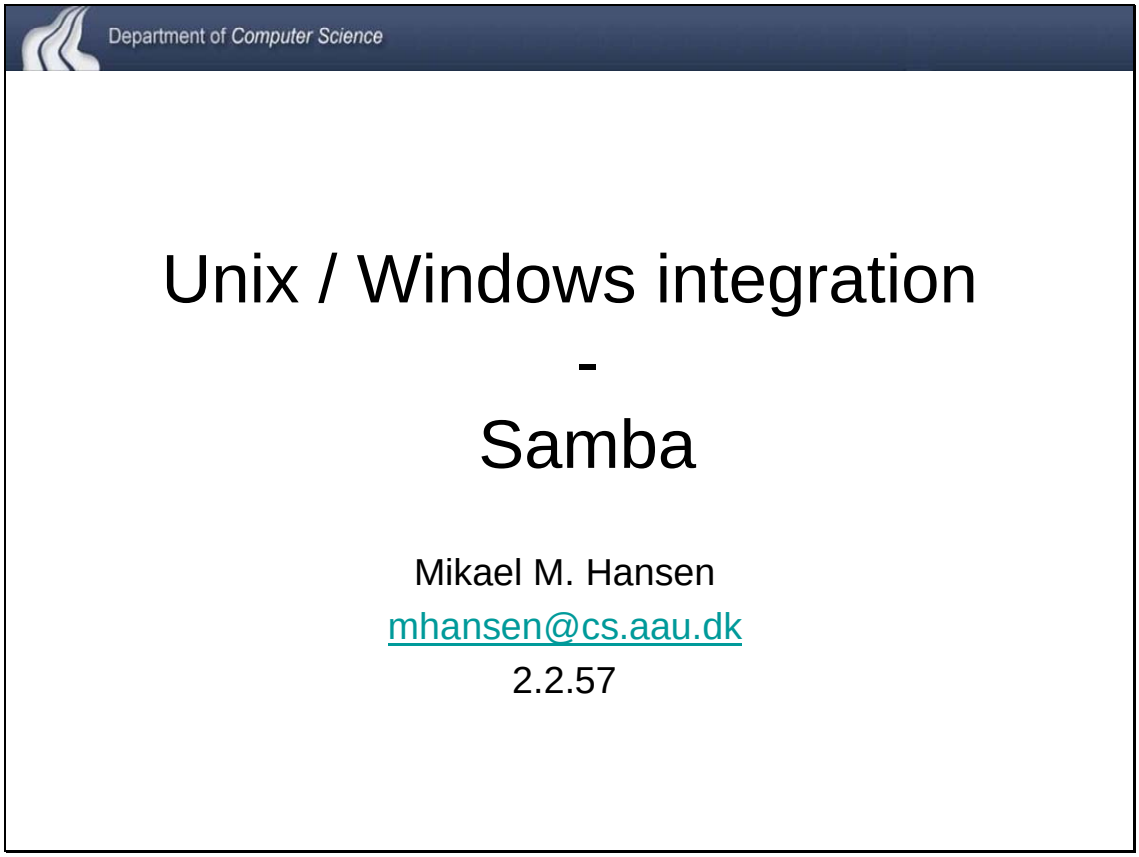

Department of Computer Science
Unix / Windows integration
-
Samba
Mikael M. Hansen
mhansen@cs.aau.dk
2.2.57

Department of Computer Science

TOC

- Mine indlæg
- Dagens program: Unix / Windows integration
  - Windows "Teorien"
    - NT
    - AD
  - Samba
    - Historien
    - Teorien
    - Server modes

2

Department of Computer Science

Mine indlæg

- 14/2: Linux administration
- 28/2: E-Mail services og protokoller
- 4/3: Mail servers, Anti-Spam tools
- 6/3: Unix/Windows integration – Samba
- 11/3: Systemadministrations arbejdsprocesser og procedure
  - » Spørgestime (bog og praksis)
- 27/3: Systems and Network Management

3

Department of Computer Science

Unix / Windows integration

Formål:

At give basalt kendskab til integration imellem Windows og Unix vha. Samba. Herunder kendskab til Samba pakken og dens muligheder og begrænsninger.

Department of Computer Science

Unix / Windows integration

Del 1 – ”Teorien”

Department of Computer Science

NT kontra Active Directory

- NT (<= NT4)
  - Domæner
    - Security boundry er domænet
    - Domæne kontroller: 1PDC, x BDC'er
      - (single master replication)
    - Trust imellem domæner (ikke-transitiv)
    - Netbios og WINS
    - Indhold er flad
- AD (>= Windows 2000)
  - Forest
    - Kan indeholde 1 til flere domæner
      - Den første er forest root-domæne
    - Security boundry er din forrest
    - Multi master replication
    - Trust imellem forests (=>transitiv)
    - DNS
    - Indhold er hierarkisk (pga. LDAP)

6

Department of Computer Science

Windows

- SID i stedet for UID
  - Eks: S-1-5-21-4294955119-3368514841-2087710299-500
  - Sidste kaldes en RID og angiver elementet.
    - Eks. 500
  - SID - RID angiver domænet.
    - Eks. S-1-5-21-4294955119-3368514841-2087710299

7

Department of Computer Science

NETBIOS

- Network Basic Input/Output System
  - API som tillader applikationer på separate computere at snakke sammen
  - Kører over TCP/IP
    - Tidligere over f.eks. NetBEUI
  - Bruges til Windows networking
    - NT style
    - Workgroup mod
  - F.eks.
    - Network Neighbourhood
    - Map network drive

8

Department of Computer Science

NETBIOS

- Har tre grundfunktioner:
  - Name service (udp 137)
    - Så applikationer kan registrere et navn
  - Session service (tcp 138)
    - Så applikationer på forskellige computere kan tale sammen over en etableret forbindelse
  - Datagram distribution service (udp 138)
    - Så applikationer på forskellige computere kan tale sammen, uden en forbindelse.

9

Department of Computer Science

NETBIOS

- NETBIOS navn
  - er det korte navn der gives til Windows computeren
- Hvordan et navn bestemmes afhænger af hvilken node type maskinen er:
  - b-node: NETBIOS broadcast (via UDP broadcast)
  - p-node: NETBIOS unicast (via UDP unicast) til en WINS server
  - m-node: Først "b-node" med fallback til "p-node"
  - h-node: NETBIOS unicast til WINS server med fallback til NETBIOS broadcast (via UDP broadcast)

10

Department of Computer Science

NETBIOS

- Som default er Windows er en ”b-node”
- Af hensyn til browsing:
  - Vælges en DMB pr. ”domain”
  - Der vælges en LMB pr subnet pr. ”domain”.
    - Hvem der vinder valget afhænger af OS
    - Hver boot af en maskine tvinger et valg igennem
- Master browsere vedligeholder en liste af navne og adresser
- Alternativt anvendes WINS …

11

Department of Computer Science

WINS

- Windows Internet Naming Service
- Microsofts implementation af en NetBIOS name server i Windows
- Er en
  - Central mappering af navne til adresser
  - Kan være distribueret over subnets.
  - Opdateret dynamisk (når en maskine booter)
  - Er flad (dvs. et navn kan kun optræde engang)
    - Et navn kan optræde med flere roller

12

Department of Computer Science

WINS

- Et eksempel: (fra CS WINS serveren)

```
"LFS1#03" 1173794210 130.225.194.8 130.225.195.38 64R
"LFS0#00" 1173793990 130.225.194.4 64R
"LFS1#20" 1173794210 130.225.194.8 130.225.195.38 64R
"LFS0#03" 1173793990 130.225.194.4 64R
"LFS1#00" 1173794210 130.225.194.8 130.225.195.38 64R
"LFS0#20" 1173793990 130.225.194.4 64R
```

13

Department of Computer Science

NetBIOS / WINS

- Et eksempel:

1. DHCP server kontaktes (faktisk DHCP discover)
2. DHCP svar (med ip info, og NETBIOS node type og wins server addresse)
3. PC bliver en h-node
4. PC kontakter WINS server (Her er jeg. Jeg hedder…)
5. Brugeren skriver f.eks. \\lfs0\mhansen
6. PC kontakter WINS server (Hvem er lfs0#20?
7. WINS server svarer med en IP xxx
8. PC kontakter IP'en xxx og beder om mhansen shares

14

Department of Computer Science

DNS

- DNS kender I
  - Navn til IP
  - IP til Navn mappering
- Forskellige record typer:
  - A, MX, PTR, NS, CNAME, SRV
- SRV bruges meget i AD
  - Alle roller findes vha. SRV records
  - F.eks. gc._msdcs.mydomain.com

15

Department of Computer Science

LDAP

- En protokol ikke en database
- Et LDAP directory udgøres af:
  - En Base
  - Et antal grene (evt, med undergrene)
  - Grene udgøres af komponenterne:
    - dc: Domain component
    - ou: Organisational Unit
    - cn: Common Name
    - M.fl.
  - Stien fra en element til base kaldes for en
    - dn: Distinguished Name

16

Department of Computer Science

LDAP

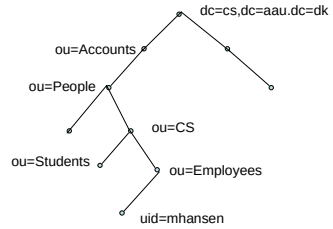
- Hver node kan indeholde elementer fra de understøttede skemaer:
  - Skema: definition af objekter
- Man søger ved at angive:
  - Et start sted
  - Hvad man søger efter (filteret)
  - Evt. et søge scope
- Læs evt.
  - http://www.openldap.org/doc/admin23/

17

Department of Computer Science

LDAP

- Skal vi tegne et eksempel?



dn: uid=mhansen,ou=Employees,ou=CS,ou=People,ou=Accounts,dc=cs,dc=aau.dc=dk 18

Department of Computer Science

LDAP

- Eksempel, en entry

```
dn: uid=mhansen,ou=Employees,ou=CS,ou=People,ou=Accounts,dc=cs,dc=aau,dc=dk
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
objectClass: aauPerson
cn: Mikael M. Hansen
sambaPrimaryGroupSID: S-1-5-21-2129259131-3331630079-4045832457-15797
uid: mhansen
gidNumber: 7398
sambaSID: S-1-5-21-2129259131-3331630079-4045832457-15796
sn: Hansen
loginShell: /usr/dist/bin/zsh
sambaProfilePath: \\%L\mhansen\.windowsprofile
uidNumber: 7398
mail: mhansen@cs.aau.dk
ou: Computer Science
homeDirectory: /user/mhansen
sambaHomeDrive: U:
structuralObjectClass: inetOrgPerson
sambaAcctFlags: [U]
gecos: Mikael M. Hansen
```

19

Department of Computer Science

Unix / Windows integration

Del 2 - Samba

Department of Computer Science

Historien

- 1992: Andrew Tridgell offentligjorde sin implementation af en NetBIOS compatibel Filserver til unix
  - Han havde et behov som han løste
- 1999: Samba 2.0 var ude.
  - Ziff-Davis Publishings Netbench måler samba (på linux) til at performe mindste dobbelt så hurtigt som NT

21

Department of Computer Science

Idag

- Andrew Tridgell er stadig i spidsen for teamet.
- Flere virksomheder betaler folk for at udvikle på Samba f.eks.
  - Novell, RedHat
  - IBM
  - HP
- Version 2.2 bragte mulighed for AD domain membership
- Vi er i dag på 3.0.28.
- 4.0 serien er i technology preview

22

Department of Computer Science

Selve pakken

- De binære (serverne):
  - sbin/smbd
    - File og print operationer + local authentificering
  - sbin/nmbd
    - Alt navne registrering/resolution
  - sbin/winbindd
    - Fjern authentificering og medlemskab af AD domain

23

Department of Computer Science

Selve pakken

- lib/smb.conf
  - Konfigurationsfilen.
  - Der er kun den ene.
- bin/smbclient
  - klientprogram til file og print services
- bin/smbstatus
  - Lister status af samba serveren. (Er der nogen på)
- bin/testparm
  - Tester om konfigurationsfilen er ok

24

Department of Computer Science

Samba

- To ting har grundlæggende indflydelse på hvordan samba opfører sig:
  - Server type
  - Security mode
- Lad os kigge lidt på dem…

25

Department of Computer Science

Server Types

- Samba kan være tre typer:
  - Standalone
    - Workgroup mode
  - Domain member
    - Medlem af et Domæne
      - (NT4, AD ellers samba (NT4))
  - Domain Controller
    - Ansvarlig for et domæne
      - (nt4, ikke AD)

26

Department of Computer Science

Security modes

- Share level security
  - security = share i smb.conf
  - Brugeren autentificeres per share
- User level security
  - security = user i smb.conf
- Domain security
  - security = domain
  - workgroup = domainname
- ADS security
  - security = ADS
  - realm = your.kerberos.realm
- Server security (deprecated)
  - security = server

27

Department of Computer Science

Accounts

- Samba skal kende
  - Brugerne
  - Deres passwords
  - Logon hours, profile, m.m.
- Windows sender krypterede passwords til serveren
  - LANMAN og NT hashes
    - 16 bit evt. NULL padded
- Samba kender kun Unix/Linux systemets brugere/passwords (/etc/passwd eller tilsvarende).
  - Så den skal have noget mere / andet
    - De krypterede windows passwords

28

Department of Computer Science

Accounts

- Derfor har samba account backends
  - tdbsam
  - ldapsam
  - smbpasswd (er på vej ud)
  - andre, men brug dem ikke
- De Windows specifikke ting gemmes også i backenden
  - F.eks. Logon hours

29

Department of Computer Science

SID <- ->UID mappering

- To måder
  - Når en bruger oprettes i Samba account backend oprettes der samtidig en bruger på systemet
  - Man bruger idmap til at gemme SID til UID mapperingen
    - En bruger (SID) får en "tilfældig" uid. Mapperingen gemmes dog til næste gang
      - Lokalt, man kan distribueres vha. LDAP

30

Department of Computer Science

Overblik

- Samba kan altså virke på et hav af forskellige måder. Men forskellige konsekvenser til følge.
  - Hvad gør man?
- Se på kravene og miljøet
  - Hvor er brugerne i dag?
    - NIS eller LDAP -> ldapsam
    - AD -> ADS member
    - NT4 -> Samba Domain Control (ldapsam)
  - Er det et lille testmiljø
    - Smbpasswd (hvis man kan oprette brugere lokalt)

31

Department of Computer Science

2 eksempler

- Den simple:
  - Standalone server.
  - smbpasswd backend
- Den komplekse:
  - Domain Control
  - ldapsam backend

32

Department of Computer Science

Den simple

- etc/smb.conf:

```
[global]
workgroup = andeby
netbios name = joakim
security = share
passdb backend = smbpasswd

[pengetanken]
comment = "Bliv væk!"
path = /q/disk_0
read only = yes
guest ok = yes
```

33

Department of Computer Science

Den simple

- For hver bruger: (på samba serveren)

```
root# groupadd "LoginID"
root# useradd –g "LoginID" -c "Name of User" "LoginID"
root# passwd "LoginID"
Changing password for user "LoginID"
New Password: XXXXXXXXX
Retype new password: XXXXXXXXX
root# smbpasswd -a "LoginID"
New SMB password: XXXXXXXXX
Retype new SMB password: XXXXXXXXX
Added user "LoginID"
```

34

Department of Computer Science

Den komplekse

- Kræver en kørende LDAP server
  - F.eks. OpenLDAP
- Samba schema er loadet
  - Findes i Samba source
- LDAP directoriet er loadet med data
  - Man kan bruge slapadd –l ”filename” til det.
  - Se eks på næste side
- Netværk og name resolution virker.

35

Department of Computer Science

Den komplekse

- Eksempel indhold af ldif fil

```
dn: cn=updateuser,dc=abmas,dc=biz
objectClass: person
cn: updateuser
sn: updateuser
userPassword: not24get

dn: cn=sambaadmin,dc=abmas,dc=biz
objectClass: person
cn: sambaadmin
sn: sambaadmin
userPassword: buttercup
```

36

Department of Computer Science

Den komplekse

- etc/smb.conf

```
[global]
workgroup = andeby
netbios name = joakim
security = domain
passdb backend = ldapsam:ldap://massive.abmas.biz
domain logons = Yes
domain master = Yes
wins support = Yes
ldap suffix = dc=abmas,dc=biz
ldap machine suffix = ou=People
ldap user suffix = ou=People
ldap group suffix = ou=Groups
ldap idmap suffix = ou=Idmap
ldap admin dn = cn=sambaadmin,dc=abmas,dc=biz
idmap backend = ldap://massive.abmas.biz
```

37

Department of Computer Science

Den komplekse

```
[pengetanken]
comment = "Bliv væk!"
path = /q/disk_0
read only = yes
guest ok = yes

[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No
```

38

Department of Computer Science

Den komplekse

- Kør nu bin/smbpasswd –w ”password”
  - Den smider passwordet for brugeren der kan skrive til LDAP’en i private/secrets.tdb
  - Brugen så vi tidligere:
    - *cn=sambaadmin,dc=abmas,dc=biz*
- Så mangler der kun at komme brugere i LDAP’en

39

Department of Computer Science

Den komplekse

- Brugere i LDAP’en
  - En løsning; smbldap-tools
    - En pakke med diverse værktøjer der kan hjælpe med at oprette, nedlægge og modificere bruger,grupper m.m.
  - En anden løsning: scripts
    - Skriv selv scripts der smider det rigtige i LDAP’en

40

Department of Computer Science

Printserver

- Samba som printserver
  - Afhænger af print systemet på maskinen
- To modeller
  - Den klassiske
  - CUPS
- Et print, grundlæggende
  - Klient forbinder sig til printer share
  - Samba autentificere brugeren (hvis nødvendigt)
  - Printfile kopieres til sambas spool område
  - Klienten lukker forbindelsen
  - Samba kører print kommandoen
  - Print systemet håndterer jobbet
  - Samba sletter printfilen i spool området

41

Department of Computer Science

Printserver

- Den klassiske:

```
[global]
printing = sysv
load printers = yes

[printers]
path = /var/spool/samba
printable = yes
public = yes
writable = no
```

42

Department of Computer Science

Printserver

- CUPS:

```
[global]
load printers = yes
printing = cups
printcap name = cups
[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
public = yes
guest ok = yes
writable = no
printable = yes
```

43

Department of Computer Science

Printserver

- Download af printerdrivere
  - Man kan på en Samba printserver installere printerdrivere for sine printere
  - Disse kan så hentes og installeres af klienten når den connecter til printeren.
  - Kræver en [print$] share.
    - Navnet er hardcoded i windows klienter.

```
[print$]
comment = Printer Drivers
path = /etc/samba/drivers
browseable = yes
guest ok = no
read only = yes
write list = root
```

44

Department of Computer Science

Printserver

- Download af drivere
  - To måder
    - Automatisk med cupsaddsmb:
      - En binær fra CUPS installationen
      - $cups$/sbin/cupadaddsmb –u user printername
      - Henter drivere, PPD fra CUPS og placerer den i [print$] sharen på samba serveren.
    - Manuelt via Windows Print properties dialog på Samba serveren
      - GUI peg og klik

45

Department of Computer Science

Winbind

- Domæne logon på Unix/Linux box
  - Tillader domæne brugere og gruppe at optræde lokalt på unix boxen
    - Via NSS, PAM
  - Meget nyttigt hvis man er I et windows miljø, men gerne vil have enkelte unix bokse integreret
    - F.eks. Print server
  - Benytter MSRPC for at finde brugere og grupper samt autentificere brugere

46

Department of Computer Science

Winbind

- Krav
  - Installerer et NSS og PAM modul på systemet.
    - Ret i /etc/nsswitch.conf
      - passwd: files winbind
  - Lave en mappering imellem uid/gid og SID
    - Laver den selv i LDAP eller en tdb fil
    - Eller lad Samba gøre det
  - Samba server skal joines til domænet
    - Have en account i domænet

47

Department of Computer Science

Winbind

- lib/smb.conf:

```
[global]
separator =\
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template homedir = /home/winnt/%D/%U
template shell = /bin/bash
```

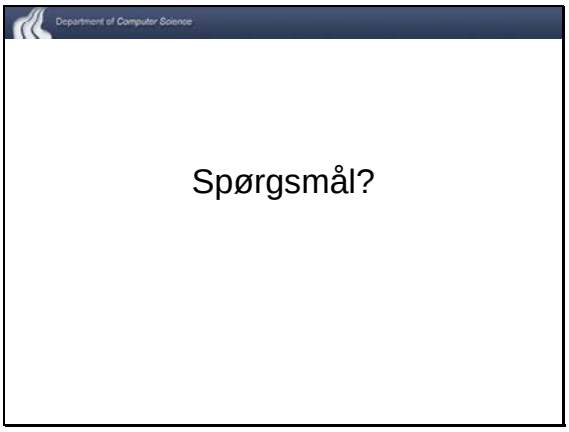
48

Department of Computer Science

Winbind

- Join samba til windows domænet
  - bin/net rpc join –U Administrator
- Så startes winbindd dæmonen og man kan via bin/wbinfo –u se brugerne fra windows domænet.
- Nu kan windows brugere f.eks. ssh til unix boksen.

49


Department of Computer Science
Spørgsmål?