Samba in Business

PrimaStasys Inc

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

Agenda

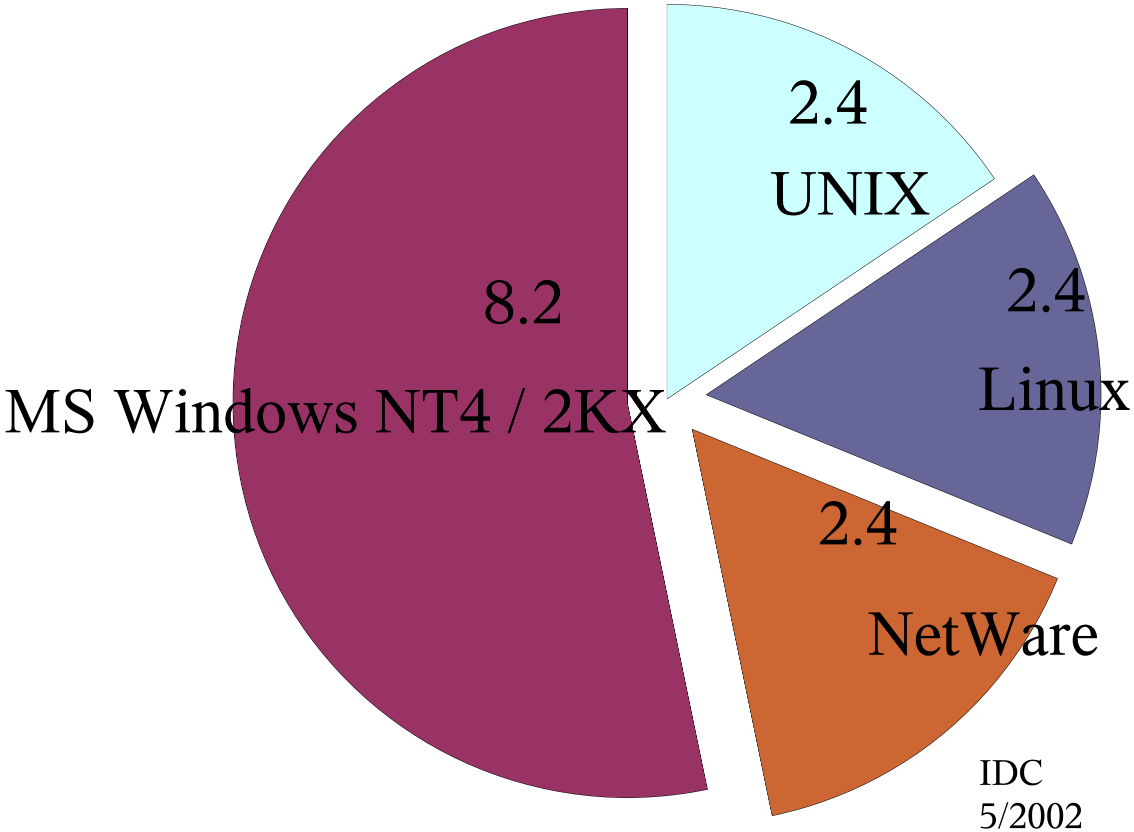
- Definition of the Integration Problem
- Technical Background
- The bigger picture
  - Samba as a replacement for NT4 / Win2K back end servers
  - General Samba configuration
- Futures

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 Servers

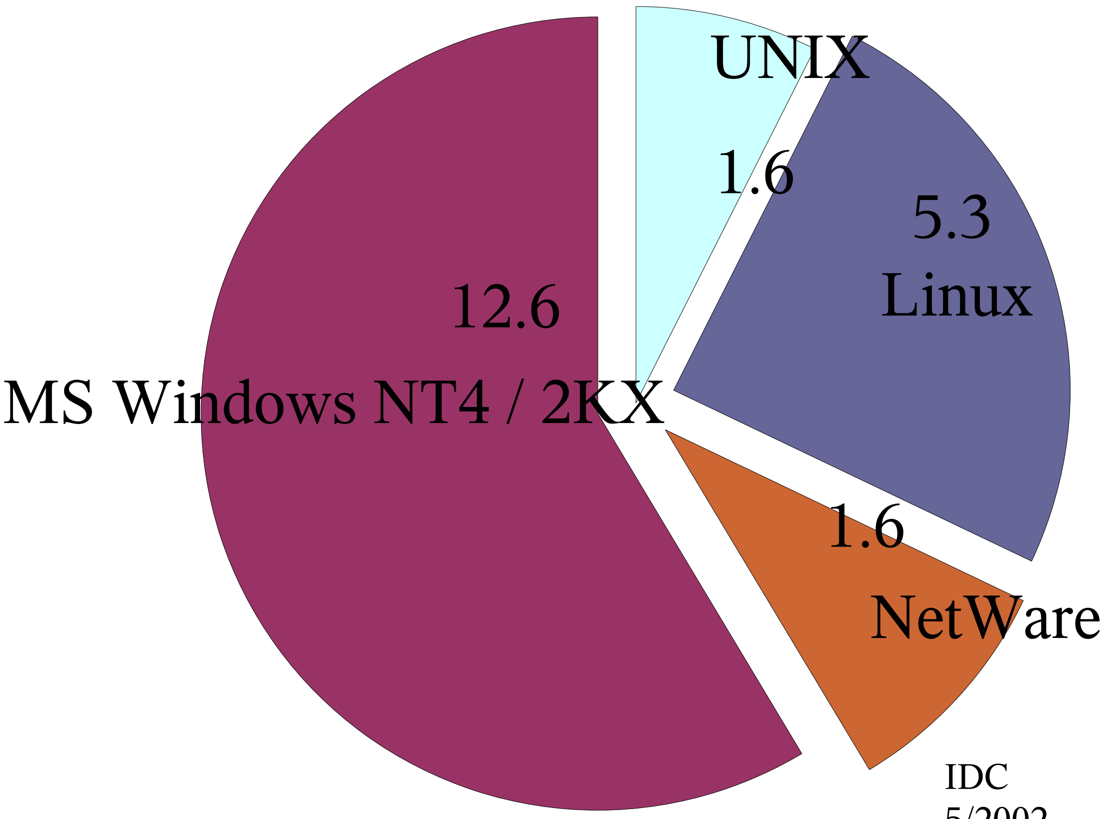


IDC
5/2002

Market Share – Forecast 2005

PrimaStasys Inc

21.1 Million Servers



IDC
5/2002

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

PrimaStasys Inc

- 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

PrimaStasys Inc

- 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
    - uses proprietary protocols

ADS And ID Management

- AD is the Authentication and Identity management backend of choice for Business
  - Provides centralized network user identity administration
  - Integrates with external directories through tools like MIIS (was MMS – Microsoft Metadirectory Service)
- The demand for LDAP is growing
  - Alternative to ADS
  - Standards compliant

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 Service 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 resolution
  - 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.x 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

Samba Winbind

- Cons:
  - Same UID/GID across all Samba servers ONLY with LDAP Account backend
    - Complex configuration
  - Exposes ALL backend accounts
    - NT4 Domain / Active Directory Domain

Samba-3 Configuration

- Components:
  - *smb.conf* file controls behavior
    - smbd, nmbd, winbindd are the operative daemons
  - *nsswitch.conf* file for identity management
  - Infrastructure tools
    - user and machine scripts
    - share management scripts
    - domain management tools
      - Eg: SRVTOOLS.EXE, NESUS.EXE, MMC
  - Group Management

Administration

- How do you want to manage Samba?
  - From MS Windows clients (workstations)
  - From UNIX server
- Management from MS Windows clients requires:
  - Interface scripts
    - Add / Delete / Modify users
    - Add / Delete / Modify groups
    - Add machines (Domain Member Servers / Clients)
    - Change User Group Membership
    - Create / Delete / Modify Shares
    - Printer control programs
  - Pre-execution Scripts

CIFS Security

- Security Modes affect network design
  - Network Operation Controls
    - Workgroups
    - Domains
  - Authentication Methods
  - Local UNIX security and Windows Users and Groups
  - Access Control Lists
    - Much abused

Security Modes / Models

- There are only 2 security models
  - Share Mode
    - Like Windows for Workgroups
    - Has passwords for
      - Full Control
      - Read Only
  - User Mode
    - Like MS Windows NT/2K
    - Uses username and password tuple

Samba Security Modes

- Set via *smb.conf* file *[global]* parameter
  - ***security = XXXXX***
- security = SHARE
  - Accepts password from client, sequentially scans */etc/passwd* until the first match is found
- security = USER (default)
  - Uses *username* and *password* from client
- Encrypted Password Support
  - Default for all security modes

Share Mode *smb.conf* file

```
[global]
# Default workgroup = WORKGROUP, we want MIDEARTH
workgroup = MIDEARTH
# Behavior like Windows for Workgroups
security = share

# We want a read only anonymous file server
[Plans]
path = /home/Plans
read only = Yes
guest ok = Yes
```

User Mode *smb.conf* file

```
# Global parameters
[global]
# Default is “security = USER”
workgroup = BILLMORE

# The following are for CUPS printing
support
printcap name = CUPS
disable spoolss = Yes
printing = cups

# Get rid of the printer wizard in NT/200x
show add printer wizard = No
```

Samba-Specific Security Modes

- security = SERVER
  - Obsoleted, uses pass-through authentication
  - Used with *password server* parameter to redirect authentication to a specified server

•Samba-Specific Security Modes

PrimaStasys Inc

- security = DOMAIN
  - Machine is an NT4 style Domain Member Server (DMS)
    - Can be a workstation or a server
  - Does NOT mean it is a Domain Controller
- security = ADS
  - Machine is a member of an Active Directory Domain

NT4 Style Domains

- Samba-3 supports NT4 style Domain architecture

  - Can be an NT4 style PDC or BDC

  - Can NOT be a mixed:

ie: Samba-3 PDC or BDC ***with*** NT4 BDC or PDC

NT4 Domain Controller (PDC)

```
# Global parameters
[global]
        workgroup = PROMISES
# Netbios name default is hostname
# We want name DIAMOND in browser
        netbios name = DIAMOND
# Maps UNIX root to Windows Administrator
        username map = /etc/samba/smbusers
# Netlogon server defines Domain Control
        domain logons = Yes
```

NT4 Domain Controller (BDC)

```
# Global parameters
[global]
      workgroup = PROMISES
# Netbios name default is hostname
# We want DIAMOND
      netbios name = DIAMOND
# Maps UNIX root to Windows Administrator
      username map = /etc/samba/smbusers
      domain logons = Yes
# Default domain master = Yes means is PDC
# We want BDC
      domain master = No
```

Note: Must be joined to Domain!

```
net rpc join -Uroot%password
```

NT4 Domain Member (DMS)

- Can be (same configuration):
  - Domain Member Server (DMS)
  - Domain Member Client (DMS)

```
# Global parameters
[global]
       workgroup = BILLMORE

# The following means be a DMS
       security = DOMAIN
```

Samba is Scalable

- Samba-3 scales beyond MS Windows NT4
    - Can have LDAP directory behind it
    - NT4 can NOT have an LDAP directory behind it
        - For that you need Windows 200x Active Directory

Samba-3 Exclusions

- Samba-3 is NOT an Active Directory replacement
- Samba-3 is a unique entity that has emerged from years of wrestling with Windows networking issues
  - It is scalable and flexible
  - Requires appropriate backend

Scalability: Definition

- First and foremost:
  - Network clients can get uninterrupted services
    - Network logon service
    - File and Print service
    - etc.
- This means:
  - The right service in the right place at all times
    - Load distribution
    - Replication
    - Upset/disaster recovery

Scalability: Load Distribution

- Achieved by:
  - Sufficient network bandwidth
    - Either local or WAN
  - Distribution of servers
    - Network Logon services
    - File and Print services
    - Other hosted services
      - Web, Mail, Proxy, SQL, etc. (Not Samba issues)

Scalability: Network Logon

- Domain Control
  - The core of Network Logon provision (3A's):
    - Authentication
    - Authorization
    - Access Control

Scalability: Location of

- NT4 Style uses one PDC and BDCs
  - Not structured
    - Active Directory has LDAP based hierarchy
  - Rule of thumb is on DC per 30-50 workstations
    - This is an unreliable rule, some sites operate well with one DC for hundreds of workstations
  - Good advice:
    - network segment that has the PDC should have a BDC also

Backend Choices

- POSIX Only
  - Can be */etc/passwd* based, or through NSS
    - If NSS, can be in LDAP, NIS, etc.
- Plain Text *smbpasswd* file based

•Backend Choices

- *tdbsam*
  - Stores Security Account Manager (SAM) information in a binary file:

    /etc/samba/passdb.tdb OR ***/usr/local/samba/lib/private/passdb.tdb***
- *ldapsam*
  - Stores POSIX and SAM data in LDAP

Auxiliary Backends

- Experimental / Special Interest Backends
  - XML
  - SQL

Cross Domain Identity

- IDMAP
  - Local storage OR LDAP based
  - Used to store mappings of foreign domain / machine SIDs to local UID/GIDs
  - If stored in LDAP can provide consistent UID/GIDs for each NT SID encountered
    - Can be machine SID or Domain SID

Backend Configuration

- Control is via the *smb.conf* parameter in *[global]* known as *passdb backend*
  - Recommended options:
    smbpasswd (default)
    tdbsam
    ldapsam

Infrastructure Tools

- Scripts provide glue between Windows network management environment and Samba host OS
  - Called by Samba (smbd)
- Three Classes of Scripts (see next slide)
  - Identity
  - Resource
  - Control

Script Class: Identity Mgmt

PrimaStasys Inc

- Identity management
  - add/delete/modify user scripts
  - add/delete/modify group scripts
  - add machine script
  - change password

Scripts for POSIX Backend

- POSIX Backend means accounts in:
  - /etc/passwd, /etc/shadow, /etc/group
  - SMB Passwords in:
    - /etc/samba/smbpasswd*(passdb backend = smbpasswd)*
    - /etc/samba/passdb.tdb *(passdb backend = tdbsam)*
    - SMB passwords are maintained by Samba

```
add user script = /usr/useradd -m %u
delete user script = /usr/userdel -r %u
add group script = /usr/groupadd %g
delete group script = /usr/groupdel %g
add user to group script = /usr/usermod -G %g %u
add machine script = /usr/useradd -s /bin/false -d /dev/null %u
```

Scripts for LDAP Backend

- Must store both POSIX account information as well as Samba SAM information in LDAP
  - Does not work if only SAM info is stored in LDAP
- Requires LDAP Server (OpenLDAP is a good one)
- Requires LDAP Client tools
  - pam_ldap
  - nss_ldap

smbldap_tools Scripts

PrimaStasys Inc

```
add user script = /opt/idealx/smbldap-useradd -a -m '%u'
delete user script = /opt/idealx/smbldap-userdel '%u'
add group script = /opt/idealx/smbldap-groupadd -p '%g'
delete group script = /opt/idealx/smbldap-groupdel '%g'
add user to group script = /opt/idealx/smbldap-groupmod -m '%u' '%g'
delete user from group script = /opt/idealx/smbldap-groupmod -x '%u' '%g'
set primary group script = /opt/idealx/smbldap-usermod -g '%g' '%u'
add machine script = /opt/idealx/smbldap-useradd -w '%u'
```

Note: Macros need to be quoted

Configuration control file is in:
/etc/smbldap_tools/smbldap.conf

Script Class: Resource Mgmt

- Resource management
  - add/delete share
  - add/delete printer

Script Class: System Control

- System Control
  - shutdown
  - abort shutdown
  - etc.

Integrating Windows Networks

PrimaStasys Inc

- Provides authentication integration
  - User logs onto machine (workstation or server) once
    - Has transparent access to resources
- Provides file and print sharing
- Samba can integrate into both Windows network designs
  - NT4
  - ADS

NT4 Style Domains

- Native support is built into Samba
- Requires use of *winbindd*
  - Use *NSS* for passwd, group resolution
  - Stores mapping table locally in *winbindd_idmap.tdb* file

Active Directory

- Requires compilation with ADS option
  - Requires Kerberos libraries
    - MIT 1.3.1 or later
    - Heimdal 0.61 or later
- Windows 2003 ADS requires the latest KRB versions

Oops!

- Some UNIX and Linux vendors do NOT include ADS support in the Samba they ship!
  - Sun
  - Slackware
  - Others?

Finding Information

- ALWAYS Visit the Source Luke!
  - http://www.samba.org/samba/
  - Documentation
    - Man pages, Official Books
    - Listing of published books
  - Mailing Lists
    - General, Technical
  - Bug Tracking System
    - http://bugzilla.samba.org/
  - Other Sources

Documentation

- Official (means part of Samba sources)
  - 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
  - Man Pages
  - Contributed Presentations, etc. on Samba.Org

Documentation

- Unofficial
  - There is a lot of it, most is of high quality
  - Much is out of date
- Many books: http://www.samba.org/samba/books.html
- Samba-Team encourage unofficial source work!
  - There is nothing exclusive in the title: "Official Documentation"

Is there time for questions?