Tutorial:
Migration from NT4 to Samba-3

John H Terpstra
Samba-Team
jht@samba.org
Agenda

- NT4 to Samba-3 Migration
  - Review Chapter 31
- Review New Samba-HOWTO
  - Chapters 30, 11, 12, 20-24
- Live Conversion from NT4 PDC to Samba-3 PDC

Please turn to chapter 31 of the HOWTO
Why Migrate?

- Improve manageability
- Improved User Functionality
- Cost control (reduction)
- Reduce exposure – NT4 Obsoleted
- Avoid MS License 6 implications
- Reduce dependency on technology single supplier
Why Integrate?

- Leverage Active Directory
- Preserve existing IT investments
- Do not reinvent infrastructure
- Adding storage – not replacing
  - NAS / Device / Server decision
- Fear
- Staff Familiarity
Samba-3 v's MS Windows NT

- Cost of ownership
- Support availability with NO strings attached
- Features that future life
- Stability, Reliability, Performance, Manageability
Missing from Samba-3

- NT4 Domains -> Win2K and Active Directory
  - Group Policies now go into ADS
    - Machine / System Policies
    - User Policies
  - Logon Scripts can be in ADS
  - Application and Menu Control in ADS
  - Software controls now in Active Directory
Planning Migration

- Read Samba-3 documentation
- Identify environment differences
- Understand what needs to be migrated
- Design BEFORE migration
  - Know how differences will be handled
  - Educate users so they know what to expect
Impact of Site Size

- There are 3 major Site Types
  - <= 50 Users
    - Want simple conversion with NO pain
  - 50 – 250 Users
    - Want new features
    - Can manage some in-house complexity
  - Large Scale Sites
    - Solution / Implementation MUST scale well, complex needs
    - Cross departmental decision process
    - Local expertise in most areas
Planning for Success

◆ Decide which approach is needed – 3 Choices
  – Simple Conversion (total replacement)
  – Upgraded Conversion (could be one of integration)
  – Complete Redesign (completely new solution)

◆ Take sufficient time
  – Avoid Panic
  – Test ALL assumptions
Simple Conversion

- Keep Implementation Simple
- Suck all accounts from NT4 into Samba-3
  - Make least number of operational changes
  - Take least amount of time to migrate
- Live versus Isolated Conversion
  - Integrate Samba-3 then migrate while users are active
- Change of control (ie: swap out)
Upgraded Conversion

- Translate NT4 features to new host OS features
- Copy and improve
  - Old environment to Samba-3
  - Make progressive improvements
- Minimise user impact
- Maximise functionality
- Take advantage of lower maintenance opportunity
Complete Network Redesign

- **Decide**
  - Authentication
    - database location and access
  - ID Mapping
    - Dynamic or Fixed
  - Desktop Management Methods

- **Identify Needs for:**
  - Manageability, Scalability, Security, Availability
Implementation - I

• Authentication database back end
  – Winbind
    ◆ External Samba or NT4/200x server
      – External server could use Active Directory or NT4 Domain
    ◆ Can use pam_mkhomedir.so to auto-create home dirs
  – Database type
    ◆ smbpasswd, tdbsam, ldapsam, MySQL
Implementation – II

◆ Access Control:
  – On the Share itself - Use NT4 Server Manager
  – On the file system
  – Unix permissions on files and directories
  – Posix ACLs enablement in file system?
  – Through Samba share parameters
    ◆ Not recommended – except as only resort
Implementation – III

- Policies
  - Group Policy Editor (NT4)
    - User and Group Profiles
      - Watch out for bleed-through effect
      - Migrate or create new ones
    - Platform specific so use platform tool to change from a Local to a Roaming profile
    - Can use new profiles tool to change SIDs (NTUUser.DAT)
Implementation - IV

- Logon Scripts
  - Location
  - Dynamic Generation
Samba Implementation Choices — V

- User and Group mapping to Unix/Linux
  - *username map* facility may be needed
  - Use *smbgroupedit* to connect NT4 groups to Unix groups
  - Use *pdbedit* to set/change user configuration

**NOTE:**
- If migrating to LDAP back end it may be easier to dump initial LDAP database to LDIF, then edit, then reload into LDAP
Samba Implementation Choices – VI

- OS specific scripts / programs may be needed
  - Add / delete Users
    - Note OS limits on size of name
      - Linux 8 chars
  - Add / delete machines
    - Applied only to domain members
      - Note: up to 16 chars
  - Add / delete Groups
    - Linux limit is 16 char, no spaces and no upper case chars (groupadd)
Migration Tools

- Domain Control (NT4 Style)
- Profiles, Policies, Access Controls, Security
  - Migration Tools
    - Samba: `net`, `rpcclient`, `smbpasswd`, `pdbedit`, `profiles`, `editreg`
    - Windows: NT4 Domain User Manager, Server Manager (SrvTools and NEXUS)

- Authentication
  - New SAM back end (`smbpasswd`, `tdbsam`, `ldapsam`, `mysql`)
Future Outlook

- Management and Control Tools
- Extended Windows Registry integration
- Samba AD Policy Implementation
  - Group Policy Object handling
  - Support for new nested group memberships
  - Machine policy implementation
- Roll-out and Deployment enhancements
Background Information

- Samba-HOWTO-Collection
  - Official Team Documentation
  - Official Samba-3 HOWTO and Reference Guide
    - In Print Nov 2003
- Samba Web site
- Man pages
- SWAT Home page
Summarize So Far ...

- Migration from NT4 PDC to Samba can be done now
- Samba-3 misses some Windows 200x/XP features
  - Samba-3 features compensate for forgone Windows functionality
- Planning and clean implementation will be key to deployment success
Chapter 11 – Passdb

- Samba-3 supports multiple concurrent backends
  - smbpasswd, tdbسام, Idapsam, mysql, xml

- LDAP is only suitable backend for distributed infrastructures
  - PDC + BDCs
    - Need to use idmap backend to ensure consistent UID/GIDs across network
  - Alternative to Active Directory
Passdb tools

- New tools for managing passdb data:
  - Pdbedit
    - Manages detailed content of passdb backend
    - Used together with smbpasswd
    - Can migrate data between backends
  - Need to understand importance of correct LDAP Schema design
    - Also need to have site-specific scripts to manage LDAP backends
Chapter 12 — Group Mapping

- Samba-3 has `group_mapping.tdb` file
  - Stores relationships between UNIX Groups and Windows NT Groups
  - New Tool:
    - `net groupmap ...`
  - Ties with Winbind
    - `winbindd` now does all ID Mapping
      - Handles UNIX ID to Windows SID mapping
    - Uses files: `winbindd_cache.tdb`, `winbindd_idmap.tdb`
Chapter 20 – VFS Modules

- **New Modules**
  - audit
  - extd_audit
  - fake_perms
  - recycle
  - netatalk

- **New configuration syntax**
  - No longer supports external config files
  - Use in-line configuration settings in smb.conf
Chapter 21 – Winbind

- **Note 3 Components**
  - PAM Authentication (pam_winbind.so)
  - NSS Identity Resolution (libnss_winbind.so)
  - IDMAP Handling

- **Winbindd is MUCH more important in Samba-3 than it previously was**
Chapters 22 -24 – Environment Control

❖ Need to be informed about
   – Remote Management Options
   – Logon Script Magic
   – Policy Handling
   – Profile Management
     ❖ Particularly as relates to Group Policy Objects in AD

❖ Management Tools for the above!
Chapter 26 – PAM

- Some PAM implementation support new configuration options
  - Documented
- Need to know how to configure PAM for UNIX / Linux local logins using SMB passdb backend database Accounts
- Opportunity for distributed authentication
Live Migration

- Demonstration of NT4 PDC to Samba PDC
  - Using tdbsam (for simplicity)
Discussion / Questions / Feedback

Nothing Ever Ends: Every Conclusion Is a New Start!