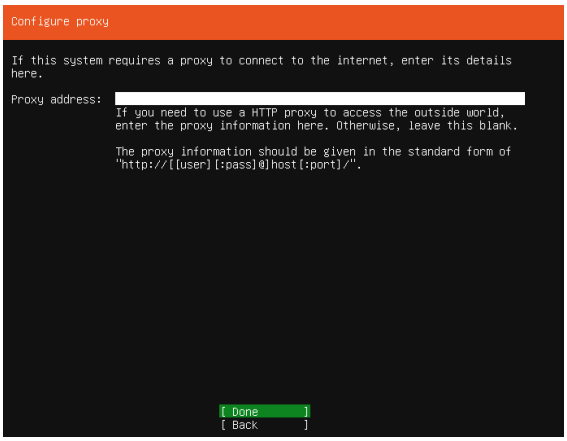

NAME TYPE NOTES
[enp0s3 eth -
DHCPv4 10.0.10.100/8
08:00:27:ae:39:ee / Intel Corpor
(PRO/1000 MT Desktop Adapter)
[Create bond ▸]
◂ (close)
Info ▸
Edit IPv4 ▸
Edit IPv6 ▸
Add a VLAN tag ▸
it Ethernet Controller


Edit enp0s3 IPv4 configuration
IPv4 Method:
Automatic (DHCP) ◂
Manual
Disabled
]
[Cancel]

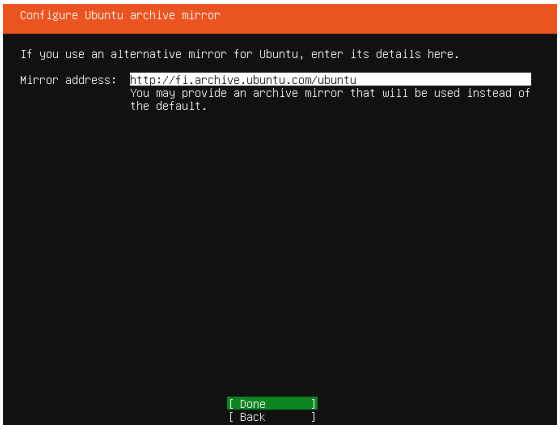

Configure at least one interface this server can use to talk to other machines,
Edit enp0s3 IPv4 configuration
IPv4 Method: [Manual ▾]
Subnet: 10.0.0.0/8
Address: 10.0.10.10
Gateway: 10.0.10.1
Name servers: 10.0.10.2
IP addresses, comma separated
Search domains:
Domains, comma separated
[Save]
[Cancel]
[Done]
[Back]


Network connections
Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.
NAME TYPE NOTES
[enp0s3 eth - ▸]
static 10.0.10.10/8
08:00:27:ae:39:ee / Intel Corporation / 82540EM Gigabit Ethernet Controller
(PRO/1000 MT Desktop Adapter)
[Create bond ▸]
[Done]
[Back]

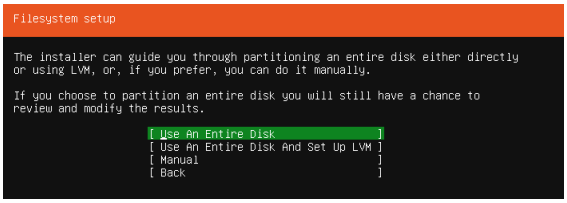
Tämän jälkeen meiltä kysytään välityspalvelin/Proxy tietoja, jätämme tässä tapauksessa sen tyhjäksi, kun sellaista ei meidän ympäristössämme ole.



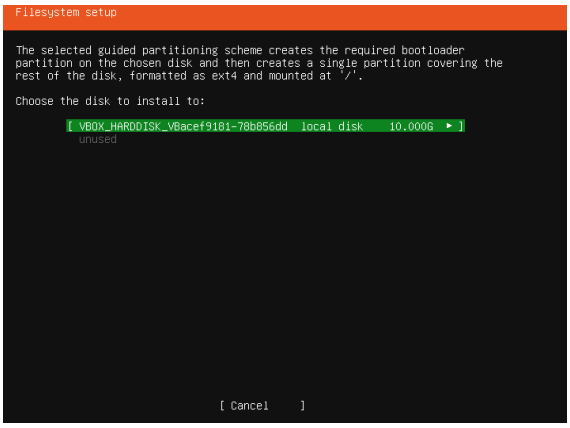
Nyt valitsemme palvelimen josta Ubuntu hakee asennus tai media tiedostoja. Tässä kannattaa valitse geologaatioksi lähin, eli meidän tapauksessamme Suomi / .fi



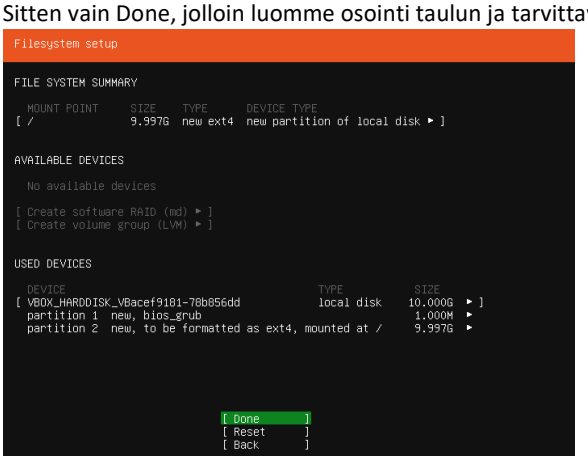
Nyt osiomme levyn, tässä tapauksessa voimme osioida koko levyn, kun levyllä ei ole ennestään mitään tietoa.



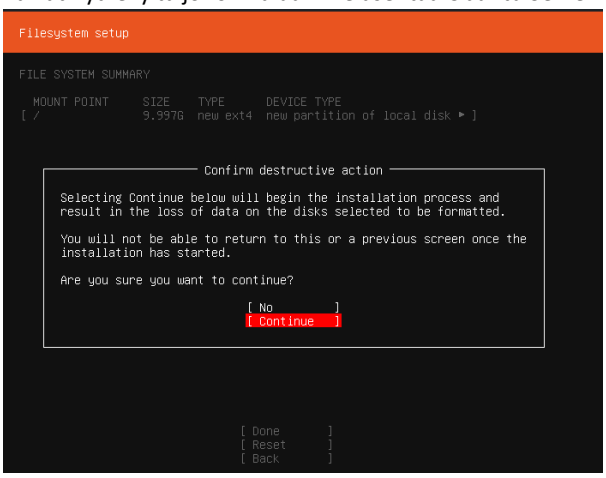
Valitsemme virtuaalisen levymme (10GB)



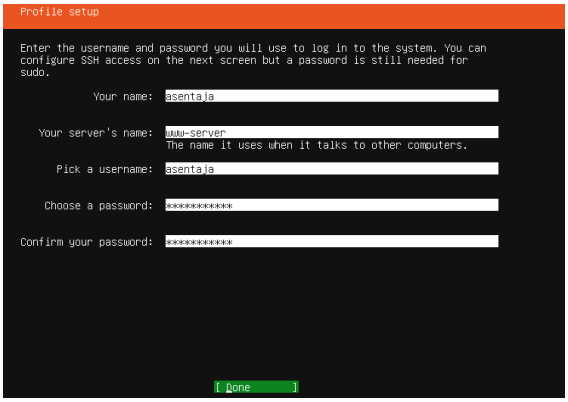
Sitten vain Done, jolloin luomme osointi taulun ja tarvittavat osiot levylle



Asennus vielä varmistaa, että olethan varma, kun tätä ei voi enää kumota ja olemassa olevat tiedot häviät nyt levyltä johon haluamme asentaa Ubuntu Serverin



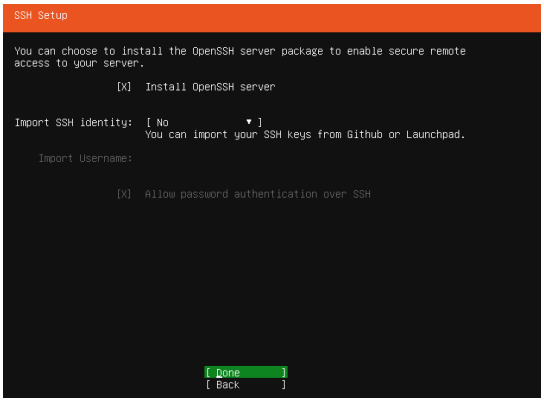
Tämän jälkeen luomme tilin, palvelimen nimen sekä salasanan palvelimelle. Done eteenpäin



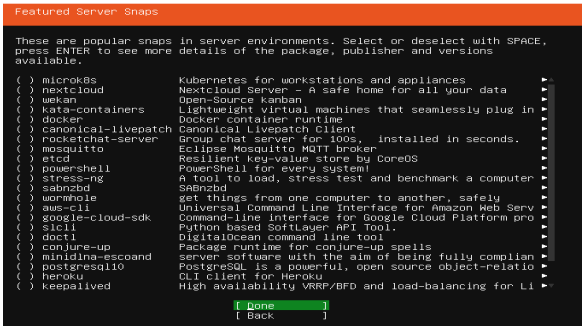
Tässä vaiheessa palvelin kysyy haluamme asentaa SSH palvelimen koneelle. Suosittelen sitä helpottamaksi etähallintaa.

Joten ruksaamme Install OpenSSH server ja emme tuo vanhaa SSH avainta, joten valitsemme No Import SSH identity kohtaan.

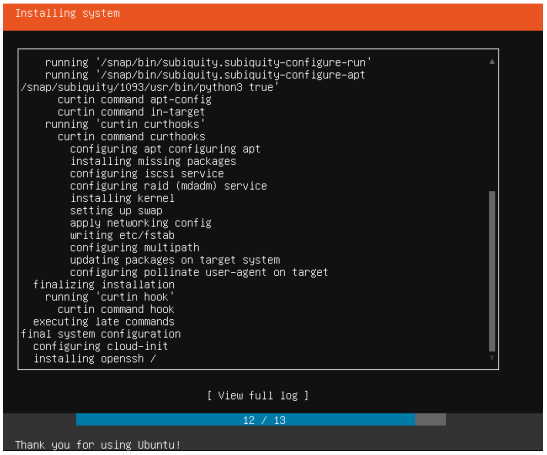
Done eteenpäin



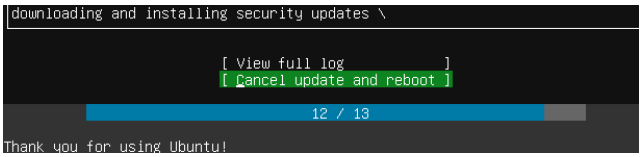
Voimme vielä asennuksen tässä välissä valita valinnaisia asennus paketteja, mutta meidän tapauksessamme emme niitä tarvitse nyt. Done eteenpäin.



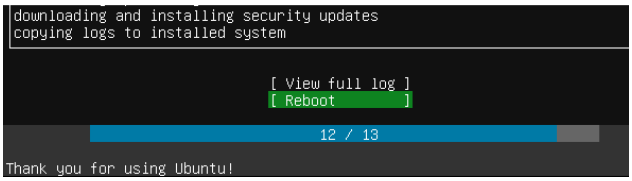
Nyt sitten vain katsomme, kun asennus suorittaa tehtävänsä loppuun



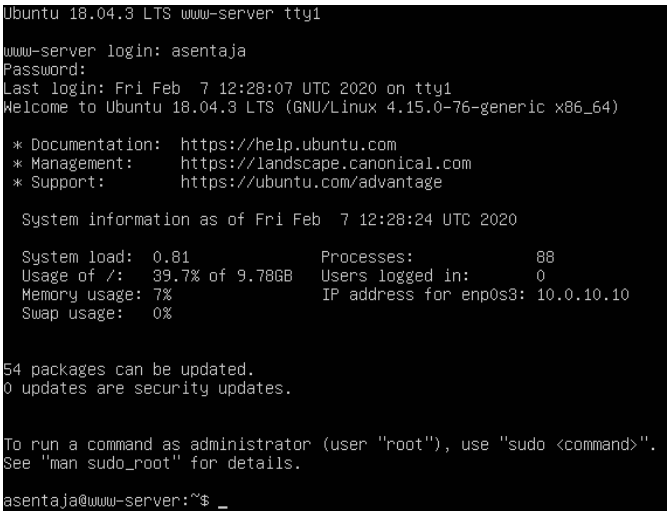
Asennuksen lopuksi palvelin myös päivittää itsensä uusimpiin saatavilla oleviin paketteihin, mikäli siis palvelimella on toimiva yhteys ulospäin / Internet



Lopuksi voimme käynnistää palvelimen uudelleen.



Käynnistyksen jälkeen voimme kirjautua palvelimelle luodulla tunnuksella



Seuraavaksi vielä tarkistamme onko tullut mitään päivityksiä Ubuntuun, ennen kuin alamme asentamaan WordPress ympäristöä.
Suoritamme sudo apt-get update ja sen jälkeen sudo-apt get upgrade komennot

```
asentaja@www-server:~$ sudo apt-get update
[sudo] password for asentaja:
Sorry, try again.
[sudo] password for asentaja:
Hit:1 http://fi.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://fi.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://fi.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://fi.archive.ubuntu.com/ubuntu bionic-security InRelease
Reading package lists... Done
asentaja@www-server:~$
```

```
asentaja@www-server:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following packages will be upgraded:
  apt apt-utils base-files bsdutils cloud-init dmeventd dmsetup dpkg fdisk grep initramfs-tools
  initramfs-tools-bin initramfs-tools-core landscape-common libapt-inst2.0 libapt-pkg5.0 libblkid1
  libdevmapper-event1.02.1 libdevmapper1.02.1 libfdisk1 libldap-2.4-2 libldap-common liblvm2app2.2
  liblvm2cmd2.02 libmount1 libprocps6 libpython3.6 libpython3.6-minimal libpython3.6-stdlib
  libsmartcols1 libuuid1 lvm2 mdadm mount netplan.io nplan open-vm-tools procps
  python3-distupgrade python3-gdbm python3-software-properties python3.6 python3.6-minimal snapd
  software-properties-common sosreport ubuntu-minimal ubuntu-release-upgrader-core ubuntu-server
  ubuntu-standard unattended-upgrades util-linux uuid-runtime xkb-data
54 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 29.4 MB of archives.
After this operation, 2,989 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.38) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for dbus (1.12.2-1ubuntu1.1) ...
Processing triggers for rsyslog (8.32.0-1ubuntu4) ...
Processing triggers for mime-support (3.60ubuntu1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for install-info (6.5.0.dfsg.1-2) ...
Processing triggers for plymouth-theme-ubuntu-text (0.9.3-1ubuntu7.18.04.2) ...
update-initramfs: deferring update (trigger activated)
Processing triggers for initramfs-tools (0.130ubuntu3.9) ...
update-initramfs: Generating /boot/initrd.img-4.15.0-76-generic
asentaja@www-server:~$
```

Ensimmäiseksi asennamme Apache www -palvelimen komennolla:
sudo apt-get install apache2

```
asentaja@www-server:~$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.2-0 ssl-cert
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.2-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,730 kB of archives.
After this operation, 6,982 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

```
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.38) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
asentaja@www-server:~$ _
```

Tämän jälkeen asennamme tietokanta sekä tietokanta hallinta sovelluksen WordPress sovellusta varten (tässä tapauksessa MariaDB):

apt-get install mariadb-server mariadb-client

```
asentaja@www-server:~$ sudo apt-get install mariadb-server mariadb-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  galera-3 libaio1 libcgi-fast-perl libcgi-pm-perl libconfig-inifiles-perl libdbd-mysql-perl
  libdbi-perl libencode-locale-perl libfcgi-perl libhtml-parser-perl libhtml-tagset-perl
  libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl libjemalloc1
  liblwp-mediatypes-perl libmysqlclient20 libterm-readkey-perl libtimedate-perl liburi-perl
  mariadb-client-10.1 mariadb-client-core-10.1 mariadb-common mariadb-server-10.1
  mariadb-server-core-10.1 mysql-common socat
Suggested packages:
  libclone-perl libmldbm-perl libnet-daemon-perl libsql-statement-perl libdata-dump-perl
  libipc-sharedcache-perl libwww-perl mailx mariadb-test tinyca
The following NEW packages will be installed:
  galera-3 libaio1 libcgi-fast-perl libcgi-pm-perl libconfig-inifiles-perl libdbd-mysql-perl
  libdbi-perl libencode-locale-perl libfcgi-perl libhtml-parser-perl libhtml-tagset-perl
  libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl libjemalloc1
  liblwp-mediatypes-perl libmysqlclient20 libterm-readkey-perl libtimedate-perl liburi-perl
  mariadb-client mariadb-client-10.1 mariadb-client-core-10.1 mariadb-common mariadb-server
  mariadb-server-10.1 mariadb-server-core-10.1 mysql-common socat
0 upgraded, 30 newly installed, 0 to remove and 0 not upgraded.
Need to get 24.1 MB of archives.
After this operation, 184 MB of additional disk space will be used.
Do you want to continue? [Y/n] _
Setting up mariadb-client-10.1 (1:10.1.44-0ubuntu0.18.04.1) ...
Setting up mariadb-client (1:10.1.44-0ubuntu0.18.04.1) ...
Setting up mariadb-server-10.1 (1:10.1.44-0ubuntu0.18.04.1) ...
Created symlink /etc/systemd/system/mysql.service → /lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/mysqld.service → /lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/multi-user.target.wants/mariadb.service → /lib/systemd/system/ma
riadb.service.
Setting up mariadb-server (1:10.1.44-0ubuntu0.18.04.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.38) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
asentaja@www-server:~$
```

Tämän jälkeen suoritamme hieman tietoturva asetuksia uudelle MariaDB tietokanta palvelimelle komennolla:
sudo mysql_secure_installation

```
asentaja@www-server:~$ sudo mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
asentaja@www-server:~$ _
```

Kun olemme suorittaneet hieman palvelin hardeningiä, asennamme PHP sovelluksia oheisella komennolla:
sudo apt-get install php php-mysql

```
asentaja@www-server:~$ sudo apt-get install php php-mysql
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libapache2-mod-php7.2 libsodium23 php-common php7.2 php7.2-cli php7.2-common php7.2-json
  php7.2-mysql php7.2-opcache php7.2-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php7.2 libsodium23 php php-common php-mysql php7.2 php7.2-cli php7.2-common
  php7.2-json php7.2-mysql php7.2-opcache php7.2-readline
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,129 kB of archives.
After this operation, 18.0 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

```
Creating config file /etc/php/7.2/apache2/php.ini with new version
Module mpm_event disabled.
Enabling module mpm_prefork.
apache2_switch_mpm Switch to prefork
apache2_invoke: Enable module php7.2
Setting up php-mysql (1:7.2+60ubuntu1) ...
Setting up php7.2 (7.2.24-0ubuntu0.18.04.2) ...
Setting up php (1:7.2+60ubuntu1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
asentaja@www-server:~$
```

Kun olemme asentaneet PHP sovellukset, luomme tietokannan WordPress asennusta varten.
Aloita antamalla komennon:
sudo mysql -u root -p

```
asentaja@www-server:~$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 47
Server version: 10.1.44-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> _
```

Sen jälkeen annamme oheiset komennot, joiden vaiheista löytyy seuraavat kuvan kaappaukset

Eli ensin luomme tietokannan, jonka jälkeen luomme käyttäjän ja sille salasanan (toki oikeassa ympäristössä hieman tietoturvallisempia salasana kuin password). Lopuksi annamme vielä äsken luodulle käyttäjälle oikeudet tälle luomaamme tietokannalle.

CREATE DATABASE wordpress_db;
CREATE USER 'wp_user'@'localhost' IDENTIFIED BY 'password';
GRANT ALL ON wordpress_db.* TO 'wp_user'@'localhost' IDENTIFIED BY 'password';
FLUSH PRIVILEGES;
Exit;

```
MariaDB [(none)]> CREATE DATABASE wordpress_db;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> CREATE USER 'wp_user@localhost' IDENTIFIED by 'password';
Query OK, 0 rows affected (0.00 sec)
```

```
MariaDB [(none)]> GRANT ALL ON worpress_db.* TO 'wp_user@localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> EXIT;
Bye
asentaja@www-server:~$ _
```

Tietokannan luonnin jälkeen käymme lataamassa ja asentamassa WordPress sovelluksen palvelimelle:
cd /tmp (vaihdamme kansion /tmp)
wget https://wordpress.org/latest.tar.gz (lataamme wget sovelluksella Wordpress palvelimelta uusimman sovelluksen)

```
asentaja@www-server:~$ cd /tmp
asentaja@www-server:/tmp$ wget https://wordpress.org/latest.tar.gz
--2020-02-08 13:15:05--  https://wordpress.org/latest.tar.gz
Resolving wordpress.org (wordpress.org)... 198.143.164.252
Connecting to wordpress.org (wordpress.org)|198.143.164.252|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12389281 (12M) [application/octet-stream]
Saving to: ‘latest.tar.gz’

latest.tar.gz           100%[===================================>]  11.81M  3.85MB/s    in 3.1s

2020-02-08 13:15:09 (3.85 MB/s) - ‘latest.tar.gz’ saved [12389281/12389281]

asentaja@www-server:/tmp$ _
```

Puramme paketin komennolla:
tar -xvf latest.tar.gz

```
wordpress/wp-admin/widgets.php
wordpress/wp-admin/setup-config.php
wordpress/wp-admin/install.php
wordpress/wp-admin/admin-header.php
wordpress/wp-admin/post-new.php
wordpress/wp-admin/themes.php
wordpress/wp-admin/options-reading.php
wordpress/wp-trackback.php
wordpress/wp-comments-post.php
asentaja@www-server:/tmp$
```

Tämän jälkeen kopioimme WordPress kansion uuteen paikkaan, annamme hieman oikeusmuutoksia kansioihin, sekä luomme uuden kansion wp-content kansioon ja sille myös hieman oikeusmuutoksia

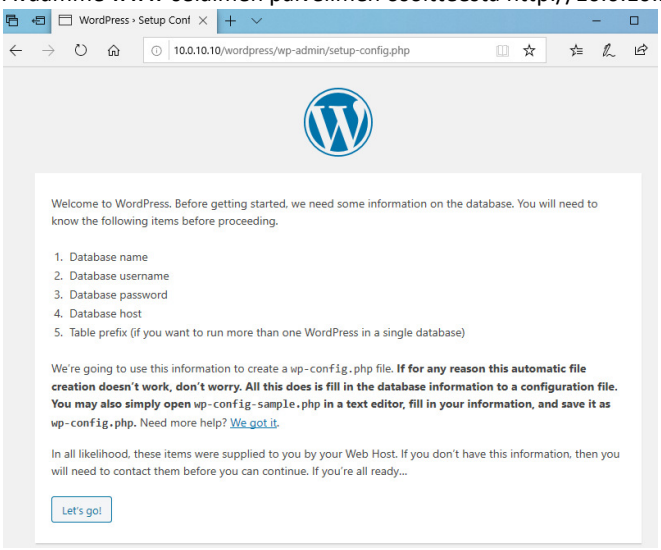
sudo cp -R wordpress /var/www/html/
sudo chown www-data:www-data /var/www/html/wordpress/
sudo chmod -R 755 /var/www/html/wordpress/
sudo mkdir /var/www/html/wordpress/wp-content/uploads
sudo chown -R www-data:www-data /var/www/html/wordpress/wp-content/uploads

```
asentaja@www-server:/tmp$ sudo cp -R wordpress /var/www/html/
asentaja@www-server:/tmp$
```

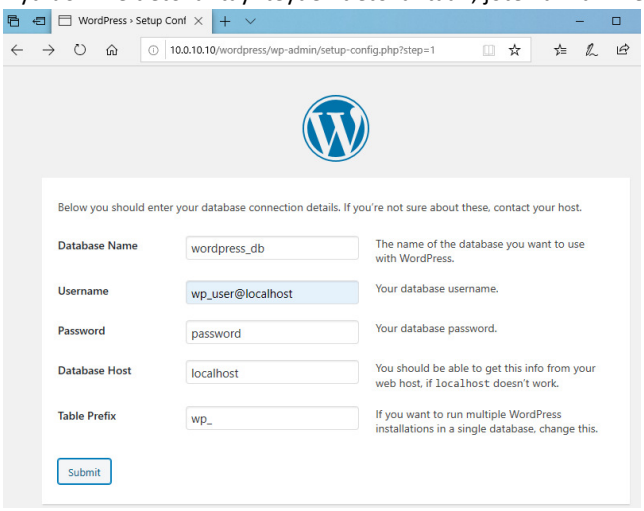
```
asentaja@www-server:/tmp$ sudo cp -R wordpress /var/www/html/
asentaja@www-server:/tmp$ sudo chown www-data:www-data /var/www/html/wordpress/
asentaja@www-server:/tmp$ sudo chmod -R 755 /var/www/html/wordpress/
asentaja@www-server:/tmp$ sudo mkdir /var/www/html/wordpress/wp-co
wp-comments-post.php  wp-config-sample.php  wp-content/
asentaja@www-server:/tmp$ sudo mkdir /var/www/html/wordpress/wp-content/uploads
asentaja@www-server:/tmp$ sudo chown -R www-data:wwww-data /var/www/html/wordpress/wp-content/upload
s/
chown: invalid group: ‘www-data:wwww-data’
asentaja@www-server:/tmp$ sudo chown -R www-data:www-data /var/www/html/wordpress/wp-content/uploads
/
asentaja@www-server:/tmp$
```

Tämän jälkeen voimme siirtyä itse WordPress sovelluksen asennukseen käyttöön.

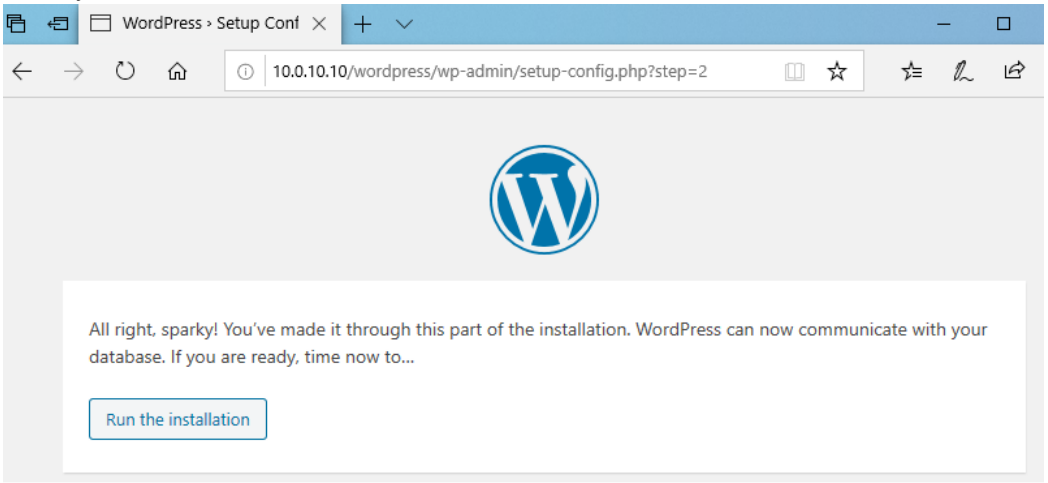
Avaamme www-selaimen palvelimen osoitteesta http://10.0.10.10/wordpress



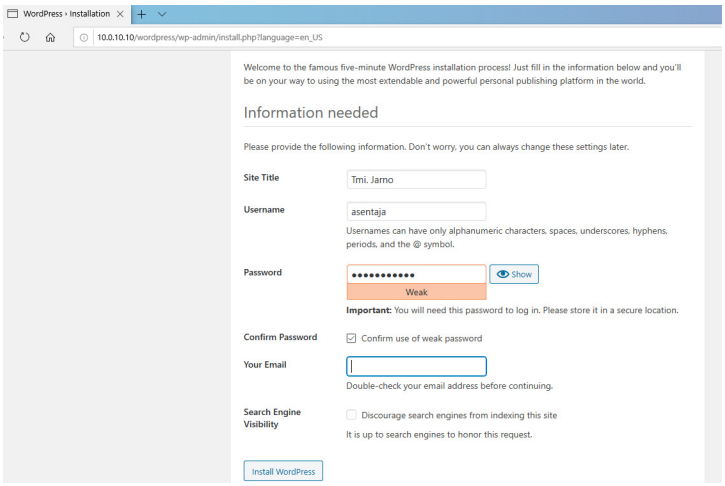
Nyt luomme tietokantayhteyden tietokantaan, joten annamme tarvittavat tiedot:



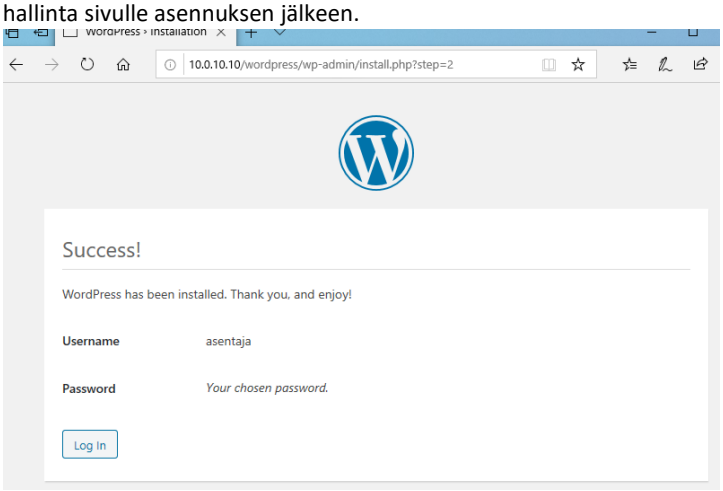
Tämän jälkeen itse asennus voi alkaa.



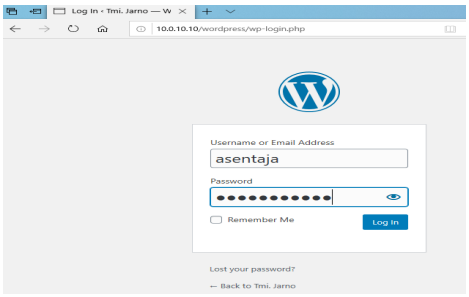
Tämän jälkeen annamme esitiedot sivustolle sekä luomme ylläpito tunnuksen. Ja kun taas on kyseessä testiasennus, niin voimme käyttää heikkoa salasanaa. Oikeassa asennuksessa pitää käyttää vahvaa salasanaa.



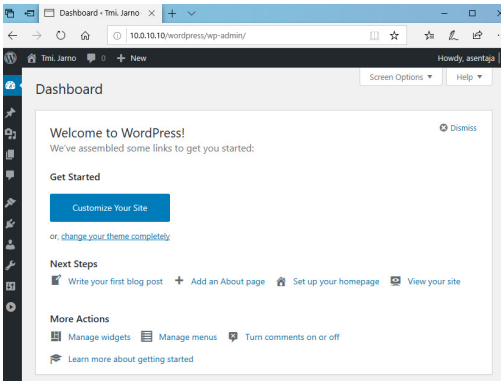
Ja lopuksi asennus kertoo, että kaikki on asennettu onnistuneesti ja voit kirjautua ensimmäistä kertaa hallinta sivulle asennuksen jälkeen.



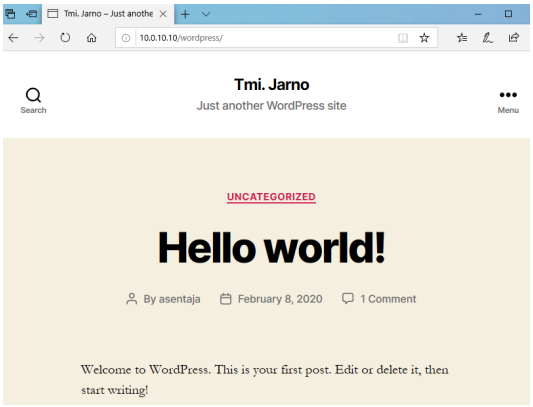
Tässä tapauksessa hallinta sivun osoite on http:/10.0.10.10/wordpress/wp-login.php johon sitten annamme asentaja tunnuksen ja oikean salasanan.



Kirjautumisen jälkeen olemme ylläpitosivustolla

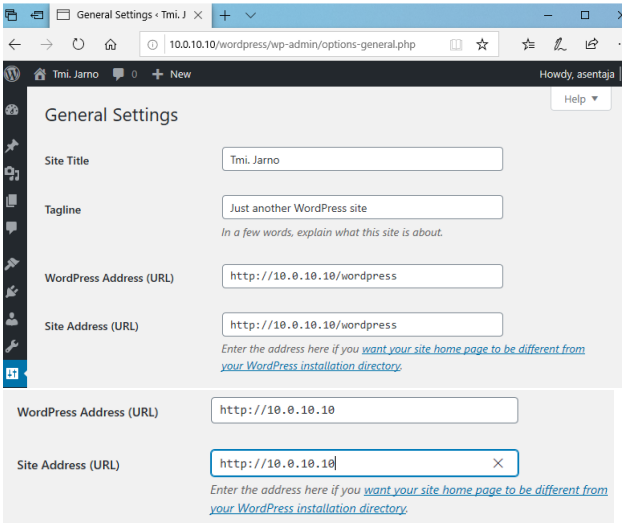


Ja voimme myös katsoa miltä meidän uuden ja hienot www -sivut näyttävät.



Nyt teemme vielä hieman muutoksia sivuston URL osoitteeseen, eli muutamme sivut toimimaan suoraan http://10.0.10.10/ (ja hieman myöhemmin myös suoraan www.jarno.local DNS nimellä.

Eli avaamme Settings sivun vasemmalta hallinta sivustosta ja muutamme WordPress Address sekä Site Address http://10.0.10.10



Nyt meidän pitää vielä tehdä muutoksia itse Apache www -palvelimen asetuksiin, jotta sivut toimivat oikein

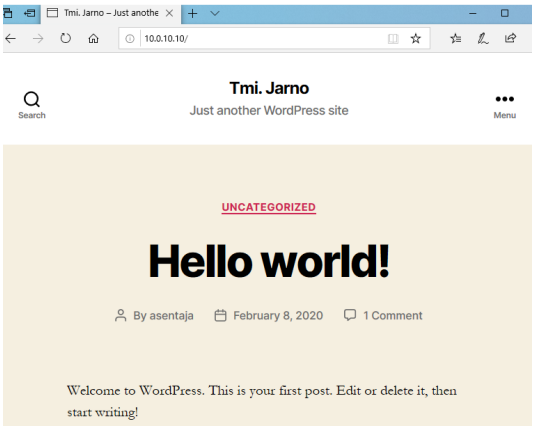
cd /etc/apache2/sites-available / menemme kansioon /etc/apache2/sites-available
sudo nano 000-default.conf / muokkaamme nano editorilla tiedostoa 000-default-conf
DocumentRoot /var/www/html/wordpress / muutamme riviä DocumentRoot
sudo service apache2 restart / käynnistämme www palvelimen uudelleen

```
asentaja@www-server:~$ cd /etc/apache2/sites-available/
asentaja@www-server:/etc/apache2/sites-available$ sudo nano 000-default.conf
```

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/wordpress
```

```
asentaja@www-server:/etc/apache2/sites-available$ sudo service apache2 restart
asentaja@www-server:/etc/apache2/sites-available$
```

Ja tämän jälkeen sivut toimivat suoraan http://10.0.10.10 ja hallinta sivusta http://10.0.10.10/wp-admin.php



Ubuntu palvelimen liittäminen Active Directoryyn

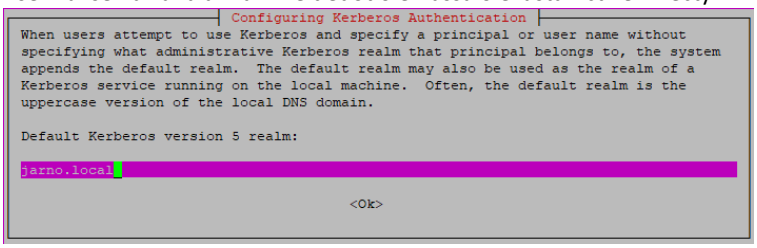
Tämän jälkeen liitämme vielä tämän palvelimen Windows toimialueelle hallintaa ja ylläpitoa varten. Voimme myös tämän jälkeen kirjautua palvelimelle Active Directory tunnuksilla, jotta meillä olisi keskitetty käyttäjähallinta (AD) eikä tarvitse erillisiä Ubuntu Server Linux tunnuksia ylläpitää.

Asennamme aluksi hieman paketteja Ubuntu palvelimelle:
sudo apt-get install realmd sssd sssd-tools samba krb5-user packagekit adcli ntp

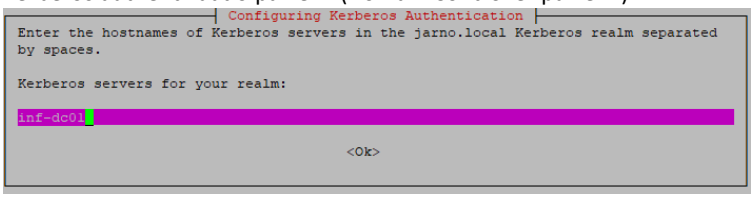
```
Last login: Sun Feb  9 08:05:52 2020
asentaja@www-server:~$ sudo apt-get install realmd sssd sssd-tools samba krb5-us
er packagekit adcli ntp
[sudo] password for asentaja:
```

```
0 upgraded, 96 newly installed, 0 to remove and 0 not upgraded.
Need to get 25.7 MB of archives.
After this operation, 121 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

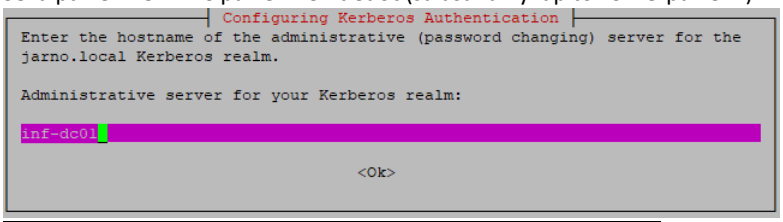
Asennuksen aikana annamme tiedot olemassa olevasta Active Directyn nimestä



Kerberos authentikaatio palvelin (Domain Controller palvelin)



Sekä palvelimen PDC palvelimen tiedot (salasanan ylläpito FSMO palvelin).




```
Processing triggers for ufw (0.36-0ubuntu0.18.04.1) ...
Processing triggers for mime-support (3.60ubuntu1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.38) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for dbus (1.12.2-1ubuntu1.1) ...
asentaja@www-server:~$
```

Asennuksen jälkeen muokkaamme vielä aikapalvelinta (NTP), kun Kerberos authetikaatio on aika sidonnainen palvelu ja kellon ajan pitää olla on synkronisaatiossa AD sekä Ubuntu palvelimen kanssa.

Oheisella komennolla muokkaamme tiedosta missä kerrottaan NTP -palvelin:
sudo nano /etc/ntp.conf

```
asentaja@www-server:~$ sudo nano /etc/ntp.conf
asentaja@www-server:~$
```

Lisäämme meidän toimialueemme DC -palvelimen

```
# Specify one or more NTP servers.
inf-dc01.jarno.local
```

Ja tämän jälkeen käynnistämme NTP -palvelun uudelleen:
Sudo systemctl restart ntp

```
asentaja@www-server:~$ sudo systemctl restart ntp
asentaja@www-server:~$
```

Nyt teemme hieman muutoksia asetus tiedostoihin, jossa kerromme mm. toimialueen nimen
Sudo nano /etc/realmd.conf

```
  GNU nano 2.9.3                        /etc/realmd.conf                        Modified

[users]
    default-home = /home/%U
    default-shell = /bin/bash
[active-directory]
    default-client = sssd
    os-name = Ubuntu Server
    os-version = 18.04
[service]
    automatic-install = no
[jarno.local]
    fully-qualified-names = no
    automatic-id-mapping = yes
    user-principal = yes
    manage-system = no
```

Sudo /etc/krb5.conf

```
  GNU nano 2.9.3                         /etc/krb5.conf                         Modified

[libdefaults]
        default_realm = JARNO.LOCAL
```

```
asentaja@www-server:~$ sudo nano /etc/krb5.conf
asentaja@www-server:~$
```

sudo systemctl restart ntp realmd

```
asentaja@www-server:~$ sudo systemctl restart ntp realmd
asentaja@www-server:~$
```

Nyt voimme tarkistaa, että authentikaatio toimii
sudo kinit administrator@JARNO.LOCAL

```
asentaja@www-server:~$ sudo systemctl restart ntp realmd
asentaja@www-server:~$ sudo kinit administrator@JARNO.LOCAL
kinit: Cannot find KDC for realm "JARNO.LOCAL" while getting initial credentials
```

Näyttää siltä, ettei DNS nimen selvitys toimi, eikä Ubuntu löydä AD palvelinta.
Joten teemme hieman muutoksia DNS asetuksiin:
Sudo nano /etc/resolv.conf

```
asentaja@www-server:~$ sudo nano /etc/resolv.conf
```

```
 GNU nano 2.9.3                          /etc/resolv.conf

# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 10.0.10.2
options edns0
```

Tämän jälkeen authetikaatio toimii Active Directory tunnuksella Ubuntu palvelimelta.

```
asentaja@www-server:~$ sudo kinit administrator@JARNO.LOCAL
Password for administrator@JARNO.LOCAL:
asentaja@www-server:~$
```

Tämän jälkeen liitämme meidän Ubuntu palvelimen Active Directory toimialueelle:
sudo realm --verbose join JARNO.LOCAL

```
asentaja@www-server:~$ sudo realm --verbose join JARNO.LOCAL
 * Resolving: _ldap._tcp.jarno.local
 * Performing LDAP DSE lookup on: 10.0.10.2
 * Successfully discovered: jarno.local
 * Successfully enrolled machine in realm
asentaja@www-server:~$
```

Lopuksi teemme vielä muutoksia, että myös Active Directory käyttäjille muodostuu kirjautumisen aikana oma kotikansion Ubuntu palvelimelle:

Sudo nano /etc/pam.d/common-session

Create new user home dir
session required pam_mkhomedir.so skel=/etc/skel/ umask=0077

```
 GNU nano 2.9.3                    /etc/pam.d/common-session                    Modified

#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
session [default=1]                     pam_permit.so
# here's the fallback if no module succeeds
session requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required                        pam_permit.so
# Create new user home dir
session required pam_mkhomedir.so skel=/etc/skel/ umask=0077
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional                        pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session optional                        pam_sss.so
session optional        pam_systemd.so
# end of pam-auth-update config
```

Sekä muutoksia ssd.conf tiedostoon:
access_provider = ad
Sudo /etc/sssd/sssd.conf

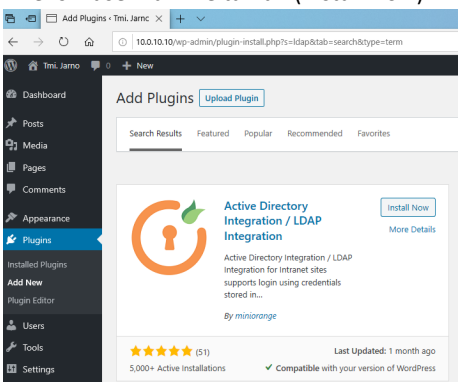
```
 GNU nano 2.9.3                  /etc/sssd/sssd.conf                  Modified

cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False
fallback_homedir = /home/%u
simple_allow_users = $
access_provider = ad
```

LDAP integraation tekeminen WordPress sovellukselle

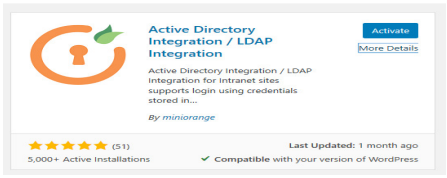
Ja kun olemme luoneet LDAP yhteyden Ubuntu palvelimen ja Active Directoryn kanssa, on myös luontevaa, että WordPress palveluun voi myös kirjautua Active Directory tunnuksella

Tähän käytämme oheista Active Directory Integraation lisäosaa WordPressissä

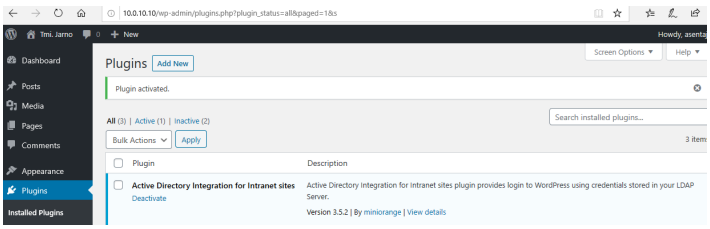
Eli ensin asennamme tämän (Install Now)



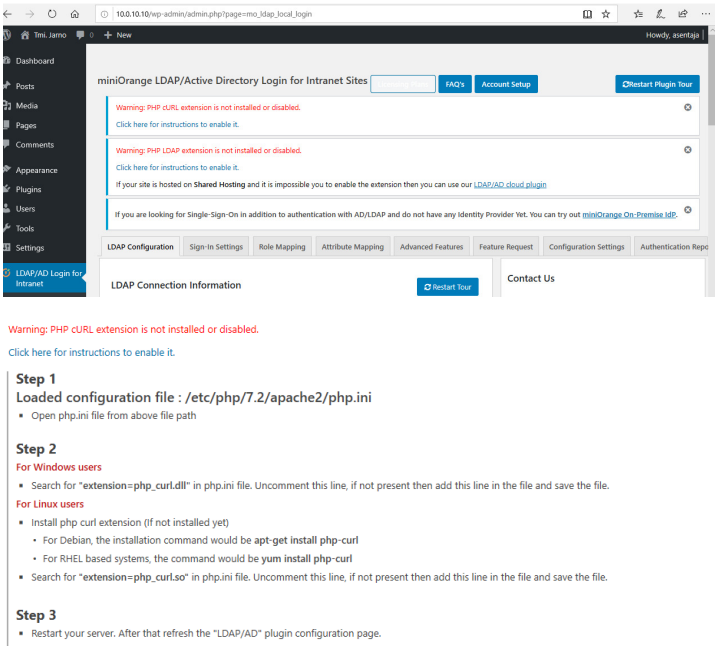
Jonka jälkeen vielä aktivoimme tämän lisäosan.



Nyt näimme, että tämä lisäosa on asentunut



Meidän pitää vielä hieman asentaa lisäosia (php-curl sekä php-ldap). Mutta tämä LDAP integraatio lisäosa kyllä kertoo miten tämä tehdään



Warning: PHP cURL extension is not installed or disabled.

Click here for instructions to enable it.

Step 1

Loaded configuration file : /etc/php/7.2/apache2/php.ini

- Open php.ini file from above file path

Step 2

For Windows users

- Search for "**extension=php_curl.dll**" in php.ini file. Uncomment this line, if not present then add this line in the file and save the file.

For Linux users

- Install php curl extension (If not installed yet)
  - For Debian, the installation command would be **apt-get install php-curl**
  - For RHEL based systems, the command would be **yum install php-curl**
- Search for "**extension=php_curl.so**" in php.ini file. Uncomment this line, if not present then add this line in the file and save the file.

Step 3

- Restart your server. After that refresh the "LDAP/AD" plugin configuration page.

Eli ensin asennamme php-curl osan:

```
asentaja@www-server:~$ sudo apt-get install php-curl
[sudo] password for asentaja:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  php7.2-curl
The following NEW packages will be installed:
  php-curl php7.2-curl
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 30.7 kB of archives.
After this operation, 130 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
Creating config file /etc/php/7.2/mods-available/curl.ini with new version
Setting up php-curl (1:7.2+60ubuntu1) ...
Processing triggers for libapache2-mod-php7.2 (7.2.24-0ubuntu0.18.04.2) ...
asentaja@www-server:~$ _
```

Ja asennuksen jälkeen lisäämme /etc/php/7.2/apache
extension=php_curl.so

```
 GNU nano 2.9.3                    /etc/php/7.2/apache2/php.ini                         Modified

;extension=odbc
;extension=openssl
;extension=pdo_firebird
;extension=pdo_mysql
;extension=pdo_oci
;extension=pdo_odbc
;extension=pdo_pgsql
;extension=pdo_sqlite
;extension=pgsql
;extension=shmop

extensionn=php_curl.so_
```

Sudo apt-get install php-ldap

```
asentaja@www-server:~$ sudo apt-get install php-ldap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  php7.2-ldap
The following NEW packages will be installed:
  php-ldap php7.2-ldap
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 25.6 kB of archives.
After this operation, 114 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

```
Setting up php7.2-ldap (7.2.24-0ubuntu0.18.04.2) ...

Creating config file /etc/php/7.2/mods-available/ldap.ini with new version
Setting up php-ldap (1:7.2+60ubuntu1) ...
Processing triggers for libapache2-mod-php7.2 (7.2.24-0ubuntu0.18.04.2) ...
asentaja@www-server:~$
```

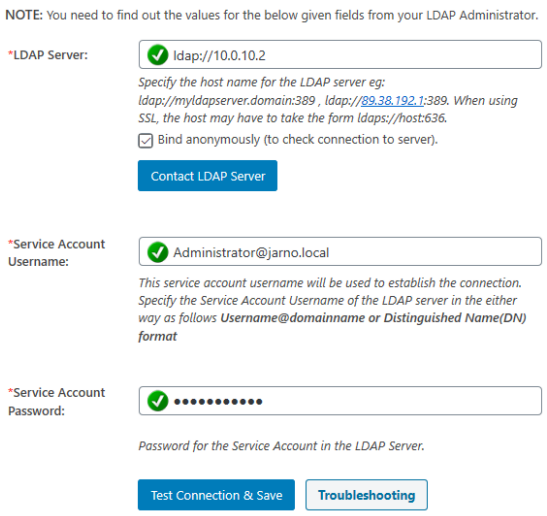
Sudo nano /etc/php/7.2/apache2/php.ini

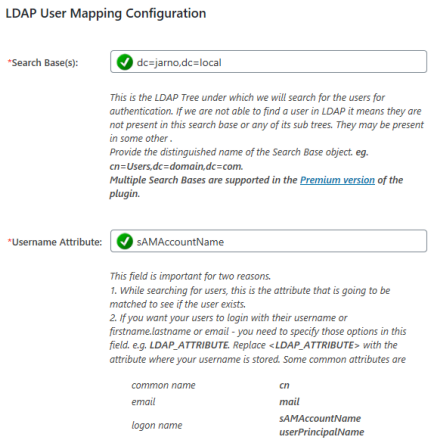
```
asentaja@www-server:~$ sudo nano /etc/php/7.2/apache2/php.ini _
```

extension=php_ldap.so

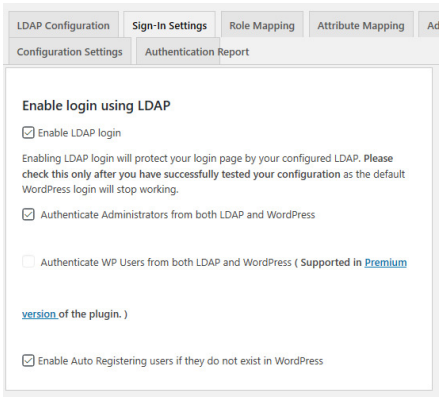
```
 GNU nano 2.9.3                    /etc/php/7.2/apache2/php.ini                         Modifie

;extension=mysqli
;extension=oci8_12c  ; Use with Oracle Database 12c Instant Client
;extension=odbc
;extension=openssl
;extension=pdo_firebird
;extension=pdo_mysql
;extension=pdo_oci
;extension=pdo_odbc
;extension=pdo_pgsql
;extension=pdo_sqlite
;extension=pgsql
;extension=shmop

extension=php_curl.so
extension=php_ldap.so
```

Näiden muutosten jälkeen voimme konfiguroida tämän LDAP liitännäisen kuntoon:

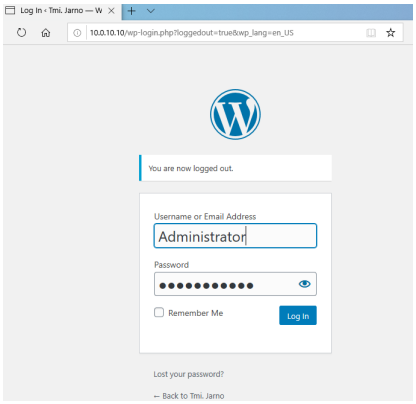




Ja jotta voimme kirjautua AD/LDAP tunnuksilla, niin meidän pitää vielä aktivoida Sing-In Settings välilehdeltä Enable LDAP login



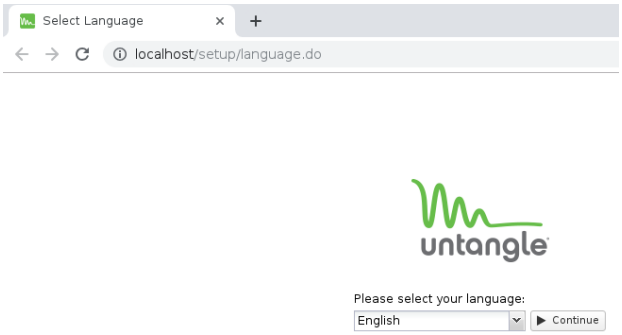
Ja nyt voimme siis kirjautua myös Active Directory tunnuksella WordPress hallintasivulle:



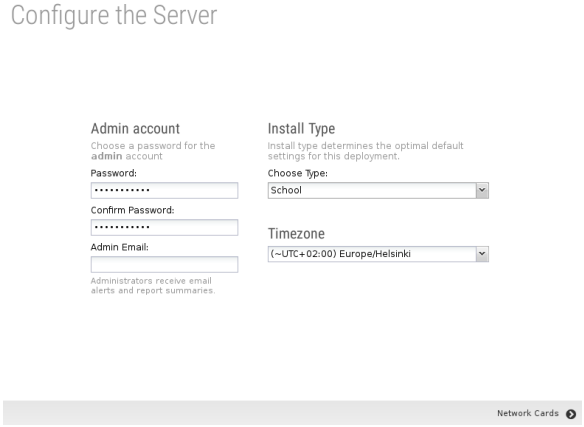
Untangle palomuurin asennus

Tuomme Virtualbox ympäristöön valmiiksi luodun Untangle virtuaalikone appliancen ja käynnistämme sen. Tämän jälkeen meille ilmestyy hetken päästä oheiset asetus ikkunat

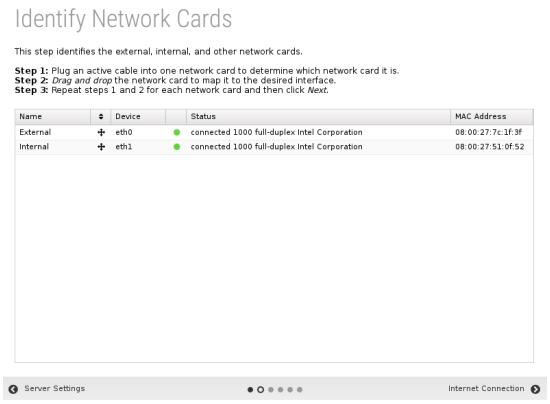
Valitsemme asennus kielen, menemme oletuksella eli English



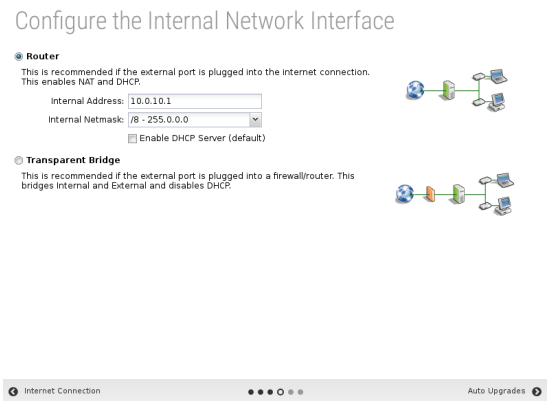
Nyt luomme pääkäyttäjän salasanan, sekä annamme hieman tietoja kuten asennus tyypistä sekä aikavyöhykkeestä:



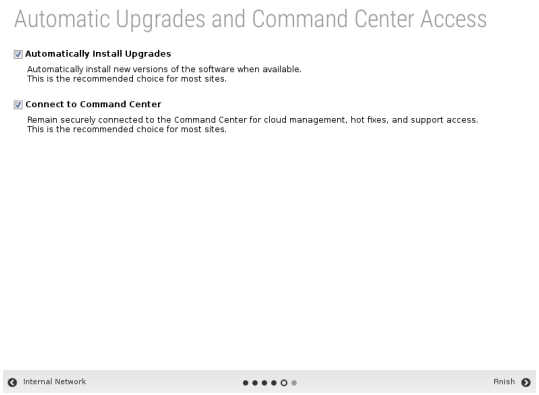
Tämän jälkeen valikoimme verkkokortit, eli kumpi on ns. WAN(Internet) puolella ja kumpi lähiverkon (LAN) puolella



Nyt määrittelemme verkkoasetukset lähiverkon puolelle ja otamme pois DHCP palvelun, kun meillä on lähiverkossa jo oma Windows Server 2019 Core DHCP palvelin



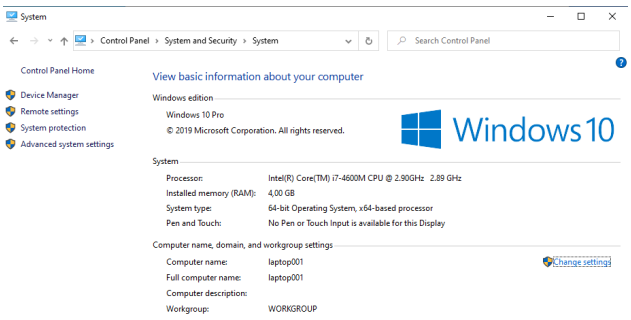
Voimme valita tässä, että automaattiset päivitykset asennettaan automaattisesti, suositeltu.



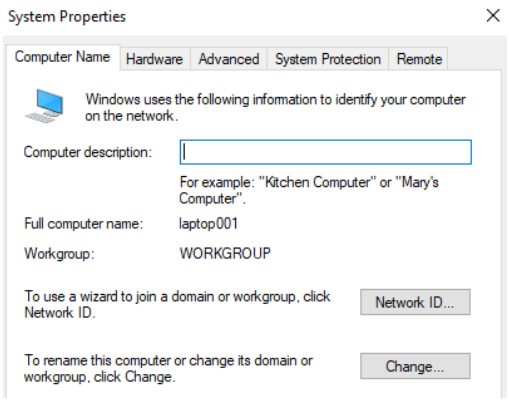
Ja tämän jälkeen asennus on tehty ja voimme käynnistää hallinta sovelluksen.

Windows toimialuepalvelujen toiminnan tarkastus

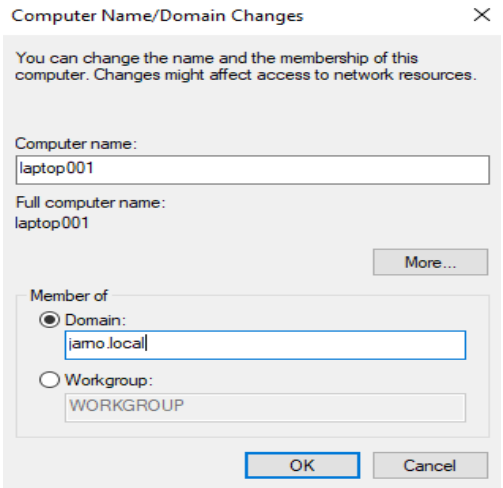
Liitämme ensin työaseman toimialueelle käyttäen Control Panel sovellusta, jos menemme System and Security -> System -> Change Settings



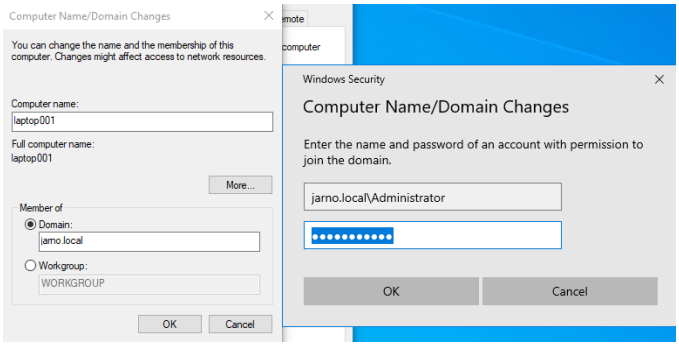
Valitsemme Change



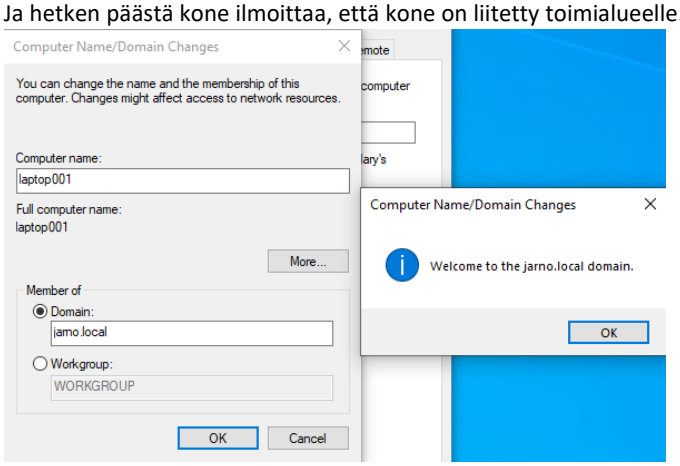
Ja nyt annamme Domain kohtaan toimialueen nimen, eli jarno.local



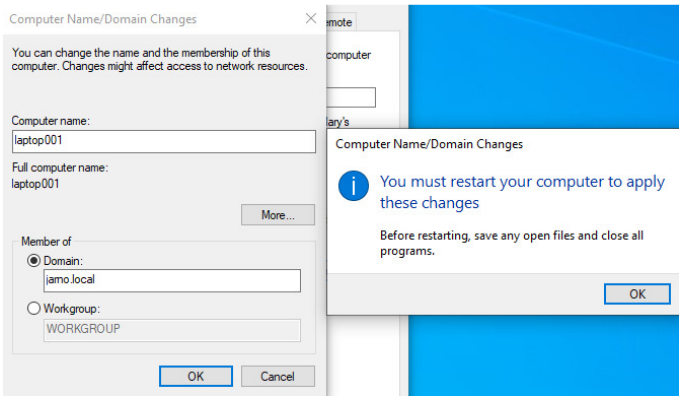
Annamme Administrator tason tunnuksen tiedot



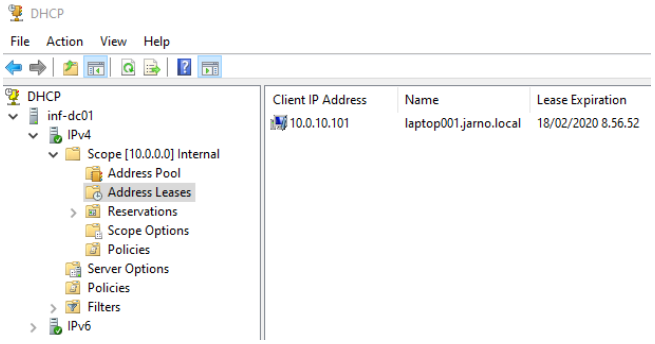
Ja hetken päästä kone ilmoittaa, että kone on liitetty toimialueelle.



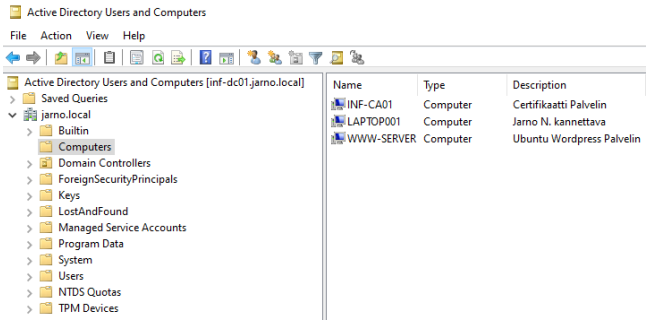
Lopuksi pitää vielä kone käynnistää uudelleen.



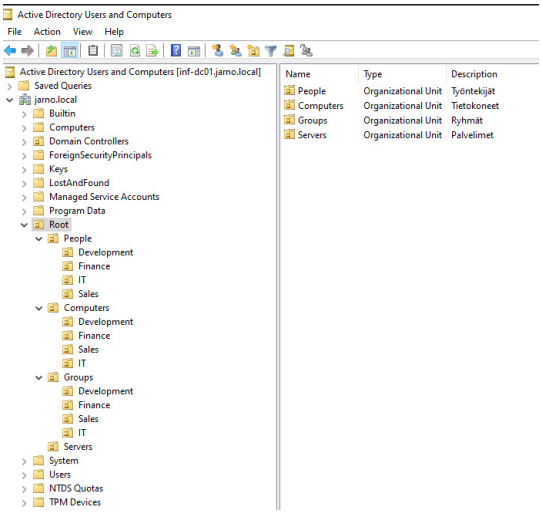
Tarkistamme että DHCP palvelin toimii, eli kuten näemme, palvelin on jakanut IP -osoitteen tälle meidän juuri toimialueelle liitetylle työasemalle



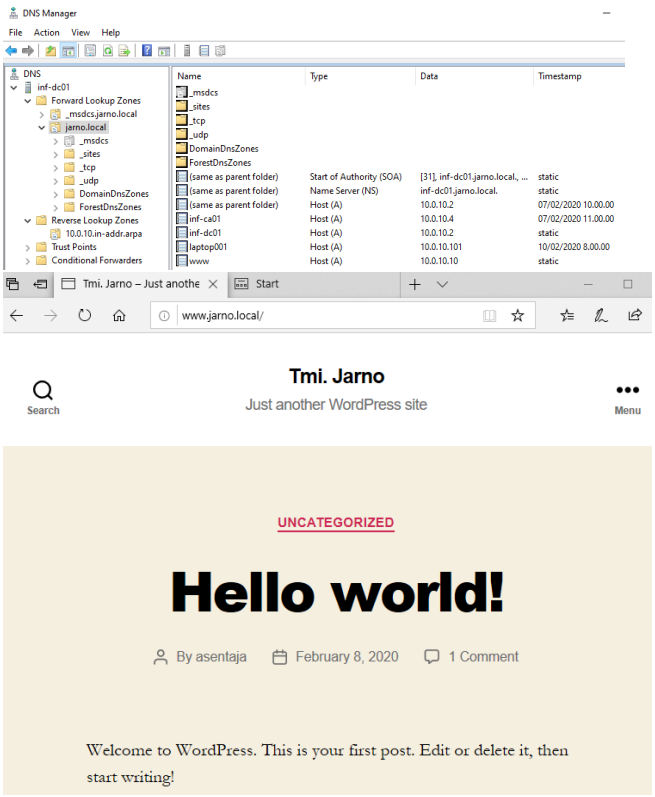
Myöskin palvelimia ja työasemia on ilmestynyt Active Directoryn Computers Containeriin



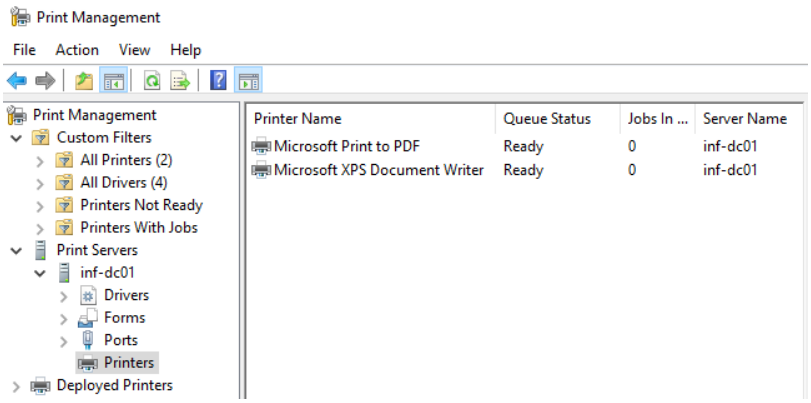
Olen luonut Active Directoryyn oheisen hierarkian työntekijöitä, tietokoneita, ryhmiä ja palvelimia varten helpottaakseni ylläpitoa.



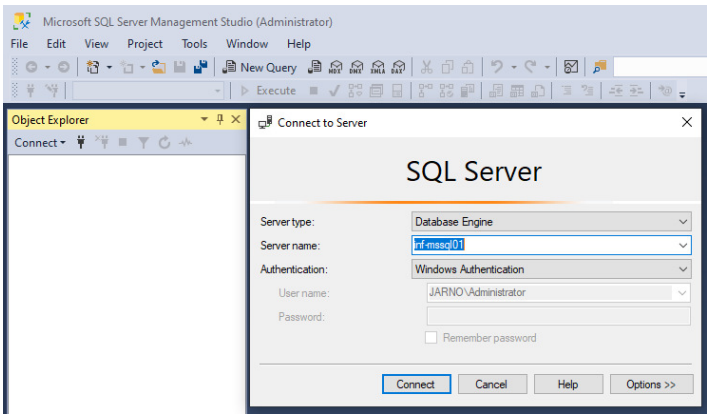
Ja myöskin DNS palvelu toimii, kun sinne on rekisteröitynyt tietotueita.
Luomme myös uuden A -record tyyppisen tietueen meidän www -palvelinta varten, jotta voimme myös päästä DNS nimellä kirjautua (www.jarno.local)



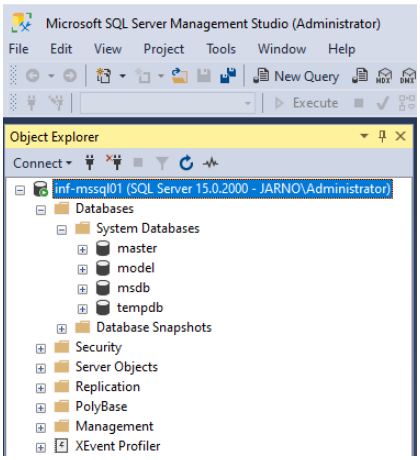
Ohessa myös tulostuspalvelu toiminnassa, tosin ei ole yhtään jaettua tulostinta.



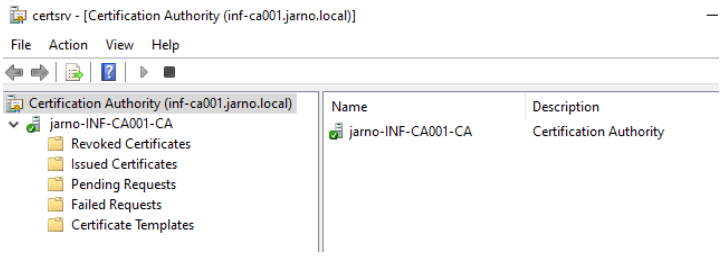
Tarkistamme SQL Serverin toiminnan, asentamalla ensin Microsoft SQL Server Management Studio ja sen jälkeen kirjautumalla toimialueen Administrator käyttäjällä tietokanta moottoriin



Ja kun nyt olemme kirjautuneena tietokantamoottoriin



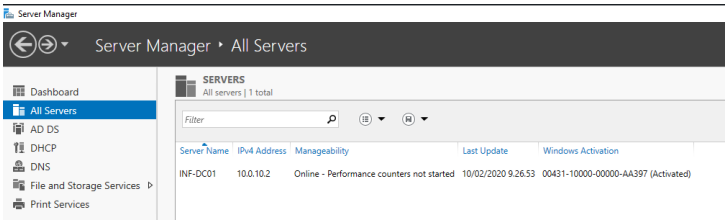
Tarkistamme Certificate Authorityn toiminnan, näyttää toimivan



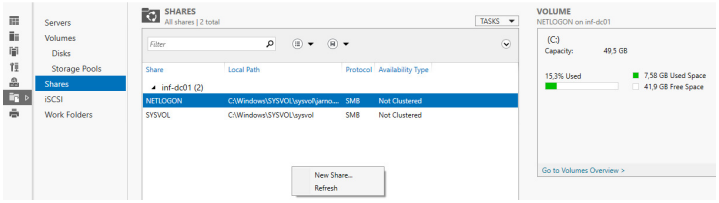
Verkkolevyjen konfigurointi

Seuraavaksi luomme jaettuja verkkolevyjä toimialueelle. Luomme kansion Work, jonne tulee tiimien omat verkkolevyt sekä Home jonne tulevat käyttäjien omat kotikansiot.

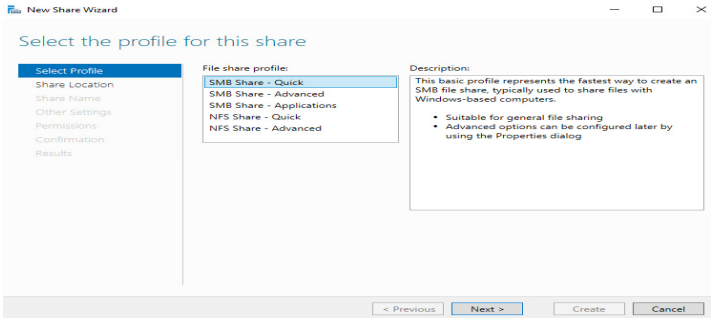
Käynnistämme Server Manager sovelluksen



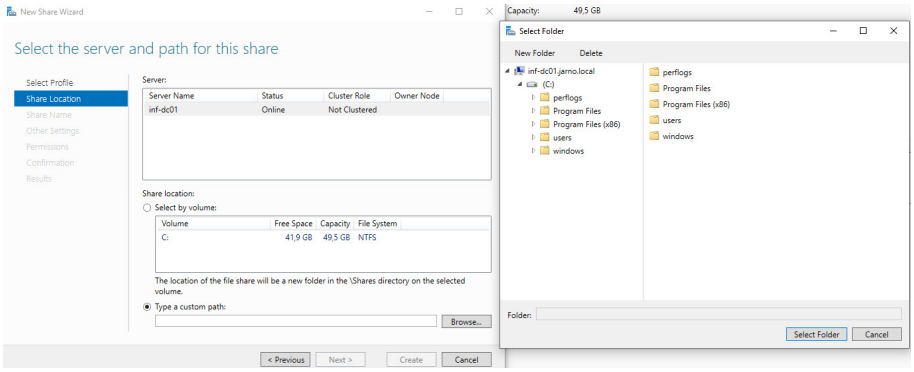
Sieltä File and Storage Services -> Shares -> New Share



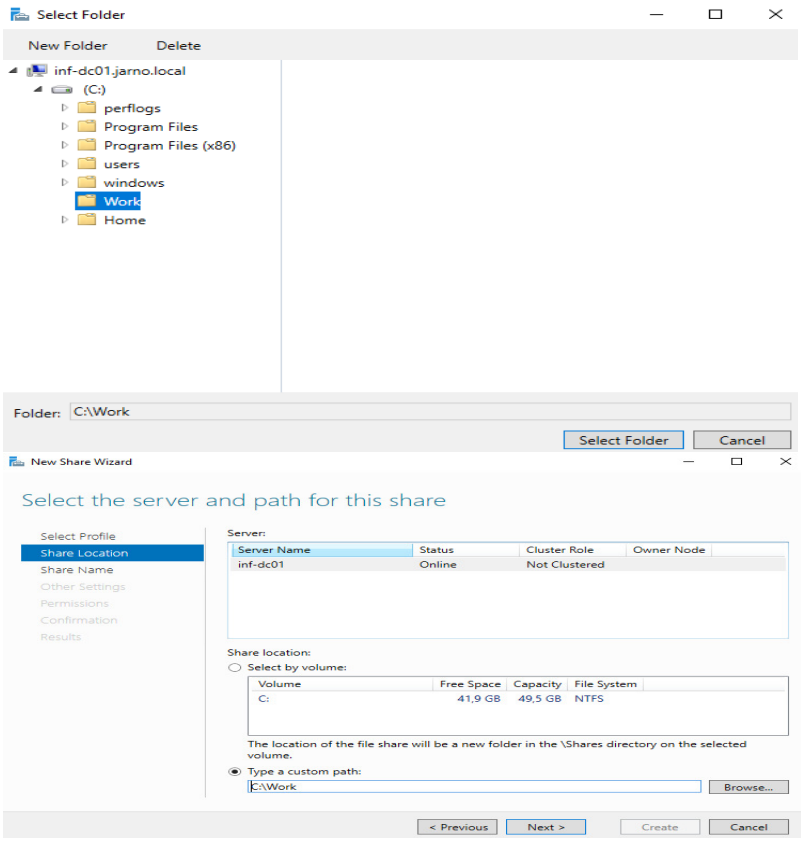
Valitsemme SMB Share – Quick ja sitten Next



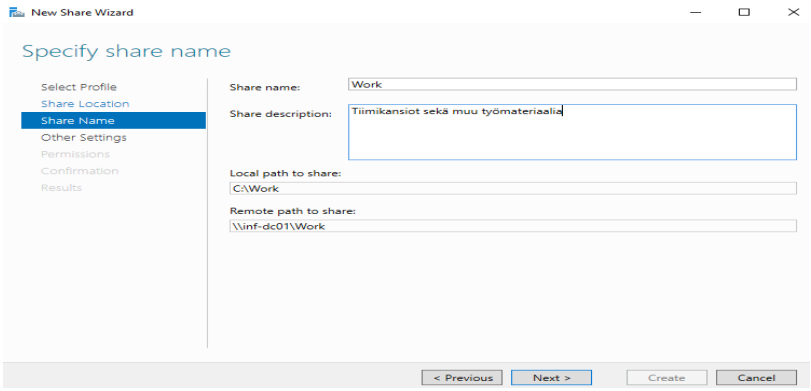
Nyt valitsemme Type a custom Path / ja sitten luomme juurikansioon Work sekä Home



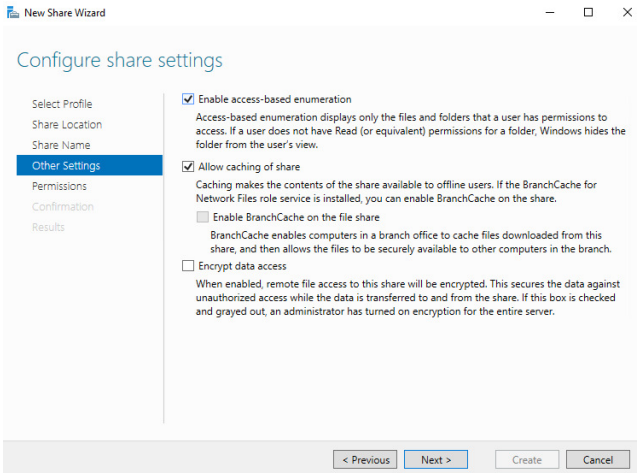
Valitsemme Work kansion sekä Select Folder, jotta pääsemme eteenpäin



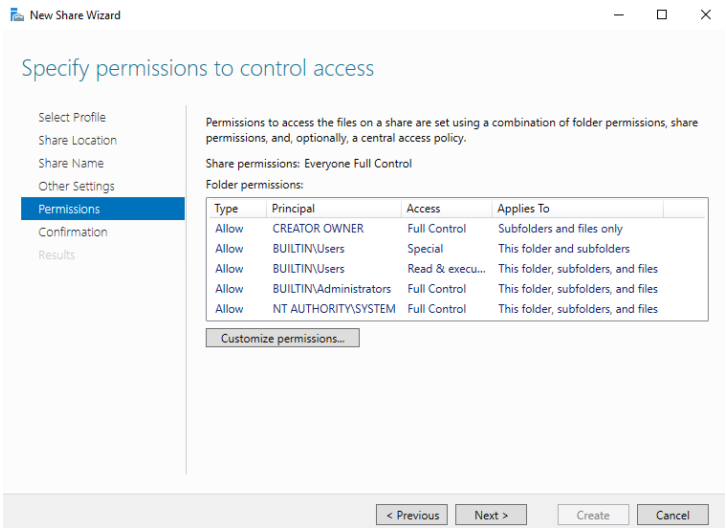
Tässä voimme vielä antaa kuvauksen jaolle / Share description



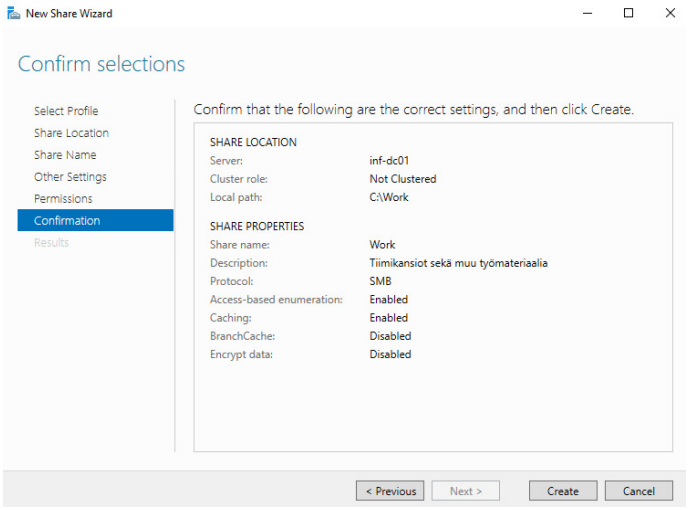
Nyt voimme vielä valita lisäasetuksia, oletuksena on päällä Allow caching of share ja suosittelen myös lisäämään Enable access-based enumeration, eli tämä tarkistaa, jos käyttäjä ketä yrittää listata kansiosta jaossa ja ei ole luku oikeuttaa kansioon, niin se piilottaa sen listauksesta.
Eli tämä näyttää vain ne kansiot johon käyttäjällä on pääsy.



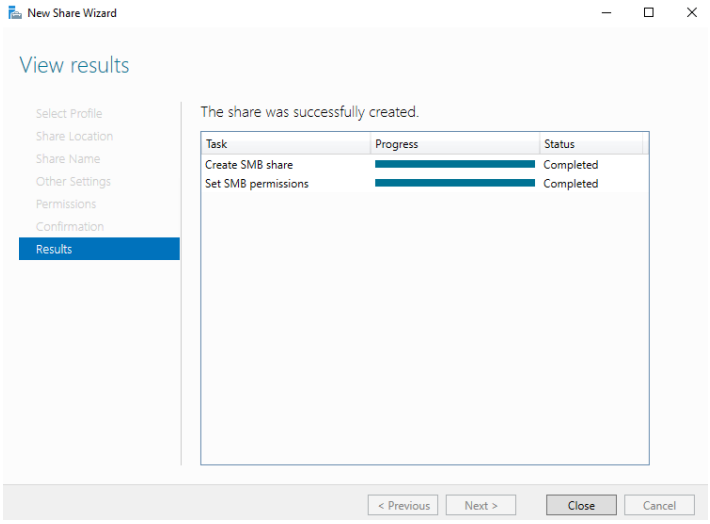
Tämän jälkeen voimme vielä hallinnoida NTFS oikeuksia, mutta näitä voimme vielä säätää tämänkin jälkeen, joten menemme oletuksilla Next eteenpäin



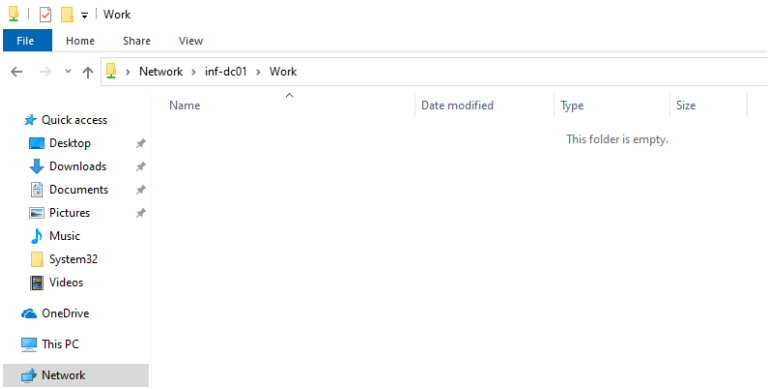
Lopuksi saamme vielä varmistus ikkunan muutoksista jota olemme tekemässä, Create luodaksemme jaon.



Ja onnistuneen luonnin jälkeen saamme oheisen ikkunan, Close

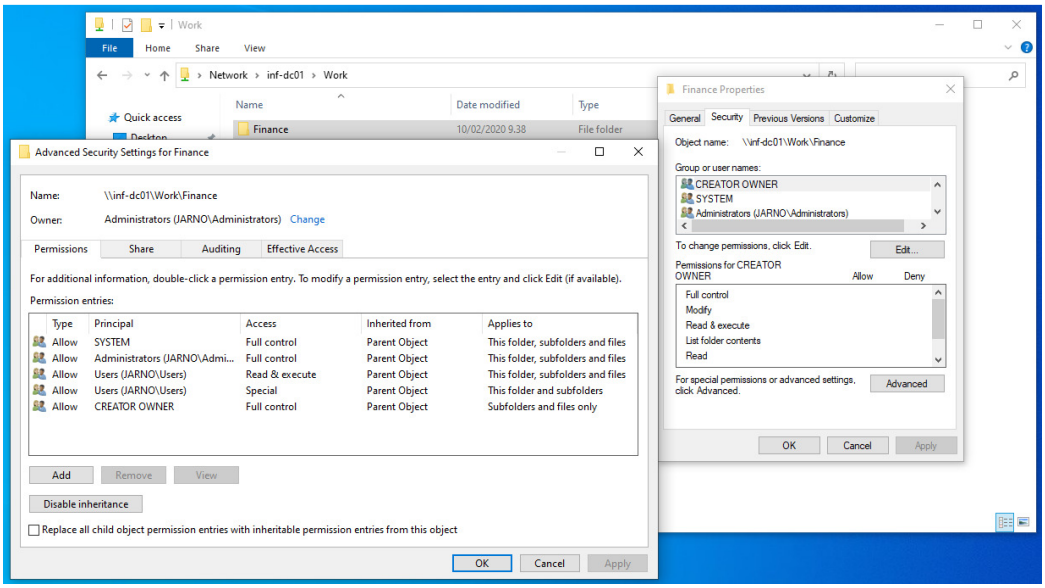


Ja nyt voimme avata uuden jaon osoitteesta \\inf-dc01\Work

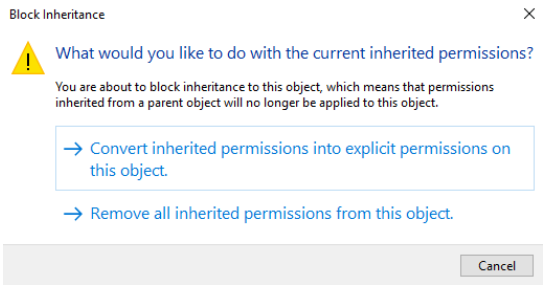


Nyt teemme hieman oikeusmuutoksia / NTFS Security tähän Work kansioon. Olemme luoneet sinne Finance nimesin kansion, jonne haluamme sallia vain pääsyn ALL-Finance Active Directory Security ryhmän jäsenille. Oikeuksia tulee oikea oppisesti jakaa vain ryhmille, ei suoraan käyttäjille, jotta hallinta olisi helpompaa ryhmien kautta.
Eli Finance kansion kohdalta hiiren oikea -> Properties -> Security -> Advanced -> Disable inheritence.

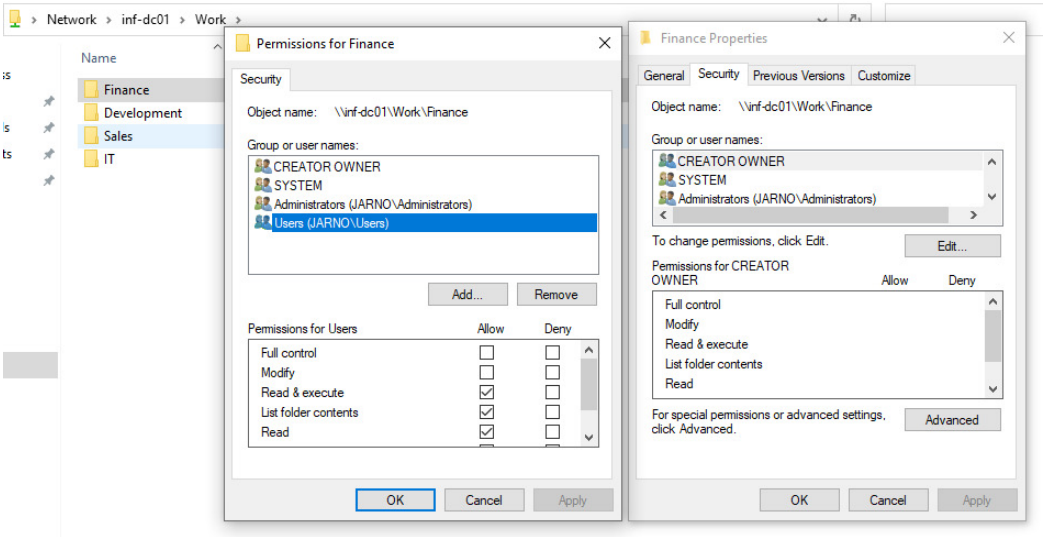
Tämä siksi, että voimme poistaa kansioon periytyneet oikeudet ylätasolta, eli c:\shares kansiosta ja sen jälkeen voimme vasta tehdä NTFS oikeus muutoksia tähän kansioon.

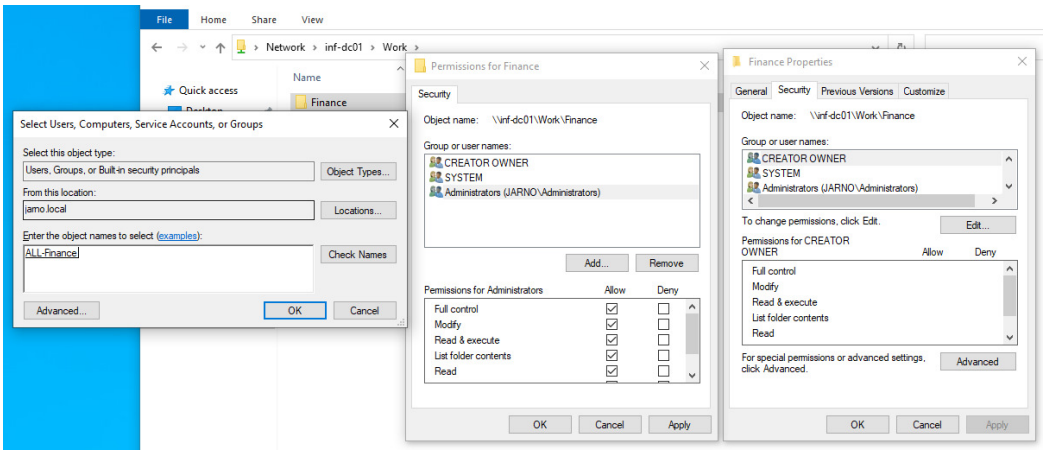


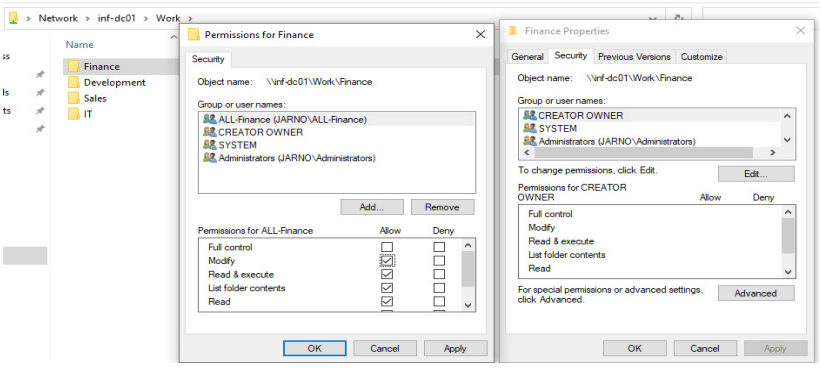
Tähän vastataan Convert inherited permisssions into explicit permission on this object, eli säilytetään olemassa olevat oikeudet



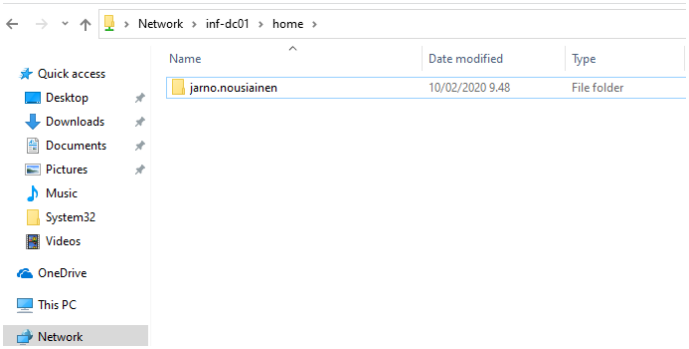
Tämän jälkeen voimme tehdä muutoksia tämän kansion NTFS oikeuksien määrittelyyn. Eli valitsemme Edit ja poistamme Users (Jarno\Users) ja sitten lisäämme ALL-Finance Active Directory ryhmän ja annamme tälle ryhmälle Modify oikeudet.
Full Control tason oikeutta en suosittele antamaan, koska sillä voivat tämä All-Finance ryhmän jäsenet tehdä hallinnasta haastavaa ylläpitäjän kannalta 😊



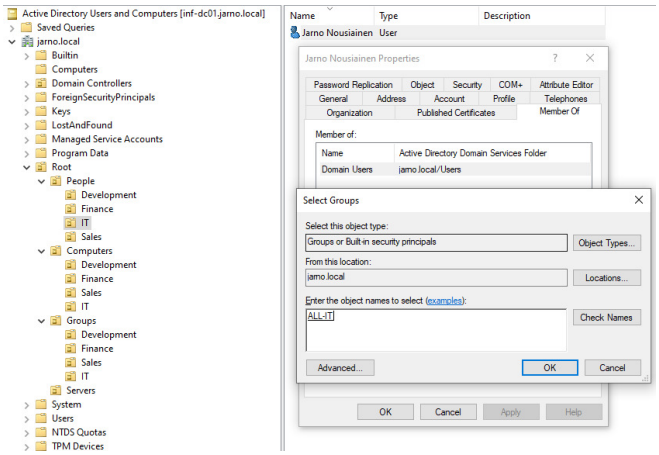




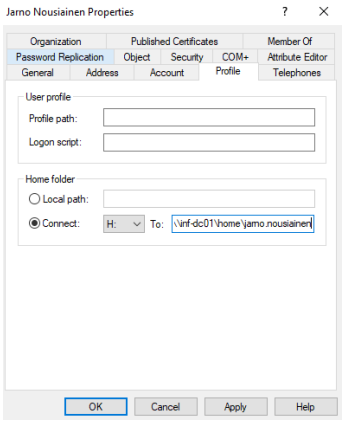
Kun olemme muuttaneet Finance kansion oikeuksia, voimme luoda Active Directory käyttäjälle jarno.nousiainen oman kotikansion c:\Shares\home nimellä jarno.nousiainen.
Tämän jälkeen poistamme siltäkin myös periytyvät oikeudet, jonka jälkeen poistamme Users ryhmältä oikeudet tähän kansioon jarno.nousiainen sekä lopuksi lisäämme Active Directory käyttäjälle jarno.nousiainen Modify oikeudet tähän jarno.nousiainen kansioon.



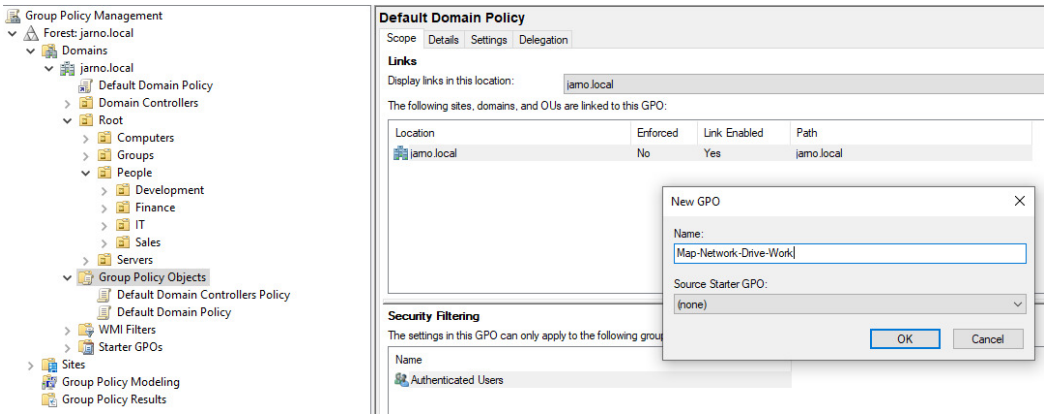
Lisäämme myös tässä välissä jarno.nousiainen@jarno.local käyttäjän Active Directory ryhmään ALL-IT, jotta voimme tarkistaa, että tämä Work kansioon Access-based enumeration (ABE) toimii, eli käyttäjän jarno.nousiainen@jarno.local ei pitäisi nähdä kansiota Finance Work verkkojaossa ollenkaan, vaan pelkästään IT kansion johon tällä ryhmällä ALL-IT on oikeudet päästä.



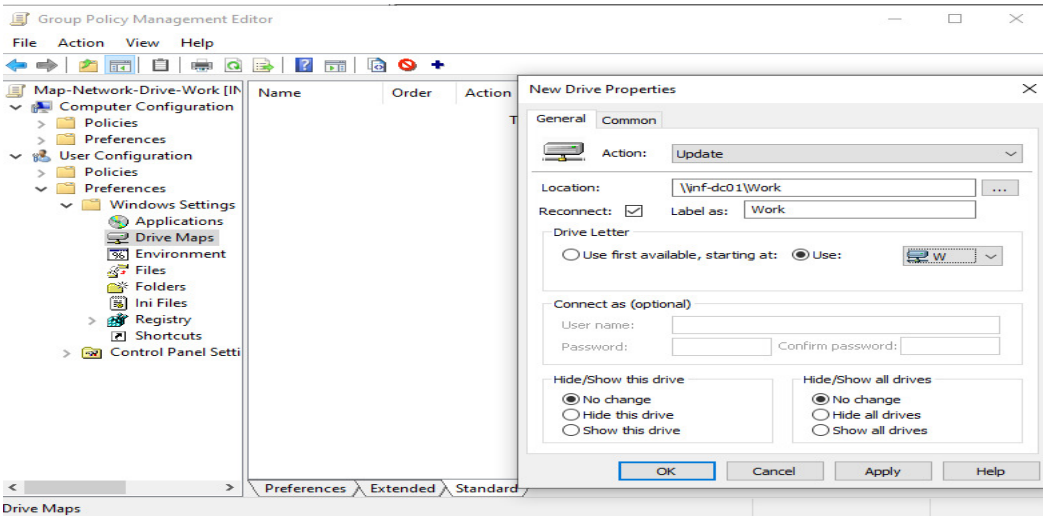
Lisäämme myös jarno.nousiainen@jarno.local Active Directory käyttäjälle Profile välilehdelle Home folder kohtaan tämän \\inf-dc01\home\jarno.nousiainen verkkolevyksi ja annamme sille kirjaimen H:



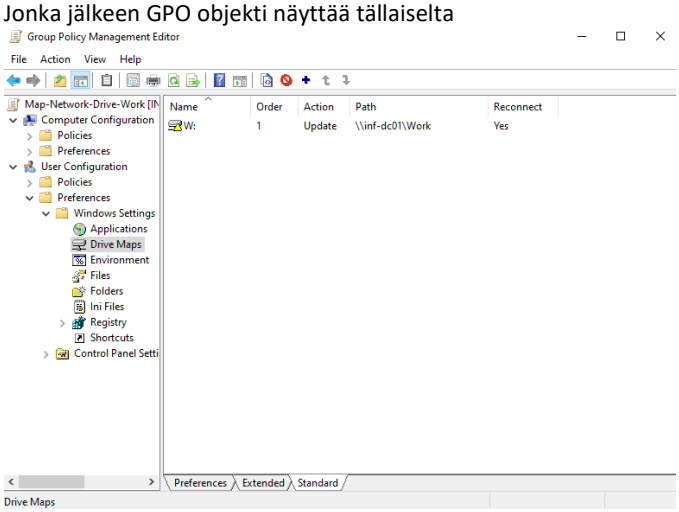
Tämän jälkeen luomme Group Policy Objecti jolla liitämme verkkolevyksi kaikille käyttäjille c:\Shares\Work levyn
GPO Objectin nimeksi tulee Map-Network-Drive-Work



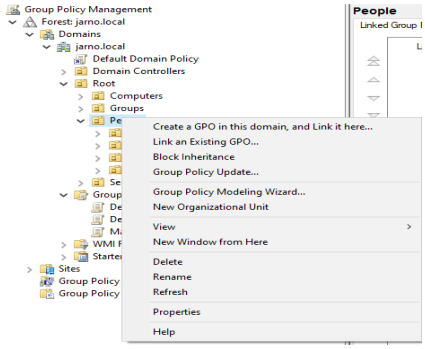
Muokkaamme User Configuration -> Prefences -> Windows Settings -> Drive Maps oheisen kuvan mukaisesti.
Action -> Update
Location -> \\inf-dc01\Work
Reconnect ruksi
Label as: -> Work
Driver Letter -> Use W



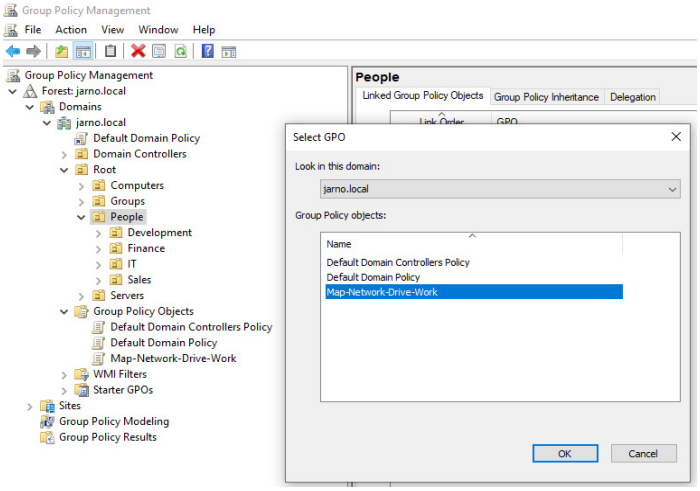
Jonka jälkeen GPO objekti näyttää tällaiselta



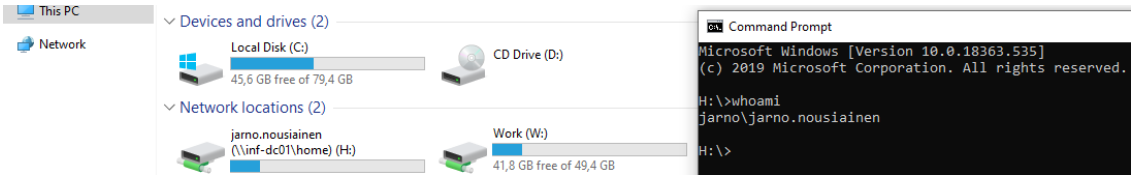
Tämän jälkeen vielä linkitämme tämän luomamme GPO objectin OU:hun People klikkaamalla OU:n People kohdalla hiiren oikealla ja valitsemalla Link and Existing GPO



Ja valitsemme Map-Network-Drive-Work



Ja tämän jälkeen, kun olemme kirjautuneet Windows 10 v1909 koneelle käyttäjällä jarno.nousiainen@jarno.local niin näemme sekä Home ja Work kansion This PC näkymässä



Sekä kun menemme Work kansioon, näemme vain Common (avoin kaikille käyttäjille) ja IT kansion johon meillä on vain pääsy.
Finance kansiota emme näe, kun meille ei ole siihen lukuoikeutta.