



Winbind as Identity Management Connector

Fabrizio Manfred Furuholmen

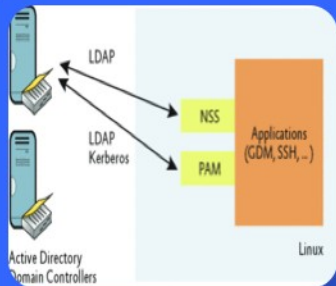


- Overview
- Introduction
- Solution
- Case study
- Results



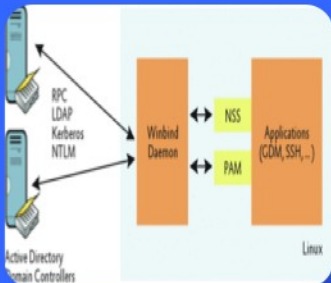
Winbind unifies UNIX and Windows NT account management by allowing a UNIX box to become a full member of an Windows domain.

- Authenticate user credentials by using PAM (SSO)
- Resolve user identities and group identities by using the NSS.
- Store mappings between Unix UIDs and GIDs and Active Directory security identifiers, or SIDs



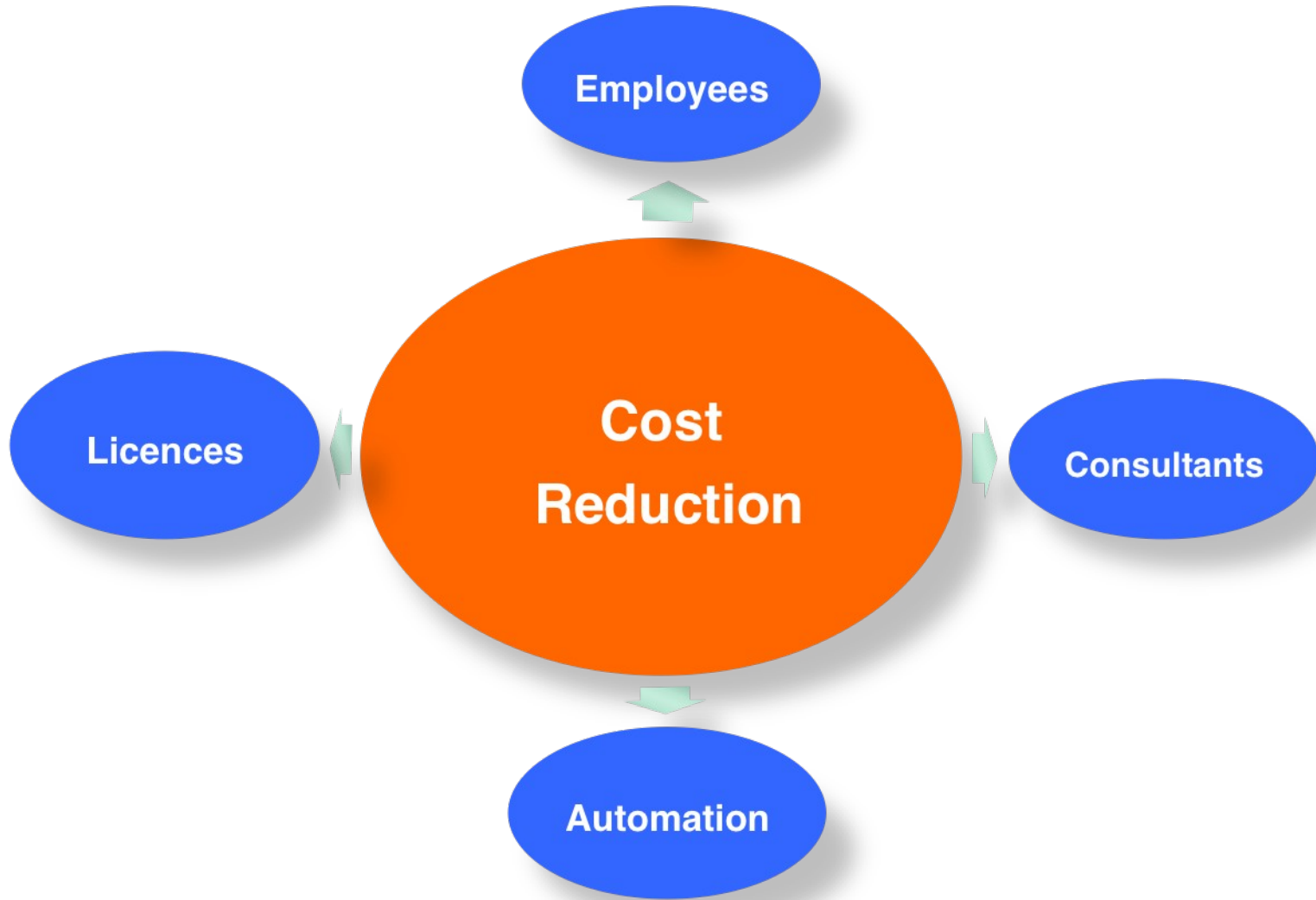
LDAP+KRB

- No daemon required
- Custom schema support
- More services supported (network, rpc, protocols..)



Winbind

- Mapping SID<->GID/UID
- Cache
- Ticket kerberos handling
- Multi domain / Multi backend
- Group Policy
- Remote Administration



Simplify administration tasks

Centralized Identity administration
 Centralized Security Policy
 Reduced complexity



Standard ("de facto")

- Compatibility
- Consultant independent (consultant go home)



Licence Cost

Opensource Server side, services
 Opensource client side, desktop replacement



ADS

- Directory Services (Identity Management)
- RFC 2307bis UNIX Storage
- MMC
- Password Policy
- Application Deploy
- **Group Policy**

FOSS

- Winbind
- Samba Fileserver
- Linux Terminal Server
- Mailserver
- openAFS

VMware

- Consolidation for services infrastructure
- High Availability
- Backup

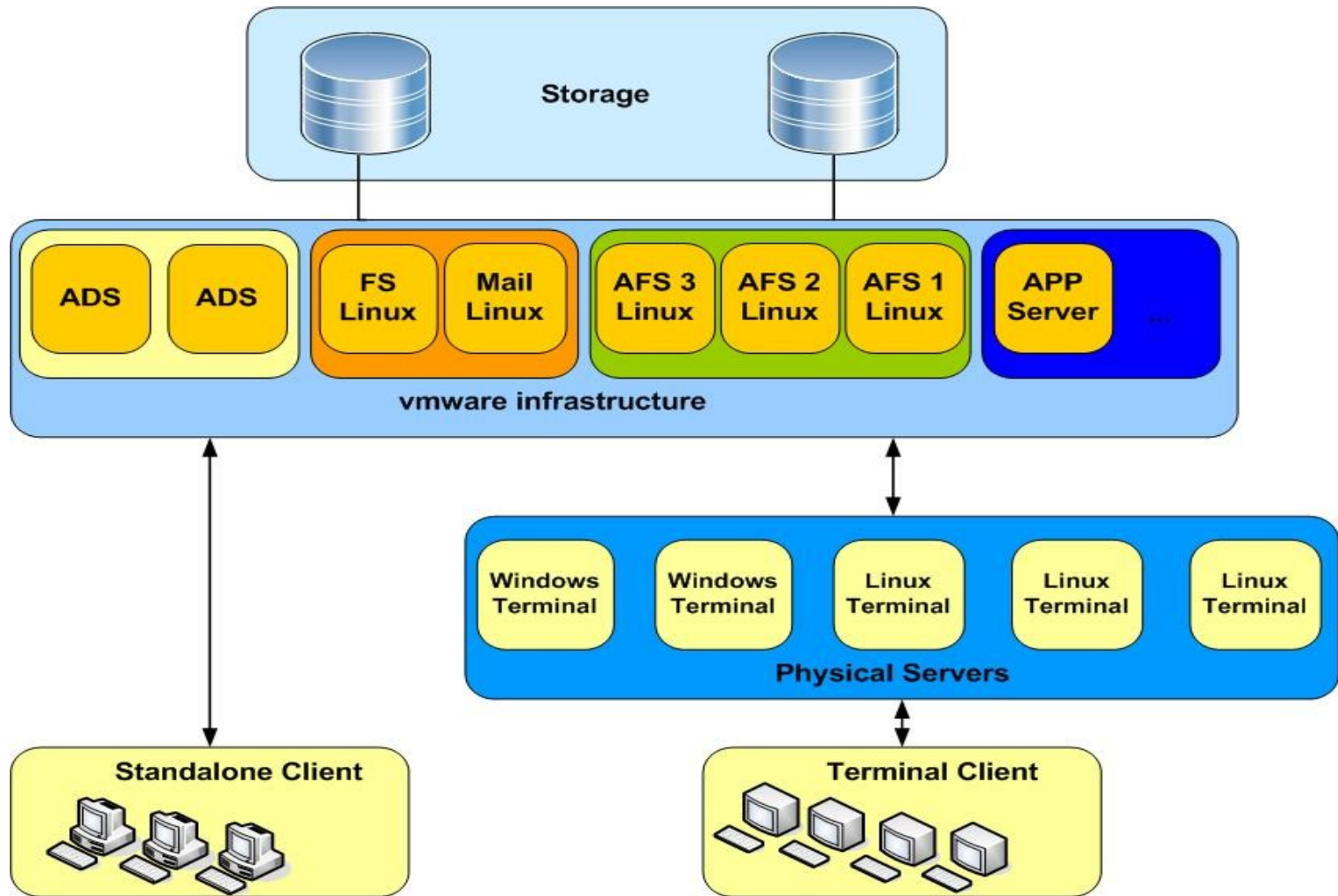
Company

- Head Quarter in Italy 350 users
- 5 Branch Office in Italy 20-60 users
- 550 Total users

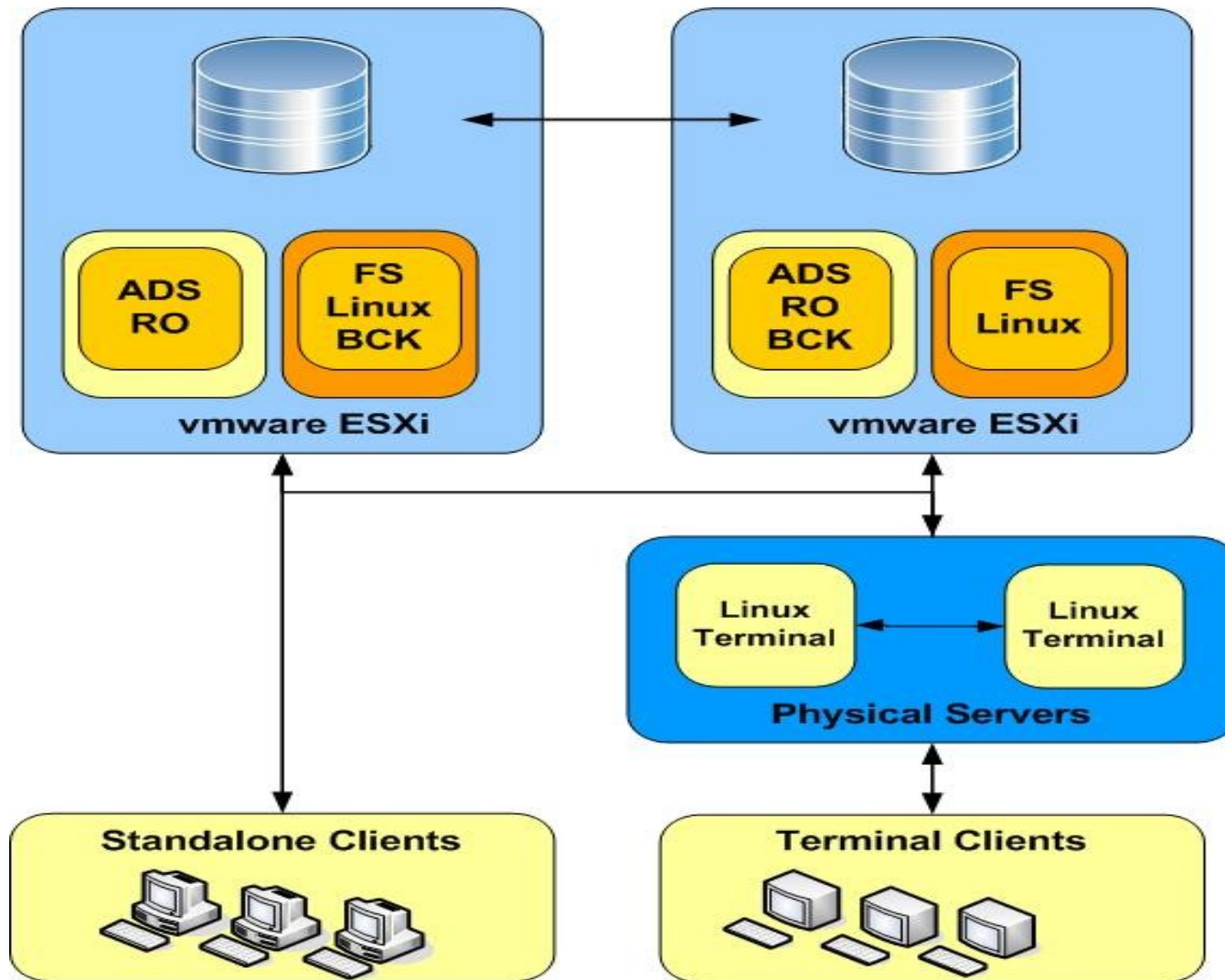
- Wide Area Network
- 6 Windows NT domain base Samba with openLDAP

- 400 PC Windows XX
- 150 PC Linux

- No IT stuff on the branch office or with low profile
- Consultants for unix environment and for project



Architecture Branch



AUTH (PAM)

- Login on Unix (gdm, ftp, ssh..)
- Saslauthd (smtp,imap..)
- Kerberos Ticket (aklog, Firefox, ..)

AUTZ (NSS)

- UID/GID lookup (MAP)
- Ptserver lookup users and groups

STORAGE

- RFC2307 Backend
- Local storage

Requirements

- NTP
- KRB5 configuration

Domain smb.conf

- workgroup = BEOLINK
- netbios name = FURUHOLMEN
- realm = BEOLINK.ORG
- server string = Samba Server
- security = ADS
- svcctl list = SOME IMPORTANT PROCESS ...
- eventlog list = SOME IMPORTANT LOG

Storage

- idmap domains = BEOLINK.ORG
- idmap config BEOLINK.ORG:backend = ad
- idmap config BEOLINK.ORG:default = yes
- Idmap config BEOLINK.ORG:readonly = yes
- idmap alloc backend = tdb
- winbind use default domain = Yes
- winbind nested groups = Yes
- winbind enum groups = yes
- winbind enum users = yes

Map

- idmap alloc config:range = 5000 - 9999
- idmap config BEOLINK:range = 10000 - 30000
- winbind nss info = rfc2307
- winbind nested group = Yes

Cache

- winbind offline logon = true
- winbind refresh tickets = true
- winbind cache time = 600
- idmap negative cache time = 120

pam_winbind

- account sufficient /lib/security/pam_winbind.so
- session required /lib/security/pam_winbind.so
- /etc/security/pam_winbind.conf
 - cached_login = yes
 - krb5_auth = yes

pam_mkhome

- creates home directories for users on the fly.
- session required /lib/security/pam_mkhome.so skel=/etc/skel umask=0022

NSS

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

NSCD

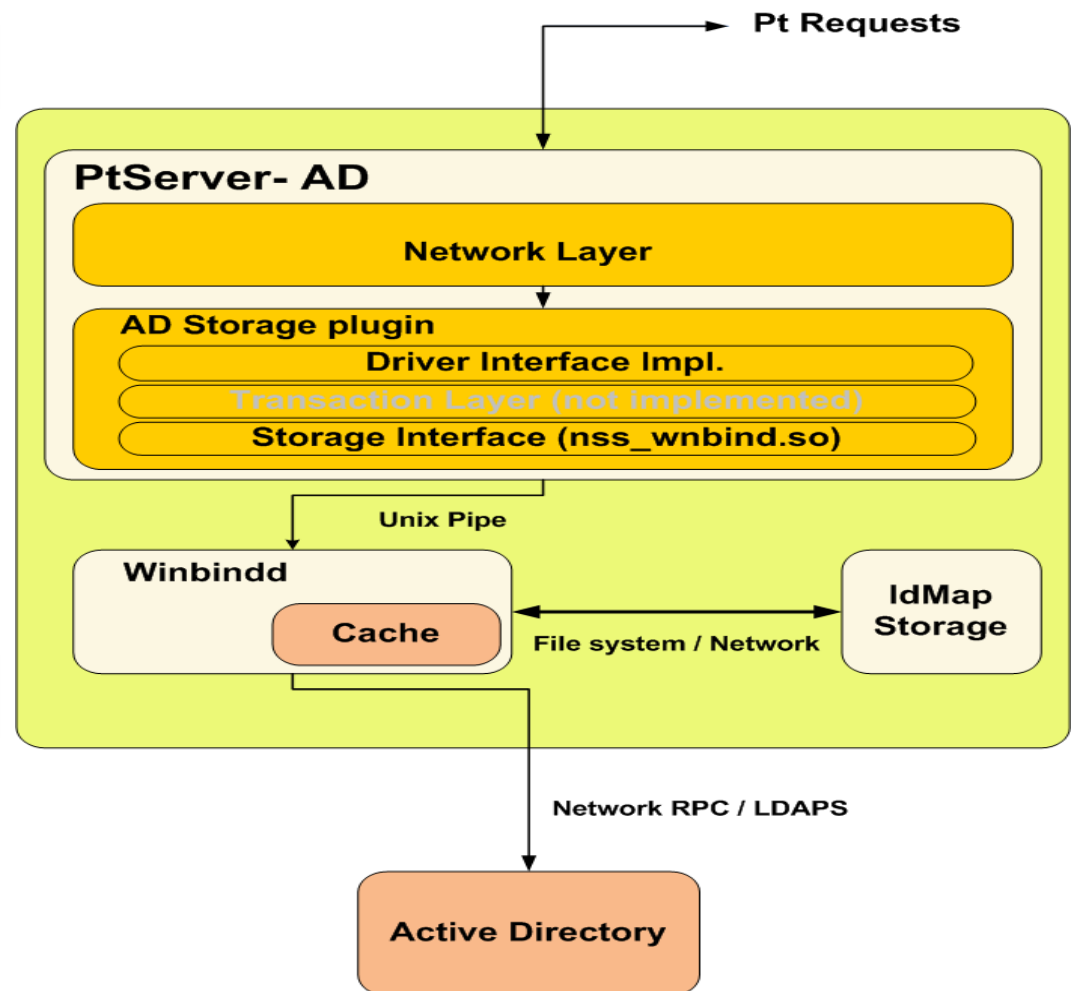
- Disable nscd

Advantages

- Single identity (single storage)
- uid mapping
- gid mapping
- Real time update
- Pluggable in existing infrastructure

Disvantages

- Reliability
- Performance



Application	Cold cache	Warm cache	Remote cold cache	Remote warm cache
Ldap	2X	-	2.5X	-
Ldap+ns cd	2X	1X	2.5X	1X
winbind	-	-	4X	1.2X
ptserver	-	-	2X	1X

Value for execution time

test Properties [?] [X]

Member Of	Dial-in	Environment	Sessions
General	Address	Account	Profile
Telephones	Organization	Remote control	Terminal Services Profile
COM+	UNIX Attributes		

To enable access to this user for UNIX clients, you will have to specify the NIS domain this user belongs to.

NIS Domain:

UID:

Login Shell:

Home Directory:

Primary group name/GID:

OK Cancel Apply Help

```

unixUserPassword: ABCD!efgh12345$67890
uid: test
msSFU30Name: test
msSFU30NisDomain: beolink
uidNumber: 10000
gidNumber: 10000
unixHomeDirectory: /home/test
loginShell: /bin/sh
  
```

```

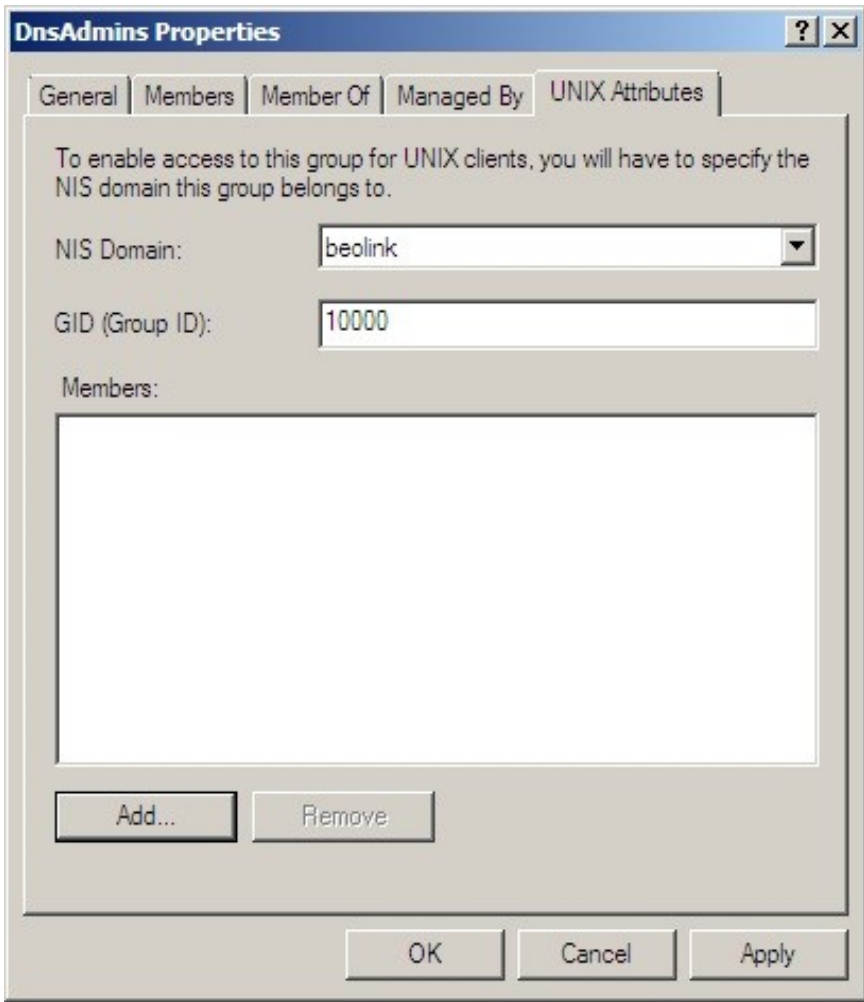
[root@afs1 test]# ls -l
total 0
-rw-r--r-- 1 root root      0 Apr 22 11:06 local.txt
-rw-r--r-- 1 test domain admins 0 Apr 22 11:06 remote.txt
[root@afs1 test]# _
  
```

```

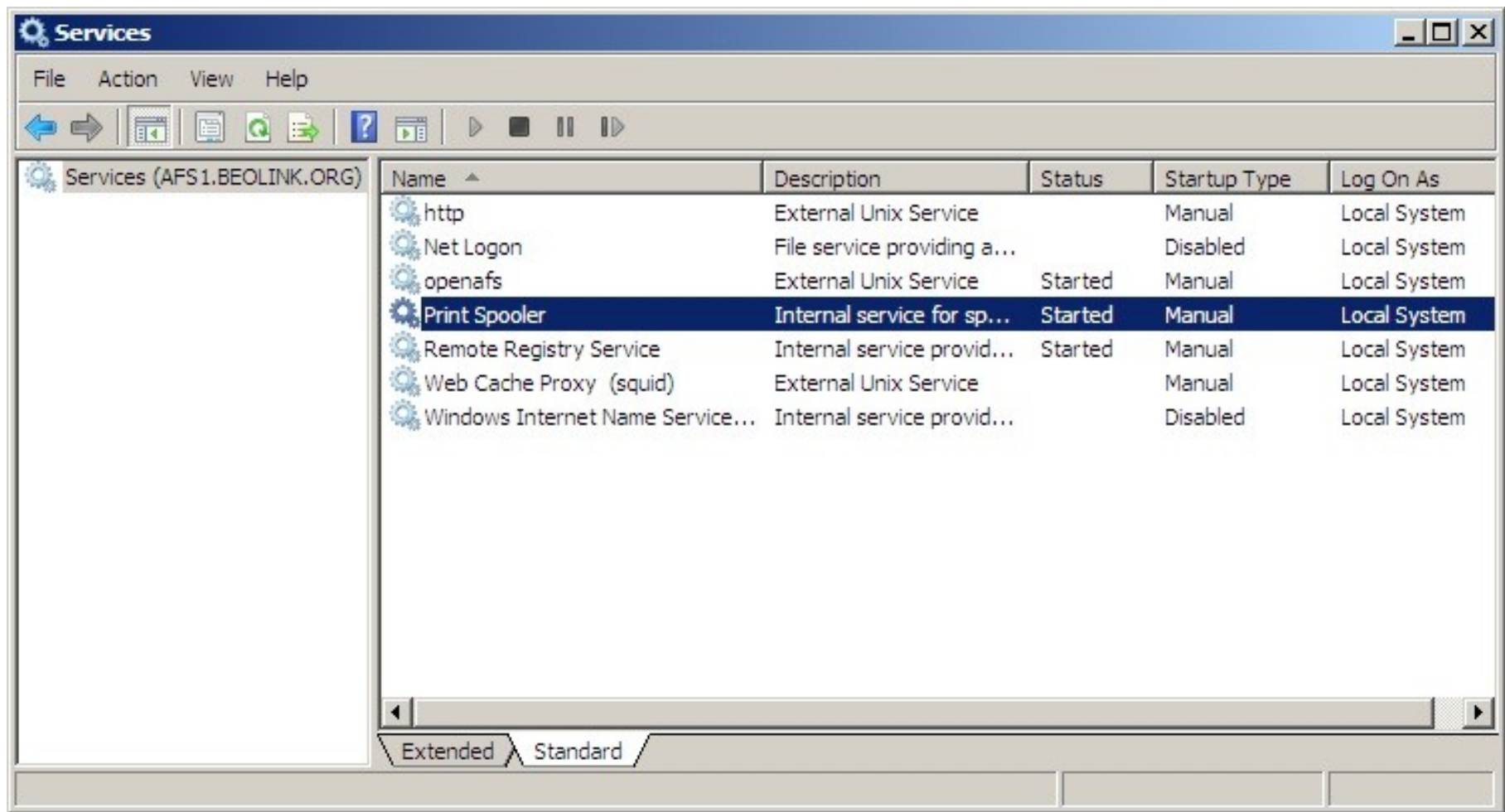
total 0
-rw-r--r-- 1 0 0 0 Apr 22 11:06 local.txt
-rw-r--r-- 1 10000 10001 0 Apr 22 11:06 remote.txt
[root@afs1 test]# _
  
```

```

[root@afs1 test]# finger test
Login: test                               Name: test
Directory: /home/test                     Shell: /bin/sh
Never logged in.
No mail.
No Plan.
  
```



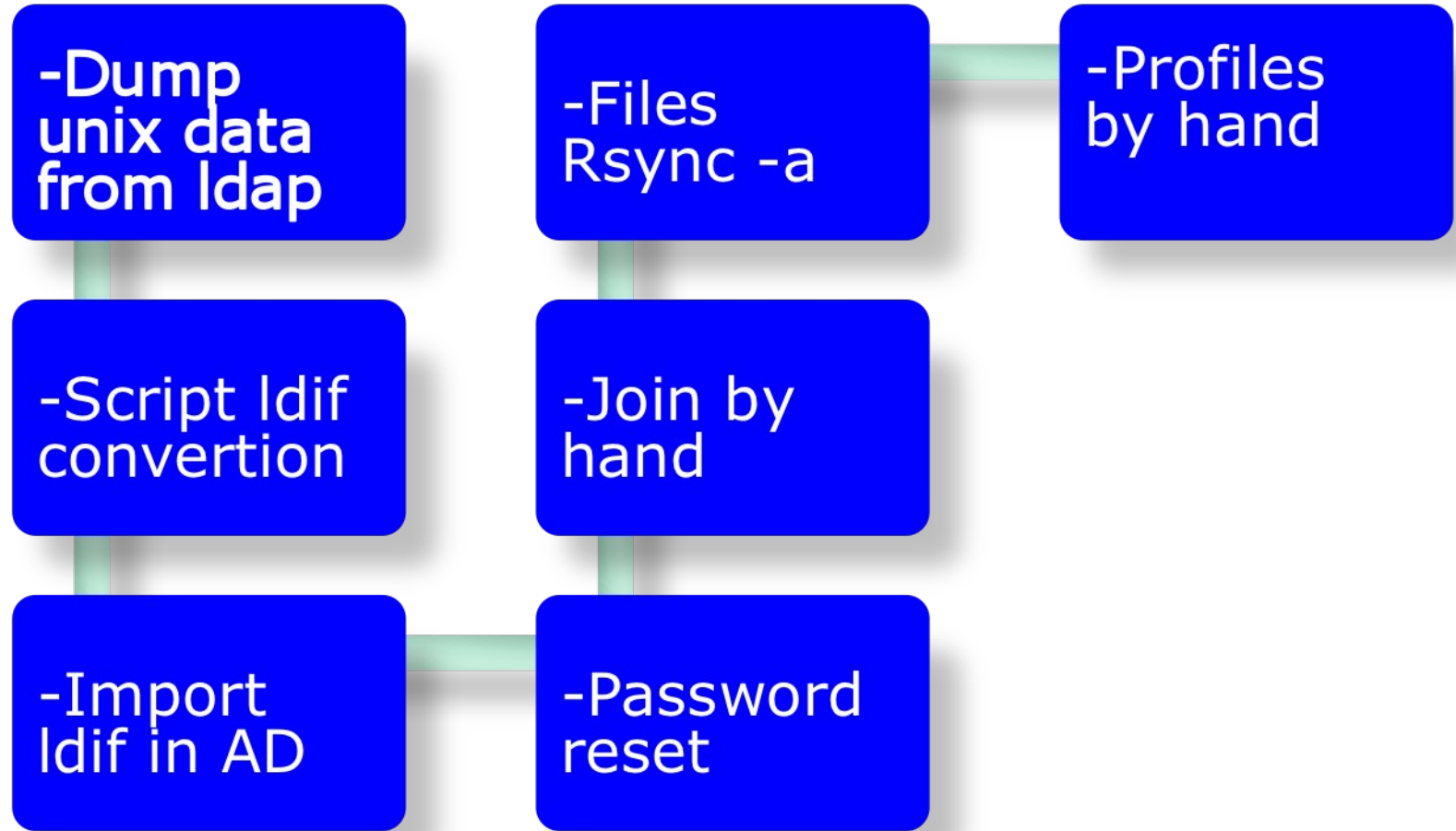
msSFU30Name: Domain Users
msSFU30NisDomain: beolink
gidNumber: 10000



The screenshot shows the Windows Services console window titled 'Services'. The window has a menu bar (File, Action, View, Help) and a toolbar with various icons. The main area displays a list of services in a table format. The 'Print Spooler' service is selected and highlighted in blue.

Name	Description	Status	Startup Type	Log On As
http	External Unix Service		Manual	Local System
Net Logon	File service providing a...		Disabled	Local System
openafs	External Unix Service	Started	Manual	Local System
Print Spooler	Internal service for sp...	Started	Manual	Local System
Remote Registry Service	Internal service provid...	Started	Manual	Local System
Web Cache Proxy (squid)	External Unix Service		Manual	Local System
Windows Internet Name Service...	Internal service provid...		Disabled	Local System

At the bottom of the window, there are tabs for 'Extended' and 'Standard'.



Terminal Server

- 9 LTSP with 250 users
- 2 Windows Terminal 60 users

ADS

- 1 Domain
- 2 AD 550 Windows users
-

Fileserver

- 1 Samba server in HQ with 350 users
- 5 Samba server in branches office with 20/50 users

Licenses

The Unix account is a CAL (cost)

Synchronous

**Per domain synchronous child with
user and group enumeration**

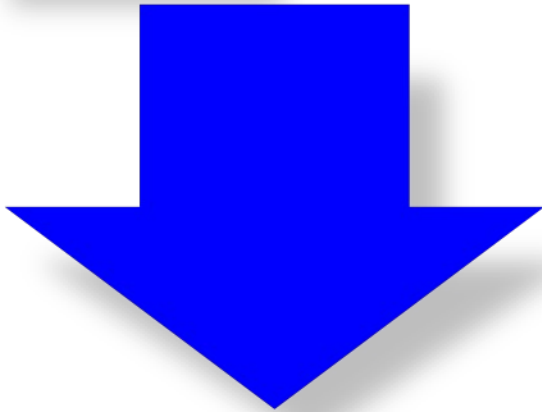
Cache

Single cache for all elements



Cost increased

15% Licenses



Cost reduced

-20% Employees

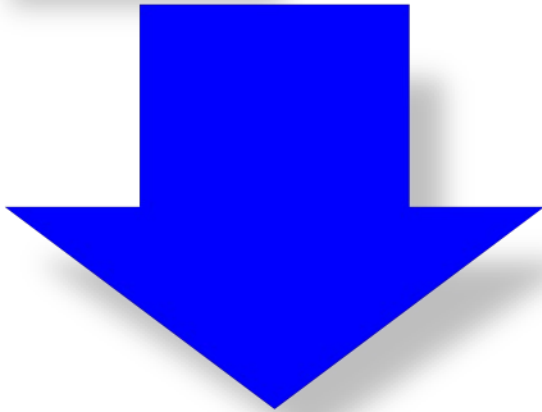
-30% Consultants

Unchaged Service Level



Cost increased

15% Licenses

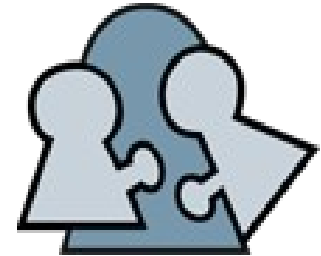


Cost reduced

-20% Employees

-30% Consultants

Global financial crisis of 2008–2009



openAFS Conference Rome September 28-30

<http://www.dia.uniroma3.it/~afscon09/>



Thank you !

Website: www.beolink.org

Email: manfred@freemails.ch