Winbind as Identity Management Connector

Fabrizio Manfred Furuholmen
Agenda

- 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
Windbind vs pam_krb/ldap

**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
Goal

Cost Reduction

Employees
Licences
Consultants
Automation
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
Solution Components

**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

vmware ESXi

ADS RO
FS Linux BCK

Physical Servers

Linux Terminal

Standalone Clients

Terminal Clients

vmware ESXi

ADS RO BCK
FS Linux

11/05/09
Winbind connectors

**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
Winbind configuration 1/5

Requirements

- NTP
- KRB5 configuration

Domain smb.conf

- workgroup = BEOLINK
- netbios name = FURUHOLMEN
- realm = BEOLINK.ORG
- server string = Samba Server
- security = ADS
- svcct1 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
Winbind configuration 3/5

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
Winbind configuration 4/5

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_mkhomedir

- creates home directories for users on the fly.
- session required /lib/security/pam_mkhomedir.so skel=/etc/skel umask=0022
Winbind configuration 5/5

NSS

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

NSCD

- Disable nscd
Write your connector

**Advantages**

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

**Disadvantages**

- Reliability
- Performance
## Performance

<table>
<thead>
<tr>
<th>Application</th>
<th>Cold cache</th>
<th>Warm cache</th>
<th>Remote cold cache</th>
<th>Remote warm cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ldap</td>
<td>2X</td>
<td>-</td>
<td>2.5X</td>
<td>-</td>
</tr>
<tr>
<td>Ldap+ns cd</td>
<td>2X</td>
<td>1X</td>
<td>2.5X</td>
<td>1X</td>
</tr>
<tr>
<td>winbind</td>
<td>-</td>
<td>-</td>
<td>4X</td>
<td>1.2X</td>
</tr>
<tr>
<td>ptserver</td>
<td>-</td>
<td>-</td>
<td>2X</td>
<td>1X</td>
</tr>
</tbody>
</table>

### Value for execution time
unixUserPassword: ABCD!efgh12345$67890
tid: test
msSFU30Name: test
msSFU30NisDomain: beolink
uidNumber: 10000
gidNumber: 10000
unixHomeDirectory: /home/test
loginShell: /bin/sh
msSFU30Name: Domain Users
msSFU30NisDomain: beolink
gidNumber: 10000
Administration Tasks - Processes
Migration

- Dump unix data from ldap
- Script ldif conversion
- Import ldif in AD
- Files Rsync -a
- Join by hand
- Password reset
- Profiles by hand
Achievements

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
Don’t forget..

Licenses
The Unix account is a CAL (cost)

Synchronous
Per domain synchronous child with user and group enumeration

Cache
Single cache for all elements
Results

Cost increased
15% Licenses

Cost reduced
-20% Employees
-30% Consultants

Unchanged Service Level
Results

Cost increased
15% Licenses

Cost reduced
-20% Employees
-30% Consultants

Werbung

openAFS Conference Rome September 28-30

http://www.dia.uniroma3.it/~afscon09/
Thank you!

Website: www.beolink.org
Email: manfred@freemails.ch