Samba-3: Integration and Cost Reduction

John H Terpstra, CTO
PrimaStasys, Inc., USA

UUG BYU, February 19, 2004
Core Messages

- FLOSS holds the keys to innovation
- Server adoption of FLOSS is maturing
  - Protocols are already unified or standardized
- Standardization precedes commoditization
- The Desktop is the current battle-ground
Outline

- Key Challenges FLOSS Faces Today
  - The Role of Standardization
    - Particularly in Large Scale Markets
  - Threats
    - Warrant of Fitness and Public Interest
    - The Battle for the Desktop
    - Responsive Action

- Samba-3 Opportunities
  - Replacement of MS Windows NT4
  - Integration with MS Windows Active Directory
Key User Challenges

- People are creatures of habit
  - Challenged by disruption
  - Dependant on the familiar
  - Sociological factors affect consumer choice

- Change is painful
  - Re-orientation
  - Fear of the unknown
The FLOSS Challenge

• FLOSS is highly disruptive
  – Business Model Changes
    • Forces the business focus to customer service
    • Makes technology a commodity

• FLOSS is under attack
  – Intellectual Property Disputes
    • Patent Claims
    • Licensing Terms
    • Copyright Claims
Consequences of Protection

- Software Patents / Licensing
  - Limit diffusion of innovation
    - Those who pay get to use it
    - Designed to disadvantage non-customers

- Copyrights Protect Author Rights
  - Identifies the Innovator
  - Protected through a delicate legal system

- Central Issue is Reward for Effort
Debunking Myths

• FLOSS is supported software
  - User support
  - Mailing lists with a difference
  - Service Companies

• FLOSS does NOT destroy Innovation
  - Users are tired of forced software updates
  - All products tend towards commoditization
    • That increases the need for innovation
Escape the Maze

• First priority is to understand the problem
  - Who does innovation?
  - What factors drive innovation?
  - How are the fruits of innovation delivered?
  - Who benefits from innovation?

• Need to understand products and their life cycles
  - How do FLOSS and proprietary software compete?
PLC and Standardisation

- PLC theory started with Boston Consulting Group
  - Measuring successful business practices
  - Product Portfolio Matrix
  - How products behave from inception through obsolescence
    - Need to understand key factors

- Standardization is a pre-cursor to mass consumerism

(PLC = Product Life Cycle)
Product Portfolio Matrix

BCG Product Portfolio Matrix

- Wild Cats
- Dogs
- Stars
- Cash Cows

- Market Growth: High, Low
- Market Share: Small, Large
PLC Definition

Product Life Cycle

Sales

Time

Innovators 2.5%

Early Adoptors 13.5%

Early Majority 34.0%

Late Majority 34.0%
Software Development Cycle
Two Roads to the Consumer

- Monopoly and Market Manipulation
  - Selective appeal to customers who can enhance corporate profits
  - Control of distribution channels
  - Valued by investors
    - (who do not like service businesses)

- Standardized Commodity Markets
  - Presumes free market operation
  - Forces shift from technology to needs satisfaction process based service business
Monopolization: Benefit and Risk Factors

- Corporate profit motive is most strong
  - Discriminate in selection of customers

- Technology as a tool
  - To coerce update cycles
  - Maintain barriers against competitive market entry

- Seeks protection of Intellectual Property
  - Patents, Copyrights, Licensing

- Sensitive to the Law of Diminishing Returns
  - Profit versus cost of development limits Innovation
Commoditization: Benefit and Risk Factors

• What is Standardization?
  – Process by which products are made to conform with publicly arbitrated specifications that are designed to eliminate incompatibilities in competitive offers and provide a uniform platform for software deployment.

• What does Standardization do?
  – Removes technology barriers
  – Opens the market to mass commodity adoption
  – Reduces costs of ownership
  – Increases the need for innovation through service
FLOSS and Standardization

- **Natural Partners**
  - Development process is by mutual assent
  - Much focus on backwards compatibility
    - Protects consumer investment in infrastructure

- **Promotes Innovation**
  - Not subject to Law of Diminishing Returns
    - Development model is not economically driven

  - Distribution is economically driven
    - By consumer needs
    - By consumer willingness to pay for services
      - Outsource provision opportunities
Warrant of Fitness

- Recent reaction to software that is provided without Warranty
  - Claims that GPL software is not FIT for Sale
  - Position is that consumers need to be protected

- Monopoly mindset reaction to FLOSS invasion of market
The Public Interest & Software

- Warranty is not necessary when source code is open
  - Anyone can fix something that is broken
  - Anyone can add functionality

- Position that the consumer is best protected by freedom to change without constraint
  - Allows innovation and adaptation of software to new task requirements
FLOSS and the Consumer

- FLOSS and Standardization reduces the cost of market entry for new consumers

- Expands the total market size
  - More consumers = greater service opportunity
    - Product customization
    - Delivery standardization
    - Customer hand-holding (Service Specialisation)

- Combined effect is HIGHER MARKET VALUE
FLOSS Status

- The Server is largely won for FLOSS
  - Apache, Samba, MySQL, PostgreSQL, SQUID, CUPS
  - Linux and xxxBSD

- The Desktop is Maturing
  - KDE / Gnome
  - Applications
    - OpenOffice, Evolution, Mozilla, GIMP

- Conclusion: Desktop is the current challenge
Desktop Dominance – Step I

- **Education**
  - The applications users need already exist
  - Help build reference sites
  - Involvement of LUGs

- **Certification**
  - Linux Professional Institute
Desktop Dominance – Step II

• Get more applications
  – Accounting, Project Management, Reporting, Database client tools

  – Convince development houses to build for FLOSS platforms
    • Convince developers that there is a market for specialty and niche solutions
Desktop Dominance – Step III

• Demonstrate commercial viability
  – Business model built around service and support
  – Close partnership with major FLOSS vendors who have consumer orientation

• Promote greater public acceptance of FLOSS standardization
Call to Action

- All involved in FLOSS activities
  - Help more users with solutions to their problems
  - Help businesses executives to understand the problem solution process
    - Importance of support contracts
    - How to find support staff
  - Help Value Added Resellers to understand HOW to be profitable through customer service and support

- Call for Open Public Standards in Software!
What is Samba-3?

- File and Print Server
- Domain Security Context Controller
  - Handles network logon and access control
- Compatibility
  - Servers
    - MS Windows NT4 / 2000 / 2003
  - Clients
    - MS Windows 9x / Me / NT4 / 2000 / XP Professional
Samba-3: Recent Development

- Goals and Devel. Directions for Samba-3

- New Features & Tools
  - Identity Management
    - `passdb backend`, `idmap backend`, Group Mapping
    - Virtual File System Drivers

- Future Directions & Concerns

- Overview of Integration Choices
  - Kerberos, LDAP/PADL, Samba, VAS
Samba-3: Goals

- Answer user demand for Migration
  - NT4 to Samba-3
    - Better Domain Control
    - Improved Interdomain Trusts
    - Ability to migrate NT4 user and group accounts to Samba-3

- Native Active Directory Integration
  - Ability to run with plain CIFS over TCP/IP

- New / Better Bug Tracking
  - http://bugzilla.samba.org
Samba-3 – More Goals

• More Secure
  – Compatibility with Windows XP/2003
    • schannel and signing support
      – No more need for registry changes on clients

• Better Documentation
  – New Samba-HOWTO-Collection
    • Published by Prentice Hall
      – Can be ordered from Amazon.Com now
  – New Samba-3 by Example
    • Published by Prentice Hall, ISBN: 0-13-147221-6
      – Can be pre-ordered from Amazon.Com now
Samba-3 – More Goals

- Better Internationalisation
  - Required a move to Unicode
  - Necessary to enable newer NT/2KX protocols

- More / Better Admin Tools
  - Allow management of users and groups
    - Not complete yet
      - New `net` command
      - Introduction of the `group_mapping.tdb`
      - Addition of the `profiles` tool
      - Addition of the `editreg` tool (not complete)
New Features

- Active Directory Support
  - LDAP/Kerberos
  - Can join ADS Realm
- Unicode Enabled
- New Authentication Subsystem
  - New loadable multi-module support
    - Passdb, VFS
- Better Security
- New default filename mangling system
- **Net** command
- Windows 32-bit error codes
- Better printer handling
- Migration Support
- Interdomain Trusts
- More ...
Identity Management Changes

- **New passdb backend parameter**
  - Default: smbpasswd, guest
  - Optional:
    - tdbsam, ldapsam, mysql, xmlsam, ldap_compat

- Default preserved Samba-2.2.x behaviour as much as possible

- The *guest* parameter is default
  - Provides default account for the guest user
LDAP Improvements

- Compatibility mode - migrate when ready

- New schema
  - Has support for future features
    - Logon Hours, Logon Machines, Password change control, more ...

- Recommended to use OpenLDAP 2.1.x or later
  - Can use: Sun One ID Server (iPlanet), IBM Tivoli Identity Manager, Microsoft ADAM, Novell eDirectory
Virtual File System Support

- Recycle Bin facility extended
  - New Syntax – read HOWTO for details

- Audit & Extd_Audit modules
  - Extd_audit logs to normal log files
  - Audit logs to syslog only

- Fake_perms module for Profile support
  (for read-only profiles)

- Others: NetAtalk, Read_Only,
  example modules to encourage 3rd party devel.
New Tools

- New or enhanced commands:
  - `pdbedit, net, profiles, editreg, SWAT`
    - Note: editreg is not complete

- New Samba Components:
  - `wrepld` (not complete)
  - `winbindd` – now manages ID-mapping
    - `group_mapping.tdb`
      - stores NT <-> UNIX ID database
Samba-3 by Example

Practical Exercises to Successful Deployment

JOHN H. TERPSTRA

Get Samba running right, the first time... every time!

With the Samba 3 cookbook you've been searching for! This book's complete configuration files, step-by-step implementation instructions, network diagrams, and automated scripts make Samba 3 deployment a breeze. From small-office networks to enterprise environments, these proven configuration and script solutions will do the job.

Networking/Samba

"The breadth of technical information provided in this book ensures that even the most demanding Samba users will find something they need."

—Andrew Tridgell, President and CEO, Samba Team and the original author of Samba

About the Author

JOHN H. TERPSTRA is a long-time member of the Samba Team, a loose-knit group of about 30 people who contribute regularly to Samba. He co-authored The Official Samba 2 & 3 Network Reference Guide.

ABOUT THE EDITIONS

Bruce Perens is an Open Source evangelist, developer, and consultant whose software is a major component of most successful, embedded and Internet-based Linux systems. He has contributed to the Open Source Software Initiative, and Software in the Public Interest. As Debian GNU/Linux Project Leader, he was instrumental in getting the system to two U.S. Space Shuttleflights.
Samba Futures

- Samba-4 is already well under way
  - Re-write from the ground up
    - Being done by Andrew Tridgell – Founder of Samba
    - Improved Modularization
    - Code Clean Up, PIDL (new IDL Compiler)
  - Approx. 2 Years from completion

- Samba-3 will gain back-ports of some Samba-4 features
Facts to Note

- CIFS is not a standard
  - Constantly changing
    • Microsoft updates add proprietary functionality
  - Protocol is extremely complex
  - Risk that after any service pack or on-line update an old protocol may be broken
    • Affects Microsoft clients as much as Samba
    • Means ALL systems must be kept up to date and at the same update / revision level
Future Concerns

- What MAY change
  - We need to understand the market to see what may happen

  ... Let's look at some graphs
Installed Desktop Market

Desktop Client Installed Base

- Units (millions)
- Year

Legend:
- Other
- Linux
- MacOS
- MS Win32
Market Conclusions

- MS Windows is Dominant Server Platform
  - CIFS is the dominant File and Print Protocol
    - Is NOT secure
      - Must change!!!!!!
    - Is NOT UNIX/Linux oriented
      - Protocol addresses the needs of NTFS

- Windows 200x/XP server shipments exceeds UNIX+Linux
  - Therefore likely to remain dominant well into the future!
Even More Futures

- CIFS is complex - it is time to replace it
  - Session encryption built-in
    - Protected by legislation against reverse engineering
  - Opportunity for Microsoft to replace underlying file system architecture
    - If NTFS can be replaced with an object based technology that has dynamically expandable metadata capabilities:
      - Means new security measures can easily be added
Market Information

- MS Windows NT4
  - Migrating to MS Windows Server 200x
    - With Active Directory
  - Migrating to Samba-3
    - To avoid licensing costs

- Microsoft Active Directory adoption is growing

- NAS / UNIX / Linux CIFS usage is growing

- Therefore:
  - Integration need growing
**Problem Definition**

- **CIFS File System operations require**
  - **Authentication**
    - Front-end to access controls
    - Datastore location is a network design decision
      - Can be local to each device or centralized
    - Must know limitation of protocols and methods
  - **Identity Resolution**
    - Needed to provide unique attributes per user
    - Used to control access to CIFS resources
    - Needs to bridge disparate identity attributes
User Identity Differences

- UNIX / Linux User Identifiers
  - Older – 32 bit Unsigned Int
  - Newer – 64 bit Unsigned Int

  - uid=543(jht) gid=876(users) groups=876(users),71(ntadmin),238(engrs)

- MS Windows has complex security identifiers
  - Incompatible with UNIX / Linux eg:

  - S-1-5-21-1593769616-160655940-3590153233-2013
Bridging the ID Gap

- MS Windows Security Identifiers
  - Design Issues
    - Map to UNIX compatible UID/GID
      - On central store
      - On client / domain member server
    - Store extended information in AD Schema
Cross Machine Integrity

How to ensure integrity:

- Provide Consistent UID/GID for all users
- Essential for cross protocol file sharing
  - CIFS / NFS

Centralization v's Synchronization

- Sync solution requires more supervision
- How secure is sync method?
Technical Background

- **Microsoft Active Directory**
  - Kerberos / LDAP support
  - In a Windows only environment this uses proprietary protocols

- **AD is the Authentication and Identity management backend of choice**
  - Provides centralized network user identity administration
  - Integrates with external directories through tools like MIIS (was MMS – Microsoft Metadirectory Service)
What works with AD?

- Interoperability Choices
  - Kerberos – complex to install, addresses Authentication
  - LDAP – Identity Management, does not address Authentication
  - Samba Windbind
    - Authentication and Identity Management
    - Has own ID Map solution
  - Vintela Authentication Services
    - Authentication and Identity Management
    - RFC2307 schema extension for UID/GIDs
Pure MIT / Heimdal Kerberos

Key Limitations

- Must generate a per client keytab file
  - Need to migrate keytab to each client

- Time must be kept in sync between AD servers and all Kerberos clients
  - Uses extra external process (NTP)

- Inconvenient Authentication Only solution
  - Requires client machine pseudo-user account in AD
  - Must sync /etc/passwd with AD User Accounts to provide UID/GIDs etc.
  - No disconnected mode operation
PADL LDAP Tools

- Available from PADL Software
  - Two modules:
    - pam_ldap, nss_ldap
  - Benefits:
    - Runs on most UNIX platforms today, Free
    - Supports RFC2307 + MS Windows Services for Unix

- Disadvantages
  - Poor Scalability
  - Lacks secure authentication to AD
  - No disconnected mode operation
Samba Winbind

• Has three parts:
  – PAM: pam_winbind.so, handles authentication
  – NSS: libnss_winbind.so, handles identity management
  – Daemon: winbinddd, handles communication with remote NT4 DC's and with Active Directory DCs
  – Caches user ID info in winbinddd_cache.tdb

• New to Samba-3.0.0 winbind also does all Samba ID Map handling
  – Stores mapping info in winbinddd_idmap.tdb
  – Maps Windows SIDs to Unix UIDs/GIDs
Vintela Authentication Services

- **Commercial Solution**
  
  - AD RFC2307 AD Schema Extension
  
  - Microsoft Management Console Snap-In
    - UNIX Account enablement / disablement
    - Stores UID/GIDs and other UNIX account attributes
  
  - Uses secure Kerberos authentication
    - LDAP over Kerberos
  
  - AD member client cache
    - Stores only UNIX enabled account info
    - Does periodic intelligent sync to keep current
Making the Choice

Viable choices are:

<table>
<thead>
<tr>
<th>Method</th>
<th>Authentication</th>
<th>ID Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samba Winbind</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Vintela Authentication Services</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Both</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>
Questions / Comments

Presentation Available From: http://samba.org/~jht/Presentations