Migration of NT4 to Samba-3

John H Terpstra, CTO
PrimaStasys Inc.
jht@primastasys.com

Overview of John H Terpstra

- Long term Samba-Team member
  - Author of official Samba documentation
    - The Official Samba-3 HOWTO and Reference Guide
      - ISBN: 0131453556
      - Open Source version: Samba-HOWTO-Collection
    - Samba-3 by Example
      - ISBN: 0131472216
      - Open Source version: Samba-Guide
  - Author of additional books
    - Hardening Linux, ISBN: 0072254971 – release soon
    - OpenLDAP by Example, ISBN: 0131488732 (October 2004)
    - More in production

Agenda

- Economic and political factors in choosing Samba
- Windows network choices
- Samba deployment and topology decisions
- Migration planning
- Information Resources
- Problem solution process

Note: Samba-3 by Example book is the core reference document for this Tutorial

Justifying Migration

- Clearly visualize the solution
  - What are the benefits?
  - Why is Samba the best choice?
  - Demonstrate benefits regularly?
- Gain organizational buy-in
- Establish control metrics before starting
  - Provide step-by-step accountability
  - implementation cost / benefit controls
- Perform regular audits

Valid IT Cost Factors

- Hardware
  - Acquisition cost
  - Maintenance and support costs
- Operating System
  - Acquisition cost
  - Maintenance costs
- Network and Desktop Operation
  - Installation Cost
  - Maintenance, Staff & Administration Costs
  - Training of Users

Software Cost Factors

PrimaStasys Inc

- Software
  - Acquisition cost
  - Maintenance
  - Administration
  - User support
  - Sufficiency to meet organizational needs
    - An inadequate solution results in opportunity loss

Risk and Exposure Factors

- Hardware obsolescence during service period
- Probability of Isolation
  - Problem resolution
  - Staffing
- Technology Exposure
  - Intellectual Property concerns
  - Likely change in client protocols

Identifying Hidden Costs

- What is downtime?
  - Lost productivity
    - Viruses are targeting vulnerable MS Windows products
      - Cost of recovery / re-installation
      - Lost opportunity cost
- Potentially productive time spent avoiding downtime
  - Patching and updating

Additional Costs

- Expenses paid for anti-virus and anti-worm products
  - Have limited effectiveness
    - Work after the event
      - Only after the AV manufacturer has a fix
- Resources spent on fixing broken patches
  - Microsoft patches that do not work or that interrupt productivity

Samba-3 network design

- Network requirements
- Choosing the back end database
- Configuring the Samba server

Understand Requirements

- Be aware that management requirements are often expressed in non-technical terms
  - Be sure to deliver what is demanded
    - Measure user needs and requirements
      - Involve users in key change decisions
    - Avoid unnecessary user complexity
      - In desktop impact of change
      - In Samba implementation
        - If complexity is necessary implement it gradually
          - Test every change made on a test network
  - Plan your deployment as if preparing to hand over to your successor
    - Make yourself obsolete as soon as you can

Basic Design Guidelines

- Number of Users is Critical
  - 1–20 users means a *workgroup* may be sufficient
    - Can use *share mode* security
      - S3bE Chapter 2, Examples 2.1 and 2..2
    - Can use a simple *user mode* security design
      - S3bE Chapter 2, Example 2.4
  - 15–50 users *workgroup* may still be best
    - Use *user mode* security but clients can be *workgroup* configured
      - S3bE Chapter 3

More Capable Designs

- 25-100 users *Domain Security* should be seriously considered
    - Improved security becomes a MUST
    - Use *user mode* security
    - Enable Domain Logons (network logon service)
    - Manual machine and user account management is an option
        - Not recommended
        - Best to implement account script interface
        - Can use old style *smbpasswd* back end
            - Is the default if *passdb backend* is not specified
        - Use of group mapping should be implemented
    - S3bE Chapter 3

Advanced Designs

- 100-250 users - *Domain Security* is essential
  - Use firewall on all sensitive servers
  - Use *passdb backend = tdbsam*
    - Note: Can scale to well over 4000 users
  - Consider network administration
    - Use of NT4 Domain User Manager
      - Requires functioning scripts
  - Networks with over 150 users typically span multiple network segments or VLANS
- Limitation of *tdbsam*
  - Can not be replicated across Domain Controllers
  - Means multiple segment design performance problem
- S3bE Chapter 4

The Full Enchilada

- 150-500 users - Beware of management issues
  - Need to tame Windows clients
    - Use roaming profiles
    - Use default user profile
      - Can be used without roaming profile storage
        - effect is low maintenance, zero storage, roaming profiles
    - Implement folder redirection
      - reduces roaming profile file transfer overheads
    - Implement point-'n-click printer driver download
      - ie: Upload to Samba
- S3bE Chapter 5

Introduction of LDAP Back End

- Ideal for routed (multi-segmented) networks
- Scalability at its best
- Complex installation
  - More demanding of network management
  - Best when all servers use the same LDAP directory (user and group account data store)
- Need to use scripts to manage accounts
  - Can use Idealx scripts
    - See http://samba.idealx.org

OpenLDAP Implementation Steps

- Configure *slapd.conf*
  - Schema components
    - Need *samba.schema*
      - Has dependencies
  - Suffix, rootdn, rootpw
  - Directory location
  - Specify indexes
- Configure NSS and PAM
  - Requires nss_ldap and nss_pam tools
- S3bE Chapter 6

Samba and LDAP Configuration

- Installation and configuration of Idealx scripts
  - Can use home-brewed scripts
  - Verify that the scripts work when run manually
- Samba smb.conf
  - Set account scripts (see S3bE Chapter 6, sect 6.3.4)
  - Set LDAP suffix, ldap machine suffix, ldap user suffix, ldap group suffix, ldap idmap suffix, ldap admin dn, idmap backend, idmap uid, idmap gid
  - Add LDAP admin dn passwd (rootpw in slapd.conf)
  - Test, test, test

Samba/LDAP Design Possibilities

- Fail-over LDAP server configuration
- Use of Master and Slave LDAP servers
- Catentating LDAP directories
- Basic and advanced LDAP design possiblities
  - distributing the directory
- Review of S3bE Chapter 7

Performing Migration

- Replacement of Windows NT4 Servers
  - Stand-alone servers
  - Domain member servers
    - Can join NT4 Domains, Samba Domains, Active Directory Domains (Windows 200x ADS)
- Replacement of the NT4 Domain
  - Migration to Samba-3 Domain Control
  - Integrating Samba-3 with Active Directory Domain Control
- S3BE Chapter 8 & 9

Migration Choices

- Samba-3 can replace NT4 Domain Control
  - But Samba-3 can NOT be a BDC to an NT4 PDC
  - NT4 can NOT be a BDC to a Samba-3 PDC
  - Note: Being fixed in Samba-3.2.x
- Samba-3 can be an ADS Domain member server
  - Uses Kerberos protocols plus CIFS protocols

Migration of NT4 Domain

- Choice of back end
  - Beware – contrary to indications in S3bE import/export of data is a challenge
    - Need to migrate from /etc/passwd to LDAP before migration of smbpasswd can be done
    - When migrating from LDAP to smbpasswd – must migrate from POSIX accounts from LDAP to /etc/passwd first
    - Use pdbedit to import/export smbpasswd only
  - Can use tdbsam OR ldapsam
    - Note
      - limitation of tdbsam
      - complexity of LDAP management
- S3bE Chapter 8

Before Migration

- Clean up NT4 Domain User and Group data
- Beware of OS limitations on user and group names
    - May require conversion (change) of user and group names to comply with OS constraints
        - Samba inherits the base OS limitations
- Always do a check migration run to identify accounts that may not migrate correctly/fully
    - Some accounts may NOT have passwords
- Decide policy on machine accounts
    - May be best to rejoin domain following migration

Samba-3 Domain Member Client

- Uses PAM/NSS
- Permits local UNIX/Linux logins using NT4/Samba/ADS Domain credentials
  - user name and password
- Requires joining of the Samba-3 client to the NT4/Samba/ADS domain
- S3bE chapter 9 (client section)

Samba-3 Domain Member Server

PrimaStasys Inc

- Uses NSS/PAM for identity management
- Note winbind options
- Use of IDMAP for SID/[U,G]ID mapping for domain member clients
    - IDMAP tables in LDAP directory are auto-populated by the first Samba-3 Domain Member server that needs to map SIDs to UIDs/GIDS
- S3bE Chapter 9 (server section)

SQUID and Samba-3

- Can implement transparent SPNEGO authentication
- Chapter 11

Performance Factors

- Use of WINS
  - What is WINS?, How does it relate to DNS?
  - What effect on network broadcast activity?
- Location of BDCs
- Effect of multiple versions of Windows updates
- SANS and MSDFS
- Data replication techniques
- A word regarding hardware
- S3bE Chapter 12

Questions

PrimaStasys Inc

Your Turn