

# Projektpräsentation

## NIS/LDAP-Migration mit Samba-Integration

Christian Wenke, OFFIS, 2003

# Überblick

- Ausgangssituation
- Problemstellung
- Anforderungen
- Alternativen
- Kosten-Nutzen-Analyse
- Soll-Konzept
- Hardware-Auswahl LDAP-Server
- Realisierung LDAP-Server
- Realisierung Samba Domain-Controller
- Realisierung der Clients
- PAM / NSS
- Resumée

# Ausgangssituation

- OFFIS FuE-Bereich HS hat insgesamt ca. 50 Mitarbeiter
- Systeme:
  - Solaris (Remote-Workstations & Server, 18 Systeme)
  - Linux (Workstations, 26 Systeme)
  - Windows 2000 (Workstations, 16 Systeme)
- Solaris: NIS
- Linux: lokale Arbeitsplatzrechner mit lokalem Login
- Windows 2000: lokale Arbeitsplatzrechner mit lokalem Login
- Abteilungsserver: SUN Enterprise 250 mit Solaris/Samba als File- und NIS/NFS-Server

# Problemstellung

- Logins verteilt und nicht konsistent → unübersichtlich
- dadurch hoher Administrationsaufwand → hohe TCO
- „Unkomfortables“ Arbeiten für den Mitarbeiter, da evtl. verschiedene Logins und Passwörter vorhanden
- Rechner für neue MA zwar klonbar, aber lokale Accounts einzurichten
- dadurch höherer Administrationsaufwand auch bei neuen Rechnern

## Lösung:

zentrale Benutzerverwaltung für alle Accounts (unter Solaris, Linux und Windows)

# Anforderungen

- zentrale Benutzerverwaltung
- Client-seitige Unterstützung für Solaris, Linux und Windows
- Verwaltung nach Möglichkeit auch von allen drei Betriebssystemen aus
- Sicherheit der Passwörter bei der Übertragung und gegenüber angemeldeten Benutzern

# Alternativen

- Microsoft Active Directory
- Sun ONE Directory Server
- NIS
- OpenLDAP
- Samba als Domain Controller

# Kosten-Nutzen-Analyse (1)

## Anschaffungs- und Betriebs-Kosten:

Lösung	Kosten			Gesamt
	Anschaffung	Einführung	Betrieb (2 Jahre)	
Active Directory	475 €	2560 € ca. 4 Tage	3840 € ca. 2 Std./Monat	<b>6875 €</b>
Sun ONE Directory Server	212 €	3200 € ca. 5 Tage	3840 € ca. 2 Std./Monat	<b>7252 €</b>
NIS	0 €	1280 € ca. 2 Tage	5760 € ca. 3 Std./Monat	<b>7040 €</b>
OpenLDAP / Samba	0 €	2560 € ca. 4 Tage	5760 € ca. 3 Std./Monat	<b>8320 €</b>
alter Zustand	0 €	0 €	19200 € ca. 10 Std./Monat	<b>19200 €</b>

Zugrunde gelegter Stundensatz: 80 €

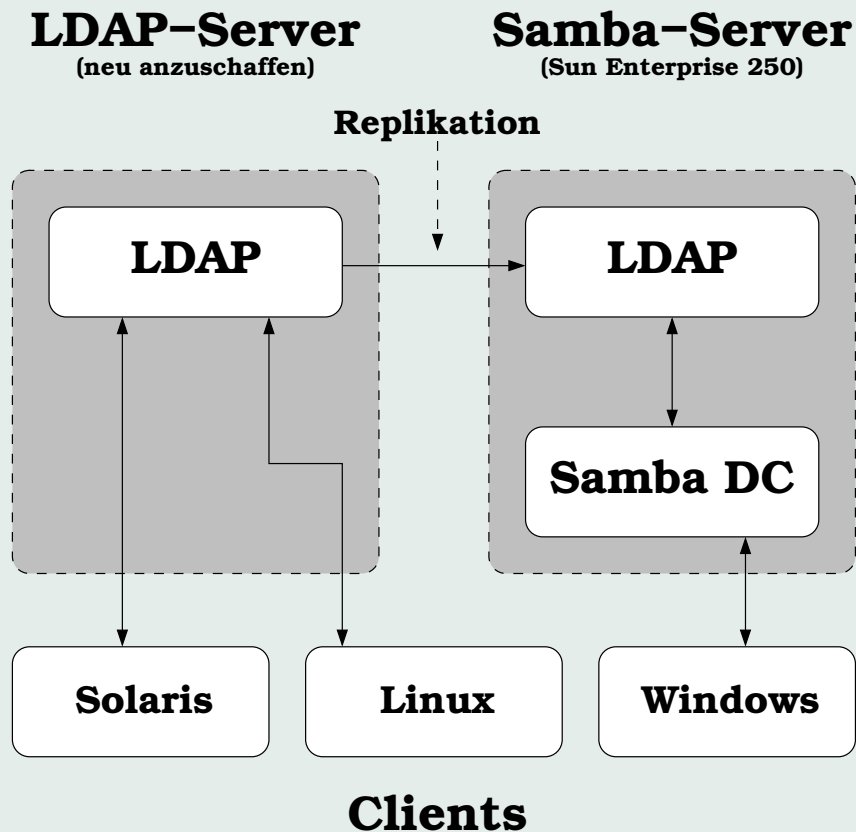
## Kosten-Nutzen-Analyse (2)

Bewertung der Alternativen:

Kriterium	Gew.	Max. Pkt.	MS ADS	NIS	Sun ONE DS	OpenLDAP / Samba DC	alter Zust.
Kosten Anschaffung (SW)	7	10	4	10	6	10	10
Kosten Einführung	4	10	8	6	6	4	10
Kosten Betrieb	10	10	8	7	8	8	2
Sicherheit	10	10	10	3	10	10	3
Flexibilität	5	10	2	4	4	8	2
Plattformunabhängigkeit	6	10	2	6	4	8	8
Herstellerunabhängigkeit	6	10	2	8	2	8	6
Client-Abdeckung	10	9	3	6	9	9	3
<b>Summe</b>		<b>570</b>	<b>304</b>	<b>358</b>	<b>392</b>	<b>492</b>	<b>284</b>



# Soll-Konzept



# Hardwareauswahl LDAP-Server

## Technische Rahmendaten:

- Sun SPARC Maschine
- SCSI-System
- 9 GB HDD
- 512 MB RAM
- 500 MHz CPU
- 19-Zoll Gehäuse

## konkret in Frage kommende Systeme:

- kleinere Systeme der „Sun Fire“ Reihe (z.B. Sun Fire V120)
- kleinere Systeme der „Sun Netra“ Reihe (z.B. Sun Netra 120 oder Netra X1)

# Realisierung LDAP-Server

## Testsystem:

- Debian GNU/Linux 3.0 (stable)
- OpenLDAP 2.0.23
- LDAP-Schemas: core, cosine, nis, inetorgperson, samba
- TLS/SSL
- ACLs (bes. für Attribute: userPassword, ImPassword, ntPassword)
- Migration der Accounts mit „MigrationTools“ von padl.com
- MigrationTools mussten angepasst werden (objectClass: sambaAccount)

# Realisierung Samba Domain-Controller

## Testsystem:

- Selber Rechner wie LDAP-Server
- Samba 2.2.3a
- Konfiguration als Domain-Controller
- Roaming Profiles, Netlogon
- Eintragen des LDAP-Servers
- Wichtig: Eindeutige und korrekte **rids**

# Realisierung der Clients

## Solaris, Linux:

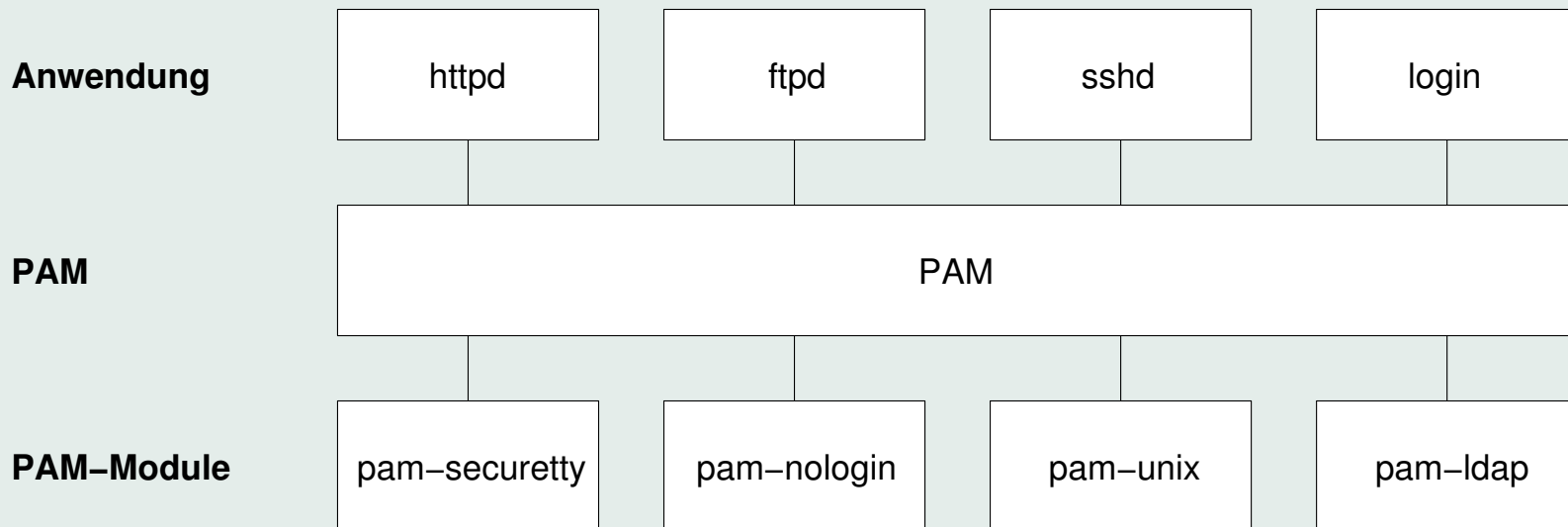
- Authentifizierung → PAM
- Namensauflösung → NSS
- Verwendung der PAM/NSS Backends von padl.com

## Windows2000:

- Rechner als Domänenmitglied über Samba Server
- Authentifikation und Namensauflösung über SMB

# PAM / NSS

- PAM → Pluggable Authentication Modules
- NSS → Name Service Switch
- Modulare Systeme zur Authentifikation bzw. Namensauflösung



# Resumée

## Probleme:

- Projektdauer von 35 Stunden etwas zu knapp
- Ausfall der Festplatte des Testservers
- Software kompilieren unter Solaris nicht ganz einfach

## weitere Entwicklung:

- Produktiveinsatz
- Integration weiterer Dienste
- langfristiger Ausbau zur Single-Sign-On Lösung

Ich danke Ihnen für Ihre  
Aufmerksamkeit