

Linux in a Windows World

South Tyrol Free Software Conference

Meran

16. November 2007

Volker Lendecke

Samba Team / SerNet



Volker Lendecke

- Co-founder SerNet - Service Network GmbH
 - Free Software as a successful business model
 - Network Security for the industry and the public sector
 - Samba-Support/Development in Germany
- For 15 years concerned with Free Software
- First patches to Samba in 1994
- Consultant for industry in IT questions
- Co-founder emlix GmbH (Embedded Systems)



Overview

- Linux clients in a Windows environment
- Aspects of Unix/Samba as a server
- Clustered Samba
- Samba4



Current market situation

- Windows is everywhere. Well, almost...
- Linux has found its way into the server space: Webservers, Mailservers, Firewalls, etc.
- Network Attached Storage (NAS): Many 100 Euro class network hard disks based on Linux/BSD and Samba
- Samba has a good position as a file server, along with many Domain Controller installations, some very prominent: City of Munich, German Parliament
- Active Directory is *the* authentication source



Linux on the Client

- There's only few servers, much more Clients
- For me Linux as a workstation OS works perfectly well for ages, but I'm not representative I think :-)
- CIFS is everywhere
- Samba adapts to the Windows client, Linux clients need to adapt to Windows servers
- Make Linux a proper domain member
- Provide good integration into Windows file and print Server infrastructure



Active Directory

- Active Directory holds all account information
 - Users, Groups, Machines, all passwords
 - Users can log in anywhere on the network, passwords are managed centrally
- Single Sign on works pretty well within the Windows world
- Linux machines need to participate: AD users need to be valid on member servers and clients



Winbind

- Linux/Samba needs to act as a first-class AD member
- Winbind fetches AD user and group information
- All AD users and groups are valid on Linux
 - Same mechanism that nss_ldap uses: nss_winbind
- Authentication of users is done via the AD infrastructure
- Group memberships (i.e. Authorization Information) is retrieved the same way Windows does it



More fancy Windows features

- Offline operation
 - Laptops users log into the domain during office hours
 - Login still works when the laptop is taken home
- Network folders usable at home
 - „make this drive available offline“
- „Power Users“
 - Users expect to be able to share their **d:\mp3** folders with colleagues without the admin interfering



winbind offline mode

- Windows workstations are normal domain members
 - Authentication is online against the DC
- For the SLED product Günther Deschner added cached credentials to winbind
- Users taking laptops home get their environment
- No online verifications of password policies
- Is this secure?
 - Anyone with physical access to the box can mess with the data anyway



Offline folders: /home @ home

- Essentially, this is not solved
- The Coda file system does offline folder access
 - Successor of the Andrew File System
 - Part of the Linux kernel for many years
 - Nobody uses it, it's abandoned (Peter Braam did Intermezzo and then Lustre, now he's rich ;-)
- Very likely a replication scheme is more appropriate
 - Network File Systems are a bad idea anyway...



Non-root share definitions

- Using Windows XP, non-Admin users can be given the privilege to maintain their own shares
- Jeremy Allison added the „usershare“ parameters
- Administrators can give users the ability to define shares
- Very strict set of settings can be done by users, „force user = root“ would be fatal
 - Path, comment, and an ACL can be set by the user



CIFS Unix Extensions

- Linux Server, Windows Client is solved
- Windows Server, Linux Client via Steve French's cifs
- What about Linux Server, Linux Clients?
 - NFS: No File Security, Needs Fifty Sysadmins
- Unix extensions to CIFS provide Posix compatibility
 - Locking better than NFS
 - Symlinks, Sockets, Device Nodes
 - KDE works using /home mounted via CIFS



Windows ACLs

- Access Control features are very often blocking Unix/Samba deployments
- Traditional Unix access control is very limited
 - Posix ACLs help, but don't make it much better
- Windows can delegate the permission to change ACLs
 - IT departments do not know if Posix is sufficient
- NFSv4 ACLs are a lot closer, but not 100%
- Samba *could* implement NTFS ACLs, Samba4 does



Clustered Samba I

- All fully correct CIFS clustering solutions so far are Active/Passive
 - Locking information often not correctly propagated
 - Non-Clustered Samba on GFS corrupts data
- File systems can only be exported via a single node
- Wasted resources, file system checks on failover
- Clustered Samba will be the first real Active/Active CIFS server



Clustered Samba II

- Requirements:
 - Shared storage access via a SAN or drbd infrastructure
 - Clustered File System like GFS or GPFS on top (OCFSv2 is not sufficient yet)
- Clustered TDB (ctdb.samba.org) implements the Samba Lock Manager
- Clustered Samba version
 - xcopy survives a node failure!



Samba 4

- Samba4 started out as a new Virtual File System to Samba3 to enable clustering, Samba3 infrastructure was very insufficient at that time
- Start from scratch, provides great infrastructure, but lacks a lot of features
- Research branch of the Samba project (smbtorture!)
- Full Samba3 successor very unlikely within 2-3 years
- Possible: Pure AD controller that utilizes Samba3 for everything else



The EU/Microsoft case

- Microsoft has been found guilty to abuse its desktop market share to gain a dominant position in the Workgroup Server Market (AD DCs are part of this)
- Remedy: Money and open up protocols
 - License on protocol information is critical
- The EU announced that the protocols will be available for Open Source Projects
- Will Samba be able to benefit? We don't know yet, we are examining the consequences closely.



Questions/comments?

Volker Lendecke, VL@SerNet.DE

SerNet - Service Network GmbH
Bahnhofsallee 1b
37081 Göttingen

Tel: +49 551 370000 0

Fax: +49 551 370000 9

<http://www.SerNet.DE>

<http://Samba.SerNet.DE>

