

samba *experience*

Samba 2.2 -> 3.0 Seamless Migration

a case study



Schlomo Schapiro
Senior Consultant
25.04.06

Agenda

- **Seamless Migration**
- **The Customer**
- **Migration Overview**
- **Challenges**
- **Solutions**
- **Lessons Learned**

Seamless Migration

- **must be identical**
 - domain SID
 - user & machine RIDs
 - machine account password hashes
 - logon scripts (drive assignments)
- **should be identical**
 - user account password hashes
 - server & share names
- **can be all different**
 - backend
 - management

Klinikum Barnim GmbH



- regional hospital in Eberswalde (Brandenburg)
- ca. 450 beds, 14 wards
- ca. 350 PC workstations used 24/7
- ca. 1000 staff working a 3-shift duty cycle
- total dependency on IT in all departments:
 - operation theaters, clinics & wards
 - labs, CT, X-ray, ...
 - internal communication
 - services for external customers (labs, CT, radiology, ...)

Current IT landscape

- Linux only used on servers and backend systems
- most systems run SLES8 (SP3)
- DRBD / heartbeat cluster with Samba 2.2.5 as PDC
- 5 major file servers with Samba 2.2
- few individual accounts (<100 user accounts total)
- no UID management, most shares only for selected users
- no ACLs
- no user groups
- manual user management (useradd, smbpasswd, ...)
- individual logon scripts per user (%U.bat) !

Migration Overview

- ongoing general migration SLES8 -> SLES9
- introduction of VMware ESX in 2005
- VMware for high availability (3 ESX Servers)
- migrated all file servers „as-is“ into VMs
- 3-step migration
 - PDC and 1 file server
previously PDC and file server on same machine
 - remaining file servers
SLES8 -> SLES9
 - extra features:
WINS Slaves
LDAP Slaves

User Management

- **Samba 3 PDC**
 - Virtual Machine, no clustering
 - LDAP based
 - better user management – GUI based
- **Samba 3 file servers**
 - optimal integration via LDAP
 - global UID management
- **Integrate other services via LDAP**
 - mail
 - proxy
 - web servers (intranet, ...)

Challenges

- (Almost) no downtime possible (2-3 hours Tue evening is the maximum possible)
- impossible to clone everything for test environment
- seamless migration a must (SIDs), no room for errors
- segmented network, rely on WINS
- logon script migration
- group management
- IP address migration (to 192.168/16)

Solutions - PDC

- Samba 3.0.14a
- LDAP server runs on PDC
- smbldap-tools
- create domain with same name & SID
- custom script to create LDIF entries from passwd and smbpasswd files taken from old PDC
- copy-and-sync of data (20G)
- create groups, sort users into new groups
- new logon scripts (KiXtart)
- switch off old PDC, connect new PDC to network with old IP

Solutions – File Servers

- Samba 3.0.14a
- use LDAP server on PDC

- exchange OS with preinstalled SLES9, data is on own HD
- very quick with Virtual Machines
- chown data files to correct UIDs
- setfacl to the new groups

Tests – Test Migration

The road to success is paved with tests

- **ca. 5 Virtual Machines make the test lab**
 - **PDC & WINS**
 - **file server**
 - **windows clients**
- **windows clients are cloned or switched from production systems to prove machine account continuity**
- **test uses independent network with identical IPs**
- **some test machines can remain in production network and use test server by changing the „WINS server“ setting and tricky routing**
- **develop groups and login scripts in test lab**

Solutions – Final Migration

- **turn test PDC into production PDC**
 - **synchronize hashes one last time**
 - **new PDC uses old PDCs IP addresses**
 - **disconnect old PDC from network**
- **turn test file server into production file server**
- **quickly verify login scripts with all user types**
- **LDAP-based user management**
 - **Browser: LAM – LDAP Account Manager 1.0.1**
 - **Windows: User Manager for Domains**
 - **Linux: smbldap-tools**

Future Features

■ Samba4WINS

- replicated & redundant WINS servers

■ personal user accounts

- Samba 3 / LDAP prerequisite to manage >1000 users
- integration with email, intranet, ...

■ Samba 4

- customer introduces now Citrix Servers, Windows admins beg for ADS and group policies
- proper sub-domains for other hospitals of the same corporation. They have already ADS.
- easier management

Lessons Learned

- Samba 3 / LDAP – complex system with many pitfalls
 - LDAP and Linux skills essential
 - adding new member servers too complex
 - no How-To for this scenario ? (Hope to write it ...)
 - but: Samba 3 is the best CIFS server
-
- wish list for Samba 4:
 - easy-to-use system out-of-the-box
 - easier integration of member servers, BDC support, ...
 - full ADS feature set – mixed Windows/Linux ADS

Thank you very much – Q&A / discussion



Schlomo Schapiro
pro|business Berlin AG
Potsdamer Platz 11
10785 Berlin
Telefon 030 / 25 93 78-23
Telefax 030 / 25 93 78-22

pro|business
Berlin AG

www.probusiness.de

sschapiro@probusiness.de

