

6105 Windows Server og datanett

Labøving: 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.

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 Oppgave a 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*.

Oppgave a: Installere Active Directory Domain Services

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

1. Logg inn på tjenermaskinen med den lokale brukeren **Administrator**.

2. **Kontroller at tjenermaskinen har fast (statisk) IPv4-adresse.** Dette er **nødvendig** når maskinen skal være domenekontroller. Har den ikke det, se oppgave e fra labøving 2a.

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**. Du vil få beskjed om at andre *features* også må installeres. Det er OK. Installasjonen tar 5-10 min!

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

5. Velg **AD DS**.

Den **gule linjen** gir beskjed om at konfigurering trengs før AD DS kan aktiveres.

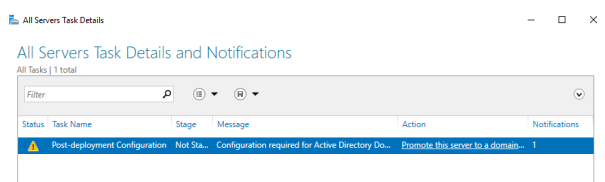
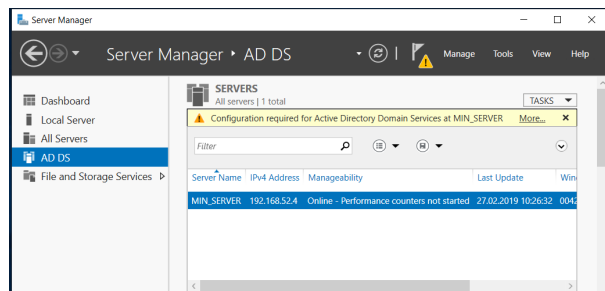
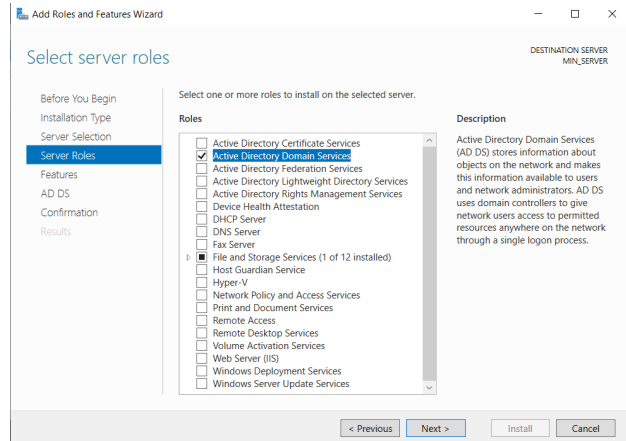
6. Klikk lenken *More* til høyre på den **gule linjen**.

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

7. Klikk lenken **Promote this server to a domain controller** i kolonnen *Action*.

8. 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 rotdometet 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**



Labøving: Domenekontroller og AD

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the window name and standard minimize, maximize, and close buttons. The main title is 'Domain Controller Options'. On the right side, it indicates 'TARGET SERVER' and 'MIN_SERVER'. A left-hand navigation pane lists several steps: 'Deployment Configuration', 'Domain Controller Options' (which is highlighted in blue), 'DNS Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select functional level of the new forest and root domain'. It contains two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server 2016'. Below this is a section 'Specify domain controller capabilities' with three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). Further down is a section 'Type the Directory Services Restore Mode (DSRM) password' with two password input fields labeled 'Password:' and 'Confirm password:'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about domain controller options' is located at the bottom of the main content area.

- Bruk **høyeste** 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:

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window at the 'DNS Options' step. The title bar and window controls are the same as in the previous screenshot. The main title is 'DNS Options'. On the right side, it indicates 'TARGET SERVER' and 'MIN_SERVER'. A yellow warning banner at the top reads: 'A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found o...Show more'. Below the banner is a left-hand navigation pane with 'DNS Options' highlighted in blue. The main content area is titled 'Specify DNS delegation options' and contains a single checkbox labeled 'Create DNS delegation' which is unchecked.

Det er ok, så gå videre.

- *The NetBIOS domain name* kan godt stå som det er (f.eks. **MITTDOMENE**). Legg merke til at NetBIOS **ikke** har hierarkiske navn og derfor ikke inneholder .local)
- På siden *Paths* kan du legge merke til navn på mappene som AD DS bruker for å lagre data 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 nå fremdeles se et par gule varseltrekanter ⚠️, men det er ok)

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

Vær tålmodig 😊

Labøving: Domenekontroller og AD

9. Windows Server restartes automatisk etter at installasjonen er ferdig.

Hva har endret seg i innloggingsvinduet? _____

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

Du vil trolig nå se at maskinen ikke har nettverksforbindelse. Det skal du fikse i oppgave b.

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

11. Åpne *Server Manager* og sjekk at følgende nye verktøy er installert under **Tools**-menyen:

- *Active Directory Administrative Center*
- *Active Directory Domains and Trusts*
- *Active Directory Module for 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.

12. 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 har Windows Server "mistet" informasjon om andre DNS-tjeneren enn seg selv. Dette må du rette opp manuelt nå:

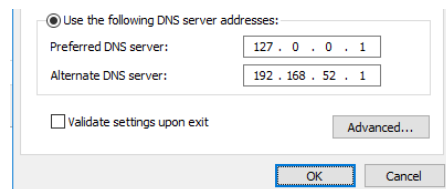
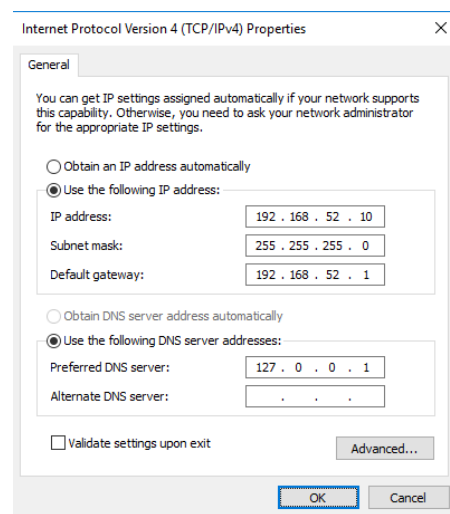
1. Kontrollere nettverkskonfigurasjon på tjenermaskinen og legg inn adresse til DNS-tjener slik:

- Gå til **Settings** ► **Network and Internet** ► **Ethernet** og klikk lenken [Network and Sharing Center](#).
- Klikk lenken *Change adapter settings*
- Høyreklikk symbolet for det lokale nettverkshortet (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 domenekontrolleren 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 domenekontrolleren **i tillegg** kjenne IP-adressen til minst én DNS-tjener som har kontakt med Internett.

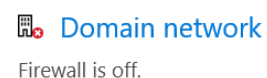
- **Legg derfor inn IP-adressen til DNS-tjeneren i VirtualBox (192.168.52.1) eller VMWare (192.168.52.2), som *Alternate DNS server***. Du kan evt. også bruke samme DNS server som din fysiske maskin bruker.



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 under **Domain network**. 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 nå "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 (domenekontoer). 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 (dobbelklikk) 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*).

Windows Server tillater i utgangspunktet ikke innlogging på server med brukerkontoer som ikke er administratorer. I oppgave f skal du derfor teste innlogging med den nye brukeren fra klientmaskinen, 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. Dessverre har ikke VirtualBox mulighet for å endre DHCP-konfigurasjon manuelt, slik VMWare har. 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 brukeren *admin*.
2. Gi klientmaskinen DNS-konfigurasjon **manuelt** i vinduet til høyre. (Tilpass evt. til de adressene du bruker)

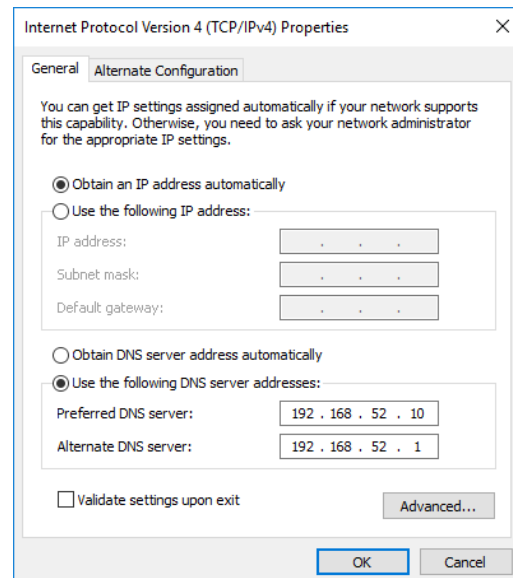
DNS-tjenere:

- ✓ *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**.

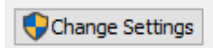
Oppgave d2: Endre DNS-tjeneradresse for klienten i DHCP tjener på VMWare

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. Det løses ved å endre oppsett 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.

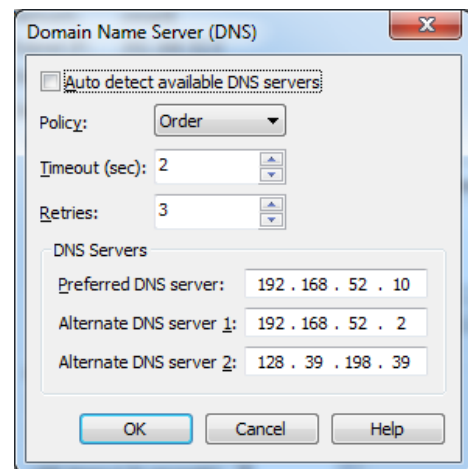
3. Klikk knappen



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 HSN),
eller bruk DNS-tjeneren hos din ISP.

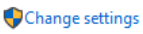


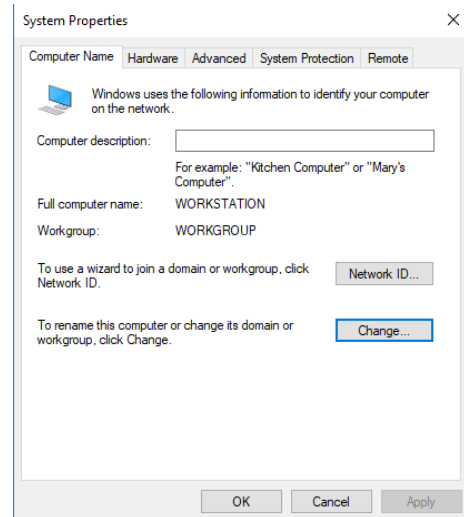
6. Klikk **OK** flere ganger for å avslutte og lagre endringene i *Virtual Network Editor*.
7. Start både tjenermaskinen og klientmaskinen.

Oppgave e: Melde klientmaskinen inn i domenet

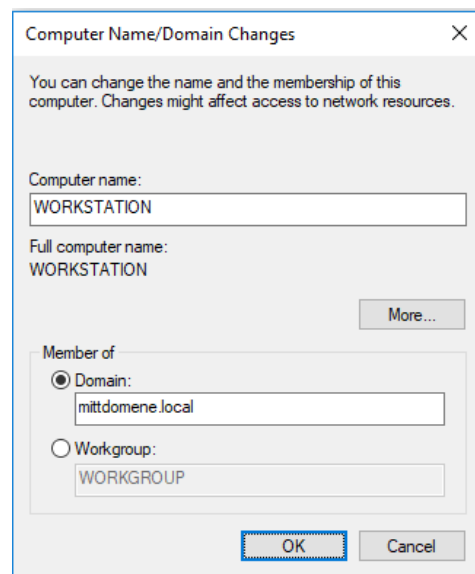
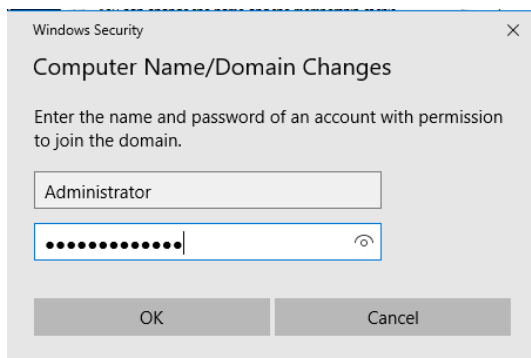
Obs! Både tjenermaskin og klientmaskin må være startet for å gjøre denne oppgaven!

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

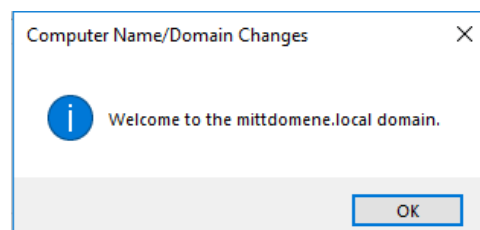
5. Vær innlogget på klientmaskinen med den lokale brukeren **admin** (som har administratorrettigheter lokalt på maskinen).
6. Start *kontrollpanelet (Control Panel)*, velg **System and Security**, og **System**.
7. Finn overskriften *Computer name, domain and workgroup settings* og klikk  **Change settings** ute til høyre.
8. I vinduet *System Properties* og fanen **Computer Name** bruker du knappen **Change...** og du får opp dialogboksen til høyre nedenfor.



9. Velg *Member of domain*, oppgi ditt domenenavn (**mittdomene.local**) og klikk OK.
Du får nå et vindu der du må oppgi brukernavn og passord til en domenkonto med rettigheter til å melde maskinen inn i domenet
10. Bruk domenkontoen **Administrator** :



11. 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.



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

Oppgave f: Logge på 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.

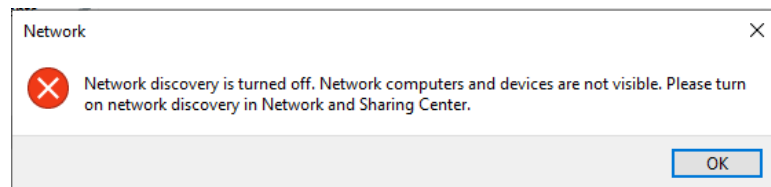
Hva endrer seg i innloggingsbildet? _____

2. Klikk 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.

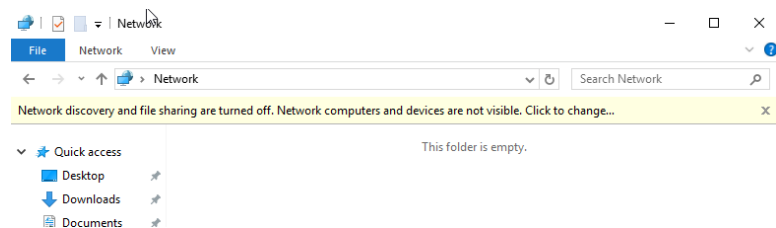
Hvorfor kan du logge inn med denne brukeren på klientmaskinen, selv om brukerkontoen ble laget på tjenermaskinen? _____

4. Start **File Explorer** og velg **Network**.

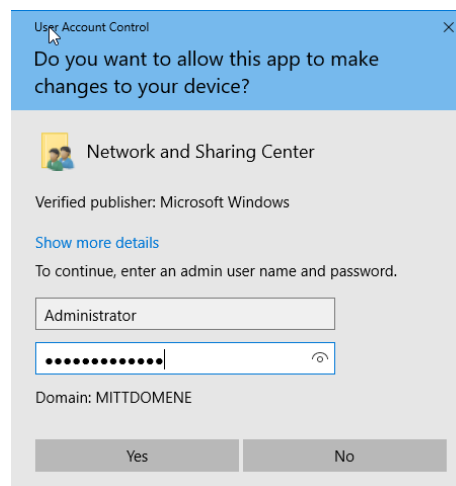
Du får kanskje en melding om at *Network discovery er skrudd av*.



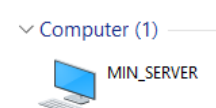
Du må skru det på igjen etter at maskinen er meldt inn i domenet. Dette gjør du ved å klikke den gule linjen øverst i vinduet:



Fordi klientmaskinen nå er medlem i domenet, kreves det autentisering som domene-administrator for å endre disse innstillingene på maskinen.



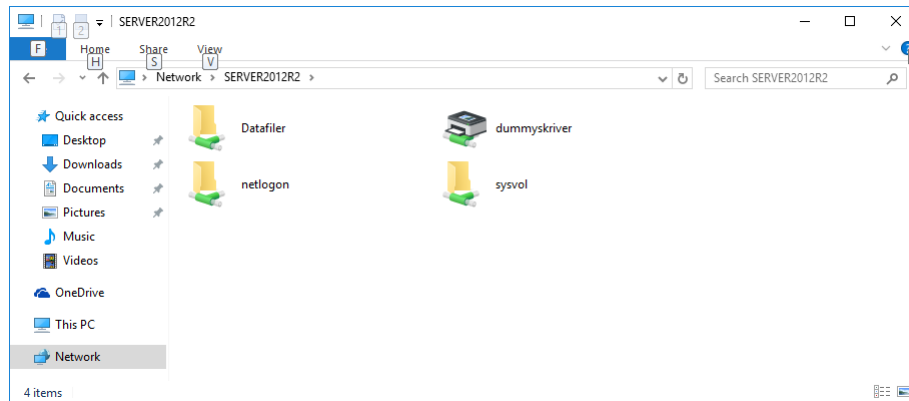
5. Kontroller at du nå ser tjenermaskinen under *Network*.



(Vent litt og trykk **F5** for å refreshe listen hvis du ikke ser den med en gang.)

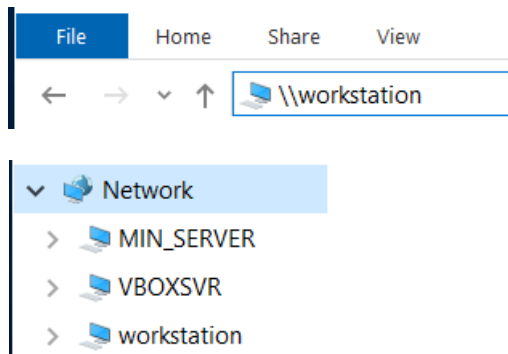
Labøving: Domenekontroller og AD

6. Åpne tjenermaskinen under *Network* og sjekk 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 nå kunne se delte ressurser på tjeneren uten å oppgi brukernavn / passord på nytt.

7. Bytt til tjenermaskinen og start *Active Directory Users and Computers* fra *Tools*-menyen i *Server Manager*.
8. Sjekk at klientmaskinen nå er synlig i mappen *Computers* under domenet. (Refresh med F5 om nødvendig.) Den ble automatisk registrert her når du meldte den inn i domenet.
9. Bruk *File Explorer* på tjenermaskinen og sjekk at du kan se klientmaskinen (**WORKSTATION**) under *Network*. (Vent litt og trykk **F5** for å refreshe listen hvis du ikke ser den med en gang.)



Hvis du ikke får opp klientmaskinen så forsøk å skrive **\\workstation** i adresselinjen øverst i File Explorer.

Slutt på øvingen.