Windows konsepter

- Et windows nettverk kan *logisk* inndeles i workgroups (arbeidsgrupper) eller domains (domener)
- Workgroup
  - Deling av ressurser i nettverk.
- Passer bra for et begrenset antall systemer
  - Medlemmer:
    - NT/2000 workstations, Windows95, Windows 3.x, MS/DOS
- Domain
  - For større nettverk
  - Krever minst en Windows NT/2000 tjener
  - Active Directory – nytt med Windows 2000

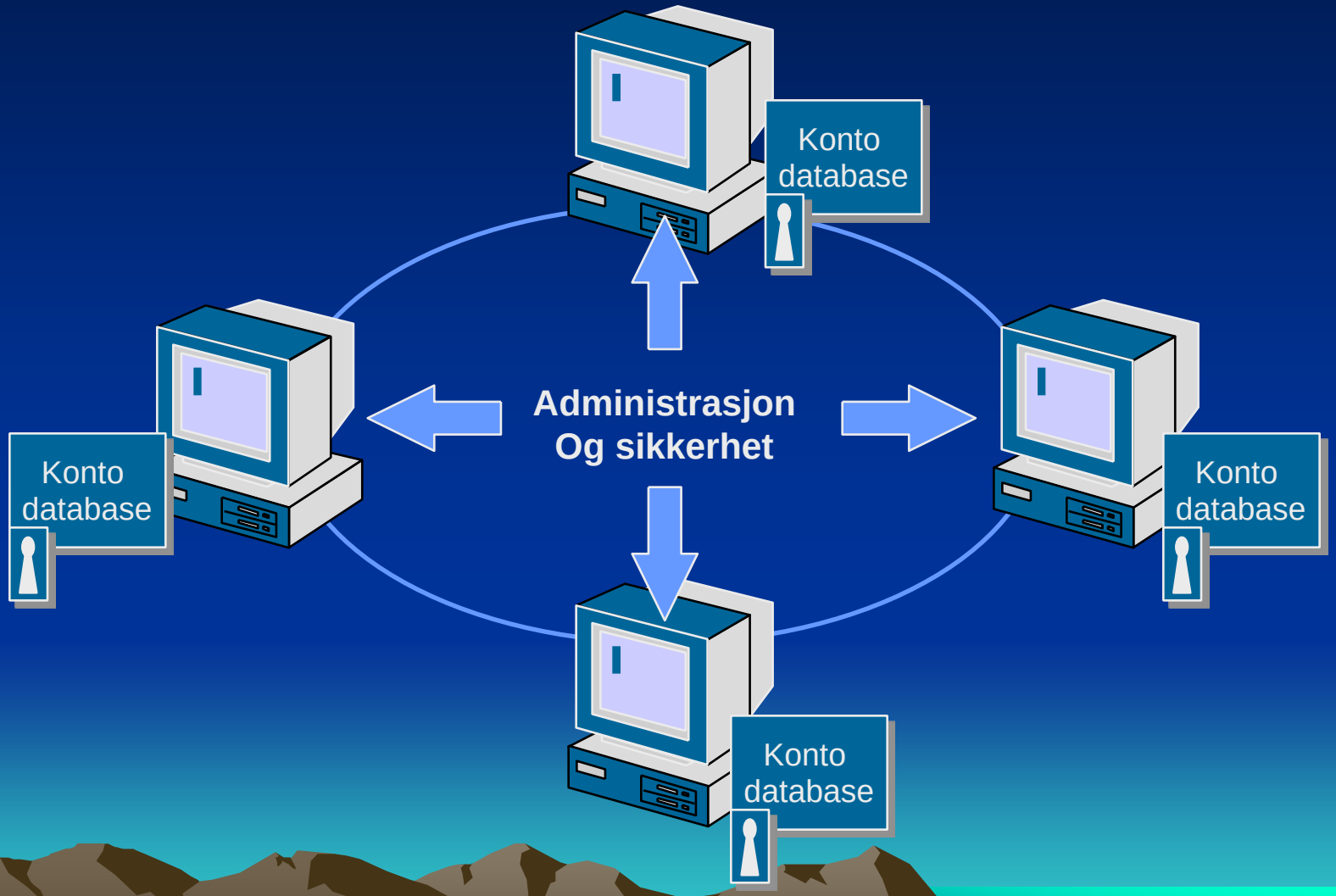
Windows konsepter

- Workgroup fordeler
  - Enkelt, billig
  - Lett å dele ressurser
  - Passer for små nettverk
  - En NT workstation kan fungere som en filtjener for W95, W3.x, DOS klienter
    - Gir NT filsystem sikkerhet (NTFS) – beskyttelse av filer og kataloger

Windows konsepter

- Workgroup ulemper
  - Hvert system har egne brukerkontoer, administrasjon og sikkerhetspolitikk
  - Ingen sentral administrasjon av brukere og ressurser
  - Brukerkontoer må dupliseres på systemene
  - Vanskelig med oversikt

Workgroup


Konto
database
Konto
database
Administrasjon
Og sikkerhet
Konto
database
Konto
database

Windows konsepter

- Domain
  - Sentralisert administrasjon og sikkerhet
  - Samme sikkerhetspolitikk i hele domene
- Medlemmer:
    - Windows XP, Vista, 7, 2000
    - Windows NT, 2000/2003/2008 tjenere
  - Medlemmer har logon sikkerhet og beskyttelse av egne ressurser

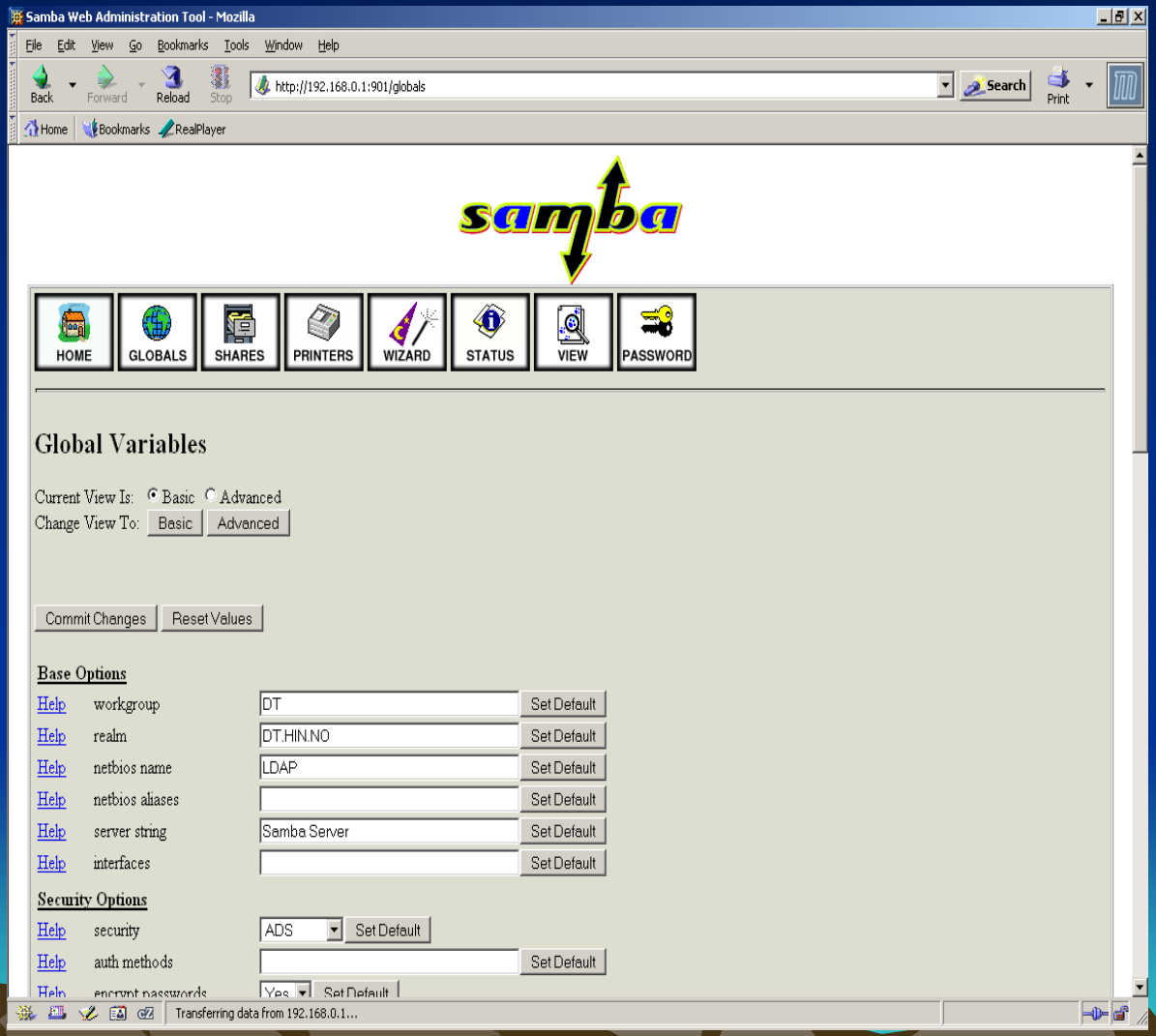
Windows konsepter

- Domain forts.
  - Klienter (ikke medlemmer):
    - Windows95/98/ME, Windows 3.x, MS-DOS
    - LAN Manager 2.x tjenere og klienter, OS/2 og Unix
    - Novell Netware klienter, Macintosh

Samba

- Integrasjon mellom Windows og Unix
  - Unix system kan delta i Windows nettverk
    - som klient – får tilgang til ressurser fra Win tjenere
      - filer, skrivere, autentisering
    - som tjener – tilbyr ressurser til win klienter
      - filtjener
      - skrivertjener
      - autentisering av klienter
  - Unix system kan fungere som Windows tjener
    - V2.2 kan fungere Windows NT 4.0 PDC
    - V3.0 kan fungere som Win2k ADS tjener

swat

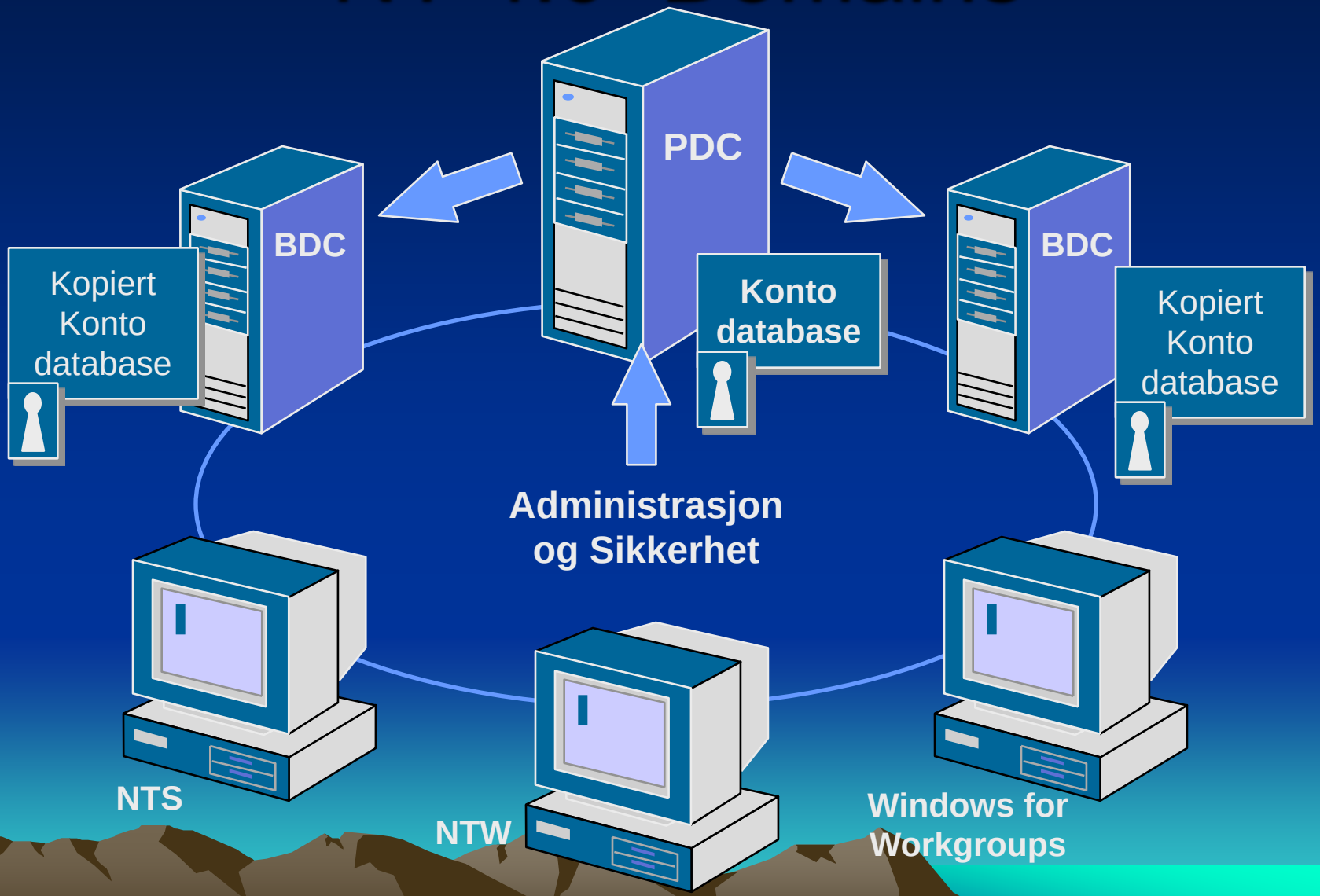


- web grensesnitt for admin av sambatjener
- Installeres sammen med samb
- avslått som standard, må aktiveres

Windows NT 4.0 konsepter

- Window NT 4.0 og Windows 2000 domener er svært forskjellige
- Windows NT 4.0 domener
  - Minst en Primary Domain Controller (PDC) må alltid være opp og kjøre i et domene
  - PDC er alltid en Windows NT tjener
  - PDC oppgaver:
    - Har master kopi av *Directory database.* Denne inneholder all sikkerhets- og brukerinformasjon for domenet
    - Validerer innloggingsforespørsler fra bruker

NT 4.0 Domains



NT 4.0 typer domene kontrollere

- Primary Domain Controller (PDC)
  - Første system som installeres i et domene
  - Har master av *Directory Database*
  - Validerer brukere
- Backup Domain Controller (BDC)
  - Har en kopi av *Directory Database*
  - Validerer brukere
- Server
  - Fil, utskrifts- og applikasjons tjener

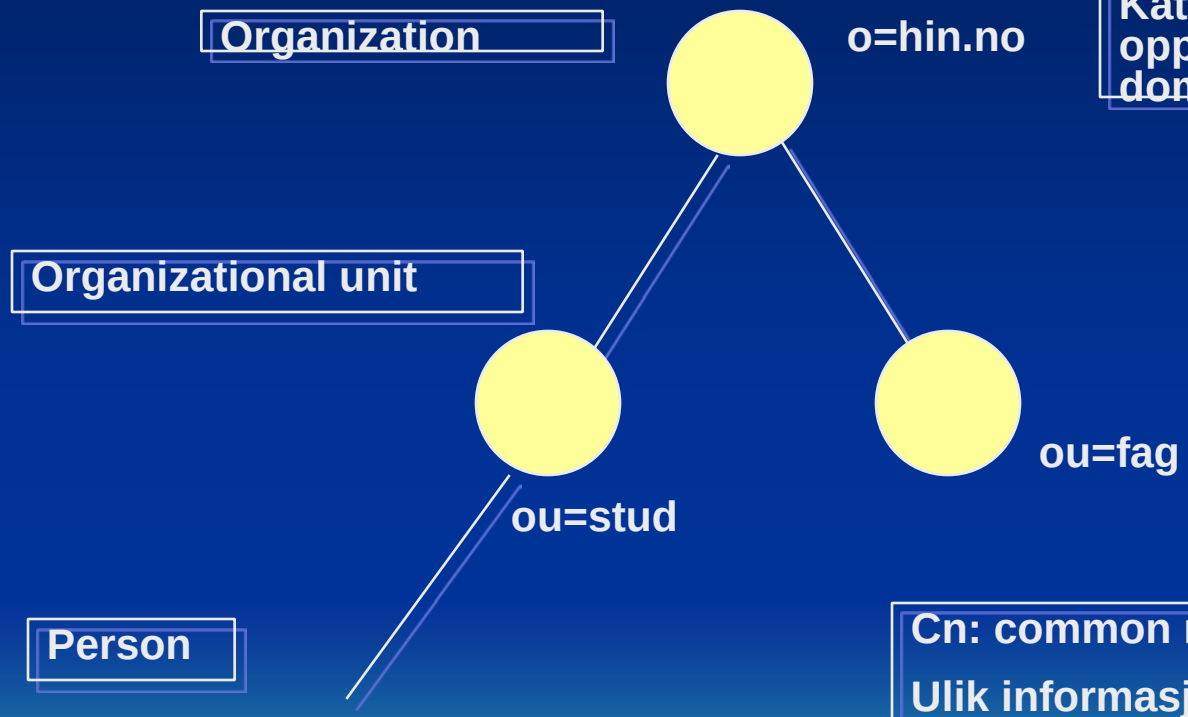
Katalogtjenester

- En katalogtjeneste er en spesialisert database optimalisert for lesing og søking etter informasjon.
- Tilbyr filtrering og rask respons på oppslag
- Skal kunne håndtere et stort volum oppslag, oppdateringer er mer sjelden og av enkel type
- Tilbyr ikke avanserte tjenester som en tradisjonell database, for eksempel transaksjoner
- Databasen kan distribueres på flere tjenersystemer
- LDAP er en protokoll for oppslag i en katalogtjeneste

LDAP

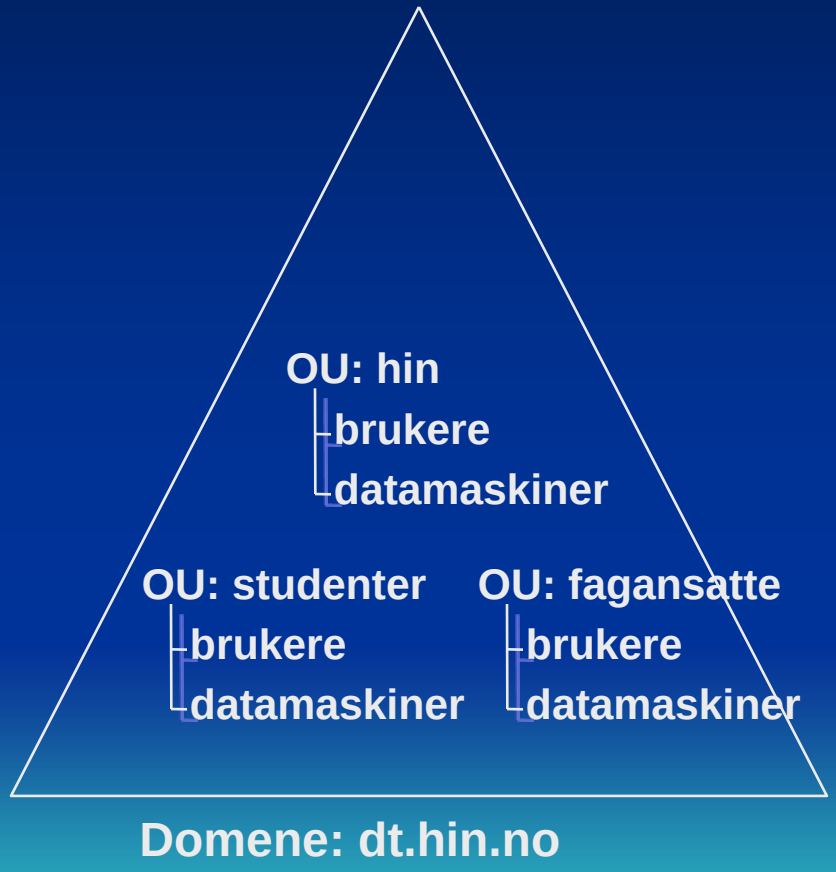
- I LDAP er katalogposter organisert i en hierarkisk tre struktur
  - Katalogtjenesten lagrer informasjon om ulike typer objekter som :
    - Brukere, brukergrupper, datamaskiner, skrivere, filer og enheter
  - LDAP har metoder for å lagre og finne objekter i katalogen
  - Objekter har egenskaper og Aksess Kontoll Lister (ACL)
  - Objekter kan organiseres i *containere* for strukturert lagring, lettere gjenfinning og delegert kontroll
  - OpenLDAP, open source implementasjon
  - Active Directory, Microsoft's utgave som benyttes i Windows 2000/2003/2008

LDAP katalog tre



Active Directory (AD) struktur

- Domene skoger (Forests)
  - Trær (Trees)
    - Domener
      - Organizational Units (OU)
        - Brukere
        - Datamaskiner
        - Grupper



AD struktur

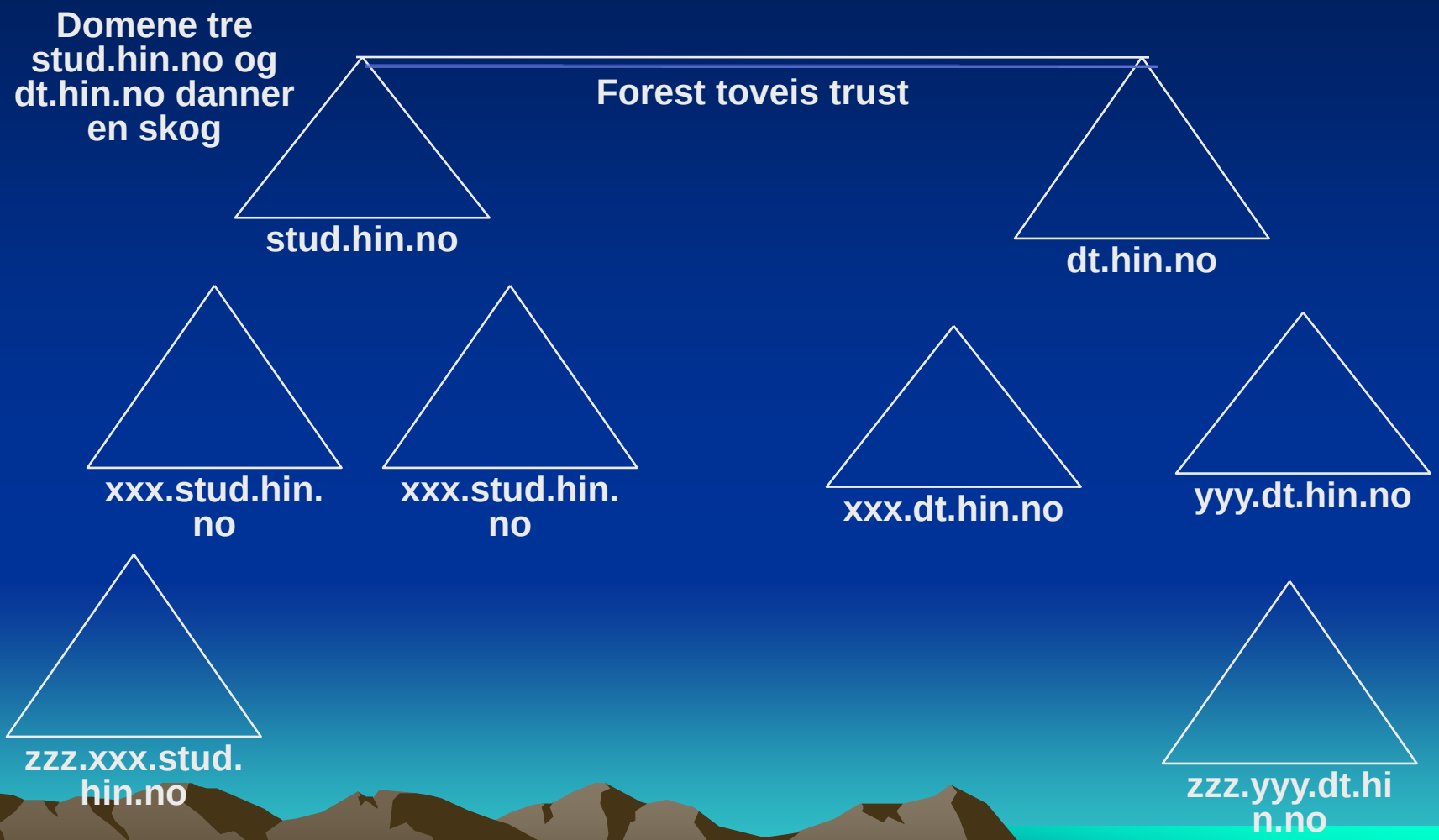
- AD benytter DNS som navnetjeneste
  - DNS navn for firma/bedrift benyttes ofte som root-domene navn i *Active Directory*
- Struktur i AD avhenger av
  - Behov for delegering av myndighet
  - Inndeling i OU's for å avspeile bedriftens
    - Organisasjonen
    - Lokasjon
    - Funksjon
  - Behov for gruppe politikk vedrørende software konfigurasjon og sikkerhetsoppsett

AD struktur

Administrasjon av OU studenter kan delegeres. Egen administrator for alle objekter i denne OU.

Gruppepolitikk på et nivå arves av alle underliggende nivå. Sikkerhetspolitikk på niva OU:hin arves av OU studenter og fagansatte

Domene trær og skoger



Domene kontroller

- Windows Server med kopi av Active Directory for sitt eget domene
  - Replikeres jevnlig mellom domenekontrollere i domenet
- Erstatter PDC og BDC i Windows NT 4.0
- En eller flere domenekontrollere i domene
  - Bedret tilgjengelighet
  - Lastfordeling av bl.a. innloggingsvalideringer

webmin

- Web basert grensesnitt mot Unix/Linux system
  - konfigurasjon og oppsett av system, brukere, tjenere etc.
  - senker terskelen for administrasjon av Linux
  - Fritt tilgjengelig fra www.webmin.com
- Sikkerhet
  - *webmin* aksess må begrenses til tiltrodde nettverk, IP adresser
  - Bruk SSL for beskyttelse av brukernavn & passord

Webmin 1.100 on ldap.dt.hin.no (Redhat Linux 9.0) - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://192.168.0.1:10000/?cat=system Search Print

Home Bookmarks RealPlayer

Webmin Feedback Log Out

Webmin System Servers Networking Hardware Cluster Others

System

Bootup and Shutdown
Change Passwords
Disk Quotas
Disk and Network Filesystems
Filesystem Backup
LDAP Users and Groups
MON Service Monitor
PAM Authentication
Running Processes
Scheduled Commands
Scheduled Cron Jobs
Security Sentries
Software Packages
SysV Init Configuration
System Documentation
System Logs
Users and Groups

Version 1.100 on ldap.dt.hin.no (Redhat Linux 9.0)

Theme By MSC.Linux

Transferring data from 192.168.0.1...

Deling av ressurser

- Ressurser kan utdeles fra en Windows arbeidsstasjon eller tjener, Linux/Samba kan gjøre tilsvarende
- Ressursene blir tilgjengelige for andre nettverksbrukere
  - Brukerne kan koble seg opp mot ressursen
- Rettigheter kan settes på ressursene
- Typiske ressurser
  - Disker, Kataloger og Skrivere

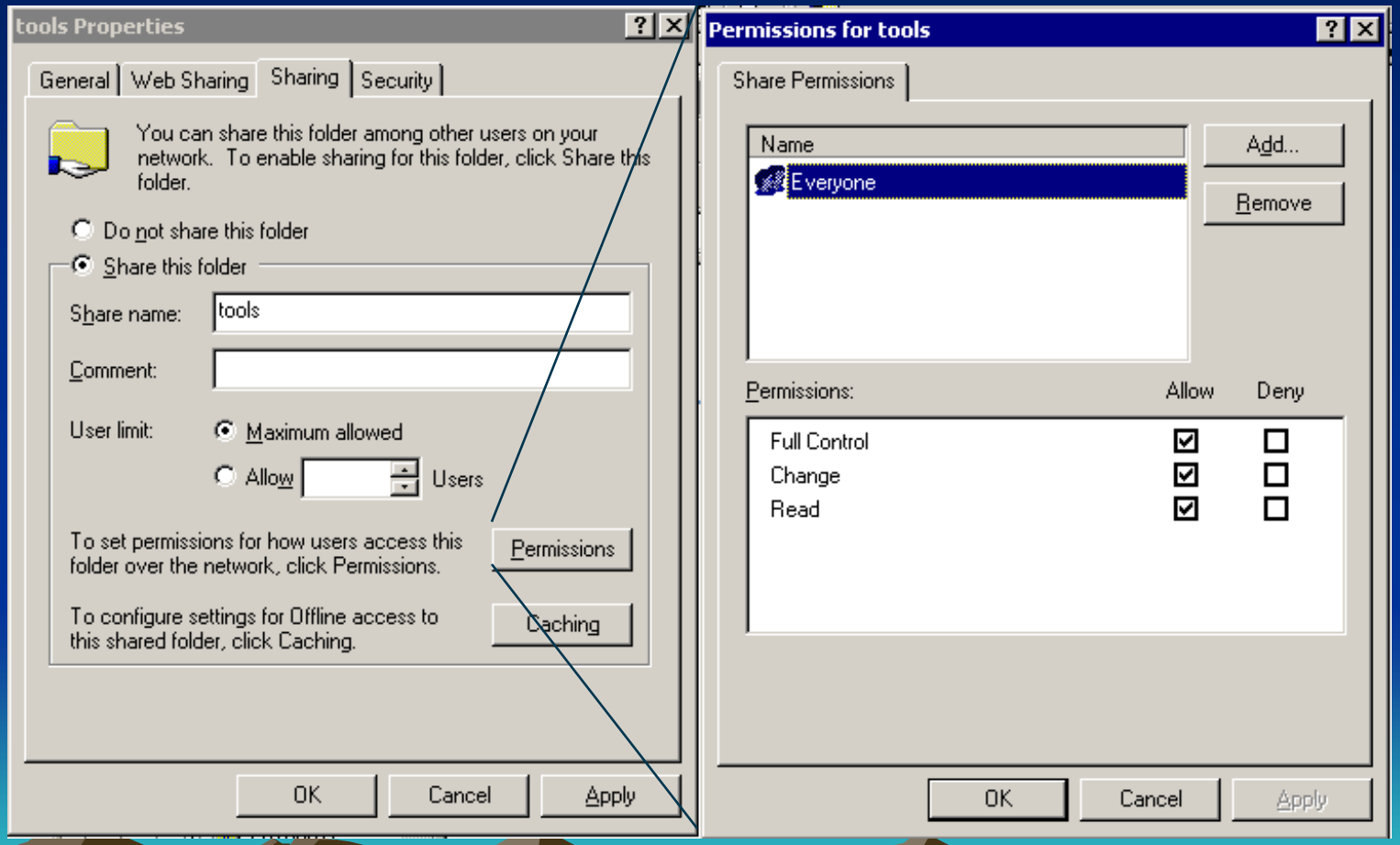
Deling av ressurser

- Disker
  - Ved deling av disker blir hele innholdet på disken tilgjengelig for nettverksbrukere
- Kataloger
  - Katalog og underkataloger med innhold blir tilgjengelig for nettverksbrukere
- Delingsrettigheter
  - Maksimal aksess for brukere som benytter en ressurs via nettverket gis ved deling av ressursen
  - Brukerne vil aldri kunne få høyere aksess en dette

Deling av ressurser

- Delingsrettigheter eksempel
  - En disk deles ut med *lese* som delingsrettighet
    - Brukere som kobler seg opp mot denne disken via nettverket vil maksimalt få les aksess mot alle kataloger og filer på denne disken
    - Selv om brukeren i NTFS har les + skriv aksess får han nå kun lese aksess
  - En disk deles ut med *Full control* som delingsrettighet
    - NTFS rettigheter nå avgjør aksess til filer og kataloger på denne disken
  - Muliggjør beskyttelse av FAT disker
    - Delingsrettighet *Lese* - maksimalt leseaksess for alle

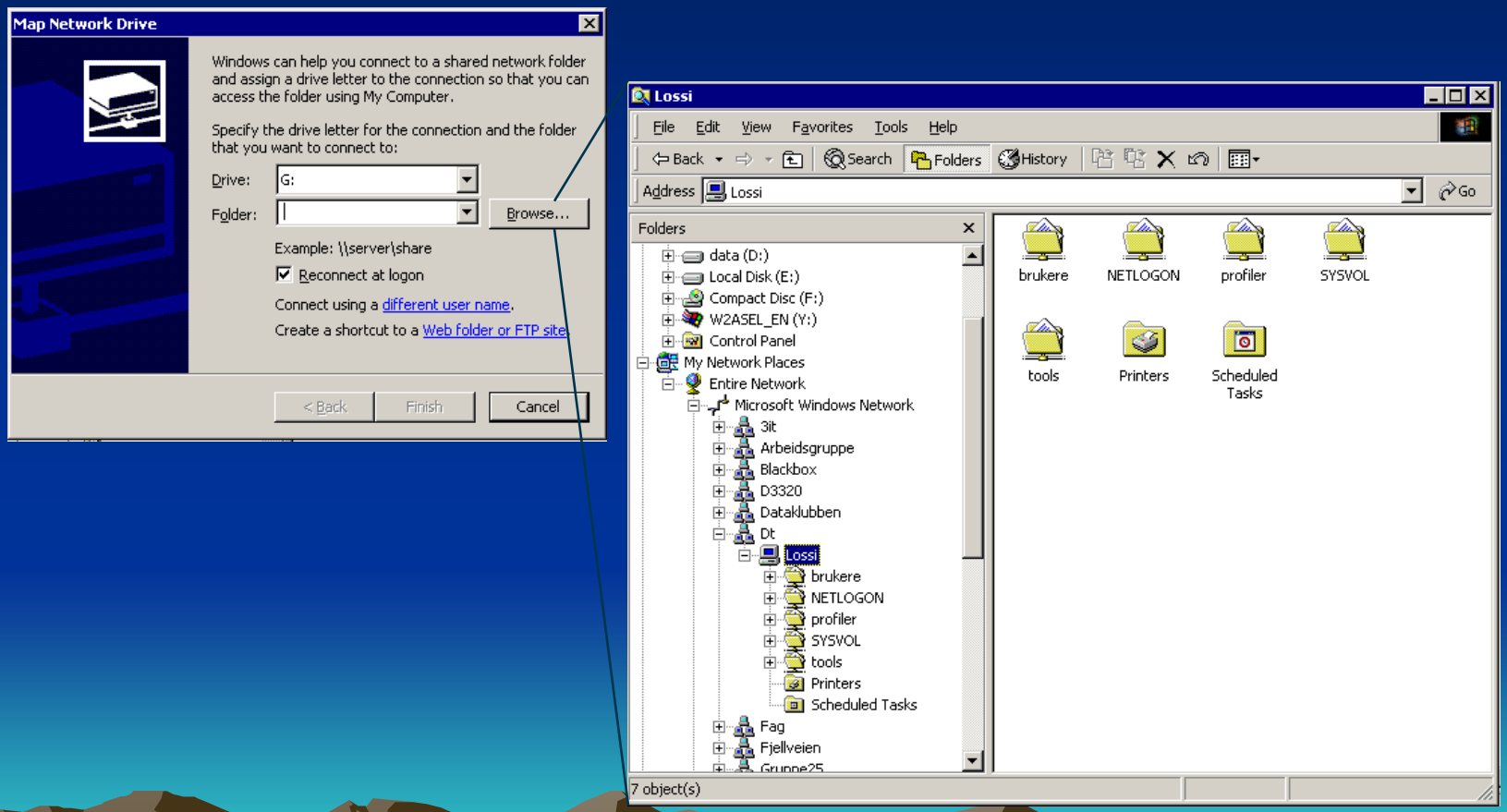
Deling av ressurser fra Windows



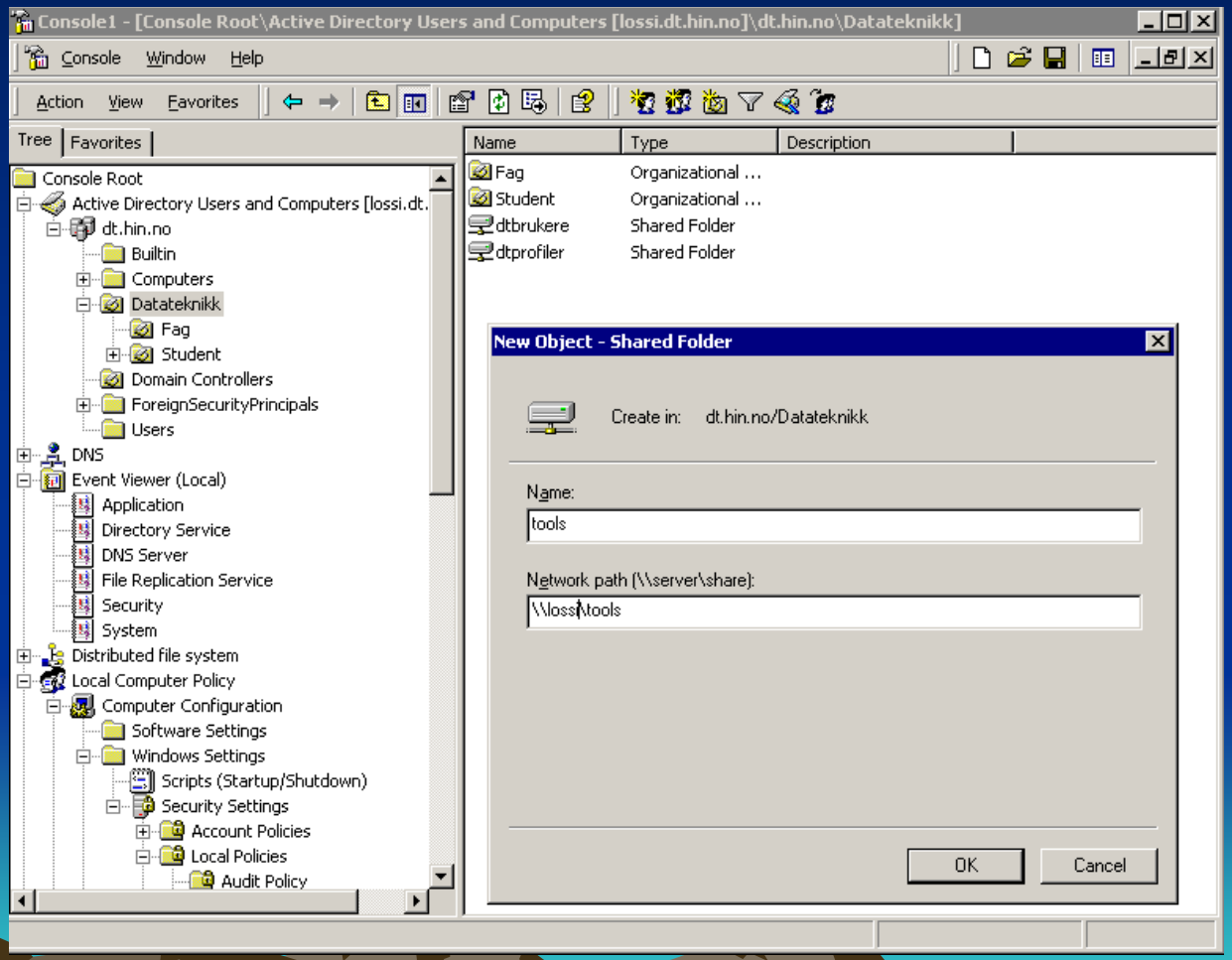
Bruk av delte ressurser

- Browsing av nettverk
  - Delt filkatalog vises under systemet som denne tilhører
- Søk i Active Directory etter ressurser med kjent navn
- Permanent oppkobling mot delte ressurser
  - Benytt Utforsker -> Map network drive
  - Viser oversikt over systemer tilgjengelig
  - Ekspander et system og en liste over delte ressurser vil vises
  - Velg den enheten du ønsker å koble deg opp mot og velg et disknavn for denne
  - Angi om dette skal skje automatisk ved neste pålogging

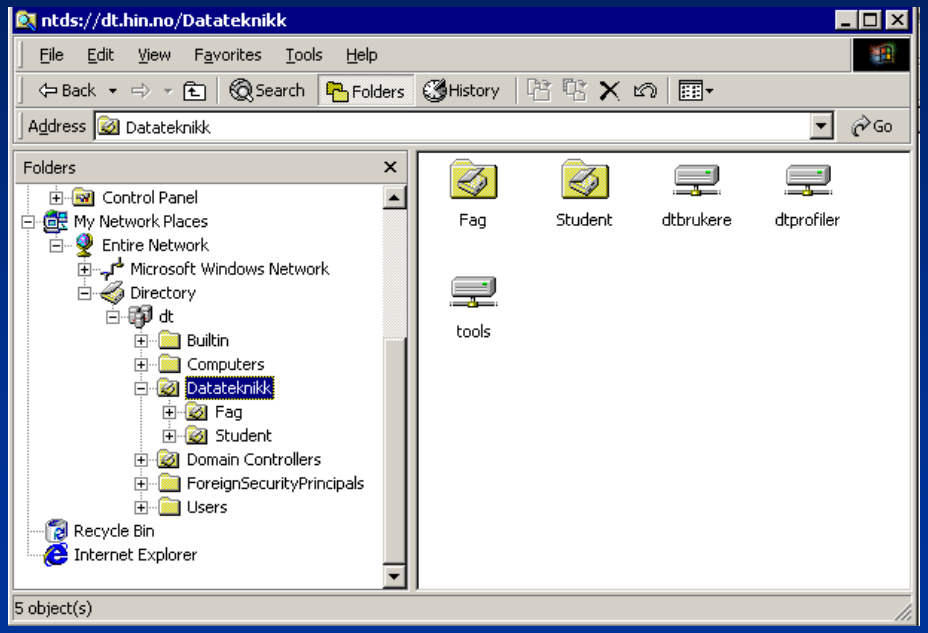
Oppkobling mot delte ressurser



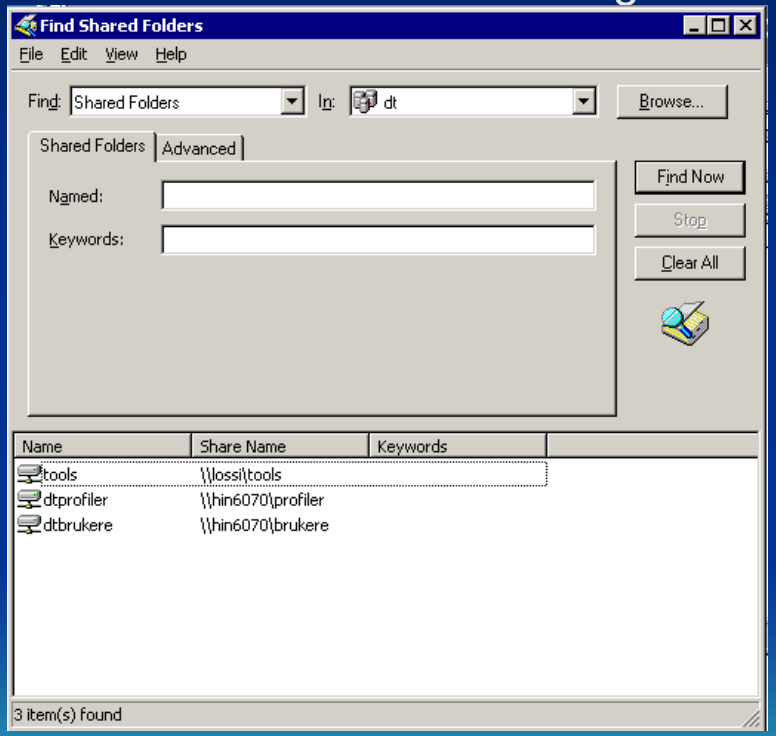
Publisering av delt katalog i Active Directory



Lokalisering av delt katalog i Active Directory



Søk i AD etter delte kataloger



Browsing i Directory dersom du vet noenlunde hvor katalogen er for eksempel i hvilket domene/OU

AD frigjør oss fra at vi må vite navnet på systemet hvor ressursen er delt !!!

Standard delte ressurser i Windows

- Delte ressurser som opprettes ved installasjon for bruk av Administratorer
  - Alle disker
    - Navn: <driveletter>$
    - f.eks. C$, D$
  - ADMIN$ - mappet til systemkatalogen
  - NETLOGON - benyttes ved innlogging på tjenere
  - PRINT$ - for deling av printere
  - REPL$
  - IPC$

Hva er SAMBA?

- Tilbyr deling av ressurser mellom Linux/Unix systemer og Windows systemer.

SAMBA historikk

- Andrew Tridgell i Digital Equipment Corporation ansvarlig for produktet PATHWORKS som gjorde det mulig å koble PC'er mot filtjenere på Digital VAX systemer.
- Videreutvikling for å kunne støtte SMB ved hjelp av revers engineering av SMB/NetBIOS protokollen ved hjelp av pakke sniffing.
- Starten på SAMBA slik vi kjenner den i dag.
- Andrew Tridgell leder fortsatt Samba utviklingen, http://www.samba.org .

TCP/IP porter i bruk

- NetBIOS nettverks browsing netbios-ns 137/tcp & udp
- NetBIOS navne tjeneste netbios-dgm 138/tcp & udp
- Fil og utskrifts tjeneste netbios-ssn 139/tcp & udp
- Port 445 benyttes av Windows 2000/XP når NetBIOS over TCP/IP er slått av
- Port 901 benyttes av SWAT
- NetBIOS tunnelert over TCP/IP gjør det mulig å route protokollen !

SMB's plass i TCP/IP modellen

<table>
<tr><td>OSI</td><td colspan="4"></td><td>TCP/IP</td></tr>
<tr><td>Application
Presentation</td><td colspan="4">SMB</td><td rowspan="2">Application</td></tr>
<tr><td>Session</td><td>NetBIOS</td><td rowspan="3">NetBEUI</td><td>NetBIOS</td><td>NetBIOS</td></tr>
<tr><td>Transport</td><td rowspan="2">IPX[1]</td><td rowspan="2">DECnet</td><td>TCP&UDP</td><td>TCP/UDP</td></tr>
<tr><td>Network</td><td>IP</td><td>IP</td></tr>
<tr><td rowspan="2">Link</td><td rowspan="2">802.2,
802.3,802.5</td><td>802.2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet or
others</td></tr>
<tr><td>802.3,802.5</td></tr>
<tr><td>Physical</td><td colspan="4"></td></tr>
</table>

Funksjonalitet

- Fil and utskriftstjenester
- Autentisering og autorisering
- Navne oppløsning
- Nettverks annonsering (browsing).

Komponenter

- Fil og utskriftstjenester utføres av smbd daemon.
- Navne oppløsning og browsing utføres av nmbd daemon.
  - Name oppløsning – kringkasting eller punkt til punkt.
  - WINS tjener.
  - Local Master Browser (LMB). Delta i valg av LMB, utføre oppgaven som LMB.
  - LMB's oppgave er å vedlikeholde en liste over tilgjengelige tjenester som vises i *Nettverksenheter*
- Autentisering mot Windows domenekontroller utføres av winbind daemon.

Sikkerhetsmodell

- Share - et enkelt passord benyttes for å aksessere en elt ressurs.
- User – hver bruker har et brukernavn og passord for aksess av delte ressurser. Brukernavn og passord lagres lokalt på SMB tjener.
- Server – Brukernavn og passord hentes fra en annen SMB tjener, Samba eller Windows, men lokale kontoer må eksistere

Sikkerhetsmodell forts.

- Domain – Samba tjener deltar i et Windows domene, brukere/passord hentes fra domene, men lokale kontoer må eksistere
  - Lokal bruker for å tilordne UID til opprettede prosesser
  - NT4 type domene kontroller
- ADS – Active Directory Server, samba tjener er med i Windows domene som native AD tjener, brukere/passord hentes fra domene
  - Benytter Kerberos

Konfigurasjon – eksempel fra filen **smb.conf**

```
[global]
   workgroup = DT
   server string = Samba Server
   hosts allow = 192.168. 127.
   hosts deny = 192.168.127.10
   printcap name = /etc/printcap
   load printers = yes
   log file = /var/log/samba/%m.log
   max log size = 0
   security = user
   encrypt passwords = yes
   smb passwd file = /etc/samba/smbpasswd
```

- Samba tjener oppsett for Windows arbeidsgruppe
- Utførlig dokumentasjon på: http://www.samba.org/

Konfigurasjon – hjemmeområder og delte områder

Hjemmeområder for brukerne

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
valid users = %S
path = /home/%S
```

Angir om ressurs vises ved nettverks browsing

Delingsnavnet settes lik brukernavnet, kun tilgang for bruker

Fellesområde med begrenset aksess:

```
[felles]
   comment = Fellesområde
   path = /home/felles/
   browseable = yes
   writeable = yes
   guest ok = no
   valid users = @teachers
```

Må ha gyldig bruker for aksess, brukere må være I brukergruppen teachers

Eksempler

smbclient – en ftp lik klient som kobler seg opp mot en Samba tjener

```
smbclient //milkyway/homes -U jdoe
Password:
Domain=[SOHO-SMB] OS=[Unix] Server=[Samba 2.2.4]
smb: \> help
```

smbmount/mount – montering av en Samba ressurs over SMB

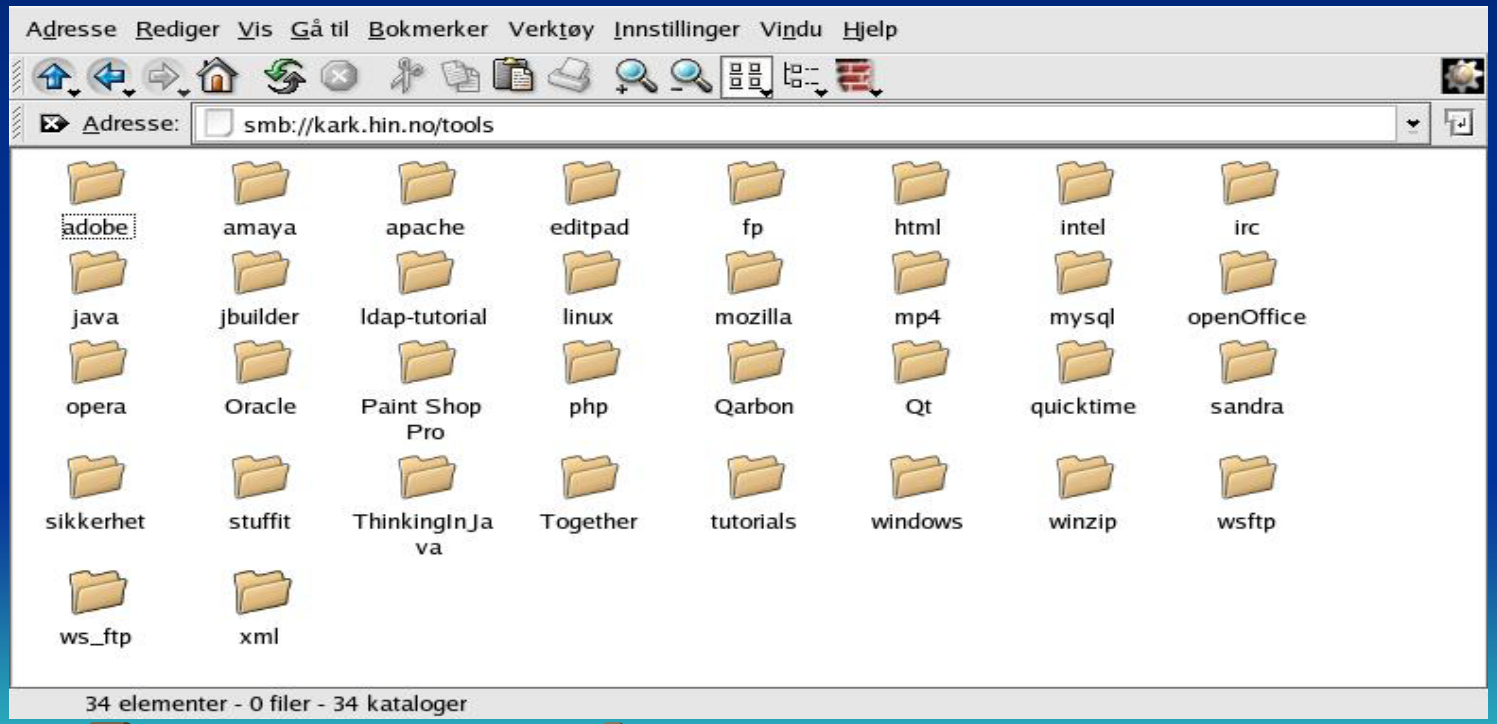
```
mount -t smbfs -o username=kc //limbo.hin.no/kc
                                          /home/kc/minefiler
Password:
```

Mount.cifs – montering av en Samba ressurs over CIFS

```
mount.cifs //kark.hin.no/kc /home/kc/minefiler -o user=kc
Password:
```

Konquerer

SMB ressurser kan akkseseres direkte fra Konquerer nettleser, adresse *smb://systemnavn/ressurs*

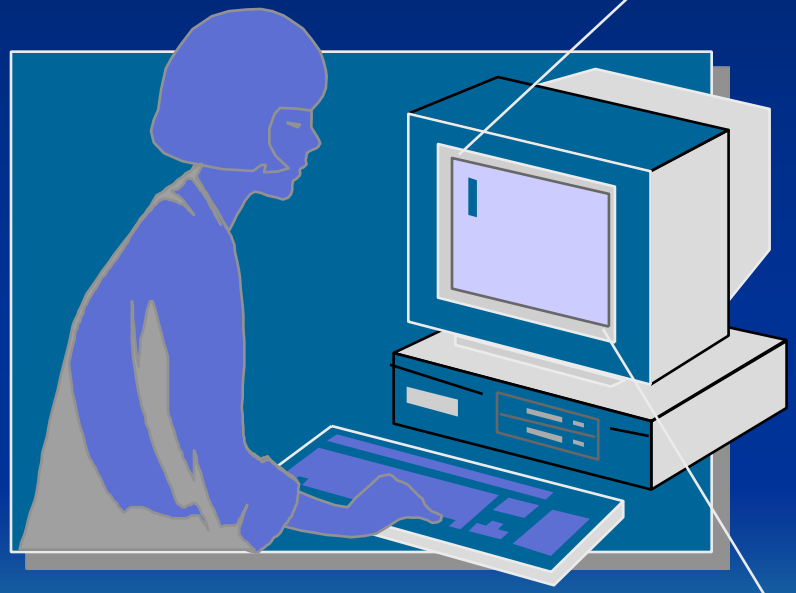


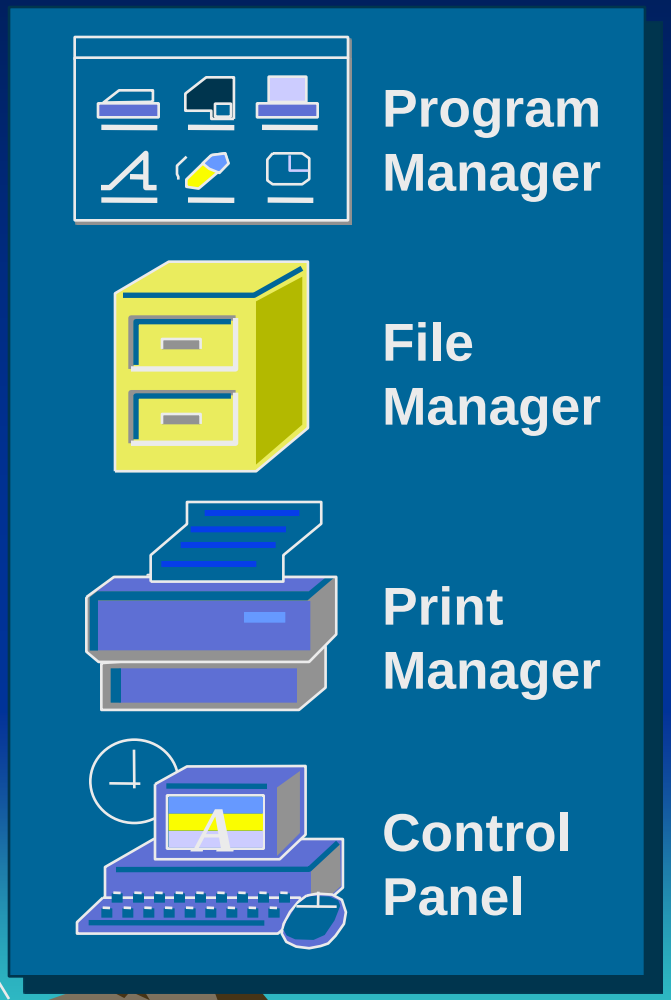
Domene brukere

- Domene brukere opprettes i Active Directory
  - Gir aksess til ressurser i domene/domene tre/skog
  - Brukere opprettes i OU etter tilhørighet
  - Innlogging mulige i hele domenet
  - Ressurser i domenet tilgjengelig for bruker basert på brukerens aksess token (SAT) og Aksess kontroll lister (ACL) på ressurser
    - *security access token (SAT)* består av SID, brukergrupper og rettigheter til brukeren

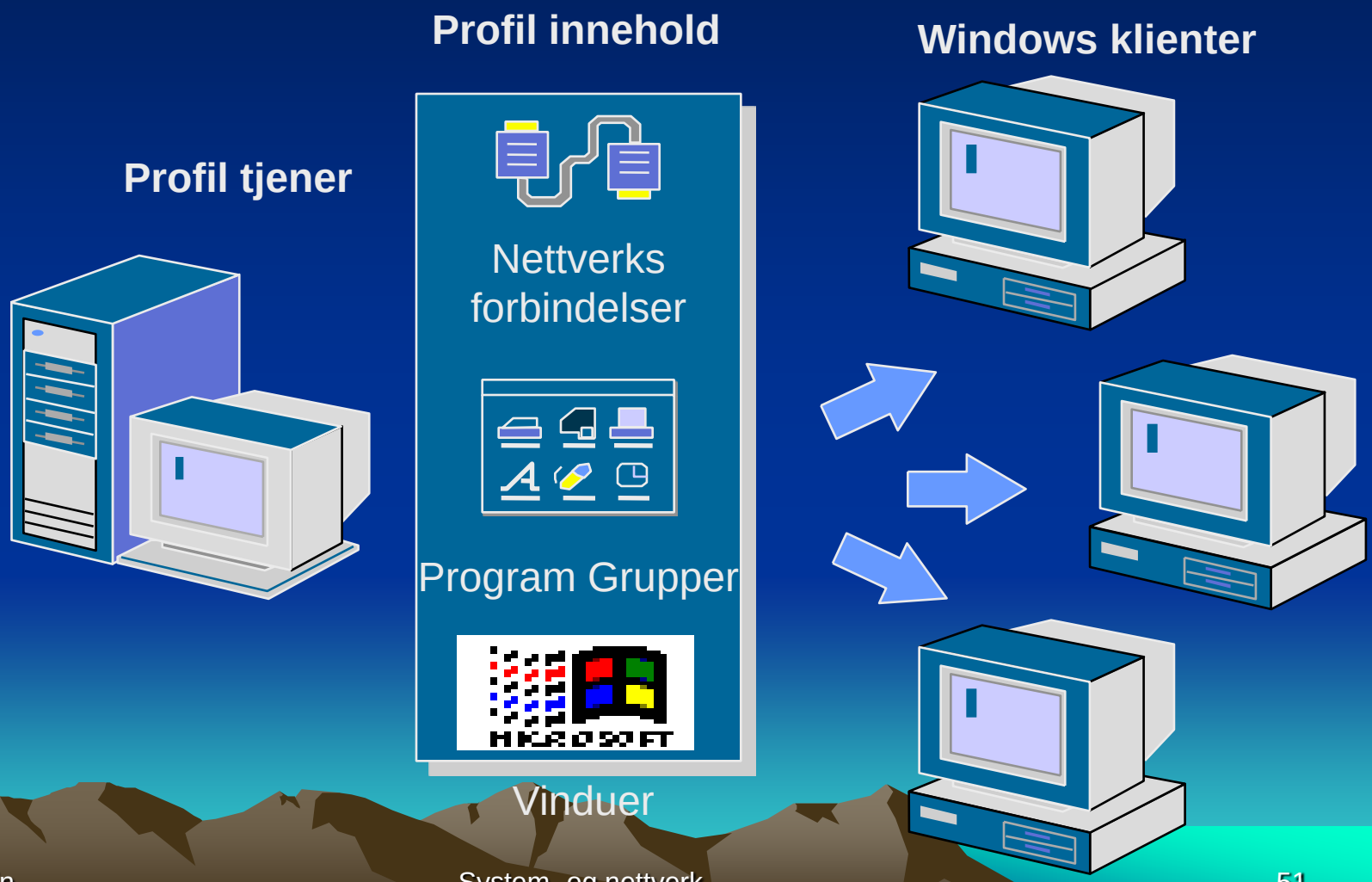
Brukerprofil innhold

Brukerprofilen inneholder oppsettet for brukeren





Tjener basert profil



Typer tjener baserte profiler

- Personlige profiler
  - Oppsett for hver bruker
  - Kan skreddersys av bruker dersom sikkerhetspolitikk tillater dette
  - Følger brukeren uansett system han benytter i domenet
- Mandatory profiles
  - Obligatoriske, kan ikke endres av brukeren

Bruker profiler

- Lokal profil lagres på klienten
  - Endringer vil ikke følge brukeren til andre klienter
  - OK hvis kun et system benyttes
- To programgrupper støttes
  - Brukerens programgrupper, hentes fra profil
  - Felles programgrupper, hentes fra mappen *All Users* i profil katalogen

Samba som Windows domenekontroller

```
[global]
 workgroup = DT
 netbios name = GANDALF
 domain logons = Yes
 security = user
 preferred master = Yes
 domain master = Yes

 # Login skript for alle brukere
 logon script = login.bat
 # path for roaming profiles
 logon path = \\%L\profiles\%U
 # Hjemmekatalog %L substitueres med systemnavn, %U med brukernavn
 logon home = \\%L\%U
 # Hjemmeområdet mappes til H:\
 logon drive = H:
```

Samba som Windows domenekontroller

```
# Nødvendige delte ressurser i domene: netlogon, profilområde og hjemmekataloger

[netlogon]
 # Login skript ligger her
 path = /home/netlogon
 writeable = no

[profiles]
 path = /home/profiles
 writeable = yes
 guest ok = no

[homes]
 browseable = no
 writable = yes
 valid users = %S
 path = /home/%D/%S
```