Universitetet i Sørøst-Norge

6105 Windows Server og datanett

Leksjon 5a Katalogtjenester og Active Directory

- Katalogtjenester
- FEIDE, Active Directory Domain Services og Single Sign-on
- Windows domener, domenenavn og DNS
- Organisering av AD, objekter og egenskaper
- Etablere AD domene, AD-databasen og administrasjonsverktøy
- Melde en maskin inn i domenet og logge inn med domenekonto

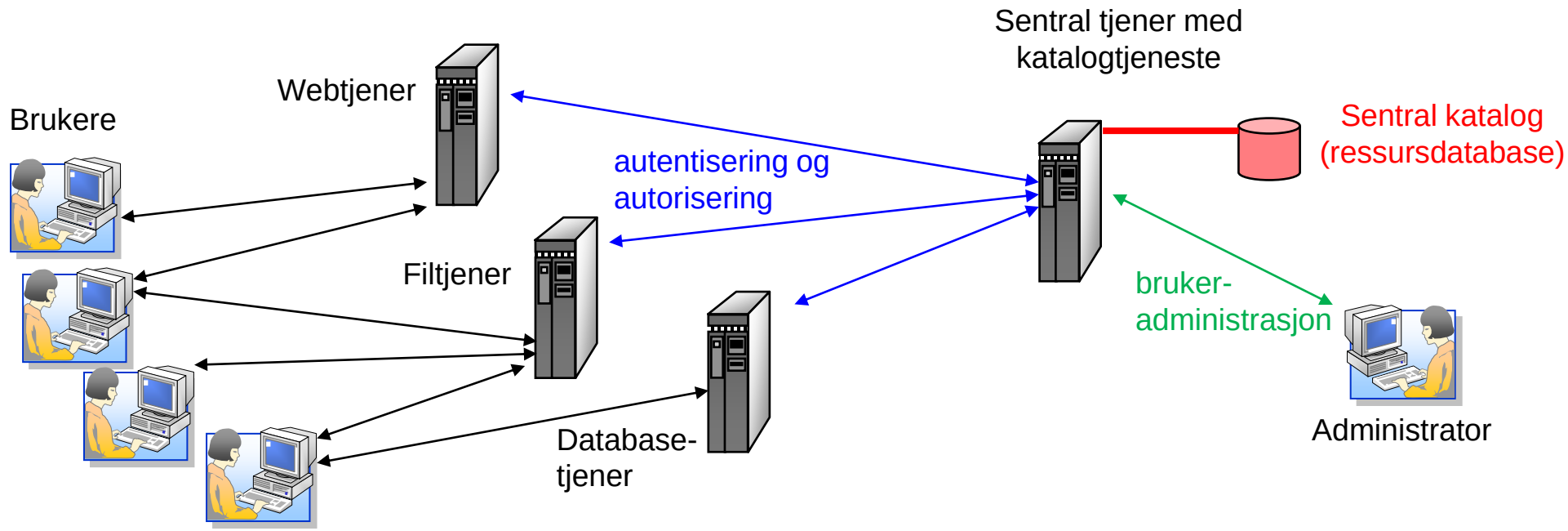
Pensum

- Kvisli: Windows Server og nettverk, kapittel 6 Windows-domener og AD DS

Relevante lenker

- http://en.wikipedia.org/wiki/Directory_service
- http://www.feide.no/
- http://en.wikipedia.org/wiki/Active_Directory

Katalogtjeneste (Directory Service)



En katalogtjeneste består av tre hovedkomponenter:

- En katalog (eng:directory), vanligvis hierarkisk organisert
  - » en database med opplysninger om ressurser i nettet (brukere, maskiner og annet)
- Programmer og verktøy for å oppdatere og lese katalogen (ressursdatabasen)
  - » brukes av administrasjonsverktøy for å vedlikeholde data i katalogen
- Protokoller for å styre ressurstilgang basert på innholdet i katalogen (ressursdatabasen)
  - » brukes bl.a. for å autentisere og autorisere brukere ved pålogging

Katalogtjeneste (Directory Service)

Hensikt / funksjon

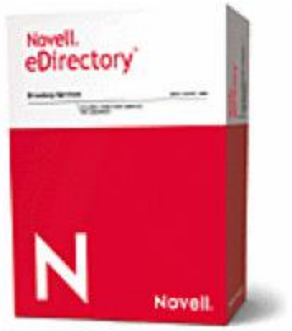
- Lagre og organisere brukerkontoer, brukergrupper og ressurser i nettet
- Autentisere brukere og maskiner
- Gjøre ressursene i nettet tilgjengelige for autoriserte brukere og programmer

Fordeler

- Ett brukernavn og passord til flere (alle) tjenester - enklere for brukerne
- Mulighet for "single sign on"
- Bedre sikkerhet med én felles bruker- og ressursdatabase

Standarder for katalogtjenester

- ISO X.500
  - » Stor og kompleks CCITT standard for katalogtjenester (innhold, aksess, sikkerhet)
- LDAP - Lightweight Directory Access Protocoll ← mest brukt i praksis
  - » Åpen og leverandøruavhengig IETF standard protokoll for å aksessere og oppdatere distribuert kataloginformasjon
  - » Enklere en X.500 standarden og basert på TCP/IP protokollene

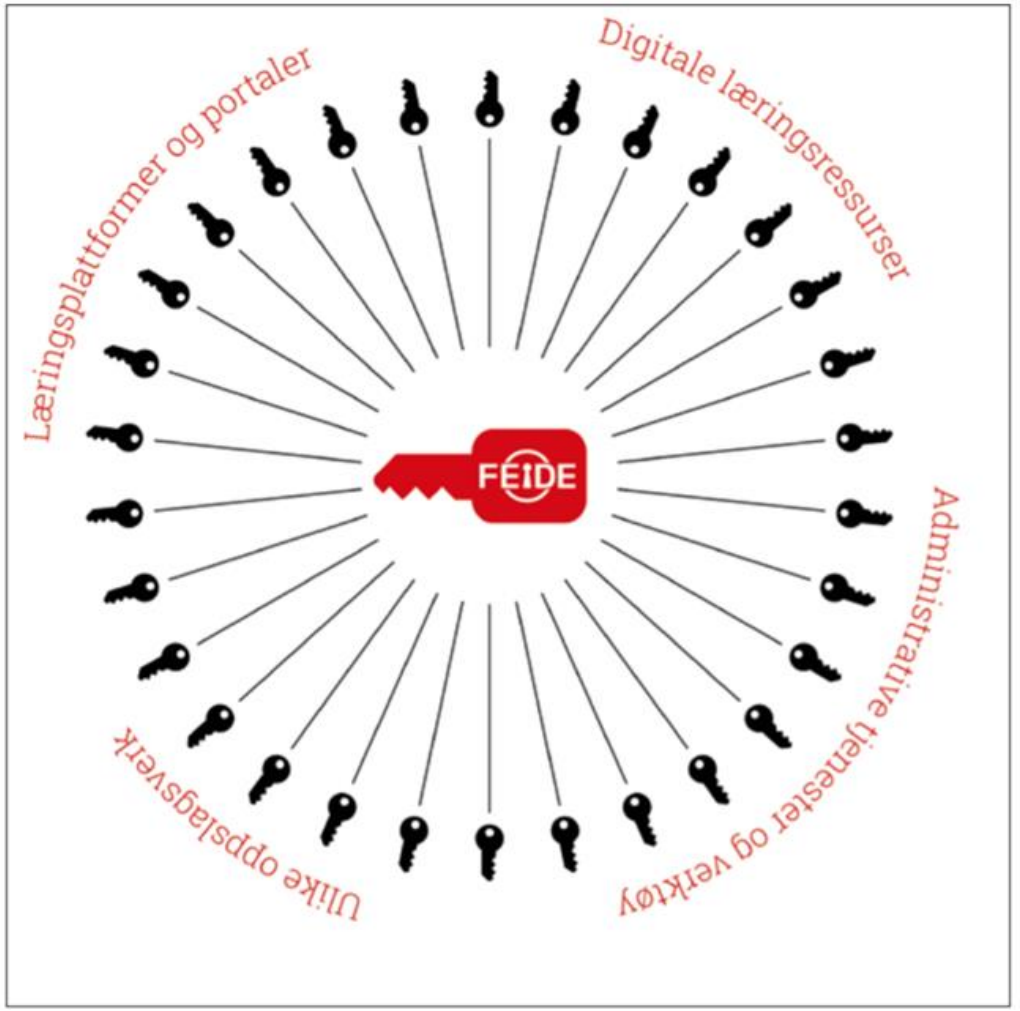


Noen katalogimplementasjoner som følger LDAP standarden

- Microsoft Active Directory (Windows nettverk)
- NetIQ eDirectory (tidligere Novell eDirectory)
- Apache Directory Server
- Oracle Internet Directory (OID)
- OpenLDAP - åpen kildekode - vanlig i Linux miljøer

Eksempel på katalogtjeneste: FEIDE (www.feide.no)

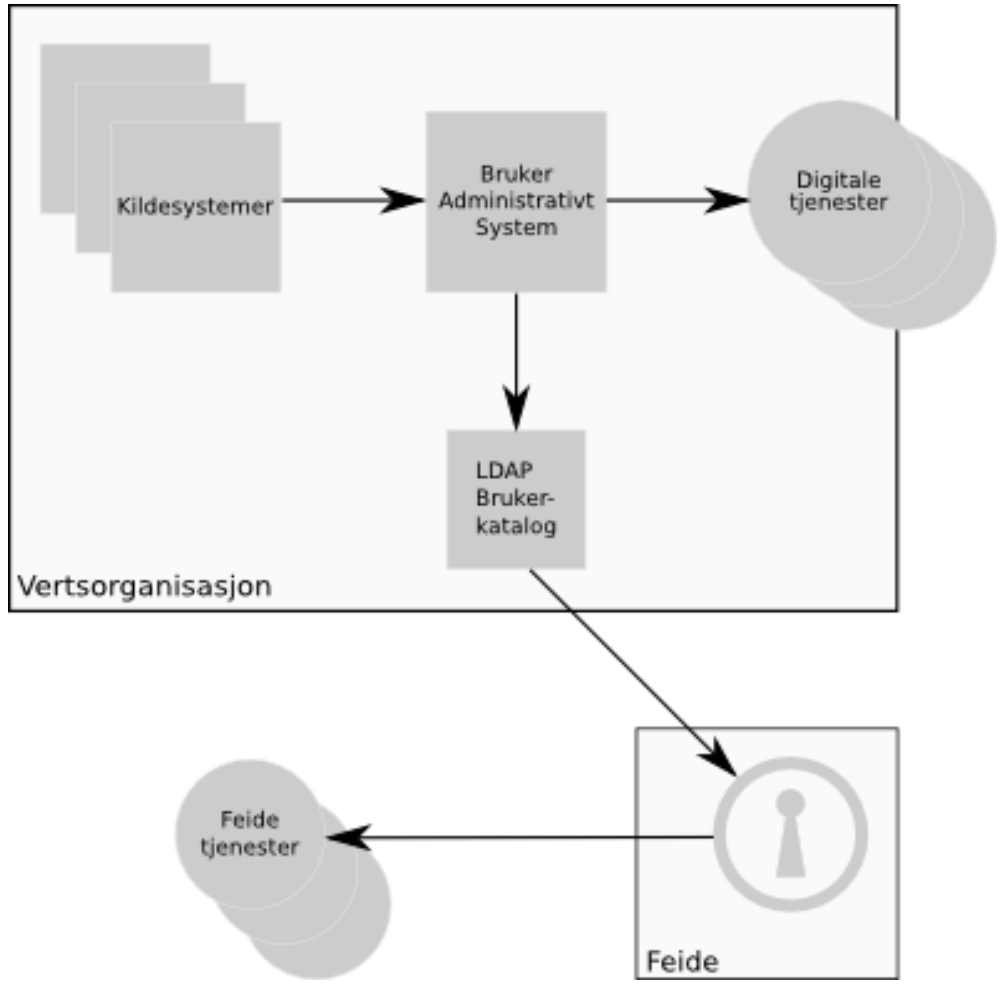
- **Felles nasjonal katalogtjeneste for utdanningssektoren**
  - Ansatte og studenter ved universiteter og høgskoler
  - Elever og lærere i videregående skole og noen grunnskoler
- **Gir tilgang til et stort antall tjenester med samme brukernavn og passord**
  - Se: https://www.feide.no/tjenester-med-feide-innlogging
- **En distribuert katalogtjeneste**
  - Brukere registreres og lagres i en lokal brukerkatalog hos hver vertsorganisasjon
  - Innlogging skjer via en nasjonal tjeneste
  - Autentisering gjøres alltid hos vertsorganisasjonen
- **Administreres av UNINETT**
  - Nasjonal innloggingstjeneste
  - Protokoller for oppslag og kommunikasjon med vertsorganiasjonene



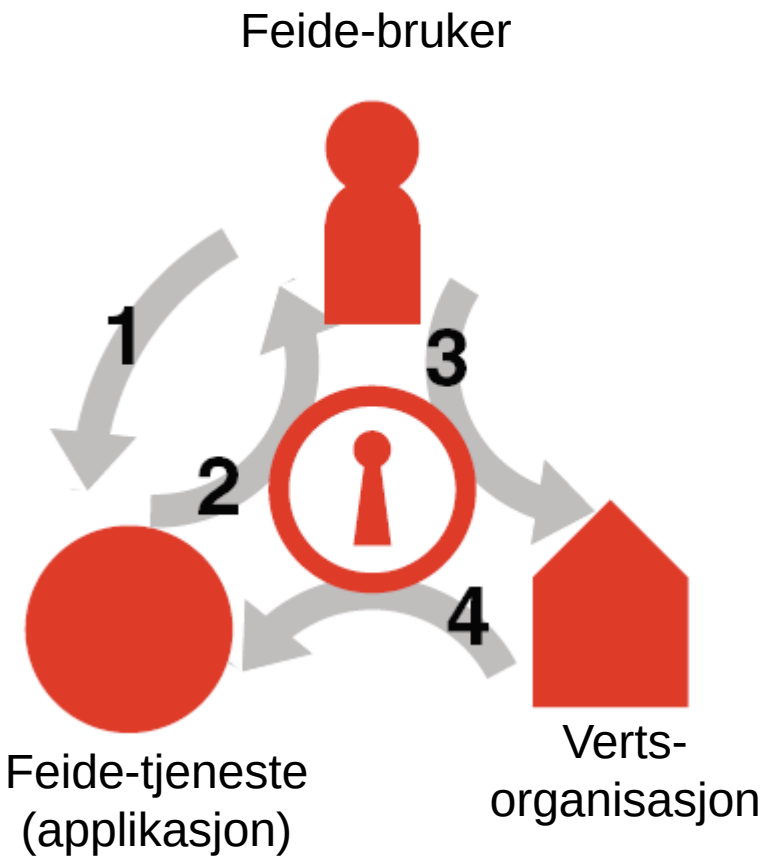
FEIDE er en distribuert katalogtjeneste

- **En lokal Identity Management (IdM) - løsning hos hver vertsorganisasjon**
  - En LDAP brukerkatalog med organisasjonens brukere
  - Vedlikeholdes lokalt av hver institusjon med et brukeradministrativt system (BAS)
  - Data kan hentes fra andre kildesystemer hos vertsorganisasjonen
- **Nasjonal autentiseringstjeneste (påloggingstjeneste)**
  - Mottar forespørsel om autentisering fra digitale tjenester som brukeren vil benytte
  - Videresender forespørsel til lokal Feide-katalog hos brukerens vertsorganisasjon
  - Informerer de digitale tjenestene om autentisering er vellykket eller ikke

Feides arkitektur



Hvordan virker innlogging med FEIDE?



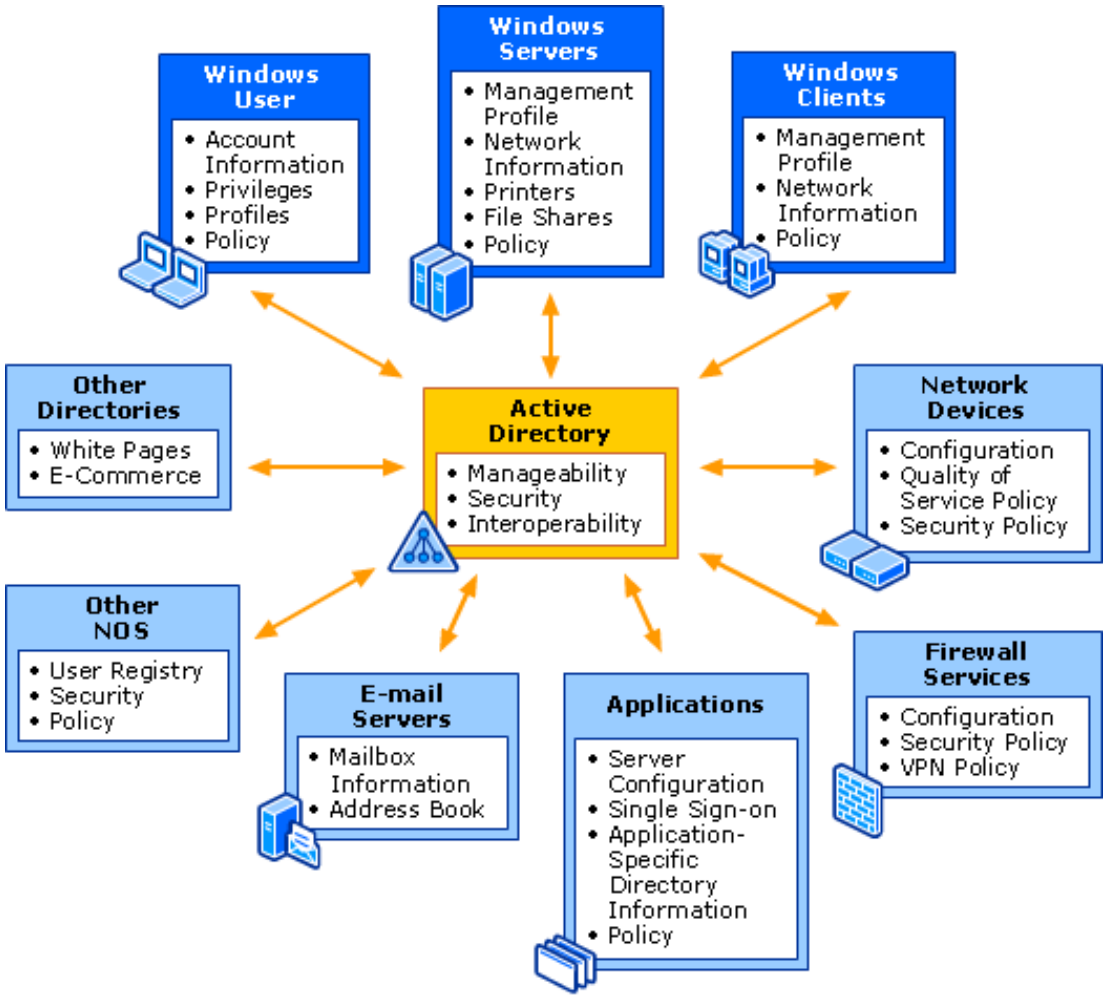
1. **Brukeren forsøker å starte den tjenesten han ønsker å benytte.**

2. **Tjenesten sender en autentiserings-forespørsel til Feide**
   - som åpner et innloggingsskjema for brukeren

3. **Brukeren skriver inn Feide-navn og passord**
   - dette retureres til Feide.
   - Feide sender navn og passord til brukerens vertsorganisasjon for kontroll.

4. **Vertsorganisasjonen sender bekreftelse på at brukeren er autentisert**
   - sendes til Feide sammen med de bruker-attributter vertsorganisasjonen har lagret for denne brukeren
   - Feide videresender bekreftelse på brukerens autentisering til tjenesten
   - sender de brukerattributtene som tjenesten behøver

Active Directory Domain Services (AD DS)



Microsoft Active Directory

Katalogtjeneste for Windows nettverk

- **Database** som lagrer objekter (maskiner, brukerkontoer m.m.) i et Windows doméne
- **Programmer** og **protokoller** som styrer pålogging og tilgangsrettigheter for alle maskiner i domenet
- **Administrasjonsverktøy** for AD databasen (bruker, maskiner, grupper m.m.)

Oppgaver

- Autentisering = pålogging
- Autorisering = tilgangskontroll

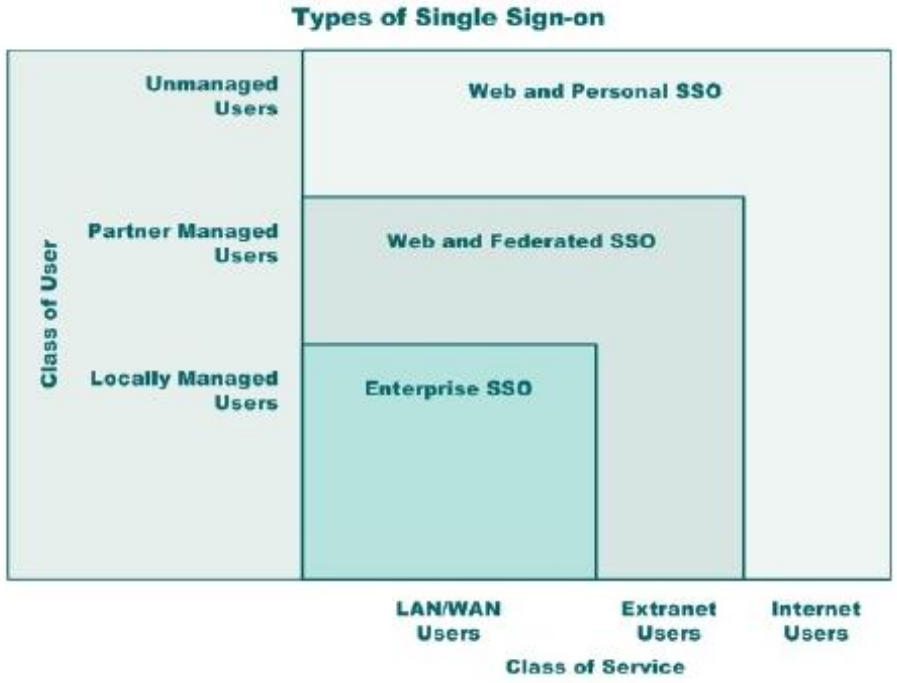
Single Sign-On - SSO

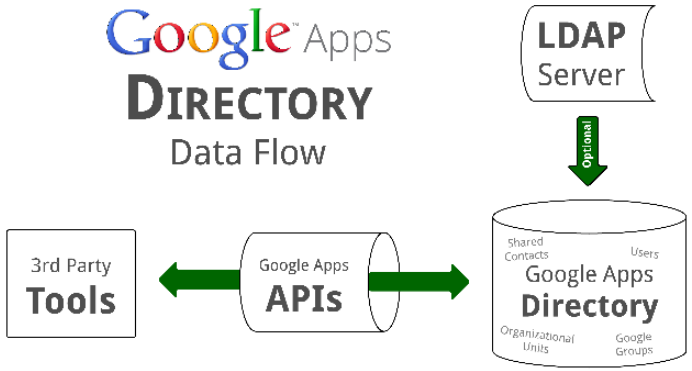
Gir tilgang til flere ulike tjenester basert på én pålogging

- Behøver **ikke** ny pålogging for hver tjeneste som skal brukes

Flere katalogtjenester tilbyr SSO

- AD DS gir SSO for alle tjenester i Windows domenet
- Feide fungerer med SSO
- Google Apps Directory
- Facebooks påloggingstjeneste

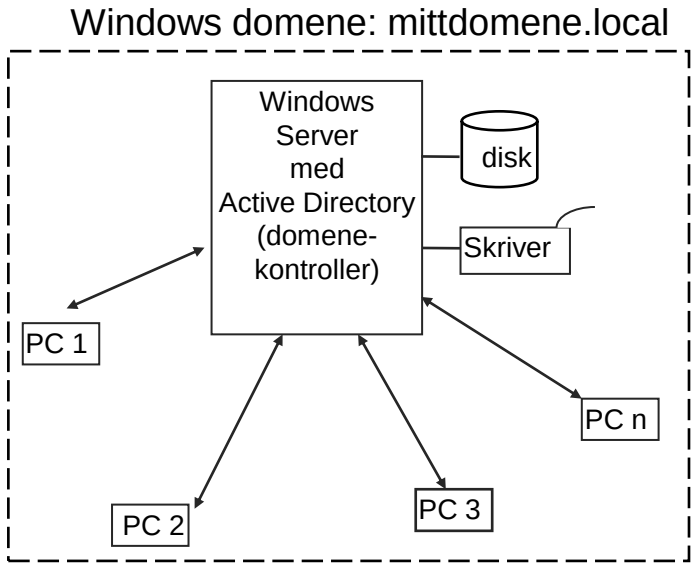




Windows domener

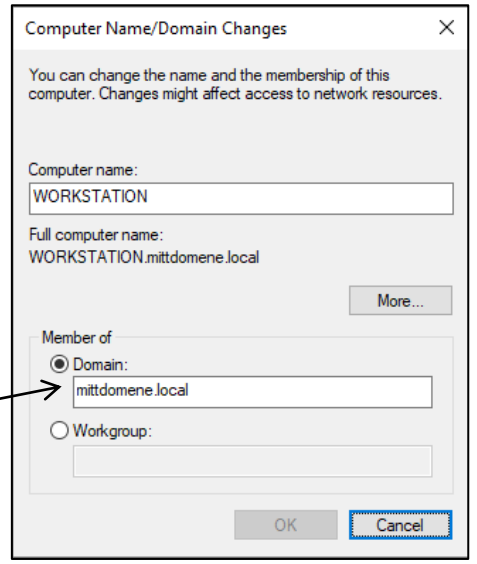
En samling av alle maskiner i nettet

- En tjenermaskin er domenekontroller
  - » Har én felles brukerdatabase (Active Directory - AD)
  - » Lagrer informasjon om alle maskiner i domenet
  - » Styrer tilgang til alle maskiner / ressurser i domenet
- Andre maskiner er **medlemmer** av domenet:
  - » Alle klientmaskiner
  - » Andre tjenere som ikke er domenekontroller
- Domenenavn bestemmes av domenekontrolleren



Kontroll av brukernavn og passord i domenet

- Hver bruker trenger bare én brukerkonto i domenet
- Tilgang / rettigheter til alle ressurser i domenet styres av domenekontrolleren
  - » Brukere og grupper defineres i Active Directory
  - » Alle maskiner må meldes inn i domenet
  - » Kontroll av brukernavn og rettigheter gjøres av AD



Windows domenenavn og DNS

Windows domener bruker DNS som navnetjeneste

- En DNS tjener må installeres sammen med AD
- DNS holder oversikt over domenenavn, maskinnavn og deres IP-adresser

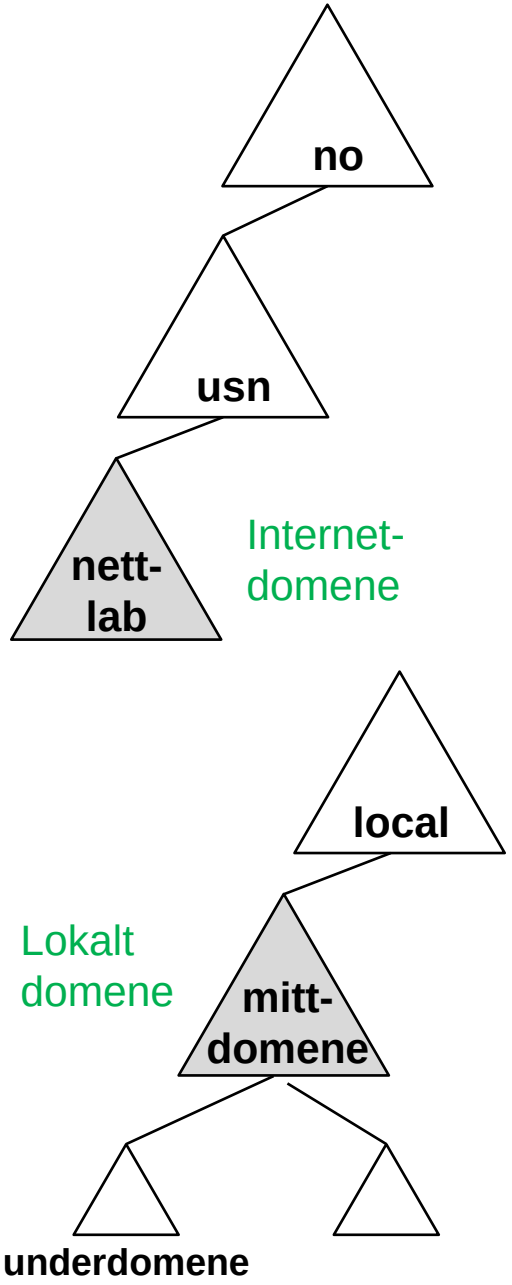
Domenenavn for Windows domener

- **Internett-domener**
  - » Windows-domener kan være underdomene av DNS-domener i Internett
  - » Domenenavn må da være del av Internetts hierarkiske navnesystem

    Eksempel: **nettlab.usn.no**
- **Lokale domener**
  - » Windows domener behøver ikke ha kobling til Internetts DNS-domener
  - » Domenet **kan** da være underdomene av det uoffisielle **.local** domenet

    Eksempel: **mittdomene.local**
  - » Brukes til "lukkede" Windows domener i lokalnett som ikke har Internett-domene
  - » Man kan fremdeles lage underdomener i AD

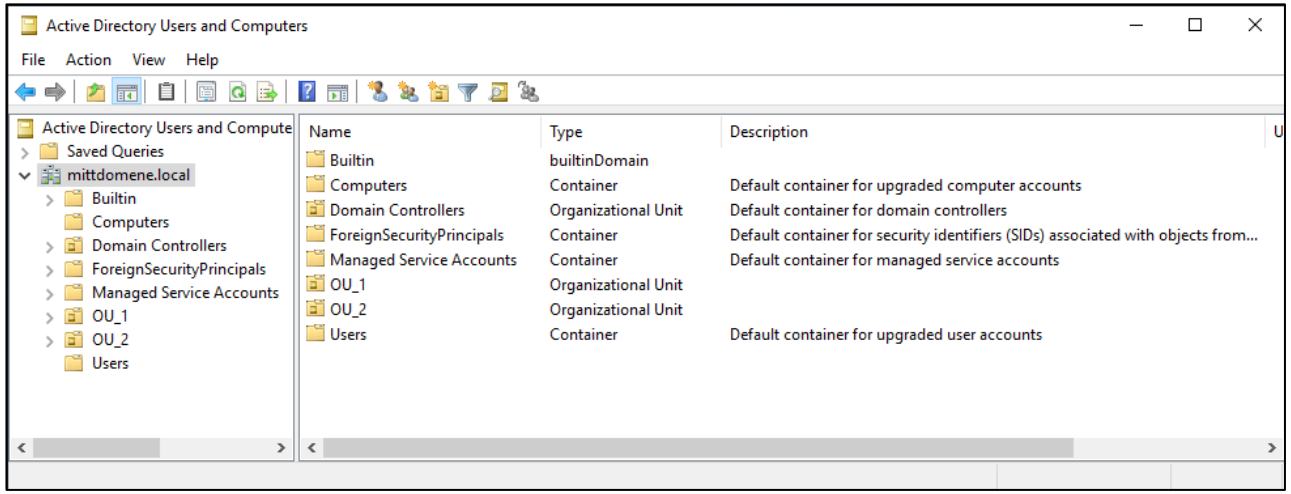
    Eksempel: **underdomene.mittdomene.local**



AD databasen består av objekter

Objekttyper

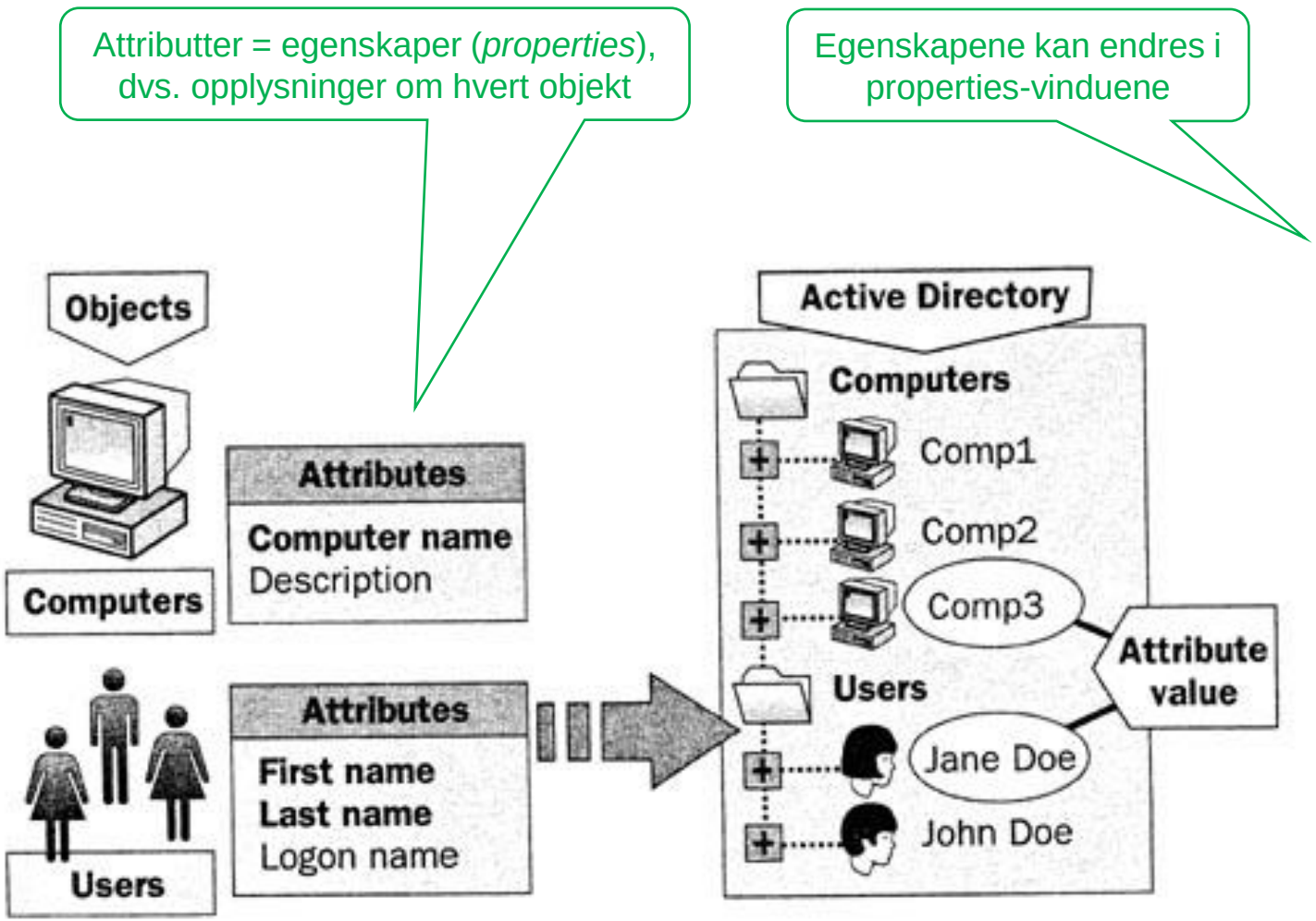
- Brukerkontoer (*Users*)
- Grupper (*Groups*)
- Kontakter (Contacts)
- Datamaskiner (*Computers*)
- Doménekontrollere (*Domain Controllers*)
- Skrivere (*Printers*)
- Delte mapper (*Shares*)
- Domenekontrollere (Domain controllers)
- Organisasjonsenheter (OU = Organizational Unit)
- m.fl.

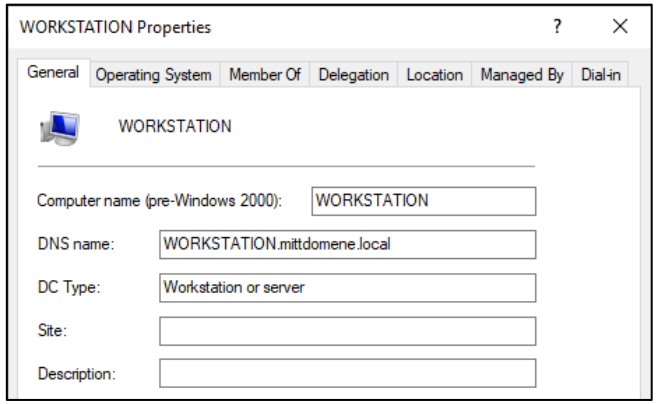


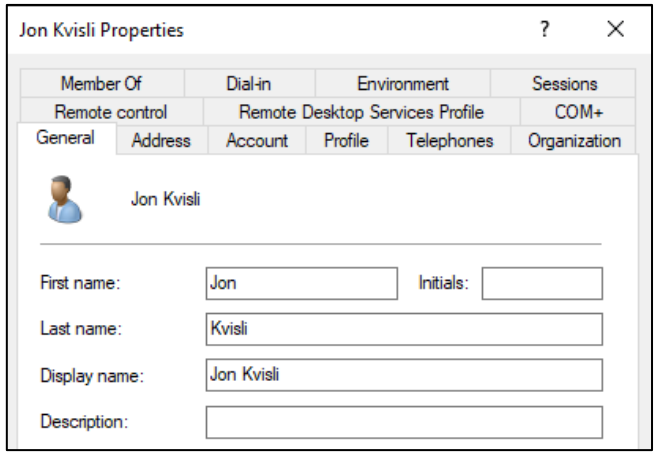
AD skjema (*Schema*) = formell definisjon av objektene ("klassedefinisjon")

- Beskriver hvilke egenskaper (attributter) som skal lagres for hvert objekt
- AD DS installeres med et "standard" skjema
- Det er mulig å lage nye, egendefinerte objekttyper (avansert systemadministrasjon!)

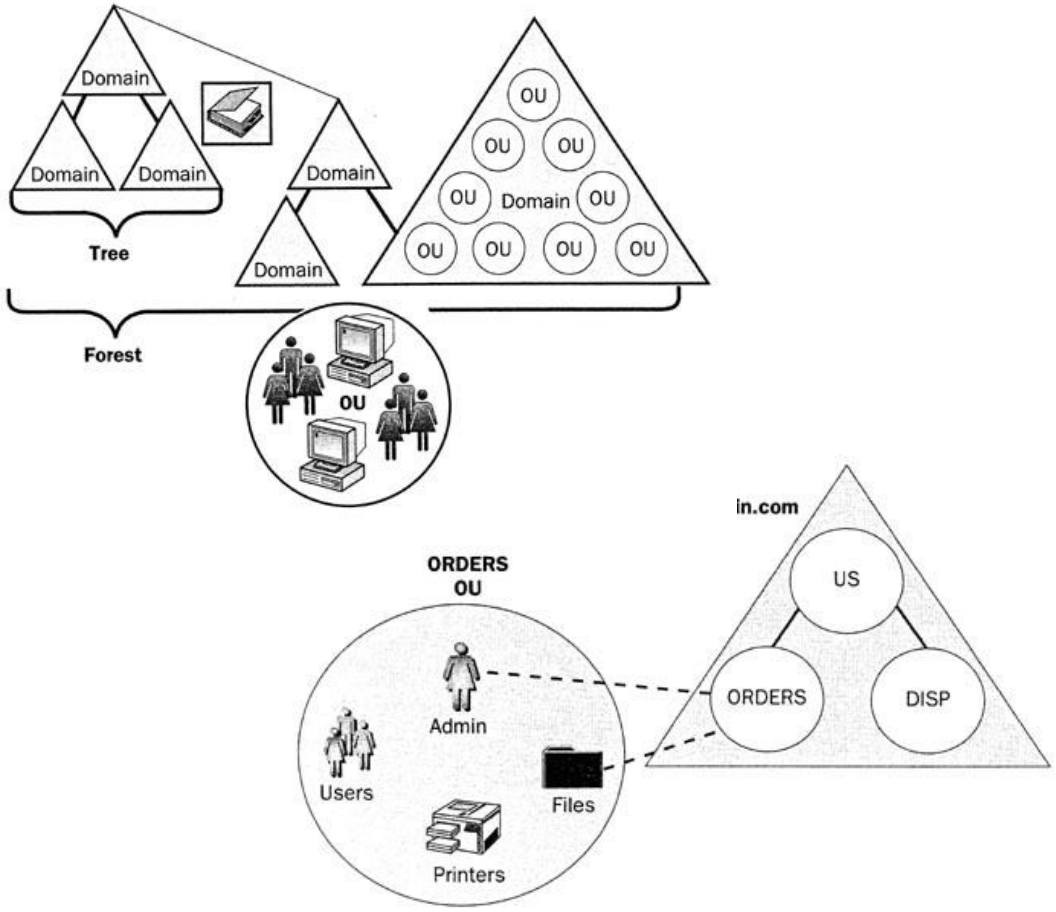
AD objektene har egenskaper (attributter)







Organisering av Windows domener



I små/middels store nett holder det med ett domene.

Trær og skoger er for store organisasjoner/nett

Domene

- En samling av maskiner, brukere og ressurser som "hører" logisk sammen
- Styres av en domenekontroller

Tre

- Et hierarki av domener i flere nivåer, med **felles** rotdomene

Skog

- En samling av flere trær uten felles rotdomene.
- Dvs. flere uavhengige domenetrær

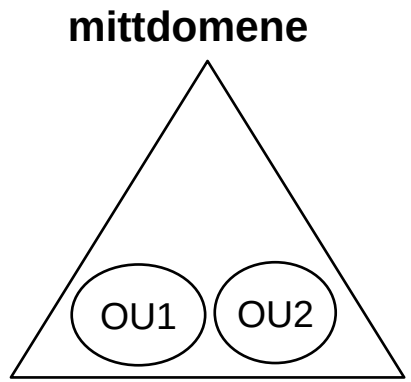
OU (Organizational Unit)

- Objekttype som "samler" brukere, grupper, maskiner, m.m.
- Brukes for å delegere brukeradministrasjon
- Ett domene kan ha flere OU'er

Oppdeling av domene i OUer

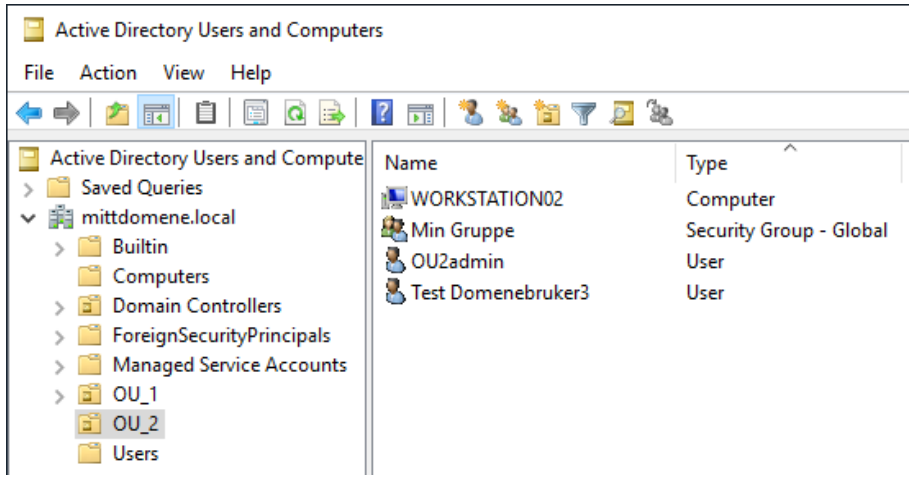
OU (Organizational Unit) =

- Et ”containerobjekt” som samler flere samhørende objekter
- Kan inneholde:
  - » Brukerobjekter
  - » Datamaskinobjekter
  - » Andre AD objekter, f.eks. grupper
- Ett domene kan ha flere OU’er
- Hver OU samler ofte objekter som tilhører samme organisasjonsenhet (avdeling)



Hvorfor OUer?

- Hensiktsmessig i store domener, for å dele dem i mindre administrative enheter
- Administrasjon av en OU kan delegeres til andre brukere
- Fordele administrasjonsarbeidet på flere



Fordeler med AD og domener

For brukeren

- Én brukerkonto / passord å forholde seg til
- Samme brukerkonto kan gi tilgang til alle ressurser i nettet
- Ressurser kan "publiseres" slik at de er lett synlige for bruker

For administrator

- Sentralisert brukeradministrasjon
- Én brukerdatabase
- Administrasjon kan delegeres til flere

Driftsmessig

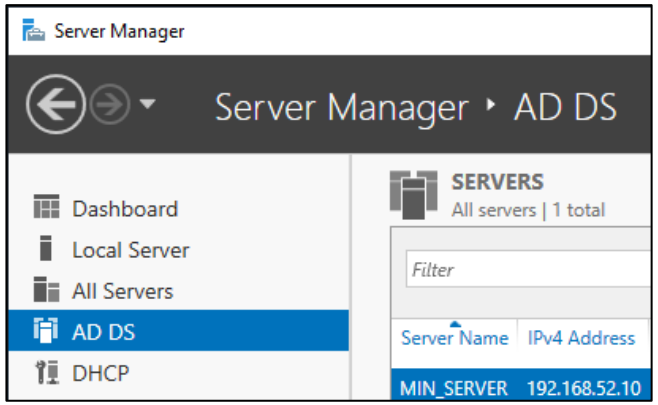
- domenet er skalerbart
  - » Dvs. antall brukere og maskiner kan vokse til store tall uten at dette gir nye problemer eller mye ekstraarbeid

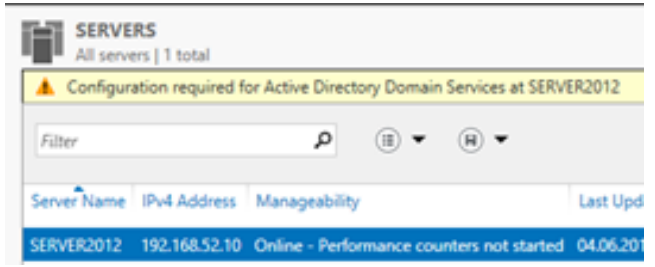
Sikkerhetsmessig

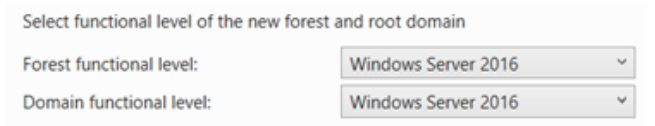
- All tilgang til nettet autentiseres og autoriseres av én tjener
- Bedre kontroll på brukeradministrasjon og rettigheter

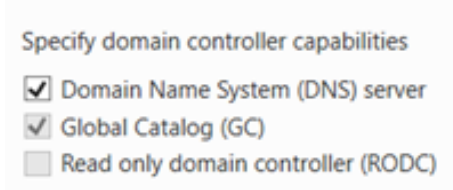
Etablering av domene og domenekontroller

1. **Tjeneren må ha fast (statisk) IP-adresse**
   - Setter sin egen adresse som primær DNS tjener hvis DNS kjøres på domenekontrolleren
2. **Installer tjenerrollen *Active Directory Domain Services***
   - og administrasjonsverktøy i **Tools** menyen
3. **Konfigurere AD DS (med *dcpromo.exe*)**
   - Nytt domene eller ny domenekontroller i eksisterende domene?
   - *Functional levels* - kompatibilitet
     - » Velg det nivået som samsvarer med Windows Server versjonen på domenekontrolleren (DCen)
     - » Hvis domenet har flere DCer velger du eldste Windows Server versjon som benyttes av noen DC i domenet
   - DNS-tjener
     - » DNS-tjener må installeres sammen med AD DS (hvis du ikke har en DNS-tjener allerede)

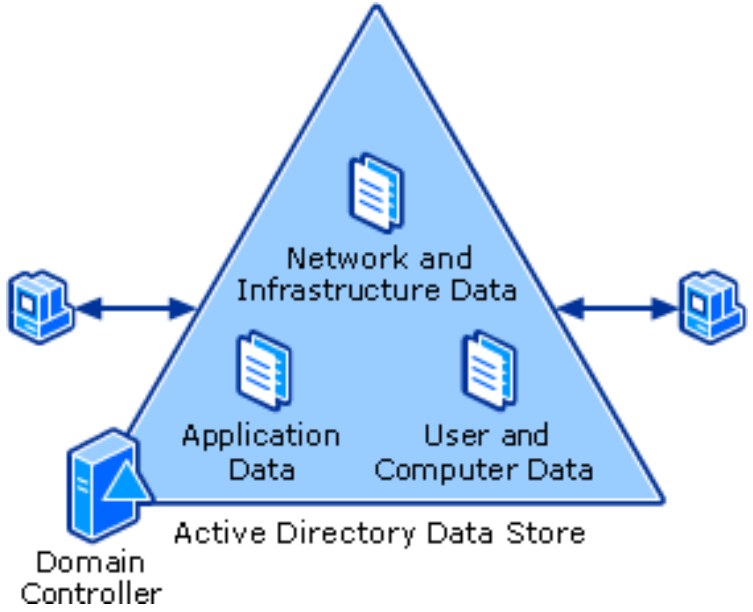


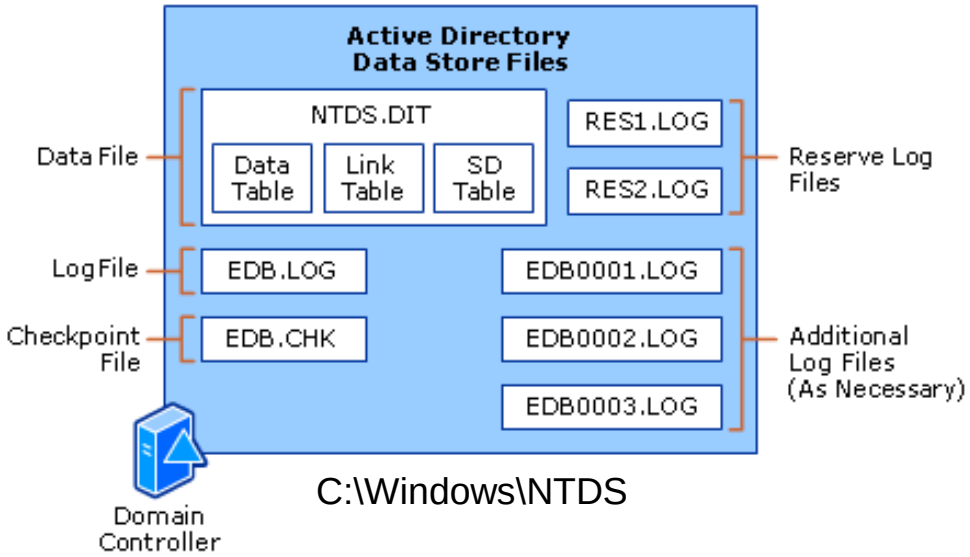






AD databasen (AD Data Store)





C:\Windows\NTDS

Tre typer data

- User and Computer Data
- Network and Infrastructure Data
- Application Data

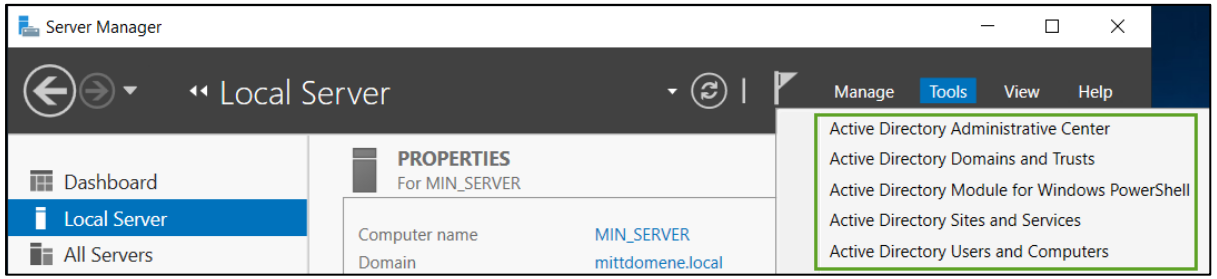
Lagres i mappen: C:\Windows\NTDS

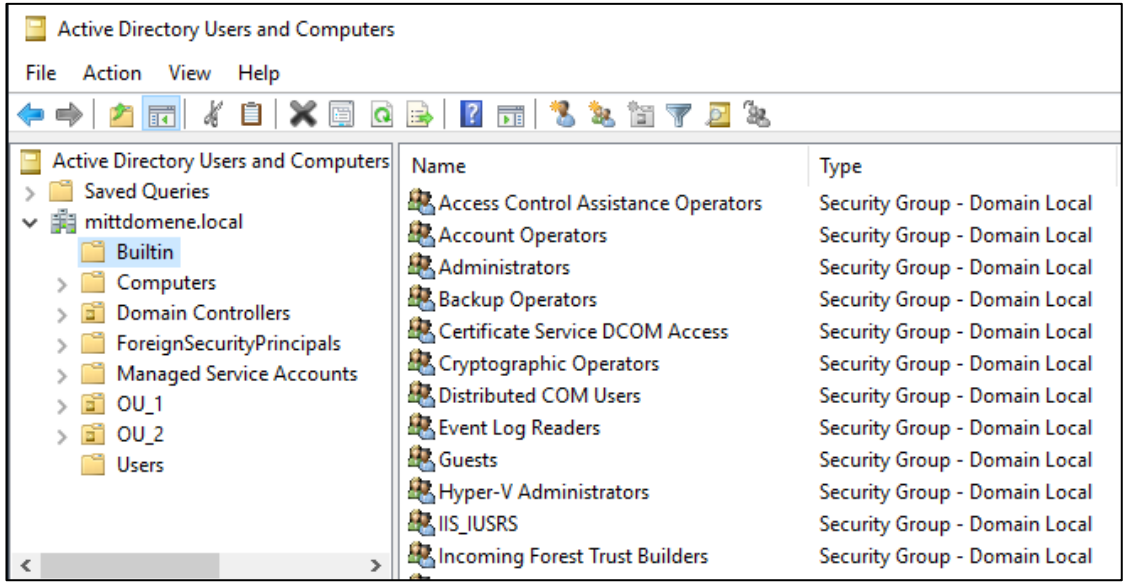
Component	Description
NTDS.DIT	The physical database file in which all directory data is stored. This file consists of three internal tables: the data table, link table, and security descriptor (SD) table.
EDB.LOG	The log file into which directory transactions are written before being committed to the database file.
EDB.CHK	The file that is used to track the point up to which transactions in the log file have been committed.
RES1.LOG, RES2.LOG	Files that are used to reserve space for additional log files if EDB.LOG becomes full.

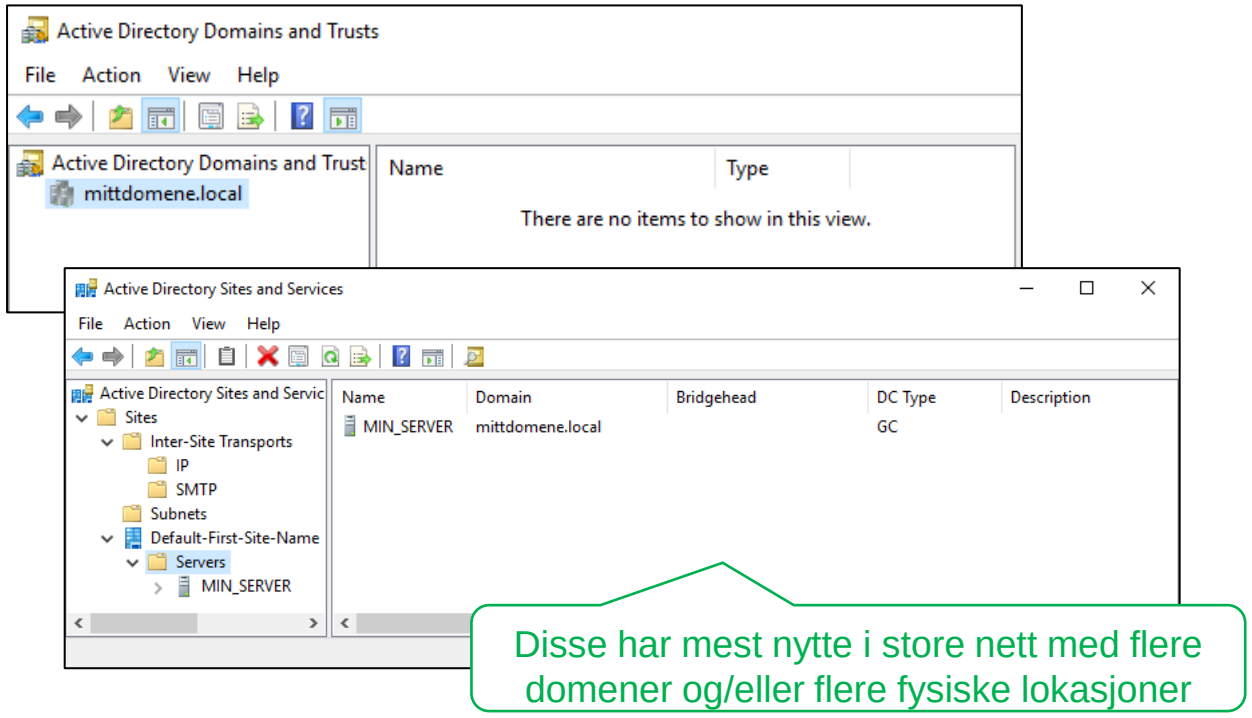
Demo: Administrasjonsverktøy i AD DS

Server Manager - Tools

- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Sites and Services
- Active Directory Users and Computers







Disse har mest nytte i store nett med flere domener og/eller flere fysiske lokasjoner

Melde en maskin inn i et Windows domene

Maskiner som skal være medlem må meldes inn i domenet

- Domenekontrollere meldes inn automatisk når de lages
- Andre maskiner må meldes inn manuelt

Dette kan gjøres fra hver maskin/klient:

- Under *System Properties* og fanen *Computer Name* bruker du knappen **Change** slik at du får opp vinduet til høyre.
- Endre feltet *Member of* fra *Workgroup* til **Domain** og skriv inn navnet på Windows-domenet
- Oppgi brukernavn og passord til en domene-konto med administrative rettigheter i domenet.