PrimaStasys Inc

How to Weave Samba-3 into your Network

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

About the speaker

PrimaStasys Inc

- Long term Samba-Team member
- Author of official Samba documentation
  - The Official Samba-3 HOWTO and Reference Guide
    - ISBN: 0131453556 (Sept 2003)
    - Open Source version: Samba-HOWTO-Collection
  - Samba-3 by Example
    - ISBN: 0131472216 (Mar 2004)
    - Open Source version: Samba-Guide
- Author of additional books
  - Hardening Linux, ISBN: 0072254971 (Jul 2004)
  - More in production

Agenda

PrimaStasys Inc

- Samba Update
- Diagnostic Approach / Methods
- Samba Security Modes
- Building Simple Servers
- Advanced Features
- Windows Client Configuration
- Future Directions

Samba Update

PrimaStasys Inc

- Current Series:
  - 3.0.x – Since Sept. 24, 2003
- Current Stable Release:
  - 3.0.12 – Released March 18, 2005.
- Next Stable Release:
  - 3.0.13 – Probable release in May, 2005
- Next Major Release:
  - 4.0 – In development for over 2 years
  - Release date not set – maybe late 2005

Progression of New Features

PrimaStasys Inc

- 3.0.12: Large directory support
- 3.0.11: Privileges support + Bug Fixes
- 3.0.10: Security Update
- 3.0.9: Bug fixes
- 3.0.8: Bug fixes
- 3.0.7: Bug fixes
- 3.0.6: Remote CUPS server / Password History
- 3.0.5: Bug fixes (Security)
- 3.0.4: Bug fixes

Overview Samba-3

PrimaStasys Inc

- 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

PrimaStasys Inc

- How do you want to manage Samba?
  - From MS Windows clients (workstations)
  - From UNIX server

Administration

PrimaStasys Inc

- 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
  - Windows Administration Tools

Diagnostic Approach / Methods

PrimaStasys Inc

1) Validate that name resolution is working
2) Validate the *smb.conf* file
3) Use the Samba log file facility to investigate ALL failures / problems
4) Use *Ethereal* to investigate network transactions
5) Use Windows client diagnostic facilities

   eg: generate netlogon.txt

Diag: Name Resolution

PrimaStasys Inc

- Use WINS
  - Requires one WINS server and EVERY client MUST be configured to use it
  - Use WINS on the UNIX/Linux server also
    - Requires NSS support in the Operating System
- Validate with:

ping 'windows_workstation_name'

nmblookup -m 'windows_workstation_name'

Diag: Validation of smb.conf

PrimaStasys Inc

- Use *testparm* to your advantage

example:

Create a master *smb.conf* file called: *smb.conf.master*

testparm -s smb.conf.master > /etc/samba/smb.conf

Then execute *testparm* without arguments

Diag: Example use of *testparm*

PrimaStasys Inc

```
marvel:~ # testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[accounts]"
Processing section "[service]"
Processing section "[pidata]"
Processing section "[homes]"
Processing section "[printers]"
Processing section "[apps]"
Processing section "[netlogon]"
Processing section "[profiles]"
Processing section "[profdata]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_DOMAIN_PDC
Press enter to see a dump of your service definitions
```

Diag: Samba Log Analysis

PrimaStasys Inc

- Samba has extensive and flexible log generation facilities
  - Example:

/etc/samba/smb.conf:

```
[global]
   log level = 1
   log file = /var/log/samba/%
m.log
   max log size = 0
   ...
   include = /etc/samba/%m.log
```

/etc/samba/mywinbox.conf:

```
[global]
   log level = 5
```

Diag: Log File Analysis

PrimaStasys Inc

- Examine contents of log files by:

```
marvel # grep -v "^\[200" mywinbox.log | less

Processing section "[apps]"
  Processing section "[homes]"
  Processing section "[printers]"
  Processing section "[netlogon]"
  Processing section "[profiles]"
  Processing section "[print$]"
  added interface ip=192.168.1.1 bcast=192.168.1.255 nmask=255.255.255.0
  added interface ip=127.0.0.1 bcast=127.255.255.255 nmask=255.0.0.0
  smbldap_open_connection: connection opened
  init_sam_from_ldap: Entry found for user: jht
  init_group_from_ldap: Entry found for group: 513
  check_ntlm_password:  authentication for user [jht] -> [jht] -> [jht]
succeeded
  frodo (192.168.1.1) connect to service apps initially as user jht
(uid=1000, gid=513) (pid 22527)
  frodo (192.168.1.1) closed connection to service jht
```

Diag: An Ethereal Trace

PrimaStasys Inc

```
⊞ Frame 14 (312 bytes on wire, 312 bytes captured)
⊞ Ethernet II, Src: 00:50:56:40:00:ae, Dst: 00:10:5a:24:76:e0
⊞ Internet Protocol, Src Addr: 192.168.1.243 (192.168.1.243), Dst Addr: 192.168.1.1 (
⊞ Transmission Control Protocol, Src Port: 1044 (1044), Dst Port: microsoft-ds (445),
⊞ NetBIOS Session Service
⊟ SMB (Server Message Block Protocol)
    ⊞ SMB Header
    ⊟ Session Setup AndX Request (0x73)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 254
        Max Buffer: 16644
        Max Mpx Count: 50
        VC Number: 0
        Session Key: 0x00000000
        Security Blob Length: 93
        Reserved: 00000000
      ⊞ Capabilities: 0xa00000d4
        Byte Count (BCC): 195
      ⊟ Security Blob: A15B3059A25704554E544C4D53535000...
          ⊟ GSS-API
              ⊟ SPNEGO
                  ⊟ negTokenTarg
                      ⊟ responseToken
                          ⊟ NTLMSSP
                              NTLMSSP identifier: NTLMSSP
                              NTLM Message Type: NTLMSSP_AUTH (0x00000003)
                            ⊞ Lan Manager Response: 00
                              NTLM Response: Empty
                              Domain name: NULL
                              User name: NULL
                            ⊞ Host name: LIGHTRAYXP
                              Session Key: Empty
                            ⊞ Flags: 0x20800a15
        Native OS: Windows 2002 2600 Service Pack 1
        Native LAN Manager: Windows 2002 5.1
        Primary Domain:
```

```
00a0  00 00 00 00 00 40 00 00  00 14 00 14 00 40 00 00   .....@.. .....@..
00b0  00 00 00 00 00 55 00 00  00 15 0a 80 20 4c 00 49   .....U.. .... L.I
00c0  00 47 00 48 00 54 00 52  00 41 00 59 00 58 00 50   .G.H.T.R .A.Y.X.P
00d0  00 00 57 00 69 00 6e 00  64 00 6f 00 77 00 73 00   ..W.i.n. d.o.w.s.
00e0  20 00 32 00 30 00 30 00  32 00 20 00 32 00 36 00    .2.0.0. 2. .2.6.
```

Diag: Windows Diagnostics

PrimaStasys Inc

- References:

Regarding TCP/UDP Ports:

http://support.microsoft.com/default.aspx?scid=kb;en-us;832017

Debugging Network Logon:

cd c:\winnt\debug

View (using notepad): netsetup.txt and netlogon.txt files

Diag: Win 2000 Pro *netsetup.txt*

PrimaStasys Inc

NetSetup - Notepad

File Edit Format Help

```
04/13 12:39:55 ----------------------------------------------------------------
04/13 12:39:55 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2 name
04/13 12:39:55 NetpCheckNetBiosNameNotInUse: for 'WORKGROUP' returned: 0x858
04/13 12:39:55 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x858
04/13 12:39:55 NetpValidateName: name 'WORKGROUP' is valid for type 2
04/13 12:39:55 ----------------------------------------------------------------
04/13 12:39:55 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2 name
04/13 12:39:55 NetpCheckNetBiosNameNotInUse: for 'WORKGROUP' returned: 0x858
04/13 12:39:55 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x858
04/13 12:39:55 NetpValidateName: name 'WORKGROUP' is valid for type 2
04/13 12:39:55 ----------------------------------------------------------------
04/13 12:39:55 NetpDoDomainJoin
04/13 12:39:55 NetpMachineValidToJoin: 'WIN2KP'
04/13 12:39:55 NetpGetLsaPrimaryDomain: status: 0x0
04/13 12:39:55 NetpMachineValidToJoin: status: 0x0
04/13 12:39:55 NetpJoinWorkgroup: joining computer 'WIN2KP' to workgroup 'WORKGROUP'
04/13 12:39:55 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2 name
04/13 12:39:55 NetpCheckNetBiosNameNotInUse: for 'WORKGROUP' returned: 0x858
04/13 12:39:55 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x858
04/13 12:39:55 NetpValidateName: name 'WORKGROUP' is valid for type 2
04/13 12:39:55 NetpSetLsaPrimaryDomain: for 'WORKGROUP' status: 0x0
04/13 12:39:55 NetpControlServices: open service 'NETLOGON' failed: 0x424
04/13 12:39:56 NetpJoinWorkgroup: status:  0x0
04/13 12:39:56 NetpDoDomainJoin: status: 0x0
04/13 12:40:25 ----------------------------------------------------------------
04/13 12:40:25 NetpValidateName: checking to see if 'WIN2KP' is valid as type 1 name
04/13 12:40:25 NetpCheckNetBiosNameNotInUse for 'WIN2KP' [MACHINE] returned 0x0
04/13 12:40:25 NetpValidateName: name 'WIN2KP' is valid for type 1
04/13 12:42:03 ----------------------------------------------------------------
04/13 12:42:03 NetpValidateName: checking to see if 'MYGROUP' is valid as type 2 name
04/13 12:42:03 NetpCheckNetBiosNameNotInUse for 'MYGROUP' [ Workgroup as MACHINE]
returned 0x0
04/13 12:42:03 NetpValidateName: name 'MYGROUP' is valid for type 2
04/13 12:42:03 ----------------------------------------------------------------
04/13 12:42:03 NetpValidateName: checking to see if 'MYGROUP' is valid as type 2 name
04/13 12:42:03 NetpCheckNetBiosNameNotInUse for 'MYGROUP' [ Workgroup as MACHINE]
returned 0x0
04/13 12:42:03 NetpValidateName: name 'MYGROUP' is valid for type 2
04/13 12:42:03 ----------------------------------------------------------------
04/13 12:42:03 NetpDoDomainJoin
04/13 12:42:03 NetpMachineValidToJoin: 'WIN2KP'
04/13 12:42:03 NetpGetLsaPrimaryDomain: status: 0x0
04/13 12:42:03 NetpMachineValidToJoin: status: 0x0
04/13 12:42:03 NetpJoinWorkgroup: joining computer 'WIN2KP' to workgroup 'MYGROUP'
04/13 12:42:03 NetpValidateName: checking to see if 'MYGROUP' is valid as type 2 name
04/13 12:42:03 NetpCheckNetBiosNameNotInUse for 'MYGROUP' [ Workgroup as MACHINE]
```

Security Modes

PrimaStasys Inc

- Summary
  - SHARE mode == Windows for Workgroups
    - Not well maintained – being obsoleted
  - USER mode
    - commonly in use
  - SERVER mode
    - Deprecated – do not use if it can be avoided
  - DOMAIN mode
    - NT4 Domain Members Server / Client
  - ADS mode
    - Active Directory Member Server / Client

CIFS Security

PrimaStasys Inc

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

Security Modes / Models

PrimaStasys Inc

- 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

Samba Security Modes - SHARE

PrimaStasys Inc

- Set via *smb.conf* file *[global]* parameter

  security = XXXXX

  eg: security = SHARE

  - Accepts password from client, sequentially scans */etc/passwd* until the first match is found

Share Mode *smb.conf* file

PrimaStasys Inc

```
[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
```

Samba Security Modes - USER

PrimaStasys Inc

- security = USER (default)
  - Obtains *username* and *password* from client
  - Encrypted Password Support
    - NOTE: Default for all security modes

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

PrimaStasys Inc

- **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 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

PrimaStasys Inc

- 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

Building Simple Servers

PrimaStasys Inc

- Simple
  - Simple read-only server
  - Simple print server
  - Simple anonymous file server
- Major Server Types
  - Stand-alone
  - Domain Controller (NT4 PDC or BDC)
  - Domain Member Server (DMS) or Client (DMC)

Simple Servers

PrimaStasys Inc

- Read-Only File Server
- Anonymous File Server
- Print Server

Simple Read-Only Server

PrimaStasys Inc

```
# Global Parameters
[global]
        workgroup = MIDEARTH
        security = SHARE

[Plans]
        path = /plans
        read only = Yes
        guest ok = Yes
```

Simple Anonymous File Server

PrimaStasys Inc

```
# Global Parameters
[global]
        workgroup = MIDEARTH
        security = SHARE

[TMPFILES]
        comment =  Fund Tracking & Management Files
        path = /data/ftmfiles
        read only = No
        force user = abmas
        force group = office
        guest ok = Yes
```

Simple Print Server

PrimaStasys Inc

```
# Global Parameters
[global]
        workgroup = MIDEARTH
        security = SHARE
        printcap name = CUPS
        disable spoolss = Yes
        show add printer wizard = No
        wins support = yes
        printing = CUPS

[printers]
        path = /var/spool/samba
        printable = Yes
        guest ok = Yes
        use client driver = Yes
        browseable = No
```

Major Server Types

PrimaStasys Inc

- Stand-alone Server
- Domain Control
  - PDC
  - BDC
- Domain Members
  - Server
  - Client

Stand-Alone Server

PrimaStasys Inc

```
# Global parameters
[global]
        workgroup = BILLMORE
        printcap name = CUPS
        disable spoolss = Yes
        show add printer wizard = No
        printing = cups

[master]
        comment = Master work area files
        path = /data
        read only = No

[printers]
        comment = Print Temporary Spool Configuration
        path = /var/spool/samba
        guest ok = Yes
        printable = Yes
        use client driver = Yes
        browseable = No
```

NT4 Domain Controller (PDC)

PrimaStasys Inc

```
# 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)

PrimaStasys Inc

```
# 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 join the Domain!

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

NT4 Domain Member (DMS)

PrimaStasys Inc

- Can be either:
  - Domain Member Server (DMS)
  - Domain Member Client (DMS)

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

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

- DMS and DMC use identical Samba *smb.conf* Configuration

Advanced Features

PrimaStasys Inc

- Account Information Storage
  - Where account information is stored
- Identity Mapping
  - Windows SIDs to UNIX UIDs and GIDs
  - Username Maps
  - Group Mapping
  - Nested Group Mapping
- Access Control List
- Privileges and Rights (NEW)

Account Information Storage

PrimaStasys Inc

- The Windows Account information has 2 parts:
  - POSIX (UNIX) accounts
    - Provides:
      - UID, GID, login name, UNIX home directory, etc.
  - SambaSAMAccount
    - Provides:
      - Windows network passwords
      - Windows profile location
      - Password controls
      - Access time and/or machine controls
      - etc.
- All considered as happening at the Backend!

Backend Configuration

PrimaStasys Inc

- Control is via the *smb.conf* parameter in *[global]* known as *passdb backend*
  - Recommended options:

    smbpasswd (default)
    - permits only basic security settings

    tdbsam (permits extended Domain Settings)

    ldapsam (permits greatest control flexibility)

Backend Choices

PrimaStasys Inc

- POSIX Only
  - Can be */etc/passwd* based, or through NSS
    - If NSS, can be in LDAP, NIS, etc.
  - POSIX is NOT a Samba backend
    - It is THE UNIX default database
- Plain Text *smbpasswd* file based
  - One of the following:

    /etc/samba/smbpasswd

    /usr/local/samba/lib/private/smbpasswd

Backends New to 3.0.x

PrimaStasys Inc

- *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
  - Previously Samba-2.2.x had to be compiled for either smbpaswd *OR* LDAP
    - Now it is natively capable of any backend

Auxiliary Backends

PrimaStasys Inc

- Experimental / Special Interest Backends
  - XML
  - SQL

Infrastructure Tools

PrimaStasys Inc

- 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

PrimaStasys Inc

- 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
```

Samba-3 Exclusions

PrimaStasys Inc

- 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

Samba is Scalable

PrimaStasys Inc

- 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

Scalability: Definition

PrimaStasys Inc

- 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

PrimaStasys Inc

- 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

PrimaStasys Inc

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

Enable Domain Control by:

```
domain logons = Yes
```

On DMS machines: Use Winbind for IDMAP support

Scalability: Location of

PrimaStasys Inc

- 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

Scripts for LDAP Backend

PrimaStasys Inc

- 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 (for UNIX/Linux login only)

  nss_ldap (for ID resolution)

smbldap_tools Scripts

PrimaStasys Inc

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

Note: Macros need to be quoted

Configuration control file is in:

/etc/smbldap_tools/smbldap.conf

Script Class: Resource Mgmt

PrimaStasys Inc

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

Script Class: System Control

PrimaStasys Inc

- System Control
  - shutdown
  - abort shutdown
  - etc.

Cross Domain Identity Management

PrimaStasys Inc

- IDMAP Backend
  - 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
  - Needed for foreign machine SIDs and foreign domain SIDs

Configuration of IDMAP

PrimaStasys Inc

- Local IDMAP file
  - Must run ***winbindd***
  - Usually located in:

    /var/spool/samba/winbindd_idmap.tdb

    or

    /var/cache/samba/winbindd_idmap.tdb

    or

    /usr/local/samba/var/locks/winbindd_idmap.tdb

```
[global]
...
    idmap uid = 15000-20000
    idmap gid = 15000-20000
...
```

Configuration of IDMAP

PrimaStasys Inc

- Using LDAP backend
  - Must run winbindd
  - Stores mapping data in LDAP
  - Must have same UID/GID range on all clients

```
ldap suffix = dc=abmas,dc=biz
ldap admin dn = cn=Manager,dc=abmas,dc=biz
ldap idmap suffix = ou=Idmap
Idmap backend = ldap:ldap://frodo.abmas.biz:389
```

Integration into Windows Nets

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 old and new Windows network designs:

  NT4

  ADS

NT4 Style Domains

PrimaStasys Inc

- 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

NT4 Domain Member (DMS)

PrimaStasys Inc

- Can be (same configuration):

  Domain Member Server (DMS)

  Domain Member Client (DMC)

  - Note: Must join the Domain

    net rpc join -W 'domain_name' -U 'admin_name'

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

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

Active Directory

PrimaStasys Inc

- Requires compilation with ADS option
  - Requires Kerberos libraries
    - MIT 1.3.1 or later (current 1.4)
    - Heimdal 0.61 or later (current 0.63)
- Windows 2003 ADS requires the latest KRB versions

NOTE:

PrimaStasys Inc

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

ADS Domain Membership

PrimaStasys Inc

- Uses Kerberos authentication protocols
- Requires correct configuration
  - Example DC: *london.abmas.biz*

```
security = ADS
workgroup = LONDON
realm = abmas.biz
```

- Requires joining the Domain by:

```
net ads join -Uadministrator%password
```

Kerberos for ADS DMS

PrimaStasys Inc

- Use default *krb5.conf* file
- Do NOT specify the encryption types!
  - If you do, be forewarned that you may break interoperability with Windows 200x
- Must use latest versions of MIT Kerberos or Heimdal
  - If using Heimdal, you must have an */etc/krb5.conf* file to satisfy library needs

NSS Configuration for ADS DMS

PrimaStasys Inc

/etc/nsswitch.conf

```
# /etc/nsswitch.conf

passwd:         files winbind
group:          files winbind

hosts:          files dns wins
```

PAM Configuration for ADS DMS

PrimaStasys Inc

Example: /etc/pam.d/login

```
#%PAM-1.0
auth sufficient    pam_unix2.so    nullok
auth sufficient    pam_winbind.so use_first_pass use_authtok
auth required      pam_securetty.so
auth required      pam_nologin.so
auth required      pam_env.so
auth required      pam_mail.so
account sufficient pam_unix2.so
account sufficient pam_winbind.so user_first_pass use_authtok
password required  pam_pwcheck.so nullok
password sufficient   pam_unix2.so nullok use_first_pass use_authtok
password sufficient   pam_winbind.so  use_first_pass use_authtok
session sufficient pam_unix2.so    none
session sufficient pam_winbind.so  use_first_pass use_authtok
session required   pam_limits.so
```

Username Mapping

PrimaStasys Inc

- Control file is */etc/samba/smbusers*

```
# This file allows you to map usernames from the
clients to the server.
# Unix_name = SMB_name1 SMB_name2 ...
#
# Cf. section 'username map' in the manual page of
# smb.conf for more information.

root = administrator admin
;nobody = guest pcguest smbguest
billp = “William Porter”
maryo = mobrien
horris = “WIZARDS\Horri Sams”
```

Group Mapping

PrimaStasys Inc

- Makes use of the *net groupmap* tool:

```
frodo:~ # net groupmap list

Domain Admins (S-1-5-21-726309263-4128913605-1168186429-512)
    -> Domain Admins
Domain Users (S-1-5-21-726309263-4128913605-1168186429-513)
    -> Domain Users
Domain Guests (S-1-5-21-726309263-4128913605-1168186429-514)
    -> Domain Guests
Print Operators (S-1-5-21-726309263-4128913605-1168186429-550)
    -> Print Operators
Backup Operators (S-1-5-21-726309263-4128913605-1168186429-551)
    -> Backup Operators
Replicator (S-1-5-21-726309263-4128913605-1168186429-552)
    -> Replicator
Domain Computers (S-1-5-21-726309263-4128913605-1168186429-553)
    -> Domain Computers
```

Access Control Points

PrimaStasys Inc

- Share Definition
  - In share stanza in *smb.conf*
- File System Permissions
- Share Permissions
  - Set using MMC or NT4 Domain Server Manager
- Windows NT/2K ACLs
  - Warning Will Robinson! Danger!

CIFS Security - ACLs

PrimaStasys Inc

- Access Control Lists
  - Much abused
    - Need to understand HOW ACLs will be backed up and copied to other servers
    - Satisfy yourself that there is no other solution before using ACLs

Network Rights and Privileges

PrimaStasys Inc

- Set using the *net rpc rights grant* facility:

```
frodo: net -S MASSIVE  -U root%not24get rpc rights grant \
        "MEGANET2\Domain Admins" SeMachineAccountPrivilege \
        SePrintOperatorPrivilege SeAddUsersPrivilege \
        SeDiskOperatorPrivilege SeRemoteShutdownPrivilege

Successfully granted rights.
```

Verify Rights & Privileges

PrimaStasys Inc

```
frodo # net rpc rights list accounts -Uroot%not24get

MEGANET2\bobj
SeMachineAccountPrivilege

...

BUILTIN\Backup Operators
No privileges assigned

BUILTIN\Server Operators
No privileges assigned

BUILTIN\Administrators
No privileges assigned

Everyone
No privileges assigned

MEGANET2\Domain Admins
SeMachineAccountPrivilege
SePrintOperatorPrivilege
SeAddUsersPrivilege
SeRemoteShutdownPrivilege
SeDiskOperatorPrivilege
```

Future Developments

PrimaStasys Inc

- Samba-3 Development will continue
  - Life Cycle – at least 2 years
  - Major improvements planned
    - Winbind scalability
    - Management
      - UNIX processes via Windows MMC
      - Accounts
- Samba-4 development advancing rapidly
  - Will be given major attention at SambaXP 2005

See: http://www.sambaxp.org

Finding Information

PrimaStasys Inc

- ALWAYS Visit the Source!
  - 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

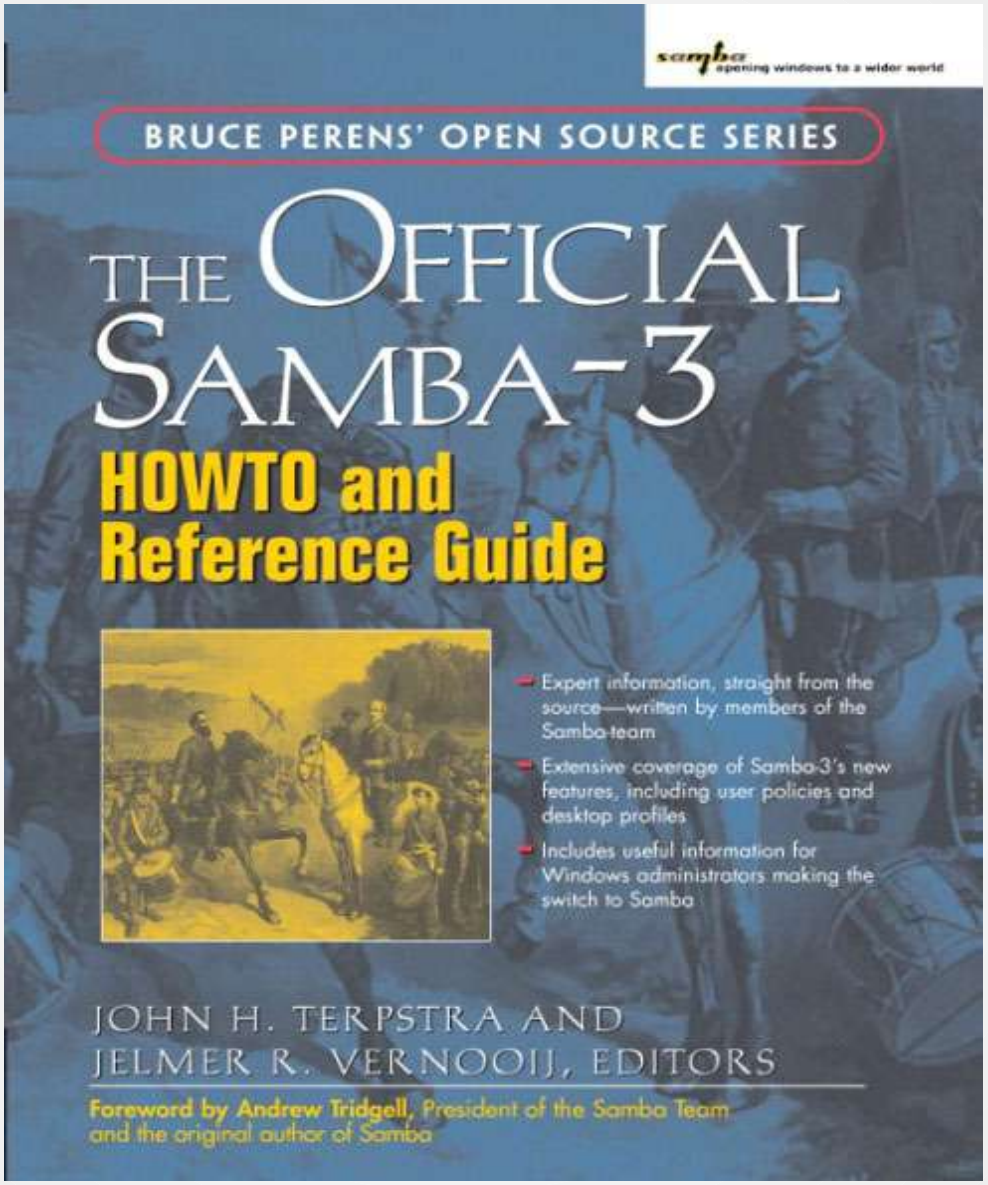
Documentation

PrimaStasys Inc

- Official (means part of Samba sources)
  - The Official Samba-3 HOWTO and Reference Guide
    - ISBN: 0131453556
    - Open source version:
      Samba-HOWTO-Collection (PDF and HTML)
  - Samba-3 by Example
    - ISBN: 0131472216
    - Open Source version: Samba-Guide (PDF and HTML)
  - Man Pages
  - Contributed Presentations, etc. on Samba.Org

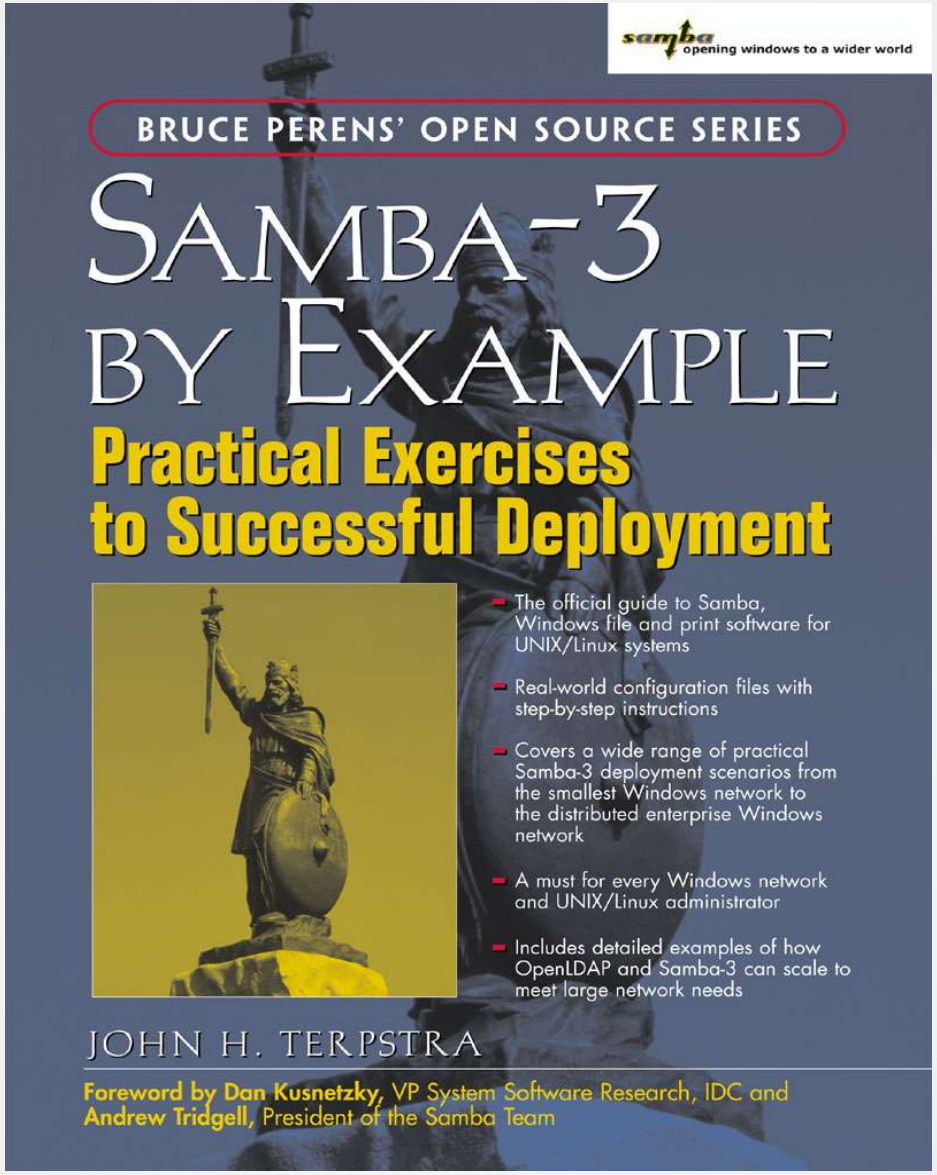
The Official Samba-3 HOWTO

PrimaStasys Inc



Samba-3 by Example

PrimaStasys Inc



Documentation

PrimaStasys Inc

- Unofficial
  - There is a lot of it
  - Most is of high quality
  - Much is out of date
    - It is time consuming to keep documentation up to date

More Documentation

PrimaStasys Inc

- Many books
  - See: http://www.samba.org/samba/books.html
- Samba-Team encourage unofficial source work!
  - There is nothing exclusive in the title: "Official Documentation"

Q&A / Feedback

PrimaStasys Inc

END -» FINISHED -» DONE -» Questions