# Designing & Implementing a Samba Networking Solution

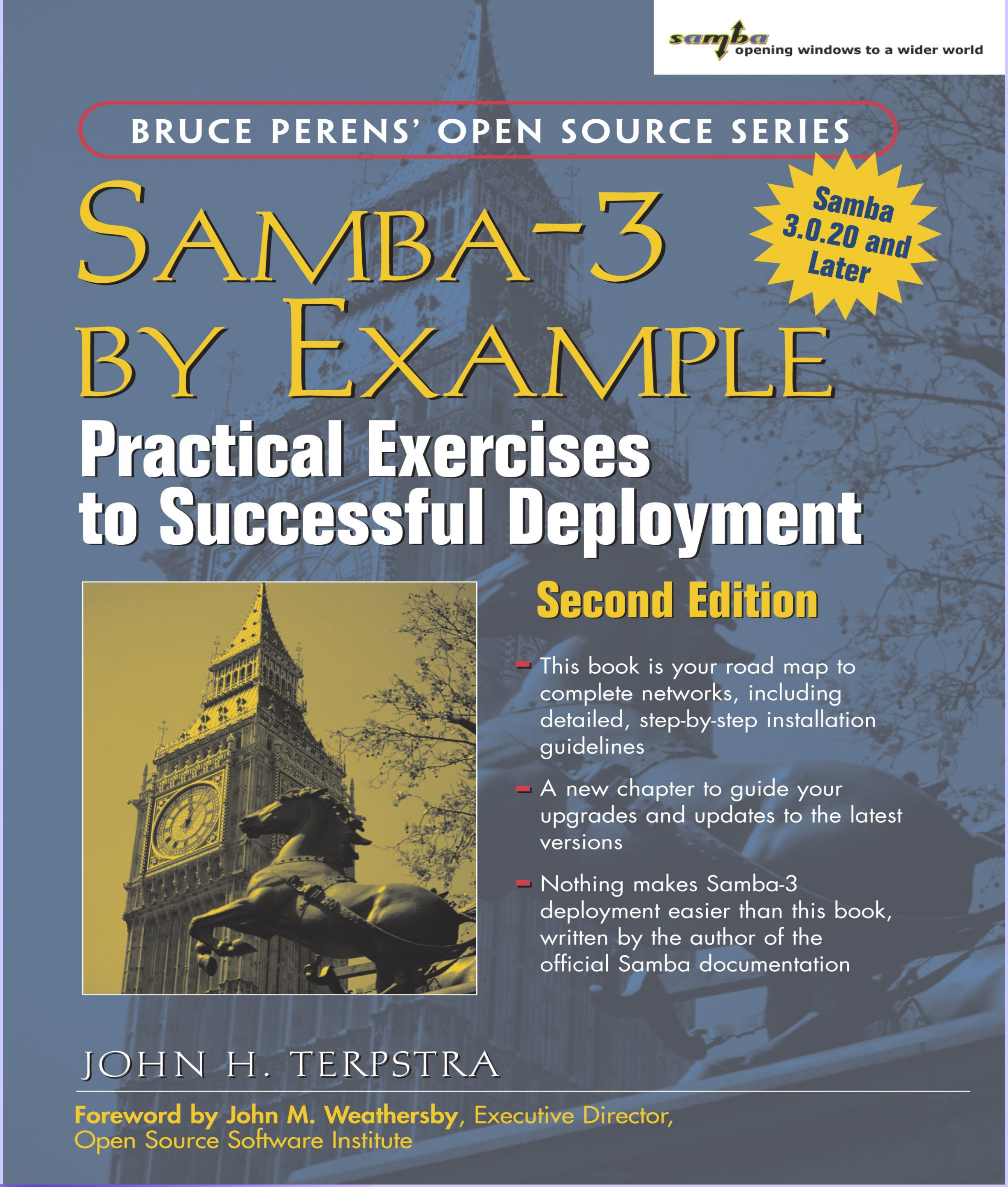
John H Terpstra,
CTO, PrimaStasys Inc.

jht@primastasys.com
jht@samba.org

9th Annual
CIFS Conference & Plugfest

# Who is John H Terpstra?

- Author:
  - Samba-3 by Example
  - Samba-3 HOWTO and Reference Guide
  - Hardening Linux
- Samba-Team member since 1995



samba opening windows to a wider world

BRUCE PERENS' OPEN SOURCE SERIES

# Samba-3 by Example

## Practical Exercises to Successful Deployment

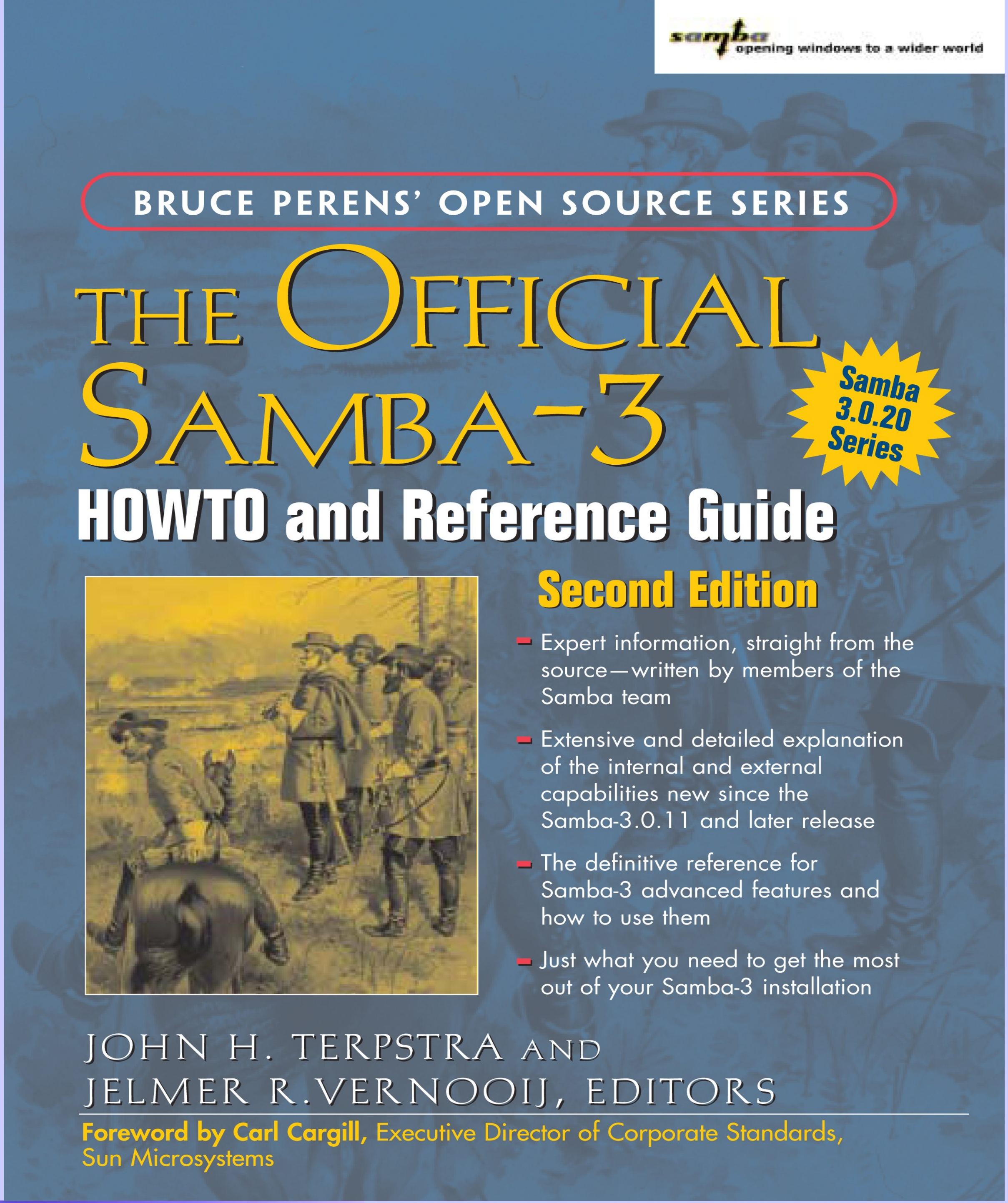
Samba 3.0.20 and Later

**Second Edition**

- This book is your road map to complete networks, including detailed, step-by-step installation guidelines
- A new chapter to guide your upgrades and updates to the latest versions
- Nothing makes Samba-3 deployment easier than this book, written by the author of the official Samba documentation

JOHN H. TERPSTRA

**Foreword by John M. Weathersby**, Executive Director, Open Source Software Institute



samba opening windows to a wider world

BRUCE PERENS' OPEN SOURCE SERIES

# THE OFFICIAL SAMBA-3 HOWTO and Reference Guide

Samba 3.0.20 Series

## Second Edition

- Expert information, straight from the source—written by members of the Samba team
- Extensive and detailed explanation of the internal and external capabilities new since the Samba-3.0.11 and later release
- The definitive reference for Samba-3 advanced features and how to use them
- Just what you need to get the most out of your Samba-3 installation

JOHN H. TERPSTRA AND
JELMER R.VERNOOIJ, EDITORS

**Foreword by Carl Cargill,** Executive Director of Corporate Standards, Sun Microsystems

# Overview

- Identify task requirements
- Implementation Decisions
- Management Implications
- Case Examples
  - A transportation company network
  - A hospital network
- Performance Metrics

# Task Requirements

# Adoption Strategy

- Samba will replace an NT4 domain?
  - If true, consider PDC/BDC needs
  - If false, will Samba be an NT4 domain member server?
- Does the site already have Active Directory?
  - If yes, consider Samba as an ADS domain member
- Will Samba be used as a stand-alone server?

- Application software platform dependencies?

# Server Management

- How will Samba servers be managed?
  - From UNIX/Linux command line
    - Use *net* and *pdbedit* tools
  - Web-based tool
    - Interactive Management Console (Idealx)
    - LDAP Account Manager
    - SWAT (Samba Web Administration Tool)

# Server Management (contd)

- From Windows MMC
  - LDAP Administrator
  - QCD Interstructures MMC snap-in (commercial)
- Using Windows NT4 Tools
  - NT4 Domain User Manager
  - NT4 Server Manager
- Windows 200X tools
  - MMC Computer Manager (shares and file system only)
  - Windows Explorer (file system only)

# Server Management (contd)

- How will data be backed up?
  - Data backup validation
  - Cross-platform recovery should be considered
- How will data be migrated between servers?
  - MS Windows Explorer, and other GUI tools
  - Windows command line tools
  - Use of *rsync*
    - Means UIDs/GIDs need to be same on all Samba servers
  - Use of backup and restore software

# Legal Requirements

- Do Sarbanes-Oxley regulations apply?
  - How will network security be established and monitored?
    - Exception handling procedures are mandatory
    - Auditing needs must be planned
      - Does no good if not monitored
- Patches and updates are essential
    - What are site quality assurance and control needs?
    - How, and by whom, will these be decided?

# Implementation Decisions

# Implementation Decisions: Architecture Replacement

- Domain replacement
  - Existing domain account migration:
    *net rpc vampire*
  - Consider whether it may be expedient to make a fresh start
  - If PDC and BDC servers are needed use LDAP account backend
    - Adds complexity and flexibility
- Example: A site uses LDAP for Samba, mail, Radius, and several web/business applications

# Implementation Decisions: Integration into Existing Domains

- If existing domain is NT4 based
  - Consider future migration (NT4 is EOL)
  - Samba-3 can be an NT4 DMS (domain member server) – It can NOT be a BDC where NT4 is PDC
    - Samba-3 does NOT support SAM replication
    - Also Samba-3 can NOT be a PDC to an NT4 BDC
- If existing domain is ADS
  - Samba-3 can be
    - A native ADS DMS (uses Kerberos authentication)
    - An NT4 DMS (uses RPC technology)

# Implementation Decisions

- Many sites consider Samba too complex and too limited in capability
  - Thus some have moved from Samba to ADS
  - Result also is use of Samba-3 as a stand-alone server (SAS)
    - Adds to management overhead
    - Sometimes dictated by degree of difficulty to provide support for LDAP and/or Kerberos needed for advanced operation
- Security implications of SAS are poorly understood

# Implementation Decisions: Account Back-end

- Use of LDAP account backend
  - Samba-3 does not permit safe replication of *tdbsam* back-end account data
    - Use of PDC plus BDCs requires use of LDAP with Samba-3.
  - Use of LDAP requires account creation and management scripts
  - Remote administration is possible only with LDAP interface scripts
    - LDAP directory management policies and procedures are necessary – particularly with multiple administrators

# Implication of Account Back-end Choice

- The *tdbsam* back-end puts accounts in various files:
  - */etc/samba/passdb.tdb*
    - user and machine SAM (Windows user accounts)
  - */var/lib/samba/group_mapping.tdb*
    - Group mappings (Windows Group accounts)
  - */var/lib/account_policy.tdb*
    - Account and network security settings
    - User rights and privilege settings
    - Can NOT be replicated – must be set per-server!

# Implication of Account Back-end Choice (contd)

- LDAP directory contains
  - */etc/samba/passdb.tdb*
  - */var/lib/samba/group_mapping.tdb*
- LDAP directory does NOT contain
  - */var/lib/samba/account_policy.tdb* settings
  - Microsoft domains permit single point of control, Samba-3 requires per machine control
    - Will be fixed in 3.0.2x series (hopefully!)
    - Bad logon lockout broken if BDCs are used

# Danger Will Robinson!

- Do not use bad account lock-out controls with Samba-3 PDC/BDC combinations
  - Use of NT4 Domain User Manager to set controls will only set the PDC and leave the BDC un-set.
  - Use of *pdbedit* tool can set PDC and BDCs
    - BUT one site that used it ended up with over 60% of legitimate users locked out

# User Rights & Privileges

- Samba-3.0.11 introduced new user rights and privileges capabilities
  - Permits delegation of administrative rights
    - Admin users and groups
    - Set share ACLs (Disk Operator Privilege)
    - Printer admin
    - Add machine accounts
    - Take ownership of file system objects
- Use the *net* tool to manage these rights, or use the NT4 Domain User Manager

# Re: User Rights & Privileges

- User rights and privileges are stored in the */var/lib/samba/account_policy.tdb* file
  - They must be set *'per server'*
    - On NT4 these are set *'per domain'*
- Currently it is difficult to set admin rights for domain users on a DMS
  - That will be fixed soon (maybe!)

# Touch-points: PDC and SAS

- No problems with implementation
  - Best to use *tdbsam*
  - Keep *smb.conf* as simple as possible
  - User rights and privileges can be used
  - Account aging works fine
  - Bad logon lockouts work fine
- Can be remotely managed & printing OK
- Potential problems setting inter-domain trusts
  - Use *winbindd* when using inter-domain trusts

# Touch-points: BDC

- BDCs
  - Must use LDAP (including nss_ldap for ID resol.)
  - Can set user rights and privileges – per server
  - Account aging works
  - Bad logon handling does not work reliably
    - Will result in false lock-outs
      - (ie: Correct credentials result in lockouts)
      - Does not permit Sarbanes-Oxley compliance
        - Will be fixed sometime soon (maybe!)
  - Remote management OK, just like PDC

# Touch-points: DMS

- Samba domain – use NSS and LDAP and set *smb.conf* to use local accounts
  ***OR***
  For NT4 or ADS DMS – use NSS and *winbindd*

- Current problems with setting up domain user rights and privileges
  - Will be fixed soon (maybe!)
  - Needed for share ACLs admin and for printer admin

# Touch-points: DMS (contd)

- If NT4 or ADS DMS
  - Need IDMAP support
    - NSS *winbind* method stores UID/GID to SID mappings in */var/lib/samba/winbindd_mapping.tdb* and */var/lib/samba/winbindd_cache.tdb* files
    - If there are multiple DMSs the mappings will most likely be different on each server
      - Solutions:<br>*idmap_rid* – uses user RID as UID<br>*idmap_ad* – obtains UID from SFU ADS schema extn.

- Use of LDAP to store IDMAP data overcomes all limitations and is only method that is compatible with multi-domain environments

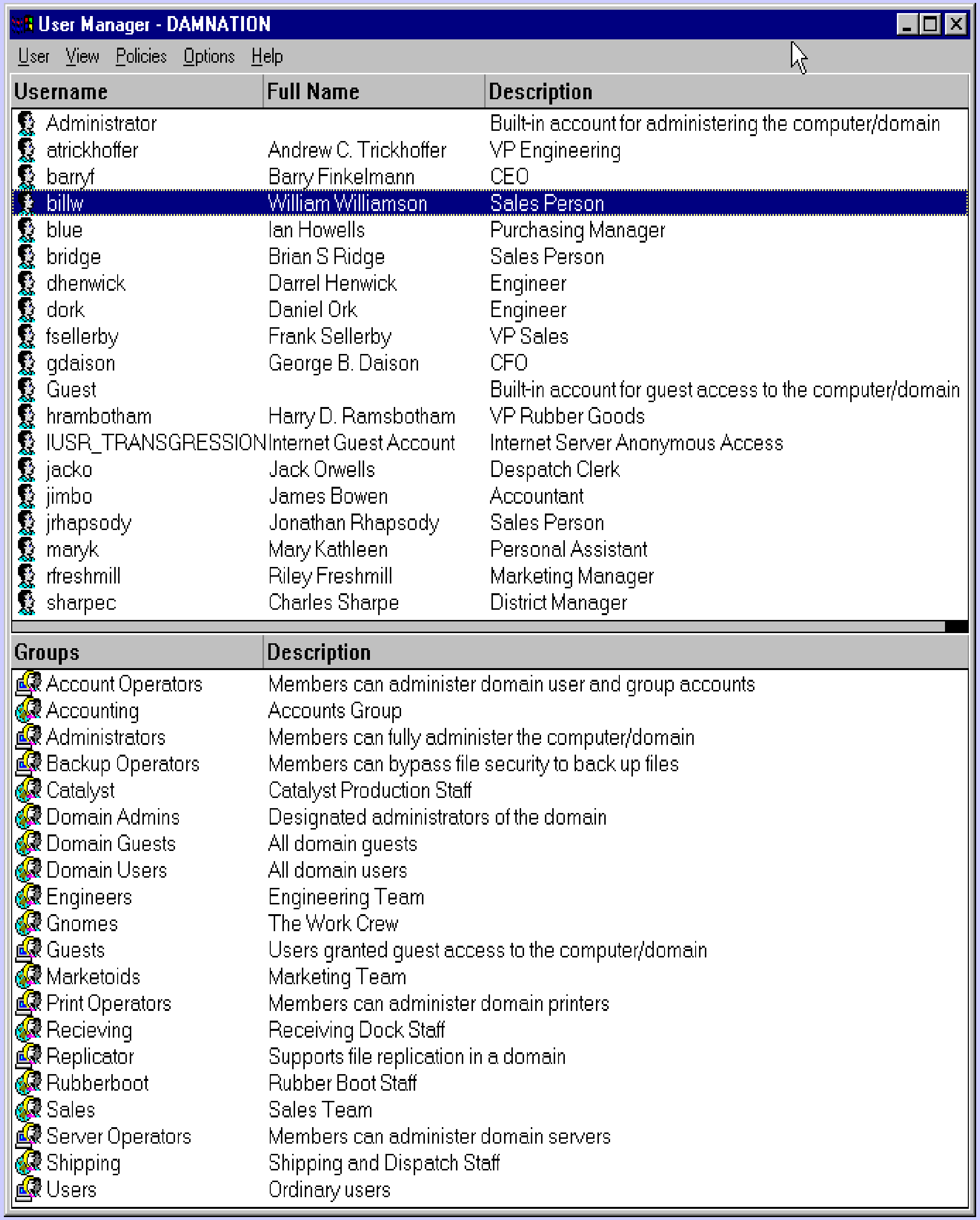
# Management Implications

# Management Implications

- Let it be said:
  - Samba is not Windows NT4!
  - Samba is not Microsoft Active Directory!
- But Samba CAN be managed
  - Mostly using the NT4 Domain User Manager
  - Using command line tools
  - IMC, LAM
  - A number of commercial tools
    - MMC snap-ins (Interstructures), Power SMB Editor, ...

# Use of the NT4 Domain User Manager

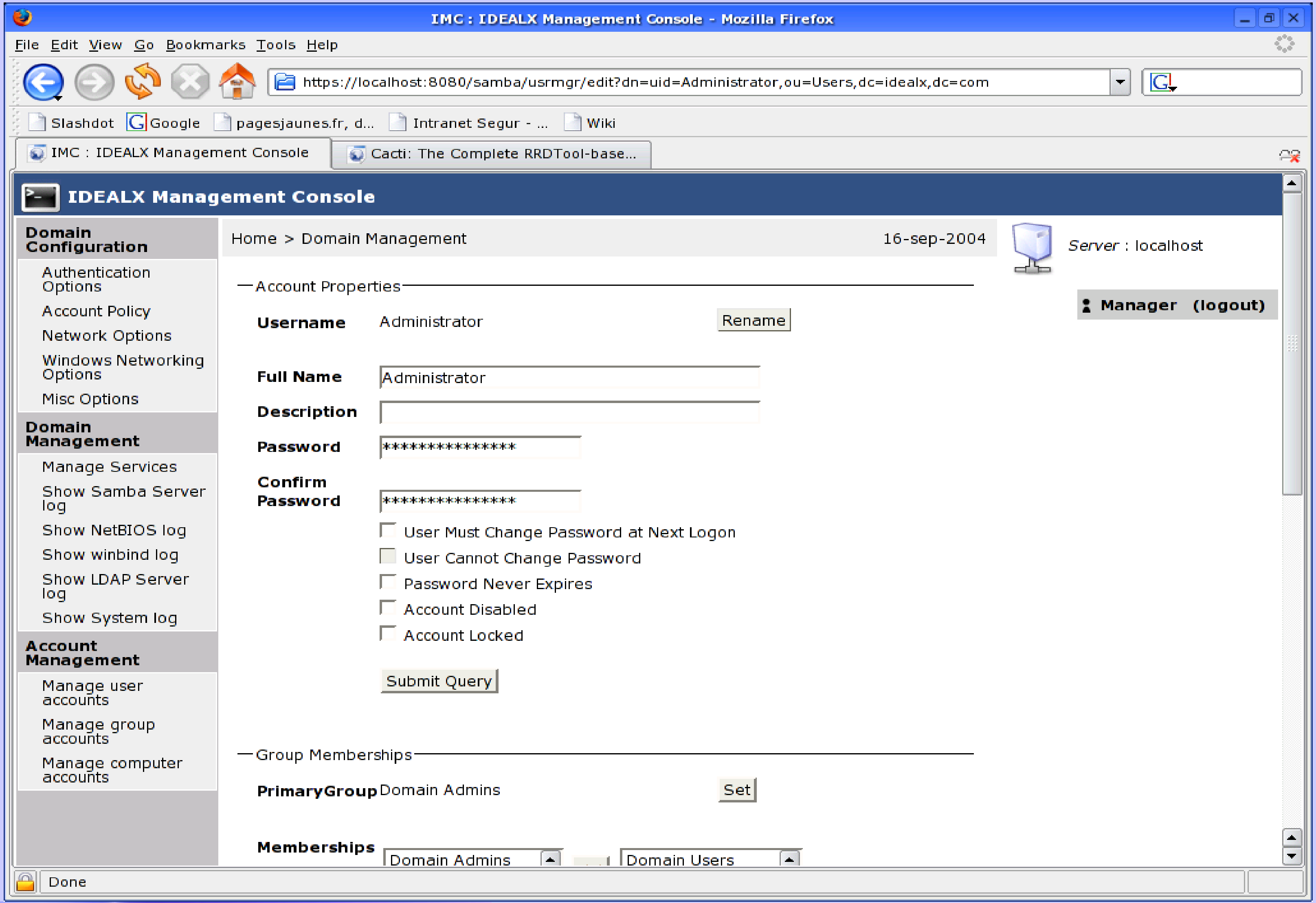
- Can manage
  - Users
  - Groups
  - Set domain policies
  - Manage password aging
  - Set bad login handling policies
- Has Limitations!



| Username | Full Name | Description |
|---|---|---|
| Administrator | | Built-in account for administering the computer/domain |
| atrickhoffer | Andrew C. Trickhoffer | VP Engineering |
| barryf | Barry Finkelmann | CEO |
| billw | William Williamson | Sales Person |
| blue | Ian Howells | Purchasing Manager |
| bridge | Brian S Ridge | Sales Person |
| dhenwick | Darrel Henwick | Engineer |
| dork | Daniel Ork | Engineer |
| fsellerby | Frank Sellerby | VP Sales |
| gdaison | George B. Daison | CFO |
| Guest | | Built-in account for guest access to the computer/domain |
| hrambotham | Harry D. Ramsbotham | VP Rubber Goods |
| IUSR_TRANSGRESSION | Internet Guest Account | Internet Server Anonymous Access |
| jacko | Jack Orwells | Despatch Clerk |
| jimbo | James Bowen | Accountant |
| jrhapsody | Jonathan Rhapsody | Sales Person |
| maryk | Mary Kathleen | Personal Assistant |
| rfreshmill | Riley Freshmill | Marketing Manager |
| sharpec | Charles Sharpe | District Manager |

| Groups | Description |
|---|---|
| Account Operators | Members can administer domain user and group accounts |
| Accounting | Accounts Group |
| Administrators | Members can fully administer the computer/domain |
| Backup Operators | Members can bypass file security to back up files |
| Catalyst | Catalyst Production Staff |
| Domain Admins | Designated administrators of the domain |
| Domain Guests | All domain guests |
| Domain Users | All domain users |
| Engineers | Engineering Team |
| Gnomes | The Work Crew |
| Guests | Users granted guest access to the computer/domain |
| Marketoids | Marketing Team |
| Print Operators | Members can administer domain printers |
| Recieving | Receiving Dock Staff |
| Replicator | Supports file replication in a domain |
| Rubberboot | Rubber Boot Staff |
| Sales | Sales Team |
| Server Operators | Members can administer domain servers |
| Shipping | Shipping and Dispatch Staff |
| Users | Ordinary users |

# IMC – Interactive Management Console



Account Properties

**Username** Administrator

**Full Name** Administrator

**Description**

**Password** ***************

**Confirm Password** ***************

□ User Must Change Password at Next Logon

□ User Cannot Change Password

□ Password Never Expires

□ Account Disabled

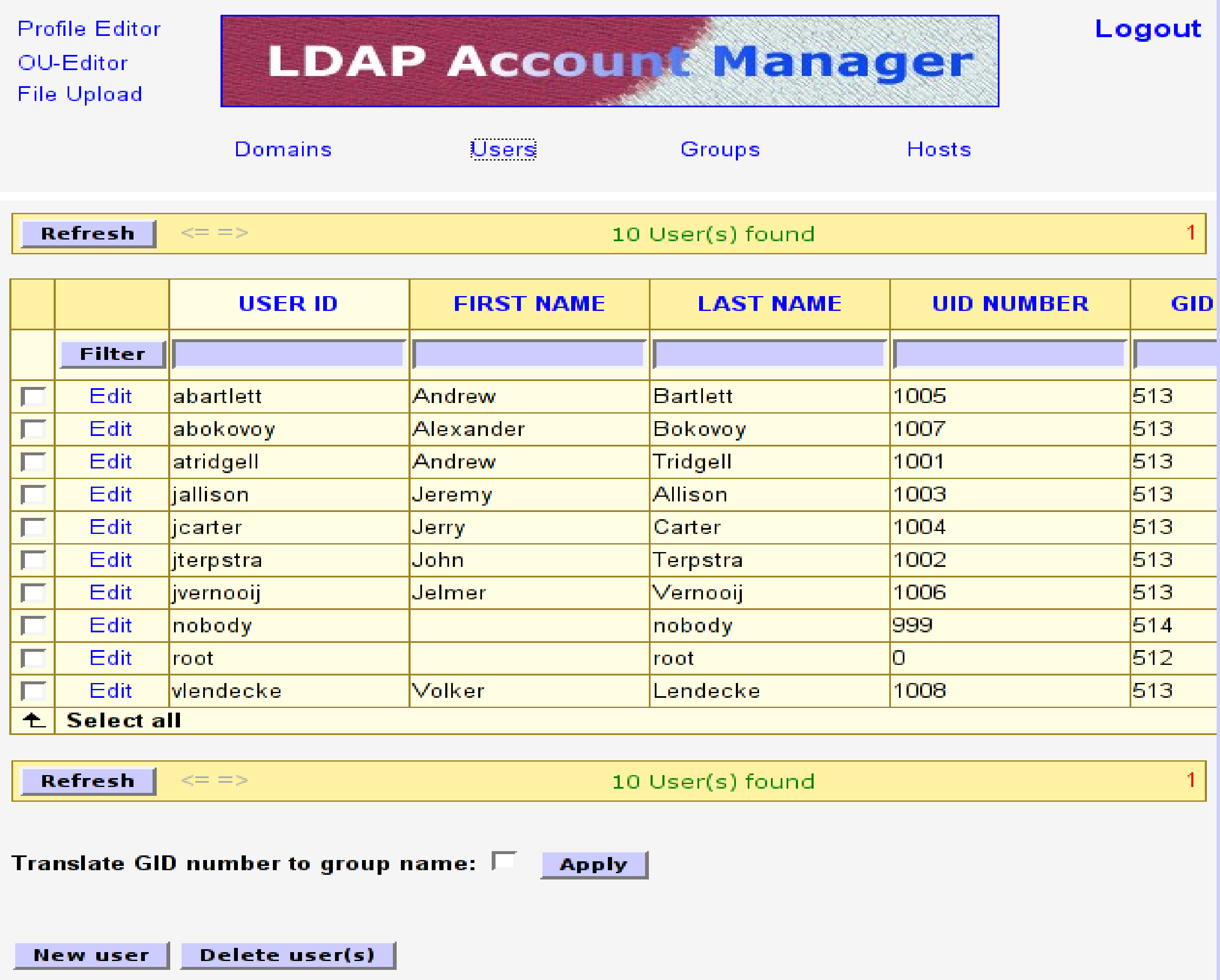
□ Account Locked

Group Memberships

**PrimaryGroup** Domain Admins

**Memberships** Domain Admins | Domain Users

# LDAP Account Manager (LAM)



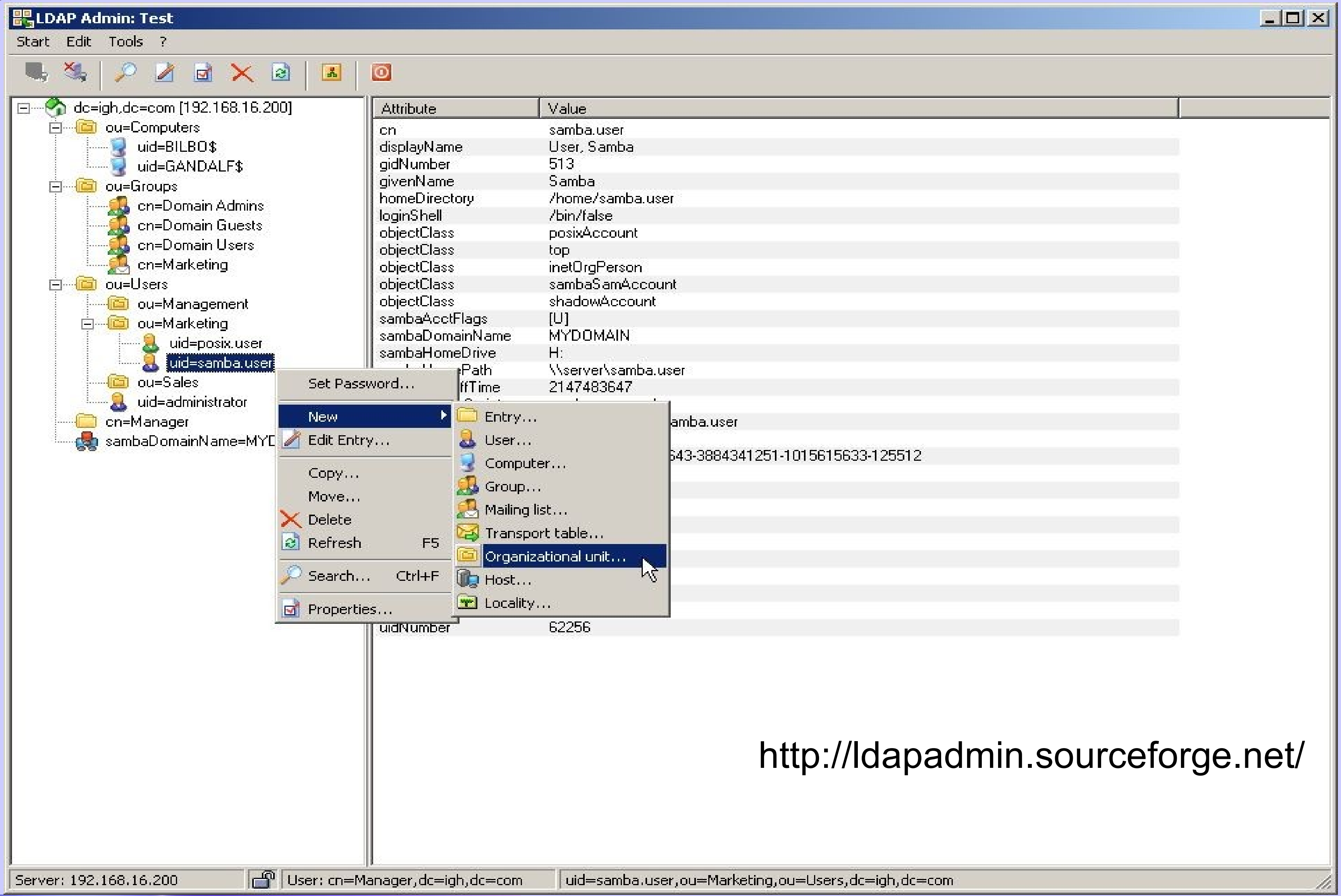
10 User(s) found

| | | USER ID | FIRST NAME | LAST NAME | UID NUMBER | GID |
|---|---|---|---|---|---|---|
| □ | Edit | abartlett | Andrew | Bartlett | 1005 | 513 |
| □ | Edit | abokovoy | Alexander | Bokovoy | 1007 | 513 |
| □ | Edit | atridgell | Andrew | Tridgell | 1001 | 513 |
| □ | Edit | jallison | Jeremy | Allison | 1003 | 513 |
| □ | Edit | jcarter | Jerry | Carter | 1004 | 513 |
| □ | Edit | jterpstra | John | Terpstra | 1002 | 513 |
| □ | Edit | jvernooij | Jelmer | Vernooij | 1006 | 513 |
| □ | Edit | nobody | | nobody | 999 | 514 |
| □ | Edit | root | | root | 0 | 512 |
| □ | Edit | vlendecke | Volker | Lendecke | 1008 | 513 |

10 User(s) found

Translate GID number to group name: □

# Ldap administrator



```
dc=igh,dc=com [192.168.16.200]
  ou=Computers
    uid=BILBO$
    uid=GANDALF$
  ou=Groups
    cn=Domain Admins
    cn=Domain Guests
    cn=Domain Users
    cn=Marketing
  ou=Users
    ou=Management
    ou=Marketing
      uid=posix.user
      uid=samba.user
    ou=Sales
    uid=administrator
  cn=Manager
  sambaDomainName=MYD
```

| Attribute | Value |
|---|---|
| cn | samba.user |
| displayName | User, Samba |
| gidNumber | 513 |
| givenName | Samba |
| homeDirectory | /home/samba.user |
| loginShell | /bin/false |
| objectClass | posixAccount |
| objectClass | top |
| objectClass | inetOrgPerson |
| objectClass | sambaSamAccount |
| objectClass | shadowAccount |
| sambaAcctFlags | [U] |
| sambaDomainName | MYDOMAIN |
| sambaHomeDrive | H: |
| Path | \\server\samba.user |
| ffTime | 2147483647 |
| | amba.user |
| | 643-3884341251-1015615633-125512 |
| uidNumber | 62256 |

Server: 192.168.16.200 | User: cn=Manager,dc=igh,dc=com | uid=samba.user,ou=Marketing,ou=Users,dc=igh,dc=com

http://ldapadmin.sourceforge.net/

# Case Examples

# Case Examples

- A Hospital
- A Transport Company

# Hospital Samba-3 Deployment

- Infrastructure
  - 1400 PCs, 2800 users
  - NT4 Domain for X-Ray application
    - Will be migrated to ADS and Windows 2003 soon
  - Samba-3 domain has all user accounts
    - Samba-3 PDC, 3 BDCs, 1 DMS
  - Inter-domain trusts are used to provide access to the NT4 domain file resources
- Current Issues:
  - Needs Sarbanes-Oxley compliance is needed

# Hospital DMS

- HP dual Xeon 2GHz, 4GB RAM
  - RAID(5) Array
  - SuSE SLES 9
- Average load relatively low
  - Performance is acceptable
  - Typical concurrent user count is approx. 600

# Transport Company

- Infrastructure
  - 3 locations
  - 1400 users
  - Head Office has a large IBM 8 CPU server, 16GB RAM with VMWare ESX Server
    - Hosts 8 machines (PDC, BDC, Apps Server, Lotus Notes Server, etc.)
    - More on performance later
- Samba-3.0.15pre2 and OpenLDAP
  - LDAP used for Samba, mail, dial-up PPP, apps.

# Transport Company (contd)

- Using SQUID proxy with *ntlm_auth* access control
  - SQUID front-ends a single dedicated content filter
- Each branch office has a BDC and a SQUID server
- Complex client configuration with roaming profiles, folder redirection, logon scripts auto-install printers on a 'per user' basis.
- Current Issues: Privileges and Sarbanes-Oxley

# Anticipation of Performance Needs

# Performance Metrics

- Note: The following are comparative metrics do NOT assume that they mean anything in real life!
- Over the wire has NIC and protocol stack overheads
- Locally executed smbtorture tests includes overhead of running clients
  - These are highly subjective tests
  - The results do NOT imply real-world guidance

# Client Details

- Client Machine
  - AMD Dual MP1600, 1GB RAM
    - (Tyan Thunder K7X board), built-in 1Gb Ethernet NIC 3Ware 7500-4 IDE RAID controller with 4x160GB WD 7200rpm drives configured as RAID(5) and reiserfs
    - SuSE SLES 9 i386
    - Samba-4 smbtorture with load file clients.txt from dbench 3.0.3 release.
      - Command:

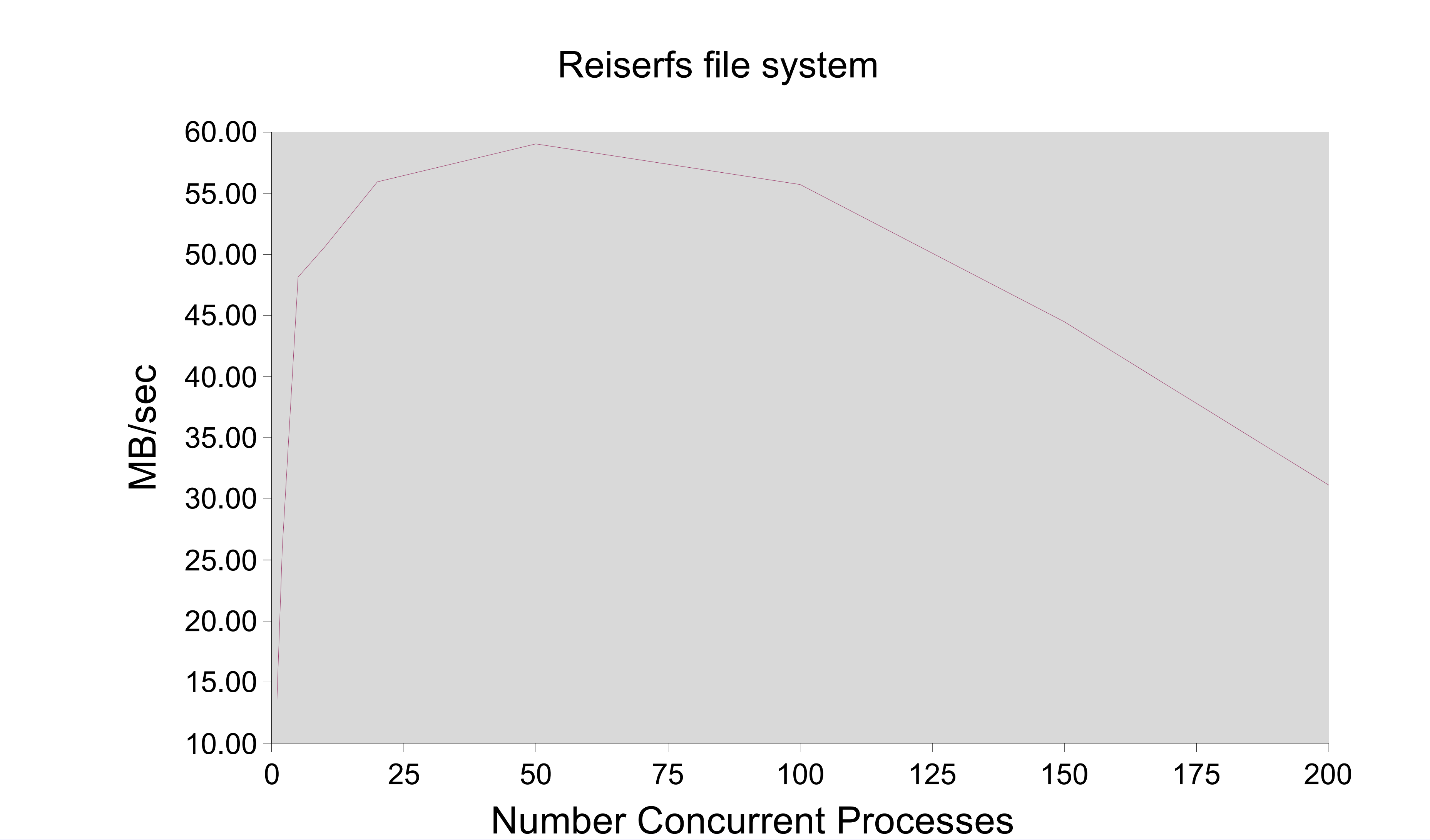
```
smbtorture //server/netbench -t 300 --loadfile=client.txt \
--num-progs='n' -U% BENCH-NBENCH
```

n = 1,2,5,10,20,50,100,150,200,250,500

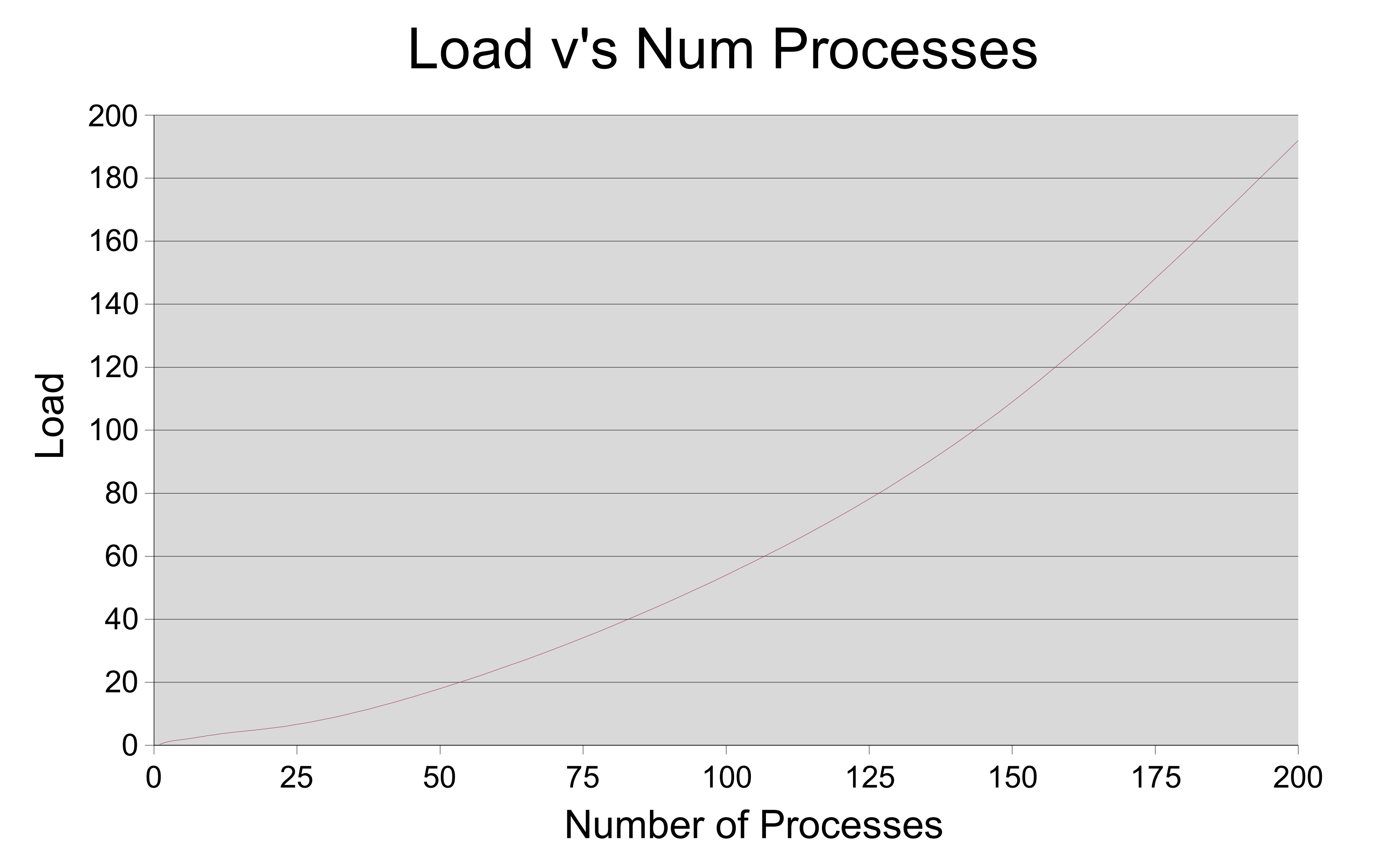
# Server Details

- Server
  - Dual Opteron 244, 2GB RAM (Tyan K8W board)
    - SuSE Linux Professional 9.3 x86_64
    - Dual AMCC 3Ware 9500-S8 SATA RAID Controllers
      - Each with 6 Western Digital Raptor 10,000rpm drives
      - Configuration RAID(0), the 2 RAID drives configured as md(0) RAID(0)
    - Samba 3.0.20pre2 SVN Release 8510

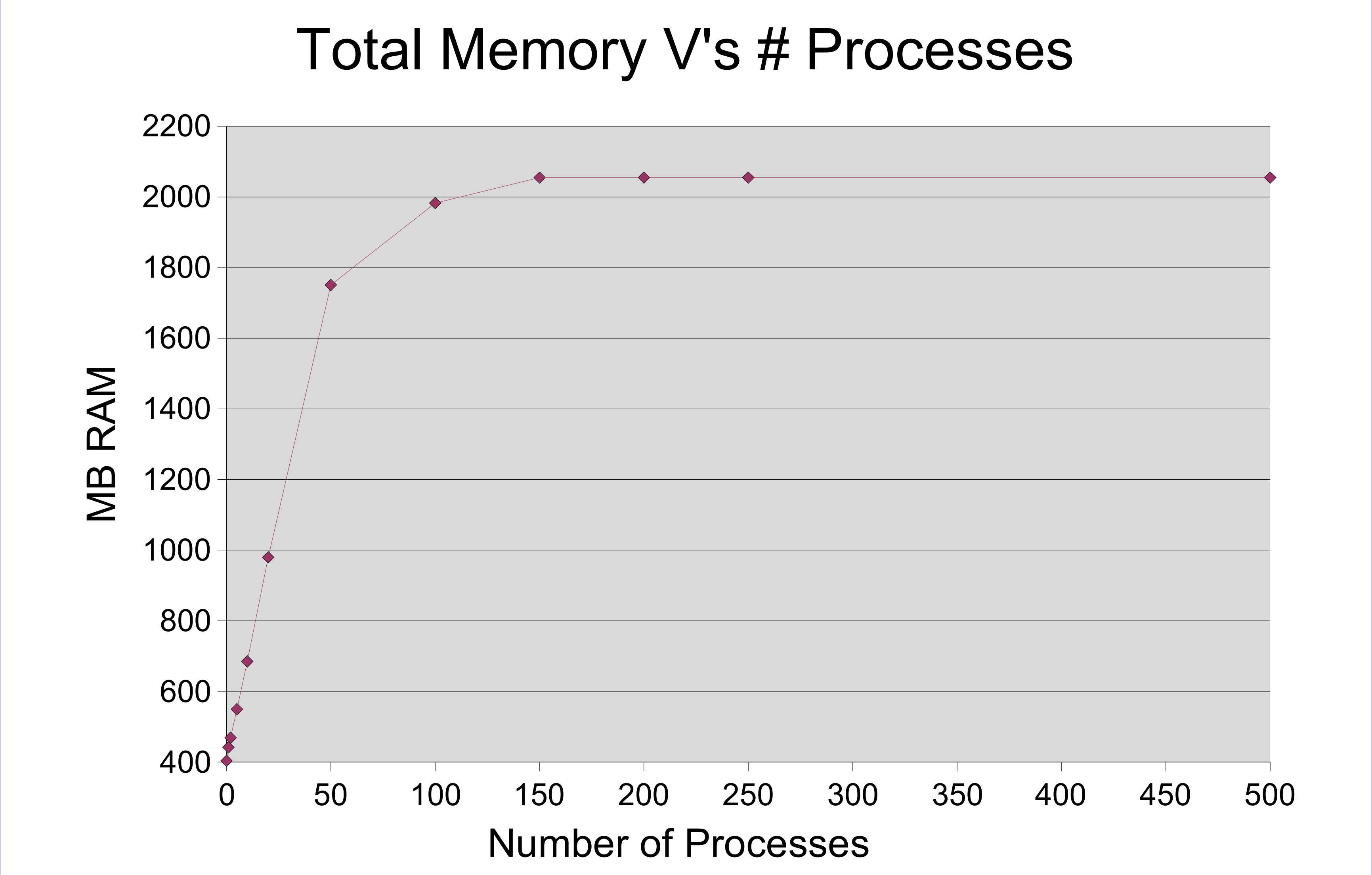
# Dual Opteron 244 (1.8GHz) Over 1Gb Ethernet



# Dual Opteron 244 (1.8GHz) Over 1Gb Ethernet



# Dual Opteron 244 (1.8GHz) Over 1Gb Ethernet



# Locally Executed *smbtorture* Results Compared

- Opteron Server – same as previous slides
  - Comparing reiserfs and XFS

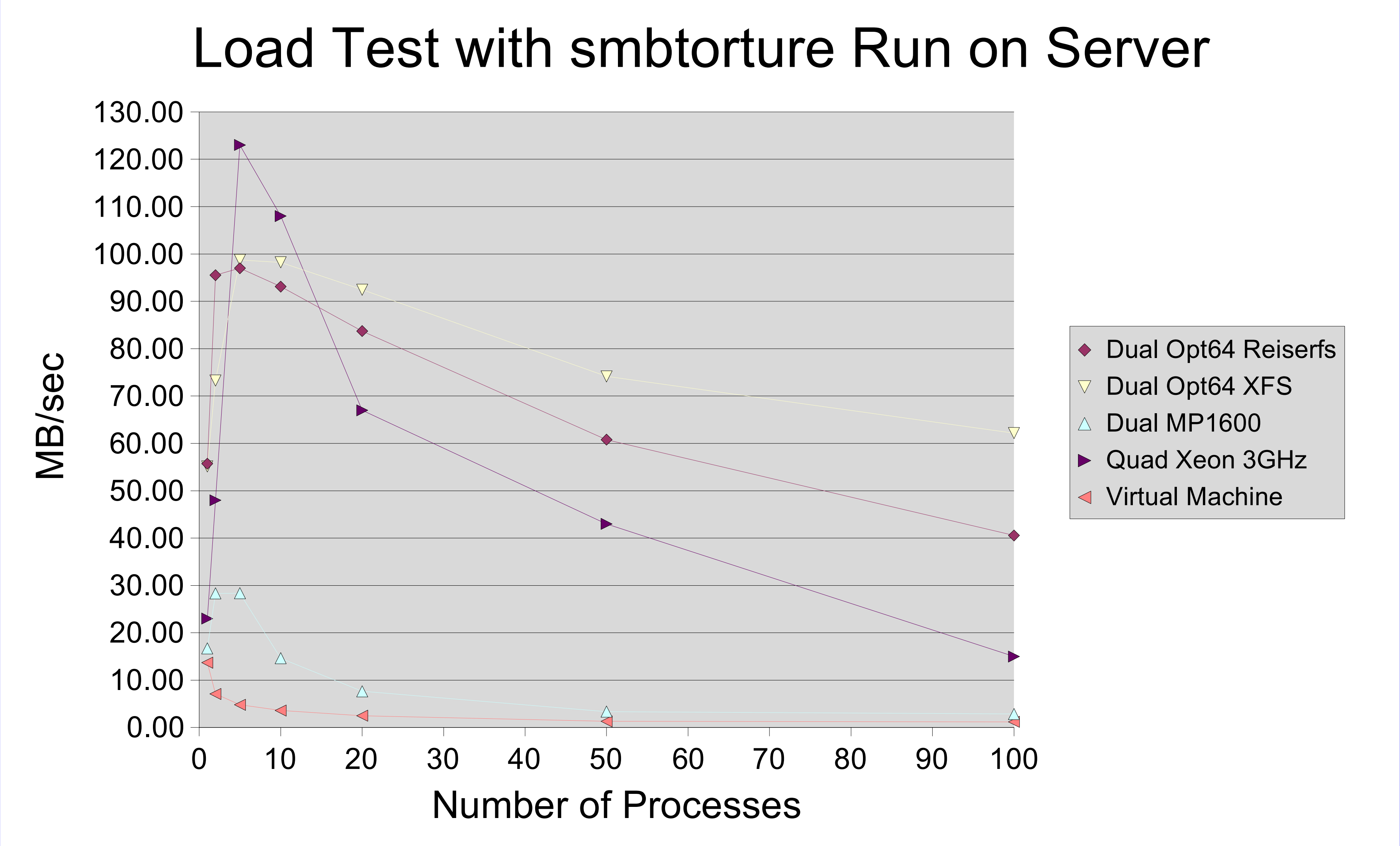
    Note: Ext2fs and Ext3fs = same results as reiserfs

- AMD MP1600 Server – same as previous slide

# Locally Executed *smbtorture* Results Compared

- Dell PowerEdge 6800, Quad Xeon 3.0 Ghz 2GB RAM
  - PERC4ei SCSI RAID Controller, 4x70GB (1 spare) 15,000rpm Ultra 320 SCSI HDD in RAID(5) Array
  - SuSE SLES 9 x86_64, Samba 3.0.20pre2,Rel.8510
- Virtual Machine is running SLES 9 i386 on VMWare ESX Server Version 5
  - Host Server is 8-Way 2.4GHz Xeon with 16GB RAM, running 8 virtual servers – 1 CPU per VMC.

# Comparative Server Tests



# Sanity Check-point

- The virtual machine array includes:
  - A Samba-3.0.15pre2 PDC and a Samba-3.0.15pre2 BDC
  - A Windows Server 2003 running Lotus Notes
  - A Web server
  - A dedicated application server (8 Foxbase users)
- The BDC serves 140 concurrent users for office file & print
- Performance is acceptable!

# Summary

- Samba-3 is used in some very large sites
  - It is effective and efficient (if well deployed)
- Current trend is integration into ADS domains
  - Some migration from NT4 to Samba

–Emerging Interests:

- Management
- Sarbanes-Oxley Compliance
- Privileges

Discussion