#### Samba-3: New Directions

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

Co-Founder Samba-Team jht@samba.org



#### Agenda

- Goals and Directions for Samba-3
- New Features
  - Identity Management
    - The new passdb backend
    - The role of *idmap backend*
    - Group Mapping
  - Virtual File System Drivers
- New Tools

#### 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

opening windows to a wider world

#### 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 "The Official Samba-3 HOWTO and Reference Guide", ISBN: 0-13-145355-6
      - Can be pre-ordered from Amazon.Com now



#### Samba-3 HOWTO & Ref Guide

TERISTRA

F

#### Networking/Samba

"The breadth of technical information provided (in this book) ensures thet even the most demanding of administrators will find something they need." --Andrew Tridgell, President of the Samba Team and the original author of Samba

#### THE OFFICIAL SAMBA-3 HOWTH and Reference Builde

#### JOHN H. TERISTRA AND JELMER R. VERNOOIJ, EDITORS

The practical, authoritative, step-by-step guide to cutting IT costs with Samba-31 It is to be definite gate to using Santa-2 in protectice environments. It tegts with the innerse encurt of #0MTD internation published by the Santa-2 in protectice environments in the word ... but that's just the beginning. The boot's Santa-Team either have agained and edited this naterial around the practical seeds of working Windows administration burkduing and what are present to be present as well.

Wieler you're deploying Santae brithe find time, mlegrading Santae Into a Windows 2000 Achte Directory envlorment, mlysiding fram AT 4 or Santae 2, a crusing Santae in a UHKQ/Luna ei vonnemt you'll frad riep-by step suktoru, caredu by edied for accuracy, pactorally, and clarby frad i learnai you reed to make intelligent deployment decisions, get etist, and use Santae 25 powerbu een learnas to maker intelligent deployment decisions, get unning task, and use Santae 25 powerbu een learnas to maker in performance and mit hab cost.

#### Step-by-step installation techniques and proven configurations that work "right out of the box"

Essential Samba-3 information that leverages your Windows networking knowledge

Detailed coverage of Samba-3's powerful new rest/machine account management, newonit browsing, and mapping capabilities

Authoritative explanations of advanced leatures such as interdomain inusts and loadable VFS file system drivers

Dear information on Now Samba-3 handles Windows desidop/userpolicies and profiles

Practical fectiniques for optimizing network printing

Specific guidance for migration from Windows NT 4 or Semba 2.x

Troubleshooting bechniques that draw on the knowledge of the entire Samba community

#### ABOUT THE EDITORS

LOHIN H. TERPST RA and JELMER R. VEHNOOU are members of the global Samta Team, a locae tintigroup of about 30 people also contribute regularly to Samba, John H. Terpital is a co-founder of the Samba Team.

Series Exitor GRUCE FORENS is an Open Source-exangelist, developer, and consultant whose software is a major component, of most commercial embeddied Linux offerings. He founded or co-bunded Linux Standard Gase, Open Source inflative, and Software in the Public Interest. As Geblan GNL/Linux Project Leader, he was leatmented in geblag the system on two U.S. Space Southe Lingts.

U.S. \$49.99 Canado \$75.99 PREMICE HALL Portestanti Technical Reference Upper Sactile Recr, NJ 07458 www.clafcom



BRUCE PERENS' OPEN SOURCE SERIES

#### THE OFFICIA SAMBA-3 HOWTO and Reference Guide



 Expert information, straight from the source—written by members of the Samba-team

saryba

 Extensive coverage of Samba-3's new features, including user policies and desktop profiles

Includes useful information for Windows administrators making the switch to Samba

JOHN H. TERPSTRA AND JELMER R. VERNOOIJ, EDITORS

Foreword by Andrew Tridgell, President of the Samba Team and the original author of Samba

#### 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)

opening windows to a wider world

#### **New Features**

- Active Directory Support
  - LDAP/Kerberos
  - Can join ADS Realm
- Unicode Enabled
- New Authentication Subsystem
  - New loadable multimodule 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 available so administrators can migrate when they are ready
- New schema
  - Has support for future features
    - Logon Hours, Logon Machines, Password change control, more ...



#### LDAP Recommendations

- 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 3<sup>rd</sup>
   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 and the need for Standardisation

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

Samba-Team Co-Founder jht@samba.org



#### Agenda

- Short history of Samba/MS Windows protocols
- Brief review of recent protocol changes
- The future of Samba
  - What must change
  - What may change
  - Preferred Action
- Summary

#### Short History

- Server Message Block (SMB) protocol
  - Developed by IBM/3Com/Microsoft
  - Documented as in RFC1001/1002
  - Published by Xopen Committee
- Approx. 1992:
  - Windows NT3.1 protocol enhancements
- Approx. 1995:
  - Extended for NT4

#### More Recent History

- Protocol Renamed to:
  - Common Internet File System (CIFS)
    - Provides significant extensions
    - Samba-Team helped to document protocol
      - Necessary for implementation
        - NT4 / 200x Domain Control Implementation
    - Microsoft Published Documentation
      - Does NOT cover DCE RPC Protocols
        - Does NOT cover the Domain Control Protocols that sit on top of them either



#### **Recent Changes**

- Original protocols very insecure
  - Uses anonymous connection to IPC\$ share
    - Trusted and can open possible exploits
  - Microsoft have implemented techniques to tighten security
- Original SMB protocols use: SMB / NetBIOS / TCP/IP == NetBT Uses B/Cast or WINS (NOT DNS)
- Also uses:
   DCE RPC / Named Pipes / NetBT Slide 17

#### More Recent Changes

- MS Windows 200x / XP
  - Can run without NetBIOS over TCP/IP
    - Can run: SMB / TCP/IP == NetBIOSless SMB
      - Heavily depends on DNS
  - Introduces Digital Signing
    - Encryption
      - schannel, sign'n'seal
    - Not the same as encrypted passwords!
  - New protocol extensions (DCE RPC)
    - Auto added with service packs

opening windows to a wider world

#### Futures – I

- What MUST change:
  - CIFS is not a standard
    - Constantly changing
      - Adding 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



#### Futures – II

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

#### ... Let's look at some graphs



#### The Installed Server Market





## New Server Shipment OS Profile



opening windows to a wider world

#### Installed Desktop Market





#### More Futures

- Conclusion from market information:
  - MS Windows is Dominant Server Platform
    - CIFS is the dominant File and Print Protocol
      - Is Insecure
        - Must be made more secure!!!!!
      - Is NOT UNIX/Linux oriented
        - Protocol addresses the needs of NTFS and Win200x/XP
  - Windows 200x/XP server shipments exceeds UNIX+Linux
    - Therefore likely to remain dominant well into the future!

samba opening windows to a wider world

#### **Even More Futures**

- CIFS is so complex that 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 meta-data capabilities:
      - Means new security measures can easily be added



#### Futures – III

#### Action

- If we want MS Windows networking to be more UNIX/Linux enabled:
  - Need CIFS protocol extensions that are:
    - More POSIX oriented (NOT just Windows ACLs)
    - Semantically closer UNIX/Linux file system support
  - Need client drivers for MS Windows
- Need agreed public standards
  - So Businesses / Governments can specify them
- Need a clear roadmap to the future

opening windows to a wider world

#### Summary

- The future of MS Windows networking protocols will remain uncertain and unpredictable
  - We need a roadmap for stability and interoperability
- Samba is threatened by changes to the protocols
  - We need publicly arbitrated standard protocols for all IT file and print services

# Integrating UNIX and Linux with Active Directory

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



## Agenda

- Definition of the Integration Problem
- Technical Background
- Review of Solution Choices
  - Kerberos
  - LDAP
  - Samba Winbind
  - Vintela Authentication Services
- Making the choice for CIFS ID Management
- Demonstration

#### Market Information

- MS Windows NT4 Migrating to MS Windows Server 200x
  - With Active Directory
  - NAS / UNIX / Linux CIFS usage is growing
- Therefore:
  - Integration need growing



#### Server Market Share - 2001

#### 15.4 Million of Servers





#### Market Share – Forecast 2005

#### 21.1 Millions of Servers





#### **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 Windows only environment also 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 Athentication
  - 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

opening windows to a wider world

### 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 Service for Unix
- Disadvantages
  - Poor Scalability
  - Lacks secure authentication to AD
  - No disconnected mode operation

opening windows to a wider world

#### Samba Winbind

#### Has three parts:

- PAM: pam\_winbind.so, handles authentication
- NSS: libnss\_winbind.so, handles identity management
- Daemon: winbindd, handles communication with remote NT4 DC's and with Active Directory DCs
- Caches user ID info in winbindd\_cache.tdb
- New to Samba-3.0.0 winbind also does all Samba ID Map handling
  - Stores mapping info in winbindd\_idmap.tdb
  - Maps Windows SIDs to Unix UIDs/GIDs



## Samba Winbind Pros:

- NO disconnected mode operation
- Authentication and Identity Management
  - UNIX Accounts AND for Samba
- Scalable through caching of data
- Cons:
  - Same UID/GID across all Samba servers ONLY with LDAP Account backend
    - Complex configuration
  - Exposes ALL backend accounts
    - NT4 Domain / Active Directory Domain

opening windows to a wider world

### 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

opening windows to a wider world

#### Vintela Evaluation

- Pros:
  - Has disconnected mode operation
  - Easy configuration
  - Consistent UID/GIDs
  - No local accounts needed
  - Scalable
  - UNIX / Linux machines get AD Machine Account
- Cons:
  - Commercial (Payware)

#### Making the Choice for CIFS

#### Viable choices are:

Method	Authentication	ID Management
Samba Winbind	OK	OK
Vintela Authentication		
Services	OK	OK
Both	OK	OK



#### **Demonstration & Questions**

