6105 Windows Server og datanett

Labøving 5a: Domenekontroller og AD DS

Etter installasjon av Windows Server, er tjenermaskinen din en *stand-alone tjener* i en arbeidsgruppe (*workgroup*). I denne øvingen skal du installere tjenerrollen *Active Directory Domain Services* og deretter *promotere* tjenermaskinen til å bli *domenekontroller* for et nytt Windows-domene.

Forkunnskaper og forutsetninger

Du bør ha sett gjennom leksjon 5a *Katalogtjenester og Active Directory* før du gjør denne øvingen. Øvingen er ikke avhengig av tidligere øvinger bortsett fra øvingene til leksjon 1.

Oppgavebeskrivelse

Her forklares kort hva øvingen går ut på for de som ønsker å finne løsningen selv.

Hvis du ønsker punkt-for-punkt veiledning kan du hoppe rett til **Detaljert veiledning** på neste side.

a) Installer tjenerrollen Active Directory Domain Services og promoter tjeneren til en domenekontroller for et nytt domene med navn **mittdomene.local**

b) Oppdater IP-konfigurasjon på tjeneren slik at IP-adressen til DNS-tjeneren i VirtualBox / VMware settes som *Alternate DNS server*

c) Lag en ny brukerkonto på tjenermaskinen med ditt eget navn/brukernavn.

d) Her bør du følge de detaljerte veiledningene i oppgave d1 (VirtualBox) eller d2 (VMware)

e) Meld klientmaskinen inn i det nye domenet.

f) Logg inn på domenet med den nye domenebrukeren du laget i oppgave c)

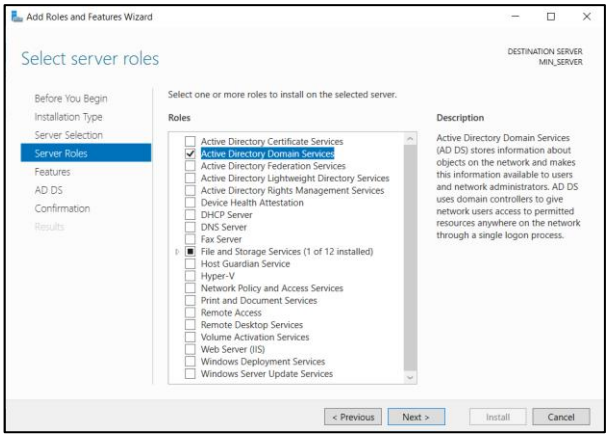
- På klientmaskinen: Sjekk at du ser tjenermaskinen og delte mapper/skrivere under *Network* i *File Explorer.*
- På tjenermaskinen Sjekk at du ser klientmaskinen under *Computers* i *Active Directory Users and Computers.*

Detaljert veiledning

Oppgave a: Installere Active Directory Domain Services

Du skal nå installere tjenerrollen Active Directory Domain Services (ADDS, og deretter konfigurere ADDS med Active Directory Domain Services Installation Wizard.

1. Logg inn på Windows Server med den lokale brukeren **Administrator**.
2. **Kontroller at tjenermaskinen har fast (statisk) IPv4-adresse.** Dette er **nødvendig** når maskinen skal være domenekontroller. Se labøving 2a, *Oppgave c Manuell IPv4-konfigurasjon i Windows Server.*
3. Start *Server Manager* og klikk lenken Add roles and features**,** eller bruk *Manage*-menyen opp til høyre.

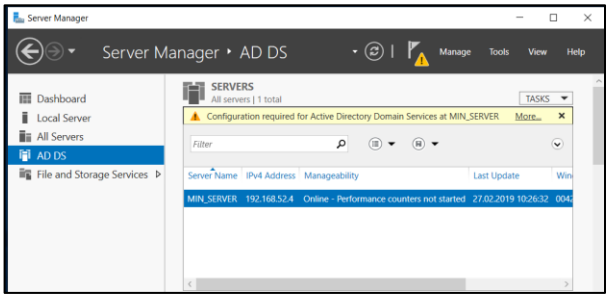


4. Installer tjenerrollen **Active Directory Domain Services.**
5. Du vil få beskjed om at flere *features* også må installeres.

   Add Features

   Det er OK. Installasjonen tar 5-10 min!

Når installasjonen er ferdig vil du i *Server Manager* se at valget **AD DS** har blitt lagt til i menyen til venstre.

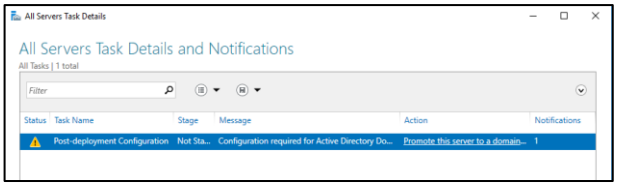


6. Velg **AD DS** i venstre kolonne.

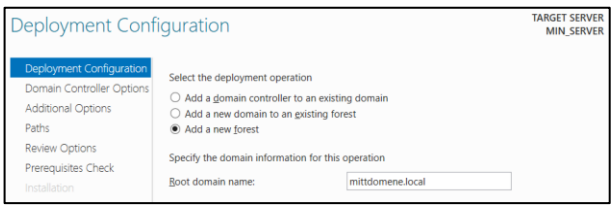
   Den gule linjen gir beskjed om at konfigurasjon kreves før AD DS kan aktiveres.

7. Bruk lenken ***More..*** til høyre på den gule linjen.

   Da vil du få opp vinduet All Server Task Details and Notifications.

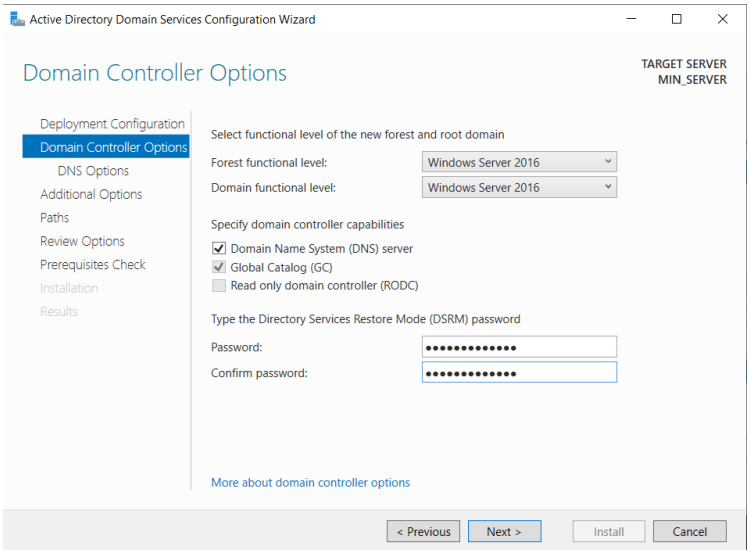


8. Klikk lenken Promote this server to a domain controller i kolonnen *Action.*
9. Gjennomfør veiviseren med disse valgene:



   - Fordi dette er ditt første domene må du opprette en *ny AD-skog* (***Add a new forest***). Skogen vil bestå bare av det nye domenet.

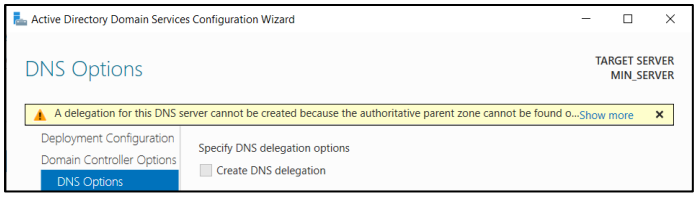
- Velg selv domenenavn for **rotdomenet** i den nye AD-skogen. Siden du ikke har et offisielt domenenavn i Internett, bør du velge et "lokalt" domenenavn, som f.eks. **mittdomene.local**



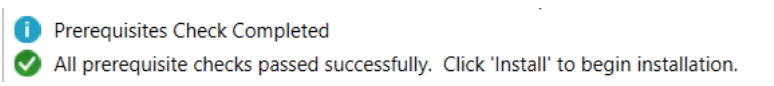
- Bruk **høyeste** tilgjengelige Windows Server versjon som *Forest functional level* og *Domain Functional Level)*
- Velg **Domain Name System (DNS) Server**. Du får en ferdig konfigurert DNS-tjener. I en senere øving skal du lære mer om DNS-tjeneren og hvordan du konfigurerer den.
- Som passord for *Directory Services Restore Mode (DSRM),* kan du bruke samme passord som for brukeren Administrator

Du vil få en gul advarsel knyttet til DNS Server på neste side.

Det er ok, så bare gå videre.



- På siden *Additional Options* kan feltet *The NetBIOS domain name* godt stå som det er (f.eks. **MITTDOMENE**). Legg merke til at NetBIOS **ikke** har hierarkiske navn og derfor ikke inneholder rotdomenet *.local*
- På siden *Paths* kan du legge merke til navn på mappene som AD DS bruker for å lagre databasen og loggfiler. Du trenger ikke endre noe her.
- Veiviseren vil sjekke at noen krav til serveren er innfridd før du kan trykke **Install.**
  Du vil fremdeles se et par gule varseltrekanter ⚠, men det er ok så lenge det siste punktet er grønt:



Opprettelse av domenet og installasjon av DNS-server kan ta noen minutter.
Vær tålmodig ☺

10. Windows Server omstartes automatisk etter at installasjonen er ferdig**.**

    Hva har endret seg i innloggingsvinduet? _____

11. Logg inn som **Administrator** for det nye **domenet**. (Denne domenebrukeren er den samme som tidligere var lokal bruker på tjenermaskinen.)

Nå vil du trolig se at maskinen **ikke** har (inter-)nettforbindelse.
Det skal du fikse etterpå i oppgave b: *Oppdatere DNS-informasjon på tjenermaskin*.

Du skal først sjekke at alle viktige komponenter på domenekontrolleren kjører som de skal:

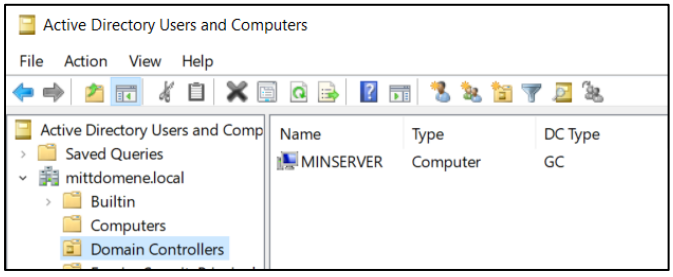
12. Bruk *Server Manager* og sjekk at disse nye verktøyene er installert under **Tools**-menyen:

    - Active Directory Administrative Center
    - Active Directory Domains and Trusts
    - Active Directory Module for Windows PowerShell
    - Active Directory Sites and Services
    - **Active Directory Users and Computers**
    - **DNS**

    De to siste administrasjonsverktøyene skal vi bruke mye i kommende øvinger. De andre har vi lite bruk for i dette emnet.

13. Start *Active Directory Users and Computers* og åpne symbolet merket med domenenavnet ditt (f.eks. **mittdomene.local**).

    - Du skal nå se tjenermaskinen din i mappen *Domain Controllers*.
    - Mappen *Computers* vil vise andre medlemsmaskiner i domenet.
      Den er foreløpig tom.



Oppgave b: Oppdatere DNS-informasjon på tjenermaskin

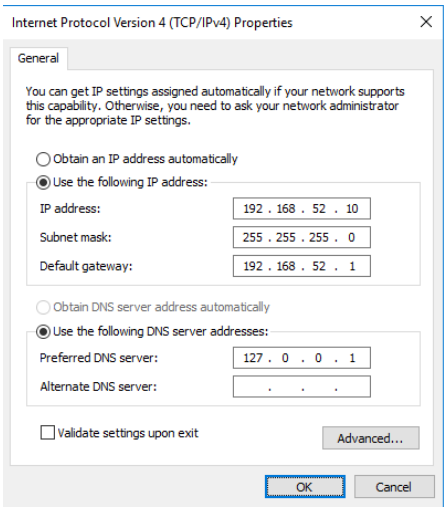
Under installasjon av AD DS og DNS blir foretrukket DNS-tjener satt til maskinen selv og alternativ DNS server blir satt blank. Dermed har Windows Server "mistet" informasjon om andre DNS-tjeneren enn seg selv. Dette må du rette opp manuelt nå:

1. Kontroller nettverkskonfigurasjon på tjenermaskinen og legg inn adresse til DNS-tjener slik:

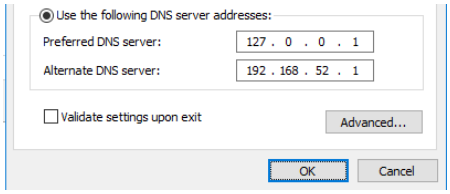
    - Gå til **Settings ► Network & Internet ► Ethernet,** og bruk lenken *Change adapter options*
    - Høyreklikk på symbolet for det lokale nettverkskortet (Ethernet), og velg **Properties**.
    - Åpne **Properties** for *Internet Protocol Version 4 (TCP/IPv4).* Denne vil se omtrent slik ut:

    Installasjonsrutinen for AD DS har nå satt *Preferred DNS server* til *loopbackadressen* (127.0.0.1 dvs. *localhost*). Det betyr at domene-kontrolleren nå er DNS-tjener for seg selv. Det er nødvendig for å kunne oversette DNS-navn på maskiner i Windows-domenet

    For å kunne oversette DNS-navn som tilhører **andre** Internet-domener, må domene-kontrolleren **i tillegg** kjenne IP-adressen til minst én DNS-tjener som har kontakt med Internett.

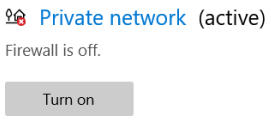
    - **Legg derfor inn IP-adressen til DNS-tjeneren i VirtualBox (192.168.52.1) eller VMWare (192.168.52.2), som *Alternate DNS server*.** Du kan alternativt bruke samme DNS-server som din fysiske maskin bruker.

2. Lukk vinduene og kontroller at DNS innstillingene fungerer ved å **ping**'e et maskinnavn i Internett, f.eks. **www.usn.no**.

Oppgradering til domenekontroller vil **kanskje** også ha aktivert Windows brannmuren for domenenett (Domain networks). Vi velger å slå av denne inntil videre:

3. Gå til **Settings ► Update and Security ► Windows Security ► Firewall and network protection.**
4. Sjekk status for brannmuren for aktiv profiler (eller alle profiler). Hvis den er på, så skru den **av**. Fordi serveren står i et (virtuelt) LAN bak NAT-ruteren i VirtualBox / VMware, så kan den ikke nås "utenfra", og det er trygt å skru av brannmuren.



Oppgave c: Lage din egen brukerkonto i AD domenet (domenekonto)

Brukeren **Administrator** har rettigheter til å lage nye brukerkontoer i domenet (domene-kontoer). I labøving 2b laget du en lokal brukerkonto på tjenermaskinen (**Lokal tjenerbruker**) mens den var i arbeidsgruppe. Etter at du har promotert tjeneren til domenekontroller, vil denne brukerkontoen fungere som en domenekonto. Du skal nå sjekke dette:

1. Start **Active Directory Users and Computers** fra *Tools*-menyen i *Server Manager*
2. Åpne domenet ditt, og mappen **Users.** Du bør finne igjen brukerkontoen **Lokal tjenerbruker** i listen.

   - Åpne (dobbeltklikk) denne brukeren og studer egenskapene til brukerkontoen før du lukker vinduet.

3. Lag en ny domenebruker til deg selv ved å høyreklikke på mappen **Users** og velge **New ► User.**

   - Bruk ditt eget navn i *First name*, *Last name* og *Full name*
   - Velg selv påloggingsnavn (*User logon name*).
   - Velg passord selv (ett du husker!)
   - Angi at passordet aldri utløper (*Password never expires*).

Obs! Windows Server tillater i utgangspunktet ikke innlogging på server med brukerkontoer som ikke er administratorer. (Dette skal du endre senere i labøving 5b oppgave a.)

Derfor skal du her bare teste innlogging med den nye brukeren fra **klientmaskinen** (oppgave f), men først må du melde klienten inn i domenet i oppgave d og e.

Oppgave d1: Endre DNS-tjeneradresse for klienten i VirtualBox

Hvis du bruker VMWare kan du hoppe rett til oppgave d2

Fordi Windows-tjeneren nå er DNS-tjener for Windows-domenet, må **klientmaskinen** også bruke denne som DNS-tjener. Klienten får IP-konfigurasjonen sin automatisk fra DHCP tjeneren i VirtualBox. I et "normalt" driftsmiljø ville vi nå ha lagt inn tjenermaskinens IP-adesse som primær DNS-tjener i DHCP-tjenerens konfigurasjon slik at alle klienter automatisk får denne.

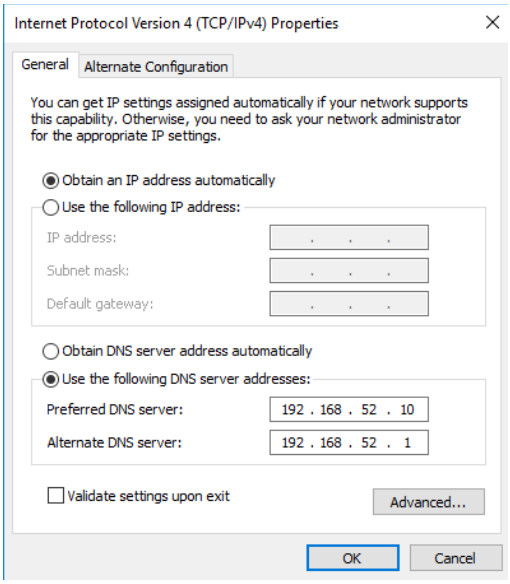
Dessverre har ikke VirtualBox mulighet for å endre DHCP-konfigurasjon manuelt. DHCP-tjeneren i VirtualBox vil automatisk bruke de DNS-tjenerne som brukes av den fysiske maskinen. Med VirtualBox må du derfor konfigurere DNS-tjenere **manuelt** på Windows klientmaskinen slik:

1. Start klientmaskinen med Windows og logg inn med den lokale brukeren **admin**.
2. Gi klientmaskinen DNS-konfigurasjon **manuelt** i vinduet til høyre. (Tilpass evt. til de adressene du bruker.)

DNS-tjenere:

- ✓ *Preferred DNS server*: **192.168.52.10**
  Dette er DNS-tjeneren på tjenermaskinen din
- ✓ *Alternate DNS server*: **192.168.52.1**
  Dette er DNS-tjeneren i VirtualBox.

(Du kan alternativt også bruke adressen til en DNS-tjener hos din ISP.)

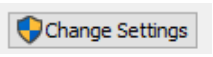


3. Lukk vinduet og sjekk at DNS virker ved å pinge et **maskinnavn** utenfor eget nett, f.eks. **www.usn.no**.

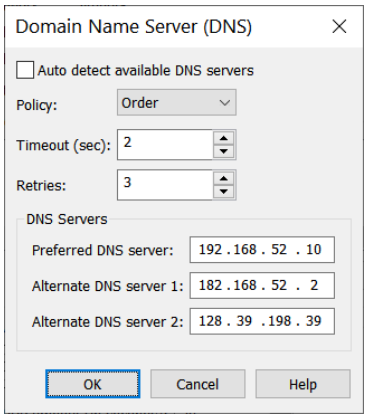
Oppgave d2: Endre DNS-tjeneradresse for klienten i DHCP tjener på VMWare

Hvis du bruker VirtualBox skal du ikke gjøre denne oppgaven.

Fordi domenekontrolleren nå er DNS-tjener for Windows-domenet, må klientmaskinen også få denne informasjonen. Klienten får IP-konfigurasjonen sin automatisk fra DHCP tjeneren i VMWare. Vi skal derfor endre IP-adresse til DNS-tjener i DHCP-oppsettet i VMWare:

1. Slå av alle virtuelle maskiner og **avslutt** *VMWare Player.*
2. Start programmet **vmnetcfg** (*VMWare Virtual Network Editor*) slik du gjorde i øving 2a oppgave d1 eller d2.
3. Klikk knappen 

4. Merk **VMnet8** (type NAT) og bruk knappen **NAT Settings…** og **DNS settings...**
5. **Fjern** haken foran *Auto detect available DNS servers*, og oppgi følgende DNS servere:
   - ✓ **192.168.52.10** (DNS-tjener på SERVER2012)
   - ✓ **192.168.52.2** (DNS-tjener i VMWare)
   - ✓ **128.39.198.39** (DNS-tjener hos USN), eller bruk DNS-tjeneren hos din ISP.



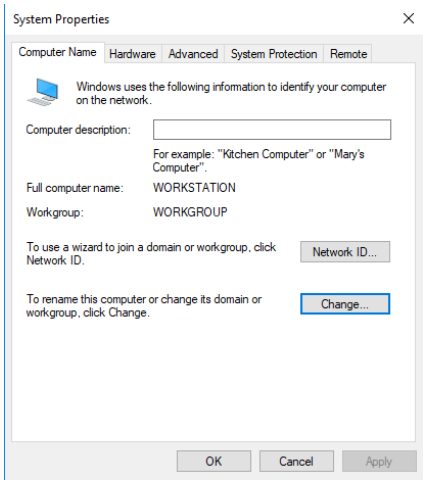
6. Klikk **OK** flere ganger for å avslutte og lagre endringene i *Virtual Network Editor.*
7. Start både tjenermaskinen og klientmaskinen.

Oppgave e: Melde klientmaskinen inn i Windows-domenet

Obs! Både tjenermaskin og klientmaskin må være startet for å gjøre denne oppgaven!

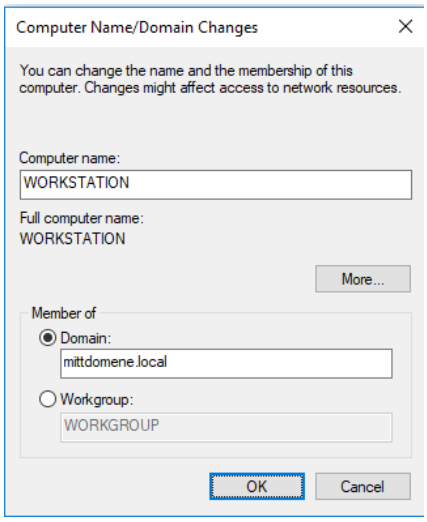
Du skal nå melde klientmaskinen inn i det nye Windows-domenet. Dette er nødvendig for å kunne logge inn på klienten med domenebrukere som er registrert i AD DS på tjeneren.

1. Vær innlogget på klientmaskinen med den lokale brukeren **admin** (som har administratorrettigheter lokalt på maskinen).
2. Start **Settings → System → About**
3. Bruk lenken Advanced system settings under overskriften *Related Settings* et stykke ned på siden.
4. I vinduet *System Properties* velger du fanen ***Computer Name,*** og knappen **Change…** i bildet til høyre.



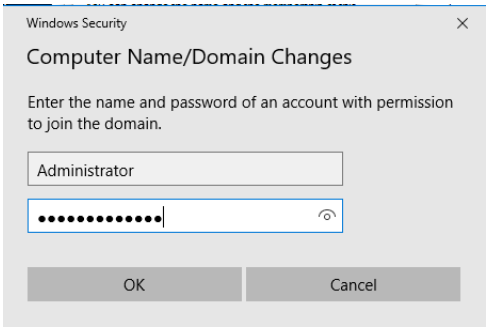
   Du får opp dialogboksen *ComputerName/Domain Changes* nedenfor:

5. Velg **Domain** under *Member of,* oppgi ditt domenenavn (**mittdomene.local**) og klikk OK.

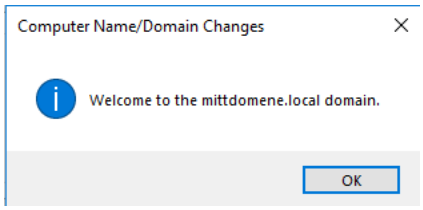


Du får nå et vindu der du må oppgi brukernavn og passord til en **domenekonto** med rettigheter til å melde maskinen inn i domenet

6. Bruk domenekontoen **Administrator**:



Hvis alt går bra, blir klientmaskinen meldt inn i domenet, og du får opp bekreftelsesvinduet til høyre.

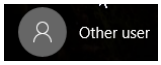


Innmelding til domenet vil ikke få effekt før Windows startes på nytt.

7. Bekreft omstart og vent til du får opp innloggingsvinduet.

Oppgave f: Logge på Windows-domenet fra klientmaskin

Etter at klientmaskinen er meldt inn i domenet kan du logge på **domenet** fra denne maskinen. Dvs. du kan logge på klientmaskinen med en **domenebruker** f.eks. den du laget i oppgave c).

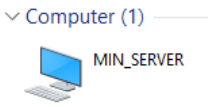
1. Start klientmaskinen og klikk 

i innloggingsbildet.

   Hva endrer seg i innloggingsbildet? _____

2. Klikk på lenken *How do I sign in to another domain?* og les forklaringen.
3. Logg inn med **din egen domenebruker** som du laget i AD DS i oppgave c.
   Det tar litt tid å logge inn første gang med en ny bruker.

   Hvorfor kan du logge inn med denne brukeren på klientmaskinen, selv om brukerkontoen ble laget på tjenermaskinen? _____
4. Start **File Explorer** (**Filutforsker**) og velg **Network**.
   Kontroller at du ser tjenermaskinen under *Network*, og åpne denne.

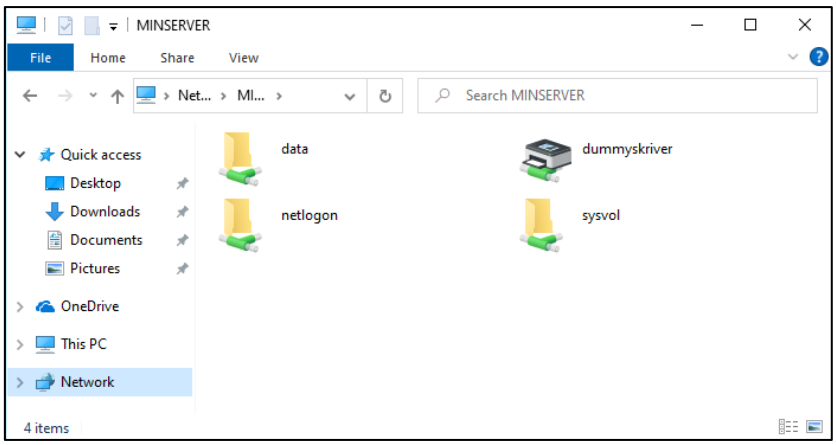
   

   (Trykk **F5** for å refreshe listen hvis du ikke ser den med en gang.)

   Hvis du heller ikke ser tjenermaskinen under Network etter refresh, kan du prøve å skrive tjenerens UNC-navn (**\\MIN_SERVER**) i adressefeltet i *File Explorer (Filutforsker)*:

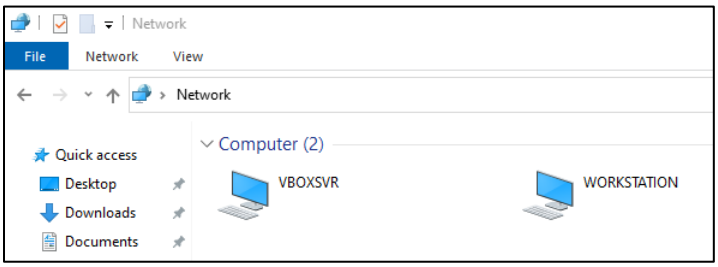
   

5. Når du har åpnet tjenermaskinen under *Network* kan du sjekke at du har tilgang til delte mapper og skrivere på tjeneren.

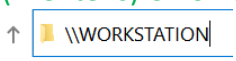


Fordi klientmaskinen nå er medlem av domenet og du har logget på med en domenebruker, skal du kunne se delte ressurser på tjeneren **uten** å oppgi brukernavn / passord på nytt.

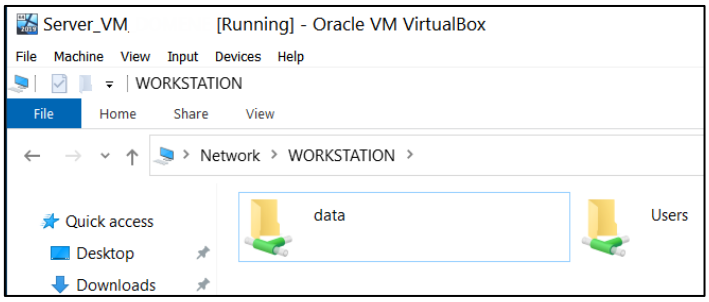
6. Bytt til **tjenermaskinen** (innlogget som **Administrator**) og start **Active Directory Users and Computers** fra *Tools*-menyen i *Server Manager*.
7. Sjekk at klientmaskinen (**WORKSTATION**) nå er synlig i mappen *Computers* under domenet. (Refresh med F5 om nødvendig.) Denne maskinkontoen ble opprettet automatisk i AD når du meldte maskinen inn i domenet.
8. Bruk *File Explorer (Filutforsker)* på tjenermaskinen og se etter klientmaskinen under *Network*.



Hvis du **ikke** ser klientmaskinen under Network, kan du her også prøve å skrive maskinens (klientens) UNC-navn (**\\WORKSTATION)** i adressefeltet i *File Explorer (Filutforsker):*



Etter at du har åpnet klientmaskinen bør du kunne se mapper som er delt fra klienten:



Slutt på øvingen.