IBM Global Services

From OS/2 to Windows to Samba
A Journey to Open Source

John Janosik – jpjanosi@us.ibm.com
Bill Marshall - bmarsh@us.ibm.com

samba eXPerience 2005

May 4, 2005

Agenda

- Environment
- Simple file server migration
- Complex file server migration with Posix ACLs
- OS/2 to NT Domain migration
- NT to Samba Domain migration
- Conclusion

Environment – March 2002

- **Seriously started looking for a migration option away from OS/2**
- **4 terabytes of data on 50 servers**
- **OS/2 domain with 6000+ users**
- **Mostly Windows NT & 2000 clients**
  - Approximately 4000 Windows clients had joined a NT domain for minimal client management
  - Users sign on to systems with local accounts
- **Knew OS/2 was end of life, but had been waiting for direction on where to go**
  - Windows clients had been causing problems against OS/2 servers (session setup with vc=0 was using resources)
  - XP service pack 1 broke more things
- **Throughout 2002 we experimented with Samba servers for IT use**

Theory of Migration – January 2003

- **Realized there were 3 main problems to solve in order to transparently move users from OS/2 to another platform**
- **In no particular order:**
  - Operating system transparency
    - Samba/Linux looks like Windows, but can it function like OS/2?
  - Location transparency
    - Ability to move data from \\server01 to \\bigserver02 without users needing to change anything.
  - Authentication transparency
    - For a Windows domain you can “net vampire”
    - Deliver a new NT account, with the same password, without the user having to know or change anything

Data Migration

- **Tried many options to move the data from OS/2 to Linux**
- **Needed an incremental method**
  - Servers up to 280 GB in size
  - Boot knoppix CD on the OS/2 server, mount OS/2 HPFS partition and rsync
    - Found bugs in the HPFS driver
  - Net use to Samba and push from OS/2 server
    - OS/2 xcopy does not handle large trees
    - Windows xcopy moved the data across the network twice
  - Eventually, used rsync and smbfs
    - However, there were some problems in smbfs against OS/2 servers
    - Steve French helped with code changes to work around some problems
    - Added a windows based perl script to do a tree compare and a final copy
- File ownership and ACLs were another matter

File Server Migration

- **All users are able to map through a Samba hosted distributed file system (location transparency)**
  - \\rchfs\home\userid or \\rchfs\group\share
- **Migrations took place during the weekly Friday night outage window**
- **When a server was replaced:**
  - Server was renamed and kept online
  - Once comfortable the data had migrated (a couple weeks), reloaded the system with Linux and reused the hardware
- **Administrators had minimal Linux skills, came from Windows background**
  - Created simple perl client/server code to create Samba shares and set initial ACLs from the Windows command prompt

Automation of Share Migration

- **OS/2 REXX scripts created:**
  - Linux bash scripts to smbmount OS/2 servers under Linux
  - Bash scripts to rsync the data from OS/2 to Linux
  - Cutover scripts to add Netbios aliases to smb.conf, etc.
  - smb.conf entries for shares
- **During the week, the majority of the data was rsync'd**
- **On Friday nights**
  - a final sync of the data was done
  - Linux/Samba system moved into production
- **At the end or our migrations, "at" jobs on Linux were used to do the migrations automatically**

Simple Server Authorization - smb.conf sample

- **No ACL support in JFS & Red Hat kernels in 2002/2003**
- **Initially, used smb.conf parameters to allow & restrict access**
- **If needed, created “fake” groups for all shared project space and used force group to put people into the group**

```
[vaj30]
   comment = Temporary VAJ space
   path = /home/group/vaj30
   writeable = yes
;   read list = vaj30
   write list = vaj30
   force group =  vaj30
   create mask = 0770
   force create mode = 0770
   force directory mode = 0770
   directory mask = 0770
   valid users = @vaj30, root
```

Simple File Server Authentication

- **No real domain (winbind) integration against OS/2**
  - Initially, /etc/passwd & /etc/group built from OS/2 information and used **security=server** for passwords
    - **security=server** unreliable in Samba 2.x, OK in 3.x
  - Then **security=user** with smbpasswd built from password hashes dumped every 10 minutes from DC
    - Later realized this meant we could easily stop using our OS/2 DCs once all the OS/2 servers were converted
  - Passwords changed via web, added hook to push the hashes to Linux
- **Home directory servers migrated & merged first**
  - Used DNS & Netbios aliases to combine servers
- **First server migrated from OS/2 to Linux/Samba in late January 2003**
  - No one noticed!

Complex ACL File Server Migration

- **Some servers did not fit the simple access control scheme**
- **Samba & kernel improvements allowed us to continue**
  - Built a kernel w/ JFS to allow ACLs and upgraded Samba
- **OS/2 command file was used to export the ACLs from HPFS**
- **Linux Perl script read the output from OS/2 and used setfacl on JFS**
- **OS/2 ACLs allowed read, write, execute and delete so they map easily to Posix ACLs**

OS/2 to NT Domain Migration & Authentication Transparency

- **Merge of OS/2 and NT domain**
  - All users created in NT domain in a “big bang”
  - At first, continued running security=user
  - Documentation changes told people the OS/2 domain was gone
  - Next, configured winbind and joined Samba servers to the NT domain
  - Samba servers with security=domain were modified to fail over to smbpasswd file on bad password
    - Smbpasswd file was correct
    - Domain passwords were incorrect until a password change
    - Still running Samba 2.2.X.
  - Password changes via web interface
    - Update NT domain passwords
    - Pushed updated smbpasswd to all systems with rsync until all systems were in the domain and running winbind

Alternate OS/2 Domain Migration Options

- **Pushing LM hash into NT SAM**
  - Required changing ACLs on registry entries in the SAM on the domain controller
  - This option rejected because the gain was minimal for the risk
- **If migration occurred now bypass NT migration**
  - Easy to script creation of ldif of Samba attributes via information dumped from OS/2 domain
  - We didn’t have experience with Samba domains at the time and the performance issues were not yet solved.

NT to Samba Domain Migration

- **Research started in April 2004**
  - Samba 3.0.4 was current at the time
- **LDAP passdb backend was our only option**
  - Had multiple NT DCs
  - Did not want to give up redundancy
  - Wanted to learn skills that would apply to customer use of Samba

Initial Assesment

- **Performance issues with our setup**
  - smbldap tools useradd slowed down as number of users grew
  - Migrating users/groups via vampire took too long
    - timed out during the group migration
  - Some RPCs made by winbind were handled inefficiently by Samba domain controllers
- **We thought about moving away from winbind on the member servers**
- **Migration was postponed until the end of 2004 and winbind was retained for supplying posix users/groups on member servers**

Migration Improvements

- **The IDEALX smbldap tools were fixed to store the next uid/gid in LDAP instead of iterating through the users or groups**
- **Options to reduce migration time**
  - Vampire to tdb with local posix users/groups, then dump to ldif
    - Fastest but required patch to pdbedit
    - Would not work for customers who already had users in ldap and just wanted to add Samba attribtues
  - Vampire to tdb with LDAP posix users/groups, then use pdbedit to switch backends
    - Slower but the process can be split up
    - Once posix users/groups were in place subsequent runs to a new passdb.tdb took less than an hour

Performance Improvements

- **Iteration of all users/groups was affecting us in the following cases**
  - winbind querying the domain sequence number
  - winbind querying the members of a group
- **Logs showed 50 seconds spent waiting for LDAP query.**
  - An OpenLDAP developer in IBM provided a patch that improved synchronous LDAP searches from 50 seconds to 3 seconds on our 20,000 account test box
- **Even with openLDAP improvements winbind was still timing out**

Workarounds

- **Stopped winbind from querying domain sequence number**
  - Samba DC is returning current time anyway
- **Created “winbind timeout” smb.conf parameter**
  - Even with these workarounds sometimes the default timeout of 10 seconds was not enough
- **Added new LDAP passdb backend function to directly query LDAP for primary group members**
  - The only large group was domain users which all our users had as their primary group
- **The “winbind cache time” was set to 1 day and the cache was primed offshift via a cron job**
- **Migration was possible but a corporate change freeze caused another delay**

Forced to Action

- **February 2005 NT security vulnerability**
- **Get off of NT, pay for support, or get exploited**
- **Current Samba**
  - Test domain Samba 3.0.11rc/ OpenLDAP 2.2.20
    - OpenLDAP client patch
    - Samba patch to extend ldapsam:trusted
  - File servers Samba 3.0.10
    - patch to extend winbind client rpc timeout
    - patch to disable query domain info rpc in winbind

Migration

- **Initial vampire run was during working hours**
- **Took ~2 hours creating posix users/groups in LDAP but samba attributes in tdb.**
- **Shut down NT BDCs**
- **Re-ran vampire on isolated network to eliminate chance of changes getting missed during run**
  - Much quicker since posix users/groups already there
- **Used pdbedit to migrate passdb.tdb to LDAP**
- **Moved Samba DCs into production and established trusts wth AD domain**

Conclusion & miscellany

- **Samba is *very* flexible**
  - Used 6 different configurations for **security=** & ACLs
- **Built a partnership with the developers in the IBM Linux Technology Center**
- **Experience with large scale external deployments**
  - School district with 50,000+ userids
  - School district with 300-400 servers (one domain per school)
- **Experience with Samba on iSeries Linux & AIX**
- **Samba does “Microsoft” DFS very well. Try it**

Questions?

John Janosik – jpjanosi@us.ibm.com
Bill Marshall - bmarsh@us.ibm.com