



Linux i en MS-verden

Bjørn Tore Sund
Overingeniør IT
Matematisk Institutt
Universitetet i Bergen
bjornts@mi.uib.no



UiBs motivasjon

- IT-strategi på “åpen kildekode”.
- Eksisterende Windows-klientnettverk m/AD-infrastruktur.
- Studentlabber og ansattmaskiner med linux-tilbud.
- SSO og felles brukernavn/passord.



En liten oversikt

- Enslig maskin
 - Active Directory
 - Kerberos
 - Winbind
 - Services for Unix?
 - Samba-klient
- Større skala
 - LDAP mot AD
 - Samba 3.0
 - 2.6-kernel m/cifs



Active Directory

- Microsofts administrasjonsverktøy
- Bl.a. autentisering og aksess
- LDAP-protokoll for autentisering.
- Policy...



Det virker bare nesten...

- uid og gid kan variere
- uid og gid kan vanskelig hentes fra unix-server m/samba
- Hjemmekatalog på windowsserver har ikke unix-filsystem – du trenger noe lokalt til dot-filer.



Før du begynner

- Kjenn din AD-server.
- Kompiler/installer Samba3.0
m/winbind- og AD-støtte.
- Vær snill med din MSCE. Du vil
trenge hennes hjelp.



Filer å kjenne

- `/etc/krb5.conf`
- `/etc/samba/smb.conf`
- `/etc/nsswitch.conf`
- `/etc/pam.d/*`



smb.conf

- security = ADS
- encrypt passwords = yes
- winbind separator = +
- idmap uid = 10000-20000
- winbind gid = 1000-2000
- (og noen til)



- kinit brukernavn@DOMAIN
- /etc/init.d/nscd stop (og FJERN den)
- net rpc join -S PDC -U Administrator
- /etc/init.d/winbindd start
- /etc/init.d/nmbd start
- /etc/init.d/smbd start



/etc/nsswitch.conf

- passwd: files winbind
- shadow: files
- group: files winbind



Sambaserver

- mangle filenames = yes
- unix extensions = yes
- oplock krever egentlig linux
- Gnome trenger egne knep...
- Med i AD-domene som server



Services for Unix

- Microsofts løsning for uid+gid
- Ligner bare litt på rfc2307s
standard-definisjon
- Mangler funksjonalitet for å hente
UiD og GiD fra eksisterende unix.
- Legg heller inn felter manuelt...



Standarden

- rfc2307:

The following attributes are defined in this document:

uidNumber
gidNumber
gecos
homeDirectory
...

- SFU3.0:

- samAccountname: nmabs
- msSFU30GidNumber: 3600
- msSFU30UidNumber: 28826
- msSFU30LoginShell: /bin/tcsh
- msSFU30HomeDirectory: /Home/stud4/nmabs
- ...



UiD og GiD er verre

- <http://www.padl.com/> - finn ad.so
- idmap backend=ad:[ldap://serverip/](#) i smb.conf
- Tryner på SFU3.0, tryner på for mange brukere, tryner på at brukere mangler uid eller gid...



Stabilitet? Skalerbarhet?

- Stabiliteten er stort sett grei.
- Prosessen er vanskelig å automatisere og standardisere.
- Sliter med mange brukere og rare gamle brukerdatabaser.



AD er LDAP

- Legg inn felter manuelt eller konfigurerer i `/etc/ldap.conf`
- Importer uid og gid med scripts
- Proxybruker med leserett i AD.
- Passord i `/etc/ldap.conf`
- `nss_ldap` virker! Krypter! Krypter!



Kernel 2.6.max

- cifs kjernemodul eller smbfs kjernemodul for filsystem.
- cifs noe raskere, smbfs visstnok mer stabilt.
- Blant de mer ustabile tingene i 2.5, og under kraftig utvikling fortsatt.



Samba 3.0+

- Samba 3.0+ på både klient og server.
- Den brukes for diskmontering, ingenting mer.
- Så mye unix-støtte som mulig. Kan trenge separat server for MS.



Andre ting?

- Fungerer med automount etter masse dill i /etc/pam.d/system.auth
- Mangler Single Sign-On.
- Test i produksjon foregår nå!