

The Samba-3: Overview, Authentication, Integration

John H Terpstra, CTO
PrimaStasys Inc.

jht@PrimaStasys.Com or jht@samba.org

About the speaker

- 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)
 - [OpenLDAP by Example](#), ISBN: 0131488732 (Nov 2004)
 - More in production

Agenda

- Overview of Samba-3.0.x
- Samba Administration
- CIFS Security
 - Security Modes / Models
 - Backend Choices
 - Infrastructure Tools
- Integrating Samba-3 into MS Windows Networks
 - NT4 Style Domains, Active Directory
- Finding Information

- Components:
 - *smb.conf* file controls behavior
 - ◆ *smbd*, *nmdbd*, *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

- 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
 - ♦ Windows Administration Tools

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

•CIFS Security - ACLs

- 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

- 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

- 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
```

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

- 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

- 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)



JOHN H. TERPSTRA 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
```

- 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-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 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

- 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)

- 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

- 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

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

•Backends New to 3.0.x

- *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 smbpasswd *OR* LDAP
 - Now it is natively capable of any backend

- Experimental / Special Interest Backends
 - XML
 - SQL

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

- 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

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

- 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
```


- 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 login only)
 - nss_ldap (for ID resolution)

```
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

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

- System Control
 - ◆ shutdown
 - ◆ abort shutdown
 - ◆ etc.



Cross Domain Identity Management

- 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

- 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
```

```
...
```

- 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
```

- 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

- 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)

- 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
```

- 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

NOTE:

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

- 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
```

- 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

/etc/nsswitch.conf

```
# /etc/nsswitch.conf
```

```
passwd:          files winbind
```

```
group:           files winbind
```

```
hosts:           files dns wins
```

Example: */etc/pam.d/login*

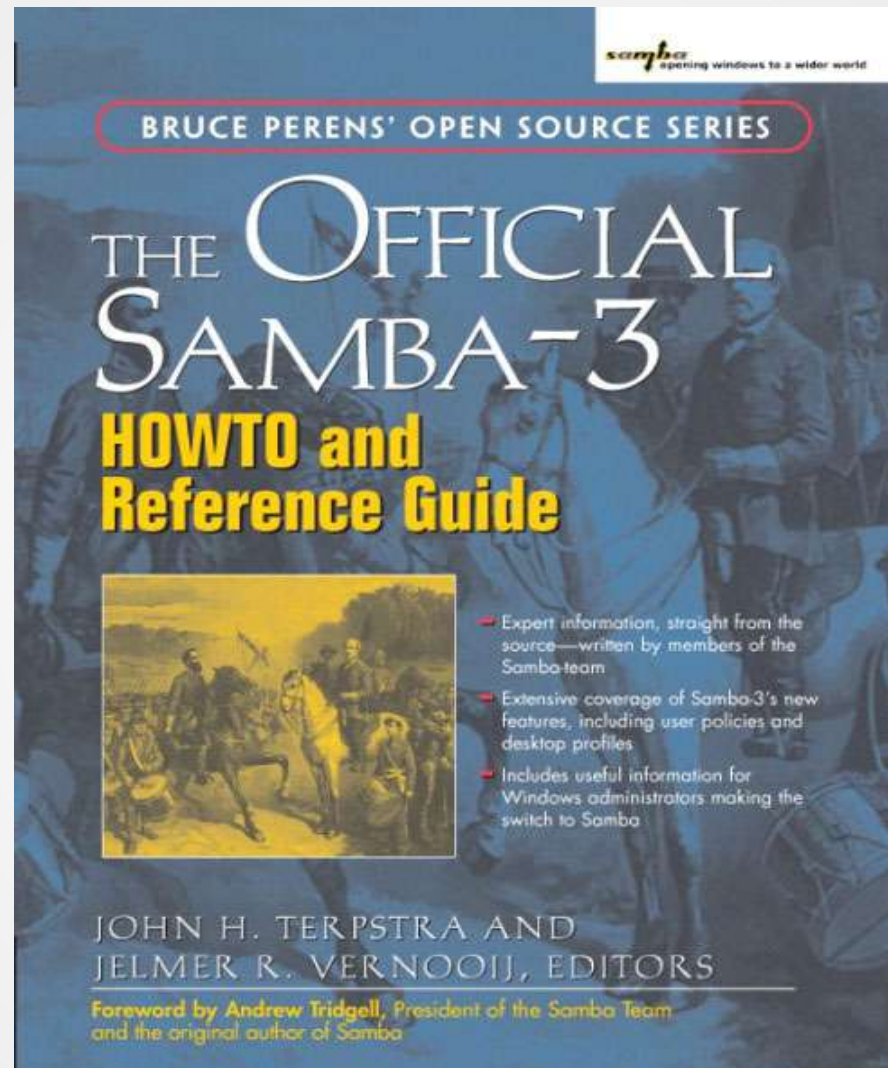
#%PAM-1.0

<i>auth sufficient</i>	<i>pam_unix2.so nullok</i>
<i>auth sufficient</i>	<i>pam_winbind.so use_first_pass use_authtok</i>
<i>auth required</i>	<i>pam_securetty.so</i>
<i>auth required</i>	<i>pam_nologin.so</i>
<i>auth required</i>	<i>pam_env.so</i>
<i>auth required</i>	<i>pam_mail.so</i>
<i>account sufficient</i>	<i>pam_unix2.so</i>
<i>account sufficient</i>	<i>pam_winbind.so user_first_pass use_authtok</i>
<i>password required</i>	<i>pam_pwcheck.so nullok</i>
<i>password sufficient</i>	<i>pam_unix2.so nullok use_first_pass use_authtok</i>
<i>password sufficient</i>	<i>pam_winbind.so use_first_pass use_authtok</i>
<i>session sufficient</i>	<i>pam_unix2.so none</i>
<i>session sufficient</i>	<i>pam_winbind.so use_first_pass use_authtok</i>
<i>session required</i>	<i>pam_limits.so</i>

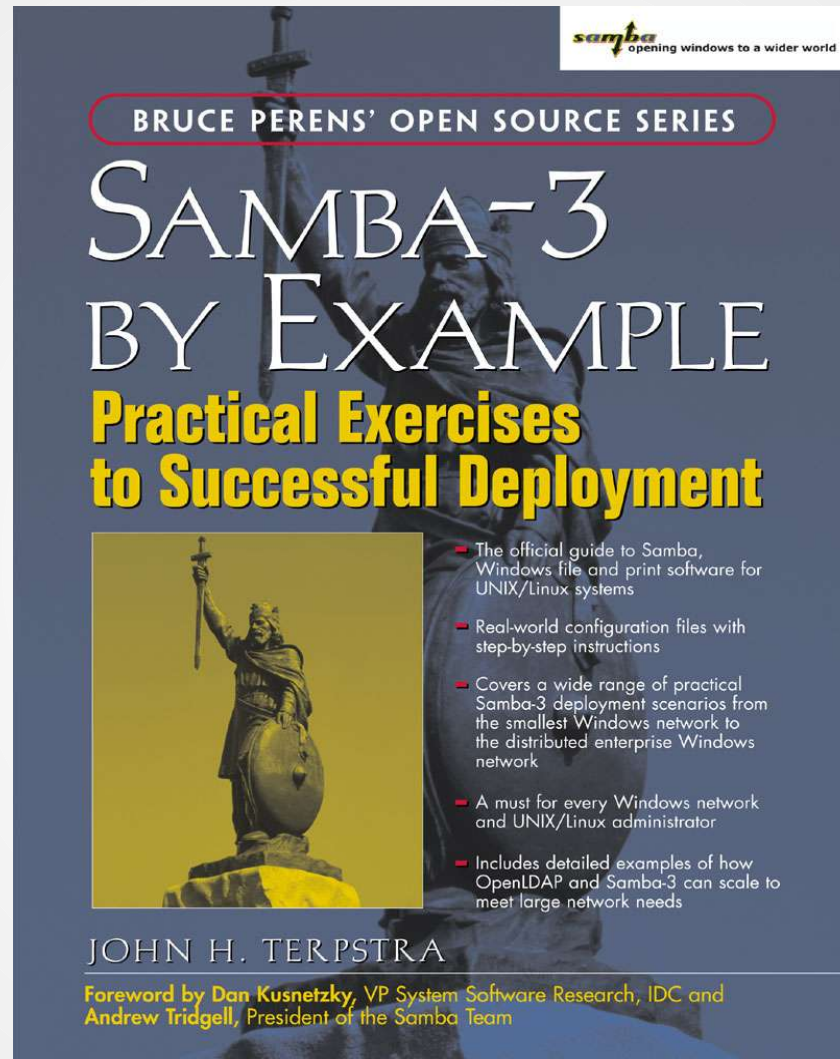
- ALWAYS Visit the Source!
 - <http://www.samba.org/samba/>
 - Documentation
 - ◆ Man pages & Official Books
 - ◆ Listing of published books
 - Mailing Lists
 - ◆ General, Technical
 - Bug Tracking System
 - ◆ <http://bugzilla.samba.org/>
 - Other Sources

- 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



Samba-3 by Example



- 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

- 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

END ->> FINISHED ->> DONE ->> Questions