

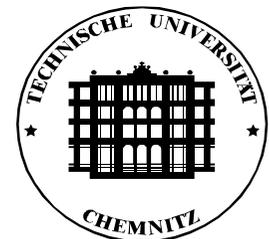
# **samba** 2.0

## **Wieviel NT braucht der Mensch ?**

**Eigenschaften und Einsatzmöglichkeiten der neuen Samba-Release**

**Frank Schubert, Frank Schöniger**  
**Technische Universität Chemnitz**  
**Fakultät für Informatik**

**30. März 1999**



# Überblick

---

- 1. Was ist Samba ?**
- 2. Neues in Samba 2.0**
- 3. Samba als Primary Domain Controller (PDC)**
- 4. Resümee**
- 5. Demonstration - Samba als PDC unter Linux**

# 1. Was ist Samba ?

---

## Samba:

- Implementation des SMB/CIFS-Protokolls für UNIX-Systeme
- Server und Client
  - UNIX stellt File- und Druckdienste für SMB-Clients bereit
  - Nutzung (anderer) SMB-Server unter UNIX
- frei verfügbar (GNU Public License)
- aktuelle Version: 2.0.3
- Quelle: <http://www.samba.org>

# 1. Was ist Samba ?

---

## Protokolle und Dienste:

- SMB -- Server Message Block
  - Basisprotokoll, entwickelt von Microsoft und Intel (u.a.)
  - geteilte Benutzung von Ressourcen im Netz  
(Files, Drucker, Kommunikationseinrichtungen etc.)

neu: **CIFS -- Common Internet File System**

- öffentliche Version von SMB entwickelt von MS und anderen Firmen
- ausgerichtet auf Internet („*internet friendly SMB version*“)
- Quelle: <http://www.microsoft.com/workshops/networking/cifs>

- NBT -- NetBIOS over TCP/IP
  - Auflösung „flacher“ NetBIOS-Namen in IP-Adressen
  - WINS -- Windows Internet Name Service  
(name serving and browsing)

# 1. Was ist Samba ?

---

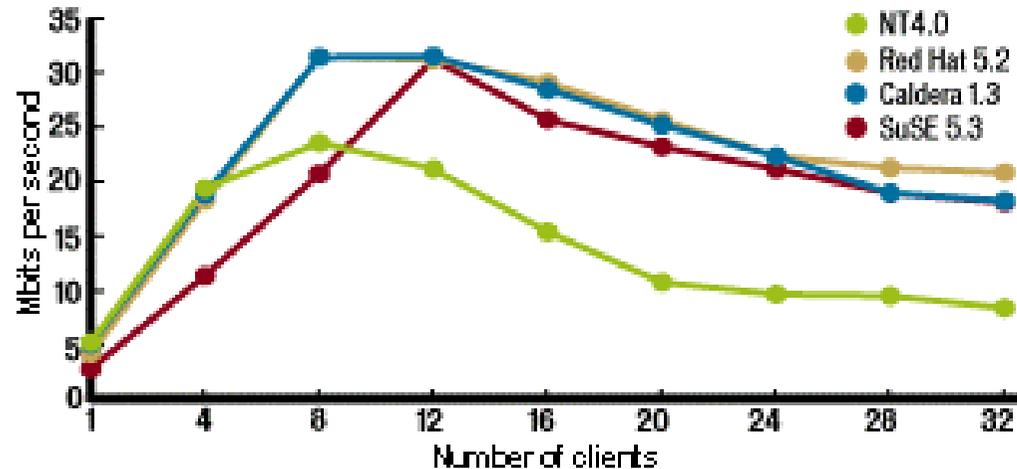
## Komponenten:

- `smbd, nmbd` zentrale Serverprozesse
- `smbclient` ftp-like SMB-Zugang
- `testparm` Test des Konfigurationsfiles (*[smb.conf](#)*)
- `smbstatus` Anzeigen der vom `smbd` aktuell verwalteten Verbindungen
- `nmblookup` Abfrage von NetBIOS-Namen
- `smbpasswd` Ändern von SMB-verschlüsselten Paßwörtern (lokal und entfernt)
- etc.

## 2. Neues in Samba 2.0

- **Performanceverbesserungen**

- bereits seit Version 1.9.18 sind „opportunistic locks“ verfügbar
- NetBench 5.0:



- **Korrektheit**

- Unterstützung NT-spezifischer SMB-Requests  
(64 bit view auf Filesystem, Handling großer Files)

## 2. Neues in Samba 2.0

---

- **Verbesserung der Portabilität**

- Nutzung von *GNU autoconf* → kein Editieren der Makefiles von Hand

- **SWAT -- Samba Web Administration Tool**

- Web-basiertes Werkzeug zur Konfiguration von Samba

- **Domain-Client Funktionalität**

- Samba kann Dienste eines NT PDC nutzen, um Nutzer zu authentifizieren

- **Aktualisierung der Dokumentation**

- sämtliche Dokumentationen wurden aktualisiert
  - Dokumentenformat erlaubt Generierung von HTML, SGML, Text, Man-Page-Format (Standard: HTML und Man-Pages)

# 3. Samba als PDC

---

## Primary Domain Controller (PDC):

- für die Verwaltung einer NT-Domain verantwortlicher Server (NT-Server)

## NT-Domain:

- zusammengehörige Einheit von Rechnern und Benutzern mit „zentraler Sicherheitsverwaltung“

!! Unterschied zur Arbeitsgruppe (Workgroup)

## *PDC-Funktionalität in Samba ?*

- ursprünglich für das Release 2.0 angekündigt
- tatsächlich jedoch nicht enthalten, immer noch im Experimentierstadium
- verfügbar als Samba 2.1--prealpha (via cvs)
- für nächste Release versprochen

→ *Inwieweit wird Samba NT-Server vollständig ersetzen können ???*

# 3. Samba als PDC

---

## Grundlegende Aufgaben eines PDC

- Verwaltung von Accounts für Computer und Benutzer
- Verwaltung von Benutzergruppen
- Authentifizierung
- Accounting
- File- und Printservicing
- Verwaltung von server-basierten Benutzerprofilen
- Zentrale Vorgabe von Systemrichtlinien (Policies)
  
- Lizenzmanagement
- Softwareverteilung

→ **Was davon kann Samba ???**

# 3. Samba als PDC

---

## *Verwaltung von Accounts für Computer und Benutzer*

- einheitliche Verwaltung von UNIX- und NT-Nutzern
- Computer-Accounts durch spezielle Einträge in /etc/passwd
- Arbeit mit Paßwortverschlüsselung → spezielle Datei für Authentifizierung (smbpasswd)  
(bei Anmeldung als NT-Domain-User immer erforderlich)

## *Verwaltung von Benutzergruppen*

- Abbildung auf UNIX-Nutzergruppen
- spezielle „map“-Files für Kennzeichnung von lokalen und Domain-Administratoren

# 3. Samba als PDC

## Authentifizierung beim PDC

- Authentifizierungsinformation auf Server (smbpasswd)  
`des_encrypt(md4(unicode(password)), well_known_des_key)`

- Challenge-Response-Verfahren

**Server:** challenge (8 byte random data)

**Client:** md4(unicode(password)) => 16 Byte  
+ 5 Byte (null) => 21 Byte == 168 Bit  
== 3 \* 56 Bit (--> 3 DES-keys)

```
response <= des_encrypt(challenge, key1)+  
            des_encrypt(challenge, key2)+  
            des_encrypt(challenge, key3)
```

**Server:**

```
des_decrypt(Auth.-info aus smbpasswd) => md4(unicode(password))  
split(response) => (resp1, resp2, resp3)  
challenge1 <= des_decrypt(resp1, key1)  
challenge2 <= des_decrypt(resp1, key2)  
challenge3 <= des_decrypt(resp1, key3)  
if(challenge == (challenge1 & challenge2 & challenge3))  
    client authentifiziert  
    senden eines Zugriffstokens (incl. Security ID)
```

- Samba liefert korrekte Implementation des Authentifizierungsprotokolls
- separate Verwaltungsdatei (smbpasswd) notwendig (*!! nur für root lesbar !!*)
- entgegen allen Gerüchten: Samba funktioniert mit NT4.0 SP3 und SP4 !!

# 3. Samba als PDC

---

## Accounting

- Protokollierung in spezielles log-File (smb.log)
- wünschenswert: direktes logging nach /etc/wtmp

## File- und Printservicing

- einzige Einschränkung: automatisches Laden von Druckertreibern vom Server unter NT ist noch in Entwicklung

## Verwaltung von server-basierten Benutzerprofile

- Benutzerprofil: Vielzahl nutzerspezifischer Einstellungen (vom Startmenü bis zum IE-Cache)
- Samba:
  - a) im Home-Verzeichnis des Benutzers
    - smb.conf: *logon path = \\%N%\%U\profile*
    - Probleme bei aufeinanderfolgender Anmeldung versch. Nutzer (altes share [homes] noch verbunden)
  - b) spezielles Profile-Verzeichnis (separates share [profiles])
    - smb.conf: *logon path = \\%N%\profiles\%U*

# 3. Samba als PDC

---

## **Zentrale Vorgabe von Systemrichtlinien ( Policies )**

- Allgemeingültige Einstellungen und Nutzungsrestriktionen
- spezielles Verzeichnis (*share [NETLOGON]*) auf dem Server
- File *NTconfig.POL* enthält Policies
- kann mit Policy-Editor (*poledit.exe*) von NT-Workstation aus bearbeitet werden

## **Softwareverteilung und Lizenzmanagement**

- bisher nicht unterstützt
- Problem: Oft werden spezielle, auf dem Server arbeitende Systeme benötigt (z.B. Saberlan, SMS). → Nicht unter UNIX verfügbar !!

# 3. Samba als PDC

---

## *Anmerkung zur Administration*

- traditionell: *smb.conf*
- neu ab Samba 2.0: *SWAT*

alternativ:

### *Einsatz von Werkzeugen auf den NT-Clients*

- Policy-Editor und Ändern von Nutzerpaßwörtern o.k.
- User- und Server-Manager funktionieren erst ansatzweise

# 4. Resümee

---

- ***Samba ist ein wichtiger Beitrag zur Integration von UNIX- und MS- Welten***
  - Verringerung des Administrationsaufwandes
  - Kostenreduktion
  - einheitliche Umgebung für die Benutzer
- ***Einsatz als PDC in kleineren Netzen durchaus sinnvoll***
- ***fast täglich neue Fortschritte zu verzeichnen !!!***

# 5. Demonstration - Samba als PDC unter Linux

---

## Installation und Konfiguration von Samba als PDC unter Linux

- Source-Code vom cvs-Server der Samba-Entwickler holen ([www.samba.org](http://www.samba.org))
- mit *configure* Makefiles erzeugen und compilieren, *make install*
- Samba wird in */usr/local/samba* installiert (*/usr/local/samba/bin* in PATH eintragen!)
  - *smb.conf* in */usr/local/samba/lib/*
  - *smbpasswd* in */usr/local/samba/private*
- Eintrag in */etc/inetd.conf* für den Aufruf von *swat*
- evtl. Eintrag in */etc/inetd.conf/* für den Aufruf von Samba (*smbd* und *nmbd*)
  - besser: *smbd* und *nmbd* als Daemon starten (Performance)
- *smb.conf* erzeugen (per Hand oder mit *swat*)
  - Freigaben für die home-Verzeichnisse der Nutzer (share *[HOMES]*)
  - share *[NETLOGON]*
  - share *profiles*
  - Drucker

# 5. Demonstration - Samba als PDC unter Linux

---

## Einbindung der NT-Arbeitsstationen

- Anlegen eines Computeraccounts für jeden Client im `/etc/passwd` - File des Samba-Servers:  
nutzernamen = Computernamen+`$`; kein Paßwort; keine login-Shell  
`haendel$:x:43:100::/tmp:/bin/false`
- Eintragen des Paßwortes für den Computeraccount (=Computernamen in Kleinbuchstaben)  
`smbpasswd -a -m computernamen`
- alle Unix-Nutzer die in der NT-Domain arbeiten dürfen, müssen explizit in `smbpasswd` eintragen  
`smbpasswd -a nutzer`
- Erstellen der System -Policies; auf dem Share `NETLOGON` hinterlegen
- auf den NT-Maschinen in der Netzwerksteuerung die entsprechende Domain eintragen  
(„*Willkommen in der Domain XYZ*“)
- Die NT-Maschine ist nun nach dem Neustart Mitglied der entsprechenden Domain und startet automatisch mit den hinterlegten Policies. Alle entsprechend eingetragenen Nutzer haben nun Zugang zu der NT-Maschine